Microsoft System Center 2012 R2

Technical Documentation for System Center 2012 R2 Virtual Machine Manager

Microsoft Corporation

Published: July 14, 2014

Authors

Anat Kerry, John Downing, and Rayne Wiselman

Applies To

System Center 2012 – Virtual Machine Manager

System Center 2012 Service Pack 1 (SP1) – Virtual Machine Manager (VMM)

System Center 2012 R2 Virtual Machine Manager

Feedback

Send suggestions and comments about this document to sc2012docs@microsoft.com.

Copyright

Revision History

Release Date	Changes
October 17, 2013	Initial release of this document.
November 1, 2013	Minor updates to this guide.
November 7, 2013	Minor change to Remote Console figure. No change to technical information.
November 14, 2013	Added a new topic that explains how to configure Windows Azure Pack to use the Remote Desktop Gateway.
November 27, 2013	• Updated support for XenServer 6.1. • Updates to WSUS content to reflect changes in System Center 2012 R2 Virtual Machine Manager.
December 4, 2013	Added a note about creating a Windows Server 2012 R2 Hyper-V cluster from VMM running on Windows Server 2012 in the topic Creating and Modifying Hyper-V Host Clusters in VMM.
December 11, 2013	Updated system requirements for Hyper-V hosts.

Release Date	Changes
March 10, 2014	Minor technical and grammatical updated to the guide. New topic, Cross-Forest Domain Trusts in VMM.
April 24, 2014	1. 0. 1. Added port information for SMB under Ports and Protocols for VMM 2. Added step about verifying V2V at How to Convert VMware Virtual Machines to Hyper-V 3. Added more information about prerequisites for How to Create a Guest Cluster by Using a Service Template in VMM 4. Added note about issues with drag and drop not working in How to Migrate a Virtual Machine in VMM 5. Added an explanation about what RemoteConsoleConnect.pfx is for in Remote Console in System Center 2012 R2
July 14, 2014	• System Requirements for System Center 2012 R2 Virtual Machine Manager has been moved to a new location: System Requirements for System Center 2012 R2 • We now recommend not using AlwaysOn in Microsoft SQL Server. If you use AlwaysOn, and you are running an asynchronous commit mode, the replica of the database can be out of date for a period of time after each commit. This can make it appear as if the database were back in time which might cause loss of customer data, inadvertent disclosure of information, or possibly elevation of privilege.

Contents

Virtual Machine Manager 17

Getting Started with System Center 2012 - Virtual Machine Manager 17
- Overview of System Center 2012 - Virtual Machine Manager 17
- What's New in System Center 2012 - Virtual Machine Manager 23
  - What's New in VMM in System Center 2012 R2 23
  - What's New in VMM in System Center 2012 SP1 27
  - What's New in System Center 2012 - Virtual Machine Manager 39
- Resources for System Center 2012 - Virtual Machine Manager 42

Deploying System Center 2012 - Virtual Machine Manager 44
- Cross-Forest Domain Trusts in VMM 44
- Pre-Creating the VMM Database 44
- Installing System Center 2012 - Virtual Machine Manager 45
  - Installing a VMM Management Server 46
    - How to Install a VMM Management Server 46
  - Installing and Opening the VMM Console 50
    - How to Install the VMM Console 50
    - How to Connect to a VMM Management Server by Using the VMM Console 52
  - Installing and Opening the VMM Self-Service Portal 52
    - How to Install the VMM Self-Service Portal 53
    - How to Open the VMM Self-Service Portal 55
  - How to Uninstall VMM 56
  - Specifying a Service Account for VMM 58
  - Configuring Distributed Key Management in VMM 58
  - How to Upgrade from the Evaluation Version of VMM 60
  - Installing VMM from a Command Prompt 60
- Installing a Highly Available VMM Management Server 71
  - How to Install a Highly Available VMM Management Server 72
  - How to Install a VMM Management Server on an Additional Node of a Cluster 75
  - How to Connect to a Highly Available VMM Management Server by Using the VMM Console 77
  - How to Uninstall a Highly Available VMM Management Server 78

Upgrading System Center 2012 - Virtual Machine Manager 80
- Upgrading to VMM in System Center 2012 R2 80
  - Planning an Upgrade of Virtual Machine Manager 82
    - Planning Considerations for Upgrading VMM 83
      - Choosing Service Account and Distributed Key Management Settings During an Upgrade 85

How to Move a VMM Database to Another Computer ... 87
Performing a VMM Upgrade ... 87
Tasks to Perform Before Beginning the VMM Upgrade ... 88
How to Perform VMM Upgrade ... 89
How to Upgrade a High Availability VMM Management Server ... 91
How to Upgrade VMM on a Different Computer ... 94
Performing Post-Upgrade Tasks in VMM ... 95
How to Reassociate a Host or Library Server ... 96
How to Update the VMM Agent ... 97
How to Restore Windows Azure Hyper-V Recovery Manager Provider ... 98
Troubleshooting a VMM Upgrade ... 98
Upgrading to VMM in System Center 2012 SP1 ... 99
Planning an Upgrade to VMM in System Center 2012 SP1 ... 100
Prerequisites for Upgrading to VMM in System Center 2012 SP1 ... 100
Planning Considerations for Upgrading to VMM in System Center 2012 SP1 ... 100
Choosing Service Account and Distributed Key Management Settings During an Upgrade ... 103
How to Move a VMM Database to Another Computer ... 105
Performing an Upgrade to VMM in System Center 2012 SP1 ... 105
Tasks to Perform Before Beginning the Upgrade to VMM in System Center 2012 SP1 ... 105
How to Upgrade to VMM in System Center 2012 SP1 ... 106
How to Upgrade to a Highly Available VMM Management Server ... 109
How to Upgrade to VMM on a Different Computer ... 112
Performing Post-Upgrade Tasks in VMM ... 113
How to Reassociate a Host or Library Server ... 114
How to Update the VMM Agent ... 115
Troubleshooting a VMM Upgrade ... 116
Upgrading to System Center 2012 - Virtual Machine Manager ... 116
Planning an Upgrade to System Center 2012 - Virtual Machine Manager ... 117
Prerequisites for Upgrading to VMM ... 117
Planning Considerations for Upgrading to VMM ... 120
Choosing Service Account and Distributed Key Management Settings During an Upgrade ... 124
How to Move a VMM Database to Another Computer ... 126
Performing an Upgrade to System Center 2012 - Virtual Machine Manager ... 127
Tasks to Perform Before Beginning the Upgrade to VMM ... 127
How to Upgrade to System Center 2012 - Virtual Machine Manager from VMM 2008 R2 SP1 ... 128
How to Upgrade to a Highly Available VMM Management Server ... 130
How to Upgrade a VMM Console ... 133
How to Upgrade the VMM Self-Service Portal ... 134
How to Upgrade to VMM on a Different Computer ... 135
Performing Post-Upgrade Tasks in VMM ... 135

How to Reassociate a Host or Library Server ... 137
How to Update the VMM Agent ... 138
Troubleshooting a VMM Upgrade ... 139

Administering System Center 2012 - Virtual Machine Manager ... 140
Configuring Fabric Resources in VMM ... 140
Preparing the Fabric in VMM ... 141
Preparing the Fabric Scenario in VMM ... 142
Creating Host Groups in VMM ... 145
How to Create a Host Group Structure in VMM ... 146
How to Configure Host Group Properties in VMM ... 147
Configuring the VMM Library ... 149
How to Add a VMM Library Server or VMM Library Share ... 155
How to Associate a VMM Library Server with a Host Group ... 158
How to Add File-Based Resources to the VMM Library ... 159
How to Create or Modify Equivalent Objects in the VMM Library ... 160
How to View and Remove Orphaned Resources in VMM ... 163
Configuring Networking in VMM ... 164
Common Scenarios for Networking in VMM in System Center 2012 ... 165
Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2 ... 166
Configuring Logical Networking in VMM Overview ... 175
Configuring Logical Networking in VMM Illustrated Overview ... 184
How to Configure Global Network Settings in VMM ... 186
How to Create a Logical Network in VMM ... 190
How to Modify or Delete a Logical Network in VMM ... 195
How to Create IP Address Pools for Logical Networks in VMM ... 196
How to Create Custom MAC Address Pools in VMM ... 200
How to Release Inactive IP or MAC Addresses in VMM ... 203
How to Add an IPAM Server in VMM in System Center 2012 R2 ... 204
Configuring Load Balancing in VMM Overview ... 208
How to Add Hardware Load Balancers in VMM ... 213
How to Create VIP Templates for Hardware Load Balancers in VMM ... 216
How to Create VIP Templates for Network Load Balancing (NLB) in VMM ... 218
Configuring Ports and Switches for VM Networks in VMM ... 220
Configuring Ports and Switches in VMM Illustrated Overview ... 230
How to Create a Port Profile for Uplinks in VMM ... 234
How to Create a Port Profile for Virtual Network Adapters in VMM ... 236
How to Create a Port Classification in VMM ... 237
How to Add a Virtual Switch Extension Manager in System Center 2012 SP1 ... 238
How to Add a Virtual Switch Extension or Network Manager in System Center 2012 R2 ... 240
How to Create a Logical Switch in VMM ... 242

How to Configure Network Settings on a Host by Applying a Logical Switch in VMM 245
How to View Host Network Adapter Settings and Increase Compliance with Logical Switch Settings in VMM ... 248
Configuring VM Networks and Gateways in VMM ... 249
Configuring VM Networks in VMM Illustrated Overview ... 255
How to Add a Gateway in VMM in System Center 2012 SP1 ... 268
How to Add a Gateway in VMM in System Center 2012 R2 ... 269
How to Use a Server Running Windows Server 2012 R2 as a Gateway with VMM ... 272
How to Create a VM Network in VMM in System Center 2012 SP1 ... 282
How to Create a VM Network in VMM in System Center 2012 R2 ... 286
How to Create IP Address Pools for VM Networks in VMM ... 291
How to Release Inactive IP Addresses for VM Networks in VMM ... 294
How to View VMM Network Configuration Diagrams in VMM ... 295
Configuring Storage in VMM ... 296
Managing Virtual Fibre Channel in VMM ... 301
Adding and Classifying Virtual Fibre Channel Fabrics ... 303
Managing Virtual Fibre Channel Zones ... 305
Managing Virtual SANs ... 307
Managing Storage LUNs for Virtual Fibre Channel ... 309
Creating a VM for Virtual Fibre Channel ... 310
Creating a Service Tier for Virtual Fibre Channel ... 310
How to Add and Classify SMI-S and SMP Storage Devices in VMM ... 311
How to Add Windows File Server Shares in VMM ... 314
How to Assign SMB 3.0 File Shares to Hyper-V Hosts and Clusters in VMM ... 315
How to Create Storage Classifications in VMM ... 318
How to Select a Method for Creating Logical Units in VMM ... 319
How to Provision Storage Logical Units in VMM ... 319
How to Allocate Storage Logical Units to a Host Group in VMM ... 320
How to Allocate Storage Pools to a Host Group in VMM ... 322
How to Remove Storage Logical Units in VMM ... 323
How to Create a Storage Pool from Physical Disks in VMM ... 323
How to Create a File Share from a Storage Pool in VMM ... 324
How to Set a Disk Witness for a File Server Cluster Quorum in VMM ... 325
Using Infrastructure Servers in VMM ... 325
How to View Infrastructure Servers ... 326
How to Add an Infrastructure Server to VMM ... 326
How to Remove an Infrastructure Server from VMM ... 327
How to View the Properties of an Infrastructure Server in VMM ... 327
Adding and Managing Hyper-V Hosts and Scale-Out File Servers in VMM ... 327
Adding Hyper-V Hosts and Host Clusters, and Scale-Out File Servers to VMM ... 328
Adding Windows Servers as Hyper-V Hosts in VMM Overview ... 332
How to Add Trusted Hyper-V Hosts and Host Clusters in VMM ... 334
How to Add Hyper-V Hosts in a Disjointed Namespace in VMM ... 337

How to Add Untrusted Hyper-V Hosts and Host Clusters in VMM 339
How to Add Hyper-V Hosts in a Perimeter Network in VMM 341
Adding Physical Computers as Hyper-V Hosts or as Scale-Out File Servers in VMM Overview 344
Prepare the Physical Computers in VMM 349
How to Add a PXE Server to VMM 349
How to Add Driver Files to the VMM Library 351
How to Create a Host or a Physical Computer Profile to Provision a Hyper-V Host in VMM 353
How to Discover Physical Computers and Deploy as Hyper-V Hosts in VMM 361
Configuring Hyper-V Host Properties in VMM 368
How to Configure Storage on a Hyper-V Host in VMM 371
How to Configure Network Settings on a Hyper-V Host in VMM 376
How to Configure Host BMC Settings in VMM 381
How to Configure Network Settings on a Host by Applying a Logical Switch in VMM 383
How to Add a Top-of-Rack Switch in VMM in System Center 2012 R2 387
How to View Compliance Information for a Physical Network Adapter on a Host in VMM 389
Creating and Modifying Hyper-V Host Clusters in VMM 390
Creating a Hyper-V Host Cluster in VMM Overview 391
Creating a Hyper-V Host Cluster in VMM Prerequisites 393
How to Create a Hyper-V Host Cluster in VMM 396
Modifying a Hyper-V Host Cluster in VMM 400
How to Add a Node to a Hyper-V Host Cluster in VMM 401
How to Remove a Node from a Hyper-V Host Cluster in VMM 404
How to Uncluster a Hyper-V Host Cluster in VMM 405
Configuring Hyper-V Host Cluster Properties in VMM 406
How to Configure Storage on a Hyper-V Host Cluster in VMM 409
Modifying a Scale-Out File Server in VMM 413
How to Add a Node to a Scale-Out File Server in VMM 414
How to Remove a Node From a Scale-Out File Server in VMM 415
How to Remove and Uncluster a Scale-Out File Server in VMM 416
Configuring Dynamic Optimization and Power Optimization in VMM 416

How to Configure Dynamic Optimization and Power Optimization 420
How to Run Dynamic Optimization on a Host Cluster 421
Managing VMware ESX and Citrix XenServer in VMM 422
Managing VMware ESX Hosts Overview 422
How to Add a VMware vCenter Server to VMM 429
How to Add VMware ESX Hosts to VMM 431
How to Configure Network Settings on a VMware ESX Host 434
How to Configure Host BMC Settings in VMM 436
How to Import VMware Templates 438
How to Convert VMware Virtual Machines to Hyper-V 439
Managing Citrix XenServer Overview 441
How to Add XenServer Hosts to VMM 448
Configuring XenServer Host Properties 450
How to Configure Network Settings on a Citrix XenServer Host 452
How to Configure Host BMC Settings in VMM 455
Managing Fabric Updates in VMM 457
How to Install a WSUS Server for VMM 459
How to Add an Update Server to VMM 462
How to Configure Update Baselines in VMM 463
How to Scan for Update Compliance in VMM 466
Performing Update Remediation in VMM 467
How to Remediate Updates on a Stand-Alone Hyper-V Host in VMM 468
How to Perform Rolling Updates on a Hyper-V Host Cluster in VMM 469
How to Remediate Updates on Infrastructure Servers in VMM 470
How to Create and Remove Update Exemptions for Resources in VMM 472
How to Perform On-Demand WSUS Synchronizations in VMM 473
How to Update WSUS Settings in VMM 474

How to Integrate Fabric Updates with Configuration Manager 475
Creating and Deploying Virtual Machines and Services in VMM 477
Creating a Private Cloud in VMM 477
Creating a Private Cloud in VMM Overview 477
How to Create a Private Cloud from Host Groups 479
How to Create a Private Cloud from a VMware Resource Pool 484
How to Increase the Capacity of a Private Cloud 489
How to Delete a Private Cloud 490
Configuring Self-Service in VMM 490
Configuring Self-Service in VMM Overview 491
How to Create a Self-Service User Role in VMM 494
How to Open a New Session While You Are Logged On to the VMM Console 499
How to Enable Self-Service Users to Share Resources in VMM 500
Configuring the Library to Support Self-Service Users 501
How to Configure the Library to Support Self-Service Users 503
How to Import and Export Physical Resources To and From the Library 507
Creating and Deploying Virtual Machines in VMM 509
Creating and Deploying Virtual Machines Overview 509
Understanding Virtual Machine Placement and Ratings in VMM 512
Understanding Generation 1 and Generation 2 Virtual Machines in VMM 515
Requirements for Linux-Based Virtual Machines 518
How to Install the VMM Agent for Linux 519
How to Create and Deploy a Virtual Machine from a Blank Virtual Hard Disk 520
How to Create and Deploy a Virtual Machine from an Existing Virtual Hard Disk 524
How to Create and Deploy a Virtual Machine from an Existing Virtual Machine 529
How to Create and Deploy a Virtual Machine from a Template 533

How to Deploy a Virtual Machine by Converting a Physical Computer (P2V) 538
P2V Prerequisites in VMM 538
How to Convert Physical Computers to Virtual Machines by Using VMM 543
How to Deploy a Virtual Machine by Converting a Virtual Machine (V2V) 545
How to Convert Citrix XenServer Virtual Machines to Hyper-V 546
How to Convert VMware Virtual Machines to Hyper-V 546
Using OVF Packages to Create Virtual Machines in System Center Virtual Machine Manager 2012 548
How to Deploy a Virtual Machine Stored in the VMM Library 553
How to View and Modify Properties of a Deployed Virtual Machine in VMM 555
Creating Profiles and Templates in VMM 555
Creating Profiles and Templates in VMM Overview 556
How to Create a Hardware Profile 558
How to Create a Guest Operating System Profile 559
How to Create an Application Profile in a Service Deployment 561
How to Create a SQL Server Profile in a Service Deployment 563
How to Create a Virtual Machine Template 565
Creating and Deploying Services in VMM 570
Creating and Deploying Services Overview 570
Common Scenarios for Services 572
Preparing to Create Services in VMM 573
Creating Service Templates in VMM 574
How to Create a Service Template in VMM 575
How to Add a Tier to a Service Template 576
How to Add Networking Components to a Service Template 578
How to Configure a Hardware Load Balancer for a Service Tier 579
How to Configure NLB for a Service Tier 581

How to Determine the Virtual IP Address for a Service 588
How to Configure the Properties of a Service Template 589
How to Create a Guest Cluster by Using a Service Template in VMM 592
Deploying Applications with Services in VMM 600
Application Framework Resources in VMM 600
Deploying Services in VMM 601
How to Deploy a Service in VMM 601
How to Configure Deployment Settings for a Service 604
How to View and Manage a Deployed Service 606
Scaling Out a Service in VMM 607
How to Scale Out a Service in VMM 607
Updating a Service in VMM 609
How to Create an Updated Service Template in VMM 610
How to Update a Service Template to Use an Updated Resource in VMM 611
How to Apply Updates to a Deployed Service in VMM 612
Exporting and Importing Service Templates in VMM 613
How to Export a Service Template in VMM 614
How to Import a Service Template in VMM 615
Rapid Provisioning of Virtual Machines Using SAN Copy Overview 617
How to Create a SAN Copy-Capable Template from a New Virtual Machine 621
How to Create a SAN Copy-Capable Template from an Existing Virtual Machine 624
How to Deploy a New Virtual Machine from the SAN Copy-Capable Template 627
Migrating Virtual Machines and Storage Overview 628
Configuring Virtual Machine Settings in VMM 633
Configuring Availability Options for Virtual Machines Overview 633
How to Configure Priority in VMM for a Virtual Machine on a Host Cluster 634

How to Configure Availability Sets in VMM for Virtual Machines on a Host Cluster 635
How to Configure Preferred and Possible Owners for a Virtual Machine on a Host Cluster 636
Configuring Resource Throttling for VMM 637
How To Configure Processor and Memory Throttling for VMM 639
Deploying Virtual NUMA for VMM 640
How to Configure Virtual NUMA for VMM 641
Creating Virtual Machine Role Templates by Using VMM and Windows Azure Pack 642
Migrating Virtual Machines and Storage in VMM 644
Migrating Virtual Machines and Storage Overview 644
How to Migrate a Virtual Machine in VMM 649
How to Run a Quick Storage Migration in VMM 652
How to Run a Live Migration in VMM 654
Monitoring and Reporting in VMM 657
Configuring Operations Manager Integration with VMM 658
How to Connect VMM with Operations Manager 659
How to Enable PRO Tips in VMM 665
How to Configure SQL Server Analysis Services for VMM 666
Using Reporting in VMM 667
Performing Maintenance Tasks in VMM 670
How to Create and Assign a Servicing Window in VMM 670
How to Place a Host in Maintenance Mode in VMM 672
Back Up and Restore Virtual Machine Manager 673
Remote Console in System Center 2012 R2 681
How to Configure Windows Azure Pack to use the Remote Desktop Gateway 691
Configuring Security in System Center 2012 - Virtual Machine Manager 692
Configuring Run As Accounts in VMM 692

How to Create a Run As Account in VMM 693
How to Disable and Enable Run As Accounts in VMM 694
How to Delete a Run As Account in VMM 694
Creating User Roles in VMM 695
How to Add Users to the Administrator User Role in VMM 697
How to Create a Delegated Administrator User Role in VMM 698
How to Create a Read-Only Administrator User Role in VMM 699
How to Create a Tenant Administrator User Role in VMM 700
Disable Support for SSL 2.0 701
Ports and Protocols for VMM 702
Clear Text Passwords in Unattend.xml 704
Troubleshooting System Center 2012 - Virtual Machine Manager 705
Microsoft Server Application Virtualization 706
Server Application Virtualization Overview 706
Server Application Virtualization Release Notes 709
Installing Server Application Virtualization 711
Server Application Virtualization Software Requirements 713
How to Install the Server Application Virtualization Sequencer 714
How to Install the Server Application Virtualization Agent 715
How to Remove the Server Application Virtualization Agent 717
How to install the Server Application Virtualization PowerShell Cmdlets 718
Packaging Applications With Server Application Virtualization 719
How to Sequence a New Server Application 721
How to Update an Existing Virtual Application Package 724
How to Edit an Existing Virtual Application Package 725
How to Perform Post-Sequencing Configuration 726

How to Save a Server Virtual Application Package 728
How to Deploy a Virtual Application Package for Testing 729
Server Application Virtualization Sequencer Technical Reference 731
Server Application Virtualization Cmdlets 732
Sequencer Console 734
Deployment Configuration Tab 735
Properties Tab 736
Change History Tab 737
Files Tab 740
Virtual Registry Tab 741
Virtual File System Tab 742
OSD Tab 743
Dialog Pages 744
Application Selection Page 745
Best Practices for Server Application Virtualization 745
Options 747
Wizard Pages 750
Create New Package Wizard 750
Prepare Computer Page 751
Upgrade Configuration Wizard 752
Select Installer Page 753
Package Name Page 754
Installation Page 755
Configure Software Page 755
Troubleshooting Server Application Virtualization 756
Server Application Virtualization Privacy Statement 757

Virtual Machine Manager

Virtual Machine Manager (VMM) is a management solution for the virtualized datacenter, enabling you to configure and manage your virtualization host, networking, and storage resources in order to create and deploy virtual machines and services to private clouds that you have created.

The following topics provide information to help you deploy and use VMM.

- Getting Started with System Center 2012 - Virtual Machine Manager
- Deploying System Center 2012 - Virtual Machine Manager
- Upgrading to System Center 2012 - Virtual Machine Manager
- Upgrading to VMM in System Center 2012 SP1
- Administering System Center 2012 - Virtual Machine Manager
- Configuring Security in System Center 2012 - Virtual Machine Manager
- Troubleshooting System Center 2012 - Virtual Machine Manager

Getting Started with System Center 2012 - Virtual Machine Manager

The following topics provide information to help you get started with learning about Virtual Machine Manager (VMM).

- Overview of System Center 2012 - Virtual Machine Manager
- What's New in System Center 2012 - Virtual Machine Manager
- Resources for System Center 2012 - Virtual Machine Manager

Overview of System Center 2012 - Virtual Machine Manager

Virtual Machine Manager (VMM) is a management solution for the virtualized data center. You can use it to configure and manage your virtualization host, networking, and storage resources in order to create and deploy virtual machines and services to private clouds that you have created.

Deploying VMM

A deployment of VMM consists of the following.

Name	Description
VMM management server	The computer on which the VMM service runs.

Name	Description
	It processes commands and controls communications with the VMM database, the library server, and virtual machine hosts.
VMM database	A Microsoft SQL Server database that stores VMM configuration information such as virtual machine and service templates, and profiles.
VMM console	The program that you can use to connect to a VMM management server in order to centrally view and manage physical and virtual resources, such as virtual machine hosts, virtual machines, services, and library resources.
VMM library and VMM library server	The catalog of resources (for example, virtual hard disks, templates, and profiles) that are used to deploy virtual machines and services. A library server hosts shared folders that are used to store file-based resources in the VMM library.
VMM command shell	The Windows PowerShell–based command shell that makes available the cmdlets that perform all functions in VMM.
VMM Self-Service Portal (optional) **Note** As of System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed.	A website that users who are assigned to a self-service user role can use to deploy and manage their own virtual machines in private clouds.

For information about deploying VMM, see Deploying System Center 2012 - Virtual Machine Manager.

Configuring security for VMM

You can perform the following tasks to configure security in VMM.

Task	Description	For more information
Configure Run As accounts	Create Run As accounts to provide the necessary credentials for performing	Configuring Run As Accounts in VMM

Task	Description	For more information
	operations in VMM.	
Create user roles	Create self-service users, delegated administrators, and read-only administrators to ensure that users can perform the appropriate actions on the appropriate resources in VMM.	Creating User Roles in VMM
Review ports and protocols	Review ports and protocols, and as appropriate, modify ports that VMM uses for communication and file transfers between the VMM components.	Ports and Protocols for VMM

Configuring fabric resources in VMM

The following resources in VMM are referred to as '*fabric*', and you must configure them before you can deploy virtual machines and services to a private cloud or to virtual machine hosts. You can use VMM to configure and manage the following fabric resources.

Resource	Description	For more information
Virtual machine hosts	Microsoft Hyper-V Server or Hyper-V in Windows Server, Citrix XenServer, and VMware ESX hosts and host clusters on which you will deploy virtual machines and services. You can create host groups to organize your hosts based on physical site location, resource allocation, or other criteria.	Adding and Managing Hyper-V Hosts and Scale-Out File Servers in VMM Managing Citrix XenServer Overview Managing VMware ESX Hosts Overview Creating Host Groups in VMM
Networking	Networking resources, such as logical networks, IP address pools, and load balancers that are used to deploy virtual machines and services.	Configuring Networking in VMM
Storage	Storage resources, such as storage classifications, logical units, and storage pools that	Configuring Storage in VMM

Resource	Description	For more information
	are made available to Hyper-V hosts and host clusters.	
Library servers and library shares	A catalog of resources (for example, virtual hard disks, templates, and profiles) that are used to deploy virtual machines and services.	Configuring the VMM Library

Deploying virtual machines and services in VMM

After you configure your hosts and your networking, storage, and library resources, you can perform the following tasks to deploy virtual machines and services in VMM.

In VMM, a service is a set of virtual machines that are configured and deployed together and are managed as a single entity. An example is the deployment of a multiple-tier line-of-business application.

Task	Description	For more information
Create private clouds	Combine hosts and networking, storage, and library resources to create a private cloud.	Creating a Private Cloud in VMM Overview
Configure self-service	Create a self-service user role that can create, deploy, and use virtual machines and services in one or more private clouds.	Configuring Self-Service in VMM
Create sequenced applications	Use Microsoft Server Application Virtualization (Server App-V) to sequence applications that VMM will deploy.	Microsoft Server Application Virtualization
Create profiles	Create profiles (hardware profiles, guest operating system profiles, application profiles, and SQL Server profiles) that will be used in a template to deploy virtual machines.	Creating Profiles and Templates in VMM

Task	Description	For more information
	For example, an application profile provides instructions for installing applications such as Server App-V applications, Web Deploy applications, and SQL Server data-tier applications (DACs), and for running scripts during the deployment of a virtual machine. You can use hardware profiles and guest operating system profiles when you deploy virtual machines through a virtual machine template or a service template. You can use application profiles and SQL Server profiles only when you deploy virtual machines through a service template.	
Create virtual machine templates	Create virtual machine templates that can be used to create new virtual machines and to configure tiers in VMM services.	How to Create a Virtual Machine Template
Create service templates	Use the Service Template Designer to create service templates that can be used to deploy services.	Creating Service Templates in VMM
Deploy virtual machines	Deploy virtual machines to private clouds or hosts by using virtual machine templates.	Creating and Deploying Virtual Machines in VMM
Deploy services	Deploy services to private clouds or hosts by using a service template.	Creating and Deploying Services in VMM
Scale out a service	Add more virtual machines to a deployed service.	Scaling Out a Service in VMM
Update a service	Make changes to a deployed	Updating a Service in VMM

Task	Description	For more information
	service.	
Support tenants by using VMM with Windows Azure Pack	Use VMM with Windows Azure Pack to enable tenants to deploy preconfigured virtual machines.	Creating Virtual Machine Role Templates by Using VMM and Windows Azure Pack

Scalability

The different elements in a VMM deployment can scale as described in the following table.

VMM element	In System Center 2012 – Virtual Machine Manager	In System Center 2012 SP1	In System Center 2012 R2
Virtual machine hosts	400	1,000	1,000
Virtual machines	8,000	25,000	25,000
User roles	300	1,000	1,000
Tenants (based on one user role per tenant accessing the system)		1,000	1,000
Concurrent jobs	250	250	250
Concurrent clients (such as VMM consoles and Windows PowerShell sessions)	50	50	50
Job history records	2 Millions	5 Millions	5 Millions
Tenants		1,000	1,000

Managing the VMM environment

You can perform the following tasks to manage the servers, virtual machines, and services in your VMM environment.

Task	Description	For more information
Manage update compliance of	Scan servers (for example,	Managing Fabric Updates in

Task	Description	For more information
servers (for example, Hyper-V hosts and library servers)	Hyper-V hosts and library servers) for update compliance, view update compliance status, and perform update remediation by using a Windows Server Update Services (WSUS) server.	VMM
Monitor the health and performance of virtual machines and their hosts and provide reports	Use Operations Manager with VMM and enable Performance and Resource Optimization (PRO).	Configuring Operations Manager Integration with VMM
Perform common maintenance tasks such as backing up the VMM database	Perform common maintenance tasks, such as using maintenance mode to prepare to take a host offline, or backing up and restoring the SQL Server database that VMM uses.	Performing Maintenance Tasks in VMM

What's New in System Center 2012 - Virtual Machine Manager

This section provides the following information about improvements and capabilities in VMM:

- A description of what was added in System Center 2012 R2, What's New in VMM in System Center 2012 R2.
- A description of what was added in System Center 2012 Service Pack 1 (SP1), What's New in VMM in System Center 2012 SP1.
- A categorized list of several tasks that you can perform in System Center 2012 – Virtual Machine Manager (VMM), What's New in System Center 2012 - Virtual Machine Manager.

For an overview of VMM, see Overview of System Center 2012 - Virtual Machine Manager.

What's New in VMM in System Center 2012 R2

The following sections summarize Virtual Machine Manager (VMM) enhancements and other changes in the System Center 2012 R2 release.

Networking

- Site-to-site Network Virtualization using Generic Routing Encapsulation (NVGRE) gateway. Windows Server® 2012 R2 delivers new functionality for site-to-site gateways for Hyper-V network virtualization, by using all Microsoft software. This functionality enables hosting providers of virtualized networks to achieve higher capacity and better reliability, and to enable the majority of tenant scenarios. Support includes multiple site-to-site tunnels and direct Internet access through a network address translation (NAT) firewall. Tenants can use preferred IP addressing for all of their virtual machines, in multiple sites and in the cloud, all supported by Windows Server 2012 R2 and VMM. For more information, see How to Add a Gateway in VMM in System Center 2012 R2 and How to Create a VM Network in VMM in System Center 2012 R2.
- NVGRE support. Because the VMM APIs are more flexible, network services such as load balancers can function as network virtualization gateways, and switch extensions can use network virtualization policy to interpret all IP addressing information in packets that are sent. Communication between commonly used Cisco switch extensions and VMM is expanded through support for using these switch extensions with Hyper-V network virtualization. For more information, see How to Add a Virtual Switch Extension or Network Manager in System Center 2012 R2.
- IP Address Management (IPAM) integration with VMM. For more information, see How to Add an IPAM Server in VMM in System Center 2012 R2.
- Top-of-rack (TOR) switch integration with VMM. For more information, see How to Add a Top-of-Rack Switch in VMM in System Center 2012 R2.
- IP address management for virtual machines. Hosting providers and enterprises can more easily manage IP addresses for virtual machines across the data center. After virtual machine deployment, you can view IP addresses for each virtual network adapter, and you can change or add IP addresses without logging on to the virtual machines. For virtual machine migration, you can assign new IP addresses from an IP pool in the destination subnet. In addition, virtual machines in a guest cluster can set their own IP addresses on networks that use Hyper-V network virtualization.

  For more information, see How to View and Modify Properties of a Deployed Virtual Machine in VMM and How to Create a Guest Cluster by Using a Service Template in VMM.

Virtual machines and cloud

- Support for generation 2 virtual machines. You can now create generation 2 virtual machines and virtual machine templates that are based on these virtual machines. Generation 2 virtual machines provide new functionality such as a Secure Boot and boot from SCSI virtual DVD. For more information about generation 2 virtual machines, and a comparison with generation 1 virtual machines, see Understanding Generation 1 and Generation 2 Virtual Machines in VMM.
- Differencing disks. Optimized support for differencing disks (both .vhd and .vhdx file formats) improves the performance and reduces the costs of virtual machine provisioning. This support can be critical in hosting scenarios in which large numbers of virtual machines are

created from a small set of initial virtual disks. For more information, see Creating and Deploying Virtual Machines Overview.

- Live cloning of virtual machines. The System Center 2012 R2 release of VMM supports a new Hyper-V feature in Windows Server 2012 R2. By using live cloning, you can export virtual machines without downtime. You can then avoid creating and configuring new virtual machines to match existing virtual machines. For more information, see How to Create and Deploy a Virtual Machine from an Existing Virtual Machine.
- Online resizing of .vhdx files. For Hyper-V hosts that are running Windows Server 2012 R2, the System Center 2012 R2 release of VMM supports online resizing of .vhdx files that are on SCSI bus, while the disks are in use. This supports the Online Resizing feature of Hyper-V.
- Enhanced support for Windows Server 2012 Dynamic Memory features. You can change and apply Dynamic Memory settings on a running or paused virtual machine.
- Ability to grant permissions to users for each cloud. Administrators can easily customize the scope of permitted actions that users and user roles can perform on a per-cloud basis. This ability eliminates the need to create a new user role for every combination of action/user/cloud. For more information, see Creating User Roles in VMM.
- Leverage of the new Hyper-V file transfer APIs in Windows Server 2012 R2 to transfer files to guest operating systems. This transfer is supported when both the host's and the guest's operating system is Windows Server 2012 R2, the guest is running virtualization guest services, and the guest is not connected to any network that has access to VMM library servers. When a virtual machine is running on a Windows Server 2012 R2 host and has no connection to a network that has access to VMM library servers, file transfers during servicing take advantage of these new Hyper-V APIs.
- Ability to create Windows-based and Linux-based virtual machines and multi-VM Services, from a gallery of templates.
- Faster live migration, and support for migration of the Windows Server 2012 R2 operating system. For more information, see How to Run a Live Migration in VMM.
- Support for Oracle Linux 5 (x86 and x64), Oracle Linux 6 (x86 and x64), and Debian GNU/Linux 7.0 (x86 and x64), as guest operating systems for deployment from templates to Hyper-V hosts.

Fabric

- Replacement of host profiles by physical computer profiles. You can use physical computer profiles in the same manner that you used host profiles to provision a bare-metal computer to a Hyper-V host. In addition, you can use physical computer profiles to provision a bare-metal computer as a Windows Scale-Out File Server cluster. For more information about using physical computer profiles, see Adding Physical Computers as Hyper-V Hosts or as Scale-Out File Servers in VMM Overview.

Storage

- Support for virtual Fibre Channel. The System Center 2012 R2 release of VMM supports management of Fibre Channel fabrics and the automated provisioning of virtual machines

with connectivity to storage over Fibre Channel fabrics. For more information about virtual Fibre Channel, see Managing Virtual Fibre Channel in VMM.

- Management of zones.
- Leverage of the Windows Server 2012 Offloaded Data Transfers (ODX) capability. Fast file copy in System Center 2012 R2 Virtual Machine Manager greatly improves the time performance of file transfers and virtual machine deployments, mostly by leveraging the Windows ODX feature. For more information about fast file copy, see Creating and Deploying Virtual Machines Overview.
- Shared .vhdx support. The System Center 2012 R2 release of VMM supports shared .vhdx storage in a service tier. You can therefore use guest clustering to deploy in-guest high-availability applications. You can also use Microsoft SQL Server failover clustering and high-availability VMM with shared .vhdx storage to provide a highly available SQL Server farm. For more information, see How to Create a Guest Cluster by Using a Service Template in VMM.
- Provisioning of Scale-Out File Server clusters from bare-metal computers. By using physical computer profiles, you can provision bare-metal computers to be scale-out file servers, and you can choose to cluster the provisioned computers into a Scale-Out File Server cluster. You can use a single step to accomplish both provisioning and clustering. For more information, see How to Create a Host or a Physical Computer Profile to Provision a Hyper-V Host in VMM and **How to Create a Scale-Out File Server Cluster in VMM**.
- Integration of storage with differencing disks. Differencing disks reduce storage requirements by allowing a large percentage of disk data to be shared among multiple virtual disks, optimizing storage costs.
- Storage spaces File. File server management encompasses the full life cycle of a file server, from provisioning to steady-state management. This frees a cloud administrator from having to build or integrate different tools for storage management. Management of the file server supports the Windows Server 2012 R2 integrated experience for storage, computing, and networking, from initial provisioning to ongoing monitoring. This integrated experience incorporates management at scale across multiple racks and thousands of managed devices.

Services

Support for scripts that create a guest cluster. The script that runs on the first deployed virtual machine can be different from the script that runs on the other virtual machines in the tier. For more information, see How to Create a Guest Cluster by Using a Service Template in VMM.

Infrastructure

- Ability of automatic tasks to resume after virtual machine failover.
- Expanded computer scope for VMM update management. Due to added support for infrastructure servers, you can add servers such as Active Directory, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and other management servers that are not VMM host servers, as managed computers. You can then use a Windows Server Update Services (WSUS) server to manage updates for these infrastructure servers in the

same way that you manage updates for other computers in the VMM environment. For more information, see Using Infrastructure Servers in VMM.

- Update of management packs with new metrics for chargeback purposes that are based on both allocation and utilization. This update provides better integration with chargeback and reporting, and it enables monitoring of tenant-based utilization of resources that allows chargeback and billing. For more information, see **About VMM Monitored Data From Operations Manager**.

Additional enhancements and other general changes

- Discontinued support, in System Center 2012 R2 Virtual Machine Manager, of the VMM feature that enabled conversion of existing physical computers into virtual machines through the physical-to-virtual (P2V) conversion process. For information about how to use an earlier version of VMM to mitigate this change, see the How to perform a P2V in a SCVMM 2012 R2 environment blog entry.
- Support for Windows Server 2012 R2 and Windows 8.1, in various roles such as the VMM management server, the VMM library server, and the Hyper-V host.
- Removal of the preconfigured chargeback report. For information about other methods that you can use for creating chargeback reports, see Installing and Configuring Chargeback Reports in System Center 2012 - Service Manager and Chargeback: A scenario example.
- Improved integration between VMM and Windows Azure Hyper-V Recovery Manager in Windows Server 2012 R2. VMM is enhanced to provide the infrastructure that Hyper-V Recovery Manager requires to enable cloud-based replication. This enhancement supports recovery scenarios of VMM-managed private clouds and data centers. For more information, see Deployment Guide for Hyper-V Recovery Manager on MSDN.
- Addition of the Remote Console feature in VMM in Windows Server 2012 R2. This feature enables tenants to access the console of their virtual machines in an environment where it is usually not possible—for example, when the virtual machines are on an isolated network, or in an untrusted network. For more information, see Remote Console in System Center 2012 R2.
- In Setup, addition of direct links to missing prerequisites.
- In Setup, automatic collation of language. Setup automatically configures collation according to the language of the server operating system.

See Also

What's New in VMM in System Center 2012 SP1

What's New in System Center 2012 - Virtual Machine Manager

What's New in VMM in System Center 2012 SP1

Here are some general changes in VMM in the System Center 2012 SP1 release that you might need to consider:

- The VMM Self-Service Portal is no longer supported in System Center 2012 SP1. Instead, we recommend that you use System Center 2012 SP1 - App Controller as the self-service portal solution. For more information about App Controller, see App Controller.
- Self-service users can now use the VMM console instead of the VMM Self-Service Portal to perform tasks such as deploying virtual machines and services.
- High availability with N_Port ID Virtualization (NPIV) is no longer supported. VMM is compatible with virtual Fibre Channels that are configured for virtual machines in Hyper-V.
- The OVF tool is no longer supported. Instead, to import and to export an OVF package to Hyper-V, you can use the Microsoft Virtual Machine Converter (MVMC) which converts the VMDK/VHD file. For more information, see Using OVF Packages to Create Virtual Machines in System Center Virtual Machine Manager 2012.

The following tables summarize VMM enhancements and other changes in the System Center 2012 SP1 release.

Deploying VMM	**For more information**
Enhancements to the matrix of supported versions of operating systems and other required software.	For a complete list of supported and required configurations, see **System Requirements for System Center 2012 - Virtual Machine Manager**.
Integration with Windows Server 2012 which delivers numerous enhancements to the Microsoft Hyper-V features, as follows: • Large virtual machines • Clusters that can support a larger numbers of nodes • Storage management through SMI-S (Storage Management Initiative – Specification)	See the Supported Storage Arrays section in Configuring Storage Overview.
Ability to manage vSphere 5.1 and Citrix XenServer 6.0 .	For more information about Citrix, see Managing Citrix XenServer Overview. For more information about vSphere see How to Add VMware ESX Hosts to VMM and How to Configure Network Settings on a VMware ESX Host.

Configuring Fabric Resources in VMM - Networks	**For more information**
New model for virtual machine networking,	**Network Virtualization**

Configuring Fabric Resources in VMM - Networks	For more information
including network virtualization and virtual local area networks (VLANs) for network isolation.	How to Create a VM Network in VMM in System Center 2012 SP1
Management of the Hyper-V extensible switch, including deployment and configuration of virtual switch extensions using a new logical switch concept.	How to Add a Virtual Switch Extension Manager in System Center 2012 SP1
Support for network virtualization that includes support for using Dynamic Host Configuration Protocol (DHCP) to assign customer addresses using Network Virtualization with Generic Routing Encapsulation (NVGRE) to virtualize the IP address of a virtual machine.	**Network Virtualization**
Software-defined networking with support for Hyper-V network virtualization and switch extension management. This allows a constant network configuration in the datacenter.	Configuring VM Networks and Gateways in VMM Configuring Ports and Switches for VM Networks in VMM How to Add a Virtual Switch Extension Manager in System Center 2012 SP1
Introduction of a logical switch that allows you to manage individual switch instances across multiple Hyper-V hosts as a single entity.	How to Create a Logical Switch in VMM
Ability to deploy and manage third-party switch extensions, such as Cisco 1KV and InMon. For organizations that have investments in these third-party products, these can be integrated into VMM.	How to Create a Logical Switch in VMM

Configuring Fabric Resources in VMM - Storage	For more information
Support for file shares that leverage the new 3.0 version of the Server Message Block (SMB) protocol that is introduced in Windows Server 2012. VMM in this release includes support for designating network file shares on Windows Server 2012 computers as the storage location for virtual machine files, such as configuration, virtual hard disk (.vhd/.vhdx) files and checkpoints.	For more information about SMB 3.0 in Windows Server 2012, see Server Message Block Overview. For more information about how to create a highly available SMB 3.0 file share, see Scale-Out File Server for Application Data Overview, and steps 1 and 2 of the Deploy Scale-Out File Server scenario that is linked to from that topic.

Configuring Fabric Resources in VMM - Storage	For more information
SMB 3.0 file shares provide the following benefits when they are used with VMM in this release: • Hyper-V over SMB supports file servers and storage with improved efficiency compared to traditional storage area networks (SANs). • If you use SMB 3.0 file shares as the storage locations for virtual machine files, you can "live migrate" virtual machines that are running between two standalone Hyper-V hosts or between two stand-alone Hyper-V host clusters. Because the storage location is a shared location that is available from the source and destination hosts, only the virtual machine state must transfer between hosts. You can create SMB 3.0 file shares on standalone Windows Server 2012 file servers and on clustered Windows Server 2012 file servers. If you use a standalone file server, you can designate an SMB 3.0 file share as the virtual machine storage location on a Windows Server 2012 Hyper-V host cluster. However, this is not a highly available solution.	
The new Windows Standards-Based Storage Management service replaces the Microsoft Storage Management Service in System Center 2012 – Virtual Machine Manager. The new service uses the Windows Storage Management application programming interface (API), a WMI-based programming interface that is included in Windows Server 2012. This new API enables you to discover storage by using multiple provider types. **Important** The Windows Storage Management API supersedes the Virtual Disk Service (VDS) interface. Therefore, if you are using a storage array that uses	Configuring Storage Overview

Configuring Fabric Resources in VMM - Storage	For more information
only the VDS hardware provider (and not SMI-S), storage area network (SAN) transfer capabilities will no longer be available. A SAN transfer enables you to migrate a virtual machine from one location to another when the virtual hard disk is located on a storage array. The logical unit number (LUN) that contains the virtual machine is remapped from the source computer to the destination computer instead of transferring the files over the network. In this release, VMM supports the following types of storage providers and arrays: • SMI-S CIM–XML, which existed in System Center 2012 – Virtual Machine Manager. For more information about the supported storage arrays, see the Supported Storage Arrays section of Configuring Storage Overview. • Symmetric multiprocessing (SMP) Supported array: Dell EqualLogic PS Series using iSCSI.	
Support for auto (dynamic) iSCSI target systems, such as the Dell EqualLogic PS Series. System Center 2012 – Virtual Machine Manager supports only static iSCSI target systems.	
Support for thin provisioning of logical units through VMM. Your storage array must support thin provisioning. And thin provisioning must be enabled for a storage pool by your storage administrator.	
Integration with third-party SANs and file-based storage on Windows Server 2012 File server.	

Configuring Fabric Resources in VMM - Hyper-V	For more information
Support for using a virtual hard disk that is in the .vhdx format as the base operating system image.	How to Discover Physical Computers and Deploy as Hyper-V Hosts in VMM
Operating system deployment that utilizes deep discovery and Consistent Device Naming (CDN). CDN allows VMM to predictably assign network interface controllers (NICs) to the correct networks and teams. During the discovery process, you can run *deep discovery* to see more detailed information about the physical computer hardware before you deploy the operating system. In this release, deep discovery functionality is only partially enabled. You can view the physical network adapter information, information about the CPU, and the amount of memory. You can configure network options such as logical switches, and you can change the settings for the network adapter that VMM automatically designates as the management network adapter.	How to Discover Physical Computers and Deploy as Hyper-V Hosts in VMM How to Create a Host or a Physical Computer Profile to Provision a Hyper-V Host in VMM
Support for physical network adapter configuration as follows: • IP configuration • Logical switch creation • NIC Teaming	
Support for Host vNIC configuration.	
Support for startup disk selection as part of operating system deployment.	
Enhanced default auto disk selection logic as part of operating system deployment.	

Virtual Machines and Services	For more information
Support for deployment of services to virtual machines in a domain or workgroup that does not have a trust relationship with the domain of	Preparing to Create Services in VMM

Virtual Machines and Services	For more information
the VMM management server.	
In Hyper-V only, support for the deployment of services to virtual machines that are not connected, where the service instance does not have network connectivity to the VMM management server, to a VMM library server, or to both.	Preparing to Create Services in VMM
When deploying a virtual machine as part of a service and creating a SQL Server profile, added support for SQL Server 2012 as an instance of Microsoft SQL Server.	How to Create a SQL Server Profile in a Service Deployment

Application profiles:
• For the deployment of application packages, added support for updated versions of the following applications:
  • Web Deploy 3.0
  • Data-tier Application Framework (DAC Fx) 3.0
  • Server App-V SP1
• Support for application profiles that run multiple scripts before and after installing an application on a virtual machine, and if a script fails, the capability to rerun if specified to do so in the profile.
• Support for deploying MSDeploy packages to existing Internet Information Services (IIS) servers, whether they are virtual or physical, managed by VMM or not (Web Application Host).
	How to Create an Application Profile in a Service Deployment

Support for adding Windows Server 2012 roles and features when creating and deploying services, such as the Windows Server Update Services role.	
Support for IIS application hosts, which allow you to deploy websites into pre-existing IIS web farms.	How to Apply Updates to a Deployed Service in VMM
Support for the new version of the virtual hard disk format that is introduced in Windows Server 2012. This new format is referred to as	For more information about the benefits of the VHDX format in Windows Server 2012, see

Virtual Machines and Services	For more information
VHDX. Compared to the older VHD format, VHDX has a much larger storage capacity of up to 64 TB. The VHDX format also provides data corruption protection during power failures. Additionally, it offers improved alignment of the virtual hard disk format to perform well on large-sector physical disks. Support for VHDX includes the following: • You can convert a virtual hard disk for a virtual machine that is deployed to a Windows Server 2012-based host from the .vhd to .vhdx virtual hard disk format. The conversion includes any associated checkpoints. • If you create a new virtual machine with a blank virtual hard disk, VMM determines whether the format should be .vhd or .vhdx, depending on the operating system of the host that is selected during placement. If it is a Windows Server 2012–based host, VMM uses the .vhdx format. If it is a Windows Server 2008 R2 with SP1–based host, VMM uses the .vhd format. • If you provision a physical computer as a Hyper-V host, you can specify a .vhdx file as the image for the base operating system. • You can use VMM to "rapidly provision" any virtual machines that use VHDX-based virtual hard disks from SAN-copy capable templates. • A VMM library server that runs Windows Server 2012 automatically indexes .vhdx files. • In addition to the small and large blank .vhd files that were available in previous versions of VMM, the VMM library in System Center 2012 SP1 also contains both a small (16 gigabytes (GB)) and a large (60 GB) blank .vhdx files.	Hyper-V Virtual Hard Disk Format Overview. Rapid Provisioning of Virtual Machines Using SAN Copy Overview
Support for provisioning a physical computer as a Hyper-V host. When you provision a physical	For background information about adding a physical computer as a Hyper-V host, see

Virtual Machines and Services	For more information
computer as a Hyper-V host, you can use a Windows Server 2012-based virtual hard disk that is in the .vhdx or .vhd format as the base operating system image.	Adding Physical Computers as Hyper-V Hosts Overview.
Linux-based virtual machines are now fully supported with the following: • Added settings for Linux-specific operating system specialization when you are creating a Linux-based virtual machine template.  **Important** These settings are supported only when the Linux virtual machine is deployed on Hyper-V. • Ability to include a Linux virtual machine template in a service template that deploys a multi-tier application or service. • Updated Windows PowerShell cmdlets to support this new functionality.	How to Create a Virtual Machine Template Requirements for Linux-Based Virtual Machines
Ability to configure availability options for virtual machines on Hyper-V host clusters by using the VMM console, without having to open Failover Cluster Manager.	Configuring Availability Options for Virtual Machines Overview

Live Migration	For more information
Live migration outside a cluster. This is in addition to supporting live migration within a cluster. Live migration outside a cluster allows you to perform live migration between two standalone computers that are not cluster nodes.	For more information about live migration in Windows Server 2012, see the following topics: • Virtual Machine Live Migration Overview • Virtual Machine Storage Migration Overview • Migrating virtual machines and storage in System Center SP1 - Virtual Machine Manager
Live migration between nodes in two different clusters. You can migrate between nodes within a cluster, or between nodes in different clusters.	Migrating Virtual Machines and Storage Overview How to Run a Live Migration in VMM

Live Migration	For more information
Storage migration, which allows for the migration of virtual machine storage. You can migrate storage in order to update the physical storage available in Hyper-V, or to mitigate bottlenecks in storage performance. Storage can be added to either a standalone computer or a Hyper-V cluster. Then, virtual machines can be moved to the new storage while they continue to run.	Migrating Virtual Machines and Storage Overview How to Run a Live Migration in VMM
Live VSM. By using live virtual system migration (VSM) you can migrate both virtual machines and storage in a single action.	Migrating Virtual Machines and Storage Overview How to Run a Live Migration in VMM
Concurrent live migration. You can perform multiple concurrent live migrations of virtual machines and storage. The allowable number of concurrent live migrations can be configured manually. Attempted concurrent live migrations in excess of the limit will be queued.	Migrating Virtual Machines and Storage Overview How to Run a Live Migration in VMM

VMM Console	For more information
Integration of third-party user interface (UI) add-ins for the VMM console that can extend the functionality of the console. For example, you can create console add-ins that will allow you to do the following: • Add ribbon entries in the VMM console to launch web browsers and Windows applications directly from the ribbon. • Enable new actions or additional configuration for VMM objects by writing an application that uses context that is passed regarding the selected VMM objects. • Embed custom Windows Presentation Foundation (WPF) UI or web portals directly into the VMM console's main views to provide a more fully integrated experience.	Virtual Machine Manager Add-in SDK on MSDN.
Several significant performance enhancements	

VMM Console	For more information
to the VMM console. Load times are decreased and the performance of sorting and filtering views is significantly improved. For viewing job history, jobs are now loaded incrementally and the views have a richer set of data-filtering options, reducing the effect of large sets of jobs on console performance.	
Overview pages in the VMM console now display various reports about usage and capacity metrics for services, tenants and clouds.	

Additional Improvements	For more information
Performance and scalability: • Increased the scale of a VMM management server to be able to manage 1000 hosts and 25,000 virtual machines.  **Note** Scale limits remain consistent no matter which supported hypervisors are used. VMM can manage 25,000 virtual machines, wherever they are located. • Support for a 64 node cluster. • Performance enhancement to the VMM console.	
Integration with Operation Manager as follows: • Ability to use Operations Manager to view information related to application hosts, load balancers, and user roles while also being able to monitor virtual machines, services, host systems, network adapters, and other elements of the fabric. • Receive notifications from Operations Manager if the load on a cloud has exceeded a chosen threshold of fabric capacity. Concurrently review other clouds for available excess capacity that can be	Configuring Operations Manager Integration with VMM

Additional Improvements	For more information
reallocated to meet the demand. • Generate reports that track the resource usage of each configured service or service user, to aid in capacity planning.	
Support for updateable Help for VMM cmdlets.	For more information about how to download the most recent help content for VMM cmdlets, see About_VMM_2012_Updating_Help. Alternatively, you can type the following command in a command shell: `Get-Help about_VMM_2012_Updating_Help`

Network Virtualization

VMM in this release provides support for the network virtualization capabilities that are available in Windows Server 2012.

Network virtualization provides the ability to run multiple virtual network infrastructures, potentially with overlapping IP addresses, on the same physical network. With network virtualization, each virtual network infrastructure operates as if it is the only one that is running on the shared network infrastructure. This enables two different business groups that are using VMM to use the same IP addressing scheme without conflict. In addition, network virtualization provides isolation so that only virtual machines on a specific virtual network infrastructure can communicate with each other.

Network virtualization in Windows Server 2012 is designed to remove the constraints of VLAN and hierarchical IP address assignment for virtual machine provisioning. This enables flexibility in virtual machine placement because the virtual machine can keep its IP address regardless of which host it is placed on. Placement is not limited by physical IP subnet hierarchies or VLAN configurations.

To virtualize the network in Windows Server 2012, each virtual machine is assigned two IP addresses as follows:

- *A customer address*. This IP address is visible to the virtual machine and is used by customers to communicate with the virtual machine.
- *A provider address*. This IP address is used by the Hyper-V computer that hosts the virtual machine. It is not visible to the virtual machine.

In this release, you can virtualize the IP address of a virtual machine by using *Network Virtualization with Generic Routing Encapsulation (NVGRE)*. In NVGRE, all of the virtual machines packets are encapsulated with a new header before they are sent on the physical network. IP encapsulation offers better scalability because all of the virtual machines on a specific host can share the same provider IP address.

VMM creates the necessary IP address mappings for virtual machines to take advantage of the network virtualization capabilities in Windows Server 2012. To assign provider addresses, VMM

uses an IP address pool that is associated with a logical network. To assign customer addresses, VMM uses an IP address pool that is associated with a virtual machine subnet that is, in turn, associated with a virtual machine network.

In this release, you can now assign customer addresses through DHCP or by using static IP addresses. When you create an IP address pool for a virtual machine subnet, the pool is automatically enabled to provision IP addresses by either mechanism. For DHCP to work correctly, the new DHCPv4 Server Switch Extension is required on all Windows Server 2012 Hyper-V hosts.

For more information about network virtualization in Windows Server 2012, see Hyper-V Network Virtualization Overview.

See Also

What's New in VMM in System Center 2012 R2

What's New in System Center 2012 - Virtual Machine Manager

What's New in System Center 2012 - Virtual Machine Manager

This topic provides a categorized list of several tasks that you can perform in System Center 2012 – Virtual Machine Manager (VMM).

Deploying VMM

Task	For more information
Install a highly available VMM management server.	Installing a Highly Available VMM Management Server

Configuring Security in VMM

Task	For more information
Create Run As accounts to provide the necessary credentials for performing operations in VMM.	Configuring Run As Accounts in VMM
Use the new capabilities available to the Delegated Administrator and Self-Service User roles to give users the ability to perform tasks that are new to VMM.	Creating User Roles in VMM
Create a Read-Only Administrator user role	Configuring Run As Accounts in VMM

Configuring Fabric Resources in VMM

Task	For more information
Configure network options such as virtual network adapters and logical switches during the discovery of physical computers on the network (for example, bare-metal computers) and automatic operating system installation in order to convert them into managed Hyper-V hosts.	Adding Physical Computers as Hyper-V Hosts or as Scale-Out File Servers in VMM Overview
Use the VMM console to create a Hyper-V cluster from two or more standalone Hyper-V hosts that are managed by VMM.	Creating and Modifying Hyper-V Host Clusters in VMM
Use Citrix XenServer as a virtual machine host.	Managing Citrix XenServer Overview
Use the VMM console to configure networking resources , such as logical networks, IP address pools, and load balancers, to be used to deploy virtual machines and services.	Configuring Networking in VMM
Use the VMM console to configure the storage resources, such as storage classifications, logical units, and storage pools, to be used by Hyper-V hosts and host clusters.	Configuring Storage in VMM
Scan servers, such as Hyper-V hosts and library servers, for update compliance based on an update baseline, view update compliance status, and perform update remediation by using a Windows Server Update Services (WSUS) server.	Managing Fabric Updates in VMM
Perform resource balancing by migrating virtual machines within host clusters that support live migration (Dynamic Optimization).	Configuring Dynamic Optimization and Power Optimization in VMM
Turn off hosts that are not needed to meet resource requirements within a host cluster and then turn the hosts back on when they are needed again (Power Optimization).	Configuring Dynamic Optimization and Power Optimization in VMM

Deploying Virtual Machines and Services in a Private Cloud in VMM

Task	For more information
Create a private cloud by combining hosts and networking, storage, and library resources together.	Creating a Private Cloud in VMM Overview
Use Server Application Virtualization (Server App-V) to sequence applications to be deployed by VMM.	Microsoft Server Application Virtualization
Create a custom capability profile to limit the resources that are used by virtual machines that are created in a private cloud.	How to Create a Private Cloud from Host Groups
Create an application profile that provides instructions for installing Microsoft Server App-V applications, Microsoft Web Deploy 2.0 applications, and Microsoft SQL Server data-tier application framework (DAC Fx) 2.0, as well as for running scripts when you deploy a virtual machine as part of a service.	How to Create an Application Profile in a Service Deployment
Create a SQL Server profile that provides instructions for customizing an instance of Microsoft SQL Server for a SQL Server DAC application when you deploy a virtual machine as part of a service.	How to Create a SQL Server Profile in a Service Deployment
Deploy virtual machines to private clouds by using virtual machine templates.	Creating and Deploying Virtual Machines in VMM
Use the Service Template Designer to create service templates that can be used to deploy services.	Creating Service Templates in VMM
Deploy services to private clouds or hosts by using a service template.	Creating and Deploying Services in VMM
Scale out a service: Add additional virtual machines to a deployed service.	Scaling Out a Service in VMM
Update a service: Make changes to a deployed service.	Updating a Service in VMM
Export and import service templates and virtual machine templates.	Exporting and Importing Service Templates in VMM

See Also

What's New in VMM in System Center 2012 R2

What's New in VMM in System Center 2012 SP1

Resources for System Center 2012 - Virtual Machine Manager

The following resources are available for Virtual Machine Manager (VMM).

Evaluation software for System Center 2012 – Virtual Machine Manager

Name	Description	Location
System Center 2012 – Virtual Machine Manager evaluation VHD	Provides a downloadable pre-configured virtual hard disk (VHD) to create a virtual machine that runs an evaluation version of System Center 2012 – Virtual Machine Manager. Intended for evaluation and deployment planning purposes only.	Microsoft Download Center
System Center 2012 R2 Virtual Machine Manager	Provides a downloadable pre-configured virtual hard disk (VHD) to create a virtual machine that runs an evaluation version of System Center 2012 – Virtual Machine Manager in System Center 2012 R2. Intended for evaluation and deployment planning purposes only.	Microsoft Download Center

Documentation for VMM

The following documentation is available for VMM:

Name	Description	Location
VMM technical documentation	Provides content about VMM for the following areas: • Getting Started • Deploying • Administering • Configuring Security • Scripting	Virtual Machine Manager in the TechNet Library
VMM troubleshooting content	Provides information about troubleshooting VMM. For example, a list of known issues with VMM, and possible resolutions or workarounds for those known issues.	Troubleshooting System Center 2012 - Virtual Machine Manager on the TechNet Wiki
VMM technical documentation (download)	Provides a downloadable document that contains most of the VMM content that is available in the TechNet Library.	Microsoft Download Center
VMM technical documentation (E-Book)	Provides an E-Book that contains most of the VMM content that is available in the TechNet Library.	E-Book Gallery for Microsoft Technologies
VMM cmdlet reference (download)	Provides the VMM cmdlet help topics.	Microsoft Download Center
Microsoft Server Application Virtualization (Server App-V) documentation	Provides information about using Server App-V to sequence applications that can be deployed by System Center 2012 – Virtual Machine Manager.	Microsoft Server Application Virtualization in the TechNet Library
Release Notes for VMM	Provides information about issues and workarounds for VMM	Release Notes for System Center 2012 – Virtual Machine Manager

Other resources

To ask a question about or to discuss VMM, go to System Center Virtual Machine Manager Forums.

For blog posts from the VMM engineering team, see System Center: Virtual Machine Manager Engineering Team Blog.

For more information about Virtual Machine Manager, see System Center Virtual Machine Manager TechCenter.

Deploying System Center 2012 - Virtual Machine Manager

The following topics provide information to help you deploy and configure Virtual Machine Manager (VMM):

- Specifying a Service Account for VMM
- Configuring Distributed Key Management in VMM
- Pre-Creating the VMM Database
- Installing System Center 2012 - Virtual Machine Manager
- Installing a Highly Available VMM Management Server
- **How to Move a High Availability Deployment of VMM 2012 R2 to a Windows Server 2012 R2 Cluster**

Before you begin the deployment of VMM, ensure that you read the release notes at **Release Notes for System Center 2012 - VMM**, and review system requirements at **System Requirements for System Center 2012 - Virtual Machine Manager**.

After completing the deployment of VMM, it is strongly recommended that you apply the latest Update Rollup that is available from Microsoft Support.

For an overview of VMM, see Overview of System Center 2012 - Virtual Machine Manager.

Cross-Forest Domain Trusts in VMM

In your environment you might have user accounts in one forest and your VMM servers and host in another. In this environment, you must establish a two-way trust between the two cross-forest domains. One-way trusts between cross-forest domains are not supported in VMM.

Pre-Creating the VMM Database

In some organizations, the system administrator that is installing Virtual Machine Manager (VMM) does not have the necessary permissions to create the database that is required by VMM. In this case, the VMM database needs to be created by an authorized administrator before the installation starts. Later, during Setup, you can point at this pre-created database. The VMM database needs to be pre-created as described below.

You can create SQL Scripts with the specified parameters, and then hand these scripts to the SQL administrators to ensure that the database is configured correctly.

How to pre-create the VMM database

1. Create a new database with the following settings:
   - Name: VirtualManagerDB
   - Collation: Latin1_General_100_CI_AS, but aligned with the specific SQL Server instance collation
2. Grant db_owner permissions for this database to the VMM service account
3. Run Setup to install VMM, and on the **Database configuration** page, select to use an existing database. Enter the details of the pre-created database.
4. Specify the VMM service account as the user for the database connection.

Installing System Center 2012 - Virtual Machine Manager

This section shows how to install the different components of Virtual Machine Manager (VMM). Before you install VMM, ensure that the computer meets the minimum hardware requirements and that all prerequisite software is installed. For information about hardware and software requirements for VMM, see **System Requirements for System Center 2012 - Virtual Machine Manager**.

This section also shows how to uninstall VMM.

For information about upgrading to System Center 2012 – Virtual Machine Manager from a previous version of VMM, see Upgrading System Center 2012 - Virtual Machine Manager.

Note
As of System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed.

In This Section

Installing a VMM Management Server

Describes how to install a VMM management server.

Installing and Opening the VMM Console

Describes how to install the VMM console and then use the VMM console to connect to a VMM management server.

Installing and Opening the VMM Self-Service Portal

Describes how to install and then open the VMM Self-Service Portal.

How to Uninstall VMM

Describes how to uninstall VMM.

How to Upgrade from the Evaluation Version of VMM

Describes how to upgrade from an evaluation version of VMM to a licensed version by providing a valid product key

Installing VMM from a Command Prompt

Provides information about how to use .ini files with configurable settings to install features of VMM

Installing a VMM Management Server

This section describes how to install a VMM management server.

Before installing a VMM management server, ensure that the computer meets the minimum hardware requirements and that all prerequisite software is installed. For information about hardware and software requirements for VMM, see **System Requirements for System Center 2012 - Virtual Machine Manager**.

Before you begin the installation of the VMM management server, ensure that you have a computer with a supported version of Microsoft SQL Server installed and running.

For information about installing a highly available VMM management server, see Installing a Highly Available VMM Management Server.

In this Section

Task	Description
How to Install a VMM Management Server	Describes how to install a VMM management server.

How to Install a VMM Management Server

You can use the following procedure to install a System Center 2012 – Virtual Machine Manager (VMM) management server. To install a VMM manger from a command prompt, see Installing VMM from a Command Prompt.

Before you begin the installation of the VMM management server, ensure that you have a computer that is running a supported version of Microsoft SQL Server software. Setup will not automatically install an Express edition of SQL Server. For information on supported versions of

SQL Server and other requirements, see System Requirements: VMM Database. For more general information on SQL Server and System Center, see SQL 2012 and System Center 2012 R2.

In some organizations it might be necessary to pre-create the VMM database before installing VMM. For more information about pre-creating and then using the pre-created database, see Pre-Creating the VMM Database.

In System Center 2012 Service Pack 1 (SP1) and in System Center 2012 R2, we recommend that you do not use the AlwaysOn feature in Microsoft SQL Server. If you use AlwaysOn, and you are running an asynchronous commit mode, the replica of the database can be out of date for a period of time after each commit. This can make it appear as if the database were back in time which might cause loss of customer data, inadvertent disclosure of information, or possibly elevation of privilege.

To complete this procedure, you need, at a minimum, membership in the local Administrators group (or equivalent) on the computer that you are configuring.

To install a VMM management server

1. To start the Virtual Machine Manager Setup wizard, on your installation media, right-click **setup.exe**, and then click **Run as administrator**.

   Note
   Before you begin the installation of VMM, close any open programs and ensure that no restarts are pending on the computer. For example, if you have installed a server role by using Server Manager or have applied a security update, you may need to restart the computer and then log on to the computer by using the same user account to finish the installation of the server role or the security update.

2. On the main setup page, click **Install**.

   If you have not installed the Microsoft .NET Framework, VMM will prompt you to install it now.

3. On the **Select features to install** page, select the **VMM management server** check box, and then click **Next**.

   Note
   The VMM console is automatically installed when you install a VMM management server.

   If you are installing the VMM management server on a computer that is a member of a cluster, the wizard will ask whether you want to make the VMM management server highly available. For more information about installing a highly available VMM management server, see Installing a Highly Available VMM Management Server.

4. On the **Product registration information** page, provide the appropriate information, and then click **Next**. If you do not enter a product key, VMM will be installed as an evaluation

version that expires in 180 days after installation.

5. On the **Please read this license agreement** page, review the license agreement, select the **I have read, understood, and agree with the terms of the license agreement** check box, and then click **Next**.
6. On the **Join the Customer Experience Improvement Program (CEIP)** page, select either option, and then click **Next**.
7. If the **Microsoft Update** page appears, select whether you want to use Microsoft Update, and then click **Next**.

   Note
   If you previously chose to use Microsoft Update on this computer, the **Microsoft Update** page does not appear.
8. On the **Installation location** page, use the default path or type a different installation path for the VMM program files, and then click **Next**.

   The setup program checks the computer on which you are installing the VMM management server to ensure that the computer meets the appropriate hardware and software requirements. If the computer does not meet a prerequisite, a page that contains information about the prerequisite and how to resolve the issue appears. For information about hardware and software requirements for VMM, see **System Requirements for System Center 2012 - Virtual Machine Manager**.

   If the computer meets all prerequisites, the **Database configuration** page appears.
9. On the **Database configuration** page, perform the following steps:
   a. On the **Database configuration** page, specify the name of the computer that is running SQL Server. If you are installing the VMM management server on the same computer that is running SQL Server, then in the **Server name** box, either type the name of the computer (for example, **vmmserver01**) or type **localhost**. If the SQL Server is in a cluster, type the cluster name.
   b. Ensure that the port on the computer that is running SQL Server is open. Then, specify the port that you want to use to communicate with the computer that is running SQL Server. Do not do this unless all of the following conditions are true:
      - SQL Server is running on a remote computer.
      - The SQL Server Browser service is not started on that remote computer.
      - SQL Server is not using the default port of 1433.

      Otherwise, leave the **Port** box empty.
   c. Select or type the name of the instance of SQL Server that you want to use.
   d. Specify whether to create a new database or to use an existing database. If the account to which you are installing the VMM management server does not have the appropriate permissions to create a new SQL Server database, select the **Use the following credentials** check box, and then provide the user name and password of an account that has the appropriate permissions.
10. Click **Next**.
11. On the **Configure service account and distributed key management** page, specify the

account that the VMM service will use. Realize that you cannot change the identity of the VMM service account after installation. For more information about which type of account to use, see Specifying a Service Account for VMM.

Under **Distributed Key Management**, select whether to store encryption keys in Active Directory Domain Services (AD DS). For more information about key management, see Configuring Distributed Key Management in VMM.

After you select an account and, if necessary, enter AD DS information, click **Next**.

12. On the **Port configuration** page, use the default port number for each feature or provide a unique port number that is appropriate in your environment, and then click **Next**.

    Important
    You cannot change the ports that you assign during the installation of a VMM management server unless you uninstall and then reinstall the VMM management server. Also, do not configure any feature to use port 5986, because that port number is preassigned.

13. On the **Library configuration** page, select whether to create a new library share or to use an existing library share on the computer.

    Note
    The default library share that VMM creates is named MSSCVMMLibrary, and the folder is located at %SYSTEMDRIVE%\ProgramData\Virtual Machine Manager Library Files. ProgramData is a hidden folder, and you cannot remove it.

    After the VMM management server is installed, you can add library shares and library servers by using the VMM console or by using the VMM command shell.

    After you specify a library share, click **Next**.

14. On the **Installation summary** page, review your selections and do one of the following:
    - Click **Previous** to change any selections.
    - Click **Install** to install the VMM management server.

    After you click **Install**, the **Installing features** page appears and displays the installation progress.

15. On the **Setup completed successfully** page, click **Close** to finish the installation.

    To open the VMM console, ensure that the **Open the VMM console when this wizard closes** check box is selected. Alternatively for VMM in System Center 2012 SP1 or in System Center 2012 R2, you can click the **Virtual Machine Manager Console** icon on the desktop.

During Setup, VMM enables the following firewall rules. These rules remain in effect even if you later uninstall VMM.

- Windows Remote Management
- Windows Standards-Based Storage Management

Note
If Setup does not finish successfully, consult the log files in the

%SYSTEMDRIVE%\ProgramData\VMMLogs folder. ProgramData is a hidden folder.

Installing and Opening the VMM Console

The procedures in this section describe how to install the VMM console and then use it to connect to a VMM management server.

Important
You cannot use the VMM console from one version of VMM to connect to a different version of VMM.

Before installing the VMM console, ensure that the computer meets the minimum hardware requirements and that all prerequisite software is installed. For information about hardware and software requirements for VMM, see **System Requirements for System Center 2012 - Virtual Machine Manager**.

Note
The VMM console is automatically installed when you install a VMM management server.

In this Section

Follow these steps to install the VMM console and then use the VMM console to connect to a VMM management server.

Task	Description
Step 1: How to Install the VMM Console	Describes how to install the VMM console.
Step 2: How to Connect to a VMM Management Server by Using the VMM Console	Describes how to use the VMM console to connect to a VMM management server.

How to Install the VMM Console

You can use the following procedure to install a VMM console.

To complete this procedure, you need, at a minimum, membership in the local Administrators group (or equivalent) on the computer that you are configuring.

To install the VMM console

1. To start the Virtual Machine Manager Setup Wizard, on your installation media, right-click **setup.exe**, and then click **Run as administrator**.
2. On the main setup page, click **Install**.
3. On the **Select features to install** page, select the **VMM console** check box, and then

click **Next**.

4. On the **Please read this notice page**, click **I agree with the terms of this notice**, and then click **Next**.
5. Review the information on the **Customer Experience Improvement Program** page, and then click **Next**.
6. On the **Microsoft Update** page, select whether you want to use Microsoft Update, and then click **Next**.

   Note
   If you previously chose to use Microsoft Update on this computer, the **Microsoft Update** page does not appear.
7. On the **Installation location** page, type an installation path for the VMM program files or use the default path, and then click **Next**.

   The setup program checks the computer on which you are installing the VMM console to ensure that the computer meets the appropriate hardware and software requirements. If your computer does not meet a prerequisite, a page that contains information about the prerequisite and how to resolve the issue appears.

   For information about hardware and software requirements for VMM, see **System Requirements for System Center 2012 - Virtual Machine Manager**.

   If your computer meets all prerequisites, the **Port configuration** page appears.
8. On the **Port configuration** page, type the port that you want to use for the VMM console to communicate with the VMM management server, and then click **Next**.

   Note
   The port setting that you assign for the VMM console should match the port setting that you assigned for the VMM console during the installation of the VMM management server. The default port setting is 8100. Also, do not assign port number 5986, because it is preassigned.
9. On the **Installation summary** page, review your selections and do one of the following:
   - Click **Previous** to change any selections.
   - Click **Install** to install the VMM console.

   After you click **Install**, the **Installing features** page appears and displays the installation progress.
10. On the **Setup completed successfully** page, click **Close** to finish the installation.

    To open the VMM console, ensure that the **Open the VMM console when this wizard closes** check box is selected.

Note
If setup does not finish successfully, consult the log files in the %SYSTEMDRIVE%\ProgramData\VMMLogs folder. ProgramData is a hidden folder.

How to Connect to a VMM Management Server by Using the VMM Console

You can use the following procedure to use the VMM console to connect to a VMM management server.

To use the VMM console, you must be a member of a user role in VMM.

To connect to a VMM management server by using the VMM console

1. On a computer on which the VMM console is installed, click **Start**, click **All Programs**, click **Microsoft System Center 2012**, click **Virtual Machine Manager**, and then click **Virtual Machine Manager Console**. Alternatively for VMM in System Center 2012 SP1 and in System Center 2012 R2, you can click the **Virtual Machine Manager Console** icon on the desktop.
2. In the **Connect to Server** dialog box, do one of the following:
   - If you installed the VMM console on the same computer as the VMM management server, the **Server name** box contains the local VMM management server (localhost) using the port that you assigned during the installation of the VMM management server. The default port setting is 8100.
   - To use the VMM console to connect to a VMM management server that is installed on a different computer, in the **Server name** box, type the name of the computer on which the VMM management server is installed, followed by a colon, and then the connection port that you assigned during the installation of that VMM management server. For example, type **vmmserver01:8100**.
3. If you want to connect using an account other than the current account, select **Specify credentials** and then enter a **User name** and **Password**.

   Note
   If you want to connect to another VMM management server the next time that you open the VMM console, ensure that the **Automatically connect with these settings** check box is not selected.
4. Click **Connect**.
5. If your account belongs to more than one user role for this VMM management server, the **Select User Role** dialog box appears. In the **Select User Role** dialog box, select the user role that you would like to use for your session, and then click **OK**.

Installing and Opening the VMM Self-Service Portal

Note
As of System Center 2012 Service Pack 1 (SP1), the Virtual Machine Manager (VMM) Self-Service Portal has been removed.

You can use the VMM Self-Service Portal in System Center 2012 – Virtual Machine Manager to perform the following tasks:

- Create a new virtual machine from a template and deploy the virtual machine to a private cloud to which you have been assigned.
- Perform actions on a virtual machine, such as start, stop, and shut down. Your administrator determines the actions that you can perform on a virtual machine.

In System Center 2012 – Virtual Machine Manager, you can also use the VMM console to perform these tasks. Your administrator might grant you additional capabilities when you use the VMM console—capabilities that are not available when you use the VMM Self-Service Portal. For example, your administrator might grant you the ability to create and share virtual machine templates.

The procedures in this section describe how to install and then open the VMM Self-Service Portal.

Before you install the VMM Self-Service Portal, ensure that the computer meets the minimum hardware requirements and that all prerequisite software is installed. For information about hardware and software requirements for VMM, see **System Requirements for System Center 2012 - Virtual Machine Manager**.

In this section

Follow these steps to install the VMM Self-Service Portal.

Task	Description
Step 1: How to Install the VMM Self-Service Portal	Describes how to install the VMM Self-Service Portal
Step 2: How to Open the VMM Self-Service Portal	Describes how to open the VMM Self-Service Portal

How to Install the VMM Self-Service Portal

Note
As of System Center 2012 Service Pack 1 (SP1), the Virtual Machine Manager (VMM) Self-Service Portal has been removed.

You can use the following procedure to install the VMM Self-Service Portal in System Center 2012 – Virtual Machine Manager (VMM).

Note
If there is a problem with setup completing successfully, consult the log files in the **%SYSTEMDRIVE%\ProgramData\VMMLogs** folder. **ProgramData** is a hidden folder.

Membership in the local Administrators group, or equivalent, on the computer that you are configuring is the minimum required to complete this procedure.

How to install the VMM Self-Service Portal

1. To start the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard, on your installation media, right-click **setup.exe**, and then click **Run as administrator**.

   Note
   Before beginning the installation of VMM, close any open programs and ensure that there are no pending restarts on the computer. For example, if you have installed a server role by using Server Manager or have applied a security update, you may need to restart the computer and then log on to the computer with the same user account to finish the installation of the server role or the security update.

2. On the main setup page, click **Install**.
3. On the **Select features to install** page, select the **VMM Self-Service Portal** check box, and then click **Next**.
4. On the **Please read this notice page**, click **I agree with the terms of this notice**, and then click **Next**.
5. On the **Microsoft Update** page, select whether or not you want to use Microsoft Update, and then click **Next**.

   Note
   If you have previously chosen to use Microsoft Update on this computer, the **Microsoft Update** page does not appear.

6. On the **Installation location** page, use the default path or type a different installation path for the VMM program files, and then click **Next**.

   The computer on which you are installing the VMM Self-Service Portal will be checked to ensure that the appropriate hardware and software requirements are met. If a prerequisite is not met, a page will appear with information about which prerequisite has not been met and how to resolve the issue.

   For information about hardware and software requirements for VMM, see **System Requirements for System Center 2012 - Virtual Machine Manager**.

   If all prerequisites have been met, the **Self-Service portal configuration** page will appear.

7. On the **Self-Service portal configuration** page, specify the following:
   - The name of the VMM management server to which the VMM Self-Service Portal will connect.
   - The port that the VMM Self-Service Portal will use to communicate with the VMM management server.
   - Under **Web Server**, the port that self-service users will use to connect to the VMM Self-Service Portal.

     If the default port for the VMM Self-Service Portal (port 80) is being used by another web site on the computer, you must either use a different dedicated port or specify a host header for the Self-Service Portal. For more information about host headers, see Configure a Host Header for a Web Site (IIS 7).

8. On the **Installation summary** page, review your selections and do one of the following:
   - Click **Previous** to change any selections.
   - Click **Install** to install the VMM Self-Service Portal.

   After you click **Install**, the **Installing features** page appears and installation progress is displayed.
9. On the **Setup completed successfully** page, click **Close**.

How to Open the VMM Self-Service Portal

Note
As of System Center 2012 Service Pack 1 (SP1), the Virtual Machine Manager (VMM) Self-Service Portal has been removed.

You can use either of the following procedures to open the VMM Self-Service Portal. To use the VMM Self-Service Portal, client computers must be running Internet Explorer 8.

Before users can access the VMM Self-Service Portal, you must create at least one Self-Service User user role and add the appropriate user accounts or Active Directory groups as members of the user role. For more information about creating Self-Service User user roles, see How to Create a Self-Service User Role in VMM.

Note
In System Center 2012 – Virtual Machine Manager, self-service users can also use the VMM console to perform the same tasks that they can perform in the Self-Service Portal. In addition, there are some tasks that self-service users can perform only by using the VMM console.

In the VMM console, self-service users only see the objects and tasks that are within the scope of their user role. For more information about using the VMM console, see Installing and Opening the VMM Console.

To open the VMM Self-Service Portal on the Web server

1. On a computer on which the VMM Self-Service Portal is installed, click **Start**, click **All Programs**, click **Microsoft System Center 2012**, click **Virtual Machine Manager**, and then click **Virtual Machine Manager Self-Service Portal**.
2. On the logon page, provide the appropriate credentials, and then click **Log On**.

To open the VMM Self-Service Portal in a Web browser

1. In a Web browser, specify the Self-Service Portal web site in one of the following formats:
   - If the Self-Service Portal web site is using a dedicated port, type **http://** followed by the computer name of the web server, a colon (:), and then the port number. For example, type **http://webserver:80**.
   - If the Self-Service Portal web site is not using a dedicated port, then type **http://**

followed by the host header name.

- If SSL has been enabled, then you must type **https://** for the start of the web site address.

2. On the logon page, provide the appropriate credentials, and then click **Log On**.

How to Uninstall VMM

You can use the following procedures to uninstall a VMM management server, the VMM console, or the VMM Self-Service Portal.

Note
As of System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed.

Before uninstalling VMM, ensure that the VMM console and the VMM command shell are closed.

Note
If there is a problem with uninstallation completing successfully, consult the log files in the **%SYSTEMDRIVE%\ProgramData\VMMLogs** folder. **ProgramData** is a hidden folder.

Membership in the local Administrators group, or equivalent, on the computer that you are configuring is the minimum required to complete these procedures.

To uninstall a VMM management server

1. On the computer on which the VMM management server is installed, click **Start**, and then click **Control Panel**.
2. Under **Programs**, click **Uninstall a program**.
3. Under **Name**, double-click **Microsoft System Center 2012 Virtual Machine Manager**.
4. On the **What would you like to do?** page, click **Remove features**.
5. On the **Select features to remove** page, select the **VMM management server** check box, and then click **Next**.

   Note
   If you also want to uninstall the VMM console, select the **VMM console** check box.
6. On the **Database options** page, select whether you want to retain or remove the VMM database, and, if necessary, credentials for the database, and then click **Next**.
7. On the **Summary** page, review your selections and do one of the following:
   - Click **Previous** to change any selections.
   - Click **Uninstall** to uninstall the VMM management server.

   After you click **Uninstall**, the **Uninstalling features** page appears and uninstallation progress is displayed.
8. After the VMM management server is uninstalled, on the **The selected features were**

removed successfully page, click **Close**.

The following firewall rules, which were enabled during VMM Setup, remain in effect after you uninstall VMM:

- File Server Remote Management
- Windows Standards-Based Storage Management firewall rules

Note

If there is a problem with setup completing successfully, consult the log files in the **%SYSTEMDRIVE%\ProgramData\VMMLogs** folder. **ProgramData** is a hidden folder.

To uninstall the VMM console

1. On the computer on which the VMM console is installed, click **Start**, and then click **Control Panel**.
2. Under **Programs**, click **Uninstall a program**.
3. Under **Name**, double-click **Microsoft System Center 2012 Virtual Machine Manager**.
4. On the **What would you like to do?** page, click **Remove features**.
5. On the **Select features to remove** page, select the **VMM console** check box, and then click **Next**.

   Note

   If a VMM management server is also installed on the computer, you must also uninstall the VMM management server.
6. On the **Summary** page, review your selections and do one of the following:
   - Click **Previous** to change any selections.
   - Click **Uninstall** to uninstall the VMM console.

   After you click **Uninstall**, the **Uninstalling features** page appears and uninstallation progress is displayed.
7. After the VMM console is uninstalled, on the **The selected features were removed successfully** page, click **Close**.

To uninstall the VMM Self-Service Portal

1. On the computer on which the VMM Self-Service Portal is installed, click **Start**, and then click **Control Panel**.
2. Under **Programs**, click **Uninstall a program**.
3. Under **Name**, double-click **Microsoft System Center 2012 Virtual Machine Manager**.
4. On the **What would you like to do?** page, click **Remove features**.
5. On the **Select features to remove** page, select the **VMM Self-Service Portal** check box, and then click **Next**.
6. On the **Summary** page, review your selections and do one of the following:

- Click **Previous** to change any selections.
- Click **Uninstall** to uninstall the VMM Self-Service Portal.

After you click **Uninstall**, the **Uninstalling features** page appears and uninstallation progress is displayed.

7. After the VMM Self-Service Portal is uninstalled, on the **The selected features were removed successfully** page, click **Close**.

Specifying a Service Account for VMM

During the installation of a VMM management server, on the **Configure service account and distributed key management** page, you will need to configure the System Center Virtual Machine Manager service to use either the Local System account or a domain account.

Consider the following before you configure the account that is used by the Virtual Machine Manager service:

- It is not supported to change the identity of the Virtual Machine Manager service account after installation. This includes changing from the local system account to a domain account, from a domain account to the local system account, or changing the domain account to another domain account. To change the Virtual Machine Manager service account after installation, you must uninstall VMM (selecting the **Retain data** option if you want to keep the SQL Server database), and then reinstall VMM by using the new service account.
- If you specify a domain account, the account must be a member of the local Administrators group on the computer.
- If you specify a domain account, it is strongly recommended that you create an account that is specifically designated to be used for this purpose. When a host is removed from the VMM management server, the account that the System Center Virtual Machine Manager service is running under is removed from the local Administrators group of the host. If the same account is used for other purposes on the host, this can cause unexpected results.
- If you plan to use shared ISO images with Hyper-V virtual machines, you must use a domain account.
- If you are using a disjointed namespace, you must use a domain account. For more information about disjointed namespaces, see Naming conventions in Active Directory for computers, domains, sites, and OUs.
- If you are installing a highly available VMM management server, you must use a domain account.

Configuring Distributed Key Management in VMM

During the installation of a System Center 2012 – Virtual Machine Manager (VMM) management server, you must decide whether to store the keys to encrypted data on the local computer or configure distributed key management. On the **Configure service account and distributed key management** page of Setup, you can select to use distributed key management to store

encryption keys in Active Directory Domain Services (AD DS) instead of storing the encryption keys on the computer on which the VMM management server is installed.

By default, VMM encrypts some data in the VMM database by using the Data Protection Application Programming Interface (DPAPI). For example, VMM encrypts Run As account credentials and passwords in guest operating system profiles. VMM also encrypts product key information in virtual hard disk properties for virtual machine role scenarios and configuration. The encryption of this data is tied to the specific computer on which VMM is installed and the service account that VMM uses. Therefore, if you move your VMM installation to another computer, VMM will not retain the encrypted data. In that case, you must enter this data manually to fix the VMM objects.

Distributed key management, however, stores the encryption keys in AD DS. Therefore, if you must move your VMM installation to another computer, VMM will retain the encrypted data because the other computer will have access to the encryption keys in AD DS.

Important

For virtual machine roles, if the encrypted data is not retained, you will not be able to enter it manually, so you will not be able to manage the roles.

If you choose to enable distributed key management, coordinate with your AD DS administrator about creating the appropriate container in AD DS for storing the cryptographic keys.

The following are requirements and considerations for using distributed key management in VMM:

- You must create a container in AD DS before you install VMM. You can create the container by using Active Directory Service Interfaces Editor (ADSI Edit). To install **ADSI Edit**, in **Server Manager** add the feature **AD DS Tools** under **Remote Server Administration Tools**. After installation, **ADSI Edit** is listed on the **Tools** menu in **Server Manager**.
- You must create the container in the same domain as the user account with which you are installing VMM. Also, if you specify a domain account that the VMM service will use, that account must also be in the same domain.

  For example, if the installation account and the service account are both in the corp.contoso.com domain, you must create the container in that domain. So, if you want to create a container that is named **VMMDKM**, you specify the container location as `CN=VMMDKM,DC=corp,DC=contoso,DC=com`.
- After the AD DS administrator has created the container, the account with which you are installing VMM must have Full Control permissions to the container in AD DS. Also, the permissions must apply to this object and all descendant objects of the container.
- If you are installing a highly available VMM management server, you must use distributed key management to store encryption keys in AD DS.

  Distributed key management is required in this scenario because when the Virtual Machine Manager service fails over to another node in the cluster, the Virtual Machine Manager service still needs access to the encryption keys in order to access data in the VMM database. This access is possible only if the encryption keys are stored in a central location like AD DS.

- For future upgrades that involve virtual machine roles, we recommend that you use distributed key management during setup. This will help ensure that virtual machine roles are properly upgraded, and that you can manage them after the upgrade.
- On the **Configure service account and distributed key management** page, you must specify the location of the container in AD DS by typing. For example, by typing **CN=VMMDKM,DC=corp,DC=contoso,DC=com**.

How to Upgrade from the Evaluation Version of VMM

If you did not provide a product key when you installed Virtual Machine Manager (VMM), VMM installs as an evaluation version that expires in 180 days after installation. You can upgrade an evaluation version to a licensed version before the evaluation version expires. After the evaluation version expires, it cannot be upgraded.

To upgrade from an evaluation version of VMM to a licensed version before the expiration date of the evaluation version, you must obtain a valid product key from Microsoft, and you must be a member of the Administrator user role. For information about System Center 2012 – Virtual Machine Manager licensing, see System Center 2012 Licensing.

Tip
The number of days remaining in your evaluation version is displayed in the title bar of the VMM console window.

To upgrade from the evaluation version of VMM to a licensed version

1. In the VMM console, in the upper left corner above the ribbon, click the down arrow, and then click **About**.
2. In the System Center 2012 – Virtual Machine Manager informational dialog box, click **Enter Product Key**.
3. In the **Enter Product Key** dialog box, enter your product key, and then click **Continue**.
4. In the **Please read this license agreement** dialog box, review the license terms, select the **I have read, understood, and agree with the terms of the license agreement** check box, and then click **Accept**.

See Also

Installing System Center 2012 - Virtual Machine Manager

Installing VMM from a Command Prompt

You can install Virtual Machine Manager (VMM) by using a command prompt. Installing VMM features involves saving installation settings in an .ini file and using the **setup.exe** command with that file.

Important

For all of these procedures, use the **Run as administrator** option to open an elevated command prompt.

Installation files

Your installation media contains .ini files for each VMM feature:

- **VMServer.ini**

  Settings for the VMM management server.
- **VMClient.ini**

  Settings for the VMM console.
- **VMEUP.ini**

  Settings for the VMM Self-Service Portal.

  Note
  As of System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed.
- **VMServerUninstall.ini**

  Uninstallation settings for the VMM management server.

The files contain key/value pairs that have default values. These entries are commented out. To edit the file, remove the comment symbol (#) and change the value.

Installing a VMM management server by using a command prompt

To install a VMM management server, edit the VMServer.ini file and then run the **setup.exe** command.

Note
When you install a VMM management server, the VMM console is automatically installed.

Configuring options for a VMM management server in the installation file

Option	Values	Default
ProductKey	Product key in the format: xxxxx-xxxxx-xxxxx-xxxxx-xxxxx	*xxxxx-xxxxx-xxxxx-xxxxx-xxxxx*
UserName	Optional display name for the user who is installing the features. **Note** This is not the user account for the installation.	Administrator

Option	Values	Default
CompanyName	Optional display name for the organization that is installing the features.	Microsoft Corporation
ProgramFiles	Location for VMM files.	C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager
CreateNewSqlDatabase	0: Use an existing Microsoft SQL Server database. 1: Create a new SQL Server database.	1
SqlInstanceName	Name of the new or existing instance of SQL Server.	MICROSOFTVMM
SqlDatabaseName	Name of the new or existing SQL Server database.	VirtualManagerDB
RemoteDatabaseImpersonation	0: Do not impersonate the administrator account for SQL Server. **Important** The user that runs **setup.exe** must be an administrator for the server that is hosting SQL Server. 1: Impersonate the administrator account for SQL Server by using the provided credentials. **Important** The user who runs **setup.exe** must provide values for the *SqlDBAdminName*, *SqlDBAdminPassword*, and *SqlDBAdminDomain* parameters.	0
SqlMachineName	Name of the server that is hosting SQL Server. Do not specify **localhost**. Instead, specify the	<*sqlmachinename*>

Option	Values	Default
	actual name of the computer.	
(various ports)	For information about ports, see Ports and Protocols for VMM.	IndigoTcpPort: 8100 IndigoHTTPSPort: 8101 IndigoNETTCPPort: 8102 IndigoHTTPPort: 8103 WSManTcpPort: 5985 BitsTcpPort: 443
CreateNewLibraryShare	0: Use an existing library share. 1: Create a new library share.	1
LibraryShareName	Name of the file share to be used or created.	MSSCVMMLibrary
LibrarySharePath	Location of the existing file share or the new file share to be created.	C:\ProgramData\Virtual Machine Manager Library Files
LibraryShareDescription	Description of the share.	Virtual Machine Manager Library Files
SQMOptIn	0: Do not opt in to the Customer Experience Improvement Program (CEIP). 1: Opt in to CEIP. For more information about CEIP, see Microsoft Customer Experience Improvement Program. For CEIP privacy information, see Privacy Statement for the Microsoft Customer Experience Improvement Program.	0
MUOptIn	0: Do not opt in to Microsoft Update. 1: Opt in to Microsoft Update. For more information about Microsoft Update, see Frequently Asked Questions. For Microsoft Update privacy information, see Update Services	0

Option	Values	Default
	Privacy Statement.	
VmmServiceLocalAccount	0: Use a domain account for the VMM service (scvmmservice). 1: Use the Local System account for the VMM service. **Note** To use a domain account, when you run **setup.exe**, provide values for the *VMMServiceDomain*, *VMMServiceUserName*, and *VMMServiceUserPassword* parameters. For more information about service accounts, see Specifying a Service Account for VMM.	0
TopContainerName	Container for Distributed Key Management (DKM); for example, “CN=DKM,DC=contoso,DC=com”. For more information about DKM, see Configuring Distributed Key Management in VMM.	VMMServer
HighlyAvailable	0: Do not install as highly available. 1: Install as highly available. For information about highly available installations, see Installing a Highly Available VMM Management Server.	0
VmmServerName	Clustered service name for a highly available VMM management server. **Important** Do not enter the name of the failover cluster or the name of the computer on which the highly available	<*VMMServerName*>

Option	Values	Default
	VMM management server is installed. For more information, see How to Install a Highly Available VMM Management Server.	
VMMStaticIPAddress	IP address for the clustered service name for a highly available VMM management server, if you are not using Dynamic Host Configuration Protocol (DHCP). **Note** Both IPv4 and IPv6 are supported.	*<comma-separated-ip-for-HAVMM>*
Upgrade	0: Do not upgrade from a previous version of VMM to System Center 2012 – Virtual Machine Manager. 1: Upgrade from a previous version.	1

Installing a VMM management server by using a command prompt

After you edit VMServer.ini, open an elevated command prompt, and then run **setup.exe** by using the following parameters:

- */server*

  Specifies installation of the VMM management server.
- */i* or */x*

  Specifies whether to install (*/i*) or uninstall (*/x*) the server.
- */f <filename>*

  Specifies the .ini file to use.

  Important
  Be sure that this parameter points to the correct .ini file. If **setup.exe** does not find an .ini file, it will perform the installation by using its own default values.
- */VmmServiceDomain <domainName>*

  Specifies the domain name for the account that is running the VMM service (scvmmservice). Use this parameter only if you set *VmmServiceLocalAccount* to 0 in VMServer.ini.
- */VmmServiceUserName <userName>*

Specifies the user name for the account that is running the VMM service (scvmmservice). Use this parameter only if you set *VmmServiceLocalAccount* to 0 in VMServer.ini.

- */VmmServiceUserPassword <password>*

  Specifies the password for the account that is running the VMM service (scvmmservice). Use this parameter only if you set *VmmServiceLocalAccount* to 0 in VMServer.ini.

- */SqlDBAdminDomain <domainName>*

  Specifies the domain name for the administrator account for the SQL Server database. Use this parameter if the current user does not have administrative rights to SQL Server.

- */SqlDBAdminName <userName>*

  Specifies the user name for the administrator account for the SQL Server database. Use this parameter if the current user does not have administrative rights to SQL Server.

- */SqlDBAdminPassword <password>*

  Specifies the password for the administrator account for the SQL Server database. Use this parameter if the current user does not have administrative rights to SQL Server.

- */IACCEPTSCEULA* (as of System Center 2012 SP1)

  Notes acceptance of the Microsoft Software License Terms. This is a mandatory parameter.

For example, to use a VMServer.ini file that is stored in C:\Temp with a SQL Server administrator account of contoso\SQLAdmin01 and a VMM service account of contoso\VMMadmin14, use the following command:

setup.exe /server /i /f C:\Temp\VMServer.ini /SqlDBAdminDomain contoso /SqlDBAdminName SQLAdmin01 /SqlDBAdminPassword password123 /VmmServiceDomain contoso /VmmServiceUserName VMMadmin14 /VmmServiceUserPassword password456 /IACCEPTSCEULA

Uninstalling a VMM management server by using a command prompt

To uninstall a VMM management server, edit the VMServerUninstall.ini file and then run the **setup.exe** command.

Configuring options for uninstalling a VMM management server

Option	Values	Default
RemoteDatabaseImpersonation	0: Local SQL Server installation. 1: Remote SQL Server installation. When you run **setup.exe**, provide a value for the *SqlDBAdminName*, *SqlDBAdminPassword*, and *SqlDBAdminDomain* parameters unless the user who is running **setup.exe** is an administrator for	0

Option	Values	Default
	SQL Server. Replaces the OnRemoteServer setting in VMM 2008 R2.	
RetainSqlDatabase	0: Remove the SQL Server database. 1: Do not remove the SQL Server database. **Important** To remove the SQL Server database, when you run **setup.exe**, provide a value for the *SqlDBAdminName*, *SqlDBAdminPassword*, and *SqlDBAdminDomain* parameters unless the user who is running Setup is an administrator for SQL Server.	0
ForceHAVMMUninstall	0: Do not force uninstallation if **setup.exe** cannot verify whether this node is the final node of the highly available installation. 1: Force the uninstallation. For more information about uninstalling a highly available VMM management server, see How to Uninstall a Highly Available VMM Management Server.	0

Uninstalling a VMM management server by using a command prompt

To uninstall a VMM management server by using a VMServerUninstall.ini file that is stored in C:\Temp, with a SQL Server administrator account of contoso\SQLAdmin01, use this command:

setup.exe /server /x /f C:\Temp\VMServerUninstall.ini /SqlDBAdminDomain contoso /SqlDBAdminName SQLAdmin01 /SqlDBAdminPassword password123

Installing or uninstalling a VMM console by using a command prompt

To install a VMM console, edit the VMClient.ini file and then run the **setup.exe** command.

To uninstall a VMM console, run the **setup.exe** command. There is no separate .ini file for uninstalling the VMM console.

Note
Do not attempt to uninstall the VMM console from a system that includes a VMM management server. You must first uninstall the VMM management server.

Configuring options for a VMM console

Option	Values	Default
ProgramFiles	Location for VMM files.	C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager
IndigoTcpPort	Port that is used for communication between the VMM management server and the VMM console.	8100
MUOptIn	0: Do not opt in to Microsoft Update. 1: Opt in to Microsoft Update. For more information about Microsoft Update, see Frequently Asked Questions. For Microsoft Update privacy information, see Update Services Privacy Statement.	0
VmmServerForOpsMgrConfig	This setting is not used. For more information, see Configuring Operations Manager Integration with VMM.	<*VMMServerName*>

Installing a VMM console by using a command prompt

After you edit VMClient.ini, use an elevated command prompt to run **setup.exe** by using the following parameters:

- */client*

  Specifies installation of the VMM console.
- */i* or */x*

  Specifies whether to install (*/i*) or uninstall (*/x*) the console.
- */f <filename>*

  Specifies the .ini file to use.

  Important
  Be sure that this parameter points to the correct .ini file. If **setup.exe** does not find an .ini file, it will perform the installation by using its own default values.
- */opsmgr*

  Specifies whether to configure a preinstalled instance of System Center Operations Manager 2007.

  Caution
  Do not use this parameter. For more information, see Configuring Operations Manager Integration with VMM.

For example, to use a VMClient.ini file that is stored in C:\Temp, use this command:

setup.exe /client /i /f C:\Temp\VMClient.ini

Installing the VMM Self-Service Portal by using a command prompt

Note
In System Center 2012 SP1, the VMM Self-Service Portal has been removed.

To install the VMM Self-Service Portal, edit the VMEUP.ini file and then run the **setup.exe** command.

To uninstall the VMM Self-Service Portal, run the **setup.exe** command. There is no separate .ini file for uninstalling the VMM Self-Service Portal.

Configuring options for the VMM Self-Service Portal installation

Option	Values	Default
ProgramFiles	Location in which to store program files.	C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager
VmmServerName	Name of the VMM management server that this VMM Self-Service Portal connects to.	*<machineName>*

Option	Values	Default
IndigoTcpPort	Port that is used for communication between the VMM management server and the VMM Self-Service Portal.	8100
SelfServicePortalTcpPort	Port that users use to connect to the VMM Self-Service Portal.	80
SelfServicePortalHeader	If other websites on this server are using the same port, specify a header for the VMM Self-Service Portal. For more information about headers, see How to Install the VMM Self-Service Portal.	*<headerName>*
MUOptIn	0: Do not opt in to Microsoft Update. 1: Opt in to Microsoft Update. For more information about Microsoft Update, see Frequently Asked Questions. For Microsoft Update privacy information, see Update Services Privacy Statement.	0

Installing or uninstalling the VMM Self-Service Portal by using a command prompt

After you edit VMEUP.ini, use an elevated command prompt to run **setup.exe** by using the following parameters:

- */eup*

  Specifies installation of the VMM Self-Service Portal.
- */i* or */x*

  Specifies whether to install (*/i*) or uninstall (*/x*) the VMM Self-Service Portal.
- */f <filename>*

  Specifies the .ini file to use.

Important

Be sure that this parameter points to the correct .ini file. If **setup.exe** does not find an .ini file, it will perform the installation by using its own default values.

To use a VMEUP.ini file that is stored in C:\Temp to install the VMM Self-Service Portal, use this command:

setup.exe /eup /i /f C:\Temp\VMEUP.ini

To uninstall the VMM Self-Service Portal, use this command:

setup.exe /eup /x

Installing a Highly Available VMM Management Server

The procedures in this section describe how to do the following in Virtual Machine Manager (VMM):

- How to Install a Highly Available VMM Management Server
- How to Install a VMM Management Server on an Additional Node of a Cluster
- How to Connect to a Highly Available VMM Management Server by Using the VMM Console
- How to Uninstall a Highly Available VMM Management Server

Before you begin the installation of a highly available VMM management server, ensure the following:

- You have installed and configured a failover cluster running Windows Server 2008 R2, or Windows Server 2008 R2 with Service Pack 1 (SP1), or Windows Server 2012. For more information about installing and configuring a failover cluster, see Overview of Failover Clusters, or Failover Clustering Overview for Windows Server 2012.
- All computers on which you are installing the highly available VMM management server meet the minimum hardware requirements and that all prerequisite software is installed on all computers. For information about hardware and software requirements for VMM, see **System Requirements for System Center 2012 - Virtual Machine Manager**.
- You have created a domain account that will be used by the Virtual Machine Manager service. You must use a domain account for a highly available VMM management server. For more information about using a domain account, see Specifying a Service Account for VMM.
- You are prepared to use distributed key management to store encryption keys in Active Directory Domain Services (AD DS). You must use distributed key management for a highly available VMM management server. For more information about distributed key management, see Configuring Distributed Key Management in VMM.
- You have a computer with a supported version of Microsoft SQL Server installed and running before you start the installation of VMM. For information about supported versions of SQL Server for the VMM database, see **System Requirements for System Center 2012 - Virtual Machine Manager**.

The following are some recommendations to consider for installing highly available VMM management servers in VMM:

- We recommend that you use a highly available installation of SQL Server.
- We recommend that the highly available installation of SQL Server is installed on a separate failover cluster from the failover cluster on which you are installing the highly available VMM management server.
- We also recommend that you use a highly available file server for hosting your library shares.

The following are some additional considerations about highly available VMM management servers in VMM:

- You can only have one implementation of a highly available VMM management server on a given failover cluster.
- You can have VMM management servers installed on as many as sixteen nodes on a failover cluster, but there can only be one node active at any time.
- You cannot perform a planned failover (for example, to install a security update or to do maintenance on a node of the cluster) by using the VMM console. To perform a planned failover, use Failover Cluster Manager.
- During a planned failover, ensure that there are no tasks actively running on the VMM management server. Any running tasks will fail during a failover. Any failed jobs will not start automatically after a failover.
- Any connections to a highly available VMM management server from the VMM console or the VMM Self-Service Portal will be lost during a failover. The VMM console will be able to reconnect automatically to the highly available VMM management server after a failover.

Note

As of System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed.

How to Install a Highly Available VMM Management Server

You can use the following procedure to install a highly available VMM management server on the first node of a cluster in Virtual Machine Manager (VMM). To install on the other nodes of the cluster, see How to Install a VMM Management Server on an Additional Node of a Cluster.

Membership in the local **Administrators** group, or equivalent, on the computer that you are configuring is the minimum required to complete this procedure.

To install a highly available VMM management server on the first node of a cluster

1. On the first node of your cluster, start the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard. To start the wizard, on your installation media, right-click **setup.exe**, and then click **Run as administrator**.

   Note

   Before beginning the installation of VMM, close any open programs and ensure that there are no pending restarts on the computer. For example, if you have installed a server role by using Server Manager or have applied a security update, you may need to restart the computer and then log on to the computer

with the same user account to finish the installation of the server role or the security update.

2. On the main setup page, click **Install**.
3. On the **Select features to install** page, select the **VMM management server** check box. The VMM console is automatically installed when you install a VMM management server.

   We recommend that you do not install the VMM Self-Service Portal on the same highly available server as the VMM management server. For more about installing the Self-Service Portal, see Installing and Opening the VMM Self-Service Portal.

   Note
   As of System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed.
4. When you are prompted whether you want to make the VMM management server highly available, click **Yes**.
5. On the **Select features to install** page, click **Next**.
6. On the **Product registration information** page, provide the appropriate information, and then click **Next**. If you do not enter a product key, VMM will be installed as an evaluation version that expires in 180 days after installation.
7. On the **Please read this license agreement** page, review the license agreement, select the **I have read, understood, and agree with the terms of the license agreement** check box, and then click **Next**.
8. On the **Join the Customer Experience Improvement Program (CEIP)** page, select either option, and then click **Next**.
9. On the **Microsoft Update** page, select whether or not you want to use Microsoft Update, and then click **Next**.

   Note
   If you have previously chosen to use Microsoft Update on this computer, the **Microsoft Update** page does not appear.
10. On the **Installation location** page, use the default path or type a different installation path for the VMM program files, and then click **Next**.

    The computer on which you are installing the highly available VMM management server will be checked to ensure that the appropriate hardware and software requirements are met. If a prerequisite is not met, a page will appear with information about which prerequisite has not been met and how to resolve the issue. If all prerequisites have been met, the **Database configuration** page will appear.

    For information about hardware and software requirements for VMM, see **System Requirements for System Center 2012 - Virtual Machine Manager**.
11. On the **Database configuration** page, do the following:
    - Specify the name of the computer that is running Microsoft SQL Server. If you are installing the highly available VMM management server on the same computer that is running SQL Server (which is not recommended), in the **Server name** box, either

type the name of the computer (for example, vmmserver01) or type **localhost**.

- Specify the port to use for communication with the computer that is running SQL Server, if all of the following conditions are true:
  - SQL Server is running on a remote computer.
  - The SQL Server Browser service is not started on that remote computer.
  - SQL Server is not using the default port of 1433.

  Otherwise, leave the **Port** box empty.
- Select or type the name of the instance of SQL Server to use.
- Specify whether to create a new database or to use an existing database. If the account with which you are installing the VMM management server does not have the appropriate permissions to create a new SQL Server database, select the **Use the following credentials** check box and provide the user name and password of an account that does have the appropriate permissions.

After you have entered this information, click **Next**.

12. On the **Cluster configuration** page, do the following:
    - In the **Name** box, type the name you want to give to this highly available VMM management server implementation. For example, type **havmmcontoso**. Do not enter the name of the failover cluster or the name of the computer on which the highly available VMM management server is installed.

      You will use this clustered service name when you connect to this highly available VMM management server implementation by using the VMM console. Because there will be multiple nodes on the failover cluster that have the VMM management server feature installed, you need a single name to use when you connect to your VMM environment by using the VMM console.
    - If you are using static IPv4 addresses, you must specify the IP address to assign to the clustered service name. The clustered service name and its assigned IP address will be registered in DNS. If you are using IPv6 addresses or you are using DHCP, no additional configuration is needed.

    After you have entered this information, click **Next**.
13. On the **Configure service account and distributed key management** page, do the following:
    - Under **Virtual Machine Manager Service Account**, select **Domain account**, and then provide the name and password of the domain account that will be used by the Virtual Machine Manager service. You must use a domain account for a highly available VMM management server. For more information about using a domain account, see Specifying a Service Account for VMM.
    - Under **Distributed Key Management**, specify the location in Active Directory to store encryption keys. For example, type **CN=VMMDKM,DC=contoso,DC=com**.

      You must use distributed key management to store the encryption keys in Active Directory for a highly available VMM management server. For more information about distributed key management, see Configuring Distributed Key Management in VMM.

      After you have specified the necessary information on the **Configure service**

account and distributed key management page, click **Next**.

14. On the **Port configuration** page, provide unique port numbers for each feature and that are appropriate for your environment, and then click **Next**.

    Important
    The ports that you assign during the VMM management server installation cannot be changed without uninstalling and reinstalling the VMM management server.

15. On the **Library configuration** page, click **Next**.

    Note
    After you install VMM, you will need to add a library share. Be sure to use the **Add Default Resources** option to add Application Frameworks resources. For more information on adding a library share, see How to Add a Library Server or Library Share.

16. On the **Installation summary** page, review your selections and do one of the following:
    - Click **Previous** to change any selections.
    - Click **Install** to install the highly available VMM management server.

    After you click **Install**, the **Installing features** page appears and installation progress is displayed.

17. On the **Setup completed successfully** page, click **Close** to finish the installation.

    To open the VMM console, ensure that the **Open the VMM console when this wizard closes** check box is selected.

    For information about connecting to a highly available VMM management server by using the VMM console, see How to Connect to a Highly Available VMM Management Server by Using the VMM Console.

    To install on the other nodes of the cluster, see How to Install a VMM Management Server on an Additional Node of a Cluster.

Note
If there is a problem with setup completing successfully, consult the log files in the **%SYSTEMDRIVE%\ProgramData\VMMLogs** folder. **ProgramData** is a hidden folder.

How to Install a VMM Management Server on an Additional Node of a Cluster

You can use the following procedure to install a highly available VMM management server on an additional cluster node in Virtual Machine Manager (VMM). For installing on the first node of a cluster, see How to Install a Highly Available VMM Management Server.

Note

If there is a problem with setup completing successfully, consult the log files in the **%SYSTEMDRIVE%\ProgramData\VMMLogs** folder. **ProgramData** folder is a hidden folder.

Membership in the local **Administrators** group, or equivalent, on the computer that you are configuring is the minimum required to complete this procedure.

To install a highly available VMM management server on an additional node of a cluster

1. On an additional node of your cluster, start the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard. To start the wizard, on your installation media, right-click **setup.exe**, and then click **Run as administrator**.

   Note
   Before beginning the installation of VMM, close any open programs and ensure that there are no pending restarts on the computer. For example, if you have installed a server role by using Server Manager or have applied a security update, you may need to restart the computer and then log on to the computer with the same user account to finish the installation of the server role or the security update.
2. On the main setup page, click **Install**.
3. On the **Select features to install** page, select the **VMM management server** check box. The VMM console is automatically installed when you install a VMM management server.

   We recommend that you do not install the VMM Self-Service Portal on the same highly available server as the VMM management server. For more about installing the Self-Service Portal, see Installing and Opening the VMM Self-Service Portal.

   Note
   As of System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed.
4. When you are prompted whether you want to add this VMM management server to the existing highly VMM management server installation, click **Yes**.
5. On the **Select features to install** page, click **Next**.
6. On the **Product registration information** page, provide the appropriate information, and then click **Next**. If you do not enter a product key, VMM will be installed as an evaluation version that expires in 180 days after installation.
7. On the **Please read this license agreement** page, review the license agreement, select the **I have read, understood, and agree with the terms of the license agreement** check box, and then click **Next**.
8. On the **Join the Customer Experience Improvement Program (CEIP)** page, select either option and then click **Next**.
9. On the **Microsoft Update** page, select whether or not you want to use Microsoft Update, and then click **Next**.

   Note

If you have previously chosen to use Microsoft Update on this computer, the **Microsoft Update** page does not appear.

10. On the **Installation location** page, use the default path or type a different installation path for the VMM program files, and then click **Next**.

    The computer on which you are installing the highly available VMM management server will be checked to ensure that the appropriate hardware and software requirements are met. If a prerequisite is not met, a page will appear with information about which prerequisite has not been met and how to resolve the issue. If all prerequisites have been met, the **Database configuration** page will appear.

    For information about hardware and software requirements for VMM, see **System Requirements for System Center 2012 - Virtual Machine Manager**.

11. On the **Database configuration** page, the database server is displayed as a read-only value in the **Server name** text box. If the account you are using does not have permissions for that database, select **Use the following credentials**, and then type credentials for the database. Click **Next** to continue.
12. On the **Configure service account and distributed key management** page, provide the password of the domain account that will be used by the Virtual Machine Manager service.
13. On the **Port configuration** page, click **Next**.
14. On the **Library configuration** page, click **Next**.
15. On the **Installation summary** page, review your selections and do one of the following:
    - Click **Previous** to change any selections.
    - Click **Install** to install the highly available VMM management server.

    After you click **Install**, the **Installing features** page appears and installation progress is displayed.
16. On the **Setup completed successfully** page, click **Close** to finish the installation.

    To open the VMM console, ensure that the **Open the VMM console when this wizard closes** check box is selected.

    For information about connecting to a highly available VMM management server by using the VMM console, see How to Connect to a Highly Available VMM Management Server by Using the VMM Console.

How to Connect to a Highly Available VMM Management Server by Using the VMM Console

You can use the following procedure to connect to a highly available VMM management server by using the VMM console.

To use the VMM console, you must be a member of a user role in VMM. For more information about user roles, see Creating User Roles in VMM.

To connect to a highly available VMM management server by using the VMM console

1. On a computer on which the VMM console is installed, click **Start**, click **All Programs**, click **Microsoft System Center 2012**, click **Virtual Machine Manager**, and then click **Virtual Machine Manager Console**.

   Note
   We recommend that you install the VMM console on a different computer from the highly available VMM management server installation and use that VMM console to connect to the highly available VMM management server. For more information about installing the VMM console, see Installing and Opening the VMM Console.

2. In the **Connect to Server** dialog box, in the **Server name** box, type the clustered service name for your highly available VMM management server implementation, followed by a colon, and then the connection port that you assigned during the installation of the highly available VMM management server. For example, type **havmmcontoso:8100**.

   Important
   The clustered service name is the name that is entered on the **Cluster configuration** page during the installation of the highly available VMM management server. Do not enter the name of the failover cluster or the name of the computer on which the highly available VMM management server is installed.

   By connecting using the clustered service name, the VMM console will be able to reconnect automatically to the highly available VMM management server after a failover.

3. If you want to connect using an account other than the current account, select **Specify credentials** and then enter a **User name** and **Password**.

   Note
   If you want to connect to another VMM management server the next time that you open the VMM console, ensure that the **Automatically connect with these settings** check box is not selected.

4. Click **Connect**.
5. If your account belongs to more than one user role for this VMM management server, the Select User Role dialog box appears. In the **Select User Role** dialog box, select the user role that you would like to use for your session, and then click **OK**.

How to Uninstall a Highly Available VMM Management Server

You can use the following procedures to uninstall a highly available VMM management server. To uninstall high availability completely, you will need to uninstall highly available VMM management server from each node in the cluster.

Before uninstalling VMM, ensure that the VMM console and the VMM command shell are closed. If you are uninstalling an additional node of a highly available VMM management server, use Failover Cluster Manager to ensure that the node is not currently the owner of the highly available service. If the node is the current owner, move the service to another node in the cluster.

Membership in the local Administrators group, or equivalent, on the computer that you are configuring is the minimum required to complete these procedures.

To uninstall an additional node of a highly available VMM management server

1. On a computer on which the highly available VMM management server is installed, click **Start**, and then click **Control Panel**.
2. Under **Programs**, click **Uninstall a program**.
3. Under **Name**, double-click **Microsoft System Center 2012 Virtual Machine Manager**.
4. On the **What would you like to do?** page, click **Remove features**.
5. On the **Select features to remove** page, select the **VMM management server** check box, and then click **Next**.

   Note
   If you also want to uninstall the VMM console, select the **VMM console** check box.
6. On the **Database options** page, click **Next**.
7. On the **Summary** page, review your selections and do one of the following:
   - Click **Previous** to change any selections.
   - Click **Uninstall** to uninstall the VMM management server.

   After you click **Uninstall**, the **Uninstalling features** page appears and uninstallation progress is displayed.
8. After the VMM management server is uninstalled, on the **The selected features were removed successfully** page, click **Close**.

To uninstall the last node of a highly available VMM management server

1. On the last node on which the highly available VMM management server is installed, click **Start**, and then click **Control Panel**.
2. Under **Programs**, click **Uninstall a program**.
3. Under **Name**, double-click **Microsoft System Center 2012 Virtual Machine Manager**.
4. On the **What would you like to do?** page, click **Remove features**.
5. On the **Select features to remove** page, select the **VMM management server** check box.
6. When you are prompted whether you want to uninstall the last node of the highly available VMM management server, click **Yes**.
7. On the **Select features to remove** page, click **Next**.

   Note

If you also want to uninstall the VMM console, select the **VMM console** check box.

8. On the **Database options** page, select whether you want to retain or remove the VMM database, and, if necessary, enter credentials for the database, and then click **Next**.

   Important
   If you select **Retain database**, you can only use this database with a highly available VMM management server installation. The retained database cannot be used with a standalone installation of VMM management server.

9. On the **Summary** page, review your selections and do one of the following:
   - Click **Previous** to change any selections.
   - Click **Uninstall** to uninstall the VMM management server.
10. After you click **Uninstall**, the **Uninstalling features** page appears and uninstallation progress is displayed.
11. After the VMM management server is uninstalled, on the **The selected features were removed successfully** page, click **Close**.

Note
If there is a problem with uninstallation completing successfully, consult the log files in the **%SYSTEMDRIVE%\ProgramData\VMMLogs** folder. **ProgramData** is a hidden folder.

Upgrading System Center 2012 - Virtual Machine Manager

The following topics provide information to help you upgrade VMM.

- Upgrading to VMM in System Center 2012 R2
- Upgrading to VMM in System Center 2012 SP1
- Upgrading to System Center 2012 - Virtual Machine Manager

Upgrading to VMM in System Center 2012 R2

If you have an existing deployment of Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1), you can upgrade VMM to System Center 2012 R2. This upgrade is basically a fresh installation of System Center 2012 R2, but it retains the VMM database from the System Center 2012 SP1 deployment.

Warning

If you are upgrading two or more System Center components, you must follow the procedures that are documented in the topic Upgrade Sequencing for System Center 2012 R2.

The order in which you perform component upgrades is very important. Failure to follow the correct upgrade sequence might result in component failure for which no recovery options exist. The affected System Center components are:

1. Orchestrator
2. Service Manager
3. Data Protection Manager (DPM)
4. Operations Manager
5. Configuration Manager
6. Virtual Machine Manager
7. App Controller

Retaining encrypted data

Some data in the VMM database, such as the Run As account credentials and passwords in guest operating system profiles, are encrypted by using Windows Data Protection API (DPAPI). Consider the following issues to retain encrypted data when you perform your upgrade:

- **Management server** The VMM management server must be installed on the same computer where VMM was previously installed, unless distributed key management was used.
- **Service account** You must use the same System Center Virtual Machine Manager service account that you used in your previous installation of VMM.
- **Installation server** You can install VMM in System Center 2012 R2 on the same server where VMM in System Center 2012 SP1 is currently installed, or on a different server. However, if you install VMM on a different computer, or if you use a different service account, the encrypted data is not retained unless you configured distributed key management.

Note

Distributed key management stores the encryption keys in Active Directory Domain Services (AD DS). Later, when you move your VMM installation to another computer, the new computer has access to the encryption keys in AD DS.

The following topics provide information to help you with this upgrade:

- Planning an Upgrade of Virtual Machine Manager
- Performing a VMM Upgrade
- Performing Post-Upgrade Tasks in VMM
- Troubleshooting a VMM Upgrade

For information about performing a new VMM installation in System Center 2012 R2, see Deploying System Center 2012 - Virtual Machine Manager.

Known issues with this upgrade

The following issues have been identified when upgrading VMM to System Center 2012 R2:

Upgrading on a remote computer

Upgrading from VMM in System Center 2012 SP1 on one computer to VMM in System Center 2012 R2 on a different computer is not supported when data is retained from the original installation, and the following configurations apply:

- The original installation uses Windows DPAPI. This is the default setting if you did not configure distributed key management during setup.
- The VMM management server is configured to use any of the following encrypted values or settings:
  - Application settings (encrypted value)
  - Service setting (encrypted value)
  - SQL Server deployment (product key)
  - Web deploy package (encryption password)

Retaining the database

Data that is retained from VMM in System Center 2012 SP1 might not upgrade as expected, and an error message about the name and path of the shared library might be issued. To ensure that this does not occur, do one of the following on the Library configuration page of the Setup Wizard when you install System Center 2012 R2:

- Select the default shared library.
- Create a new library share.

WSMAN property values are not reset

The values of the MaxConcurrentOperationsPerUser and the MaxConnections properties of WSMAN (which are used by WinRM), are not reset during the upgrade. The values that existed prior to the upgrade persist after the upgrade, and they might be lower than the default values that are set by the operating system.

If you observe limited VMM throughput, it might be helpful to check these values and to reset them if needed.

Planning an Upgrade of Virtual Machine Manager

The following topic provides information to help you plan an upgrade of VMM from System Center 2012 SP1 to System Center 2012 R2:

- Planning Considerations for Upgrading VMM

Planning Considerations for Upgrading VMM

The following tables contain important considerations when you are planning to upgrade Virtual Machine Manager from System Center 2012 Service Pack 1 (SP1) to System Center 2012 R2.

Common planning considerations

Item	Planning considerations
VMware ESX hosts and certain versions of VMware vCenter Server	• If you include these hosts and their managed objects in the upgrade, they are removed from the VMM database. • If you do not want these hosts to be removed automatically, remove the hosts manually before upgrading.
Performance and Resource Optimization (PRO)	• PRO configurations are not maintained during this upgrade. • If you have an existing connection to Operations Manager, the connection is removed during the upgrade process. • If you do not want the connection to be removed automatically, manually remove the connection before upgrading. • After the upgrade process completes, you can reconfigure your connection to Operations Manager. • For information about using Operations Manager with VMM, see Configuring Operations Manager Integration with VMM.
WinRM optimization	The values of the MaxConcurrentOperationsPerUser and the MaxConnections properties of WSMAN (which are used by WinRM), are not reset during the upgrade. The values that existed prior to the upgrade persist after the upgrade, and if they are too low then the throughput of VMM might be limited.
Library server	• If you want to use the library server in VMM for System Center 2012 R2, click **Cancel** to exit the upgrade and then, if needed, move the library server to a computer that is running a supported operating system. • For information about VMM library server

Item	Planning considerations
	requirements, see **Preparing your environment for System Center 2012 R2 Virtual Machine Manager**.
Service account	For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.
Distributed key management	For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.

High availability planning considerations

Item	Planning considerations
Failover cluster	• You must create and configure a failover cluster prior to the upgrade.
Windows Azure Hyper-V Recovery Manager Provider	If Windows Azure Hyper-V Recovery Manager is implemented in the VMM environment, then after the upgrade you will need to assign the active node role to the same node that had that role before the upgrade. This ensures that the Hyper-V Recovery Manager registration information is properly restored.
VMM database	• We recommend that the VMM database reside on a high availability installation of SQL Server. We also recommend that the high availability installation of SQL Server is installed on a separate failover cluster from the failover cluster on which you are installing the high availability VMM management server. • For information about moving a VMM database to another computer, see How to Move a VMM Database to Another Computer.
Library server	• We recommend that the library server is installed on a high availability file server. • After you upgrade to a high availability VMM management server, we

Item	Planning considerations
	recommended that you relocate your VMM library to a high availability file server. • For more information about relocating your VMM library after the upgrade, see Relocating the VMM Library.
Service account	• You must configure the System Center Virtual Machine Manager service to use a domain account for a high availability VMM management server. • For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.
Distributed key management	• You must use distributed key management to store encryption keys in Active Directory Domain Services (AD DS) for a high availability VMM management server. • For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.

For additional guidance about configuring a high availability VMM management server, see **Installing a Highly Available VMM Management Server in VMM 2012**.

Tip
VMM provides automatic rollback functionality in the event of a failure during the upgrade process. When a failure is detected during the upgrade, the upgrade automatically reverts the environment to the original configuration.

Choosing Service Account and Distributed Key Management Settings During an Upgrade

This topic provides information to help you choose your service account and distributed key management settings during an upgrade of Virtual Machine Manager (VMM) from System Center 2012 Service Pack 1 (SP1) to System Center 2012 R2.

During the upgrade, on the **Configure service account and distributed key management** page, you need to specify which account to use for the System Center Virtual Machine Manager service, and whether to use distributed key management to store encryption keys in Active Directory Domain Services (AD DS). You need to choose your service account and distributed key management settings carefully. In some circumstances, depending on what you choose, encrypted data, such as passwords in templates and profiles, will not be available after the upgrade, and you will have to manually enter them. Information that is not retained about Virtual Machine Roles will not be available for you to enter after the upgrade.

For the service account, you can choose to use the Local System account or a domain account. In some cases, such as installing a high availability VMM management server, you must use a domain account. For more information, see Specifying a Service Account for VMM.

Distributed key management enables you to store encryption keys in AD DS instead of storing the encryption keys on the computer on which the VMM management server is installed. We recommend that you use distributed key management, and in some cases (such as installing a high availability VMM management server), you must use distributed key management. For more information, see Configuring Distributed Key Management in VMM.

Whether encrypted data is available after the upgrade depends on the following factors:

- The account you use to sign in when you perform the upgrade.
- The account that the Virtual Machine Manager service is using in the current installation of VMM.
- The account that the System Center Virtual Machine Manager service will use in the System Center 2012 R2 installation.

The following table provides information about accounts that are used during the upgrade.

Account used when upgrading	VMM service account in System Center 2012 SP1	VMM service account in System Center 2012 R2	Not using distributed key management	Using distributed key management
Any valid administrator account	Local system	Local system	Encrypted data is preserved	Encrypted data is preserved
Any valid administrator account	Local system	Domain account	Encrypted data is not preserved	Encrypted data is preserved
Any valid administrator account	Domain account	Local system	N/A	N/A
Same domain account as the VMM service account in System Center 2012 SP1	Domain account	Domain account	Encrypted data is preserved	Encrypted data is preserved
Different domain account from the VMM service account in System Center 2012 SP1	Domain account	Domain account	Encrypted data is not preserved	Encrypted data is not preserved

Note

If the Virtual Machine Manager service in System Center 2012 SP1 is configured to use a domain account, when you upgrade to a high availability management server in System Center 2012 R2, you must use the same domain account for the Virtual Machine Manager service. During the upgrade process, you will be required to enter the password for that domain account.

If your upgrade involves installing VMM on a different computer and using your current VMM database, encrypted data is not preserved during the upgrade unless you configured distributed key management. The benefit of using distributed key management is that the encryption keys are stored in AD DS instead of on the computer that was running VMM in System Center 2012 SP1. Therefore, if you reinstall VMM in System Center 2012 R2 on a different computer, you can access the encrypted data.

How to Move a VMM Database to Another Computer

You must move the Virtual Machine Manager (VMM) database before you upgrade to System Center 2012 R2 in the following cases:

- The VMM database is using a version of SQL Server that is not supported by System Center 2012 R2.
- The VMM database is installed on the same computer as the VMM management server, and you plan to upgrade to a high availability VMM management server.

Use the following procedures to locate information about the VMM database, such as the database name and instance name, and to move the VMM database.

To locate information about the VMM database

1. Open the **Settings** workspace.
2. In the **Settings** pane, expand **General**, and then double-click **Database Connection**.

To move a VMM database

1. Back up your existing VMM database by using tools that are available in SQL Server.
2. Copy the database backup to a computer that is running a supported version of SQL Server.
3. Use the tools in SQL Server to restore the database.

For more information about moving a SQL Server database, see Copying Databases with Backup and Restore.

Performing a VMM Upgrade

The following topics provide procedures to help you perform the upgrade:

- Tasks to Perform Before Beginning the VMM Upgrade
- How to Perform VMM Upgrade

- How to Upgrade a High Availability VMM Management Server
- How to Upgrade VMM on a Different Computer

Tasks to Perform Before Beginning the VMM Upgrade

Before you can install Virtual Machine Manager (VMM) in System Center 2012 R2, you need to uninstall the current version of VMM and prepare the environment by performing the following tasks:

1. Review **Prerequisites for Upgrading to VMM** and Planning Considerations for Upgrading VMM.
2. Complete all jobs that are currently running in VMM. You can use the console to view the jobs' status. All job history is deleted during the upgrade.
3. Close any connections to the VMM management server, including the VMM console and the VMM command shell.
4. Close any other programs that are running on the VMM management server.
5. Ensure that there are no pending restarts on the computers on which the VMM roles are installed. For example, if you have installed a server role by using Server Manager or have applied a security update, you may need to restart the computer. After you have restarted the computer, sign in to the computer with the same user account to finish the installation of the server role or the security update.
6. If Windows Azure Hyper-V Recovery Manager is implemented in the VMM environment, ensure that version 3.3.140.0 or later of Windows Azure Hyper-V Recovery Manager Provider is installed on the VMM management server. After the upgrade, you will need to re-install the Windows Azure Hyper-V Recovery Manager Provider, to ensure that it works properly.
7. Perform a full backup of the VMM database. For more information, see Back Up and Restore Virtual Machine Manager. You can also use tools that are provided by SQL Server to back up the VMM database. For more information, see Backing Up and Restoring Databases in SQL Server.
8. Uninstall the following:
    - Unless Update Rollup 4 for System Center 2012 SP1 has been applied – Uninstall Update Rollup 3 for System Center 2012 SP1, or any other Update Rollups that were applied that are earlier than Update Rollup 4.
    - All components of VMM in System Center 2012 SP1. On the **Uninstallation Options** page, click **Retain data**. For more information on how to uninstall the current VMM console, see How to Uninstall VMM.
    - Windows Automated Installation Kit (Windows AIK).
9. Ensure that the server meets all requirements for VMM in System Center 2012 R2 as described in System Requirements for System Center 2012 - Virtual Machine Manager.
    - If needed, upgrade SQL Server to a supported version. If the current version is supported in System Center 2012 R2, this upgrade is not required.
    - Install Windows 8.1 Assessment and Deployment Kit (Windows ADK).
10. You can now upgrade VMM.

How to Perform VMM Upgrade

Use the following procedure to upgrade a Virtual Machine Manager (VMM) management server to System Center 2012 R2. During this procedure, you retain the data from the System Center 2012 SP1 database.

Membership in the local Administrators group, or equivalent, on the computer that you are configuring is the minimum required to complete this procedure.

Caution

To avoid any loss of important data, before you upgrade VMM, we highly recommend that you perform a full backup of your VMM database.

To upgrade a VMM management server

1. On the current VMM management server in System Center 2012 SP1, start the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard by double-clicking **setup.exe** in your product media or on your network file share.
2. On the main setup page, click **Install**.
3. On the **Select features to install** page, select the **VMM management server** check box, and **Client** if you want to upgrade the client, and then click **Next**.

   Note

   If you are installing the VMM management server on a computer that is a member of a cluster, you will be asked whether you want the VMM management server to be a high availability server. For more information about installing a high availability VMM management server, see Installing a Highly Available VMM Management Server.
4. On the **Product registration information** page, provide the appropriate information, and then click **Next**. If you do not enter a product key, VMM will be installed as an evaluation version that expires in 180 days after installation.
5. On the **Please read this license agreement** page, review the license agreement, and if you agree with it, select the **I have read, understood, and agree with the terms of the license agreement** check box, and then click **Next**.
6. On the **Join the Customer Experience Improvement Program (CEIP)** page, select the option of your choice, and then click **Next**.
7. On the **Installation location** page, use the default path or type a different installation path for the VMM program files, and then click **Next**.

   The computer that you are upgrading is checked to ensure that the appropriate hardware and software requirements are met. If a prerequisite is not met, a page appears with information about which prerequisite has not been met and how to resolve the issue. If all prerequisites have been met, the **Database configuration** page appears.

   For information about hardware and software requirements for VMM, see System Requirements for System Center 2012 - Virtual Machine Manager.
8. On the **Database configuration** page, do the following:

- Specify the name of the computer that is running SQL Server. If you are installing the VMM management server on the same computer that is running SQL Server, in the **Server name** box, type the name of the computer (for example, **vmmserver01**), or type **localhost**.
- Specify the port to use for communication with the computer that is running SQL Server, if all of the following conditions are true:
  - SQL Server is running on a remote computer.
  - The SQL Server Browser service is not started on that remote computer.
  - SQL Server is not using default port 1433.

  Otherwise, leave the **Port** box empty.
- Select or type the name of the instance of SQL Server to use.
- Select **Existing Database**, and then select the database that you backed up from your System Center 2012 SP1 installation.
- Check **Use the following credentials**, provide the user name and password of an account that has the appropriate permissions to access the database, and then click **Next**.

9. When you are prompted whether to upgrade the database that you specified, click **Yes**.
10. On the **Configure service account and distributed key management** page, specify the account that will be used by the System Center Virtual Machine Manager service.

    Under **Distributed Key Management**, select whether to store encryption keys in Active Directory Domain Services, and then click **Next**.

    Caution
    Choose your service account and distributed key management settings carefully. Depending on what you choose, encrypted data, like passwords in templates and profiles, may not be available after the upgrade, and you will have to re-enter them manually. For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.
11. On the **Port configuration** page, provide unique port numbers for each feature as appropriate for your environment, and then click **Next**.
12. On the **Library configuration** page, chose whether to use an existing library share, or to create a new one, and then enter the library configuration information.
13. On the **Upgrade compatibility report**, review the information and do one of the following:
    - Click **Cancel** to exit the upgrade and resolve the noted issues.
    - Click **Next** to proceed with upgrade.
14. On the **Installation summary** page, review your selections and do one of the following:
    - Click **Previous** to change any selections.
    - Click **Install** to upgrade the VMM management server.

    After you click **Install**, the **Installing features** page appears and the upgrade progress is displayed.

15. On the **Setup completed successfully** page, click **Close** to finish the installation.

    To open the VMM console, ensure that the **Open the VMM console when this wizard closes** check box is selected. Alternatively, you can click the **Virtual Machine Manager Console** icon on the desktop.

How to Upgrade a High Availability VMM Management Server

If you are running Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1) on two or more nodes of a cluster that are configured with high availability, you can use the information in this topic to upgrade the VMM management servers in the cluster to high availability VMM management servers for System Center 2012 R2. You need to perform the following procedure on all the nodes that you want to upgrade.

Before you begin the upgrade process, review the High Availability Planning Considerations section in the topic Planning Considerations for Upgrading VMM.

Membership in the local Administrators group, or equivalent, on the computer that you are configuring is the minimum required to complete this procedure.

Caution

To avoid any loss of important data, before you upgrade VMM, we highly recommended that you perform a full backup of your VMM database.

To prepare for a high availability upgrade

1. Uninstall VMM in System Center 2012 SP1 from the nodes of the cluster that you want to upgrade, while choosing to retain the database.
2. Upgrading the Windows operating system is optional. Depending on whether you decide to upgrade the operating system, do the following:

   If you choose to not upgrade Windows, delete the high availability VMM resource group from the failover cluster.

   If you choose to upgrade Windows:

   a. During the upgrade, choose the upgrade option, not a fresh installation, to retain data.
   b. Note the name of your cluster, and then destroy the cluster.
   c. Upgrade the operating system on all the nodes in the cluster that you want to upgrade.
   d. Recreate the cluster by using its previous name.

   For detailed information about hardware and operating system requirements for VMM in System Center 2012 R2, see **System Requirements for System Center 2012 - Virtual Machine Manager**.
3. Use the next procedure on each node that you want to upgrade, to install VMM for System Center 2012 R2 by using the retained database.

To upgrade to high availability VMM management server

1. On the VMM management server, start the System Center 2012 Virtual Machine Manager Setup Wizard by double-clicking **setup.exe** in your product media or on your network file share.
2. On the main setup page, click **Install**.
3. On the **Select features to install** page, select the **VMM management server** check box, and **Client** if you want to upgrade the client, and then click **Next**.

   Note
   If you are installing the VMM management server on a computer that is a member of a cluster, you will be asked whether you want the VMM management server to be a high availability server. For more information about installing a high availability VMM management server, see Installing a Highly Available VMM Management Server.
4. On the **Product registration information** page, provide the appropriate information, and then click **Next**. If you do not enter a product key, VMM will be installed as an evaluation version that expires in 180 days after installation.
5. On the **Please read this license agreement** page, review the license agreement, and if you agree with it, select the **I have read, understood, and agree with the terms of the license agreement** check box, and then click **Next**.
6. On the **Join the Customer Experience Improvement Program (CEIP)** page, select the option of your choice, and then click **Next**.
7. On the **Installation location** page, use the default path or type a different installation path for the VMM program files, and then click **Next**.

   The computer that you are upgrading is checked to ensure that the appropriate hardware and software requirements are met. If a prerequisite is not met, a page appears with information about which prerequisite has not been met and how to resolve the issue. If all prerequisites have been met, the **Database configuration** page appears.

   For information about hardware and software requirements for VMM, see System Requirements for System Center 2012 - Virtual Machine Manager.
8. On the **Database configuration** page, do the following:
   - Specify the name of the computer that is running SQL Server. If you are installing the VMM management server on the same computer that is running SQL Server, in the **Server name** box, type the name of the computer (for example, **vmmserver01**), or type **localhost**.
   - Specify the port to use for communication with the computer that is running SQL Server, if all of the following conditions are true:
     - SQL Server is running on a remote computer.
     - The SQL Server Browser service is not started on that remote computer.
     - SQL Server is not using default port 1433.

     Otherwise, leave the **Port** box empty.

- Select or type the name of the instance of SQL Server to use.
- Select **Existing Database**, and then select the database that you backed up from your System Center 2012 SP1 installation.
- Check **Use the following credentials**, provide the user name and password of an account that has the appropriate permissions to access the database, and then click **Next**.

9. On the **Cluster configuration** page, do the following:
   - In the **Name** box, type a name for this high availability VMM management server implementation. For example, type **havmmcontoso**. Do not enter the name of the failover cluster or the name of the computer on which the high availability VMM management server is installed.

     You will use this clustered service name when you connect to this high availability VMM management server implementation by using the VMM console. Because there will be multiple nodes on the failover cluster that have the VMM management server feature installed, you need a single name to use when you connect to your VMM environment by using the VMM console.
   - If you are using static IPv4 addresses, you must specify the IP address to assign to the clustered service name. The clustered service name and its assigned IP address will be registered in DNS. If you are using IPv6 addresses or DHCP, no additional configuration is needed.

   After you have entered this information, click **Next**.
10. On the **Configure service account and distributed key management** page, specify the account that will be used by the System Center Virtual Machine Manager service. When you are installing a high availability VMM management server, choose a domain account.

    Under **Distributed Key Management**, select whether to store encryption keys in Active Directory Directory Services (AD DS). When you are installing a high availability VMM management server, choose the distributed key management option, and then click **Next**.

    Caution
    Choose your service account and distributed key management settings carefully. For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.
11. On the **Port configuration** page, provide unique port numbers for each feature as appropriate for your environment, and then click **Next**.
12. On the **Library configuration** page, click **Next** to continue.
13. On the **Upgrade compatibility report**, review the information and do one of the following:
    - Click **Cancel** to exit the upgrade and resolve the noted issues.
    - Click **Next** to proceed with the upgrade.
14. On the **Installation summary** page, review your selections and do one of the following:
    - Click **Previous** to change any selections.
    - Click **Install** to upgrade the VMM management server.

After you click **Install**, the **Installing features** page appears, and the upgrade progress is displayed.

15. On the **Setup completed successfully** page, click **Close** to finish the installation.

    To open the VMM console, ensure that the **Open the VMM console when this wizard closes** check box is selected. Alternatively, you can click the **Virtual Machine Manager Console** icon on the desktop.

For information, see:

- How to Connect to a Highly Available VMM Management Server by Using the VMM Console.
- How to Install a VMM Management Server on an Additional Node of a Cluster.

How to Upgrade VMM on a Different Computer

In some cases, you may not want to or may not be able to perform an upgrade on the management server on which VMM in System Center 2012 SP1 is currently installed. For example, you might need to move the VMM database to another computer before beginning the upgrade. In these cases, you can install VMM for System Center 2012 R2 on a different computer, and then use the database from the current VMM installation for the upgrade.

Use the following procedure to upgrade VMM to System Center 2012 R2 on a different computer.

Caution
To avoid any loss of important data, before you upgrade VMM, we highly recommend that you perform a full backup of your VMM database.

To upgrade VMM to System Center 2012 R2 on a different computer

1. Uninstall the current VMM deployment. On the **Uninstallation Options** page, select **Retain data**. For more information, see How to Uninstall VMM.
2. Install VMM for System Center 2012 R2 on another computer that meets all the requirements for System Center 2012 R2.
3. During the installation, do the following:
   - On the **Database configuration** page, specify the VMM database that you retained from the previous VMM installation. A message will appear that indicates the selected database was created by a previous version of VMM. To upgrade the VMM database, click **OK**.
   - On the **Configure service account and distributed key management** page, choose your service account and distributed key management settings carefully. Depending on what you choose, encrypted data, like passwords in templates and profiles, may not be available after the upgrade, and you will have to re-enter them manually. For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.

For more information, see Installing a VMM Management Server.

Performing Post-Upgrade Tasks in VMM

After you complete the Virtual Machine Manager (VMM) upgrade, you may need to make additional configuration changes to your VMM environment. For example, you may need to make the following changes:

Reassociate hosts and library servers

In some upgrade scenarios, you need to reassociate virtual machine hosts and VMM library servers with the VMM management server after the upgrade. For example, you need to reassociate hosts and library servers if you performed the upgrade on a server other than where VMM in System Center 2012 SP1 was installed.

For more information, see How to Reassociate a Host or Library Server.

Update VMM agents

After the upgrade, you need to update the VMM agents on your Hyper-V hosts and in your VMM library servers. You do not have to immediately update the VMM agents on Hyper-V hosts and library servers. The version of the VMM agent that comes with System Center 2012 SP1 is supported in System Center 2012 R2, but it does not provide all of the functionality of the VMM agent in System Center 2012 R2. To take advantage of the new functionality, update your VMM agents on your Hyper-V hosts and library servers.

For more information, see How to Update the VMM Agent.

Restore Windows Azure Hyper-V Recovery Manager

If Windows Azure Hyper-V Recovery Manager is implemented in the VMM environment, then you need to perform a few steps to restore the Windows Azure Hyper-V Recovery Manager Provider.

For more information, see How to Restore Windows Azure Hyper-V Recovery Manager Provider.

Update virtual machine templates

All virtual machine templates that were upgraded need to correctly specify the virtual hard disk that contains the operating system.

Tip

To update a virtual machine template, in the VMM console, open the Library workspace, expand **Templates**, and then click **VM Templates**. In the **Templates** pane, right-click the virtual machine template that you want to update, click **Properties**, and then go to the **Hardware Configuration** page.

Update driver packages

Driver packages that were previously added to the VMM library must be removed and added again to be correctly discovered.

For more information, see How to Add Driver Files to the VMM Library.

Relocate the VMM library

If you upgraded to a high availability VMM management server, we recommend that you relocate your VMM library to a high availability file server.

For more information, see Configuring the VMM Library.

After you create a new VMM library, you will want to move the resources from the previous VMM library to the new VMM library.

- To move file-based resources (such as ISO images, scripts, and VHDs), see How to Import and Export Physical Resources To and From the Library.
- To move virtual machine templates, see Exporting and Importing Service Templates in VMM.
- To preserve the custom fields and properties of saved virtual machines in the previous VMM library, deploy the saved virtual machines to a host and then save the virtual machines to the new VMM library.

Note

Operating system and hardware profiles cannot be moved. You need to re-create these profiles.

Install additional VMM consoles

You can install additional VMM consoles on stand-alone servers. To connect to a VMM management server that is running System Center 2012 R2, you must use the version of the VMM console that comes with System Center 2012 R2.

For more information , see Installing and Opening the VMM Console.

How to Reassociate a Host or Library Server

After you upgrade Virtual Machine Manager (VMM) to System Center 2012 R2, use the following procedure to reassociate a virtual machine host with the VMM management server.

To reassociate a host

1. In the VMM console, open the **Fabric** workspace, expand **Servers**, and then click **All Hosts**.
2. In the **Hosts** pane, ensure that the **Agent Status** column is displayed. If the **Agent Status** column is not displayed, right-click a column heading, and then click **Agent Status**.
3. Select the host that you need to reassociate with the VMM management server.

   Tip

You can use the SHIFT key or the CTRL key to select multiple hosts.

4. On the **Hosts** tab, in the **Host** group, click **Refresh**.

   If a host needs to be reassociated, the **Host Status** column for the host will display a value of **Needs Attention**, and the **Agent Status** column will display a value of **Access Denied**.

5. Right-click the host that you want to reassociate, and then click **Reassociate**.
6. In the **Reassociate Agent** dialog box, provide the necessary credentials, and then click **OK**.

   The **Agent Status** column will display a value of **Reassociating**. After the host has been reassociated successfully, the **Agent Status** column will display a value of **Responding**. And after you refresh the host again, the **Host Status** column for the host will display a value of **OK**.

   Tip
   You can see a **Reassociate agent** job in the **Jobs** workspace.

7. After you have reassociated the host, you will most likely have to update the VMM agent on the host. For more information, see How to Update the VMM Agent.

   Note
   You can reassociate a VMM library server in a similar manner. To view a list of VMM library servers, open the **Fabric** workspace, expand **Servers**, and then click **Library Servers**.

How to Update the VMM Agent

After you upgrade Virtual Machine Manager (VMM) to System Center 2012 R2, use the following procedure to update the VMM agent on a virtual machine host.

To update the VMM agent

1. In the VMM console, open the **Fabric** workspace, expand **Servers**, and then click **All Hosts**.
2. In the **Hosts** pane, right-click a column heading, and then click **Agent Version Status**. This adds the **Agent Version Status** column to the **Hosts** pane.
3. Select the host with the VMM agent that you want to update.

   Tip
   You can use the SHIFT key or the CTRL key to select multiple hosts.

4. On the **Hosts** tab, in the **Host** group, click **Refresh**.

   If a host needs to have its VMM agent updated, the **Host Status** column for the host will display a value of **Needs Attention**, and the **Agent Version Status** column will display a value of **Upgrade Available**.

5. Right-click the host with the VMM agent that you want to update, and then click **Update Agent**.
6. In the **Update Agent** dialog box, provide the necessary credentials, and then click **OK**.

   The **Agent Version Status** column will display a value of **Upgrading**. After the VMM agent is updated successfully on the host, the **Agent Version Status** column will display a value of **Up-to-date**, and the **Agent Version** column will display the updated version of the agent. After you refresh the host again, the **Host Status** column for the host will display a value of **OK**.

   Tip
   You will see **Refresh host** and **Update agent** jobs in the **Jobs** workspace.

   Note
   You can update the VMM agent on a VMM library server in a similar manner. To view a list of VMM library servers, open the **Fabric** workspace, expand **Servers**, and then click **Library Servers**.

How to Restore Windows Azure Hyper-V Recovery Manager Provider

If Windows Azure Hyper-V Recovery Manager is implemented in the VMM environment, then after the upgrade of VMM, you need to restore the Windows Azure Hyper-V Recovery Manager Provider on the VMM management server, as described below. It is recommended that you restore the provider immediately after completing the upgrade to prevent any data loss due to operations being performed before the provider is installed.

To restore the Windows Azure Hyper-V Recovery Manager Provider

1. Re-install the latest version of Windows Azure Hyper-V Recovery Manager Provider (version 3.3.140.0 or later), which you can download from the Microsoft Download Center. This restores the Provider registration information that was removed during the VMM upgrade.
2. In the Azure portal, in the jobs view, wait for the **Repair Provider** job to complete.

You can now continue to use the service from the Azure portal by re-initiating any operation that was running before the upgrade.

Troubleshooting a VMM Upgrade

For general information about troubleshooting Virtual Machine Manager (VMM), see the System Center 2012 – Virtual Machine Manager (VMM) General Troubleshooting Guide on the TechNet Wiki.

Log files

If there is a problem when you upgrade VMM to System Center 2012 R2, consult the log files that are located in the **%SYSTEMDRIVE%\ProgramData\VMMLogs** folder. Note that the **ProgramData** folder is a hidden folder and you might need to change viewing settings to view this folder.

Known issues

The following are known issues with a VMM upgrade to System Center 2012 R2:

- If multiple errors occur during upgrade, only the first error encountered is shown in the setup wizard. To see all errors that occurred, see the Log files.
- If any upgrade rollup that is earlier than Update Rollup (UR) 4 has been applied to VMM in System Center 2012 SP1, then an attempt to uninstall VMM (in order to upgrade to System Center 2012 R2) from the Windows Control Panel – might fail.

  In this case, you can try to uninstall VMM by running the Setup program directly from the products' installation media. Or, uninstall any Update Rollups that are earlier than UR4, and then try to uninstall VMM again.

Upgrading to VMM in System Center 2012 SP1

If you have an existing deployment of System Center 2012 – Virtual Machine Manager (VMM), you can upgrade to VMM in System Center 2012 Service Pack 1 (SP1). This upgrade is a fresh installation of System Center 2012 SP1. It uses the retained database from the System Center 2012 – Virtual Machine Manager deployment.

Warning

If you are planning to upgrade two or more System Center components, we strongly recommend that you first consult the guide Upgrade Sequencing for System Center 2012 SP1. The order in which you perform component upgrades is very important. Failure to follow the correct upgrade sequence might result in component failure for which no recovery options exist. The affected System Center components are:

1. Orchestrator
2. Service Manager
3. Data Protection Manager (DPM)
4. Operations Manager
5. Configuration Manager
6. Virtual Machine Manager
7. App Controller

Important

An upgrade from the Beta version of System Center 2012 SP1 to the RTM version of System Center 2012 SP1 is not supported.

Some data in the VMM database, such as Run As account credentials and passwords in guest operating system profiles, is encrypted using the Windows Data Protection application programming interface (DPAPI). To retain this encrypted data during an upgrade, the VMM management server must be installed on the same computer where VMM was previously installed. Also, you must use the same service account of the System Center Virtual Machine Manager service that you used in your previous installation of VMM.

You can perform the installation of VMM in System Center 2012 SP1 either on the same server where System Center 2012 – Virtual Machine Manager is currently installed or on a different server. However, if you install VMM on a different computer or use a different service account, this encrypted data will not be retained.

The following topics provide information to help you with this upgrade:

- Planning an Upgrade to VMM in System Center 2012 SP1
- Performing an Upgrade to VMM in System Center 2012 SP1
- Performing Post-Upgrade Tasks in VMM
- Troubleshooting a VMM Upgrade

For information about performing a new VMM installation in System Center 2012 SP1, see “VMM deployment” and other Virtual Machine Manager topics in the TechNet Library.

Planning an Upgrade to VMM in System Center 2012 SP1

The following topics provide information to help you plan an upgrade from System Center 2012 – Virtual Machine Manager (VMM) to VMM in System Center 2012 SP1:

- Prerequisites for Upgrading to VMM in System Center 2012 SP1
- Planning Considerations for Upgrading to VMM in System Center 2012 SP1

Prerequisites for Upgrading to VMM in System Center 2012 SP1

For detailed information about hardware and operating system requirements for VMM in System Center 2012 SP1, see System Requirements for System Center 2012 - Virtual Machine Manager.

Planning Considerations for Upgrading to VMM in System Center 2012 SP1

The following are some important considerations when you are planning an upgrade to Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1).

Common Planning Considerations

Item	Planning considerations
VMware ESX and certain versions of VMware vCenter Server	• If you upgrade with these hosts and their managed objects, they are removed from the VMM database. • If you do not want these hosts to be removed automatically, remove the hosts

Item	Planning considerations
	manually before upgrading. • For more information about which versions of VMware are supported, see **System Requirements: VMware ESX Hosts**.
Performance and Resource Optimization (PRO)	• PRO configurations are not maintained during this upgrade. • If you have an existing connection to Operations Manager, the connection is removed during the upgrade process. • If you do not want the connection to be removed automatically, remove the connection manually before upgrading. • After the upgrade process completes, you can reconfigure your connection to Operations Manager. • For information about using Operations Manager with VMM, see Configuring Operations Manager Integration with VMM.
Library server	• If you want to use the library server in VMM for System Center 2012 SP1, click **Cancel** to exit the upgrade, and then move the library server to a computer that is running a supported operating system. • For information about VMM library server requirements, see **System Requirements: VMM Library Server**.
Service account	For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.
Distributed key management	For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.

Highly Available Planning Considerations

The following are some important considerations when you are planning an upgrade to a highly available VMM management server.

Item	Planning considerations
Failover cluster	• You must create and configure a failover cluster before upgrading.
VMM database	• We recommend that the VMM database reside on a highly available installation of Microsoft SQL Server. We also recommend that the highly available installation of SQL Server be installed on a separate failover cluster from the failover cluster on which you are installing the highly available VMM management server. • For information about moving a VMM database to another computer, see **How to Move a VMM Database to Another Computer**.
Library server	• We recommend that the library server be installed on a highly available file server. • After you upgrade to a highly available VMM management server, we recommended that you relocate your VMM library to a highly available file server. • For more information about relocating your VMM library after the upgrade, see **Relocating the VMM Library**.
Service account	• You must configure the System Center Virtual Machine Manager service to use a domain account for a highly available VMM management server. • For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.
Distributed key management	• You must use distributed key management to store encryption keys in Active Directory Domain Services (AD DS) for a highly available VMM management server. • For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.

For additional guidance for configuring a highly available VMM management server, see Installing a Highly Available VMM Management Server.

Note

VMM provides automatic rollback functionality if a failure occurs during the upgrade process. When a failure is detected during the upgrade, the upgrade automatically reverts to the original configuration.

Choosing Service Account and Distributed Key Management Settings During an Upgrade

This topic provides information to help you choose your service account and distributed key managements settings during a System Center 2012 – Virtual Machine Manager (VMM) upgrade to System Center 2012 Service Pack 1 (SP1).

During the upgrade, on the **Configure service account and distributed key management** page, you need to specify which account to use for the System Center Virtual Machine Manager service and whether to use distributed key management to store encryption keys in Active Directory Domain Services (AD DS). Please choose your service account and distributed key management settings carefully. In some circumstances, depending on what you choose, encrypted data, such as passwords in templates and profiles, will not be available after the upgrade and you will have to re-enter them manually.

For the service account, you can choose to use either the Local System account or a domain account. In some cases, such as installing a highly available VMM management server, you must use a domain account. For more information, see Specifying a Service Account for VMM.

Distributed key management enables you to store encryption keys in AD DS instead of storing the encryption keys on the computer on which the VMM management server is installed. We recommend that you use distributed key management, and in some cases, such as installing a highly available VMM management server, you must use distributed key management. For more information, see Configuring Distributed Key Management in VMM.

Whether encrypted data is available after the upgrade depends on the following factors:

- The account that you are logged in as when you are performing the upgrade.
- The account that the System Center Virtual Machine Manager service is using in the current installation of VMM.
- The account that the System Center Virtual Machine Manager service will use in the System Center 2012 SP1 installation.

The following table provides information about accounts during an upgrade.

Account used when upgrading	System Center Virtual Machine Manager service account in System Center 2012	System Center Virtual Machine Manager service account in System Center 2012 SP1	Not using distributed key management	Using distributed key management
Any valid administrative account	Local System	Local System	Encrypted data is preserved	Encrypted data is preserved

Account used when upgrading	System Center Virtual Machine Manager service account in System Center 2012	System Center Virtual Machine Manager service account in System Center 2012 SP1	Not using distributed key management	Using distributed key management
Any valid administrative account	Local System	Domain account	Encrypted data is not preserved	Encrypted data is preserved
Any valid administrative account	Domain account	Local System	N/A	N/A
Same domain account as the System Center Virtual Machine Manager service account in System Center 2012	Domain account	Domain account	Encrypted data is preserved	Encrypted data is preserved
Different domain account from the System Center Virtual Machine Manager service account in System Center 2012 SP1	Domain account	Domain account	Encrypted data is not preserved	Encrypted data is not preserved

Note

If the System Center Virtual Machine Manager service in System Center 2012 is configured to use a domain account, when you upgrade to System Center 2012 SP1, you must use the same domain account for the System Center Virtual Machine Manager service. During the upgrade process, you will be required to enter the password for that domain account.

If you perform an upgrade where you are installing VMM on a different computer and using the VMM database from your current VMM installation, encrypted data is never preserved during the upgrade. This is because the encryption keys are stored on the computer that was running System Center 2012 – Virtual Machine Manager. This is a

benefit of using distributed key management in VMM in System Center 2012 SP1; the encryption keys are stored in AD DS instead of on the local computer. Therefore, if you have to reinstall VMM for System Center 2012 SP1 on a different computer, encrypted data can be preserved.

How to Move a VMM Database to Another Computer

You must move the Virtual Machine Manager (VMM) database before upgrading to System Center 2012 Service Pack 1 (SP1) in the following cases:

- The VMM database is using a version of Microsoft SQL Server that is not supported by System Center 2012 SP1. For information about supported Microsoft SQL Server versions, see **System Requirements: VMM Database**.
- The VMM database is installed on the same computer as the VMM management server and you plan to upgrade to a highly available VMM management server.

Use the following procedures to locate information about the VMM database such as the database name and instance name, and to move the VMM database if necessary.

To move a VMM database

1. Back up your existing VMM database using the tools that are available in Microsoft SQL Server.
2. Copy the database backup to a computer that is running a supported version of SQL Server.
3. Use the tools that are available in SQL Server to restore the database.

For more information about moving a SQL Server database, see Copying Databases with Backup and Restore.

Performing an Upgrade to VMM in System Center 2012 SP1

The following topics provide procedures to help you perform the upgrade to Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1):

- Tasks to Perform Before Beginning the Upgrade to VMM in System Center 2012 SP1
- How to Upgrade to VMM in System Center 2012 SP1
- How to Upgrade to a Highly Available VMM Management Server
- How to Upgrade to VMM on a Different Computer

Tasks to Perform Before Beginning the Upgrade to VMM in System Center 2012 SP1

Before you can install Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1), you need to uninstall the current VMM and to prepare the environment by performing the following tasks:

1. Review Prerequisites for Upgrading to VMM in System Center 2012 SP1 and Planning Considerations for Upgrading to VMM in System Center 2012 SP1.
2. Complete all jobs running in the current VMM installation; you can use the console to view jobs' status. All job history is deleted during the upgrade.
3. Close any connections to the VMM management server, including the VMM console and the VMM command shell.
4. Close any other open programs running on the VMM management server.
5. Ensure that there are no pending restarts on the computers on which the VMM roles are installed. For example, if you have installed a server role by using Server Manager or have applied a security update, you may need to restart the computer. After you have restarted the computer, log on to the computer with the same user account to finish the installation of the server role or the security update.
6. Perform a full backup of the VMM database. For information about backing up the VMM database, see Back Up and Restore Virtual Machine Manager. You can also use tools provided by Microsoft SQL Server to back up the VMM database. For more information, see Backing Up and Restoring Databases in SQL Server.
7. Uninstall the following:
    a. All components of System Center 2012 – Virtual Machine Manager. On the **Uninstallation Options** page, select **Retain data**. For more information about how to uninstall the current VMM console, see How to Uninstall VMM.
    b. Uninstall Windows Automated Installation Kit (Windows AIK).
8. Upgrade hardware, the operating system, and other software to meet the requirements of VMM in System Center 2012 SP1. Ensure that the server meets all requirements for VMM in System Center 2012 SP1, as described in System Requirements for System Center 2012 - Virtual Machine Manager.
    a. Upgrade windows to a supported version of Windows. For more information, see Download Windows Server 2012.
    b. Upgrade SQL Server to a supported version of SQL Server. If the current version is supported in System Center 2012 SP1, this upgrade is not required.
    c. Install Windows Assessment and Deployment Kit (Windows ADK).
9. Upgrade VMM.

How to Upgrade to VMM in System Center 2012 SP1

Use the following procedure to install Virtual Machine Manager (VMM) for System Center 2012 Service Pack 1 (SP1), while retaining and then connecting to the database from System Center 2012 – Virtual Machine Manager, if all VMM features are installed on the same server.

Membership in the local Administrators group, or equivalent, on the computer that you are configuring is the minimum required to complete this procedure.

 **Caution**

To avoid any loss of important data, before you upgrade VMM, we highly recommend that you perform a full backup of your VMM database.

To upgrade a VMM management server

1. On the VMM management server, on which System Center 2012 – Virtual Machine Manager is running, start the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard by double-clicking **setup.exe** on your product media or network share.
2. On the main setup page, click **Install**.
3. On the **Select features to install** page, select the **VMM management server** check box, and **Client** if you want to upgrade the client, and then click **Next**.

   Note
   If you are installing the VMM management server on a computer that is a member of a cluster, you will be asked whether you want to make the VMM management server highly available. For more information about installing a highly available VMM management server, see Installing a Highly Available VMM Management Server.
4. On the **Product registration information** page, provide the appropriate information, and then click **Next**. If you do not enter a product key, VMM will be installed as an evaluation version that expires in 180 days after installation.
5. On the **Please read this license agreement** page, review the license agreement, and if you agree with it select the **I have read, understood, and agree with the terms of the license agreement** check box, and then click **Next**.
6. On the **Join the Customer Experience Improvement Program (CEIP)** page, select either option, and then click **Next**.
7. On the **Microsoft Update** page, select whether or not you want to use Microsoft Update, and then click **Next**.

   Note
   If you have previously chosen to use Microsoft Update on this computer, the **Microsoft Update** page does not appear.
8. On the **Installation location** page, use the default path or type a different installation path for the VMM program files, and then click **Next**.

   The computer on which you are upgrading is checked to ensure that the appropriate hardware and software requirements are met. If a prerequisite is not met, a page appears with information about which prerequisite has not been met and how to resolve the issue. If all prerequisites have been met, the **Database configuration** page appears.

   For information about hardware and software requirements for VMM, see System Requirements for System Center 2012 - Virtual Machine Manager.
9. On the **Database configuration** page, do the following:
   - Specify the name of the computer that is running Microsoft SQL Server. If you are installing the VMM management server on the same computer that is running SQL

Server, in the **Server name** box, either type the name of the computer (for example, **vmmserver01**) or type **localhost**.

- Specify the port to use for communication with the computer that is running SQL Server, if all of the following conditions are true:
  - SQL Server is running on a remote computer.
  - The SQL Server Browser service is not started on that remote computer.
  - SQL Server is not using the default port of 1433.

  Otherwise, leave the **Port** box empty.
- Select or type the name of the instance of SQL Server to use.
- Select **Existing Database**, and enter the name of the database that you backed up from your System Center 2012 – Virtual Machine Manager installation.
- Check **Use the following credentials** and provide the user name and password of an account that has the appropriate permissions to access the database.

Click **Next**.

10. When you are prompted whether to upgrade the database that you specified, click **Yes**.
11. On the **Configure service account and distributed key management** page, specify the account that will be used by the System Center Virtual Machine Manager service.

    Under **Distributed Key Management**, select whether to store encryption keys in Active Directory Directory Services (AD DS).

    Click **Next** to continue.

    Caution
    Choose your service account and distributed key management settings carefully. In some circumstances, depending on what you choose, encrypted data, such as passwords in templates and profiles, will not be available after the upgrade and you will have to re-enter them manually. For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.
12. On the **Port configuration** page, provide unique port numbers for each feature as appropriate for your environment, and then click **Next**.
13. On the **Library configuration** page, choose whether to use an existing library share or to create a new one, and then enter the library configuration information.
14. On the **Upgrade compatibility report**, review the information and do one of the following:
    - Click **Cancel** to exit the upgrade and resolve the noted issues.
    - Click **Next** to proceed with the upgrade.
15. On the **Installation summary** page, review your selections and do one of the following:
    - Click **Previous** to change any selections.
    - Click **Install** to upgrade the VMM server.

    After you click **Install**, the **Installing features** page appears and upgrade progress is displayed.

16. On the **Setup completed successfully** page, click **Close** to finish the installation.

    To open the VMM console, ensure that the **Open the VMM console when this wizard closes** check box is selected. Alternatively, you can click the **Virtual Machine Manager Console** icon on the desktop.

How to Upgrade to a Highly Available VMM Management Server

If you are running System Center 2012 – Virtual Machine Manager on two or more nodes of a cluster, configured with high availability, you can use this information to perform an upgrade of the VMM management servers in the cluster to highly available VMM management servers for System Center 2012 Service Pack 1 (SP1). You need to perform the upgrade procedure below on all the nodes that you want to upgrade.

Before beginning the upgrade process, review “Highly Available Planning Considerations” in the Planning Considerations for Upgrading VMM topic.

Membership in the local Administrators group, or equivalent, on the computer that you are configuring is the minimum required to complete this procedure.

Caution
To avoid any loss of important data, before you upgrade VMM, we highly recommend that you perform a full backup on your VMM database.

To prepare for high availability upgrade

1. Uninstall System Center 2012 – Virtual Machine Manager from the nodes of the cluster that you want to upgrade, while choosing to retain the database.
2. Note the name of your cluster, and then destroy the cluster.
3. Upgrade the operating system to Windows Server 2012. See Download Windows Server 2012 (do not use a VHD for this upgrade). During the Windows upgrade, choose the upgrade option, not a fresh installation, to retain data.
4. After upgrading the operating system on all the nodes in the cluster that you want to upgrade, recreate the cluster.
5. Use the next procedure on each node that you want to upgrade to install VMM for System Center 2012 SP1 using the retained database.

To upgrade to a highly available VMM management server

1. On the VMM management server, on which System Center 2012 – Virtual Machine Manager is running, start the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard by double-clicking **setup.exe** on your product media or network share.
2. On the main setup page, click **Install**.
3. On the **Select features to install** page, select the **VMM management server** check box, and **Client** if you want to upgrade the client, and then click **Next**.

4. Setup detects that you are installing the VMM management server on a computer that is a member of a cluster. Click **Yes** in the dialog box to confirm that a cluster node is detected and that you want to install the management server and make it highly available.
5. On the **Product registration information** page, provide the appropriate information, and then click **Next**. If you do not enter a product key, VMM will be installed as an evaluation version that expires in 180 days after installation.
6. On the **Please read this license agreement** page, review the license agreement, and if you agree with the terms select the **I have read, understood, and agree with the terms of the license agreement** check box, and then click **Next**.
7. On the **Join the Customer Experience Improvement Program (CEIP)** page, select either option, and then click **Next**.
8. On the **Microsoft Update** page, select whether or not you want to use Microsoft Update, and then click **Next**.

   Note

   If you have previously chosen to use Microsoft Update on this computer, the **Microsoft Update** page does not appear.
9. On the **Installation location** page, use the default path or type a different installation path for the VMM program files, and then click **Next**.

   The computer on which you are upgrading is checked to ensure that the appropriate hardware and software requirements are met. If a prerequisite is not met, a page appears with information about which prerequisite has not been met and how to resolve the issue. If all prerequisites have been met, the **Database configuration** page appears.

   For information about hardware and software requirements for VMM, see System Requirements for System Center 2012 - Virtual Machine Manager.
10. On the **Database configuration** page, do the following:
    - Specify the name of the computer that is running SQL Server. If you are installing the VMM management server on the same computer that is running SQL Server, in the **Server name** box, either type the name of the computer (for example, **vmmserver01**) or type **localhost**.
    - Specify the port to use for communication with the computer that is running SQL Server, if all of the following conditions are true:
      - SQL Server is running on a remote computer.
      - The SQL Server Browser service is not started on that remote computer.
      - SQL Server is not using the default port of 1433.

      Otherwise, leave the **Port** box empty.
    - Select or type the name of the instance of SQL Server to use.
    - Select **Existing Database**, and enter the name of the database that you backed up from your System Center 2012 – Virtual Machine Manager installation.
    - Check **Use the following credentials** and provide the user name and password of an account that has the appropriate permissions to access the database.

Click **Next**.

11. When you are prompted whether to upgrade the database that you specified, click **Yes**.
12. On the **Configure service account and distributed key management** page, specify the account that will be used by the System Center Virtual Machine Manager service. When you are installing a highly available VMM management server, choose a domain account.

    Under **Distributed Key Management**, select whether to store encryption keys in Active Directory directory services (AD DS). When you are installing a highly available VMM management server, choose the distributed key management option.

    Click **Next** to continue.

    Important
    Choose your service account and distributed key management settings carefully. For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.
13. On the **Port configuration** page, provide unique port numbers for each feature as appropriate for your environment, and then click **Next**.
14. On the **Library configuration** page, choose whether to use an existing library share or to create a new one, and then enter the library configuration information.
15. On the **Upgrade compatibility report**, review the information and do one of the following:
    - Click **Cancel** to exit the upgrade and resolve the noted issues.
    - Click **Next** to proceed with the upgrade.
16. On the **Installation summary** page, review your selections and do one of the following:
    - Click **Previous** to change any selections.
    - Click **Install** to upgrade the VMM server.

    After you click **Install**, the **Installing features** page appears and upgrade progress is displayed.
17. On the **Setup completed successfully** page, click **Close** to finish the installation.

    To open the VMM console, ensure that the **Open the VMM console when this wizard closes** check box is selected. Alternatively, you can click the **Virtual Machine Manager Console** icon on the desktop.

For information about connecting to a highly available VMM management server by using the VMM console, see How to Connect to a Highly Available VMM Management Server by Using the VMM Console.

To install a VMM management server on an additional node of the cluster, see How to Install a VMM Management Server on an Additional Node of a Cluster.

How to Upgrade to VMM on a Different Computer

In some cases, you may not want to, or you may not be able to, perform an upgrade on the management server on which System Center 2012 – Virtual Machine Manager (VMM) is currently installed. For example, you might need to move the VMM database to another computer before beginning the upgrade. In these cases, you can install VMM for System Center 2012 Service Pack 1 (SP1) on a different computer and use the VMM database from the current VMM installation.

Upgrading from System Center 2012 – Virtual Machine Manager on one computer to VMM in System Center 2012 SP1 on a different computer is not supported when data is retained from the original installation, and the following configurations apply:

- The original installation uses Windows DPAPI. This is the default setting if you did not enable Distributed Key Management (DKM) during Setup.
- The VMM management server is configured to use any of the following encrypted values or settings:
  - Application settings (encrypted value)
  - Service setting (encrypted value)
  - SQL Server deployment (product key)
  - Web deploy package (encryption password)

Use the following procedure to upgrade VMM to System Center 2012 SP1 on a different computer.

Caution
To avoid any loss of important data, before you upgrade VMM, we highly recommend that you perform a full backup of your VMM database.

To upgrade VMM to System Center 2012 SP1 on a different computer

1. Uninstall System Center 2012 – Virtual Machine Manager, while making sure on the **Uninstallation Options** page to select **Retain data**.
2. Install VMM for System Center 2012 SP1 on the other computer:
   - During the installation, on the **Database configuration** page, specify the VMM database that you retained from the previous VMM installation. A message will appear indicating that the selected database was created by a previous version of VMM. To upgrade the VMM database, click **OK**.
   - On the **Configure service account and distributed key management** page, choose your service account and distributed key management settings carefully. In some circumstances, depending on what you choose, encrypted data, such as passwords in templates and profiles, will not be available after the upgrade, and you will have to re-enter them manually.

     For more information, see **Choosing Service Account and Distributed Key Management Settings During an Upgrade**.

For more information about installing a VMM management server, see Installing a VMM

Management Server.

Performing Post-Upgrade Tasks in VMM

After completing the Virtual Machine Manager (VMM) upgrade, you may need to make additional configuration changes to your VMM environment.

Reassociating Hosts and Library Servers

In some upgrade scenarios, you will need to reassociate virtual machine hosts and VMM library servers with the VMM management server after the upgrade. For example, you will need to reassociate hosts and library servers if you performed the upgrade on a server other than where System Center 2012 – Virtual Machine Manager was installed. To reassociate a host or library server, see **How to Reassociate a Host or Library Server**.

Updating VMM Agents

After upgrading, you will need to update the VMM agent on your Hyper-V hosts and VMM library servers. You do not have to immediately update the VMM agents on Hyper-V hosts and library servers. The older version of the VMM agent that comes with System Center 2012 – Virtual Machine Manager (VMM) is supported by System Center 2012 SP1, but it does not provide all of the functionality that the VMM agent that comes with System Center 2012 SP1 has. To take advantage of all the new functionality, update your VMM agents on your Hyper-V hosts and library servers. To update the VMM agent, see **How to Update the VMM Agent**.

Updating Virtual Machine Templates

Virtual machine template settings that specify which virtual hard drive contains the operating system are not preserved during the upgrade process. After upgrading, for all virtual machine templates that were upgraded, you will need to update the virtual machine template to specify which virtual hard disk contains the operating system.

Tip

To update a virtual machine template, in the VMM console, open the Library workspace, expand **Templates**, and then click **VM Templates**. In the **Templates** pane, right-click the virtual machine template that you want to update, click **Properties**, and then go to the **Hardware Configuration** page.

Updating Driver Packages

After upgrading, any driver packages that were previously added to the VMM library must be removed and added again to be correctly discovered. For more information about adding driver packages to the VMM library, see How to Add Driver Files to the VMM Library.

Relocating the VMM Library

After upgrading to a highly available VMM management server, we recommend that you relocate your VMM library to a highly available file server. For more information about VMM libraries, see **Configuring the Library Overview**.

After you have created a new VMM library, you will want to move the resources from the previous VMM library to the new VMM library. Here is the recommended method for moving various types of library resources:

- To move file-based resources, such as International Organization for Standardization (ISO) images, scripts, and virtual hard disks (VHDs), see How to Import and Export Physical Resources To and From the Library.
- To move virtual machine templates, see Exporting and Importing Service Templates in VMM.
- To preserve the custom fields and properties of saved virtual machines in the previous VMM library, deploy the saved virtual machines to a host and then save the virtual machines to the new VMM library.

Note

Operating system and hardware profiles cannot be moved. These profiles will need to be recreated.

Installing Additional VMM Consoles

After upgrading VMM, you can install additional VMM consoles on stand-alone servers. To connect to a VMM management server that is running System Center 2012 SP1, you must use the version of the VMM console that comes with System Center 2012 SP1.

For information about how to install the VMM console that comes with System Center 2012 SP1, see Installing and Opening the VMM Console.

How to Reassociate a Host or Library Server

After upgrading, use the following procedure to reassociate a virtual machine host with the Virtual Machine Manager (VMM) management server.

To reassociate a host after upgrading

1. In the VMM console, open the **Fabric** workspace, expand **Servers**, and then click **All Hosts**.
2. In the **Hosts** pane, ensure that the **Agent Status** column is displayed. If the **Agent Status** column is not displayed, right-click a column heading, and then click **Agent Status**. This adds the **Agent Status** column to the **Hosts** pane.
3. Select the host that you need to reassociate with the VMM management server.

   Tip

   You can use the SHIFT key or the CTRL key to select multiple hosts.
4. On the **Hosts** tab, in the **Host** group, click **Refresh**.

If a host needs to be reassociated, the **Host Status** column for the host will display a value of **Needs Attention** and the **Agent Status** column will display a value of **Access Denied**.

5. Right-click the host to reassociate, and then click **Reassociate**.
6. In the **Reassociate Agent** dialog box, provide the necessary credentials, and then click **OK**.

   The **Agent Status** column will display a value of **Reassociating**. After the host has been reassociated successfully, the **Agent Status** column will display a value of **Responding**. And after you refresh the host again, the **Host Status** column for the host will display a value of **OK**.

   Tip

   You will see a **Reassociate agent** job in the Jobs workspace.
7. After you have reassociated the host, you will most likely have to update the VMM agent on the host. To update the VMM agent, see **How to Update the VMM Agent**.

You can also reassociate a VMM library server in a similar manner. To view a list of VMM library servers, open the **Fabric** workspace, expand **Servers**, and then click **Library Servers**.

How to Update the VMM Agent

After upgrading Virtual Machine Manager (VMM), use the following procedure to update the VMM agent on a virtual machine host.

To update the VMM agent of a host

1. In the VMM console, open the **Fabric** workspace, expand **Servers**, and then click **All Hosts**.
2. In the **Hosts** pane, right-click a column heading, and then click **Agent Version Status**. This adds the **Agent Version Status** column to the **Hosts** pane.
3. Select the host whose VMM agent you want to update.

   Tip

   You can use the SHIFT key or the CTRL key to select multiple hosts.
4. On the **Hosts** tab, in the **Host** group, click **Refresh**.

   If a host needs to have its VMM agent updated, the **Host Status** column for the host will display a value of **Needs Attention** and the **Agent Version Status** column will display a value of **Upgrade Available**.
5. Right-click the host whose VMM agent you want to update, and then click **Update Agent**.
6. In the **Update Agent** dialog box, provide the necessary credentials, and then click **OK**.

   The **Agent Version Status** column will display a value of **Upgrading**. After the VMM agent has been updated successfully on the host, the **Agent Version Status** column will

display a value of **Up-to-date** and the **Agent Version** column will display the updated version of the agent. After you refresh the host again, the **Host Status** column for the host will display a value of **OK**.

Tip

You will see a **Refresh host** and an **Update agent** job in the Jobs workspace.

You can also update the VMM agent on a VMM library server in a similar manner. To view a list of VMM library servers, open the **Fabric** workspace, expand **Servers**, and then click **Library Servers**.

Troubleshooting a VMM Upgrade

For general information about troubleshooting Virtual Machine Manager (VMM), see the System Center 2012 – Virtual Machine Manager (VMM) General Troubleshooting Guide on the TechNet Wiki.

Log Files

If there is a problem during the upgrade, consult the log files that are located in the %SYSTEMDRIVE%\ProgramData\VMMLogs folder. Note that the ProgramData folder is a hidden folder.

Known Issues

The following are known issues with VMM upgrade:

- If multiple errors occur during the upgrade, only the first error is shown in the setup wizard. To review all the errors that occurred, see the log files.

Upgrading to System Center 2012 - Virtual Machine Manager

You can upgrade an existing VMM 2008 R2 SP1 environment to System Center 2012 – Virtual Machine Manager (VMM). The following topics provide information to help you perform the upgrade.

Note

Upgrading VMM 2008 R2 SP1 directly to VMM in System Center 2012 Service Pack 1 (SP1) is not supported.

- Planning an Upgrade to System Center 2012 - Virtual Machine Manager
- Performing an Upgrade to System Center 2012 - Virtual Machine Manager
- Performing Post-Upgrade Tasks in VMM
- Troubleshooting a VMM Upgrade

For information about performing a new installation of System Center 2012 – Virtual Machine Manager, see Deploying System Center 2012 - Virtual Machine Manager.

Planning an Upgrade to System Center 2012 - Virtual Machine Manager

The following topics provide information to help you plan your upgrade to System Center 2012 – Virtual Machine Manager (VMM).

- Prerequisites for Upgrading to VMM
- Planning Considerations for Upgrading to VMM

For an overview of VMM, see Overview of System Center 2012 - Virtual Machine Manager.

Prerequisites for Upgrading to VMM

This topic provides information about the software requirements for upgrading to System Center 2012 – Virtual Machine Manager (VMM). For detailed information about hardware and operating system requirements for System Center 2012 – Virtual Machine Manager, see **System Requirements: VMM for System Center 2012**.

Software	Supported version	Additional information
Virtual Machine Manager	VMM 2008 R2 SP1	• The following are not supported: Upgrading from System Center 2012 – Virtual Machine Manager Release Candidate, System Center 2012 – Virtual Machine Manager Beta, VMM 2008 R2, VMM 2008, or VMM 2007. • For information about upgrading to VMM 2008 R2 SP1, see Upgrading to VMM 2008 R2 Service Pack 1 from VMM 2008 R2.
Microsoft Windows Server	Windows Server 2008 R2	• The VMM management server is only supported on a computer that is running Windows Server 2008 R2. • For information about specific editions and service packs of Windows Server 2008 R2 that are supported, see **System Requirements: VMM**

Software	Supported version	Additional information
		Management Server. • If your VMM server for VMM 2008 R2 SP1 is installed on Windows Server 2008 SP2, you must upgrade the operating system before you can begin an in-place upgrade to System Center 2012 – Virtual Machine Manager. • For information about upgrading to Windows Server 2008 R2, see Guide for Upgrading to Windows Server 2008 R2.
Microsoft SQL Server	SQL Server 2008 R2 or SQL Server 2008	• For information about specific editions and service packs of SQL Server that are supported, see **System Requirements: VMM Database**. • System Center 2012 – Virtual Machine Manager does not support Express editions of SQL Server for the VMM database. • For information about moving a VMM database to a supported version of SQL Server, see How to Move a VMM Database to Another Computer.
SQL Server 2008 R2 Command Line Utilities	Microsoft SQL Server 2008 R2 Feature Pack	• The SQL Server 2008 R2 Command Line Utilities are not a mandatory requirement for upgrade, but they are highly recommended. • If the SQL Server 2008 R2 Command Line Utilities are not present on the VMM server, a warning is displayed in the prerequisites check during the upgrade process. You can proceed with the upgrade without installing these utilities, but these utilities are required

Software	Supported version	Additional information
		to perform certain management tasks. • To download the SQL Server 2008 R2 Command Line Utilities, see Microsoft SQL Server 2008 R2 Feature Pack.
Windows Automated Installation Kit (AIK)	Windows Automated Installation Kit (AIK) for Windows 7	• Previous versions of Windows AIK must be uninstalled before you can install Windows AIK for Windows 7. • To download Windows AIK for Windows 7, see The Windows Automated Installation Kit (AIK) for Windows 7.
Microsoft .NET Framework	.NET 3.5.1	• Microsoft .NET 3.5.1 is included in all versions of Windows Server 2008 R2. • System Center 2012 – Virtual Machine Manager automatically enables .NET 3.5.1 if it is not already enabled.
Windows Remote Management (WinRM)	WinRM 2.0	• WinRM 2.0 is included in Windows Server 2008 R2. By default, the Windows Remote Management (WS-Management) service is set to start automatically (delayed start). • If the Windows Remote Management (WS-Management) service is not started, an error is displayed during the prerequisites check. The service must be started before the upgrade can continue.

In addition to these software requirements, see Planning Considerations for Upgrading to VMM.

Planning Considerations for Upgrading to VMM

This topic presents some important issues for you to consider when you plan your upgrade to System Center 2012 – Virtual Machine Manager (VMM). In addition to these planning considerations, you should also review Prerequisites for Upgrading to VMM.

Common planning considerations

Item	Planning consideration
Microsoft Virtual Server 2005 R2	• Virtual machine hosts running Microsoft Virtual Server 2005 R2 are no longer supported in VMM. • If you upgrade a VMM environment that has Virtual Server hosts, the hosts are removed from the VMM database. • If you do not want these hosts to be removed automatically, you must remove the hosts manually before you upgrade.
VMware ESX and certain versions of VMware vCenter Server	• Virtual machine hosts running certain versions of VMware ESX and certain versions of VMware vCenter Server are no longer supported. • For more information about which versions of VMware are supported, see **System Requirements: VMware ESX Hosts**. • If you upgrade with these hosts and their managed objects, they are removed from the VMM database. • If you do not want these hosts to be removed automatically, you must remove the hosts manually before you upgrade.
Performance and Resource Optimization (PRO)	• Performance and Resource Optimization (PRO) configurations are not maintained during an upgrade to System Center 2012 – Virtual Machine Manager. • Any existing connection to Operations Manager is removed during the upgrade process. • If you do not want the Operations Manager connection to be automatically removed, you can remove the connection manually before the upgrade.

Item	Planning consideration
	• After the upgrade process completes, you can reconfigure your connection to Operations Manager. • For information about using Operations Manager with System Center 2012 – Virtual Machine Manager, see Configuring Operations Manager Integration with VMM.
Library server	• System Center 2012 – Virtual Machine Manager does not support a library server on a computer that is running Windows Server 2003. • If your library server is running Windows Server 2003 and you continue with the upgrade, you will not be able to use the library server in System Center 2012 – Virtual Machine Manager. You can only remove the library server from System Center 2012 – Virtual Machine Manager. • If you want to use the library server in System Center 2012 – Virtual Machine Manager, click **Cancel** to exit the upgrade and then move the library server to a computer that is running a supported operating system. • For information about VMM library server requirements, see **System Requirements: VMM Library Server**.
Service account	For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.
Distributed key management	For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.

Planning Considerations for highly available VMM

The following table includes several important items to consider when you plan an upgrade to a highly available VMM management server in System Center 2012 – Virtual Machine Manager.

Item	Planning consideration
Failover cluster	• You must create and configure a failover cluster prior to upgrading. • For information about installing and configuring a failover cluster, see Overview of Failover Clusters.
VMM database	• The VMM database cannot be installed on the same computer as the highly available VMM management server. • If your VMM database currently resides on the same server as the VMM server running VMM 2008 R2 SP1, you must move the VMM database to another computer. • We recommend that the VMM database resides on a highly available installation of SQL Server. We also recommend that the highly available installation of SQL Server is installed on a separate failover cluster from the failover cluster on which you are installing the highly available VMM management server. • For information about moving a VMM database to another computer, see How to Move a VMM Database to Another Computer.
Library server	• We recommend that the library server is installed on a highly available file server. • We recommend that after you upgrade to a highly available VMM management server, you should relocate your VMM library to a highly available file server. • For more information about relocating your VMM library after the upgrade, see Relocating the VMM Library.
VMM Self-Service Portal **Note** As of System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed.	• The VMM Self-Service Portal should not be installed on the same computer as the highly available VMM management server. • If your VMM Self-Service Portal currently resides on the same computer as the VMM server, we recommend that you uninstall the VMM Self-Service Portal for VMM 2008

Item	Planning consideration
	R2 SP1 before you upgrade to System Center 2012 – Virtual Machine Manager. • We recommend that you install the VMM Self-Service Portal on a highly available web server.
Service account	• You must configure the System Center Virtual Machine Manager service to use a domain account for a highly available VMM management server. • For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.
Distributed key management	• You must use distributed key management to store encryption keys in Active Directory Domain Services (AD DS) for a highly available VMM management server. • For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.

For additional guidance about configuring a highly available VMM management server, see Installing a Highly Available VMM Management Server.

Additional considerations

- System Center 2012 – Virtual Machine Manager provides an automatic rollback functionality for the event of a failure during the upgrade process. If a failure is detected during upgrade, the system automatically reverts to the pre-upgrade VMM 2008 R2 SP1 configuration.
- The names of the VMM services have changed in System Center 2012 – Virtual Machine Manager. If you have any scripts or tools that refer to these service names, you must update the service names as shown in the following table.

Version	Service display name	Service name
VMM 2008 R2 SP1	• Virtual Machine Manager • Virtual Machine Manager Agent	• vmmservice • vmmagent
System Center 2012 – Virtual Machine Manager	• System Center Virtual Machine Manager • System Center Virtual Machine Manager Agent	• scvmmservice • scvmmagent

Choosing Service Account and Distributed Key Management Settings During an Upgrade

This topic provides information to help you choose your service account and distributed key management settings during an upgrade to System Center 2012 – Virtual Machine Manager (VMM).

During an upgrade to System Center 2012 – Virtual Machine Manager, on the **Configure service account and distributed key management**, you must specify which account to use for the System Center Virtual Machine Manager service and specify whether to use distributed key management to store encryption keys in Active Directory Domain Services (AD DS). Be sure to choose your service account and distributed key management settings carefully. Certain setting selections can cause encrypted data, such as passwords in templates and profiles, to become unavailable after the upgrade so that you will have to re-enter this data manually.

For the service account, you can use either the Local System account or a domain account. In some cases, such as when you install a highly available VMM management server, you must use a domain account. For more information, see Specifying a Service Account for VMM.

Distributed key management enables you to store encryption keys in AD DS instead of storing the encryption keys on the computer on which the VMM management server is installed. The use of distributed key management is generally recommended, and may be specifically required in some cases, such as when you install a highly available VMM management server. For more information, see Configuring Distributed Key Management in VMM.

Note
Distributed key management is not available in VMM 2008 R2 SP1.

Whether encrypted data is available after the upgrade depends on the following factors:

- The account that are you are logged in as when performing the upgrade.
- The account that the Virtual Machine Manager service is using in your VMM 2008 R2 SP1 installation.
- The account that the System Center Virtual Machine Manager service will use in your installation of System Center 2012 – Virtual Machine Manager.

- The type of upgrade that you are performing. The two types of upgrades are:
  - On the computer that is running VMM 2008 R2 SP1, performing an in-place upgrade.
  - On a different computer, installing System Center 2012 – Virtual Machine Manager and using the VMM database from your VMM 2008 R2 SP1 installation.

The following table provides information for an in-place upgrade.

Account used when upgrading	VMM 2008 R2 SP1 service account	System Center 2012 – Virtual Machine Manager service account	Not using distributed key management	Using distributed key management
Any valid administrative account	Local System	Local System	Encrypted data is preserved	Encrypted data is preserved
Any valid administrative account	Local System	Domain account	Encrypted data is not preserved	Encrypted data is preserved
Any valid administrative account	Domain account	Local System	*(This configuration is not supported.)*	*(This configuration is not supported.)*
Same domain account as the VMM 2008 R2 SP1 service account	Domain account	Domain account	Encrypted data is preserved	Encrypted data is preserved
Different domain account from the VMM 2008 R2 SP1 service account	Domain account	Domain account	Encrypted data is not preserved	Encrypted data is not preserved

Note

If the Virtual Machine Manager service in VMM 2008 R2 SP1 is configured to use a domain account, when you upgrade to System Center 2012 – Virtual Machine Manager, you must use the same domain account for the System Center Virtual Machine Manager service. During the upgrade process, you will be required to enter the password for that domain account.

Encrypted data is not preserved during an upgrade in which you install System Center 2012 – Virtual Machine Manager on a different computer and use the VMM database from your VMM 2008 R2 SP1 installation. This is because the encryption keys are stored on the computer that

was running VMM 2008 R2 SP1. This failure to preserve encrypted data can be avoided by using distributed key management in System Center 2012 – Virtual Machine Manager; the encryption keys are stored in AD DS instead of on the local computer. Because of this, if you have to reinstall System Center 2012 – Virtual Machine Manager on a different computer, encrypted data can be preserved.

How to Move a VMM Database to Another Computer

In the following cases, you must move the VMM database before you upgrade to System Center 2012 – Virtual Machine Manager:

- The VMM database uses a version of Microsoft SQL Server that is not supported by System Center 2012 – Virtual Machine Manager.
- The VMM database is installed on the same computer as the VMM server and you plan to upgrade to a highly available VMM management server.

Note

If you must move the VMM database, you cannot perform an in-place upgrade of your VMM 2008 R2 SP1 environment. For more information about how to upgrade to System Center 2012 – Virtual Machine Manager in these situations, see How to Upgrade to VMM on a Different Computer.

Use the following procedures to locate information about the VMM database such as the database name and instance name, and to move the VMM database if necessary.

To move a VMM database

1. Back up your existing VMM database using tools that are available in SQL Server.
2. Copy the database backup files to a computer that is running a supported version of SQL Server.
3. Restore the database by using tools that are available in SQL Server.

For more information about moving a SQL Server database, see Copying Databases with Backup and Restore.

To locate information about the VMM database

1. Open the **Settings** workspace.
2. In the **Settings** pane, expand **General**.
3. In the **Settings** pane, double-click **Database Connection**.

For more information about moving a SQL Server database, see Copying Databases with Backup and Restore.

Performing an Upgrade to System Center 2012 - Virtual Machine Manager

The following topics provide procedures to help you upgrade to System Center 2012 – Virtual Machine Manager from VMM 2008 R2 SP1.

- Tasks to Perform Before Beginning the Upgrade to VMM
- How to Upgrade to System Center 2012 - Virtual Machine Manager from VMM 2008 R2 SP1
- How to Upgrade to a Highly Available VMM Management Server
- How to Upgrade a VMM Console
- How to Upgrade the VMM Self-Service Portal
- How to Upgrade to VMM on a Different Computer

Important

Before beginning the upgrade process, review the information in Planning an Upgrade to System Center 2012 - Virtual Machine Manager.

Tasks to Perform Before Beginning the Upgrade to VMM

Before beginning the upgrade process to System Center 2012 – Virtual Machine Manager, perform the following tasks:

- Review Prerequisites for Upgrading to VMM and Planning Considerations for Upgrading to VMM.
- Complete all jobs running in VMM. All job history is deleted during the upgrade. For information about viewing jobs, see Monitoring Jobs in VMM.
- Close any connections to the VMM server, including the VMM console and the VMM command shell, and connections made through the VMM Self-Service Portal.

  Note

  As of System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed.
- Close any other open programs running on the VMM server.
- Ensure that there are no pending restarts on the computers on which the VMM roles are installed. For example, if you have installed a server role by using Server Manager or have applied a security update, you may need to restart the computer. After you have restarted the computer, log on to the computer with the same user account to finish the installation of the server role or the security update.
- Perform a full backup of the VMM database
  - For information about backing up the VMM database, see Backing Up and Restoring the VMM Database.
  - You can also use tools provided by SQL Server to back up the VMM database. For more information, see Backing Up and Restoring Databases in SQL Server.

How to Upgrade to System Center 2012 - Virtual Machine Manager from VMM 2008 R2 SP1

Use the following procedure to perform an in-place upgrade of your existing VMM 2008 R2 SP1 installation if all VMM features are installed on the same machine.

Membership in the local Administrators group, or equivalent, on the computer that you are configuring is the minimum required to complete this procedure.

Caution

To avoid any loss of important data, before you upgrade VMM, we highly recommended that you perform a full backup on your VMM database.

To upgrade a VMM server

1. On the VMM server running VMM 2008 R2 SP1, start the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard.

   To start the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard, on your product media or network share, double-click **setup.exe**.

   Note

   Before beginning the upgrade of VMM, close any open programs and ensure that there are no pending restarts on the computer. For example, if you have installed a server role by using Server Manager or have applied a security update, you may need to restart the computer and then log on to the computer with the same user account to finish the installation of the server role or the security update.
2. On the main setup page, click **Install**.
3. On the setup dialog box, click **Yes** to confirm that you want to upgrade your existing VMM installation to System Center 2012 – Virtual Machine Manager.
4. On the **Features to be upgraded** page, click **Next**.

   Note

   All items will be selected. You cannot clear the **VMM Administrator Console** or the **VMM Self-Service Portal** check boxes.
5. On the **Product registration information** page, provide the appropriate information, and then click **Next**.
6. On the **Please read this license agreement** page, review the license agreement, select the **I have read, understood, and agree with the terms of the license agreement** check box, and then click **Next**.
7. On the **Join the Customer Experience Improvement Program (CEIP)** page, select either option and then click **Next**.
8. On the **Microsoft Update** page, select whether or not you want to use Microsoft Update, and then click **Next**.

   Note

   If you have previously chosen to use Microsoft Update on this computer, the

Microsoft Update page does not appear.

9. On the **Installation location** page, use the default path or type a different installation path for the VMM program files, and then click **Next**.

   Warning
   You cannot use the file location of the previous installation of VMM.

   The computer on which you are upgrading is checked to ensure that the appropriate hardware and software requirements are met. If a prerequisite is not met, a page appears with information about which prerequisite has not been met and how to resolve the issue. If all prerequisites have been met, the **Database configuration** page appears.

   For information about hardware and software requirements for VMM, see **System Requirements: VMM for System Center 2012**.

10. On the **Database configuration** page, verify the information for your existing installation of VMM server is correct, and click **Next**.

    Important
    If the account that you are logged in as to perform the upgrade does not have access to the SQL Server on which the VMM database for VMM 2008 R2 SP1 is located, then you must select **Use the following credentials** and provide credentials that do have access to that SQL Server.

11. On the **Configure service account and distributed key management** page, specify the account that will be used by the System Center Virtual Machine Manager service.

    Under **Distributed Key Management**, select whether to store encryption keys in Active Directory.

    Caution
    Choose your service account and distributed key management settings carefully. In some circumstances, depending on what you choose, encrypted data, like passwords in templates and profiles, will not be available after the upgrade and you will have to re-enter them manually. For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.

    After you have made your selections on the **Configure service account and distributed key management** page, click **Next** to continue.

12. On the **Port configuration** page, provide unique port numbers for each feature as appropriate for your environment, and then click **Next**.

    Note
    The ports that are currently assigned are grayed out. These port values cannot be changed without uninstalling and reinstalling VMM.

13. On the **Self-Service portal configuration** page, click **Next**.

    This page is only displayed if the VMM Self-Service Portal is installed on your VMM server.

14. On the **Upgrade compatibility report**, review the information and do one of the

following:

- Click **Cancel** to exit upgrade and resolve the noted issues.
- Click **Next** to proceed with upgrade.

15. On the **Installation summary** page, review your selections and do one of the following:
    - Click **Previous** to change any selections.
    - Click **Install** to upgrade the VMM server.

    After you click **Install**, the **Installing features** page appears and upgrade progress is displayed.
16. On the **Setup completed successfully** page, click **Close** to finish the installation.

    To open the VMM console, ensure that the **Open the VMM console when this wizard closes** check box is selected.

How to Upgrade to a Highly Available VMM Management Server

If you are running VMM 2008 R2 SP1 on a node of a cluster, you can use this procedure to perform an in-place upgrade of the VMM server to a highly available VMM management server that is running System Center 2012 – Virtual Machine Manager.

Before beginning the upgrade process, review Highly Available Planning Considerations.

Membership in the local Administrators group, or equivalent, on the computer that you are configuring is the minimum required to complete this procedure.

Caution
To avoid any loss of important data, before you upgrade VMM, we highly recommended that you perform a full backup on your VMM database.

To upgrade to a highly available VMM management server

1. On the node of your cluster that is running the VMM server, start the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard.

   To start the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard, on your installation media, double-click **setup.exe**.

   Note
   Before beginning the upgrade of VMM, close any open programs and ensure that there are no pending restarts on the computer. For example, if you have installed a server role by using Server Manager or have applied a security update, you may need to restart the computer and then log on to the computer with the same user account to finish the installation of the server role or the security update.
2. On the main setup page, click **Install**.
3. On the setup dialog box, click **Yes** to confirm that you want to upgrade your existing VMM installation to System Center 2012 – Virtual Machine Manager.

4. Click **Yes** on the dialog to confirm that a cluster node is detected and that you want to upgrade VMM on the server and make it highly available.
5. On the **Features to be upgraded** page, click **Next**.

   Note
   All items will be selected and you cannot clear any of the selections.
6. On the **Product registration information** page, provide the appropriate information, and then click **Next**.
7. On the **Please read this license agreement** page, review the license agreement, select the **I have read, understood, and agree with the terms of the license agreement** check box, and then click **Next**.
8. On the **Join the Customer Experience Improvement Program (CEIP)** page, select either option and then click **Next**.
9. On the **Microsoft Update** page, select whether or not you want to use Microsoft Update, and then click **Next**.

   Note
   If you have previously chosen to use Microsoft Update on this computer, the **Microsoft Update** page does not appear.
10. On the **Installation location** page, use the default path or type a different installation path for the VMM program files, and then click **Next**.

    Note
    You cannot use the file location of the previous installation of VMM server.

    The computer on which you are upgrading to a highly available VMM management server is checked to ensure that the appropriate hardware and software requirements are met. If a prerequisite is not met, a page appears with information about which prerequisite has not been met and how to resolve the issue. If all prerequisites have been met, the **Database configuration** page appears.

    For information about hardware and software requirements for VMM, see **System Requirements: VMM for System Center 2012**.
11. On the **Database configuration** page, verify the information for your existing installation of VMM management server is correct, and click **Next**.

    Important
    If the account that you are logged in as to perform the upgrade does not have access to the SQL Server on which the VMM database for VMM 2008 R2 SP1 is located, then you must select **Use the following credentials** and provide credentials that do have access to that SQL Server.
12. On the **Cluster configuration** page, In the **Name** box, type the name you want to give to this highly available VMM management server implementation. For example, type **havmmcontoso**.

    Warning

Do not enter the name of the failover cluster or the name of the computer on which the VMM server is installed.

You use this clustered service name to connect to this highly available VMM management server using the VMM console. Because there are multiple nodes on the failover cluster that have the VMM management server feature installed, you need a single name to use when you connect to your VMM environment by using the VMM console.

13. If you are using static IPv4 addresses, you must specify the IP address to assign to the clustered service name. The clustered service name and its assigned IP address are registered in DNS. If you are using IPv6 addresses or you are using DHCP, no additional configuration is needed.

    After you have configured the cluster settings, click **Next**.

14. On the **Configure service account and distributed key management** page, type the domain account and password that will be used by the System Center Virtual Machine Manager service. You must use a domain account for a highly available VMM management server.

    Caution
    Choose your service account carefully. In some circumstances, depending on what you choose, encrypted data, like passwords in templates and profiles, will not be available after the upgrade and you will have to re-enter them manually. For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.

    Under **Distributed Key Management**, specify the location in Active Directory to store encryption keys. For example, type **CN=VMMDKM,DC=contoso,DC=com**.

    You must use distributed key management to store the encryption keys in Active Directory for a highly available VMM management server. For more information about distributed key management, see Configuring Distributed Key Management in VMM.

    After you have specified the necessary information on the **Configure service account and distributed key management** page, click **Next**.

15. On the **Port configuration** page, provide unique port numbers for each feature and that are appropriate for your environment, and then click **Next**.

    Important
    The ports that are currently assigned are unavailable. These port values cannot be changed without uninstalling and reinstalling VMM.

16. On the **Self-Service portal configuration** page, click **Next**.

    This page is only displayed if the VMM Self-Service Portal is installed on your VMM server. We do not recommend that the VMM Self-Service Portal be installed on the same computer as the highly available VMM management server.

17. On the **Upgrade compatibility report**, review the information and do one of the following:

- Click **Cancel** to exit upgrade and resolve the noted issues.
- Click **Next** to proceed with upgrade.

18. On the **Installation summary** page, review your selections and do one of the following:
    - Click **Previous** to change any selections.
    - Click **Install** to upgrade the highly available VMM management server.

    After you click **Install**, the **Installing features** page appears and upgrade progress is displayed.
19. On the **Setup completed successfully** page, click **Close** to finish the installation.

    To open the VMM console, ensure that the **Open the VMM console when this wizard closes** check box is selected.

For information about connecting to a highly available VMM management server by using the VMM console, see How to Connect to a Highly Available VMM Management Server by Using the VMM Console.

To install a VMM management server on an additional node of the cluster, see How to Install a VMM Management Server on an Additional Node of a Cluster.

How to Upgrade a VMM Console

To connect to a VMM management server that is running System Center 2012 – Virtual Machine Manager, you must use the version of the VMM console that comes with System Center 2012 – Virtual Machine Manager.

Note
The VMM Administrator Console in VMM 2008 R2 SP1 is now referred to as the VMM console in System Center 2012 – Virtual Machine Manager.

Use the following procedure to upgrade to the VMM console that comes with System Center 2012 – Virtual Machine Manager.

Membership in the local Administrators group, or equivalent, on the computer that you are configuring is the minimum required to complete this procedure.

Important
Before upgrading to the VMM console, close the VMM Administrator Console and the Windows PowerShell – Virtual Machine Manager command shell.

To upgrade to a VMM console

- To upgrade to the VMM console that comes with System Center 2012 – Virtual Machine Manager, you can do either of the following:
    - Do an in-place upgrade by running the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard on the computer on which the VMM Administrator Console for VMM 2008 R2 SP1 is installed.

- Uninstall the VMM Administrator Console for VMM 2008 R2 SP1, and then install the VMM console that comes with System Center 2012 – Virtual Machine Manager by running the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard.

Note
To start the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard, on your product media or network share, double-click **setup.exe**.

For more information on how to uninstall the VMM Administrator Console in VMM 2008 R2 SP1, see Uninstalling VMM Components.

For more information on how to install the VMM console that comes with System Center 2012 – Virtual Machine Manager, see Installing and Opening the VMM Console.

How to Upgrade the VMM Self-Service Portal

Note
In System Center 2012 Service Pack 1 (SP1), the Virtual Machine Manager (VMM) Self-Service Portal has been removed.

To provide users self-service access to System Center 2012 – Virtual Machine Manager by using a web browser, you must use the version of the VMM Self-Service Portal that comes with System Center 2012 – Virtual Machine Manager.

Use the following procedure to upgrade to the VMM Self-Service Portal that comes with System Center 2012 – Virtual Machine Manager.

Membership in the local Administrators group, or equivalent, on the computer that you are configuring is the minimum required to complete this procedure.

How to upgrade the VMM Self-Service Portal

- To upgrade a VMM Self-Service Portal that is running VMM 2008 R2 SP1, you can do either of the following:
  - Do an in-place upgrade by running the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard on the computer on which the VMM Self-Service Portal for VMM 2008 R2 SP1 is installed.
  - Uninstall the VMM Self-Service Portal for VMM 2008 R2 SP1, and then install the VMM Self-Service Portal that comes with System Center 2012 – Virtual Machine Manager by running the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard.

Note
To start the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard, on your product media or network share, double-click **setup.exe**.

For more information on how to uninstall the VMM Self-Service Portal in VMM 2008 R2

SP1, see Uninstalling VMM Components.

For more information on how to install the VMM Self-Service Portal that comes with System Center 2012 – Virtual Machine Manager, see Installing and Opening the VMM Self-Service Portal.

How to Upgrade to VMM on a Different Computer

In some cases, you may not want to or you may not be able to do an in-place upgrade to System Center 2012 – Virtual Machine Manager. For example, you cannot perform an in-place upgrade if you have to move the VMM database to another computer before beginning the upgrade. In these cases, you can install System Center 2012 – Virtual Machine Manager on a different computer and use the VMM database from your VMM 2008 R2 SP1 installation.

Use the following procedure to upgrade to System Center 2012 – Virtual Machine Manager on a different computer.

To upgrade to System Center 2012 – Virtual Machine Manager on a different computer

1. Uninstall VMM 2008 R2 SP1, making sure on the **Uninstallation Options** page to select **Retain data**.
2. After uninstalling VMM 2008 R2 SP1, install System Center 2012 – Virtual Machine Manager on the other computer.
   - During the installation of System Center 2012 – Virtual Machine Manager, on the **Database configuration** page, specify the VMM database that you retained from the VMM 2008 R2 SP1 installation. A message will appear indicating that the selected database was created by a previous version of VMM. To upgrade the VMM database to System Center 2012 – Virtual Machine Manager, click **OK**.
   - On the **Configure service account and distributed key management** page, choose your service account and distributed key management settings carefully. In some circumstances, depending on what you choose, encrypted data, like passwords in templates and profiles, will not be available after the upgrade and you will have to re-enter them manually. For more information, see Choosing Service Account and Distributed Key Management Settings During an Upgrade.

For more information about installing a VMM management server, see Installing a VMM Management Server.

Performing Post-Upgrade Tasks in VMM

After you have upgraded to System Center 2012 – Virtual Machine Manager, you may need to make additional configuration changes to your VMM environment.

Reassociating Hosts and Library Servers

In some upgrade scenarios, you will need to reassociate virtual machine hosts and VMM library servers with the VMM management server after upgrading to System Center 2012 – Virtual Machine Manager. For example, you will need to reassociate hosts and library servers if you did not perform an in-place upgrade to System Center 2012 – Virtual Machine Manager from VMM 2008 R2 SP1. To reassociate a host or library server, see How to Reassociate a Host or Library Server.

Updating VMM Agents

After upgrading to System Center 2012 – Virtual Machine Manager, you will need to update the VMM agent on your Hyper-V hosts and VMM library servers.

You do not have to immediately update the VMM agents on Hyper-V hosts and library servers. Older versions of the VMM agent are supported by System Center 2012 – Virtual Machine Manager, but the older versions of the VMM agent do not provide all of the functionality that the VMM agent that comes with System Center 2012 – Virtual Machine Manager does. To take advantage of all the functionality of System Center 2012 – Virtual Machine Manager, update your VMM agents on your Hyper-V hosts and library servers. To update the VMM agent, see How to Update the VMM Agent.

The following older versions of the VMM agent are supported by System Center 2012 – Virtual Machine Manager:

- VMM 2008 R2 (2.0.4271.0)
- VMM 2008 R2 QFE3 (2.0.4273.0)
- VMM 2008 R2 QFE4 (2.0.4275.0)
- VMM 2008 R2 SP1 (2.0.4521.0)

Updating Virtual Machine Templates

Virtual machine template settings that specify which virtual hard drive (VHD) file contains the operating system are not preserved during the upgrade process. After upgrading to System Center 2012 – Virtual Machine Manager, for all virtual machine templates that were upgraded from VMM 2008 R2 SP1, you will need to update the virtual machine template to specify which VHD file contains the operating system.

Tip

To update a virtual machine template, in the VMM console, open the Library workspace, expand **Templates**, and then click **VM Templates**. In the **Templates** pane, right-click the virtual machine template that you want to update, click **Properties**, and then go to the **Hardware Configuration** page.

If you had a virtual machine template in VMM 2008 R2 SP1 that used a hardware profile that specified a VLAN ID, the VLAN ID is removed during the upgrade to System Center 2012 – Virtual Machine Manager. In System Center 2012 – Virtual Machine Manager, when you deploy a virtual machine from a template, the VLAN ID is automatically determined based on the logical

network specified. Ensure that your logical networks in System Center 2012 – Virtual Machine Manager are configured to use the correct VLAN IDs and that you have specified the correct logical network in your hardware profile. For more information about logical networks in System Center 2012 – Virtual Machine Manager, see Configuring Networking in VMM.

Updating Driver Packages

After upgrading to System Center 2012 – Virtual Machine Manager, any driver packages that were added to the VMM library in VMM 2008 R2 SP1 must be removed and added again to be correctly discovered. For information about adding driver packages to the VMM library, see How to Add Driver Files to the VMM Library.

Relocating the VMM Library

After upgrading to a highly available VMM management server, we recommended that you relocate your VMM library to a highly available file server. For more information about VMM libraries in System Center 2012 – Virtual Machine Manager, see Configuring the VMM Library.

After you have created a new VMM library, you will want to move the resources from the previous VMM library to the new VMM library. Here is the recommended method for moving various types of library resources:

- To move file-based resources, such as ISO images, scripts, and VHDs, see How to Import and Export Physical Resources To and From the Library.
- To move virtual machine templates, see Exporting and Importing Service Templates in VMM.
- To preserve the custom fields and properties of saved virtual machines in the previous VMM library, deploy the saved virtual machines to a host and then save the virtual machines to the new VMM library.

Note

Operating system and hardware profiles cannot be moved. These profiles will need to be recreated.

How to Reassociate a Host or Library Server

Use the following procedure to reassociate a virtual machine host with the VMM management server after upgrading to System Center 2012 – Virtual Machine Manager.

To reassociate a host after upgrading

1. In the VMM console, open the **Fabric** workspace, expand **Servers**, and then click **All Hosts**.
2. In the **Hosts** pane, ensure that the **Agent Status** column is displayed. If the **Agent Status** column is not displayed, right-click a column heading, and then click **Agent Status**. This adds the **Agent Status** column to the **Hosts** pane.
3. Select the host that you need to reassociate with the VMM management server.

Tip

You can use the SHIFT key or the CTRL key to select multiple hosts.

4. On the **Hosts** tab, in the **Host** group, click **Refresh**.

   If a host needs to be reassociated, the **Host Status** column for the host will display a value of **Needs Attention** and the **Agent Status** column will display a value of **Access Denied**.

5. Right-click the host to reassociate, and then click **Reassociate**.
6. In the **Reassociate Agent** dialog box, provide the necessary credentials, and then click **OK**.

   The **Agent Status** column will display a value of **Reassociating**. After the host has been reassociated successfully, the **Agent Status** column will display a value of **Responding**. And after you refresh the host again, the **Host Status** column for the host will display a value of **OK**.

   Tip

   You will see a **Reassociate agent** job in the Jobs workspace.

7. After you have reassociated the host, you will most likely have to update the VMM agent on the host. To update the VMM agent, see How to Update the VMM Agent.

You can also reassociate a VMM library server in a similar manner. To view a list of VMM library servers, open the Fabric workspace, expand **Servers**, and then click **Library Servers**.

How to Update the VMM Agent

To ensure that all virtual machine operations run properly after the upgrade, you must update the VMM agents on virtual machine host computers. Use the following procedure to update the VMM agent on a virtual machine host after upgrading to System Center 2012 –
Virtual Machine Manager.

To update the VMM agent of a host

1. In the VMM console, open the **Fabric** workspace, expand **Servers**, and then click **All Hosts**.
2. In the **Hosts** pane, right-click a column heading, and then click **Agent Version Status**. This adds the **Agent Version Status** column to the **Hosts** pane.
3. Select the host whose VMM agent you want to update.

   Tip

   You can use the SHIFT key or the CTRL key to select multiple hosts.

4. On the **Hosts** tab, in the **Host** group, click **Refresh**.

   If a host needs to have its VMM agent updated, the **Host Status** column for the host will display a value of **Needs Attention** and the **Agent Version Status** column will display a

value of **Upgrade Available**.

5. Right-click the host whose VMM agent you want to update, and then click **Update Agent**.

   Note
   The Update Agent button is enabled (not grayed out) only when the software version of the agent is older than the version of the VMM host.

6. In the **Update Agent** dialog box, provide the necessary credentials, and then click **OK**.

   The **Agent Version Status** column will display a value of **Upgrading**. After the VMM agent has been updated successfully on the host, the **Agent Version Status** column will display a value of **Up-to-date**. And after you refresh the host again, the **Host Status** column for the host will display a value of **OK**.

   Tip
   You will see a **Refresh host** and an **Update agent** job in the Jobs workspace.

You can also update the VMM agent on a VMM library server in a similar manner. To view a list of VMM library servers, open the Fabric workspace, expand **Servers**, and then click **Library Servers**.

Note
To update a VMM agent using the `Update-SCVMMManagedComputer` cmdlet in Windows Powershell, see How to Update the VMM Agent

Troubleshooting a VMM Upgrade

For general information about troubleshooting VMM, see the System Center 2012 – Virtual Machine Manager (VMM) General Troubleshooting Guide on the TechNet Wiki.

Log Files

If there is a problem during upgrade, consult the log files that are located in the **%SYSTEMDRIVE%\ProgramData\VMMLogs** folder. Note that the **ProgramData** folder is a hidden folder.

Known Issues

The following are known issues with upgrading to System Center 2012 – Virtual Machine Manager:

- If multiple errors occur during upgrade, only the first error encountered is shown in the setup wizard. To see all errors that occurred, see the log files.

Administering System Center 2012 - Virtual Machine Manager

The following topics provide information to help you administer Virtual Machine Manager:

- Configuring Fabric Resources in VMM

  The term fabric is used to denote the infrastructure - the software, servers, high-speed connections and switches that enable access to storage devices in a network. Describes how to configure and manage virtualization host, networking, storage, and library resources in VMM.
- Creating and Deploying Virtual Machines and Services in VMM

  Describes how to create, deploy, and manage private clouds, virtual machines, and services in VMM.
- Migrating Virtual Machines and Storage in VMM

  Describes migration in VMM, how to perform a quick storage migration, and how to run live migration.
- Monitoring and Reporting in VMM

  Describes how to integrate VMM with System Center 2012 – Operations Manager to monitor the health and performance of virtual machine hosts and their virtual machines. Also describes how to use the reporting functionality of Operations Manager.
- Performing Maintenance Tasks in VMM

  Describes how to perform common maintenance tasks in VMM.
- Remote Console in System Center 2012 R2

  Describes Remote Console, which enables tenants to access the console of their virtual machines when other remote tools or Remote Desktop is unavailable. This feature is available in System Center 2012 R2.

For an overview of VMM, see Overview of System Center 2012 - Virtual Machine Manager.

Configuring Fabric Resources in VMM

The following topics provide information to help you configure and manage your virtualization host, networking, storage, and library resources in System Center 2012 – Virtual Machine Manager (VMM):

- Preparing the Fabric in VMM
- Adding and Managing Hyper-V Hosts and Scale-Out File Servers in VMM
- Configuring Dynamic Optimization and Power Optimization in VMM
- Managing VMware ESX and Citrix XenServer in VMM
- Managing Fabric Updates in VMM

For an overview of VMM, see Overview of System Center 2012 - Virtual Machine Manager.

Preparing the Fabric in VMM

This section explains how to prepare the fabric in System Center 2012 – Virtual Machine Manager (VMM). The term fabric is used to denote the infrastructure - the software, servers, high-speed connections and switches that enable access to storage devices in a network.

This section covers the following areas:

- Preparing the Fabric Scenario in VMM
- Creating host groups
- Configuring the library
- Configuring networking
- Configuring storage

Note

Other fabric preparation tasks, such as adding hosts, adding Pre-Boot Execution Environment (PXE) servers, and adding Windows Server Update Services (WSUS) servers, are covered in the Adding and Managing Hyper-V Hosts and Scale-Out File Servers in VMM, Managing VMware ESX and Citrix XenServer in VMM, and Managing Fabric Updates in VMM sections.

The topics in this section include example scenarios that will help guide you through the process. The example scenarios refer to a fictitious organization whose domain is contoso.com.

In This Section

Preparing the Fabric Scenario in VMM

Provides an overview of the example fabric resources that the fabric configuration scenarios use.

Creating Host Groups in VMM

Provides an overview of host groups in VMM.

Configuring the VMM Library

Provides an overview of the library in VMM, including a description of the new library features.

Configuring Networking in VMM

Provides an overview of the new networking features in VMM.

Configuring Storage in VMM

Provides an overview of the new storage discovery, storage classification, and storage

allocation features in VMM.

Preparing the Fabric Scenario in VMM

The procedures in this section describe how to configure the fabric in System Center 2012 – Virtual Machine Manager (VMM).

In this section, you will configure the fabric to provide sample resources for hosts, virtual machines and services. In the example scenarios, you will create a host group structure, configure the library, and configure resources for both networking and storage. Because several of these scenarios depend on your existing hardware and physical infrastructure, consider the examples as guidelines. The examples that are used in the documentation are designed to help you to understand the logical flow from preparing the infrastructure to making the infrastructure building blocks available to a private cloud.

The following table summarizes the sample resources that are used in this section.

<table>
<tr><th>Resource</th><th>Name</th></tr>
<tr><td>Host groups</td><td>Seattle
Tier0_SEA
Tier1_SEA
Tier2_SEA
New York
Tier0_NY
Tier1_NY
Tier2_NY</td></tr>
<tr><td>Library shares</td><td>VMMServer01\SEALibrary (in Seattle)
NYLibrary01\NYLibrary (in New York)</td></tr>
<tr><td>Networking</td><td>Logical networks:<table><tr><th>Name</th><th>Description</th></tr><tr><td>FRONTEND</td><td>Public network. Use for Internet-facing Web servers.</td></tr><tr><td>BACKEND</td><td>Corporate network. Use for internal servers such as application and</td></tr></table></td></tr>
</table>

<table>
<tr><th>Resource</th><th>Name</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>database servers.
  Note
In the examples, only the BACKEND logical network is fully defined with example network sites, example IP subnets assigned and an example static IP address pool.</td></tr>
<tr><td>LAB</td><td>Lab network. Use for test and development labs.</td></tr>
</table>
Network sites for the BACKEND logical network:
<table>
<tr><th>Name</th><th>Subnet</th><th>VLAN</th></tr>
<tr><td>BACKEND - Seattle</td><td>10.0.0.0/24</td><td>7</td></tr>
<tr><td>BACKEND – New York</td><td>172.16.0.0/24</td><td>12</td></tr>
</table>
IP address pool:
<table>
<tr><td>Name</td><td>BACKEND - Seattle IP pool</td></tr>
<tr><td>Description</td><td>IP addresses for internal application and database servers - Seattle</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Resource</th><th>Name</th></tr>
<tr><td></td><td>
<table>
<tr><td>Begin IP address</td><td>10.0.0.10</td></tr>
<tr><td>End IP address</td><td>10.0.0.99</td></tr>
<tr><td>Reserved range for virtual IP addresses associated with load balancers:</td><td>10.0.0.25 – 10.0.0.35</td></tr>
<tr><td>Default gateway</td><td>10.0.0.1</td></tr>
<tr><td>DNS server</td><td>10.0.0.2</td></tr>
<tr><td>WINS server</td><td>10.0.0.3</td></tr>
</table>
MAC address pool:
<table>
<tr><td>Name</td><td>MAC pool - Seattle</td></tr>
<tr><td>Starting address</td><td>00:1D:D8:B7:1C:00</td></tr>
<tr><td>Ending address</td><td>00:1D:D8:B7:1F:E8</td></tr>
</table>
Load balancer:
<table>
<tr><td>Name</td><td>LoadBalancer01.contoso.com</td></tr>
<tr><td>VIP template</td><td>Web tier (HTTPS traffic)</td></tr>
</table>
</td></tr>
<tr><td>Storage</td><td>
Storage classifications:
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>GOLD</td><td>Storage pool based on solid-state drives (SSDs) that delivers high performance for I/O intensive applications</td></tr>
<tr><td>SILVER</td><td>Fibre Channel Serial Attached SCSI (SAS) storage (RAID 5)</td></tr>
</table>
</td></tr>
</table>

Resource	Name	
	BRONZE	**iSCSI Serial ATA (SATA) storage (RAID 5)**

See Also

Creating Host Groups in VMM

Configuring the VMM Library

Configuring Networking in VMM

Configuring Storage in VMM

Creating Host Groups in VMM

The procedures in this section describe how to create a host group structure in VMM, and how to configure host group properties. You can use host groups to group virtual machine hosts in meaningful ways, often based on physical site location and resource allocation. When you design a host group structure, consider the following:

- Several settings and resources are assigned at the host group level, such as custom placement rules, host reserve settings for placement, dynamic optimization and power optimization settings, network resource inheritance, host group storage allocation, and custom properties. By default, child host groups inherit the settings from the parent host group.

  Note
  In the properties of a virtual machine host, you can choose to override host reserve settings from the parent host group.
- You can assign host groups to the Delegated Administrator and the Read-Only Administrator user roles to scope the user roles to specific host groups. Members of these user roles can view and manage the fabric resources that are assigned to them at the host group level.
- You can create a private cloud from resources in host groups. When you create a private cloud, you select which host groups will be part of the private cloud. You can then allocate all or some of the resources from the selected host groups to the private cloud.

In This Section

Follow these procedures to configure host groups in VMM.

Procedure	Description
How to Create a Host Group Structure in VMM	Describes how to create a host group hierarchy, and how to move a host group to another location.

Procedure	Description
How to Configure Host Group Properties in VMM	Describes how to configure host group properties.

How to Create a Host Group Structure in VMM

You can use the following procedures to create a host group structure in VMM that aligns to your organizational needs.

To create a host group structure

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then do either of the following:
   - Right-click **All Hosts**, and then click **Create Host Group**.
   - Click **All Hosts**. On the **Folder** tab, in the **Create** group, click **Create Host Group**.

   VMM creates a new host group that is named **New host group**, with the host group name highlighted.
3. Type a new name, and then press ENTER.

   For example, type **Seattle**, and then press ENTER.

   Note

   To rename a host group, do either of the following:
   - Right-click the host group, and then click **Rename**.
   - On the **General** tab of the host group properties, enter the host group name in the **Name** box.
4. Repeat the steps in this procedure to create the rest of the host group structure.

   For example, create the following host group structure. This host group structure is used in the examples throughout the documentation and is used to help demonstrate the concepts. You can adapt the examples to your test environment.

   Tip

   To create a host group at a specific location in the tree, right-click the desired parent node, and then click **Create Host Group**.

   Seattle

   Tier0_SEA

   Tier1_SEA

   Tier2_SEA

   New York

   Tier0_NY

   Tier1_NY

Tier2_NY

Note

This example host group structure is based on location and the capabilities of the hardware, including the level of redundancy. For example, in Tier0 you may have clustered hosts, the fastest and most reliable storage with replication, load balancing and the most network throughput. Tier1 may have clustered hosts, but lower speed storage that is not replicated. Tier2 may consist of stand-alone hosts with the lowest speed storage, and possibly less bandwidth. This is just one example of a host group structure. In your organization you may use a different model, such as one that is based on applications or server role, type of hypervisor, business unit or delegation model.

To move a host group to another location

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then expand **All Hosts**.
3. To move a host group to another location in the tree, do any of the following:
   - Drag the host group that you want to move to its new location in the tree.
   - Right-click the host group that you want to move, and then click **Move**. In the **Parent host group** list, click a parent host group, and then click **OK**.
   - Click the host group that you want to move. On the **Folder** tab, in the **Actions** group, click **Move**. In the **Parent host group** list, click a parent host group, and then click **OK**.

See Also

Creating Host Groups in VMM

How to Configure Host Group Properties in VMM

How to Configure Host Group Properties in VMM

You can use the following procedure to configure host group properties in VMM.

To configure host group properties

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, expand **All Hosts**, and then click the host group that you want to configure.
3. On the **Folder** tab, in the **Properties** group, click **Properties**.
4. Configure any of the following settings:

Tab	Settings
General	Configure the host group name, the location in the host group hierarchy, the

	description, and whether to allow unencrypted BITS file transfers.
Placement Rules	VMM automatically identifies the most suitable host to which you can deploy virtual machines. However, you can specify custom placement rules. By default, a host group uses the placement settings from the parent host group.
Host Reserves	Host reserve settings specify the amount of resources that VMM sets aside for the host operating system to use. For a virtual machine to be placed on a host, the host must be able to meet the virtual machine's resource requirements without using host reserves. You can set host reserves for individual host groups and for individual hosts. The host reserve settings for the root host group, All Hosts, sets the default host reserves for all hosts. You can configure reserve values for the following resources: • CPU • Memory • Disk I/O • Disk space • Network I/O
Dynamic Optimization	Configure dynamic optimization and power optimization settings. Dynamic optimization balances the virtual machines load within a host cluster. Power optimization enables VMM to evacuate hosts of a balanced cluster and turn them off to save power. For more information about these settings, see Configuring Dynamic Optimization and Power Optimization in VMM.
Network	View inheritance settings, and configure whether to inherit network logical resources from parent host groups. The network logical resources include the following:

	• IP address pools • Load balancers • Logical networks • MAC address pools
Storage	View and allocate storage to a host group. For more information, see the following topics: • How to Allocate Storage Logical Units to a Host Group in VMM • How to Allocate Storage Pools to a Host Group in VMM
Custom Properties	Manage custom properties for the following object types: • Virtual machine • Virtual machine template • Host • Host cluster • Host group • Service template • Service instance • Computer tier • Cloud

See Also

Creating Host Groups in VMM

How to Create a Host Group Structure in VMM

Configuring the VMM Library

The procedures in this section describe how to perform basic configuration of the library in Virtual Machine Manager (VMM). The VMM library is a catalog of resources that provides access to file-based resources such as virtual hard disks, virtual floppy disks, ISO images, scripts, driver files and application packages that are stored on library servers, and to non file-based resources such as virtual machine and service templates and profiles that reside in the VMM database.

Note

Although the library in System Center 2012 – Virtual Machine Manager provides new functionality to support service creation and the sharing of resources in a private cloud, you can still use the library in the same way that you did for VMM 2008 R2.

The VMM library can store the following types of resources:

- **File-based resources**. File-based resources include virtual hard disks, virtual floppy disks, ISO images, scripts, driver files and application packages. To be used in VMM, a file must be added to the library. New in System Center 2012 – Virtual Machine Manager, you can store application packages that are used for service creation. These application packages include SQL Server data-tier applications, Web Deploy packages, and Server App-V packages. You can also store driver files that are used during the deployment of an operating system when you use VMM to convert a bare-metal computer to a managed Hyper-V host.

  Note

  You can also add custom resources to the library. Custom resources enable you to store resources in the library that would otherwise not be indexed and show up as available resources by the library server. If a user creates a folder with a .CR extension, and then saves the contents to a library share, the folder contents will be available to all users who can access the share. VMM will discover and import the folder into the library as a custom resource. Examples of what you may want to store as a custom resource are pre- and post-execution scripts that you want to use for service deployment, or a custom installation package.

  A library server can discover only those files that are associated with a version of an operating system that is equal or earlier than the version of the operating system that the library server is running. For example, a library server that is running Windows Server 2008 R2 will not discover .vhdx files because they are associated with Windows Server 2012. The following table lists the file types that are automatically indexed and added as physical library resources during library refreshes in VMM.

Library Resource	File Name Extension
Virtual hard disks	.vhd (Hyper-V and Citrix XenServer), .vhdx (Hyper-V), .vmdk (VMware)
ISO image files	.iso
PowerShell scripts	.ps1
SQL Server scripts	.sql
Web Deploy (MSDeploy) packages **Note** These appear in the library as the “Web Application Package” type.	.zip
SQL Server data-tier applications (DACs)	.dacpac
Server App-V packages **Note** These appear in the library as the “Virtual Application Package” type.	.osd
Driver files	.inf **Important** If you add driver files, we strongly recommend that you create a separate folder for each driver package, and that you do not mix resources in the driver folders. If you include other library resources such as .iso images, .vhd files or scripts with an .inf file name extension in the same folder, the library will not discover those resources. Also, realize that when you delete an .inf driver package from the library, VMM deletes the entire folder where the driver .inf file resides. For more information, see How to Add Driver Files to the VMM Library.

Library Resource	File Name Extension
Answer files	.inf, .xml
Custom resources	Folders with .CR extension
Virtual floppy disks	.vfd (Hyper-V), .flp (VMware)

Note
Virtual hard disks, ISO images, and virtual floppy disks that are attached to a stored virtual machine, and the configuration files for stored virtual machines, are indexed in VMM but are not displayed as physical resources. The virtual machine configuration files are created by the virtualization software but are not used by VMM. VMM stores a stored virtual machine's configuration in the VMM database. Virtual machine configuration files include .vmc, .xml, and .vmx (VMware) files.

- **Templates and profiles**. Templates and profiles are used to standardize the creation of virtual machines and services. These configurations are stored in the VMM database but are not represented by physical configuration files. There are several new types of templates and profiles in VMM, most of which are used for service creation. There are also host profiles and as of System Center 2012 R2 Virtual Machine Manager physical computer profiles, used for deploying a Hyper-V host from a bare-metal computer, and capability profiles, used to specify the capabilities of virtual machines on each type of supported hypervisor when virtual machines are deployed to a private cloud.

  Note
  The VMM library recognizes the .vmtx extension for VMware templates. If you import a VMware template, the template appears under **Templates**, in the **VM Templates** node.

- **Equivalent objects**. Equivalent objects are a user-defined grouping of library resources that are considered equivalent. For example, you may mark a Windows Server 2008 R2-based virtual disk that is located on a library share in Seattle and a Windows Server 2008 R2-based virtual disk that is located on a library share in New York as equivalent. In a template or profile, when you point to a specific virtual disk on a specific library share, VMM can substitute any equivalent object during virtual machine or service creation. By using equivalent objects, you can author templates or profiles that do not depend on particular physical resources. Therefore, you can service resources without affecting the availability of the template or profile.

  Important
  For virtual machine and service deployment, VMM supports only the use of virtual disks, .iso images and custom resources as equivalent objects.

  The VMM placement process determines which resource should be used when a resource that has equivalent objects is defined in a profile or template. Placement considers several factors, such as the association between library servers and host groups to help determine which resource to use. This helps to improve performance and optimize network bandwidth

usage. Therefore, we recommend that you use resources that have equivalent objects when you create profiles such as application and host profiles, and when you create virtual machine and service templates.

Note
The resources that you mark as equivalent can be files that are replicated by a replication technology or files that you manually copy to each location.

- **Cloud libraries**. Private cloud libraries consist of read-only library shares that are assigned to a private cloud and a **Stored Virtual Machines and Services** node where self-service users who have appropriate permissions can store virtual machines and services. An administrator or a delegated administrator whose management scope includes the library servers can add resources to the read-only library shares that they want to make available to users of the private cloud.

  During private cloud creation, VMM adds a private cloud library to the **Cloud Libraries** node, with a name that matches the private cloud name. If the administrator specifies read-only library shares and a path to store virtual machines, the library shares and the **Stored Virtual Machines and Services** nodes appear under the private cloud library. For information about how to create a private cloud, see Creating a Private Cloud in VMM Overview.
- **Self-service user content**. This node enables self-service users to upload their own resources such as authored templates, virtual disks, ISO image files, application files, scripts and other building blocks to the VMM library. They can use these resources when they author templates. Because this node enables self-service users to write to a common file path that other members of their user role have access to, self-service users with appropriate permissions can share resources with other users in the same or a different self-service user role.

  Note
  To share with users in a different self-service user role, the target self-service user role must have appropriate permissions. For information about how to configure permissions for a self-service user role, see How to Create a Self-Service User Role in VMM.
- **Stored virtual machines and services**. Users can choose to store virtual machines that are not in use to the **Stored Virtual Machines and Services** node. This node is available when you expand **Library Servers**, and then expand the library server.

  Note
  Be aware that when a self-service user stores a virtual machine or service to the library, the resource is stored in the **Stored Virtual Machines and Services** node in the private cloud library.
- **Orphaned resources**. When you remove a library share from VMM management, and there are templates that reference resources that were located on the library share, a representation of the library resource appears in the **Orphaned Resources** node. You can click an orphaned resource to view the templates that reference the orphaned resource. You can then modify the template to reference an existing resource in the VMM library.

- **Update catalog and baselines**. If you manage updates through VMM for the VMM management server and other computers that are under VMM management, Windows Server Update Services (WSUS) update baselines are stored in the VMM library. Updates are covered in more detail in Managing Fabric Updates in VMM.

Operating System Requirements

For information about the supported operating systems for the library server role, see the following topics:

- For System Center 2012 – Virtual Machine Manager or for System Center 2012 SP1 see **System Requirements: VMM Library Server in System Center 2012 and in System Center 2012 SP1**.
- For System Center 2012 R2 Virtual Machine Manager see: **Preparing your environment for System Center 2012 R2 Virtual Machine Manager**.

High Availability

To make the library server highly available, you can create highly available file shares on a clustered file server that meets the operating system requirements that are outlined in the 'Operating System Requirements' section above. For more information, see Create a Shared Folder in a Clustered File Server.

Important
Do not create highly available file shares for the VMM library on the same cluster as a highly available VMM management server installation. VMM does not support this configuration.

Example Scenario Overview

The example scenarios in this section assume that you have a VMM management server installed and a library share configured as part of VMM installation. The scenarios also use a server in a second site that you add as a library server. To demonstrate the concept of equivalent objects, it is best to use multiple library servers and library shares. The following table summarizes the example names that are used in this section.

Note
The example resource names and configuration are used to help demonstrate the concepts. You can adapt them to your test environment.

Resource	Resource Name
VMM management server	**VMMServer01.contoso.com**
Library share in Seattle (added during VMM management server installation)	**VMMServer01\SEALibrary**
Library server and share in New York	**NYLibrary01\NYLibrary**

In This Section

Use the following procedures to perform basic configuration of the VMM library.

Procedure	Description
How to Add a VMM Library Server or VMM Library Share	Describes how to add a new library server or library share.
How to Associate a VMM Library Server with a Host Group	Describes how to associate a library server with a host group. This association helps VMM to determine which resource to use when there is a set of equivalent objects.
How to Add File-Based Resources to the VMM Library	Describes how to add file-based resources to the library.
How to Create or Modify Equivalent Objects in the VMM Library	Describes how to mark file-based objects as equivalent.
How to View and Remove Orphaned Resources in VMM	Describes how to view orphaned resources, and how to resolve any issues with templates that reference the orphaned resource so that you can remove the orphaned resource.

How to Add a VMM Library Server or VMM Library Share

You can use the following procedures to add a library server and library shares to an existing System Center 2012 – Virtual Machine Manager (VMM) installation. When you add a library server to VMM management, VMM installs the VMM agent on the new library server.

Note
During VMM Setup, you can either create a library share or specify an existing share. If you accept the default, a library share that is named MSSCVMMLibrary is created on the VMM management server.

Account requirements To add a library server, you must be a member of the Administrator user role or the Delegated Administrator user role. To add a library share, you must be a member of the Administrator user role or a member of the Delegated Administrator user role where the management scope includes the library server where the share is located.

Prerequisites

- To add a library server, the server must meet the operating system requirements that are outlined as follows:
  - For System Center 2012 – Virtual Machine Manager or for System Center 2012 SP1 see **System Requirements: VMM Library Server in System Center 2012 and in System Center 2012 SP1**.

    - For System Center 2012 R2 Virtual Machine Manager see: **Preparing your environment for System Center 2012 R2 Virtual Machine Manager**.
- The library server that you want to add must be in the same domain as the VMM management server, or in a domain that has a two-way trust with the domain of the VMM management server (including domains with disjointed namespaces).
- When you add a library server, the firewall on the server that you want to add must allow File and Print Sharing (SMB) traffic to enable VMM to enumerate and display the available shares.
- When you add a library server or you add a library share to a library server that is already under VMM management, you must designate an existing share. Therefore, before you add a library server or library share, you must manually create the shared folder on the target server outside VMM.

  Important
  Do not create highly available file shares for the VMM library on the same cluster as a highly available VMM management server installation. VMM does not support this configuration.

  Note
  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.
- When you add a library server, you must specify account credentials for a domain account that has administrative rights on the computers that you want to add. You can enter a user name and password or specify a Run As account. If you want to use a Run As account, you can create the Run As account before you begin this procedure, or create it during the procedure.

  Note
  You can create Run As accounts in the **Settings** workspace. For more information about Run As accounts, see How to Create a Run As Account in VMM.

To add a library server

1. Open the **Library** workspace.
2. On the **Home** tab, in the **Add** group, click **Add Library Server**.

The Add Library Server wizard opens.

3. On the **Enter Credentials** page, enter the credentials for a domain account that has administrative rights on the servers that you want to add, and then click **Next**. You can specify a Run As account or manually enter user credentials in the format *domain_name\user_name*.

   Note
   If you do not already have a Run As account, click **Browse**, and then in the **Select a Run As Account** dialog box, click **Create Run As Account**.

4. On the **Select Library Servers** page, do the following:
   a. In the **Domain** box, enter the name of the domain that the server belongs to.
   b. In the **Computer name** box, enter the name of the server that you want to add. If you are not sure of the computer name, click **Search**, and then enter the search criteria.

      For example, enter the name of the library server in New York, **NYLibrary01**.
   c. If you want to skip Active Directory name verification, select the **Skip Active Directory name verification** check box.
   d. Click **Add** to add the server to the **Selected servers** area.
   e. To add more library servers, repeat steps 4a through 4c. When you are finished, click **Next**.

5. On the **Add Library Shares** page, select the check box next to each library share that you want to add. If you want to add the default library resources to the share that are used for services, select the **Add Default Resources** check box.

   Note
   If you add the default resources, this adds the ApplicationFrameworks folder to the library share. Resources in the ApplicationFrameworks folder include x86 and x64 versions of the Server App-V Agent, Server App-V Sequencer, Windows PowerShell cmdlets for Server App-V, and the Microsoft Web Deployment tool. The folder also includes scripts that you can add to application profiles in service templates to install virtual applications and Web applications during service deployment. If you add the default resources to multiple library shares, the files are automatically grouped as equivalent resources because of matching family names, release values, and namespace.

   When you are finished, click **Next**.

   For example, select the check box next to the **NYLibrary** share on the **NYLibrary01** library server.

6. On the **Summary** page, review the settings, and then click **Add Library Servers**.

   The **Jobs** dialog box appears. Make sure that the job indicates that the library server was successfully added, and then close the dialog box.

7. To verify that the library server and shares were added, in the **Library** pane, expand the **Library Servers** node.

   Verify that the library servers and shares are listed.

To add a library share

1. Open the **Library** workspace.
2. In the **Library** pane, expand **Library Servers**, and then click the library server where you want to add the share.
3. On the **Library Server** tab, click **Add Library Shares**.
4. On the **Add Library Shares** page, select the check box next to each library share that you want to add, and then click **Next**. If you want to add the default library resources to the share that are used for services, select the **Add Default Resources** check box.

   Note
   If you add the default resources, this adds the ApplicationFrameworks folder to the library share. Resources in the ApplicationFrameworks folder include x86 and x64 versions of the Server App-V Agent, Server App-V Sequencer, Windows PowerShell cmdlets for Server App-V, and the Microsoft Web Deployment tool. The folder also includes scripts that you can add to application profiles in service templates to install virtual applications and Web applications during service deployment. If you add the default resources to multiple library shares, the files are automatically grouped as equivalent resources because of matching family names, release values, and namespace.
5. On the **Summary** page, review the settings, and then click **Add Library Shares**.

   The **Jobs** dialog box appears. Make sure that the job indicates that the library shares were successfully added, and then close the dialog box.
6. To verify that the new library shares were added, in the **Library** pane, expand the **Library Servers** node, and then expand the library server where you added the share.

   Verify that the library shares appear under the library server name.

See Also

Configuring the VMM Library

How to Create or Modify Equivalent Objects in the VMM Library

How to Associate a VMM Library Server with a Host Group

You can use the following procedure to associate a library server with a host group in System Center 2012 – Virtual Machine Manager (VMM). During placement, VMM uses this association as an input to help determine which resource to use when a resource with equivalent objects is defined in a profile or template.

Account requirements You must be a member of the Administrator user role or a member of the Delegated Administrator user role where the management scope includes the library server that you want to configure.

To associate a library server with a host group

1. Open the **Library** workspace.

2. In the **Library** pane, expand **Library Servers**, and then click a library server.
3. On the **Library Server** tab, click **Properties**.
4. In the *Library Server Name* **Properties** dialog box, in the **Host group** list, click the host group that you want to associate the library server with, and then click **OK**.

   For example, associate the **VMMServer01.contoso.com** library server (located in Seattle) with the **Seattle** host group. Associate the **NYLibrary01.contoso.com** library server with the **New York** host group.

   Note
   You can associate a library server with only one host group. However, child host groups are automatically associated with the library server of the parent host group. Also, realize that you can associate more than one library server with a host group.

See Also

Configuring the VMM Library

How to Add File-Based Resources to the VMM Library

You can use the following procedure to add file-based resources (such as virtual hard disks and application packages, also known as physical resources) to an existing library share in System Center 2012 – Virtual Machine Manager (VMM), and then manually refresh the library share. When you add files to a library share, the files do not appear in the library until VMM indexes the files during the next library refresh. By default, the library refresh interval is one hour.

Note
One hour is the smallest value that you can configure for the library refresh interval. To change the library refresh interval, open the **Library** workspace, and then on the **Home** tab, click **Library Settings**.

For information about the types of file-based resources that the VMM library automatically indexes and adds as physical resources, see the table under the “File-based resources” bullet in Configuring the VMM Library.

Account requirements To add resources to a library share outside VMM or by using the **Explore** option in the Library workspace, a user must have appropriate share and file system permissions assigned outside VMM. This applies to administrators, delegated administrators and to self-service users (for private cloud library shares). For information about the account requirements to import and export file-based resources, see How to Import and Export File-Based Resources To and From the Library.

To add file-based resources to the library

1. Do any of the following:
   - Outside VMM, browse to the library share, and then copy the files to the share.
   - In the **Library** workspace of the VMM console, expand **Library Servers**, expand a library server, right-click a library share, and then click **Explore**. Then, copy files to

the share.

- In the **Library** workspace of the VMM console, on the **Home** tab, use the **Import Physical Resource** and **Export Physical Resource** options to import and export file-based resources between library shares. For more information, see How to Import and Export File-Based Resources To and From the Library.

For example, copy files that you want to use to the library shares in both sites (**VMMServer01\SEALibrary** and **NYLibrary01\NYLibrary**).

Note

If you want to create sets of equivalent objects, make sure that you add resources that you consider equivalent to library shares in one or more sites. For example, add a Windows Server 2008 R2-based .vhd file to multiple sites. For information about how to create equivalent objects, see How to Create or Modify Equivalent Objects in the VMM Library.

2. To be able to use the files immediately, manually refresh the library share or library server. To do this, follow these steps:
   a. Open the **Library** workspace.
   b. In the **Library** pane, expand **Library Servers**, right-click the library server or library share that you want to refresh, and then click **Refresh**.

   You can open the **Jobs** workspace to view the refresh status.
3. If the file you added is a virtual hard disk file, as a best practice, provide VMM with important information about that file. This can simplify the process of creating virtual machine templates (VM templates) based on the file. To do this:
   a. In the **Library** workspace, with **Library Servers** expanded, navigate to the library server or library share that contains the file.
   b. Right-click the file and then click **Properties**.
   c. For **Operating system**, expand the list and select the operating system that has been placed on the virtual hard disk.
   d. Optionally, for **Virtualization platform**, select the virtualization platform on which you will deploy virtual machines that use the file.

   When you have updated the properties, click **OK**.

See Also

Configuring the VMM Library

How to Add a VMM Library Server or VMM Library Share

How to Create or Modify Equivalent Objects in the VMM Library

You can use the following procedures to mark file-based library resources (also known as physical resources) as equivalent objects in System Center 2012 –
Virtual Machine Manager (VMM), and to modify equivalent objects. For example, if you have a Windows Server 2008 R2-based virtual hard disk (.vhd) file that is stored in library shares that are located in two sites, such as Seattle and New York, you can mark the .vhd files as equivalent objects. Then, when you create a template for a new virtual machine, and you specify a .vhd that

has equivalent objects, VMM can use any instance of the equivalent object instead of being site-specific. This enables you to use a single template across multiple sites.

Important
For virtual machine and service deployment, VMM supports only the use of .vhd files, .iso images and custom resources as equivalent objects.

Note
During VMM Setup of a stand-alone VMM management server, Server App-V Framework and Web Deployment Framework custom resources are automatically added to the library as equivalent objects. If you add multiple library shares with the default resources, the framework resources are all automatically marked as equivalent because they share the same family name, release value, and namespace.

Account requirements To mark objects as equivalent, you must be a member of the Administrator, Delegated Administrator or Self-Service user roles. Delegated administrators can only mark objects as equivalent on library shares that are within the scope of their user role. Self-service users can only mark objects as equivalent that are in their user role data path in the Self Service User Content node of the VMM library.

To mark objects as equivalent

1. Open the **Library** workspace.
2. In the **Library** pane, click **Library Servers**.

   Note
   If you are a self-service user, in the **Library** pane, expand **Self Service User Content**, and then click the user role data path.
3. In the **Physical Library Objects** pane (or the **Self Service User Objects** pane if you are connected as a self-service user), click the **Type** column header to sort the library resources by type.

   Note
   If you are an administrator or a delegated administrator, the **Library Server** column indicates the location of each resource.
4. Select the resources that you want to mark as equivalent by using either of the following methods:

   Important
   The resources that you want to mark as equivalent must be of the same file type. For example, you can mark equivalent .vhd files as equivalent objects, and mark equivalent .iso files as another set of equivalent objects.

   - Click the first resource, press and hold the CTRL key, and then click the other resources that you want to mark as equivalent.
   - To select a range, click the first resource in the range, press and hold the SHIFT key,

and then click the last resource in the range.

For example, if you stored a Windows Server 2008 R2-based .vhd file on the Seattle library share that is named **Win2008R2Ent**, and an equivalent .vhd file is located in the New York library share, select both of the .vhd files.

5. Right-click the selected resources, and then click **Mark Equivalent**.
6. In the **Equivalent Library Objects** dialog box, do either of the following, and then click **OK**:
   - If you want to create a new set of equivalent objects, in the **Family** list, type the family name. In the **Release** list, type a release value.

     For example, enter the family name **Windows Server 2008 R2 Enterprise**, and the release value **1.0**.

     Note
     The value in the **Release** list is a string field. Therefore, you can enter any string value.
   - If you want to add the resources to an existing set of equivalent objects, in the **Family** list, click an existing family name. In the **Release** list, click the release value.

     The library objects that are considered equivalent are listed in the lower pane.
7. To verify that the set of equivalent objects was created, in the **Library** pane, click **Equivalent Objects**.

   Verify that the objects that you marked as equivalent appear in the Equivalent Objects pane. They are grouped by family name.

To mark objects as equivalent, the objects must have the same family name, release value, and namespace. The namespace is assigned automatically by VMM. Equivalent objects that are created by an administrator or delegated administrator are assigned the Global namespace. If a self-service user creates equivalent objects within the Self Service User Content node of the Library workspace, VMM assigns a namespace value that matches the name of the self-service user role. This means that a self-service user cannot mark an object as being equivalent with another object that the self-service user role does not own.

To modify equivalent objects

1. Open the **Library** workspace.
2. In the **Library** pane, click **Equivalent Objects**.
3. In the **Equivalent Objects** pane, expand a family name, expand the release value, right-click the object that you want to modify, and then click **Properties**.
4. On the **General** tab, modify any of the values, or enter new ones. To remove an object from a set of equivalent objects, delete the family name and release values.
5. When you are finished, click **OK** to confirm the settings and to close the dialog box.

See Also

Configuring the VMM Library

How to View and Remove Orphaned Resources in VMM

You can use the following procedure to view and remove orphaned resources in the System Center 2012 – Virtual Machine Manager (VMM) library. When you remove a library share from VMM management, and there are templates that reference resources that were located on the library share, a representation of the library resource appears in the VMM library as an orphaned resource.

To remove orphaned resources, you must modify the templates that reference the orphaned resources to use valid library resources in the VMM library. If you re-add the library share, VMM does not automatically re-associate the template with the physical library resource. Therefore, you must still complete the procedures in this topic to correct template issues and to remove any orphaned resources.

Account requirements You must be a member of the Administrator user role or a member of the Delegated Administrator role to complete these procedures. Delegated administrators can view and remove only orphaned resources from library shares that were within the scope of their user role. Self-service users do not see the Orphaned Resources node.

To view and remove orphaned objects

1. Open the **Library** workspace.
2. In the **Library** pane, click **Orphaned Resources**.

   Any orphaned resources appear in the Physical Library Objects pane.

   Note

   You cannot delete an orphaned resource until templates that reference the orphaned resources are updated to reference objects that are in the VMM library.
3. To view the templates which reference an orphaned resource, right-click the orphaned resource, and then click **Properties**.
4. In the *Resource Name* **Properties** dialog box, click the **Dependencies** tab.

   The templates that reference the orphaned resource are listed.
5. To update the template to point to a valid resource, click the template name, and then do the following:
   a. In the *Template Name* **Properties** dialog box, locate the resource that is missing, and then click **Remove**. For example, if a .vhd file is missing, click **Hardware Configuration**. Under **Bus Configuration**, click the disk that does not have an associated path, and then click **Remove**.
   b. Add the new resource using a resource that is in the VMM library. For example, add a new disk, click **Browse**, and then click an existing .vhd file.
6. Repeat step 5 for any other templates that reference the orphaned object.
7. When you are finished, click **OK** to close the *Orphaned Resource* **Properties** dialog box.
8. To verify that there are no dependencies, right-click the orphaned resource, and then click **Properties**. Then, click the **Dependencies** tab.

   If there are no dependencies, VMM indicates that no dependencies are found.

9. After you have verified that there are no dependencies, right-click the orphaned resource, and then click **Delete**.

See Also

Configuring the VMM Library

Configuring Networking in VMM

Networking in Virtual Machine Manager (VMM) includes multiple enhancements that enable you, the administrator, to efficiently provision network resources for a virtualized environment:

- **In System Center 2012**: One of the networking enhancements in System Center 2012 makes it easier to connect virtual machines to a network that serves a particular function in your environment, for example, the “Backend,” “Frontend,” or “Backup” network. To do this, you associate IP subnets and, if needed, virtual local area networks (VLANs) together into named units called logical networks. Also, in logical networks where you do not use Dynamic Host Configuration Protocol (DHCP), you can simplify IP address management by configuring IP pools. Another networking enhancement in VMM in System Center 2012 is the integration of load balancers.
- **In System Center 2012 Service Pack 1 (SP1) and System Center 2012 R2**: Networking in VMM in System Center 2012 Service Pack 1 (SP1) and in System Center 2012 R2 adds more options for greater flexibility. One example is network virtualization, which extends the concept of server virtualization to allow you to deploy multiple virtual networks on the same physical network. Another example is switch extensions, which give you added capabilities with your networks, such as the ability to monitor network traffic, enhance the level of security on your networks, or provide quality of service (QoS) to let you control how your network bandwidth is used.

Configuring networking

To learn more about networking in VMM, see the following topics.

- For scenario descriptions and illustrations showing how you can use networking options in VMM to support your virtual machine configurations, see the following:
  - Common Scenarios for Networking in VMM in System Center 2012
  - Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2
  - Configuring Logical Networking in VMM Illustrated Overview
  - Configuring VM Networks in VMM Illustrated Overview
  - Configuring Ports and Switches in VMM Illustrated Overview
- For information about configuring networking options that are available in System Center 2012, System Center 2012 SP1, and System Center 2012 R2, see the following:
  - Configuring Logical Networking in VMM Overview
  - Configuring Load Balancing in VMM Overview
- For additional networking options that are available in System Center 2012 SP1 and System Center 2012 R2, see the following:
  - Configuring Ports and Switches for VM Networks in VMM

- Configuring VM Networks and Gateways in VMM

Next steps after configuring networking

For information about the next steps to take after configuring networking, see the following topics:

Topic	Step
Preparing the Fabric in VMM	Configure additional fabric resources such as storage and library resources.
Adding and Managing Hyper-V Hosts and Scale-Out File Servers in VMM Managing VMware ESX and Citrix XenServer in VMM	Configure hosts.
Creating and Deploying Virtual Machines and Services in VMM	Deploy virtual machines, individually or as part of a service.

Common Scenarios for Networking in VMM in System Center 2012

This topic presents various networking options in System Center 2012 – Virtual Machine Manager (VMM) that can help enhance and extend the ways in which you work with IP addressing, virtual local area networks (VLANs), and other elements of networking.

Important

This topic describes networking options in VMM in System Center 2012. For information about networking options in VMM in System Center 2012 Service Pack 1 (SP1) and System Center 2012 R2, see Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2.

Networking options in VMM in System Center 2012

The following table describes how you can use networking options in VMM in System Center 2012 to configure the fabric that host systems and virtual machines use.

Scenario	Key information	For more information
Connect virtual machines to a network that serves a particular function in your environment, for example, the "Backend," "Frontend," or "Backup" network. In other words, associate IP subnets and, if needed, virtual local area networks (VLANs) together into	You can design logical networks to suit your environment.	Configuring Logical Networking in VMM Overview How to Create a Logical Network in VMM

Scenario	Key information	For more information
named units , called "logical networks," that virtual machines can use.		
Simplify IP address management in VMM on networks where you do not use Dynamic Host Configuration Protocol (DHCP).	After you create logical networks, you can create IP address pools and, if needed, media access control (MAC) address pools for the logical networks.	Configuring Logical Networking in VMM Overview How to Create IP Address Pools for Logical Networks in VMM
Automatically provision load balancers in your virtualized environment.	• Either use Microsoft Network Load Balancing (NLB) or add supported hardware load balancers to VMM. • NLB is included as an available load balancer in VMM.	Configuring Load Balancing in VMM Overview

See Also

Configuring Logical Networking in VMM Illustrated Overview

Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2

Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2

This topic describes various networking options in Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1) and System Center 2012 R2. These options can enhance and extend the ways in which you work with IP addressing, virtual local area networks (VLANs), routers, switches, and other elements of networking that support your virtual machines.

Important

This topic describes networking options in VMM in System Center 2012 Service Pack 1 (SP1) and System Center 2012 R2. For information about networking options in VMM in System Center 2012, see Common Scenarios for Networking in VMM in System Center 2012.

Scenarios for creating the networking environment for hosts

The following table describes ways in which you can use networking capabilities in VMM in System Center 2012 SP1 or System Center 2012 R2 when you configure the networking environment for virtual machine hosts. For additional scenarios that apply to System Center 2012 SP1 and System Center 2012 R2, see the following:

- Scenarios for logical networks, IP address pools, and network load balancing in this topic
- Scenarios for virtual machine networks in this topic
- Scenarios for virtual switches and switch extensions in this topic

Scenario	Key information	For more information
On a host, use only part of the bandwidth of a physical network adapter, or a teamed set of network adapters, for managing that host.	• Configure a port profile for virtual network adapters that will limit the amount of bandwidth. Also configure a logical switch that includes that port profile. • Assign the logical switch to the management adapter, either in the host's properties, or in a profile that you use to provision Hyper-V hosts.	Configuring Ports and Switches for VM Networks in VMM How to Configure Network Settings on a Host by Applying a Logical Switch in VMM How to Create a Host or a Physical Computer Profile to Provision a Hyper-V Host in VMM
On a host, configure teaming of multiple physical network adapters for increased availability.	• Configure a logical switch and associate it with multiple physical adapters on the host. • The logical switch that you create for this purpose must use **Team** for the uplink mode.	Configuring Ports and Switches for VM Networks in VMM How to Configure Network Settings on a Host by Applying a Logical Switch in VMM How to Create a Host or a Physical Computer Profile to Provision a Hyper-V Host in VMM
On a host, integrate a top-of-rack (TOR) switch with VMM in System Center 2012 R2. This can simplify network configuration and help prevent	For System Center 2012 R2 only: Add a top-of-rack switch to VMM by using the Add Network Service wizard.	How to Add a Top-of-Rack Switch in VMM in System Center 2012 R2

Scenario	Key information	For more information
software misconfiguration of networks.		

Scenarios for logical networks, IP address pools, and network load balancing

The following table describes ways in which you can use networking capabilities in VMM to configure logical networks, IP address pools, and network load balancing to support your virtual machine configuration. For additional scenarios that apply to System Center 2012 SP1 and System Center 2012 R2, see the following:

- Scenarios for creating the networking environment for hosts in this topic
- Scenarios for virtual machine networks in this topic
- Scenarios for virtual switches and switch extensions in this topic

Scenario	Key information	For more information
Connect virtual machines to a network that serves a particular function in your environment, for example, the “Backend,” “Frontend,” or “Backup” network. In other words, associate IP subnets and, if needed, virtual local area networks (VLANs) together into named units, called "logical networks," that virtual machines can use.	• Logical networks, which were introduced in System Center 2012, provide a foundation for virtual machine networks (VM networks) in System Center 2012 SP1 and System Center 2012 R2. The simplest way to use a logical network that you have created is to create a VM network that uses that logical network with **No isolation**. The VM network will function as a logical network with no isolated networks within it. For more options with VM networks, see Scenarios for virtual machine networks in this topic. • Only one VM network that is configured with **No isolation** can be assigned to each logical network.	Configuring Logical Networking in VMM Overview How to Create a Logical Network in VMM How to Create a VM Network in VMM in System Center 2012 SP1 How to Create a VM Network in VMM in System Center 2012 R2
Simplify IP address management in VMM on networks where you do not use	After you create logical networks, VM networks, or both, you can create IP	Configuring Logical Networking in VMM Overview

Scenario	Key information	For more information
Dynamic Host Configuration Protocol (DHCP).	address pools and, if needed, MAC address pools for those networks.	How to Create IP Address Pools for Logical Networks in VMM
Automatically provision load balancers in your virtualized environment.	• Either use Microsoft Network Load Balancing (NLB) or add supported hardware load balancers to VMM. • NLB is included as an available load balancer with VMM.	Configuring Load Balancing in VMM Overview
Integrate VMM in System Center 2012 R2 with an IP Address Management (IPAM) server. An IPAM server is a server that is running Windows Server 2012 R2 with the IPAM Server feature installed. When two systems are integrated, the network settings are periodically synchronized between them.	For System Center 2012 R2 only: Add the IPAM server as a network service in VMM	How to Add an IPAM Server in VMM in System Center 2012 R2

Scenarios for virtual machine networks

The following table describes ways in which you can use networking capabilities in VMM to configure networks that virtual machines use. For additional scenarios that apply to System Center 2012 SP1 and System Center 2012 R2, see the following:

- Scenarios for creating the networking environment for hosts in this topic
- Scenarios for logical networks, IP address pools, and network load balancing in this topic
- Scenarios for virtual switches and switch extensions in this topic

Important

As of System Center 2012 SP1, VM networks and other VMM networking enhancements are based on Hyper-V Network Virtualization, which was introduced in Windows Server 2012. To better understand VM networks that use network virtualization, review the illustrations and descriptions of Hyper-V Network Virtualization in Network Virtualization technical details.

Scenario	Key information	For more information
Move virtual machines and their associated networks in a single operation.	• When you configure a virtual machine or virtual machine template and you specify a VM network that uses network virtualization, the VM network moves when the virtual machine is moved. A VM network can use network virtualization only if the logical network on which it is configured allows network virtualization.	Configuring VM Networks and Gateways in VMM How to Create a VM Network in VMM in System Center 2012 SP1 How to Create a VM Network in VMM in System Center 2012 R2 How to Create a Virtual Machine Template

Connect virtual machines on VM networks to computers on connected physical networks.
In System Center 2012 R2: Connect virtual machines on VM networks to computers on connected physical networks, and optionally, use network address translation (NAT).
For a similar scenario for a hosting provider, see the last line in this table.
	• For this scenario, you configure a VM network to use a gateway. First, however, you must ensure that the provider software for the gateway has been installed on the VMM management server. Then you can add the gateway to VMM.
	• Create a VM network that uses network virtualization (on a logical network that allows this), and configure the VM network with the gateway:
	  • In System Center 2012 SP1, configure the VM network with a gateway setting of **Local networks**.
	  • In System Center 2012 R2, configure the VM network with a connectivity setting of
		Configuring VM Networks and Gateways in VMM
		
		How to Add a Gateway in VMM in System Center 2012 SP1
		
		How to Use a Server Running Windows Server 2012 R2 as a Gateway with VMM
		
		How to Add a Gateway in VMM in System Center 2012 R2

Scenario	Key information	For more information
	Connect directly to an additional logical network and optionally, select **Network address translation (NAT)**. • The gateway will act as a router to the physical network.	

Manage networks that use familiar VLAN technology for network isolation, but use VMM to simplify the management process.	• Obtain information about the isolated VLANs that have been created within the physical network. Then, in VMM, create a logical network and specify the appropriate option:
	  • In System Center 2012 SP1: In most cases, select **Network sites within this logical network are not connected** only. However, if you are using private VLAN technology, also select the option for private VLANs.
	  • With System Center 2012 R2: In most cases, select **VLAN-based independent networks**. However, if you are using private VLAN technology, select the option for private VLANs instead.
	Then follow additional steps in Configuring VM Networks and Gateways in VMM.
	• The completed configuration has one VM network for each isolated VLAN in your physical network.
		Configuring VM Networks and Gateways in VMM
		
		How to Create a Logical Network in VMM
		
		How to Create a VM Network in VMM in System Center 2012 SP1
		
		How to Create a VM Network in VMM in System Center 2012 R2

Scenario	Key information	For more information
In the hosted environment that you provide, enable each tenant, client, or customer to have their own networks that are isolated from the networks of other tenants, clients, or customers.	• Use network virtualization. To do this, create a logical network as the foundation, specify that the logical network allows for VM networks that use network virtualization, and then create multiple VM networks on top of the logical network. Provide one or more VM networks for each tenant, client, or customer.	Configuring VM Networks and Gateways in VMM How to Create a Logical Network in VMM How to Create a VM Network in VMM in System Center 2012 SP1 How to Create a VM Network in VMM in System Center 2012 R2
In the hosted environment that you provide, enable your tenants, clients, or customers to "Bring your own IP". In other words, you offer them an environment in which they can use whatever IP addresses they want for their virtual machines.	• Use network virtualization. To do this, create a logical network as the foundation, specify that the logical network allows for VM networks that use network virtualization, and then create multiple VM networks on top of the logical network. Provide one or more VM networks for each tenant, client, or customer.	Configuring VM Networks and Gateways in VMM How to Create a Logical Network in VMM How to Create a VM Network in VMM in System Center 2012 SP1 How to Create a VM Network in VMM in System Center 2012 R2
In the hosted environment that you provide, enable your tenants, clients, or customers to configure some aspects of their own networks, based on limits that you specify.	• Use network virtualization, and give each tenant access to the appropriate networks through the Tenant Administrator role in VMM. (See the previous row in this table for information about network virtualization.)	Configuring VM Networks and Gateways in VMM How to Create a VM Network in VMM in System Center 2012 SP1

Scenario	Key information	For more information
		How to Create a VM Network in VMM in System Center 2012 R2 How to Create a Tenant Administrator User Role in VMM

In the hosted environment that you provide, enable your tenants to connect their virtual machines to systems on their own premises.
In System Center 2012 R2: In the hosted environment that you provide, enable your tenants to connect their virtual machines to multiple sites on their own premises, and optionally, to use Border Gateway Protocol (BGP).
	• For this scenario, you configure a VM network to use the tenant's gateway. First, however, you must ensure that the provider software (that works with the tenant's gateway) has been installed on the VMM management server. Then you can add the gateway to VMM.
	• Create the tenant's VM network so that it uses network virtualization (on a logical network that allows this option), and configure the VM network with the gateway:
	  • In System Center 2012 SP1, configure the VM network with a gateway setting of **Remote networks**.
	  • In System Center 2012 R2, configure the VM network with a connectivity setting of **Connect to another network through a VPN tunnel**, and optionally, **Enable Border Gateway Protocol (BGP)**.
	• This configuration provides a site-to-site, virtual-private-
		Configuring VM Networks and Gateways in VMM
		How to Add a Gateway in VMM in System Center 2012 SP1
		How to Create a VM Network in VMM in System Center 2012 SP1
		How to Use a Server Running Windows Server 2012 R2 as a Gateway with VMM
		How to Add a Gateway in VMM in System Center 2012 R2
		How to Create a VM Network in VMM in System Center 2012 R2

Scenario	Key information	For more information
	network (VPN) connection from the tenant's VM network (in the hosted environment that you provide) to a VPN gateway on the tenant's premises.	

Scenarios for virtual switches and switch extensions

The following table describes ways in which you can use networking capabilities in VMM to configure virtual switches and switch extensions that define connectivity and capabilities in networks that are used by virtual machines. For additional scenarios that apply to System Center 2012 SP1 and System Center 2012 R2, see the following:

- Scenarios for creating the networking environment for hosts in this topic
- Scenarios for logical networks, IP address pools, and network load balancing in this topic
- Scenarios for virtual machine networks in this topic

Scenario	Key information	For more information
In a virtualized network environment, monitor network traffic, use Quality of Service (QoS) to control network bandwidth usage, or enhance the level of security.	• In VMM, create a logical switch and associate a virtual switch extension with it. For example, use a switch extension that supports QoS (through the switch extension provider). • Before you can associate a switch extension with a logical switch, you must install provider software on the VMM management server. Some providers are included in VMM. You can also obtain them from switch manufacturers and add them to VMM.	Configuring Ports and Switches for VM Networks in VMM
Configure settings on your forwarding extension and then apply them consistently in your virtualized environment. Settings can include network objects such as logical networks, network sites, and	• In VMM, add the switch extension manager for your forwarding extension. To do this, you must first install provider software that you obtain from the switch manufacturer.	Configuring Ports and Switches for VM Networks in VMM How to Add a Virtual Switch Extension Manager in System

Scenario	Key information	For more information
VM networks.	• Then create logical switches, which bring together multiple network settings and capabilities that you want to make available on particular hosts.	Center 2012 SP1 How to Add a Virtual Switch Extension or Network Manager in System Center 2012 R2

See Also

Common Scenarios for Networking in VMM in System Center 2012

Configuring Logical Networking in VMM Illustrated Overview

Configuring Ports and Switches in VMM Illustrated Overview

Configuring VM Networks in VMM Illustrated Overview

Configuring Logical Networking in VMM Overview

With Virtual Machine Manager (VMM) in System Center 2012, System Center 2012 Service Pack 1 (SP1), or System Center 2012 R2, you can easily connect virtual machines to a network that serves a particular function in your environment, for example, the “Backend,” “Frontend,” or “Backup” network. To do this, you associate IP subnets and, if needed, virtual local area networks (VLANs) together into named units called logical networks. You can design your logical networks to fit your environment. Logical networks are an enhancement in System Center 2012 and continue as part of networking in System Center 2012 SP1 and System Center 2012 R2.

This overview provides more information about the following:

- Logical networks and the Network sites that you can create within logical networks
- Static IP address pools and MAC address pools

  If you want to configure multicasting or broadcasting in your networks, see Creating an IP address pool to support multicasting or broadcasting in this topic.
- IPAM server integration with VMM in System Center 2012 R2

Note

The procedures that this overview links to include examples that help demonstrate the concepts. For a summary of the networking examples, see the “Networking” section of the table in Preparing the Fabric Scenario in VMM. The examples are not meant to be prescriptive guidance for a lab setup. You should adapt the examples to your test environment.

Logical networks, as described in this topic, work together with the network enhancements that are described in these other overview topics:

- Common Scenarios for Networking in VMM in System Center 2012

  Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2

- Configuring Load Balancing in VMM Overview: By adding a load balancer, you can load balance requests to the virtual machines that make up a service tier.
- Configuring Ports and Switches for VM Networks in VMM (for System Center 2012 SP1 and System Center 2012 R2): Port profiles and logical switches act as containers for the properties or capabilities that you want your network adapters to have. Rather than configuring each network adapter with these properties or capabilities, you specify the capabilities in port profiles and logical switches, which you can then apply to the appropriate adapters.
- Configuring VM Networks and Gateways in VMM (for System Center 2012 SP1 and System Center 2012 R2): By configuring virtual machine networks (VM networks) on top of your logical networks, you can make use of network virtualization or other network configuration options. Gateways can increase possibilities for connectivity.

  For illustrations of the ways that VM networks can be configured in relation to logical networks, see Configuring VM Networks in VMM Illustrated Overview.

Logical networks

A logical network, together with one or more associated network sites, is a user-defined named grouping of IP subnets, VLANs, or IP subnet/VLAN pairs that is used to organize and simplify network assignments. Some possible examples include “BACKEND,” “FRONTEND,” “LAB,” “MANAGEMENT,” and “BACKUP.” Because logical networks represent an abstraction of the underlying physical network infrastructure, they enable you to model the network based on business needs and connectivity properties.

For illustrations of logical networks, see Configuring Logical Networking in VMM Illustrated Overview.

After you have created a logical network, you can use it to specify the network on which to deploy a host or a virtual machine (stand-alone or part of a service). Users can assign logical networks as part of virtual machine and service creation without having to understand the network details.

You can use logical networks to describe networks with different purposes, to create traffic isolation, and to provision networks for different types of service-level agreements (SLAs). For example, for a tiered application, you can group IP subnets and VLANs that are used for the front-end web tier as the FRONTEND logical network. You can group IP subnets and VLANs that are used for backend servers (such as application and database servers) as BACKEND. When self-service users model the tiered application as a service, they can easily pick the logical network that virtual machines in each tier of the service should connect to.

At least one logical network must exist for you to deploy virtual machines and services. By default, when you add a Hyper-V host to VMM management, VMM automatically creates logical networks that match the first DNS suffix label of the connection-specific DNS suffix on each host network adapter. For more information, see Assigning logical networks to hosts in this topic.

When you create a logical network, you can do the following:

- Create associated network sites, typically for each physical location. For each network site, you can associate IP subnets and VLANs.

  Note

Network sites are sometimes referred to as logical network definitions, for example, in the VMM command shell.

- Create IP address pools to enable VMM to automatically assign static IP addresses. You can create the pools from an IP subnet that you have associated with the network site.

Network sites and static IP address pools are more fully described in the following sections.

Note

For information about how to create a logical network, see How to Create a Logical Network in VMM.

Network sites

When you create a logical network, you can create one or more associated network sites. A network site associates one or more subnets, VLANs, and subnet/VLAN pairs with a logical network. It also enables you to define the host groups to which the network site is available. For example, if you have a Seattle host group and a New York host group, and you want to make the BACKEND logical network available to each, you can create two network sites for the BACKEND logical network. You can scope one network site to the Seattle host group (and any desired child host groups), and you can scope the other network site to the New York host group (and any desired child host groups), adding the appropriate subnets and VLANs for each location. For illustrations showing how a network site is part of a logical network, see Configuring Logical Networking in VMM Illustrated Overview. For information about how to create a network site, see How to Create a Logical Network in VMM.

The following table shows an example of the BACKEND logical network, which is made up of subnets and VLANs from both Seattle and New York.

Logical network	Network sites
BACKEND	**BACKEND – Seattle** • Scoped to the Seattle host group • Associated subnet and VLAN: 10.0.0.0/24 VLAN 7 **BACKEND – New York** • Scoped to the New York host group • Associated subnet and VLAN: 172.16.0.0/24 VLAN 12

Before you create network sites, review the following guidelines.

- If you are running System Center 2012 SP1 or System Center 2012 R2, and your network configuration will include VM networks that use network virtualization, create at least one network site and associate at least one IP subnet with the site. You can also assign a VLAN to the network site, as appropriate. Creating a network site with an IP subnet makes it possible to create an IP address pool for the logical network, which is necessary for network virtualization.

If your network configuration will not include VM networks that use network virtualization, use the other guidelines in this list, which are the same for System Center 2012, System Center 2012 SP1, and System Center 2012 R2.

- If you plan to use a load balancer that is managed by VMM to load-balance a service tier, create at least one network site and associate at least one IP subnet with the network site.
- If you want to create static IP address pools that VMM manages, create at least one network site and associate at least one IP subnet with the network site.
- If you want to use Dynamic Host Configuration Protocol (DHCP) that is already available on the network to assign IP addresses to virtual devices in a specified VLAN, create network sites with only VLANs assigned to them.
- If you want to use DHCP that is already available on the network, and you are not using VLANs, you do not have to create any network sites.

Note

For information about how to create a network site, see How to Create a Logical Network in VMM.

Static IP address pools

This section describes static IP address pools in general, and then provides information about whether to create them. Also, for System Center 2012 SP1 and System Center 2012 R2, it explains whether to create IP address pools for a logical network only or also for VM networks that are configured on that logical network. (In System Center 2012, the only type of network is a logical network and therefore when an IP address pool is created, it is always created for a logical network.)

If you associate one or more IP subnets with a network site, you can create static IP address pools from those subnets. Static IP address pools make it possible for VMM to automatically allocate static IP addresses to Windows-based virtual machines that are running on any managed Hyper-V, VMware ESX or Citrix XenServer host. VMM can automatically assign static IP addresses from the pool to stand-alone virtual machines, to virtual machines that are deployed as part of a service, and to physical computers when you use VMM to deploy them as Hyper-V hosts. Additionally, when you create a static IP address pool, you can define a reserved range of IP addresses that can be assigned to load balancers as virtual IP (VIP) addresses. VMM automatically assigns a virtual IP address to a load balancer during the deployment of a load-balanced service tier.

When you create a static IP address pool, you can configure associated information, such as default gateways, Domain Name System (DNS) servers, DNS suffixes, and Windows Internet Name Service (WINS) servers. All of these settings are optional.

IP address pools support both IPv4 and IPv6 addresses. However, you cannot mix IPv4 and IPv6 addresses in the same IP address pool.

As of System Center 2012 R2, after a virtual machine has been deployed in VMM, you can view the IP address or addresses assigned to that virtual machine. To do this, right-click the listing for the virtual machine, click **Properties**, click the **Hardware Configuration** tab, click the network adapter, and in the results pane, click the **Connection details** button.

For information about how to create static IP address pools for logical networks in System Center 2012, System Center 2012 SP1, or System Center 2012 R2, see How to Create IP Address Pools for Logical Networks in VMM. For information about how to create IP address pools for VM networks, see How to Create IP Address Pools for VM Networks in VMM.

Guideline for creating IP address pools with System Center 2012

With VMM in System Center 2012, configuring static IP address pools is optional. You can also assign addresses automatically through DHCP if it is available on the network. If you use DHCP, you do not have to create IP address pools.

Important

If you configure a virtual machine to obtain its IP address from a static IP address pool, you must also configure the virtual machine to use a static media access control (MAC) address. You can either specify the MAC address manually (during the **Configure Settings** step) or have VMM automatically assign a MAC address from the MAC address pool.

When a static IP address is assigned, VMM must determine the MAC address before the virtual machine starts. VMM uses the MAC address to identify which network adapter to set the static IP address to. This is especially important if there is more than one network adapter on the virtual machine. If the MAC address is assigned dynamically through Hyper-V, VMM cannot identify which network adapter to set the static IP address to if there is more than one network adapter.

Guidelines for creating IP address pools with System Center 2012 SP1 or System Center 2012 R2

With VMM in System Center 2012 SP1 or System Center 2012 R2, use the following guidelines to decide whether to create IP address pools and, if so, whether to create them for a logical network only or also for VM networks that are configured on that logical network. The process of creating an IP address pool for a VM network is similar to the process of creating an IP address pool for a logical network.

Important

If you configure a virtual machine to obtain its IP address from a static IP address pool, you must also configure the virtual machine to use a static MAC address. You can either specify the MAC address manually (during the **Configure Settings** step) or have VMM automatically assign a MAC address from the MAC address pool.

When a static IP address is assigned, VMM must determine the MAC address before the virtual machine starts. VMM uses the MAC address to identify which network adapter to set the static IP address to. This is especially important if there is more than one network adapter on the virtual machine. If the MAC address is assigned dynamically through Hyper-V, VMM cannot identify which network adapter to set the static IP address to if there is more than one network adapter.

The following list provides guidelines for creating IP address pools, based on the type of network configuration you are using. For descriptions of the network configurations in the list, see Configuring VM Networks and Gateways in VMM.

- **Network virtualization**: If your network configuration includes VM networks that use network virtualization, you must create IP address pools on both the logical network that provides the foundation for those VM networks, and on the VM networks themselves. If the virtual machines on the VM networks are configured to use DHCP, VMM will respond to the DHCP request with an address from an IP address pool.
- **VLAN-based configuration**: If you are using a VLAN-based network configuration, you can use either DHCP, if it is available, or IP address pools. To use IP address pools, create them on the logical network. They will automatically become available on the VM network.
- **VM network that gives direct access to the logical network ("no isolation")**: If you have a VM network that gives direct access to the underlying logical network, you can use either DHCP, if it is available, or IP address pools for that network. To use IP address pools, create them on the logical network. They will automatically become available on the VM network.
- **External networks that are implemented through a vendor network-management console**: If you are using external networks that are implemented through a vendor network-management console (in other words, if you will use a virtual switch extension manager), your IP address pools will be imported from the vendor network-management database. Therefore, do not create IP address pools in VMM. (A vendor network-management console is also known as a management console for a forwarding extension.)

Note

As of System Center 2012 R2, after a virtual machine has been deployed in VMM, you can view the IP address or addresses assigned to that virtual machine. To do this, right-click the listing for the virtual machine, click **Properties**, click the **Hardware Configuration** tab, click the network adapter, and in the results pane, click the **Connection details** button.

Creating an IP address pool to support multicasting or broadcasting

With VMM in System Center 2012 SP1 or System Center 2012 R2, if you are using network virtualization on your VM networks, you can support an application that requires multicasting or broadcasting on the VM networks. To do this, you must create an IP address pool that supports multicasting, and you must follow several other configuration requirements. (For information about what it means to use network virtualization on a VM network, see Configuring VM Networks and Gateways in VMM.) The requirements for using multicasting or broadcasting on a VM network are as follows:

- The logical network that you create must have network virtualization enabled.
- You must configure an IP address pool on the logical network and select the multicast setting for the pool.

  Note that in the Create Static IP Address Pool Wizard, the multicast setting is visible only if the pool is created on a logical network (not on a VM network) and if network virtualization is enabled on that logical network.

- For the VM network in which you want to support multicasting, the IP protocol setting (either IPv4 or IPv6) must match the IP protocol setting for the underlying logical network. To configure this, in the Create VM Network Wizard, on the **Isolation** page of the wizard, select the same IP address protocol (IPv4 or IPv6) for both the logical network and the VM network.

  Note that after you finish creating the VM network, you cannot view this protocol setting in the VMM management console. Instead, run the Windows PowerShell cmdlet Get-SCVMNetwork to view the setting. Use the following syntax, where `<VMNetworkName>` is the name of your VM network:

  ```
  Get-SCVMNetwork –Name <VMNetworkName> | Format-List Name, IsolationType, *PoolType
  ```

  In the display, a protocol (IPv4 or IPv6) is listed for **PAIPAddressPoolType** and **CAIPAddressPoolType**. **PAIPAddressPoolType** (which begins with “PA”) refers to provider addressing, that is, IP addresses in the logical network. Similarly, **CAIPAddressPoolType** (which begins with “CA”) refers to customer addressing, that is, IP addresses in the VM network.

When these configuration steps are complete, multicast and broadcast packets on the VM network will use the IP addresses from the multicast IP address pool. Within each VM network, each subnet that you configure will consume one IP address from the multicast pool.

Assigning logical networks to hosts

To make a logical network available to a host, you must associate the logical network with a physical network adapter on the host, and make it available through an external virtual network (which is also known as an external virtual switch or vSwitch). You create this association for each network adapter.

To help ensure that you can create and deploy virtual machines on your existing network, VMM uses default settings to create the necessary logical networks (or other network objects) for a Hyper-V host that is being added to VMM management or for a virtual machine that VMM is connecting to. The following list provides details about these default settings:

- **For VMM in System Center 2012:** By default, when you add a Hyper-V host to VMM management, if a physical network adapter on the host does not have an associated logical network, VMM automatically creates and associates a logical network that matches the first DNS suffix label of the connection-specific DNS suffix. For example, if the DNS suffix for the host network adapter is corp.contoso.com, VMM creates a logical network that is named “corp.” If a virtual network is not associated with the network adapter, when VMM connects a virtual machine to a logical network that is associated with the physical network adapter, VMM also creates an external virtual network and associates it with the logical network.

  Note

  No network sites are created automatically.

- **For VMM in System Center 2012 SP1 or System Center 2012 R2:** By default, when you add a Hyper-V host to VMM management, if a physical network adapter on the host does not have an associated logical network, VMM automatically creates and associates a logical network that matches the first DNS suffix label of the connection-specific DNS suffix. On the logical network, VMM also creates a VM network that is configured with “no isolation.” For example, if the DNS suffix for the host network adapter is corp.contoso.com, if necessary

VMM creates a logical network that is named “corp,” and on it, a VM network named “corp” that is configured with no isolation.

Note

No network sites are created automatically.

The default logical network name creation and virtual network creation settings are customizable. For more information, including which settings apply to VMware ESX hosts and Citrix XenServer hosts, see How to Configure Global Network Settings in VMM.

Tip

In VMM in System Center 2012 SP1 and System Center 2012 R2, port profiles and logical switches are new options that are available for network configurations. By using port profiles and logical switches, you can consistently configure identical capabilities for network adapters across multiple hosts. Rather than configuring each network adapter with specific properties or capabilities, you can specify the capabilities in port profiles and logical switches, which you can then apply to the appropriate network adapters. For more information, see Configuring Ports and Switches for VM Networks in VMM.

For information about how to configure host network settings, see the following topics:

- How to Configure Network Settings on a Hyper-V Host in VMM
- How to Configure Network Settings on a Host by Applying a Logical Switch in VMM
- How to Configure Network Settings on a VMware ESX Host
- How to Configure Network Settings on a Citrix XenServer Host

MAC address pools

VMM can automatically assign static MAC addresses to new virtual network devices on Windows-based virtual machines that are running on any managed Hyper-V, VMware ESX, or Citrix XenServer host. VMM has two default static MAC address pools: the default MAC address pool (for Hyper-V and Citrix XenServer), and the default VMware MAC address pool (for VMware ESX hosts). The default static MAC address pools are used only if you set the MAC address type for a virtual machine to “Static”. If the virtual machine setting is “Dynamic”, the hypervisor assigns the MAC address. You can either use the default MAC address pools or configure custom MAC address pools that are scoped to specific host groups.

Note

For information about how to create static MAC address pools, see How to Create Custom MAC Address Pools in VMM.

IPAM server integration with VMM in System Center 2012 R2

With System Center 2012 R2, you can add an IP Address Management (IPAM) server that runs Windows Server® 2012 R2 to the resources in VMM. When VMM and IPAM are integrated in this way, the settings in VMM will be kept in synchrony with settings stored in the IPAM server. For more information, see How to Add an IPAM Server in VMM in System Center 2012 R2.

In this section

To learn about ways that you can use logical networking, and to see illustrations of logical networks, see the following topics:

- Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2
- Configuring Logical Networking in VMM Illustrated Overview

To configure logical networking, complete the procedures in the following table.

Procedure	Description
How to Configure Global Network Settings in VMM	Describes how to configure default VMM settings for automatic logical network and virtual network creation.
How to Create a Logical Network in VMM	Describes how to create a logical network, including how to create network sites and assign IP subnets and VLANs.
How to Modify or Delete a Logical Network in VMM	Describes how to modify or delete a logical network, including associated network sites and IP address pools.
How to Create IP Address Pools for Logical Networks in VMM	Describes how to create static IP address pools for logical networks. These IP address pools are made available to hosts, virtual machines, and services.
How to Create Custom MAC Address Pools in VMM	Describes how to create custom MAC address pools so that they are available for assignment to virtual machines.
How to Release Inactive IP or MAC Addresses in VMM	Describes how to return inactive addresses to the IP address or MAC address pools to make them available for reassignment.
How to Add an IPAM Server in VMM in System Center 2012 R2	Describes how to add an IP Address Management (IPAM) server that runs Windows Server 2012 R2 to the resources in VMM so that you can use the IPAM server in a coordinated way with VMM.

Next steps after configuring logical networking

For information about the next steps to take after configuring logical networking, see the networking overviews in the following table.

Topic	Step
Configuring Load Balancing in VMM Overview	If necessary, configure load balancers in your

Topic	Step
	virtualized environment.
Configuring Ports and Switches for VM Networks in VMM (for System Center 2012 SP1 and System Center 2012 R2)	Configure port profiles and port classifications, and use them in logical switches, so that you can apply your port settings consistently to your network adapters and virtual network adapters. After you configure port settings, configure logical switches and, as necessary, switch extensions (for Quality of Service (QoS), monitoring, or security).
Configuring VM Networks and Gateways in VMM (for System Center 2012 SP1 and System Center 2012 R2)	Configure VM networks (on top of logical networks), which make it possible for you to use network virtualization or other networking options. With VM networks that use network virtualization, you can also use gateways to increase connectivity.

Next steps after completing the network configuration

For information about the next steps to take after you have completed your network configuration, see the topics in the following table.

Topic	Step
Preparing the Fabric in VMM	Configure additional fabric resources, such as storage and library resources.
Adding and Managing Hyper-V Hosts and Scale-Out File Servers in VMM Managing VMware ESX and Citrix XenServer in VMM	Configure hosts.
Creating and Deploying Virtual Machines and Services in VMM	Deploy virtual machines, either individually or as part of a service.

See Also

Configuring Networking in VMM

Configuring Logical Networking in VMM Illustrated Overview

Configuring Ports and Switches in VMM Illustrated Overview

Configuring VM Networks in VMM Illustrated Overview

Configuring Logical Networking in VMM Illustrated Overview

This overview illustrates logical networks, which are part of Virtual Machine Manager (VMM) in System Center 2012, System Center 2012 Service Pack 1 (SP1), and System Center 2012 R2. Logical networks are named networks that serve particular functions in your environment, for example, the "Backend," "Frontend," or "Backup" network.

For illustrations that are based on VMM in System Center 2012 SP1 or System Center 2012 R2 that show the relationship between logical networks and virtual machine networks (VM networks), see Configuring VM Networks in VMM Illustrated Overview.

For more information about logical networks, see Configuring Logical Networking in VMM Overview and How to Create a Logical Network in VMM.

Logical networks in VMM

The following illustration shows a logical network in VMM in System Center 2012, System Center 2012 SP1, or System Center 2012 R2. For some networking elements, fictitious names such as "Contoso1" are included to help illustrate the purpose of those elements.

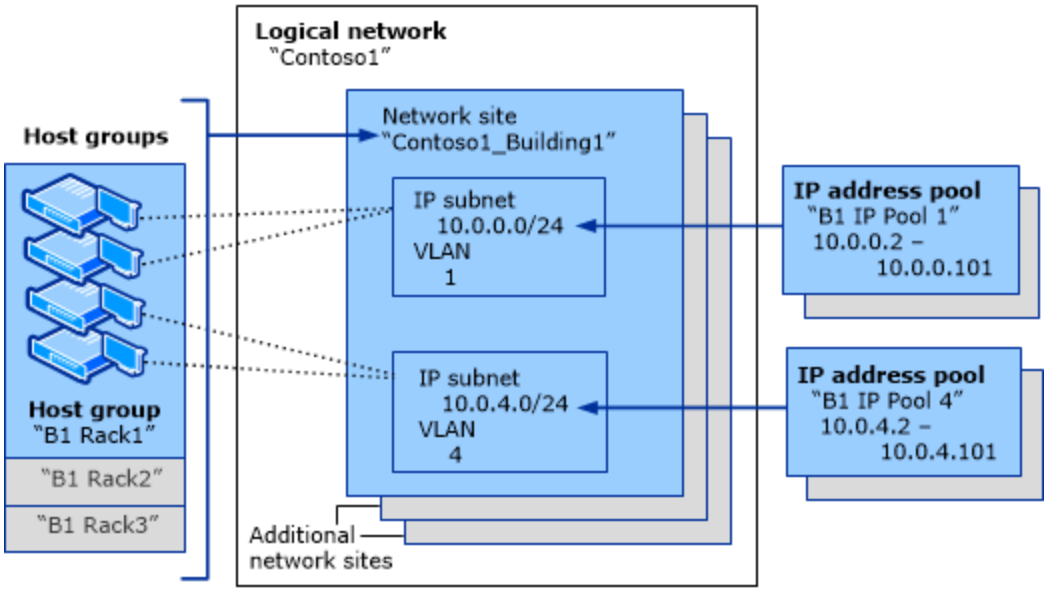


Figure 1 Logical network

This illustration shows how a logical network in VMM is a container for network sites, also called logical network definitions, and for IP subnet information, virtual local area network (VLAN) information, or both. It also shows how host groups in VMM can be associated with a network site and how IP address pools can be assigned to subnets within the logical network.

In the preceding illustration, the names of elements that you configure by running a wizard or by opening a property sheet are shown in bold text, while elements that are on a page of the wizard or on a tab of the property sheet are shown without bold text.

Network object model for logical networks

The following illustration shows the network object model for logical networks in VMM in System Center 2012, System Center 2012 SP1, and System Center 2012 R2. The illustration shows the relationships among network objects only, and does not provide information about the wizards

and property sheets through which the objects are configured in the VMM console. The illustration can be especially useful if you are learning about configuring VMM through Windows PowerShell scripts, which reflect the network object models directly.

For some objects, sample names such as "Contoso1" and "Building1" are included to help illustrate the purpose of those objects. The object that is labeled "Network site" is also known as a "logical network definition."

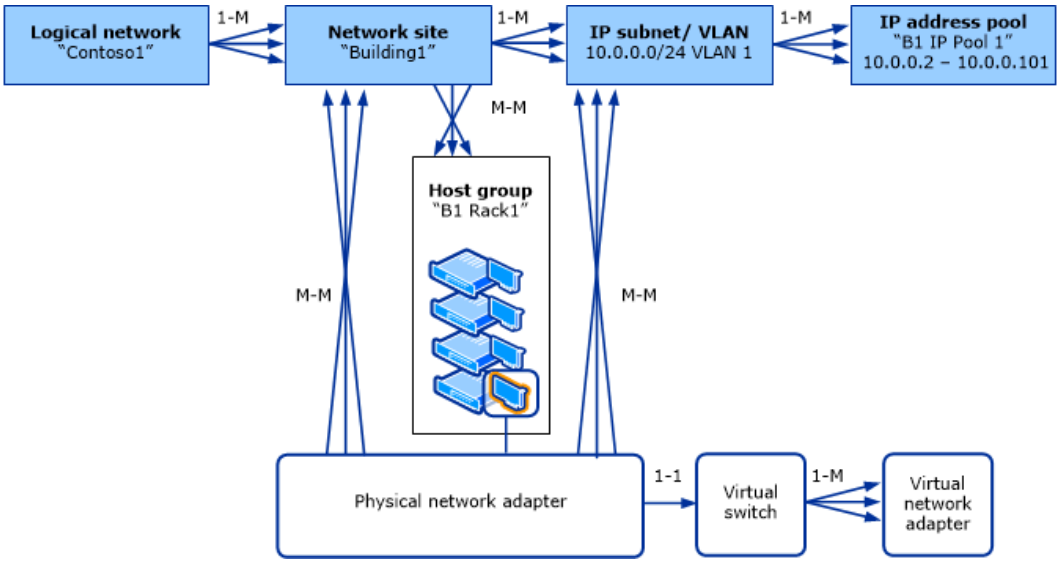


Figure 2 Object model for logical networks

The following key explains the notations on the arrows:

- **1-1** means "one to one."
- **1-M** means "one to many."
- **M-M** means "many to many."

In the preceding illustration, bold text is used for each VMM object name, regardless of how that object is configured through the VMM console.

See Also

How to Create a Logical Network in VMM

Configuring Logical Networking in VMM Overview

Configuring VM Networks in VMM Illustrated Overview

Configuring Ports and Switches in VMM Illustrated Overview

Common Scenarios for Networking in VMM in System Center 2012

Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2

How to Configure Global Network Settings in VMM

You can use the following procedure to configure global networking settings in Virtual Machine Manager (VMM). With these optional settings, you can configure the automatic creation of logical

networks, the automatic association of a host's physical network adapter with a logical network, and the automatic creation of external virtual networks on host network adapters.

The labels in the dialog box described in this procedure vary slightly among System Center 2012, System Center 2012 Service Pack 1 (SP1), and System Center 2012 R2. These differences are noted in the table that follows.

Note
This procedure is optional. Change these settings only if you want to modify the default behavior. For more information about the default behavior, see "Assigning logical networks to hosts" in Configuring Logical Networking in VMM Overview.

Account requirements To complete this procedure, you must be a member of the Administrator user role.

How to configure global networking settings

1. Open the **Settings** workspace.
2. In the **Settings** pane, click **General**.
3. In the results pane, double-click **Network Settings**.
4. Configure any of the following settings:

Area	Settings
Logical network matching	You can configure how VMM determines the logical network name to use when the automatic creation of logical networks is enabled. The following options are available. **Note** This setting is only applied when you add a host to VMM management and there is no logical network associated with a physical network adapter on the host. Changes to this setting do not affect hosts that are already under management. Also, for VMware ESX and Citrix XenServer hosts, the options of **First DNS Suffix Label** and **DNS Suffix** are not supported. Therefore, by default, ESX and XenServer

	hosts use the **Virtual Network Switch Name** option. • **First DNS Suffix Label** (the default) The first suffix label of the connection-specific DNS suffix. For example, if the DNS suffix is corp.contoso.com, VMM creates a logical network that is named “corp”. • **DNS Suffix** The full connection-specific DNS suffix. For example, if the DNS suffix is corp.contoso.com, VMM creates a logical network that is named “corp.contoso.com”. • **Network Connection Name** The network connection name. For example, if the network connection is named Local Area Connection 2, VMM creates a logical network that is named “Local Area Connection 2”. • **Virtual Network Switch Name** The name of the virtual network switch to which the physical network adapter of the host is bound. • **Disabled** You can also specify the option to use if the first logical network matching selection fails. You can select one of the following options: • **Virtual Network Switch Name** (default) • **Network Connection Name** • **Disabled**
Automatic creation of logical networks	By default, the **Create logical networks automatically** setting is enabled. If there is no logical network associated with a physical network adapter on the host, VMM automatically creates and associates a

	logical network based on the logical network matching selection. By default, this is the first DNS suffix label of the connection-specific DNS suffix. In System Center 2012 SP1 and System Center 2012 R2, on the logical network, VMM also creates a VM network configured with “no isolation.” **Note** This setting is only applied when you add a host to VMM management and there is no logical network associated with a physical network adapter on the host. Changes to this setting do not affect hosts that are already under management.
In System Center 2012: **Automatic creation of virtual networks**	In System Center 2012, by default, the **Create virtual networks automatically** setting is enabled. If the host has a physical network adapter with an associated logical network, but no virtual networks attached, VMM automatically creates an external virtual network when VMM connects a virtual machine to a logical network that is associated with the physical network adapter. For example, VMM creates an external virtual network automatically when you create a virtual machine, migrate a virtual machine, or modify a virtual machine that uses the logical network that is associated with the physical network adapter. **Note** This setting only applies to Hyper-V hosts.
In System Center 2012 SP1: **Automatic creation of virtual switches**	In System Center 2012 SP1, there is a setting labeled **Create virtual switches automatically**. However, selecting or clearing this check box has no effect. Virtual switches are not created automatically by

	VMM in System Center 2012 SP1.

See Also

Configuring Networking in VMM

Configuring Logical Networking in VMM Overview

Configuring Ports and Switches for VM Networks in VMM

Configuring VM Networks and Gateways in VMM

How to Create a Logical Network in VMM

With Virtual Machine Manager (VMM) in System Center 2012, System Center 2012 Service Pack 1 (SP1), or System Center 2012 R2, you can easily connect virtual machines to a network that serves a particular function in your environment, for example, the “Backend,” “Frontend,” or “Backup” network.

To do this, you associate IP subnets and, if needed, virtual local area networks (VLANs) together into named units called logical networks. You can design your logical networks to fit your environment.

For more information about logical networks and how they work with other network configuration options in VMM, see Configuring Logical Networking in VMM Overview.

Important
VMM does not automatically create port groups on VMware ESX hosts. Therefore, in order for logical networks to work correctly for managed ESX hosts, you must use VMware vCenter Server to configure port groups with the necessary VLANs that correspond to the network sites.

Account requirements To complete this procedure, you must be a member of the Administrator or the Delegated Administrator user role. Delegated administrators can only associate a logical network to host groups that are included in their administrative scope.

To create a logical network

1. Open the **Fabric** workspace.
2. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
3. In the **Fabric** pane, expand **Networking**, and then click **Logical Networks**.
4. On the **Home** tab, in the **Create** group, click **Create Logical Network**.

   The **Create Logical Network Wizard** opens.
5. On the **Name** page, do the following:
   a. Enter a name and optional description for the logical network.

      For example, enter the name **BACKEND**, with the description **Corporate network. Use for internal servers such as application and database servers**.
   b. If you have System Center 2012 SP1 or System Center 2012 R2, select check boxes as appropriate by using the table that follows. Otherwise, skip to the next numbered step in this procedure.

Select one or more check boxes based on how you intend to use the VM networks that will be configured on top of this logical network. The following table provides guidelines. For additional descriptions of the ways in which you can use VM networks, see Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2 and Configuring VM Networks and Gateways in VMM.

Use of the VM network or networks that will be created on top of this logical network	Action in System Center 2012 SP1	Action in System Center 2012 R2
Hyper-V network virtualization: multiple VM networks with isolation	Select **Allow new VM networks created on this logical network to use network virtualization**.	Select **One connected network** and then select **Allow new VM networks created on this logical network to use network virtualization**.
VLAN-based configuration: manage VLANs that have been created for network isolation within the physical network	Select **Network sites within this logical network are not connected**. If you are using private VLAN technology, also select **Network sites within this logical network contain private VLANs**. (Otherwise, do not select it.) For information about additional steps for this configuration, see “VLAN-based configuration” in the list in Configuring VM Networks and Gateways in VMM.	In most cases, select **VLAN-based independent networks**. However, if you are using private VLAN technology, select **Private VLAN (PVLAN) networks**. For information about additional steps for this configuration, see “VLAN-based configuration” in the list in Configuring VM Networks and Gateways in VMM.
One VM network that gives direct access to the logical network: no isolation	If this logical network will support network virtualization (in addition to having a VM network that gives direct access to the logical network), select the check box to	Select **One connected network** and select **Create a VM network with the same name to allow virtual machines to access this logical network directly**. If this

	allow network virtualization. If this logical network will not use network virtualization at all, leave all check boxes cleared.	logical network will also support network virtualization, select the check box to allow network virtualization. If you select **One connected network** but you do not create the VM network now, you will still be able to create the VM network later.
External networks: use VMM in coordination with a virtual switch extension, network manager, or vendor network-management console	Do not create the logical network manually from within VMM. Instead, follow the steps in How to Add a Virtual Switch Extension Manager in System Center 2012 SP1. The logical network settings will be imported from the database in the vendor network-management console (also known as the management console for a forwarding extension).	Follow the steps in How to Add a Virtual Switch Extension or Network Manager in System Center 2012 R2, and be sure to review the capabilities of your virtual switch extension or network manager. You might be able to configure your logical networks in VMM and then export the settings to the virtual switch extension or network manager. In any case, after you add a virtual switch extension or network manager, logical network settings configured in it will be imported into VMM.

6. Click **Next**.
7. On the **Network Site** page, take the following steps.

   Note
   For guidelines for configuring network sites, see “Network sites” in Configuring Logical Networking in VMM Overview. If you do not need to configure network sites, on the **Network Site** page, click **Next**, and then click **Finish** to complete the wizard.

   a. To create a network site, click **Add**.

VMM automatically generates a site name that consists of the logical network name, followed by an underscore and a number.

b. Review the network site name and ensure that it is no longer than 64 characters. To change the default name, in the **Network site name** box, enter a new name for the network site.

   For example, enter the name **BACKEND - Seattle**.

c. Under **Host groups that can use this network site**, select the check box next to each host group to which you want to make the logical network available.

   For example, to make the BACKEND logical network available to the Seattle host group and all its child host groups, select the check box next to **Seattle**.

d. Under **Associated VLANs and IP subnets**, enter the VLANs and IP subnets that you want to assign to the network site. To enter VLAN and IP subnet information, click **Insert row**, click the field under **VLAN** or **IP subnet**, depending on what you want to configure, and then enter a VLAN, an IP subnet, or a subnet/VLAN pair. You can insert multiple rows.

   If you have System Center 2012 SP1 or System Center 2012 R2 and you previously selected the option for private VLANs, also enter the **SecondaryVLAN** for each VLAN that you enter.

   For guidelines for configuring network sites, see “Network sites” in Configuring Logical Networking in VMM Overview.

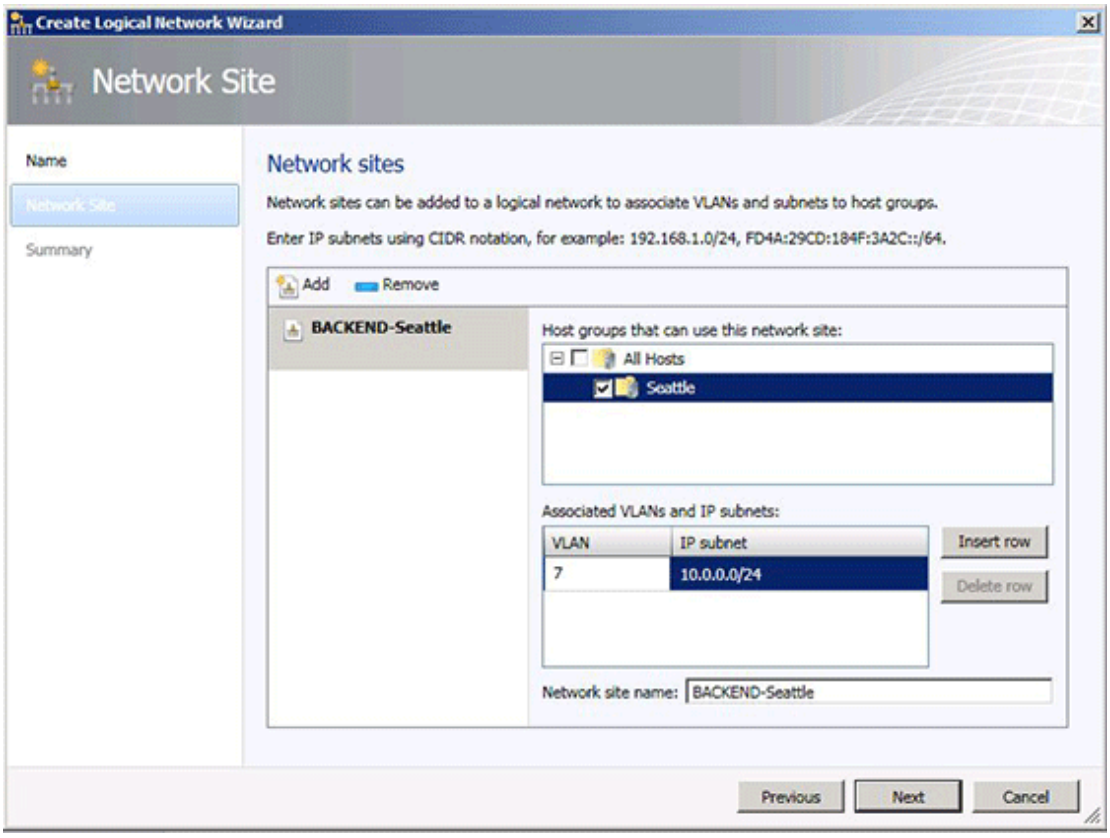
   Note
   By default, if you leave the VLAN field empty, VMM assigns a VLAN of 0. This indicates to VMM not to use VLANs. In trunk mode, VLAN 0 indicates native VLAN.

   For example, add the IP subnet/VLAN pair that makes up the example BACKEND network in Seattle, as shown in the following table.

VLAN	IP subnet
7	**10.0.0.0/24**

   Important
   In your test environment, make sure that you use VLANs and IP subnets that are available in your network.

Example of typical network site configuration



e. Optionally, create additional network sites by clicking **Add** and repeating the process.

For example, create a network site for the BACKEND logical network that is named **BACKEND – New York**, and assign it to the **New York** host group. Add the example IP subnet/VLAN pair that makes up the BACKEND network in New York.

IP subnet	VLAN
172.16.0.0/24	**12**

Note

Throughout the example scenarios, the BACKEND logical network is used as an example. Therefore, example IP subnets and VLANs are provided only for the BACKEND logical network.

f. When you complete this step, click **Next**.

8. On the **Summary** page, review the settings, and then click **Finish**.

The **Jobs** dialog box appears. Make sure the job has a status of **Completed**, and then close the dialog box.

9. Verify that the logical network appears in the **Logical Networks and IP Pools** pane. Also, if you added network sites, right-click the logical network, click **Properties**, click the

Network Site tab, and verify that the intended network sites appear on the tab.

See Also

Configuring Logical Networking in VMM Overview

Configuring VM Networks and Gateways in VMM

Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2

Configuring Logical Networking in VMM Illustrated Overview

Configuring VM Networks in VMM Illustrated Overview

Configuring Networking in VMM

How to Configure Network Settings on a Hyper-V Host in VMM

How to Modify or Delete a Logical Network in VMM

You can use the following procedures to modify or delete a logical network in Virtual Machine Manager (VMM). For example, you may want to add or remove an associated network site, or modify an IP address pool.

Account requirements To complete this procedure, you must be a member of the Administrator or the Delegated Administrator user role.

To modify a logical network

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Networking**, and then click **Logical Networks**.
3. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
4. In the **Logical Networks and IP Pools** pane, do either of the following:
   a. To modify the logical network name or associated network sites, click the logical network that you want to modify. On the **Home** tab, in the **Properties** group, click **Properties**.

      On the **Name** tab, you can modify the name and the description, and if you are running System Center 2012 SP1 or System Center 2012 R2, the options. To modify the network sites, click the **Network Site** tab. To modify a network site, click the network site that you want to modify, and then change any associated settings. You can also add and remove network sites.

      Note
      You cannot remove a network site if it has a dependent resource, for example an associated static IP address pool.

   b. To modify an associated IP address pool, in the **Logical Networks and IP Pools** pane, expand the logical network, and then click the IP address pool. On the **Home** tab, in the **Properties** group, click **Properties**.

      You can modify the name, description, the IP address range, virtual IP (VIP) address reservations, the default gateway, Domain Name System (DNS) information, and Windows Internet Name Service (WINS) information. On the **Inactive addresses** tab, you can also release inactive IP addresses back to the static IP address pool.

Note

You can view but cannot modify network site information from the IP address pool properties. To modify network site information, open the properties of the logical network.

To delete a logical network

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Networking**, and then click **Logical Networks**.
3. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
4. In the **Logical Networks and IP Pools** pane, click the logical network that you want to delete.
5. On the **Home** tab, in the **Dependencies** group, click **View Dependent Resources**.

   The **Show Dependencies** dialog box lists any items that depend on the logical network. The list can include objects such as network sites (listed under **Type** as logical network definitions), load balancers, IP address pools, hosts, virtual machines, services, and templates. Before you can delete the logical network, you must modify or delete the dependent items so that they do not reference the logical network.
6. After you modify or remove all dependencies, with the logical network selected, on the **Home** tab, in the **Remove** group, click **Remove**.
7. In response to the confirmation message, click **Yes** to remove the logical network.

See Also

Configuring Logical Networking in VMM Overview

Configuring Networking in VMM

How to Create a Logical Network in VMM

How to Create IP Address Pools for Logical Networks in VMM

You can use the following procedure to create a static IP address pool for a logical network in Virtual Machine Manager (VMM). With static IP address pools, IP address management for the virtual environment is brought within the scope of the VMM administrator.

Important

For guidelines about when IP pools are necessary on a logical network, when they are optional, and for System Center 2012 Service Pack 1 (SP1) or System Center 2012 R2, when to create an IP pool in a VM network in addition to an IP pool in the logical network, see “Static IP Address Pools” in Configuring Logical Networking in VMM Overview.

Account requirements To complete this procedure, you must be a member of the Administrator or Delegated Administrator user role.

Prerequisites

Before you begin this procedure, make sure that a logical network exists, ideally with one or more associated network sites (which are part of the logical network). The network sites must have at least one IP subnet or IP subnet/VLAN pair assigned. For more information about creating a

network site, see How to Create a Logical Network in VMM. If you do not already have network sites defined, you can create a network site when you create the static IP address pool.

To create static IP address pools for logical networks

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Networking**, and then click **Logical Networks**.
3. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
4. In the **Logical Networks and IP Pools** pane, click the logical network where you want to create the IP pool.

   For example, click **BACKEND**.
5. On the **Home** tab, in the **Create** group, click **Create IP Pool**.

   The Create Static IP Address Pool Wizard opens.
6. On the **Name** page, do the following, and then click **Next**.
   a. Enter a name and optional description for the IP address pool.
   b. In the **Logical network** list, make sure that the correct logical network is selected.

   For example, enter the following name and description for the **BACKEND** logical network, and then click **Next**.

Name:	**BACKEND – Seattle IP pool**
Description:	**IP addresses for internal application and database servers - Seattle**

7. On the **Network Site** page, select an existing network site or create a new one. Alternatively, if you are running System Center 2012 SP1 or System Center 2012 R2 and want to use multicasting or broadcasting, skip to the next numbered step.

   If you select **Use an existing network site**, select the network site and the IP subnet that you want to create the IP address pool from, and then click **Next**.

   Note
   You cannot change the virtual local area network (VLAN) or the assigned host groups for an existing network site from this page. If you try to change the host groups that can use the network site from this page, the value will revert to the original value when you continue to the next page of the wizard. To modify these values, you must modify the properties of the logical network. For more information, see How to Modify or Delete a Logical Network in VMM.

   If you select **Create a network site**, do the following, and then click **Next**:
   a. In the **Network site** name box, enter a name for the network site.
   b. In the **IP subnet** box, enter the IP subnet that you want to assign to the network site. Later in this procedure you can assign a range of IP addresses from the subnet to the pool. You must specify the IP subnet by using Classless Inter-Domain Router

(CIDR) notation, for example 10.0.0.0/24.

c. If you are using VLANs, in the **VLAN** box, enter the VLAN ID. A VLAN of 0 indicates to VMM not to use VLANs. In trunk mode, VLAN 0 indicates native VLAN.

d. Under **Host groups that can use this network site**, select the check box next to each host group to which you want to make the network site and the associated logical network available.

8. If you are running System Center 2012 SP1 or System Center 2012 R2, and you want to use multicasting or broadcasting, follow this step. Otherwise, skip to the next numbered step.

   With System Center 2012 SP1 or System Center 2012 R2, if the logical network on which you are creating the IP address pool is configured to use network virtualization, you can use this pool to support broadcasting or multicasting. To do this, on the **Network Site** page, click **Create a multicast IP address pool**, select the IP subnet that you want to use for multicasting or broadcasting, and then click **Next**. If you select this option, also see the requirements in "Creating an IP address pool to support multicasting or broadcasting" in Configuring Logical Networking in VMM Overview.

9. On the **IP address range** page, do the following, and then click **Next**:

   a. Under **IP address range**, enter the starting and ending IP addresses from the subnet that will make up the managed IP address pool. The beginning and ending IP address must be contained within the subnet.

      Note
      Be aware that you can create multiple IP address pools within a subnet. If you create multiple IP address pools within a subnet, the ranges cannot overlap.

      For example, add the following information for the **BACKEND – Seattle** network site, and then click **Next**.

Starting IP address:	**10.0.0.10**
Ending IP address:	**10.0.0.99**

      Tip
      The **Total addresses** field displays the total number of IP addresses in the specified IP address range.

   b. Under **VIPs and reserved IP addresses**, specify IP address ranges that you want to reserve, such as a range for load balancer virtual IP addresses (VIPs). The IP addresses that you want to reserve must fall within the IP address range that you specified in step 8a.

      For example, in the **IP addresses reserved for creating load balancer VIPs** box, enter the address range **10.0.0.25–10.0.0.35**, and then click **Next**.

      Note

During deployment of a service with a load-balanced service tier, VMM automatically assigns a virtual IP address to the load balancer from the reserved range of VIP addresses. After the DNS administrator registers the assigned VIP address in DNS, clients can access the service by connecting through its registered name in DNS.

10. Optionally, on the **Gateway** page, click **Insert**, and then specify one or more default gateway addresses and the metric. The default gateway address must fall within the same subnet range as the IP address pool. It does not have to be part of the IP address pool range.

    For example, enter the default gateway address **10.0.0.1**, accept the default of **Automatic** as the metric, and then click **Next**.

    Note

    The metric is a value that is assigned to an IP route for a particular network interface that identifies the cost that is associated with using that route. If you use the automatic metric, the metric is automatically configured for local routes based on the link speed.

11. Optionally, on the **DNS** page, specify Domain Name System (DNS)-related information, such as the list of DNS servers and their order, the default DNS suffix for the connection, and the list of DNS search suffixes.

    Important

    For virtual machines that will join an Active Directory domain, we recommend that you use Group Policy to set the primary DNS suffix. This will ensure that when a Windows-based virtual machine is set to register its IP addresses with the primary DNS suffix, a Windows-based DNS server will register the IP address dynamically. Additionally, the use of Group Policy enables you to have an IP address pool that spans multiple domains. In this case, you would not want to specify a single primary DNS suffix.

    For example, enter the DNS server address **10.0.0.2**, the connection-specific DNS suffix **contoso.com**, and then click **Next**.

12. Optionally, on the **WINS** page, click **Insert**, and then enter the IP address of a Windows Internet Name Service (WINS) server. You can also select the check box that indicates whether to enable NetBIOS over TCP/IP. Be aware that enabling NetBIOS over TCP/IP is not recommended if the address range consists of public IP addresses.

    For example, enter the WINS server address **10.0.0.3**, and then click **Next**.

13. On the **Summary** page, confirm the settings, and then click **Finish**.

    The **Jobs** dialog box appears. Make sure that the job has a status of **Completed**, and then close the dialog box.

14. To verify that the IP address pool was created, in the **Logical Networks and IP Pools** pane, expand the logical network where you created the pool.

    The IP address pool appears under the logical network.

15. Optionally, repeat this procedure to add IP address pools for other logical networks.

    Note
    Throughout the example scenarios, the BACKEND logical network is used as an example. Therefore, the example IP addresses are provided only for the BACKEND logical network.

Note
You can use the Windows PowerShell cmdlets, Get-SCIPAddress and Get-SCStaticIPAddressPool, to view the states of the IP addresses in an IP address pool. Use the cmdlets with the following syntax, where `<StaticIPAddressPool>` is the name of your static IP address pool:

```
$ippool=Get-SCStaticIPAddressPool -Name <StaticIPAddressPool>

Get-SCIPAddress -StaticIPAddressPool $ippool | Format-Table -property
Address,AssignedToType,State
```

From time to time, you might need to release IP addresses that are in the pool but that are marked by VMM as “inactive.” Releasing them makes them available for reassignment. For more information, see How to Release Inactive IP or MAC Addresses in VMM.

As of System Center 2012 R2, after a virtual machine has been deployed in VMM, you can view the IP address or addresses assigned to that virtual machine. To do this, right-click the listing for the virtual machine, click **Properties**, click the **Hardware Configuration** tab, click the network adapter, and in the results pane, click the **Connection details** button.

See Also

How to Release Inactive IP or MAC Addresses in VMM

Configuring Logical Networking in VMM Overview

Configuring Networking in VMM

How to Create a Logical Network in VMM

How to Create IP Address Pools for VM Networks in VMM

How to Create Custom MAC Address Pools in VMM

How to Create Custom MAC Address Pools in VMM

You can use the following optional procedure to create custom media access control (MAC) address pools for virtual machines that are running on managed hosts. By using static MAC address pools, Virtual Machine Manager (VMM) can automatically generate and assign MAC addresses to new virtual network devices. You can use either the default MAC address pools or configure custom MAC address pools that are scoped to specific host groups.

Important
If you want to use the default MAC address pools, do not complete this procedure.

VMM uses the following default MAC address pool ranges.

Default MAC Address Pool Name	Hypervisor Platform	Default MAC Address Pool Range
Default MAC address pool	Hyper-V and Citrix XenServer	00:1D:D8:B7:1C:00 – 00:1D:D8:F4:1F:FF
Default VMware MAC address pool	VMware ESX	00:50:56:00:00:00 – 00:50:56:3F:FF:FF

If you create custom MAC address pools, the following restrictions apply:

- If you want to divide one of the default pools into smaller custom pools, you must first delete the default MAC address pool or the default VMware MAC address pool. You must delete the default pool to avoid duplicate MAC address assignments.
- The first three octets of the beginning and ending MAC address must be the same.
- You must enter a valid hexadecimal values between 00 and FF.
- The ranges that you specify cannot overlap.
- The address range must not have the multi-cast bit set to 1. For example, you cannot use addresses that start with *X*1, *X*3, *X*5, *X*7, *X*9, *X*B, *X*D, or *X*F, where *X* is any value.
- To avoid conflicts with addresses reserved by Microsoft, VMware, and Citrix, do not use the following prefixes.

Reserved For	Prefixes
Microsoft	00:03:FF 00:0D:3A 00:12:5A 00:15:5D 00:17:FA 00:50:F2 00:1D:D8 (except for the 00:1D:D8:B7:1C:00 – 00:1D:D8:F4:1F:FF range that is reserved for VMM)
VMware	00:05:69 00:0C:29 00:1C:14 00:50:56 (except for the 00:50:56:00:00:00 – 00:50:56:3F:FF:FF range that is the reserved as the default VMware static range)
Citrix	00:16:3E

Important

Only complete the “To delete a default MAC address pool (optional)” procedure if you do not want to use the default pools, or you want to divide a default pool into smaller pools.

To delete a default MAC address pool (optional)

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Networking**, and then click **MAC Address Pools**.
3. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
4. In the **MAC Pools** pane, click the default MAC address pool that you want to delete.

   For example, to delete the default pool for Hyper-V, click **Default MAC address pool**.
5. On the **Home** tab, in the **Remove** group, click **Remove**.
6. When prompted whether you want to remove the default MAC address pool, click **Yes**.

To create custom MAC address pools

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Networking**, and then click **MAC Address Pools**.
3. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
4. On the **Home** tab, in the **Create** group, click **Create MAC Pool**.

   The Create MAC Address Pool Wizard opens.
5. On the **Name and Host Group** page, do the following, and then click **Next**:
   a. In the **MAC address pool name** and **Description** boxes, enter a name and optional description for the MAC address pool.

      For example, enter the following information:

MAC pool name	**MAC pool - Seattle**
Description	**MAC pool for Seattle and its child host groups (Hyper-V and XenServer)**

   b. Under **Host groups**, select the check box next to each host group to which the MAC address pool will be available.

      For example, select the check box next to the **Seattle** host group. By default, all child host groups are selected.
6. On the **MAC Address Range** page, specify the beginning and ending MAC address.

   For example, enter the following information, and then click **Next**.

   Note

   This example assumes that you have deleted the default MAC address pool.

Starting MAC address	**00:1D:D8:B7:1C:00**
Ending MAC address	**00:1D:D8:B7:1F:E8**

7. On the **Summary** page, confirm the settings, and then click **Finish**.

   The **Jobs** dialog box appears. Make sure that the job has a status of **Completed**, and then close the dialog box.

   The MAC address pool appears in the **MAC Pools** pane.
8. Optionally, repeat this procedure to create custom MAC pools for other host groups.

   Note

   If you are following the scenario examples, and have deleted the default MAC address pool, and then created a custom MAC address pool for Seattle, make sure that you create a custom MAC pool for the New York host group (and its child host groups).

Note

You can use the Windows PowerShell cmdlets, Get-SCMACAddress and Get-SCMACAddressPool, to view the states of the MAC addresses in a MAC address pool. Use the cmdlets with the following syntax, where `<MACAddressPool>` is the name of your MAC address pool:

```
$MACpool=Get-SCMACAddressPool -Name <MACAddressPool>

Get-SCMACAddress -MACAddressPool $MACpool | Format-Table -property
Address,VirtualNetworkAdapter,State
```

From time to time, you might need to release MAC addresses that are in the pool but that are marked by VMM as “inactive.” Releasing them makes them available for reassignment. For more information, see How to Release Inactive IP or MAC Addresses in VMM.

See Also

How to Release Inactive IP or MAC Addresses in VMM

Configuring Logical Networking in VMM Overview

How to Create IP Address Pools for Logical Networks in VMM

Configuring Networking in VMM

How to Release Inactive IP or MAC Addresses in VMM

You can use the following procedure to release inactive IP addresses and MAC addresses. When you release an inactive address, Virtual Machine Manager (VMM) returns the address to the static IP address or MAC address pool, and considers it available for reassignment. An IP or MAC address is considered inactive when either of the following conditions is true:

- A host that was assigned a static IP address through the bare-metal deployment process is removed from VMM management. When you remove the host, any IP and MAC addresses that were statically assigned to virtual machines on the host are also marked as inactive.
- A virtual machine goes into a missing state because it was removed outside VMM.

To release inactive IP addresses

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Networking**, and then click **Logical Networks**.
3. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
4. In the **Logical Networks and IP Pools** pane, expand the logical network, and then click the desired IP address pool.
5. On the **Home** tab, in the **Properties** group, click **Properties**.
6. Click the **Inactive addresses** tab.
7. Select the check box next to each inactive IP address that you want to release, or select the check box in the table header row to select all the addresses, and then click **Release**.

To release inactive MAC addresses

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Networking**, and then click **MAC Address Pools**.
3. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
4. In the **MAC Pools** pane, click the desired MAC address pool.
5. On the **Home** tab, in the **Properties** group, click **Properties**.
6. Click the **Inactive addresses** tab.
7. Select the check box next to each inactive MAC address that you want to release, or select the check box in the table header row to select all the addresses, and then click **Release**.

See Also

How to Create IP Address Pools for Logical Networks in VMM

How to Create Custom MAC Address Pools in VMM

Configuring Logical Networking in VMM Overview

Configuring Networking in VMM

How to Add an IPAM Server in VMM in System Center 2012 R2

With System Center 2012 R2, you can add an IP Address Management (IPAM) server that runs Windows Server 2012 R2 to the resources in Virtual Machine Manager (VMM). After you add the IPAM server, the IP address settings that are associated with logical networks and virtual machine networks (VM networks) in VMM are kept in synchrony with settings that are stored in the IPAM server.

Note

After you add an IPAM server to your VMM configuration, you can use the IPAM server to configure and monitor logical networks and their associated network sites and IP address pools. You can also use the IPAM server to monitor the usage of VM networks that you have configured or changed in VMM. However, tenants must continue to use the VMM server (not IPAM) to configure VM networks that use network virtualization—in other

words, to control the address space that is typically controlled by tenants rather than by VMM administrators.

This topic describes how you can add an IPAM server to the list of resources in VMM in System Center 2012 R2 only. For information about how to add a virtual switch extension manager to the list of resources in VMM in System Center 2012 SP1, see How to Add a Virtual Switch Extension Manager in System Center 2012 SP1.

Use the following procedure to add an IPAM server to VMM in System Center 2012 R2.

Prerequisites

Before you can add an IPAM server to your configuration in VMM, you must perform the following actions:

1. On a server running Windows Server 2012 R2, install the IPAM feature by using **Add Roles and Features** (in Server Manager) or Windows PowerShell commands. Then configure the IPAM server as described in the relevant IPAM documentation. Examples of IPAM topics on TechNet are IP Address Management (IPAM) Overview and Checklist: Deploy IPAM Server.

   Note
   The IPAM server must be installed on a domain member computer, and must meet other requirements that are described in Install IPAM Server.

2. Create or identify a domain account and, to avoid issues with expiration of the password, ensure that the account is set to never expire. Then, on the IPAM server, ensure that the account has at least the minimum necessary permissions by adding the account to the following two groups:
   - **IPAM ASM Administrators**: A local group that exists on all IPAM servers, and provides permissions for IP address space management (ASM). For more information, see Assign Administrator Roles.
   - **Remote Management Users**: A built-in group that provides access to WMI resources through management protocols, such as WS-Management through the Windows Remote Management service.
3. Confirm that the IPAM server and the VMM are being kept in time synchrony. Time synchrony depends on settings for the Windows Time Service. In most configurations, if two servers are in the same forest, Windows Time Service keeps them in synchrony. For information about the Windows Time Service command, **W32tm**, and the **/resync** option in that command, see W32tm. If you cannot control the time synchrony of the IPAM server and the VMM server, see the instructions in the “Important configuration notes” at the end of this topic.
4. Make sure that you know the fully qualified domain name (FQDN) of the IPAM server to use as a connection string.
5. Make sure that you know the names of the VMM host groups for which you want integration between the IPAM server and the VMM server. You can also choose to include all host groups in the integration.

The provider software for an IPAM server running Windows Server 2012 R2 is already included in the VMM management server in System Center 2012 R2. You do not have to install it. If you want to review the provider software on your VMM server, open the **Settings** workspace and in the

Settings pane, click **Configuration Providers**. The list of providers appears in the **Configuration Providers** pane.

To add an IPAM server in System Center 2012 R2

1. Open the **Fabric** workspace.
2. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
3. In the **Fabric** pane, expand **Networking**, and then click **Network Service**.

   Network services include gateways, virtual switch extensions, network managers (which include IPAM servers), and top-of-rack (TOR) switches.
4. On the **Home** tab, in the **Add** group, click **Add Resources**, and then click **Network Service**.

   The **Add Network Service Wizard** opens.
5. On the **Name** page, type a name and optional description, and then click **Next**.
6. On the **Manufacturer and Model** page, in the **Manufacturer** list, click **Microsoft**, and in the **Model** list, click **Microsoft Windows Server IP Address Management**. Then click **Next**.
7. On the **Credentials** page, either click **Browse** and then on the **Select a Run As Account** dialog box, specify the account described in the previous Prerequisites section, or click **Create Run As Account** and create a new Run As account with the permissions that are listed in the Prerequisites section. After you specify the account, click **Next**.
8. On the **Connection String** page, in the **Connection string** box, type the fully qualified domain name (FQDN) of the IPAM server, and then click **Next**.

   For example, you might enter the following connection string:

   IPAMserver1.contoso.com

   If you have configured a specific port on the IPAM server, the string can also end in that port number preceded by a colon (for example, **:443**). If a port number is not specified, the default port for the IPAM server is used.
9. On the **Provider** page, in the **Configuration provider** list, select **Microsoft IP Address Management Provider**, and then click **Test** to run basic validation tests with the provider. If tests indicate that the provider works as expected with the IPAM server, click **Next**.

   Results that say **Passed** or **Failed** indicate whether the provider works as expected. One possible cause of failure is insufficient permissions in the Run As account. Results that say **Implemented** and **Not implemented** are informational only, and indicate whether the provider supports a particular API.
10. On the **Host Group** page, select one or more host groups for which you want integration between the IPAM server and the VMM server.
11. On the **Summary** page, review and confirm the settings, and then click **Finish**.
12. Confirm that the IPAM server is listed under **Network Services**. Whenever you want to send or receive the latest settings to and from the IPAM server, you can right-click the listing for the IPAM server and then click **Refresh**.

On the IPAM server, to view the logical networks and related settings that were configured in VMM, navigate to **VIRTUALIZED IP ADDRESS SPACE**, and then to **Provider IP Address Space**. For each logical network, the IPAM server will have an address space (an overarching category that is found in IPAM, but not in VMM) with a name that is based on the name of the logical network. The logical network will be contained within the address space, with the name of the logical network displayed under the heading **VMM Logical Network**. To see the types of information that are stored in IPAM, expand the address space and select different views.

The following table can help you interpret some of the information that you see on the IPAM server:

VMM name	IPAM name
Logical network	VIRTUALIZED IP ADDRESS SPACE Provider IP Address Space: **VMM Logical Network** column
Network site	VIRTUALIZED IP ADDRESS SPACE Provider IP Address Space: **Network Site** column
IP address subnet	IP Address Subnet (same name in IPAM as in VMM)
IP address pool	IP Address Range
VM network	VIRTUALIZED IP ADDRESS SPACE Customer IP Address Space: **VM Network** column

Important configuration notes

- If you want to use the IPAM server to delete a logical network, delete the IP address subnets assigned to that logical network, and do not delete the name associated with the **VMM Logical Network** field on the IPAM server. The two servers will then be able to synchronize correctly, and the logical network will be deleted. If you do delete the name associated with the **VMM Logical Network** field on the IPAM server, you must go to the VMM server and delete the network sites and the logical network. Then, after the two servers synchronize, the deletion will be complete.
- If you cannot control the time synchrony of the IPAM server and the VMM server as described in the Prerequisites in this topic, you must update permissions on the IPAM server so that the provider software (included in VMM in System Center 2012 R2) can query the current time setting on the IPAM server. To do this, on the IPAM server, run **wmimgmt.msc** to open the **WMI Control (Local)** snap-in. Right-click **WMI Control (Local)**, click **Properties**, and then click the **Security** tab. Navigate to **Root\CIMV2**, click the **Security** button, select the account that you created for the Prerequisites in this topic,

and then for **Remote Enable**, select the **Allow** box.

See Also

IP Address Management (IPAM) Overview

Configuring Logical Networking in VMM Overview

How to Add a Virtual Switch Extension or Network Manager in System Center 2012 R2

How to Add a Virtual Switch Extension Manager in System Center 2012 SP1

Configuring Load Balancing in VMM Overview

Networking in Virtual Machine Manager (VMM) includes load balancing integration, so that you can automatically provision load balancers in your virtualized environment. Load balancing integration works together with other network enhancements in VMM. For information about these enhancements, see the list of topics at the end of this topic.

Load balancer integration

By adding a load balancer to VMM, you can load balance requests to the virtual machines that make up a service tier. You can use Microsoft Network Load Balancing (NLB) or you can add supported hardware load balancers through the VMM console. NLB is included as an available load balancer when you install VMM. NLB uses round robin as the load-balancing method.

To add supported hardware load balancers, you must install a configuration provider that is available from the load balancer manufacturer. The configuration provider is a plug-in to VMM that translates VMM PowerShell commands to API calls that are specific to a load balancer manufacturer and model.

Before you can use a hardware load balancer or NLB, you must create associated virtual IP (VIP) templates.

Note

For information about supported hardware load balancers, how to obtain load balancer providers, and how to add a hardware load balancer, see How to Add Hardware Load Balancers in VMM.

VIP templates

A virtual IP template contains load balancer-related configuration settings for a specific type of network traffic. For example, you could create a template that specifies the load balancing behavior for HTTPS traffic on a specific load balancer manufacturer and model. These templates represent the best practices from a load balancer configuration standpoint.

After you create a virtual IP template, users (including self-service users) can specify the virtual IP template to use when they create a service. When a user models a service, they can pick an available template that best matches their needs for the type of load balancer and the type of application.

Note

For information about how to create virtual IP templates, see How to Create VIP Templates for Hardware Load Balancers in VMM and How to Create VIP Templates for Network Load Balancing (NLB) in VMM.

Hardware load balancer workflow

The following list describes the hardware load balancer workflow to load balance a service tier:

1. In the VMM console, during creation of a static IP address pool, the administrator configures a reserved range of virtual IP addresses.

   Note
   This step can be performed at any time before a service is deployed that uses a load balancer. Realize that you must have one virtual IP address for each service tier that uses load balancing.

2. The administrator installs the load balancer configuration provider on the VMM management server.

   Note
   For information about supported load balancers and how to obtain configuration providers, see the “Prerequisites” section of How to Add Hardware Load Balancers in VMM.

3. In the VMM console, the administrator adds the load balancer to VMM management. Through the Add Load Balancer wizard, the administrator does the following:
   - Selects the host groups where the load balancer will be available
   - Specifies the load balancer manufacturer and model
   - Specifies the load balancer DNS names (or IP addresses) and the port number that is used for load balancer management
   - Specifies the affinity to logical networks
   - Selects the configuration provider
   - Optionally tests the connection to the load balancer
4. In the VMM console, the administrator creates one or more virtual IP templates. Through the Load Balancer VIP Template wizard, the administrator defines the following:
   - The port to use for the type of network traffic that will be load balanced
   - Whether the template applies to any supported load balancer or to a specific type of load balancer
   - The type of protocol to load balance (for example HTTPS)
   - Whether to enable session persistence
   - Optional health monitors that can be configured to periodically check that the load balancer is responsive
   - The type of load balancing method to use
5. A user (typically a self-service user) creates a service template. In the Service Template Designer window, they add a load balancer to a service tier, and then select which virtual IP (VIP) template to use. When the service is deployed, VMM automatically selects a virtual IP address from the reserved range in the static IP address pool and assigns it to the load

balancer. This IP address is considered the “front-end” IP address for a load-balanced service tier. VMM also assigns static IP addresses to the virtual machines that make up the service tier. These are considered “back-end” dedicated IP addresses, as they are behind the load balancer.

6. After the service is deployed, the administrator verifies in the VMM console which virtual IP address is being used as the front-end IP address for the service tier. The administrator then contacts the DNS administrator to create a DNS entry for the assigned virtual IP address. For example, if the front-end Web tier of a service is load balanced, the administrator can verify which virtual IP address is used for that tier. The DNS administrator can then create an entry in DNS for the name that users will specify to connect to the Web front-end. For example, the DNS administrator could create a DNS entry for *ServiceName*.contoso.com with the corresponding virtual IP address.

   Note
   For more detailed information about how to load-balance a service tier by using a hardware load balancer, see How to Configure a Hardware Load Balancer for a Service Tier.

NLB workflow

The following list describes the NLB workflow to load balance a service tier:

1. In the VMM console, during creation of a static IP address pool, the administrator configures a reserved range of virtual IP addresses.

   Note
   This step can be performed at any time before a service is deployed that uses a load balancer. Realize that you must have one virtual IP address for each service tier that uses load balancing.

2. In the VMM console, the administrator creates one or more virtual IP templates. Through the Load Balancer VIP Template wizard, the administrator defines the following:
   - The port to use for the type of network traffic that will be load balanced
   - The template type (in this case, the Specific template type, set to Microsoft NLB)
   - The type of protocol to load balance (TCP, UPD, or both)
   - Whether to enable session persistence
3. A user (typically a self-service user) configures a service template by doing the following:
   - For the tier that will be load balanced, the user must specify a virtual machine template that meets the specific configuration requirements for NLB. For information about the configuration requirements, see How to Configure NLB for a Service Tier.
   - In the Service Template Designer window, the user adds a load balancer, and then selects which virtual IP (VIP) template to use.

   When the service is deployed, VMM automatically selects a virtual IP address from the reserved range in the static IP address pool and assigns it to a load-balanced service tier. VMM also assigns static IP addresses to the virtual machines that make up the service tier.
4. After the service is deployed, the administrator verifies in the VMM console which virtual IP address is being used for a service. The administrator then contacts the DNS administrator to

create a DNS entry for the assigned virtual IP address. For example, if the front-end Web tier of a service is load balanced, the administrator can verify which virtual IP address is used for that tier. The DNS administrator can then create an entry in DNS for the name that users will specify to connect to the Web front-end. For example, the DNS administrator could create a DNS entry for *ServiceName*.contoso.com with the corresponding virtual IP address.

Note
For more detailed information about how to load-balance a service tier by using NLB, see How to Configure NLB for a Service Tier.

Example scenario overview

The procedures in this section include examples that help demonstrate the concepts. For a summary of the examples that are used in this section, see the “Networking” section of the table in Preparing the Fabric Scenario in VMM.

Note
The examples are not meant to be prescriptive guidance for a lab setup. You should adapt the examples to your test environment.

In this section

To configure load balancing in your virtualized environment, follow these procedures:

Procedure	Description
How to Add Hardware Load Balancers in VMM	Describes how to add supported hardware load balancers to the VMM environment so that you can load balance service requests. **Note** If you want to use Microsoft Network Load Balancing (NLB), you do not have to add a hardware load balancer. When you install VMM, NLB is automatically included as a load balancer. To use NLB, you must create NLB virtual IP templates, described in the last row of this table.
How to Create VIP Templates for Hardware Load Balancers in VMM	Describes how to create virtual IP templates that you can use during service creation to help choose a hardware load balancer that best suits the need of the application.
How to Create VIP Templates for Network Load Balancing (NLB) in VMM	Describes how to create NLB virtual IP templates that you can use during service creation to configure NLB for a service tier.

Next steps after configuring load balancing in System Center 2012 SP1 or System Center 2012 R2

For information about the next steps to take after configuring load balancing in System Center 2012 SP1 or System Center 2012 R2, see the following networking overviews:

Topic	Step
Configuring Ports and Switches for VM Networks in VMM (for System Center 2012 SP1 and System Center 2012 R2)	Configure port profiles and port classifications, and use them in logical switches, so that you can apply your port settings consistently to your network adapters and virtual network adapters. After configuring port settings, configure logical switches, and as needed, switch extensions (for Quality of Service (QoS), monitoring, or security).
Configuring VM Networks and Gateways in VMM (for System Center 2012 SP1 and System Center 2012 R2)	Configure VM networks (on top of logical networks), which allow you to use network virtualization or other networking options. With VM networks that use network virtualization, you can also use gateways to increase connectivity.

Next steps after configuring networking

For information about the next steps to take after configuring networking, see the following topics:

Topic	Step
Preparing the Fabric in VMM	Configure additional fabric resources such as storage and library resources.
Adding and Managing Hyper-V Hosts and Scale-Out File Servers in VMM Managing VMware ESX and Citrix XenServer in VMM	Configure hosts.
Creating and Deploying Virtual Machines and Services in VMM	Deploy virtual machines, individually or as part of a service.

See Also

Configuring Logical Networking in VMM Overview

Common Scenarios for Networking in VMM in System Center 2012

Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2

Configuring Ports and Switches for VM Networks in VMM

Configuring VM Networks and Gateways in VMM

Configuring Networking in VMM

How to Add Hardware Load Balancers in VMM

You can use the following procedure to discover and add hardware load balancers to System Center 2012 – Virtual Machine Manager (VMM). By adding load balancers to VMM management and by creating associated virtual IP templates (VIP templates), users who create services can automatically provision load balancers when they create and deploy a service.

Important

If you want to use Microsoft Network Load Balancing (NLB), you do not have to complete this procedure. When you install VMM, NLB is automatically included as a load balancer. To use NLB, you must create NLB virtual IP templates. For more information, see How to Create VIP Templates for Network Load Balancing (NLB) in VMM.

Account requirements To complete this procedure, you must be a member of the Administrator user role or a Delegated Administrator where the administrative scope includes the host groups to which you want to make the load balancer available.

Prerequisites

Before you begin this procedure, make sure that the following prerequisites are met:

- You must have a supported hardware load balancer. VMM supports the following hardware load balancers:
  - BIG-IP from F5 Networks, Inc.
  - Brocade ServerIron ADX from Brocade Communications Systems, Inc.
  - Citrix NetScaler from Citrix Systems, Inc.
- You must obtain the load balancer provider from the load balancer vendor, and install the provider on the VMM management server. You can use the following links to obtain the load balancer provider from your vendor's website:

  Note

  In the following list, all information and content at the listed Web addresses is provided by the owner or the users of each website. Microsoft makes no warranties, express, implied or statutory, as to the information at this website.

  - Download the BIG-IP from F5 load balancer provider

    Note

    You must create or have an existing login to the F5 website to download the provider.

  - Download the Brocade ServerIron ADX load balancer provider

    Note

You must create or have an existing login to the Brocade website to download the provider.

- Download the Citrix NetScaler load balancer provider

Important

After you install the load balancer provider, you must restart the System Center Virtual Machine Manager service. To restart the service, from an elevated command prompt, type the command **net stop scvmmservice**, press ENTER, type **net start scvmmservice**, and then press ENTER.

Also, realize that if you uninstall System Center 2012 – Virtual Machine Manager (VMM), and then reinstall it, you must also uninstall and then reinstall the load balancer provider.

- Although it is not a required prerequisite, you can create a Run As account before you begin this procedure. (You can also create the account during the procedure.) The associated credentials must have permissions to configure the load balancers that you want to add.

  For example, create a Run As account that is named **Load Balancers**.

  Note

  You can create a Run As account in the **Settings** workspace. For more information about Run As accounts, see How to Create a Run As Account in VMM.

To add a hardware load balancer

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Networking**, and then click **Load Balancers**.
3. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
4. On the **Home** tab, in the **Add** group, click **Add Resources**, and then click **Load Balancer**.

   The Add Load Balancer Wizard opens.
5. On the **Credentials** page, next to the **Run As account** box, click **Browse**, and then click a Run As account that has permissions on the load balancer. When you are finished, click **OK**, and then click **Next**.

   For example, if you created the Run As account that is described in the Prerequisites section, select the **Load Balancers** Run As account.

   Note

   If you do not already have a Run As account, click **Browse**, and then in the **Select a Run As Account** dialog box, click **Create Run As Account**.
6. On the **Host Group** page, select the check box next to each host group where the load balancer will be available. By default, any child host groups are also selected.

   For example, under **Seattle**, select the check box next to the **Seattle** host group, and then click **Next**.
7. On the **Manufacturer and Model** page, specify the load balancer manufacturer and

model, and then click **Next**.

8. On the **Address** page, do the following, and then click **Next**:
   a. Specify the IP address, fully qualified domain name (FQDN), or the NetBIOS names of the load balancers that are of the same manufacturer and model that you specified in the previous step. Separate each load balancer by using a comma or by adding the load balancer on a new line.
   b. In the **Port number** box, enter the port number that you use to connect to for management of the load balancers.

   For example, enter the FQDN **LoadBalancer01.contoso.com**, and the port number that is used to communicate with the load balancer, such as port 443.
9. On the **Logical Network Affinity** page, specify the load balancer affinity to logical networks, and then click **Next**.

   Setting the load balancer affinity enables you to provide some control over which load balancer will be used for a service. This is based on logical network information. VMM uses this information to determine the valid static IP address pools that are accessible from both the load balancer and the host group that the service tier will be deployed to. Note the following:

   - When you configure front-end affinity, select the logical networks from which the load balancer can obtain its virtual IP (VIP) address. The VIP address is the IP address that is assigned to a load balancer during the deployment of a load-balanced service tier. Clients can connect to the VIP address through a registered DNS name to access the service.

     During the deployment of a load-balanced service tier, VMM looks for static IP address pools with available VIP addresses on the logical network that you select for the “Client connection” object when you configure a load balancer in a service template.

     For the load balancer to be selected during placement, when you configure the load balancer “Client connection” object, the logical network that you select must be in the list of logical networks that are selected for front-end affinity.

     Important
     For front-end affinity, make sure that you select one or more logical networks where the associated network site with a reserved VIP address range is available to a host group or parent host group that is also available to the hardware load balancer.
   - When you configure back-end affinity, select the logical networks to which you want to make the load balancer available for connections from the virtual machines that make up a service tier.

     For the load balancer to be selected during placement, when you configure the load balancer “Server connection” object in a service template, the logical network that the NIC object is connected to must be in the list of logical networks that are selected for back-end affinity.

10. On the **Provider** page, do the following, and then click **Next**:
    a. In the **Provider** list, click an available provider to use for load balancer configuration.
    b. In the **Load balancer for configuration test** list, click an available load balancer, click **Test**, and view the test results.
11. On the **Summary** page, confirm the settings, and then click **Finish**.

    The **Jobs** dialog box appears. Make sure that the job has a status of **Completed**, and then close the dialog box.
12. Verify that the load balancer appears in the **Load Balancers** pane. The **Provider Status** column indicates whether the provider is active.

See Also

Configuring Load Balancing in VMM Overview

Configuring Networking in VMM

How to Create VIP Templates for Hardware Load Balancers in VMM

How to Configure a Hardware Load Balancer for a Service Tier

How to Create VIP Templates for Hardware Load Balancers in VMM

You can use the following procedure to create a virtual IP (VIP) template for a hardware load balancer. A VIP template contains load-balancer-related configuration settings for a specific type of network traffic. For example, you can create a template that specifies the load-balancing behavior for HTTPS traffic on a specific load balancer by manufacturer and model. These templates represent the best practices from a load-balancer configuration standpoint.

Note
For information about how to create a VIP template for Microsoft Network Load Balancing (NLB), see How to Create VIP Templates for Network Load Balancing (NLB) in VMM.

When users create a service, they can select a VIP template to use when they want to load-balance a service tier. For an overview of the load-balancer and VIP workflow, see the “Load Balancer Integration” section of the topic Configuring Load Balancing in VMM Overview.

To create a VIP template for a hardware load balancer

1. In Virtual Machine Manager (VMM), open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Networking**, and then click **VIP Templates**.
3. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
4. On the **Home** tab, in the **Create** group, click **Create VIP Template**.

   The Load Balancer VIP Template Wizard starts.
5. On the **Name** page, enter the following information, and then click **Next**:
    a. The template name and description.
    b. The VIP port to use. The VIP port is the port that is used for the type of network traffic that you want to load balance.

   For example, enter the name **Web tier (HTTPS traffic)** and a description of **Use for**

HTTPS traffic to production Web servers. Enter the VIP port **443**. When you are finished, click **Next**.

6. On the **Type** page, do either of the following, and then click **Next**:
   - Click **Generic** to create a VIP template that can be used on any supported hardware load balancer.
   - Click **Specific** to create a VIP template that applies to a specific hardware load balancer, and then specify the manufacturer and model.

     Note

     In the **Manufacturer** list, the **Microsoft** entry is for NLB. For information about creating a VIP template for NLB, see How to Create VIP Templates for Network Load Balancing (NLB) in VMM.

   Click either of the options, depending on your test environment, and then click **Next**.
7. On the **Protocol** page, click the protocol for which you want to create the virtual IP template. You can select one of the following options:
   - **HTTP**
   - **HTTPS passthrough**

     If you click this option, encryption carries all the way through to the virtual machine, and it is not decrypted at the load balancer.
   - **HTTPS terminate**

     If you select this option, the traffic is decrypted at the load balancer. When traffic is decrypted at the load balancer, the load balancer has access to more detailed information to direct traffic, such as cookies and header information. For this option to be used, a certificate must be loaded previously on the load balancer.

     In **Certificate subject name**, enter the subject name of the certificate, for example, **C=US,ST=WA,L=Redmond,O=Contoso,OU=Test,CN=www.contoso.com/emailAddress=contoso@contoso.com**.

     To help secure the traffic from the load balancer to the virtual machine, select the **Re-Encrypt** check box. This action reencrypts the HTTPS traffic from the load balancer to the virtual machine.
   - **Custom**

     If you select this option, enter a protocol name in the **Protocol name** list, or select one from the list (if values are available).

   For example, click either **HTTPS passthrough** or **HTTPS terminate**, depending on your test environment.
8. On the **Persistence** page, you can select the **Enable persistence** check box to enable session persistence (also known as affinity). If you enable persistence, the load balancer will always try to direct the same client to the same virtual machine that is behind the load balancer. This is based on the source IP address and the subnet mask that you specify (for example, 255.255.255.0), the destination IP address, or other persistence types, such as cookie or Secure Sockets Layer (SSL) session ID. (The options vary, depending

on the selected protocol.) You can also click **Custom** and then select a custom persistence type. For a custom persistence type, the persistence value is optional, depending on the load balancer manufacturer.

9. On the **Health Monitors** page, you can specify a request that will occur at regular intervals against the load balancer to verify that a load balancer is available. (Adding a health monitor is optional.) To add a health monitor, do the following:
   a. Click **Insert**.
   b. In the **Protocol** list, click the desired protocol to monitor.
   c. Under the **Request** column, click the empty field, and then enter the request.

      For example, type **GET /**. Typically, this command makes an HTTP GET request for the home page of the load balancer and checks for a header response, such as 200 OK.
   d. To modify the response type, interval, timeout, and retries values, click the field in the desired column, and then enter a new value.

      For example, under **Response**, enter **200**.

      Note

      The time-out value should be less than the interval value. The interval and time-out values are in seconds.
10. On the **Load Balancing** page, select the load balancing method to use for new connections, and then click **Next**. You can configure new connections to be directed to a server based on the least connections or on the fastest response time, or by using round robin, where each server takes a turn. You can also click **Custom**, and then in the **Custom method** list, click a custom method that your load balancer supports.
11. On the **Summary** page, review the settings, and then click **Finish**.

    The **Jobs** dialog box appears. Make sure that the job has a status of **Completed**, and then close the dialog box.
12. Verify that the VIP template that you added appears in the **VIP Templates** pane.

See Also

Configuring Load Balancing in VMM Overview

Configuring Networking in VMM

How to Add Hardware Load Balancers in VMM

How to Configure a Hardware Load Balancer for a Service Tier

How to Create VIP Templates for Network Load Balancing (NLB) in VMM

You can use the following procedure to create a virtual IP (VIP) template for Microsoft Network Load Balancing (NLB). A virtual IP template contains load balancer-related configuration settings for a specific type of network traffic. For example, you could create a template that specifies the load balancing behavior for HTTPS traffic on port 443.

When a user creates a service, they can select a virtual IP template to use when they want to load balance a service tier. For an overview of the load balancer and virtual IP workflow, see the “Load Balancer Integration” section of the topic Configuring Load Balancing in VMM Overview.

To create a virtual IP template for NLB

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Networking**, and then click **VIP Templates**.
3. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
4. On the **Home** tab, in the **Create** group, click **Create VIP Template**.

   The Load Balancer VIP Template Wizard starts.
5. On the **Name** page, enter the following information, and then click **Next**.
   a. The template name and description.
   b. The virtual IP port to use. The virtual IP port is the port that is used for the type of network traffic that you want to load balance.

   For example, enter the name **Web tier (HTTPS traffic-NLB)**, and a description of **Uses NLB to load balance HTTPS traffic to production Web servers**. Enter the virtual IP port **443**.
6. On the **Type** page, do the following, and then click **Next**:
   a. Click **Specific**.
   b. In the **Manufacturer** list, click **Microsoft**.

      By default, in the **Model** list, **Network Load Balancing (NLB)** is listed.
7. On the **Protocol** page, click the protocol that you want to create the virtual IP template for, and then click **Next**. You can select **TCP**, **UDP** or **Both TCP and UDP**.
8. On the **Persistence** page, you can select the **Enable persistence** check box to enable session persistence (also known as affinity). If you enable persistence, the load balancer will always try to direct the same client to the same virtual machine that is behind the load balancer. This is based on the source IP address and the subnet mask.

   If you select the **Enable persistence** check box, accept the default value of **Source IP** in the **Persistence type** list. In the **Subnet mask to apply** list, click either of the following options:

   - **Single**. If you select this option, NLB directs multiple requests from the same client IP address to the same host in the NLB cluster.
   - **Network**. If you select this option, NLB directs multiple requests from the same TCP/IP Class C address range to the same host in the NLB cluster. This setting ensures that clients that use multiple proxy servers to access the NLB cluster have their TCP or UDP connections directed to the same host in the NLB cluster.

   Note
   When you deploy a service where a tier is configured to use NLB, VMM automatically creates the NLB host cluster. For more information about how to configure a service tier to use NLB, including the guest operating system requirements, see How to Configure NLB for a Service Tier.

   When you are finished, click **Next**.
9. On the **Summary** page, review the settings, and then click **Finish**.

The **Jobs** dialog box appears. Make sure that the job has a status of **Completed**, and then close the dialog box.

10. Verify that the virtual IP template that you added appears in the **VIP Templates** pane.

See Also

Configuring Load Balancing in VMM Overview

Configuring Networking in VMM

How to Configure NLB for a Service Tier

Configuring Ports and Switches for VM Networks in VMM

In Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1) or System Center 2012 R2, you can consistently configure identical capabilities for network adapters across multiple hosts by using port profiles and logical switches. Port profiles and logical switches act as containers for the properties or capabilities that you want your network adapters to have. Instead of configuring individual properties or capabilities for each network adapter, you can specify the capabilities in port profiles and logical switches, which you can then apply to the appropriate adapters. This can simplify the configuration process.

Important

- For more information about the ways that you can use port profiles, logical switches, switch extensions, and other networking options to support your virtual machine configurations, see Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2.
- For illustrations that show how logical switches relate to port profiles and port classifications, see Configuring Ports and Switches in VMM Illustrated Overview.
- In System Center 2012 SP1 and System Center 2012 R2, some of the VMM networking enhancements are based on the Hyper-V Virtual Switch, which was introduced in Windows Server 2012. To understand these networking enhancements, it can be useful to review the illustrations and descriptions of the Hyper-V Virtual Switch in Hyper-V Virtual Switch Overview.

Settings

The following table provides details about port profiles, port classifications, and logical switches and the settings within them. The table includes prerequisites for specific settings. For a higher-level outline of prerequisites, see the Prerequisites section in this topic.

Networking item in VMM	Uses and settings
Native port profile for uplinks (in System Center 2012 SP1) **Hyper-V port profile for uplinks** (in System Center 2012 R2)	A port profile for uplinks (also called an uplink port profile) specifies which logical networks can connect through a particular physical network adapter. After you create an uplink port profile, add it to a logical switch, which places it in a list of profiles that are available through that logical

Networking item in VMM	Uses and settings
	switch. When you apply the logical switch to a network adapter in a host, the uplink port profile is available in the list of profiles, but it is not applied to that network adapter until you select it from the list. This helps you to create consistency in the configurations of network adapters across multiple hosts, but it also enables you to configure each network adapter according to your specific requirements. To enable teaming of multiple network adapters, you can apply the same logical switch and uplink port profile to those network adapters and configure appropriate settings in the logical switch and uplink port profile. In the logical switch, for the **Uplink mode**, select **Team** to enable teaming. In the uplink port profile, select appropriate **Load-balancing algorithm** and **Teaming mode** settings (or use the default settings). For background information about load-balancing algorithms and teaming modes, see NIC Teaming Overview.
Native port profile for virtual network adapters (in System Center 2012 SP1) **Hyper-V port profile for virtual network adapters** (in System Center 2012 R2)	A port profile for virtual network adapters specifies capabilities for those adapters and makes it possible for you to control how bandwidth is used on the adapters. The capabilities include offload settings and security settings. The following list of options provides details about these capabilities: • **Enable virtual machine queue** (offload setting): With virtual machine queue (VMQ), packets that are destined for a virtual network adapter are delivered directly to a queue for that adapter, and they do not have to be copied from the management operating system to the virtual machine. VMQ requires support from the physical network adapter. • **Enable IPsec task offloading** (offload setting): With this type of offloading, some

Networking item in VMM	Uses and settings
	or all of the computational work that IPsec requires is shifted from the computer's CPU to a dedicated processor on the network adapter. For details about IPsec task offloading, see What's New in Hyper-V Virtual Switch. IPsec task offloading requires support from the physical network adapter and the guest operating system. • **Enable Single-root I/O virtualization** (offload setting): With single-root I/O virtualization (SR-IOV), a network adapter can be assigned directly to a virtual machine. The use of SR-IOV maximizes network throughput while minimizing network latency and minimizing the CPU overhead that is required to process network traffic. SR-IOV requires support from the host hardware and firmware, the physical network adapter, and drivers in the management operating system and the guest operating system. To use SR-IOV with VMM, SR-IOV must be enabled or configured in multiple places. It must be enabled in the port profile, and in the logical switch in which you include the port profile. It must also be configured correctly on the host, when you create the virtual switch that brings together the port settings and the logical switch that you want to use on the host. In the port profile, the SR-IOV setting is in **Offload Settings**, and in the logical switch configuration, the SR-IOV setting is in the **General** settings. In the virtual switch, attach the port profile for virtual network adapters to the virtual switch by using a port classification. You can use the SR-IOV port classification that is provided in VMM, or you can create your own port classification. • **Allow MAC spoofing** (security setting):

Networking item in VMM	Uses and settings
	With media access control (MAC) spoofing, a virtual machine can change the source MAC address in outgoing packets to an address that is not assigned to that virtual machine. For example, a load-balancer virtual appliance might require this setting to be enabled. • **Enable DHCP guard** (security setting): With DHCP guard, you can protect against a malicious virtual machine that represents itself as a Dynamic Host Configuration Protocol (DHCP) server for man-in-the-middle attacks. • **Allow router guard** (security setting): With router guard, you can protect against advertisement and redirection messages that are sent by an unauthorized virtual machine that represents itself as a router. • **Allow guest teaming** (security setting): With guest teaming, you can team the virtual network adapter with other network adapters that are connected to the same switch. • **Allow IEEE priority tagging** (security setting): With Institute of Electrical and Electronics Engineers, Inc. (IEEE) priority tagging, outgoing packets from the virtual network adapter can be tagged with IEEE 802.1p priority. These priority tags can be used by Quality of Service (QoS) to prioritize traffic. If IEEE priority tagging is not allowed, the priority value in the packet is reset to 0. • **Allow guest specified IP addresses (only available for virtual machines on Windows Server 2012 R2)** (security setting): This option is available in VMM in System Center 2012 R2 only, and affects virtual machine networks (VM networks) that use Hyper-V network virtualization only. With this option, the virtual machine (guest) can add and remove IP addresses on this virtual network adapter. This can simplify the process of managing virtual

Networking item in VMM	Uses and settings
	machine settings. Guest-specified IP addresses are required for virtual machines that use guest clustering with network virtualization. The IP address that a guest adds must be within an existing IP subnet in the VM network. • **Bandwidth settings**: You can use the bandwidth settings in this type of port profile to specify the minimum and maximum bandwidth that are available to the adapter. The minimum bandwidth can be expressed as megabits per second (Mbps) or as a weighted value (from 0 to 100) that controls how much bandwidth the virtual network adapter can use in relation to other virtual network adapters.
Port classification	A port classification provides a global name for identifying different types of virtual network adapter port profiles. As a result, a classification can be used across multiple logical switches while the settings for the classification remain specific to each logical switch. For example, you might create one port classification that is named FAST to identify ports that are configured to have more bandwidth, and one port classification that is named SLOW to identify ports that are configured to have less bandwidth. You can use the port classifications that are provided in VMM, or you can create your own port classifications.
Logical switch	A logical switch brings port profiles, port classifications, and switch extensions together so that you can apply them consistently to network adapters on multiple host systems. Note that when you add an uplink port profile to a logical switch, this places the uplink port profile in a list of profiles that are available through that logical switch. When you apply the logical switch to a network adapter in a host, the uplink port profile is available in the list of

Networking item in VMM	Uses and settings
	profiles, but it is not applied to that network adapter until you select it from the list. This helps you to create consistency in the configurations of network adapters across multiple hosts, but it also makes it possible for you to configure each network adapter according to your specific requirements. To enable teaming of multiple network adapters, you can apply the same logical switch and uplink port profile to those network adapters and configure appropriate settings in the logical switch and uplink port profile. In the logical switch, for the **Uplink mode**, select **Team** to enable teaming. In the uplink port profile, select appropriate **Load-balancing algorithm** and **Teaming mode** settings (or use the default settings). For background information about load-balancing algorithms and teaming modes, see NIC Teaming Overview. **Switch extensions** (which you can install on the VMM management server and then include in a logical switch) allow you to monitor network traffic, use Quality of Service (QoS) to control how network bandwidth is used, enhance the level of security, or otherwise expand the capabilities of a switch. In VMM, four types of switch extensions are supported: • **Monitoring** extensions can be used to monitor and report on network traffic, but they cannot modify packets. • **Capturing** extensions can be used to inspect and sample traffic, but they cannot modify packets. • **Filtering** extensions can be used to block, modify, or defragment packets. They can also block ports. • **Forwarding** extensions can be used to direct traffic by defining destinations, and they can capture and filter traffic. To avoid conflicts, only one forwarding extension can

Networking item in VMM	Uses and settings
	be active on a logical switch.
Virtual switch extension manager or **Network manager**	A virtual switch extension manager (or network manager) makes it possible for you to use a vendor network-management console and the VMM management server together. You can configure settings or capabilities in the vendor network-management console—which is also known as the management console for a forwarding extension—and then use the console and the VMM management server in a coordinated way. To do this, you must ensure that the provider software (which might be included in VMM, or might need to be obtained from the vendor) is installed on the VMM management server. Then you must add the virtual switch extension manager or network manager to VMM, which enables the VMM management server to connect to the vendor network-management database and to import network settings and capabilities from that database. The result is that you can see those settings and capabilities, and all your other settings and capabilities, together in VMM. With System Center 2012 R2, settings can be imported into and also exported from VMM. That is, you can configure and view settings either in VMM or your network manager, and the two interfaces synchronize with each other.

Prerequisites

Before you configure ports, switches, and switch extensions for virtual machine networks (VM networks) in System Center 2012 SP1 or System Center 2012 R2, you must configure your logical networks and, optionally, load balancing. The logical networks form the foundation for networking configurations in VMM. For more information, see the following overviews:

- Configuring Logical Networking in VMM Overview
- (Optional) Configuring Load Balancing in VMM Overview

Also, before you configure ports, switches, and switch extensions, review the following table of prerequisites.

Configurable item	Prerequisite
Port profile for uplinks	Decide which logical networks you want to make available through the physical network adapters on your hosts. Also, if you want to enable teaming for multiple network adapters, decide whether you want to choose specific settings for the load-balancing algorithm and the teaming mode, or whether you want to use the default settings.
Port profile for virtual network adapters	Before you create a port profile for virtual network adapters, review the following guidelines: • If you want to enable VMQ, IPsec task offloading, or SR-IOV, review the requirements for these capabilities, as described in the Settings section, earlier in this topic. • Determine which security or bandwidth settings, if any, you want to use. For more information, see the Settings section, earlier in this topic.
Port classification	Decide how you want to classify ports in your networking environment. For more information, see the Settings section, earlier in this topic.
Logical switch, regardless of whether you use switch extensions	Decide how you want to combine port profiles and port classifications to provide consistent, useful settings on the network adapters in your virtualized environment. This will help you decide how to configure your logical switches. Also, decide whether you want to enable teaming for multiple network adapters to which you will apply the same logical switch.
Logical switch with virtual switch extensions from a vendor	Before you can add a virtual switch extension to a logical switch, you must install the provider software (provided by the vendor) on the VMM management server. For more information, refer to the documentation from the vendor. After you install the provider, restart the System Center Virtual Machine Manager service. When these steps are completed, in the **Extensions**

Configurable item	Prerequisite
	property of a logical switch, the virtual switch extension appears in the list of extensions that you can select.
Virtual switch extension manager or **Network manager**	Before you can add a virtual switch extension manager or network manager to VMM, you must ensure that the provider software is installed on the VMM management server. For most network managers, you must install the provider. The exception is with System Center 2012 R2 when the network manager is an IPAM server, in which case the provider is included in VMM. For more information, refer to the documentation from the vendor. After you install a provider, restart the System Center Virtual Machine Manager service. Then you can add the virtual switch extension manager or network manager as a resource in VMM.

In this section

The following topic provides illustrations of logical switches, port profiles, and port classifications:

- Configuring Ports and Switches in VMM Illustrated Overview

The following procedures can help you use VMM to configure uplink port profiles, virtual network adapter port profiles, logical switches, and switch extensions in System Center 2012 SP1 or System Center 2012 R2.

Procedure	Description
How to Create a Port Profile for Uplinks in VMM	Describes how to create a port profile for uplinks. Create port profiles before you create logical switches.
How to Create a Port Profile for Virtual Network Adapters in VMM	Describes how to create a port profile for virtual network adapters. Create port profiles before you create logical switches.
How to Create a Port Classification in VMM	Describes how to create a port classification. You can create port classifications either before or during the process of creating a logical switch.
How to Add a Virtual Switch Extension Manager in System Center 2012 SP1	Optional. Describes how to add a virtual switch extension manager in System Center 2012

Procedure	Description
	SP1. If you want to add a virtual switch extension manager, we recommend that you add it before you create your logical switch.
How to Add a Virtual Switch Extension or Network Manager in System Center 2012 R2	Optional. Describes how to add a virtual switch extension or a network manager in System Center 2012 R2. If you want to add a virtual switch extension or network manager, we recommend that you add it before you create your logical switch.
How to Create a Logical Switch in VMM	Describes how to create a logical switch to bring together port profiles, port classifications, and virtual switch extensions in ways that match your requirements. You can apply the logical switch as necessary to consistently configure the capabilities for network adapters across multiple hosts.
How to Configure Network Settings on a Host by Applying a Logical Switch in VMM	Describes how to bring together the network settings that you configured in port profiles and logical switches, by applying them to network adapters on a host. These adapters can be physical network adapters or virtual network adapters on the host. The host property through which you apply port profiles and logical switches is called a "virtual switch." This concept is the same concept as the Hyper-V Virtual Switch, which is described in Hyper-V Virtual Switch Overview.

Next steps after you configure port profiles and logical switches

For information about the next steps to take after you configure port profiles and logical switches, see Configuring VM Networks and Gateways in VMM.

Next steps after you configure networking

For information about the next steps to take after you configure networking, see the topics in the following table.

Topic	Step
Preparing the Fabric in VMM	Configure additional fabric resources, such as storage and library resources.

Topic	Step
Adding and Managing Hyper-V Hosts and Scale-Out File Servers in VMM Managing VMware ESX and Citrix XenServer in VMM	Configure hosts.
Creating and Deploying Virtual Machines and Services in VMM	Deploy virtual machines, individually or as part of a service.

See Also

Configuring Networking in VMM

Configuring Ports and Switches in VMM Illustrated Overview

How to Add a Top-of-Rack Switch in VMM in System Center 2012 R2

How to Add an IPAM Server in VMM in System Center 2012 R2

Configuring Ports and Switches in VMM Illustrated Overview

In Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1) or System Center 2012 R2, you can consistently configure identical capabilities for network adapters across multiple hosts by using logical switches in combination with other networking elements such as port profiles. Logical switches act as containers for the properties or capabilities that you want your network adapters to have. Instead of configuring individual properties or capabilities for each network adapter, you can specify the capabilities in a logical switch, which you can then apply to the appropriate adapters. This can simplify the configuration process.

The illustrations in this topic show how logical switches work with port profiles and other networking elements to help simplify the process of configuring network adapters on host systems. The illustrations represent logical switches in System Center 2012 SP1 and System Center 2012 R2.

For more details about ports and switches in VMM, see Configuring Ports and Switches for VM Networks in VMM.

For illustrations of other networking elements in VMM, see Configuring VM Networks in VMM Illustrated Overview.

Logical switches in VMM in System Center 2012 SP1 and System Center 2012 R2

The following illustration shows a single test system in the host group “Test systems” at the top. It also illustrates multiple hosts in host groups that are lower down in the illustration. For the single test system, the administrator has configured switch and port settings individually. For the host groups, a logical switch has been created, so that switch and port settings can be applied in consistent ways across host systems. Logical switches are available in VMM in System Center 2012 SP1 and System Center 2012 R2.

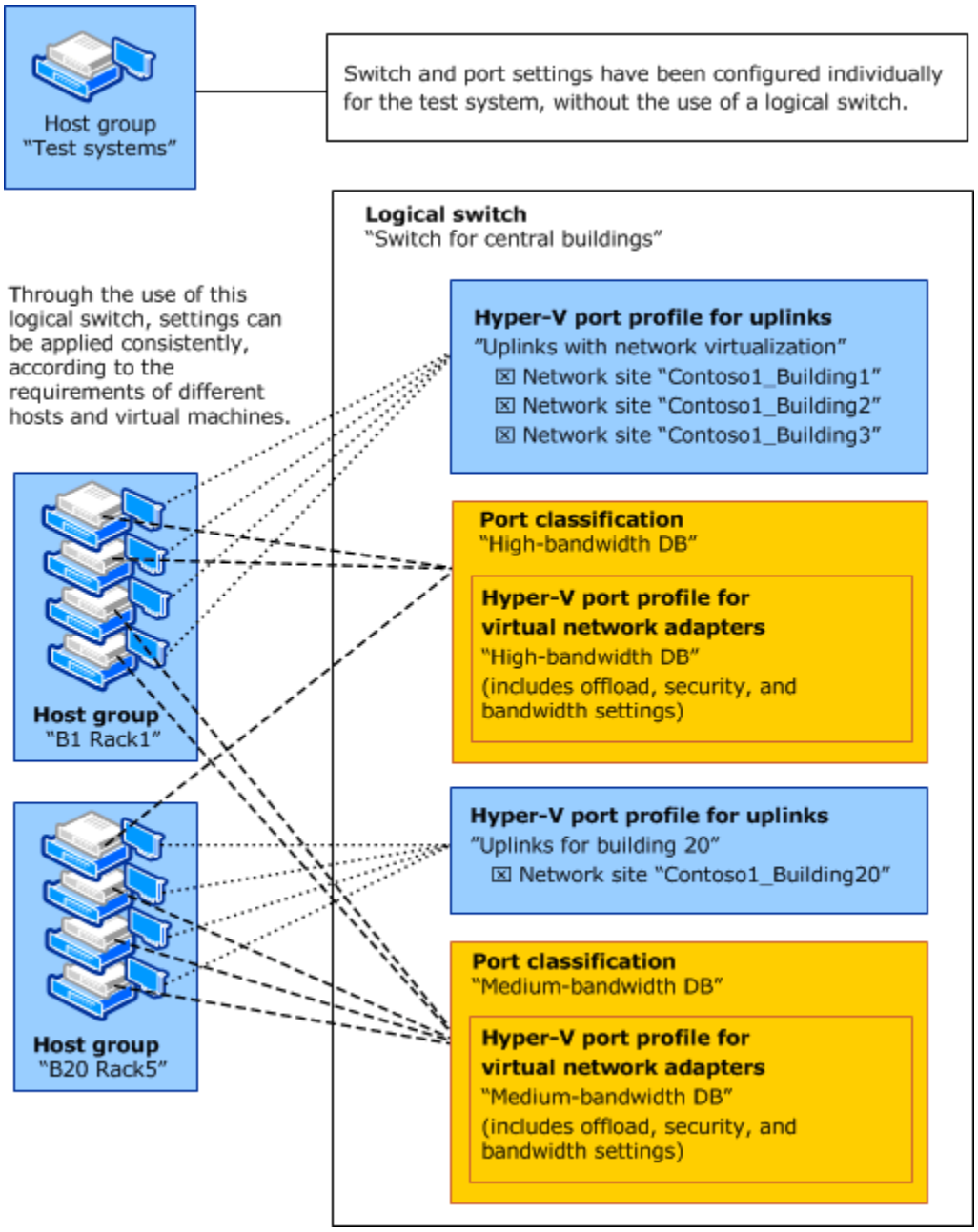


Figure 1 Logical switch

This illustration shows how a logical switch brings the following together so that you can apply them to multiple network adapters:

- Port profiles for uplinks (also called uplink port profiles)—for physical network adapters
- Port classifications—for virtual network adapters
- Port profiles for virtual network adapters

In the illustration, the logical switch contains a list of two uplink port profiles: “Uplinks with network virtualization” and “Uplinks for building 20.” (The list could contain more than two profiles.) When this logical switch is applied to a network adapter in a host system, the administrator can choose one of these uplink port profiles for that specific network adapter. The illustration indicates that the port profile called “Uplinks with network virtualization” has been applied to network adapters for a host group called “B1 Rack1” (which means building 1, rack 1). In contrast, the port profile called “Uplinks for building 20” has been applied to network adapters for a host group called “B20 Rack5” (building 20, rack 5).

Similarly, the logical switch contains two port classifications. Each port classification can contain one Hyper-V (native) port profile for virtual network adapters. The port classification called “High-bandwidth DB” (database) has been applied in some cases, and “Medium-bandwidth DB” has been applied in other cases.

A port classification in a logical switch can contain multiple switch extensions for virtual network adapters. The port classification identifies each switch extension, and it can also specify an extension port profile to use with that extension when it is used in that port classification. These additional elements are not shown in the illustration.

In the preceding illustration, the names of elements that you configure by running a wizard or opening a property sheet are shown in bold text, and elements that are on a page of the wizard or on a tab of the property sheet are shown without bold text.

Network object model for logical switches

The following illustration shows the network object model for logical switches in VMM in System Center 2012 SP1 and System Center 2012 R2. This illustration shows the relationships among network objects only, rather than indicating information about the wizards and property sheets through which the objects are configured in the VMM console. The illustration can be especially useful if you are learning about configuring VMM through Windows PowerShell scripts, which reflect the network object models directly.

For some objects in the illustration, sample names such as “Switch for central buildings” and “High-bandwidth DB” are included to help illustrate the purpose of those objects. Two of the objects, the **Set of uplink port profiles** and the **Set of port profiles for virtual network adapters**, are visible in Windows PowerShell, but not in the VMM console.

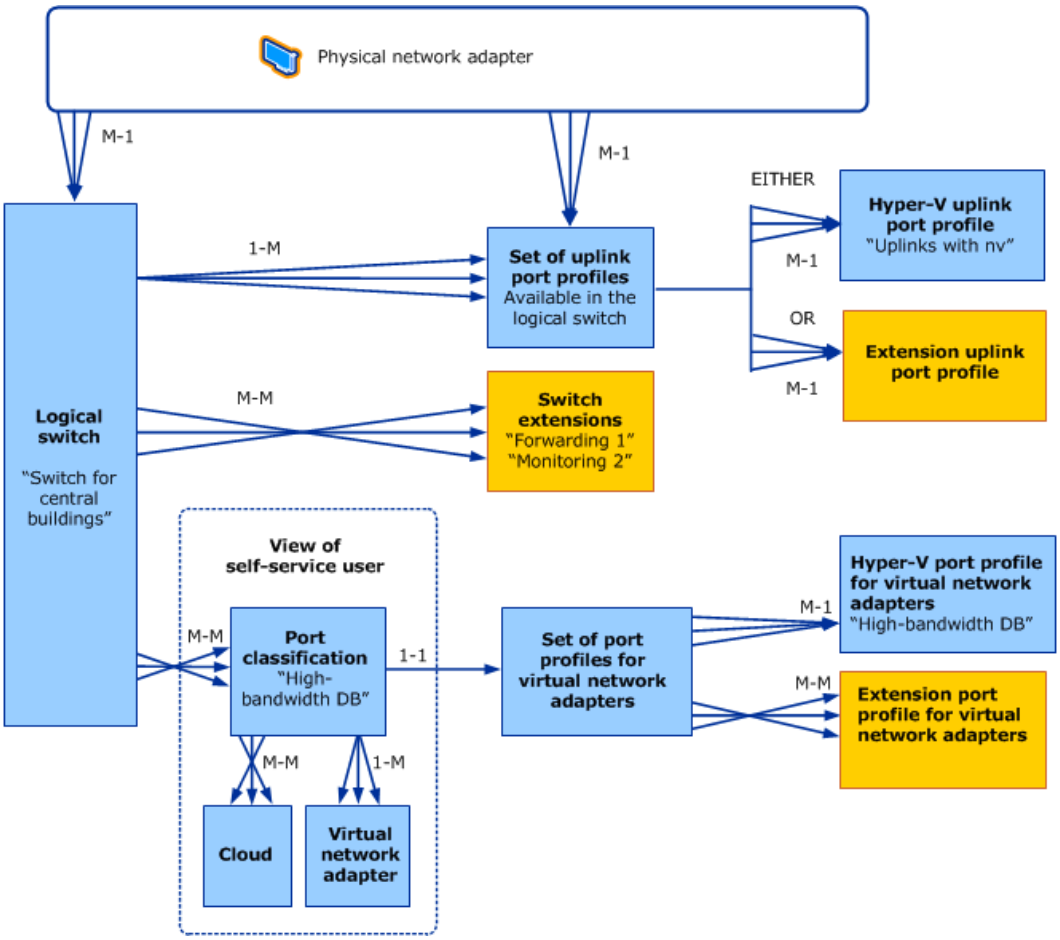


Figure 2 Object model for logical switches

As indicated in the illustration, the view of the self-service user includes only port classifications, not other port or switch objects. By choosing a port classification, for example, "High-bandwidth DB," the self-service user can easily choose an appropriate collection of settings for a particular virtual network adapter. Port classifications are created by a fabric administrator or tenant administrator, and they are made available in the cloud.

The following key explains the notations on the arrows:

- **1-1** means "one-to-one."
- **1-M** means "one-to-many."
- **M-1** means "many-to-one."
- **M-M** means "many-to-many."

In the preceding illustration, bold text is used for each VMM object name, regardless of how that object is configured through the VMM console.

See Also

Configuring Logical Networking in VMM Overview

Configuring Ports and Switches for VM Networks in VMM

Configuring VM Networks and Gateways in VMM

Configuring VM Networks in VMM Illustrated Overview

Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2

How to Create a Port Profile for Uplinks in VMM

In Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1) or System Center 2012 R2, you can consistently configure identical capabilities for network adapters across multiple hosts by using port profiles and logical switches. Port profiles and logical switches act as containers for the properties or capabilities that you want your network adapters to have. Instead of configuring individual properties or capabilities for each network adapter, you can specify the capabilities in port profiles and logical switches, which you can then apply to the appropriate adapters.

Important

For information about prerequisites and settings for port profiles and logical switches, see Configuring Ports and Switches for VM Networks in VMM.

The recommended sequence for creating port profiles and logical switches is to create the port profiles first. You will need at least one port profile for uplinks before you can create a logical switch.

Use the following procedure to create a port profile for uplinks in VMM in System Center 2012 SP1 or System Center 2012 R2.

To create a port profile for uplinks

1. Open the **Fabric** workspace.
2. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
3. In the **Fabric** pane, expand **Networking**, and then click one of the following:
   - For System Center 2012 SP1: **Native Port Profiles**
   - For System Center 2012 R2: **Port Profiles**
4. On the **Home** tab, in the **Create** group, click **Create**, and then click one of the following:
   - For System Center 2012 SP1: **Native Port Profile**
   - For System Center 2012 R2: **Hyper-V Port Profile**

   The wizard for creating port profiles opens.
5. On the **General** page, enter a name and optional description for the port profile, and then select **Uplink port profile**. If you plan to enable teaming in the logical switch that includes this uplink port profile, select options for load balancing and teaming, or use the default options. Note that if you do not enable teaming in the logical switch, these options will have no effect.

   Note

   For more information about the options in the list that follows, see NIC Teaming Overview.

   The options for load balancing and teaming are as follows:

Load-balancing algorithm: the algorithm that the team uses to distribute network traffic between the network adapters. The following options are available:

- **Hyper-V Port**: Distributes network traffic based on the Hyper-V switch port identifier of the source virtual machine. This is the default algorithm.
- **Transport Ports**: Uses the source and destination TCP ports and the IP addresses to create a hash and then assigns the packets that have that hash value to one of the available network adapters.
- **IP Addresses**: Uses the source and destination IP addresses to create a hash and then assigns the packets that have that hash value to one of the available network adapters.
- **Mac Addresses**: Uses the source and destination MAC addresses to create a hash and then assigns the packets that have that hash value to one of the available network adapters.
- **Dynamic** (in VMM in System Center 2012 R2 only): Uses the dynamic load balancing that is available in Windows Server® 2012 R2 only.
- **Host default** (in VMM in System Center 2012 R2 only): This specifies the **Dynamic** algorithm for hosts that support it, and the **Hyper-V Port** algorithm for hosts that do not.

Teaming mode: the mode of the NIC teaming. The following options are available:

- **Switch Independent**: Specifies that a network switch configuration is not needed for the NIC team. Because the network switch is not configured to know about the interface teaming, the team interfaces can be connected to different switches. This is the default mode.
- **LACP**: Uses the Link Aggregation Control Protocol (LACP) from IEEE 802.1ax (also known as IEEE 802.3ad) to dynamically identify links that are connected between the host and a given switch.
- **Static Teaming**: Requires configuration on both the switch and the host to identify which links form the team.

After you have completed all settings, click **Next**.

6. On the **Network configuration** page, do the following:
   - Select one or more network sites for this uplink port profile to support.
   - If you want to enable network virtualization (which allows you to deploy multiple VM networks on the same physical network), select the appropriate check box:
     - In VMM in System Center 2012 SP1, select **Enable Windows Network Virtualization**.
     - In VMM in System Center 2012 R2, select **Enable Hyper-V Network Virtualization**.

     Note
     The setting for enabling network virtualization requires a logical network on which you have selected **Allow new VM networks created on this logical network to use network virtualization**.

- After you have completed all settings, click **Next**.

7. On the **Summary** page, review and confirm the settings, and then click **Finish**.

After you create an uplink port profile, the next step is to add it to a logical switch, which places it in a list of profiles that are available through that logical switch. When you apply the logical switch to a network adapter in a host, the uplink port profile is available in the list of profiles, but it is not applied to that network adapter until you select it from the list. This helps you to create consistency in the configurations of network adapters across multiple hosts, but also enables you to configure each network adapter according to your specific requirements.

See Also

Configuring Ports and Switches for VM Networks in VMM

How to Create a Logical Network in VMM

How to Create a Logical Switch in VMM

Configuring Networking in VMM

How to Create a Port Profile for Virtual Network Adapters in VMM

In Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1) and System Center 2012 R2, you can consistently configure identical capabilities for network adapters across multiple hosts by using port profiles and logical switches. Port profiles and logical switches act as containers for the properties or capabilities that you want your network adapters to have. Instead of configuring individual properties or capabilities for each network adapter, you can specify the capabilities in port profiles and logical switches, which you can then apply to the appropriate adapters.

Important

For information about prerequisites and settings for port profiles and logical switches, see the “Settings” section in Configuring Ports and Switches for VM Networks in VMM. It is especially important to review the prerequisites if you plan to enable virtual machine queue (VMQ), IPsec task offloading, or single-root I/O virtualization (SR-IOV) in your port profile for virtual network adapters.

The recommended sequence for creating port profiles and logical switches is to create the port profiles first.

Use the following procedure to create a port profile for virtual network adapters.

To create a port profile for virtual network adapters

1. Open the **Fabric** workspace.
2. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
3. In the **Fabric** pane, expand **Networking**, and then click one of the following:
   - For System Center 2012 SP1: **Native Port Profiles**
   - For System Center 2012 R2: **Port Profiles**
4. On the **Home** tab, in the **Create** group, click **Create**, and then click one of the following:
   - For System Center 2012 SP1: **Native Port Profile**

- For System Center 2012 R2: **Hyper-V Port Profile**

The wizard for creating port profiles opens.

5. On the **General** page, enter a name and optional description for the port profile, click **Virtual network adapter port profile**, and then click **Next**.
6. On the **Offload Settings** page, optionally select one or more of the following settings, and then click **Next**. For more information about the settings listed in this step or the next step, in Configuring Ports and Switches for VM Networks in VMM, in the "Settings" section, see the "Native port profile for virtual network adapters" row in the table.
   - **Enable virtual machine queue**
   - **Enable IPsec task offloading**
   - **Enable Single-root I/O virtualization**
7. On the **Security Settings** page, optionally select one or more of the following settings, and then click **Next**.
   - **Allow MAC spoofing**
   - **Enable DHCP guard**
   - **Allow router guard**
   - **Allow guest teaming**
   - **Allow IEEE priority tagging**

   With System Center 2012 R2, you can also select the following setting:
   - **Allow guest specified IP addresses (only available for virtual machines on Windows Server 2012 R2)**
8. On the **Bandwidth Settings** page, optionally specify bandwidth settings for the virtual network adapter.
   - **Minimum bandwidth (Mbps)**: Specify the minimum bandwidth here in megabits per second (Mbps), or use the **Minimum bandwidth weight** option (described later in this list).
   - **Maximum bandwidth (Mbps)**: Specify the maximum bandwidth, using a value no greater than 100,000 Mbps. A value of 0 Mbps means the maximum is not configured.
   - **Minimum bandwidth weight**: Specify a weighted value from 0 to 100 that controls how much bandwidth the virtual network adapter can use in relation to other virtual network adapters.

   Note
   Bandwidth settings are not used when SR-IOV is enabled on the port profile and on the logical switch that specifies the port profile.
9. On the **Summary** page, review and confirm the settings, and then click **Finish**.

See Also

Configuring Ports and Switches for VM Networks in VMM

Configuring Networking in VMM

How to Create a Port Classification in VMM

In Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1) and System Center 2012 R2, port classifications provide global names for identifying different types of virtual network adapter port profiles. A port classification can be used across multiple logical switches while the settings for the port classification remain specific to each logical switch. For example, you might create one port classification named FAST to identify ports that are configured to have more bandwidth, and another port classification named SLOW to identify ports that are configured to have less bandwidth.

For more information about port profiles, port classifications, and logical switches, see Configuring Ports and Switches for VM Networks in VMM.

Use the following procedure to create a port classification.

Note

You can also create a new port classification from within the Create Logical Switch Wizard.

To create a port classification

1. Open the **Fabric** workspace.
2. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
3. In the **Fabric** pane, expand **Networking**, and then click **Port Classifications**.
4. On the **Home** tab, in the **Create** group, click **Create**, and then click **Port Classification**.

   The Create Port Classification Wizard opens.
5. On the **Name** page, enter a name and optional description for the port classification, and then click **OK**.

See Also

Configuring Ports and Switches for VM Networks in VMM

Configuring Networking in VMM

How to Create a Logical Switch in VMM

How to Add a Virtual Switch Extension Manager in System Center 2012 SP1

With System Center 2012 Service Pack 1 (SP1), if you add a virtual switch extension manager to Virtual Machine Manager (VMM), you can use a vendor network-management console and the VMM management server together. You can configure settings or capabilities in the vendor network-management console—also known as the management console for a forwarding extension—and then use the console and the VMM management server in a coordinated way.

To do this, you must first install the provider software (provided by the vendor) on the VMM management server. Then you can add the virtual switch extension manager to VMM, which will cause the VMM management server to connect to the vendor network-management database and import network settings and capabilities from that database. The result is that you can see those settings and capabilities, and all your other settings and capabilities, together in VMM.

Important

This topic describes how you can add a virtual switch extension manager to the list of resources in VMM in System Center 2012 SP1 only. For information about how to add a virtual switch extension manager to the list of resources in VMM in System Center 2012 R2, see How to Add a Virtual Switch Extension or Network Manager in System Center 2012 R2.

For more information about how virtual switch extension managers fit into the context of logical switches and other networking configuration elements in VMM, see the descriptions of “Logical switch” and “Virtual switch extension manager” in the settings table in Configuring Ports and Switches for VM Networks in VMM.

Prerequisites

Before adding a virtual switch extension manager to VMM, you must first obtain provider software from your vendor, install the provider on the VMM management server, and then restart the System Center Virtual Machine Manager service. If you have installed a highly available VMM management server, be sure to install the provider software on all nodes of the cluster. For more information about provider software, refer to the vendor’s documentation.

To add a virtual switch extension manager

1. Confirm that you have installed the necessary provider software. To do this, open the **Settings** workspace, and in the **Settings** pane, click **Configuration Providers**. In the **Configuration Providers** pane, review the list of installed provider software.
2. Open the **Fabric** workspace.
3. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
4. In the **Fabric** pane, expand **Networking**, and then click **Switch Extension Managers**.
5. On the **Home** tab, in the **Add** group, click **Add resources**, and then click **Virtual Switch Extension Manager**.

   The **Add Virtual Switch Extension Manager Wizard** opens.
6. On the **General** page, do the following:
   - In the **Manufacturer** list, select a provider manufacturer, in the **Model** list, select a model, and then, in the **Provider** list, select a provider.
   - In the **Connection string** box, type the connection string for the virtual switch extension manager to use.

     For example, you might enter the connection string **myextmanager1.contoso.com:443**.

     Important
     The syntax of the connection string is defined by the manufacturer of the virtual switch extension manager. For more information about the required syntax, refer to the manufacturer’s documentation.
   - Next to the **RunAs account** box, click **Browse** and, in the **Select a Run As account** dialog box, select an account, or click **Create Run As Account** to create a new account, and then click **OK**.

- After you have completed all settings, click **OK**.

7. On the **Host Groups** page, select the check box for one or more host groups to which you want the virtual switch extension manager to be available. You must select at least one host group. Click **Next** to proceed.
8. On the **Summary** page, review and confirm the settings, and then click **Finish**.
9. Verify that the virtual switch extension manager appears in the **Virtual Switch Extension Managers** pane.

See Also

Configuring Ports and Switches for VM Networks in VMM

Configuring Networking in VMM

How to Create a Logical Switch in VMM

How to Add a Virtual Switch Extension or Network Manager in System Center 2012 R2

How to Add a Virtual Switch Extension or Network Manager in System Center 2012 R2

With System Center 2012 R2, if you add a virtual switch extension or network manager to Virtual Machine Manager (VMM), you can use the console for that virtual switch extension or network manager in a way that is coordinated with the VMM management server. This helps you keep the settings that you see in VMM synchronized with the settings that you configured through an interface other than VMM.

To do this, you must first install the provider software (provided by the vendor) on the VMM management server. Then you can add the virtual switch extension or network manager to VMM.

Important
This topic describes how you can add a virtual switch extension or network manager to the list of resources in VMM in System Center 2012 R2 only. For information about how to add a virtual switch extension manager to the list of resources in VMM in System Center 2012 SP1, see How to Add a Virtual Switch Extension Manager in System Center 2012 SP1.

Use the following procedure to add a virtual switch extension or network manager to VMM in System Center 2012 R2.

Prerequisites

If you want to add a virtual switch extension or network manager to your configuration in VMM, you must first perform the following tasks:

1. Obtain provider software from the manufacturer of the virtual switch extension or network manager, install the provider on the VMM management server, and then restart the System Center Virtual Machine Manager service. If you have installed a high-availability VMM management server on a cluster, be sure to install the provider on all nodes of the cluster. For more information about installing the provider, refer to the manufacturer's documentation.
2. For your virtual switch extension or network manager, make sure that you know the manufacturer and model, the name of an account that has configuration permissions, the connection string, and the host groups to include. If certificates are used for the provider software, make sure you know how to view the thumbprint information for those certificates.

To add a virtual switch extension or network manager in System Center 2012 R2

1. Confirm that you have installed the necessary provider software. To do this, open the **Settings** workspace, and in the **Settings** pane, click **Configuration Providers**. In the **Configuration Providers** pane, review the list of installed provider software.
2. Open the **Fabric** workspace.
3. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
4. In the **Fabric** pane, expand **Networking**, and then click **Network Service**.

   Network services include gateways, virtual switch extensions, network managers, and top-of-rack (TOR) switches.
5. On the **Home** tab, in the **Add** group, click **Add Resources**, and then click **Network Service**.

   The Add Network Service Wizard opens.
6. On the **Name** page, type a name and optional description for the virtual switch extension or network manager, and then click **Next**.
7. On the **Manufacturer and Model** page, in the **Manufacturer** list, select a provider manufacturer, in the **Model** list, select a model, and then click **Next**.
8. On the **Credentials** page, either click **Browse** and then on the **Select a Run As Account** dialog box, select an account, or click **Create Run As Account** and create a new account. Then click **Next**.
9. On the **Connection String** page, in the **Connection string** box, type the connection string that is used by the virtual switch extension or network manager, and then click **Next**.

   For example, you might enter the connection string **mynetworkmanager1.contoso.com:443**.

   Important

   The syntax of the connection string is defined by the manufacturer of the virtual switch extension or network manager. For more information about the required syntax, refer to the manufacturer's documentation.
10. If the **Certificates** page appears and certificates are listed, verify that the thumbprints of those certificates match the thumbprints of the certificates that are installed on the virtual switch extension or network manager. Then select the check box to confirm that the certificates can be imported to the trusted certificate store. Click **Next**.

    Note

    If no certificates are listed, the connection string that was provided probably does not require certificates, and you can continue to the next page of the wizard. However, if no certificates are listed but your virtual switch extension or network manager requires them, confirm that the certificates were installed correctly on your device. Then, to refresh the display on the **Certificates** page of the wizard, click **Previous** and then click **Next**.

11. On the **Provider** page, in the **Configuration provider** list, select an available provider, and then click **Test** to use the selected provider to run basic validation tests against the virtual switch extension or network manager. If the tests indicate that the provider works as expected, click **Next**.

    Results that say **Passed** or **Failed** indicate whether the provider works as expected. One possible cause of failure is insufficient permissions in the Run As account. Results that say **Implemented** and **Not implemented** are informational only, and indicate whether the provider supports a particular API.
12. On the **Host Group** page, select one or more host groups to which the virtual switch extension or network manager will be available.
13. On the **Summary** page, review and confirm the settings, and then click **Finish**.

See Also

Configuring VM Networks and Gateways in VMM

How to Add a Top-of-Rack Switch in VMM in System Center 2012 R2

How to Add an IPAM Server in VMM in System Center 2012 R2

Configuring Networking in VMM

How to Add a Virtual Switch Extension Manager in System Center 2012 SP1

How to Create a Logical Switch in VMM

In Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1) or System Center 2012 R2, you can consistently configure identical capabilities for network adapters across multiple hosts by using port profiles and logical switches. Port profiles and logical switches act as containers for the properties or capabilities that you want your network adapters to have. Instead of configuring individual properties or capabilities for each network adapter, you can specify the capabilities in port profiles and logical switches, which you can then apply to the appropriate adapters.

Important

For information about prerequisites and options for port profiles and logical switches, see Configuring Ports and Switches for VM Networks in VMM. It is especially important to review the prerequisites if you plan to enable single-root I/O virtualization (SR-IOV) in your logical switch.

Note

To configure network host adapter settings and create virtual switches and virtual network adapters using Logical Switches through the use of Windows PowerShell, see Bare Metal Deploy through VMM PowerShell (Part 1), Bare Metal Deploy through VMM PowerShell (Part 2), and Hyper-V Host Network Settings through VMM PowerShell (Part 3)

The recommended order for creating port profiles and logical switches is to create the port profiles first. You will need at least one native port profile for uplinks before you can create a logical switch.

Account requirements To complete this procedure, you must be a member of the Administrator or the Delegated Administrator user role. When configuring the switch, delegated administrators can select only uplink port profiles that contain network sites that are in the administrative scope of the delegated administrator.

To create a logical switch

1. Open the **Fabric** workspace.
2. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
3. In the **Fabric** pane, expand **Networking**, and then click **Logical Switches**.
4. On the **Home** tab, in the **Create** group, click **Create Logical Switch**.

   The Create Logical Switch Wizard opens.
5. On the **Getting Started** page, review the information about logical switches, and then click **Next**.
6. On the **General** page, enter a name and optional description for the logical switch. If you want to enable single root I/O virtualization (SR-IOV), select the **Enable single root I/O virtualization (SR-IOV)** check box. Then click **Next**.

   Important
   SR-IOV enables virtual machines to bypass the switch and directly address the physical network adapter. To fully enable SR-IOV, you must also do the following:

   - Make sure that you have SR-IOV support in the host hardware and firmware, the physical network adapter, and drivers in the management operating system and in the guest operating system.
   - Create a native port profile for virtual network adapters that is also SR-IOV enabled.
   - When you configure networking settings on the host (in the host property called **Virtual switches**), attach the native port profile for virtual network adapters to the virtual switch by using a port classification. You can use the SR-IOV port classification that is provided in VMM, or create your own port classification.
7. If you are using (optional) virtual switch extensions, on the **Extensions** page, select the boxes for one or more extensions, and then arrange the order in which the extensions should be processed by clicking **Move Up** and **Move Down**. Then click **Next**.

   If an extension that you expected does not appear in the list, it is likely that the provider software has not been installed on the VMM management server. For more information about how to install a provider, refer to the documentation from the vendor.

   Important
   To avoid conflicts between extensions, only one forwarding extension can be selected at a time.

   Extensions process network traffic through the switch in the order that they are listed.
8. On the **Uplink** page, do the following:

- To configure teaming for multiple network adapters by applying this logical switch to multiple adapters, for **Uplink mode**, select **Team**. Otherwise, leave the selection as **No Uplink Team**.

  If you select **Team**, when you apply this logical switch with an uplink port profile, you will also apply two settings that are specified in the uplink port profile: the load-balancing algorithm and teaming mode settings.
- To add an uplink port profile, click **Add** and in the **Add Uplink Port Profile** dialog box, select a port profile. Then click **OK**. Repeat this process until you have added all of the uplink port profiles that you want to add.

  When you add an uplink port profile, it is placed in a list of profiles that are available through that logical switch. However, when you apply the logical switch to a network adapter in a host, the uplink port profile is applied to that network adapter only if you select it from the list of available profiles.
- To remove an uplink port profile, select the profile and then click **Remove**.

After you have completed all settings, click **Next**.

9. On the **Virtual Port** page, add one or more port classifications (which make it easy to see the intended uses for a switch), with or without the associated virtual network adapter port profiles (which add capabilities to the logical switch). Optionally, you can skip this step and then add these items later.

   To add a port classification, click **Add**, and then, in the **Add Virtual Port** dialog box, do the following:

   a. Click **Browse**.

   b. Either select a port classification or click **Create Port Classification** and specify a name and optional description for the port classification. Click **OK** until you have returned to the **Add Virtual Port** dialog box.

   c. While you are still in the **Add Virtual Port** dialog box, to include a virtual network adapter port profile, select the check box, and then in the **Native virtual network adapter port profile** list, select the port profile that you want to include.

   d. To close the dialog box and return to the **Virtual Port** page, click **OK**.

   As needed, repeat the process of adding port classifications.

10. Still on the **Virtual Port** page, to set one port classification as the default, select that classification and then click **Set Default**. To clear a default setting from the list of port classifications, click **Clear Default**.

    After you have completed all settings on the page, click **Next**.

11. On the **Summary** page, review and confirm the settings, and then click **Finish**.

    The **Jobs** dialog box appears. Make sure that the job has a status of **Completed**, and then close the dialog box.

12. Verify that the logical switch appears in the **Logical Switches** pane.

See Also

How to Configure Network Settings on a Host by Applying a Logical Switch in VMM

Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2

Configuring Ports and Switches in VMM Illustrated Overview

Configuring Ports and Switches for VM Networks in VMM

Configuring Networking in VMM

How to Configure Network Settings on a Host by Applying a Logical Switch in VMM

You can use the procedures in this topic to configure network adapters on Hyper-V hosts in System Center 2012 Service Pack 1 (SP1) or System Center 2012 R2, by applying a logical switch and port profiles to the adapters. Before you use the procedures, you must configure the logical switch and port profiles that you will apply. The network adapters that you configure can be physical network adapters or virtual network adapters on the hosts.

This topic describes one way of configuring network adapters on hosts, but there are other topics that describe different ways, as outlined in the following table:

If you have...	And you want to...	Follow steps in...
System Center 2012 SP1 or System Center 2012 R2	Assign the same logical networks and other network settings consistently to multiple network adapters across multiple hosts by using the VMM console	This topic
System Center 2012 SP1 or System Center 2012 R2	Assign the same logical networks and other network settings consistently to multiple network adapters during bare-metal provisioning of hosts by using Windows PowerShell	Bare Metal Deploy through VMM PowerShell (Part 1) Bare Metal Deploy through VMM PowerShell (Part 2) Hyper-V Host Network Settings through VMM PowerShell (Part 3) For background, see End-to-End Bare-Metal Provisioning with SCVMM 2012 SP1/R2
System Center 2012	Assign logical networks to a physical network adapter	How to Configure Network Settings on a Hyper-V Host in VMM
System Center 2012 SP1 or System Center 2012 R2	Assign logical networks manually to each physical network adapter	How to Configure Network Settings on a Hyper-V Host in VMM

Do the tasks in this topic in this order:

1. Specify whether a network adapter is used for virtual machines, host management, neither, or both
2. Configure network settings on a host by applying a logical switch

After you perform the procedures in this topic, as a best practice, review the procedures in How to View Host Network Adapter Settings and Increase Compliance with Logical Switch Settings in VMM.

Specify whether a network adapter is used for virtual machines, host management, neither, or both

Regardless of any port profiles and logical switches you are using in your network configuration, you must specify whether a network adapter in a host is used for virtual machines, host management, neither, or both. (The host must already be under management in VMM.)

To specify whether a network adapter is used for virtual machines, host management, neither, or both

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, expand **All Hosts**, and then locate and click the host group where the host resides.
3. In the **Hosts** pane, click the host that you want to configure.
4. On the **Host** tab, in the **Properties** group, click **Properties**.
5. In the *Host Name* **Properties** dialog box, click the **Hardware** tab.
6. Under **Network adapters**, click the physical network adapter that you want to configure. If you want to use this network adapter for virtual machines, ensure that **Available for placement** is checked. If you want to use this network adapter for communication between the host and the VMM management server, ensure that **Used by management** is checked.

Important

- You must make sure that you have at least one network adapter available for communication between the host and the VMM management server. Make sure that **Used by management** is checked for this network adapter.
- If you have already applied a logical switch and an uplink port profile to a network adapter, if you click **Logical network connectivity**, you can see the resulting connectivity. However, if you plan to apply a logical switch and an uplink port profile, do not make individual selections in **Logical network connectivity**. Instead, use the following procedure.

Configure network settings on a host by applying a logical switch

Before you begin the following procedure, make sure you have configured the building blocks that are needed in the procedure, including logical networks, port profiles, and logical switches. For more information, see Configuring Ports and Switches for VM Networks in VMM. If you want to configure single-root I/O virtualization (SR-IOV) for network adapters on the host, it's especially important to review the "Settings" section in that topic, because SR-IOV has specific requirements.

To configure network settings on a host by applying a logical switch

1. Open the **Fabric** workspace.

2. In the **Fabric** pane, expand **Servers**, expand **All Hosts**, and then locate and click the host group that contains the host.
3. In the **Hosts** pane, click the host that you want to configure.
4. On the **Host** tab, in the **Properties** group, click **Properties**.
5. In the *Host Name* **Properties** dialog box, click the **Virtual Switches** tab.
6. On the **Virtual Switches** tab, do the following:
   a. Select an existing logical switch from the list, or click **New Virtual Switch** and then click **New Logical Switch**.
   b. In the **Logical switch** list, select the logical switch that you want to use.
   c. Under **Adapter**, select the physical adapter that you want to apply the logical switch to.
   d. In the **Uplink Port Profile** list, select the uplink port profile that you want to apply. The list contains the uplink port profiles that have been added to the logical switch that you selected. If a profile seems to be missing, review the configuration of the logical switch and then return to this property tab.
   e. As needed, repeat the steps for applying a new logical switch.

      Important
      If you apply the same logical switch and uplink port profile to two or more adapters, the two adapters might be teamed, depending on a setting in the logical switch. To find out if they will be teamed, open the logical switch properties, click the **Uplink** tab, and view the **Uplink mode** setting. If the setting is **Team**, the adapters will be teamed. The specific mode in which they will be teamed is determined by a setting in the uplink port profile.
   f. When you have finished configuring settings, click **OK**.

      Caution
      While VMM creates the virtual switch, the host may temporarily lose network connectivity. This may have an adverse effect on other network operations in progress.

The following tips may also be useful:

Tip
Network optimizations: VMM can detect whether the operating system on your host provides the network optimizations called Virtual Machine Queue (VMQ) or TCP Chimney Offload. If VMM detects either of them, it displays a message saying **Network optimization is available**. Look for the message in the **Host Properties** dialog box, on the **Virtual Switches** tab.

For more information, see Using TCP Chimney Offload and Using Virtual Machine Queue. For information about these network optimizations in the context of VMM, see the “Network Optimization Support” section in Configuring Virtual Networks in VMM (which describes the optimizations in an earlier version of VMM).

Tip

Compliance of network settings: After you apply logical switches, you can later check to see if the network adapter settings on a host are still in compliance with the logical switch settings. If they're not, you can use VMM to bring them back into compliance. For more information, see How to View Host Network Adapter Settings and Increase Compliance with Logical Switch Settings in VMM.

See Also

Configuring Ports and Switches for VM Networks in VMM

Configuring Ports and Switches in VMM Illustrated Overview

Configuring Networking in VMM

Adding Hyper-V Hosts and Host Clusters, and Scale-Out File Servers to VMM

Managing VMware ESX and Citrix XenServer in VMM

How to Configure Network Settings on a Hyper-V Host in VMM

How to Add a Top-of-Rack Switch in VMM in System Center 2012 R2

How to Configure Global Network Settings in VMM

How to View Host Network Adapter Settings and Increase Compliance with Logical Switch Settings in VMM

In Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1) and System Center 2012 R2, you can review and control the configuration of virtual switches that have been created from logical switches. When such a virtual switch is first created, it complies with the settings that are configured in the logical switch. However, the settings on either the virtual switch or the logical switch might later be changed, resulting in a virtual switch that is out of compliance with the corresponding logical switch. VMM provides a straightforward way to see whether a virtual switch is out of compliance, and then to bring the virtual switch back into compliance. Bringing a virtual switch into compliance is also called remediating the virtual switch.

To view host network adapter settings and increase compliance with logical switch settings

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Networking**, and then click **Logical Switches**.
3. On the **Home** tab, in the **Show** group, click **Hosts**.
4. In the **Logical Switch Information for Hosts** pane, view the listings for network adapters and switches.
5. Expand or collapse the listings as needed, and click an individual virtual switch for which you want to see more information.
6. In the **Network Compliance** column, view the compliance status.
   - A value of **Fully compliant** indicates that the settings on the virtual machine host are consistent with the configuration in VMM. For example, **Fully compliant** indicates that all IP subnets and VLANs that are included in the network site are assigned to

the network adapter.

- A value of **Partially compliant** indicates that there is only a partial match between the settings on the host and the configuration in VMM.

  In the results pane, the **Logical network information** section lists the assigned IP subnets and VLANs for the network adapter. If an adapter is partially compliant, you can view the reason in the **Compliance errors** section.

- A value of **Non compliant** indicates that the settings on the host are missing from the configuration in VMM. For example, **Non compliant** indicates that none of the IP subnets and VLANs that are defined for the logical network are assigned to the physical adapter. If an adapter is non compliant, you can view the reason in the **Compliance errors** section.

Tip

In addition to the compliance information, you can also view detailed information about the network adapter, such as the assigned IP address and media access control (MAC) address.

7. To bring a non-compliant virtual switch into compliance, click the virtual switch and, in the **Network Compliance** group, click **Remediate**. If possible, VMM will bring the virtual switch into compliance.

   If you use failover clustering, you might have to review compliance and perform remediation for virtual switches on all nodes of the cluster.

See Also

Configuring Networking in VMM

Configuring VM Networks in VMM Illustrated Overview

How to Configure Network Settings on a Host by Applying a Logical Switch in VMM

Configuring Ports and Switches in VMM Illustrated Overview

Configuring VM Networks and Gateways in VMM

Networking in Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1) and System Center 2012 R2 includes a number of enhancements that provide administrators with greater flexibility in configuring networks in a virtualized environment. This overview describes two of the enhancements, virtual machine networks (VM networks) and gateways.

Important

- For more information about the ways that you can use VM networks, switch extensions, and other networking options to support your virtual machine configurations, see Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2.
- For illustrations of VM networks, see Configuring VM Networks in VMM Illustrated Overview.
- In System Center 2012 SP1 and System Center 2012 R2, many of the VMM networking enhancements are based on Hyper-V network virtualization, which was introduced in Windows Server 2012. To understand these networking enhancements, it can be useful to review the illustrations and descriptions, especially the first illustration, of Hyper-V network virtualization in Network Virtualization technical details.

The following list describes VM networks and gateways:

- **VM networks:** VM networks enable you to use network virtualization, which extends the concept of server virtualization to make it possible to deploy multiple virtual networks (VM networks) on the same physical network. However, VM networks can be configured in multiple ways:
  - **Network virtualization (Hyper-V network virtualization):** If you want to support multiple tenants (also called clients or customers) with their own networks, isolated from the networks of others, use network virtualization. To use network virtualization, create a logical network, and on top of that logical network, create multiple VM networks, each of which uses the network virtualization option:
    - In System Center 2012 SP1: **Isolate using Hyper-V network virtualization**
    - In System Center 2012 R2: **One connected network** and **Allow new VM networks created on this logical network to use network virtualization**

    With this isolation, your tenants can use any IP addresses that they want for their virtual machines, regardless of the IP addresses that are used on other VM networks. Also, you can enable your tenants to configure some aspects of their own networks, based on limits that you specify.

    Note
    Network virtualization is supported only on hosts that are running Windows Server 2012 or Windows Server 2012 R2. Hosts that are running Windows Server 2008 R2 do not support network virtualization.
  - **VLAN-based configuration:** If you are working with networks that use familiar virtual local area network (VLAN) technology for network isolation, you can manage those networks as they are, and use VMM to simplify the management process.

    Note
    The scenario that is described here is for VLANs that were set up for a specific purpose such as isolation, not for VLANs that were set up only for broadcast boundaries.

    For a VLAN-based configuration, take the following steps:

    i. Obtain information about the numbering of the isolated VLANs that have already been created in the physical network.

    ii. In VMM, create a logical network and select the appropriate option:
      - In System Center 2012 SP1: **Network sites within this logical network are not connected**. (Do not select the option for private VLANs unless you are using private VLAN technology.)
      - In System Center 2012 R2: In most cases, select **VLAN-based independent networks**. However, if you are using private VLAN technology, select **Private VLAN (PVLAN) networks**.

    Within the logical network, configure a separate network site for each existing VLAN. Give each network site a name that is meaningful to you in your environment.

iii. Create an association between those network sites and the host physical network adapter. You can do this on an individual host in VMM by modifying the properties sheet for the host (in **Hardware** under **Network adapters**). Alternatively, you can collect the information about your network sites into an uplink port profile (also called a port profile for uplinks) and a logical switch, and then apply the uplink port profile and the logical switch to host network adapters, as needed. For more information about uplink port profiles, see How to Create a Port Profile for Uplinks in VMM.

iv. Create one VM network for each network site (and VLAN) in your configuration.

- **One VM network that gives direct access to the logical network ("no isolation"):** This is the simplest configuration, where the VM network is the same as the logical network on which it is configured. This configuration is appropriate for a network through which you will manage a host. The VM network provides only the functionality of the logical network, which was introduced in System Center 2012. For this configuration, create a logical network, and then create a VM network that specifies that logical network with an appropriate setting:
  - In System Center 2012 SP1: If this logical network will support network virtualization (in addition to having a VM network that gives direct access to the logical network), select the check box to allow network virtualization. If this logical network will not use network virtualization at all, leave all check boxes cleared.
  - With System Center 2012 R2: For the logical network, select **One connected network** and then select **Create a VM network with the same name to allow virtual machines to access this logical network directly**. (If you select **One connected network** but do not select the second option, you will still be able to create the VM network later.) If this logical network will also support network virtualization, select the check box to allow network virtualization.

  The VM network will function as a logical network with no isolated networks within it. On each logical network, you can have only one VM network that is configured with **No isolation**. However, on a logical network that allows network virtualization, you can have one VM network with no isolation and other VM networks with isolation (that is, with network virtualization).
- **Using external networks that are implemented through a network manager:** With this configuration option, you can use a network manager (for example, a vendor network-management console) that allows you to configure settings on your forwarding extension, for example, settings for logical networks, network sites, and VM networks. You can configure VMM to import those settings from the vendor network-management database into VMM, which makes it easier to work with those settings in the context of your other network configuration settings. For detailed descriptions of this option, see the following topics:
  - How to Add a Virtual Switch Extension Manager in System Center 2012 SP1
  - How to Add a Virtual Switch Extension or Network Manager in System Center 2012 R2
- **Gateways:** To connect a VM network to other networks, you can configure the VM network with a gateway. (This configuration requires that, in the logical network that the VM network uses for a foundation, the network virtualization option is selected.) The steps for configuring

a VM network with a gateway depend on whether you have System Center 2012 SP1 or System Center 2012 R2:

- **In VMM in System Center 2012 SP1**: To configure a VM network to connect to another network in your environment, for the gateway setting of the VM network, select **Local networks**. Alternatively, if you are a hosting provider and you want to enable your tenants, customers, or clients to connect their virtual machines (in the hosted environment that you provide) to systems on their own premises, you can configure their VM networks with gateways. To configure a VM network this way, for the gateway setting of the VM network, select **Remote networks**. The result is a connection through a virtual private network (VPN) tunnel.
- **In VMM in System Center 2012 R2**: To configure a VM network to connect to another network in your environment, on the **Connectivity** page or tab for the VM network, choose the setting for connecting directly to an additional logical network, and specify whether that connection is to use network address translation (NAT). Alternatively, if you are a hosting provider and you want to enable your tenants, customers, or clients to connect their virtual machines (in the hosted environment that you provide) to systems on their own premises, you can configure their VM networks with connectivity through VPN. To configure a VM network this way, on the **Connectivity** page or tab for the VM network, choose the setting for a connection through a virtual private network (VPN) tunnel, with or without Border Gateway Protocol (BGP).

Before you configure a gateway, see Prerequisites for gateways in this topic.

Prerequisites

VM networks in VMM are configured by bringing other networking elements together. Before you create a VM network, create the elements (such as a logical network) on which you will build the VM network. These elements include the following:

1. Logical networks (the foundation for VM networks).
2. (Optional) Load-balancing configuration settings.
3. (Optional) Port settings and logical switches. You can use several VMM configuration elements together to consistently apply settings to multiple network adapters across multiple hosts. These configuration elements include:
   - Native port profiles for uplinks
   - Native port profiles for virtual network adapters
   - Port classifications
   - Logical switches

To learn about these networking elements, see the following topics:

- Configuring Logical Networking in VMM Overview
- Configuring Load Balancing in VMM Overview
- Configuring Ports and Switches for VM Networks in VMM

Prerequisites for gateways

If you want to add a gateway to your configuration in VMM, you must have provider software for the gateway. If the gateway is a non-Microsoft gateway, you must obtain the provider software from the manufacturer of the gateway device, install the provider on the VMM management

server, and then restart the System Center Virtual Machine Manager service. Then you can add the gateway to the list of resources in VMM. For more information about setting up a specific non-Microsoft gateway device, refer to the manufacturer's documentation.

Tip

In VMM in System Center 2012 R2, adding a gateway is called adding a "network service," and the gateway requires additional configuration steps, as described in How to Add a Gateway in VMM in System Center 2012 R2 or How to Use a Server Running Windows Server 2012 R2 as a Gateway with VMM.

After you add a gateway to VMM, to use the gateway to connect a VM network through a VPN tunnel to another site, you must select an appropriate setting for the VM network. In System Center 2012 SP1, the setting is the **Gateway** setting called **Remote networks**, and in System Center 2012 R2, it is the **Connectivity** setting called **Connect to another network through a VPN tunnel**. Before you configure this setting for a VM network, gather the necessary information from your tenant, customer, or client. The following list provides more details:

- Obtain the IP address of the remote VPN server (on the premises of the tenant, customer, or client).

  If you are running VMM in System Center 2012 R2, also obtain information about the subnets on the premises of the tenant, customer, or client. These are the subnets that are used by the tenant's virtual machines or other virtual or physical resources. In addition, if the tenant, customer, or client uses Border Gateway Protocol (BGP), obtain the relevant BGP peer IP addresses and Autonomous System Numbers (ASNs).
- Identify the authentication method to use with the remote VPN server. If the remote VPN server is configured to use a pre-shared key, you can authenticate by using a **Run As** account in which you specify the pre-shared key as the password. Alternatively, you can authenticate with a certificate. The certificate can be either a certificate that the remote VPN server selects automatically or a certificate that you have obtained and placed on your network.
- Determine whether to use the default VPN connection settings or to specify these settings. You can specify settings for the encryption, integrity checks, cipher transforms, authentication transforms, Perfect Forward Secrecy (PFS) group, Diffie-Hellman group, and VPN protocol.

The information that you gather helps you complete the gateway configuration for the VM network.

In this section

To use VMM to configure VM networks and gateways in System Center 2012 SP1 or System Center 2012 R2, complete the procedures in the following table.

Procedure	Description
How to Configure Global Network Settings in VMM	Describes how to configure default VMM settings for automatic logical network and virtual network creation.

Procedure	Description
How to Add a Gateway in VMM in System Center 2012 SP1 How to Add a Gateway in VMM in System Center 2012 R2 How to Use a Server Running Windows Server 2012 R2 as a Gateway with VMM	Describes how to add a gateway that can connect your virtualized networks to other networks. If you want to add a non-Microsoft gateway, you must first obtain provider software from the manufacturer of the gateway device, install the provider on the VMM management server, and restart the System Center Virtual Machine Manager service.
How to Create a VM Network in VMM in System Center 2012 SP1 How to Create a VM Network in VMM in System Center 2012 R2	Describes how to create a VM network, with information about deploying multiple VM networks that use network virtualization (network isolation), deploying a single VM network with "no isolation," and using the other options for VM networks that are listed earlier in this topic.
How to Create IP Address Pools for VM Networks in VMM	Describes how to create static IP address pools for VM networks. These IP address pools are made available to virtual machines and services that use the VM networks.
How to Release Inactive IP Addresses for VM Networks in VMM	Describes how to return inactive addresses to an IP address pool to make them available for reassignment.
How to View VMM Network Configuration Diagrams in VMM	Describes how to view diagrams that show the relationships among networking objects, such as logical networks and VM networks, in your VMM configuration.

Next steps after you configure networking

For information about the next steps to take after you configure networking, see the topics in the following table.

Topic	Step
Preparing the Fabric in VMM	Configure additional fabric resources, such as storage and library resources.
Adding and Managing Hyper-V Hosts and	Add and configure hosts.

Topic	Step
Scale-Out File Servers in VMM Managing VMware ESX and Citrix XenServer in VMM	
Creating and Deploying Virtual Machines and Services in VMM	Deploy virtual machines individually or as part of a service.

See Also

Configuring Networking in VMM

Configuring VM Networks in VMM Illustrated Overview

Configuring VM Networks in VMM Illustrated Overview

In Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1) and System Center 2012 R2, networking includes a number of enhancements that provide you with greater flexibility in configuring networks in a virtualized environment. This overview focuses on one of the enhancements, virtual machine networks (VM networks), although it also shows logical networks.

Logical networks, which were introduced in System Center 2012 and are also found in System Center 2012 SP1 and System Center 2012 R2, are named networks that serve particular functions in your environment. For example, you could have logical networks with names such as “Backend,” “Frontend,” or “Backup.” Logical networks are illustrated in Figure 1 and Figure 6 in this topic.

Other figures in this topic show VM networks, which are found in VMM in System Center 2012 SP1 and System Center 2012 R2. VM networks increase the number of ways you can configure networking for your virtual machines. The illustrations show four different ways that a VM network can be configured on top of a logical network.

The following table describes the illustrations in this topic.

Illustrations based on elements as you see them in the VMM console	Illustrations that show the underlying network object model
Figure 1 Logical networks in VMM	Figure 6 Network object model for logical networks
Figure 2 VM networks configured with network virtualization	Figure 7 Network object model for VM networks configured with network virtualization
Figure 3 VM networks in a VLAN-based configuration	Figure 8 Network object model for VM networks in a VLAN-based configuration
Figure 4 VM network that provides direct access to the logical network with no isolation	Figure 9 Network object model for a VM network that provides direct access to the

Illustrations based on elements as you see them in the VMM console	Illustrations that show the underlying network object model
	logical network
Figures 5a and 5b VM networks configured with an external network service	Figure 10 Network object model for VM networks configured with an external network service

For information about how to configure VM networks, see How to Create a VM Network in VMM in System Center 2012 SP1 or How to Create a VM Network in VMM in System Center 2012 R2.

For illustrations of logical switches, see Configuring Ports and Switches in VMM Illustrated Overview.

For more details about networking in VMM, see the following networking overviews:

- Configuring Logical Networking in VMM Overview
- Configuring Load Balancing in VMM Overview
- Configuring Ports and Switches for VM Networks in VMM
- Configuring VM Networks and Gateways in VMM

Logical networks in VMM

The following illustration shows a logical network in VMM in System Center 2012, System Center 2012 SP1, or System Center 2012 R2. For some networking elements, fictitious names such as “Contoso1” are included to help illustrate the purpose of those elements.

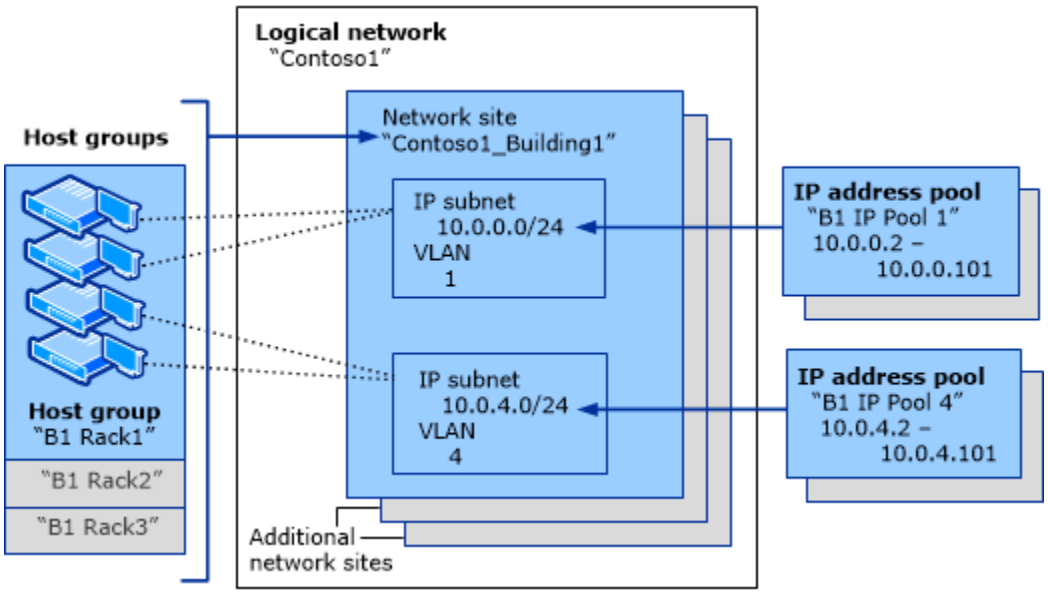


Figure 1 Logical network

This illustration shows how a logical network in VMM is a container for network sites (also called logical network definitions) and for IP subnet information, virtual local area network (VLAN)

information, or both. It also shows how host groups in VMM can be associated with a network site and how IP address pools can be assigned to subnets within the logical network.

In the preceding illustration, the names of elements that you configure by running a wizard or opening a property sheet are shown in bold text, and elements that are on a page of the wizard or on a tab of the property sheet are shown without bold text.

For an illustration that shows the underlying network object model for logical networks, see Figure 6, Network object model for logical networks.

VM networks in VMM in System Center 2012 SP1 and System Center 2012 R2

The illustrations in this section show how VM networks can be configured on top of logical networks in VMM.

Important
VM networks can be created in VMM in System Center 2012 SP1 and System Center 2012 R2.

The following illustrations show four different ways that VM networks can be configured on top of logical networks in VMM:

- VM networks configured with network virtualization: Multiple VM networks can be configured on top of one logical network.
- VM networks in a VLAN-based configuration: Networks that use familiar virtual local area network (VLAN) technology for network isolation can be managed as they are—with one VM network for each network site (and VLAN) in the configuration.
- VM network that provides direct access to the logical network with no isolation: One VM network can provide direct access to the logical network, with no isolation.
- VM networks configured with an external network service: Settings configured with a network service, such as a vendor network-management console that uses a forwarding extension, can be imported into VMM. With System Center 2012 R2, such settings can also be exported from VMM to the network service.

VM networks configured with network virtualization

The following illustration shows VM networks that are configured with network virtualization in VMM in System Center 2012 SP1 or System Center 2012 R2. For some networking elements, fictitious names, such as “AdventureWorks” and “Contoso1,” are included to help illustrate the purpose of those elements.

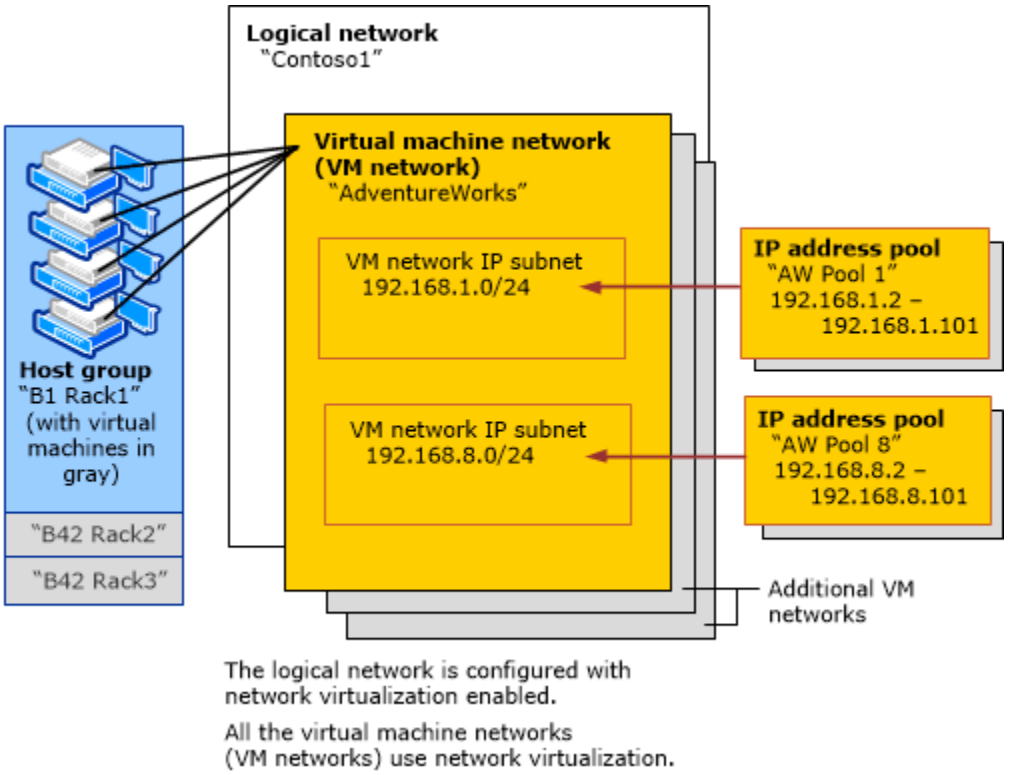


Figure 2 VM networks with network virtualization

Network virtualization extends the concept of server virtualization to make it possible for you to deploy multiple VM networks on the same logical network. In the illustration, the "AdventureWorks" VM network is configured on top of the logical network called "Contoso1." As indicated in the illustration, additional VM networks can be configured on top of the same logical network, so that additional tenants, clients, or customers can each have their own network and choose their own IP addresses, regardless of the IP addresses that are used in other VM networks.

In the preceding illustration, the names of elements that you configure by running a wizard or opening a property sheet are shown in bold text, and elements that are on a page of the wizard or on a tab of the property sheet are shown without bold text.

For an illustration that shows the underlying network object model for this configuration, see Figure 7, Network object model for VM networks configured with network virtualization.

In System Center 2012 SP1 and System Center 2012 R2, many of the VMM networking enhancements are based on Hyper-V network virtualization, which was introduced in Windows Server 2012. To understand these networking enhancements, it can be useful to review the illustrations and descriptions (especially the first illustration) of Hyper-V network virtualization in Hyper-V Network Virtualization technical details.

VM networks in a VLAN-based configuration

The following illustration shows VM networks in a VLAN-based configuration, that is, where VLANs already exist in the physical and logical networks. For some networking elements,

fictitious names, such as “Contoso2” and “VLAN_1” are included to help illustrate the purpose of those elements.

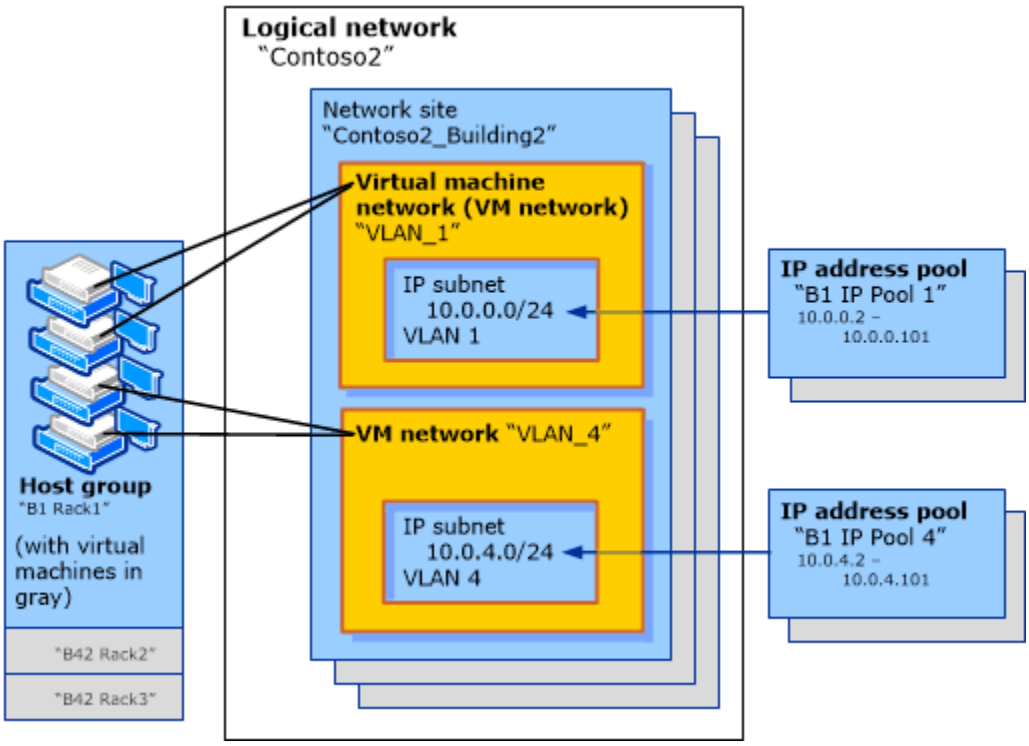


Figure 3 VM networks in a VLAN-based configuration

In the scenario that is illustrated here, the VLANs exist for a specific purpose, such as isolation, and not for broadcast boundaries only. The illustration shows two VM networks that have been created, to match the two VLANs in the underlying physical and logical networks. With more VLANs, more VM networks could be created—typically, one VM network per VLAN.

In the preceding illustration, the names of elements that you configure by running a wizard or opening a property sheet are shown in bold text, and elements that are on a page of the wizard or on a tab of the property sheet are shown without bold text.

For an illustration that shows the underlying network object model for this configuration, see Figure 8, Network object model for VM networks in a VLAN-based configuration.

VM network that provides direct access to the logical network with no isolation

The following illustration shows a VM network that is configured to provide direct access to the underlying logical network. For some networking elements, fictitious names, such as “Contoso1” and “Internet_connection1,” are included to help illustrate the purpose of those elements.

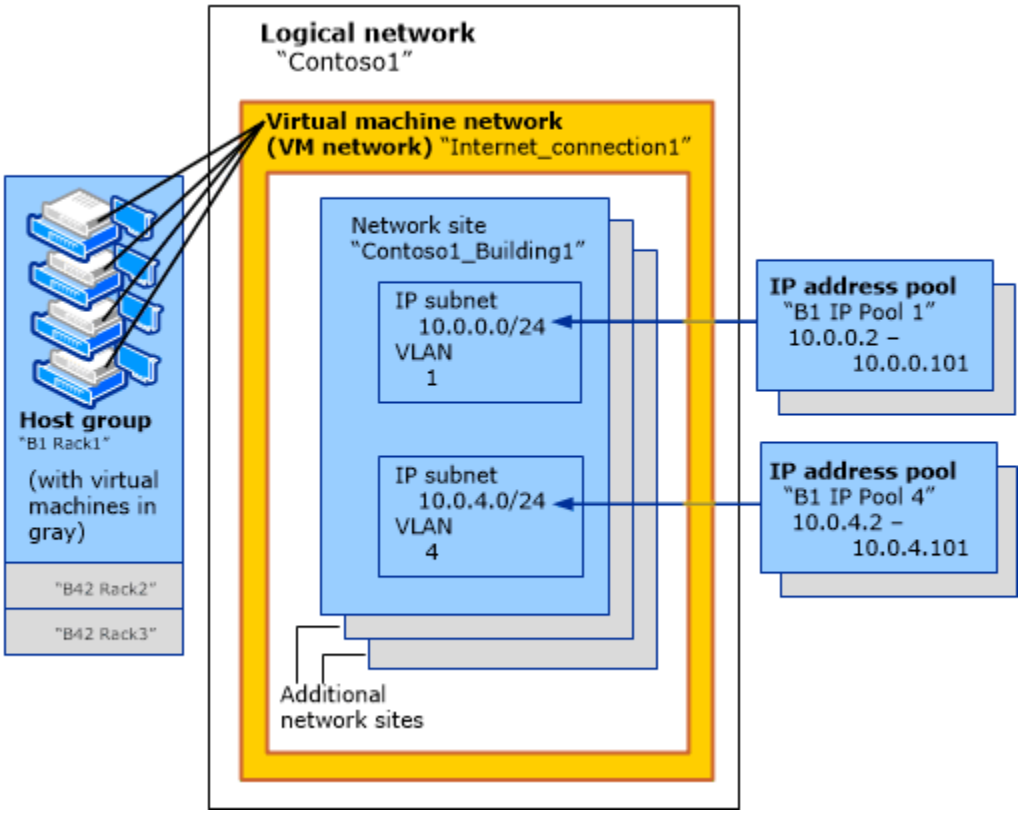


Figure 4 VM network that provides direct access to the logical network

A VM network that provides direct access to the logical network contrasts with VM networks that use network virtualization. Another way of describing this is to say that a VM network that provides direct access provides “no isolation,” while VM networks that use network virtualization provide isolation from the logical network and from each other. On each logical network, you can have only one VM network that is configured with **No isolation**. However, on a logical network that allows network virtualization, you can have one VM network with no isolation and other VM networks with isolation (that is, with network virtualization).

In the configuration shown in the illustration, when a virtual machine is deployed, the choice of the IP subnet/VLAN pair is made by VMM, based on the location (the host or the cloud) where you are deploying the virtual machine.

In the preceding illustration, the names of elements that you configure by running a wizard or opening a property sheet are shown in bold text, and elements that are on a page of the wizard or on a tab of the property sheet are shown without bold text.

For an illustration that shows the underlying network object model for this configuration, see Figure 9, Network object model for a VM network that provides direct access to the logical network.

VM networks configured with an external network service

The following illustrations show a type of external network service: a vendor network-management console that has been used to configure settings on a forwarding extension (for

example, settings for logical networks, network sites, and VM networks). The illustrations also show a VMM management server that has been configured to work with the vendor network-management database. For some networking elements, fictitious names, such as “External1” and “AdventureWorks,” are included to help illustrate the purpose of those elements.

Figure 5a shows that with VMM in System Center 2012 SP1, the VMM management server imports settings from the vendor network-management database (but cannot export settings). This contrasts with Figure 5b, later in this section.

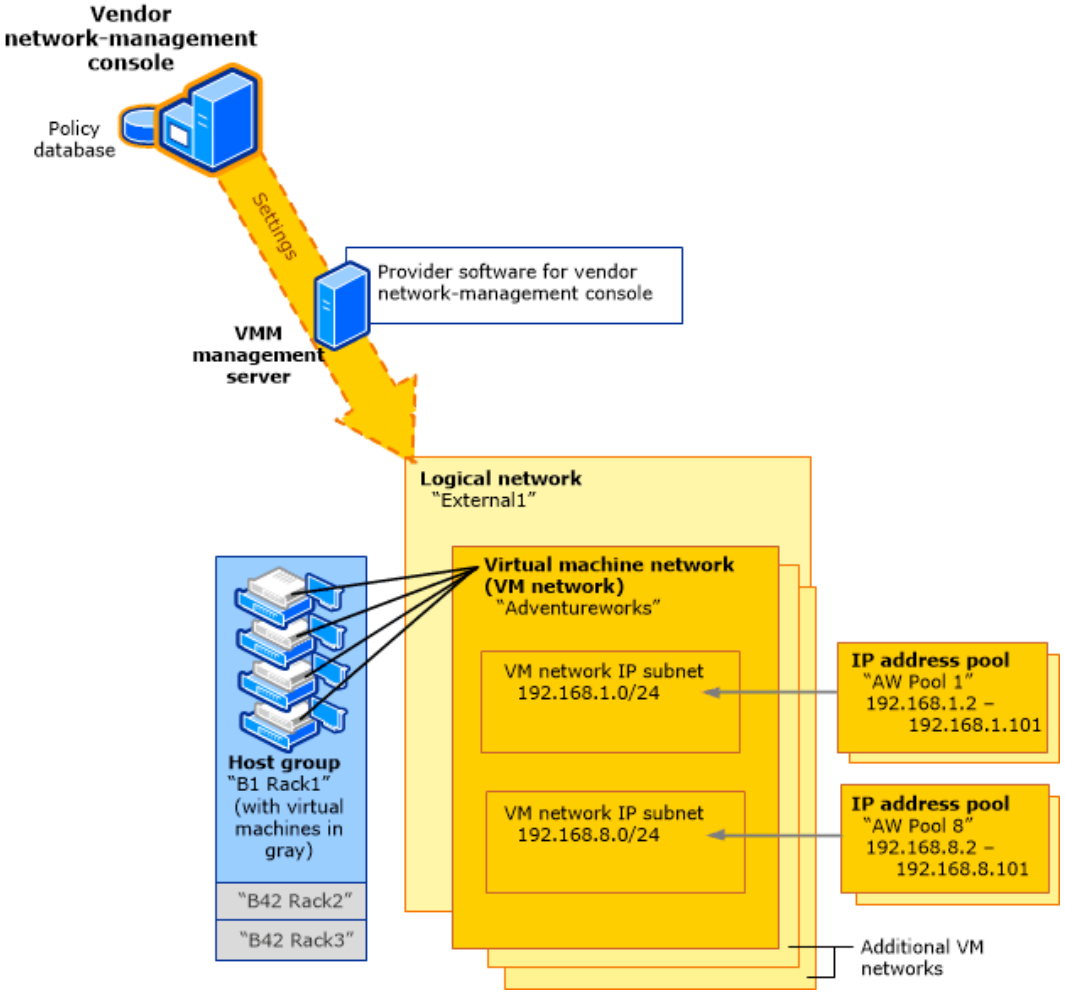


Figure 5a VM networks configured with a vendor network-management console (with VMM in System Center 2012 SP1)

Figure 5b shows that with VMM in System Center 2012 R2, the VMM management server and the vendor network-management database can both send and receive information about settings.

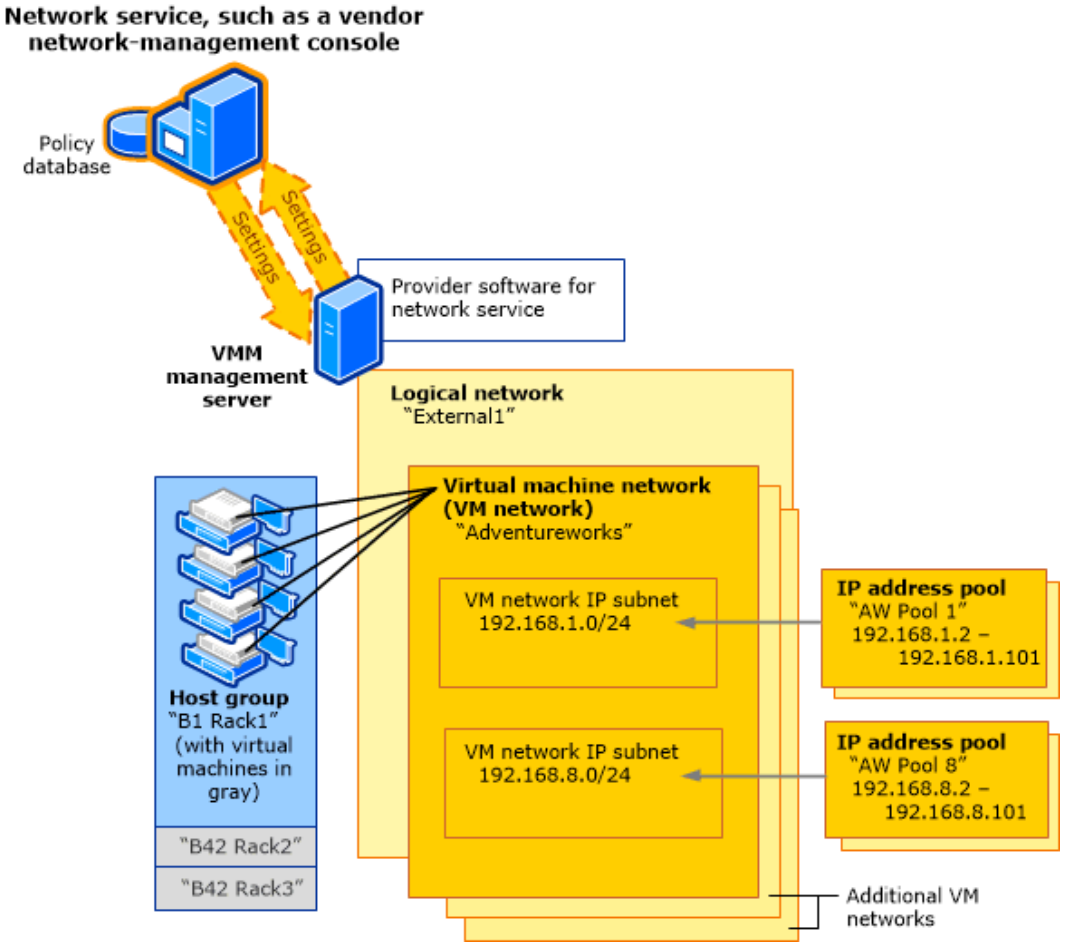


Figure 5b VM networks configured in coordination with a network service (with VMM in System Center 2012 R2)

As the preceding illustrations indicate, the VMM management server contains the appropriate provider software (which you must install). Although the illustration shows a particular configuration of VM networks as an example, the VM network configuration will reflect any configuration that you create. With the configuration that is shown in both illustrations, if network settings have been configured on the network-management console, they do not have to be configured again in VMM. Instead, the settings automatically appear in VMM.

For an illustration that shows the underlying network object model for this configuration, see Figure 10, Network object model for VM networks configured with an external network service.

Network object model for logical networks

The following illustration shows the network object model for logical networks in VMM in System Center 2012, System Center 2012 SP1, and System Center 2012 R2. The illustration shows the relationships among network objects only, rather than indicating information about the wizards and property sheets through which the objects are configured in the VMM console. The

illustration can be especially useful if you are learning about configuring VMM through Windows PowerShell scripts, which reflect the network object models directly.

For some objects, sample names such as “Contoso1” and “Building1” are included to help illustrate the purpose of those objects. (The object labeled “Network site” is also known as a “logical network definition.”)

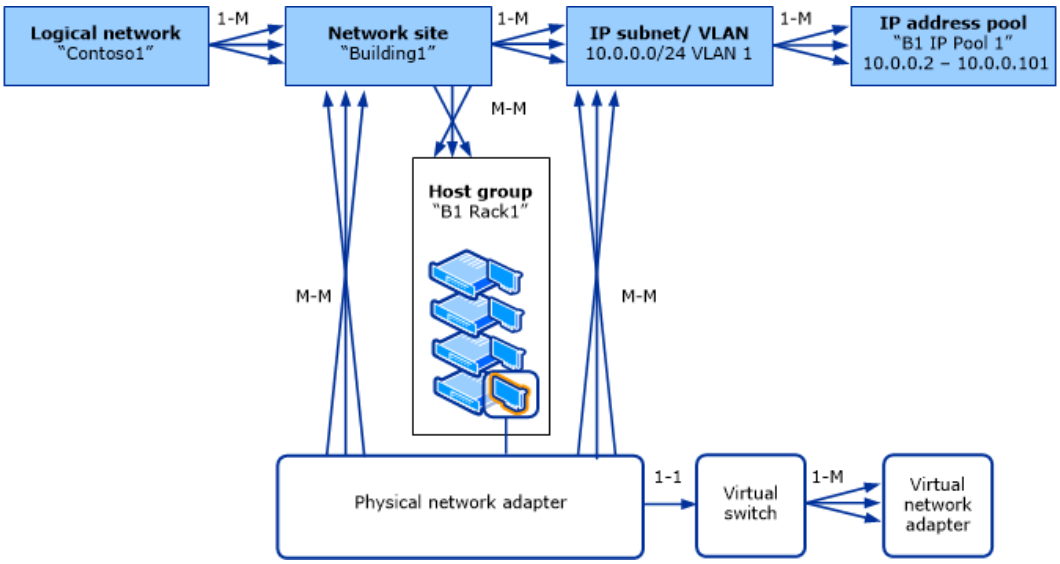


Figure 6 Object model for logical networks

The following key explains the notations on the arrows:

- **1-1** means “one-to-one.”
- **1-M** means “one-to-many.”
- **M-M** means “many-to-many.”

In the preceding illustration, bold text is used for each VMM object name, regardless of how that object is configured through the VMM console.

For an illustration of logical networks that is based on how they appear in the VMM console, see Figure 1, Logical networks in VMM.

Network object models for VM networks in VMM

The following illustrations show the network object models for logical networks and VM networks in VMM in System Center 2012 SP1 and System Center 2012 R2. These illustrations show the relationships among network objects only, rather than indicating information about the wizards and property sheets through which the objects are configured in the VMM console. The illustrations can be especially useful if you are learning about configuring VMM through Windows PowerShell scripts, which reflect the network object models directly.

Important

VM networks can be created in VMM in System Center 2012 SP1 and System Center 2012 R2.

Network object model for VM networks configured with network virtualization

The following illustration shows the network object model for VM networks that are configured with network virtualization.

For some objects, sample names such as “AdventureWorks” and “Contoso1” are included to help illustrate the purpose of those objects.

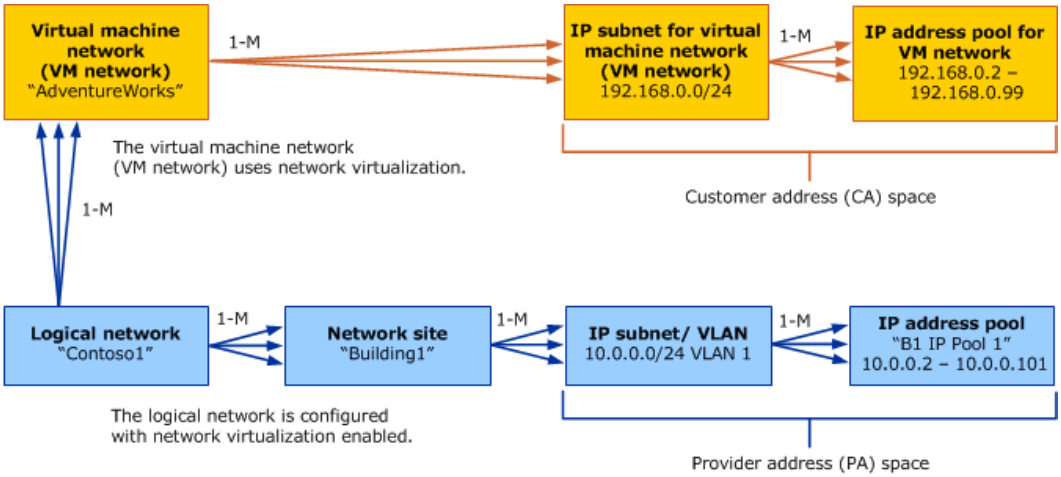


Figure 7 Object model for VM networks configured with network virtualization

As indicated in the illustration, the IP addresses on the VM network are also called the “customer address (CA) space” because these IP addresses are used by customers (or clients or tenants). The IP addresses on the logical network are also called the “provider address (PA) space” because these IP addresses are used by providers (or hosters).

The notation **1-M** means “one-to-many.”

In the preceding illustration, bold text is used for each VMM object name, regardless of how that object is configured through the VMM console.

For an illustration of this configuration that is based on how it appears in the VMM console, see Figure 2, VM networks configured with network virtualization.

Network object model for VM networks in a VLAN-based configuration

The following illustration shows the network object model for VM networks in a VLAN-based configuration.

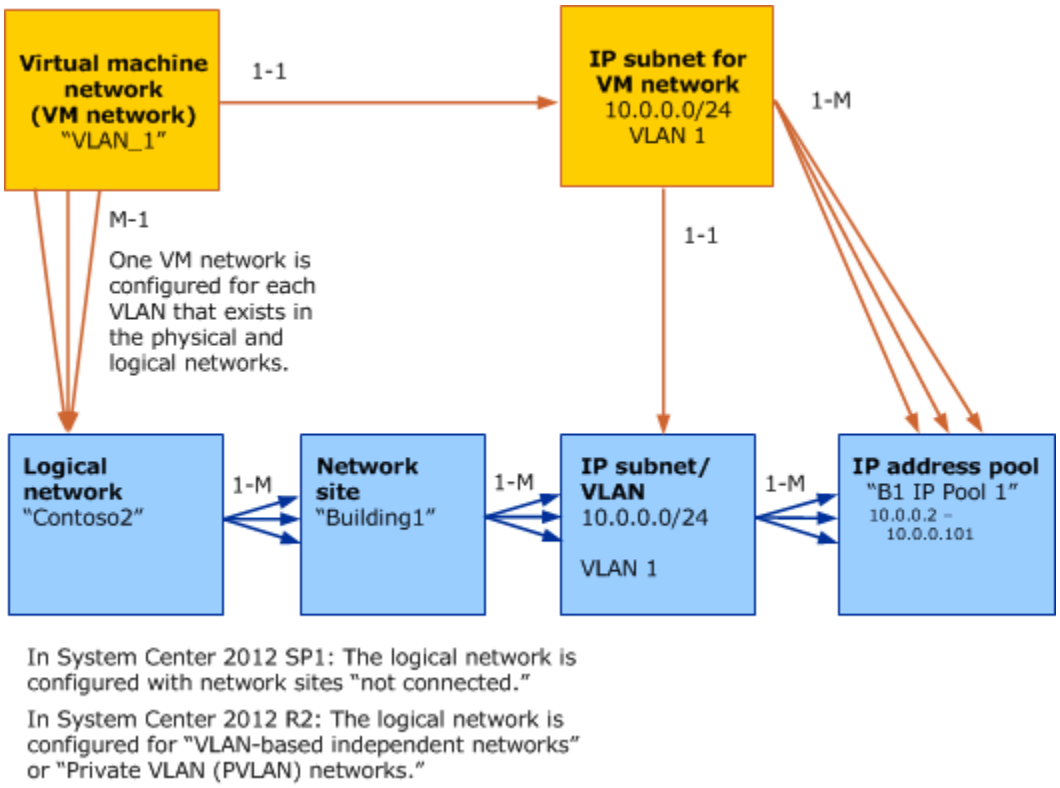


Figure 8 Object model for VM networks in a VLAN-based configuration

The following key explains the notations on the arrows:

- **1-1** means “one-to-one.”
- **1-M** means “one-to-many.”
- **M-1** means “many-to-one.”

In the preceding illustration, bold text is used for each VMM object name, regardless of how that object is configured through the VMM console.

For an illustration of this configuration that is based on how it appears in the VMM console, see Figure 3, VM networks in a VLAN-based configuration.

Network object model for a VM network that provides direct access to the logical network

The following illustration shows the network object model for a VM network that provides direct access to the logical network, with no isolation. This is the simplest configuration, where the VM network is the same as the logical network on which it is configured.

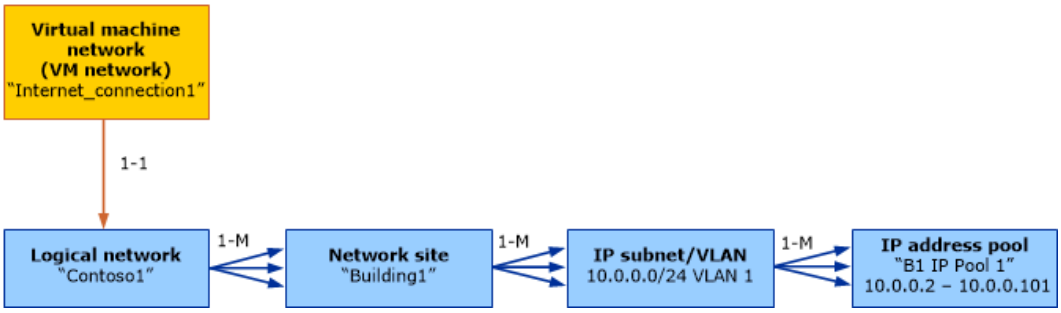


Figure 9 Object model for a VM network that provides direct access to the logical network

The following key explains the notations on the arrows:

- **1-1** means “one-to-one.”
- **1-M** means “one-to-many.”

In the preceding illustration, bold text is used for each VMM object name, regardless of how that object is configured through the VMM console.

For an illustration of this configuration that is based on how it appears in the VMM console, see Figure 4, VM network that provides direct access to the logical network with no isolation.

Network object model for VM networks configured with an external network service

The following illustration shows the network object model for VM networks that are configured with a network service, such as a vendor network-management console that works with a forwarding extension. This configuration uses a virtual switch extension manager to enable communication with the vendor network-management console.

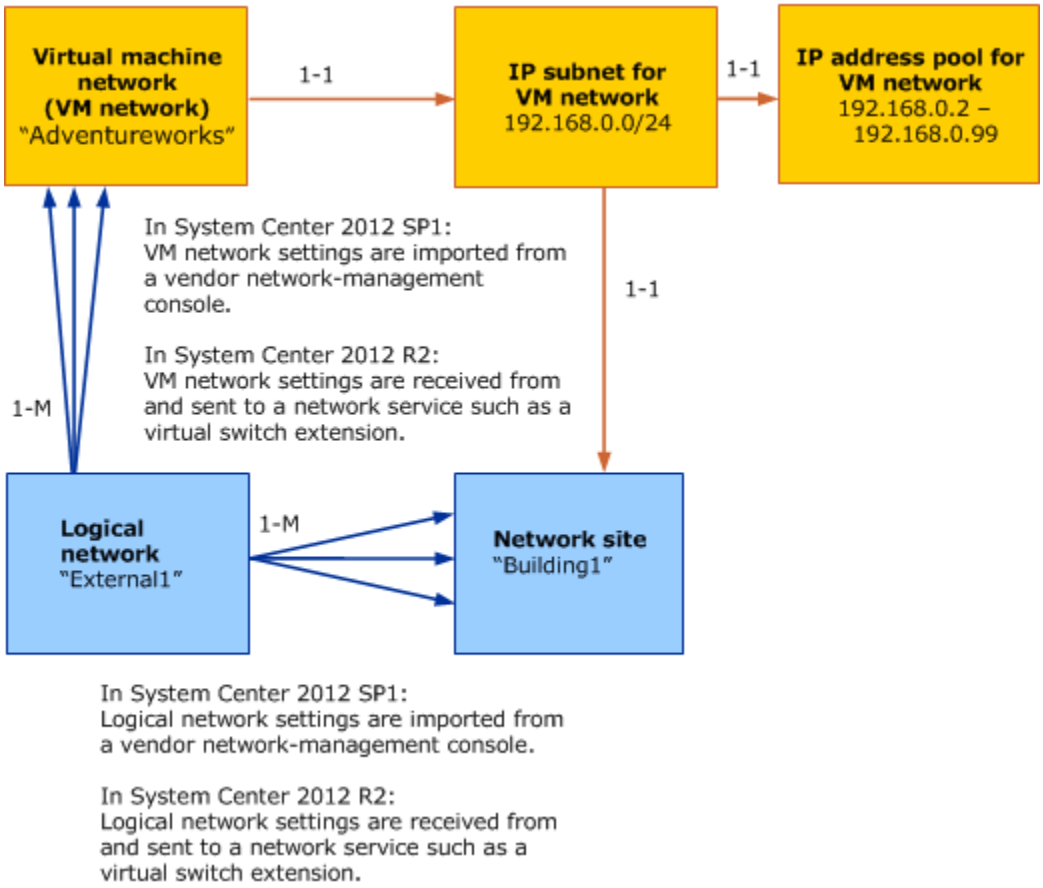


Figure 10 Object model for VM networks configured with a network service such as a vendor network-management console

The following key explains the notations on the arrows:

- **1-1** means “one-to-one.”
- **1-M** means “one-to-many.”

In the preceding illustration, bold text is used for each VMM object name, regardless of how that object is configured through the VMM console.

For an illustration of this configuration that is based on how it appears in the VMM console, see Figure 5, VM networks configured with an external network service.

See Also

How to Create a VM Network in VMM in System Center 2012 SP1

How to Create a VM Network in VMM in System Center 2012 R2

Configuring Logical Networking in VMM Overview

Configuring VM Networks and Gateways in VMM

Configuring Ports and Switches for VM Networks in VMM

Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2

How to Add a Gateway in VMM in System Center 2012 SP1

In Virtual Machine Manager (VMM) in either System Center 2012 Service Pack 1 (SP1) or System Center 2012 R2, you can connect a VM network to other networks by using a gateway.

Important
This topic describes how you can add a gateway to the list of resources in VMM in System Center 2012 SP1 only. For information about how to add a gateway to the list of resources in VMM in System Center 2012 R2, see How to Add a Gateway in VMM in System Center 2012 R2.

After you add the gateway, you can configure a VM network to use the gateway. In the VM network settings, you can choose one of two settings for the gateway, **Local networks** or **Remote networks**. To connect the VM network to a connected physical network, you will select **Local networks**. Alternatively, if you are a hoster, to allow your tenants, customers, or clients to connect their virtual machines (in the hosted environment that you provide) to systems on their own premises by using a gateway, you will select **Remote networks**. This action creates a connection through a VPN tunnel, to a VPN endpoint on the tenant's premises.

Important
For a full list of prerequisites for configuring gateways that use the **Remote networks** (VPN tunnel) setting, see the "Prerequisites for gateways" section in Configuring VM Networks and Gateways in VMM

Use the following procedure to add a gateway device to VMM.

Prerequisites

If you want to add a gateway to your configuration in VMM, you must first perform the following actions:

1. Obtain provider software from the manufacturer of the gateway device, install the provider on the VMM management server, and then restart the System Center Virtual Machine Manager service. If you have installed a highly available VMM management server on a cluster, be sure to install the provider on all nodes of the cluster. For more information about installing the provider, refer to the manufacturer's documentation.
2. Configure the logical network that will be the foundation for the VM network that will use the gateway, and ensure that network virtualization is enabled on the logical network.
3. Create an IP address pool on the logical network, and ensure that the pool includes the address that you intend to use on the gateway.
4. Ensure that the gateway is configured with an IP address that is in the IP address pool that you created. Make a note of the IP address so that you can specify it when you use the following procedure to add the gateway to VMM.

To add a gateway in System Center 2012 SP1

1. Confirm that you have installed the necessary provider software for the gateway device. To do this, open the **Settings** workspace and in the **Settings** pane, click **Configuration Providers**. In the **Configuration Providers** pane, review the list of installed provider software.

2. Open the **Fabric** workspace.
3. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
4. In the **Fabric** pane, expand **Networking**, and then click **Gateways**.
5. On the **Home** tab, in the **Add** group, click **Add resources**, and then click **Gateway**.

   The **Add Gateway Wizard** opens.
6. On the **Name** page, enter a name and optional description for the gateway, and then click **Next**.
7. On the **Credentials** page, either click **Browse** and then on the **Select a Run As Account** dialog box, select an account, or click **Create Run As Account** and create a new account. Then click **Next**.
8. On the **Manufacturer and Model** page, in the **Manufacturer** list, select a provider manufacturer, in the **Model** list, select a model, and then click **Next**.
9. On the **Logical Network** page, in the **IP Address** box, specify the IP address of the gateway interface, in the **Logical network** list, select the logical network that will be the foundation for the VM network that will use the gateway, and then click **Next**.
10. On the **Connection String** page, in the **Connection string** box, type the connection string for the gateway to use, and then click **Next**.

    For example, you might enter the connection string **mygateway1.contoso.com:443**.

    Important
    The syntax of the connection string is defined by the manufacturer of the gateway. For more information about the required syntax, refer to the manufacturer's documentation.
11. On the **Provider** page, in the **Configuration provider** list, select an available provider, click **Test** to run basic validation against the gateway using the selected provider, and then click **Next**.
12. On the **Summary** page, review and confirm the settings, and then click **Finish**.

When you are ready to configure the VM network that uses the newly added gateway, open the wizard or property sheet for the VM network, and on the **Gateway** page or tab, choose the appropriate setting for the connectivity of the gateway. You can choose either **Remote networks** or **Local networks**. If you choose **Remote networks**, you will also need to configure VPN connection settings that you have obtained from the administrator of the remote VPN gateway. For more information, see "Prerequisites for gateways" in Configuring VM Networks and Gateways in VMM and see the first procedure in How to Create a VM Network in VMM in System Center 2012 SP1.

See Also

Configuring VM Networks and Gateways in VMM

Configuring Networking in VMM

How to Create a VM Network in VMM in System Center 2012 SP1

How to Add a Gateway in VMM in System Center 2012 R2

In Virtual Machine Manager (VMM) in either System Center 2012 R2 or System Center 2012 Service Pack 1 (SP1), you can connect a VM network to other networks by using a gateway.

Important
This topic provides information about how to add a gateway to the list of resources in VMM in System Center 2012 R2 only. The following topics provide related information:

- If your VMM server is running System Center 2012 SP1, see How to Add a Gateway in VMM in System Center 2012 SP1.
- If your VMM server is running System Center 2012 R2, and you want to add a gateway server that runs Windows Server® 2012 R2, see How to Use a Server Running Windows Server 2012 R2 as a Gateway with VMM.

After you add the gateway, you can configure a VM network to use the gateway. You have several choices for the VM network settings. You can choose the setting for a connection through a VPN tunnel, with or without Border Gateway Protocol (BGP), or the setting for connecting directly to an additional logical network, with or without network address translation (NAT).

Prerequisites

If you want to add a gateway to your configuration in VMM in System Center 2012 R2, you must first perform the following tasks:

1. Obtain provider software from the manufacturer of the gateway device, install the provider on the VMM management server, and then restart the System Center Virtual Machine Manager service. If you have installed a high-availability VMM management server on a cluster, be sure to install the provider on all nodes of the cluster. For more information about installing the provider, refer to the manufacturer's documentation.
2. Make sure that you know the manufacturer and model of your gateway, the name of an account that has permission to configure the gateway, the connection string that the gateway will use, and the host groups for which the gateway should be available. If certificates are required for the gateway, for example, if the gateway is in an untrusted domain, make sure you know how to view the thumbprint information for those certificates.
3. As a best practice, in the operating system of the gateway, ensure that network adapters (physical network adapters, virtual network adapters, or both) have adapter names that indicate their intended use. For example, if your adapters have the default names Ethernet, Ethernet 2, and Ethernet 3, a best practice would be to rename them for their intended uses, such as Management, External, and Tenant. This makes them easy to recognize when you see them in a list in VMM.
4. Ensure that the logical networks (and the associated network sites) that will be connected to the gateway have been configured. For a logical network that will be the foundation for VM networks that will use the gateway, ensure that network virtualization is enabled on the logical network. Also configure IP address pools on the logical networks.

   Note
   Configure the IP address pools even if you use NAT. IP addresses used by NAT are allocated through the IP address pools.

5. Ensure that the relevant virtual switches on the affected hosts have been configured, either through port profiles and logical switches, or through direct configuration of the ports and capabilities in the virtual switch.
6. Obtain information from your tenant, customer, or client as described in the Prerequisites for gateways section in Configuring VM Networks and Gateways in VMM.

To add a gateway in System Center 2012 R2

1. Confirm that the necessary provider software for the gateway device has been installed. To do this, open the **Settings** workspace, and in the **Settings** pane, click **Configuration Providers**. In the **Configuration Providers** pane, review the list of installed provider software.
2. Open the **Fabric** workspace.
3. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
4. In the **Fabric** pane, expand **Networking**, and then click **Network Service**.

   Network services include gateways, virtual switch extensions, network managers, and top-of-rack (TOR) switches.
5. On the **Home** tab, in the **Add** group, click **Add Resources**, and then click **Network Service**.

   The **Add Network Service Wizard** opens.
6. On the **Name** page, type a name and an optional description for the gateway, and then click **Next**.
7. On the **Manufacturer and Model** page, in the **Manufacturer** list, click a provider manufacturer, and in the **Model** list, click a model. Then click **Next**.
8. On the **Credentials** page, either click **Browse** and then on the **Select a Run As Account** dialog box, select an account, or click **Create Run As Account** and create a new account. The account must have appropriate permissions in the domain that the gateway is connected to. After you have selected or created an account, click **Next**.
9. On the **Connection String** page, in the **Connection string** box, type the connection string for the gateway to use, and then click **Next**.

   Important
   The syntax of the connection string is defined by the manufacturer of the gateway. For more information about the required syntax, refer to the manufacturer's documentation.
10. On the **Certificates** page, if certificates are listed, verify that the thumbprints of those certificates match the thumbprints of the certificates that are installed on the gateway. Then select the check box to confirm that the certificates can be imported to the trusted certificate store. Click **Next**.

    Note
    If no certificates are listed, the connection string that was provided probably does not require certificates, and you can continue to the next page of the wizard. However, if no certificates are listed but your gateway requires them, confirm that

the certificates were installed correctly on your gateway. Then, to refresh the display on the **Certificates** page of the wizard, click **Previous** and then click **Next**.

11. On the **Provider** page, in the **Configuration provider** list, select an available provider, and then click **Test** to use the selected provider to run basic validation tests against the gateway. If the tests indicate that the provider works correctly for the gateway, click **Next**.
12. On the **Host Group** page, select one or more host groups to which the gateway will be available.
13. On the **Summary** page, review and confirm the settings, and then click **Finish**.
14. After the gateway is created, under **Network Services**, find the listing for the gateway. Right-click the listing, click **Properties**, click **Connectivity**, and then specify the following:
    - Select **Enable front end connection**, and then select the gateway network adapter and the network site that provide connectivity outside the hosting-provider or enterprise datacenter. If you will allow VPN connections, the network site needs to be routable to and from the Internet. Also, the network site must have a static IP address pool.
    - Select **Enable back end connection**, and then select a gateway network adapter and network site in a logical network within the hosting-provider or enterprise datacenter. The logical network must have Hyper-V network virtualization enabled. Also, the network site must have a static IP address pool.

When you are ready to configure the VM network that uses the newly added gateway, open the wizard or property sheet for the VM network, and on the **Connectivity** page or tab, choose the appropriate setting for the connectivity of the gateway. You can choose the setting for a connection through a VPN tunnel, with or without Border Gateway Protocol (BGP), or the setting for connecting directly to an additional logical network, with or without network address translation (NAT). For more information, see the Prerequisites for gateways section in Configuring VM Networks and Gateways in VMM.

See Also

Configuring VM Networks and Gateways in VMM

How to Create a VM Network in VMM in System Center 2012 R2

Configuring Networking in VMM

How to Use a Server Running Windows Server 2012 R2 as a Gateway with VMM

In Virtual Machine Manager (VMM) in either System Center 2012 R2 or System Center 2012 Service Pack 1 (SP1), you can connect a VM network to other networks by using a gateway.

Important

This topic provides information about how to use a virtual machine running Windows Server 2012 R2 as a gateway with VMM in System Center 2012 R2. The configuration uses a host cluster that runs Windows Server 2012 R2 and is configured with high availability. If you do not want to create this configuration, you might want to read other topics:

- If your VMM server is running System Center 2012 SP1, see How to Add a Gateway in VMM in System Center 2012 SP1.
- If your VMM server is running System Center 2012 R2, but you want a more general list of steps for adding a gateway (including a gateway that does not run Microsoft software) to the list of resources in VMM, see How to Add a Gateway in VMM in System Center 2012 R2.

Gateway configuration and options

A gateway running Windows Server 2012 R2 is also called a Windows Server Gateway. The configuration uses a host cluster that runs Windows Server 2012 R2, and the gateway itself is virtual-machine based. The gateway consists of a pair of virtual machines that work with the host cluster to help provide high availability and good performance for the gateway. For information about the hardware requirements for a Windows Server Gateway, see Windows Server Gateway Hardware and Configuration Requirements.

You can configure the gateway in a variety of ways, as described in the second half of Windows Server Gateway. One of the main choices that you make when configuring a Windows Server Gateway is whether to make it a forwarding gateway:

- A gateway configured without forwarding provides communication between a network that uses network virtualization and another network. After you add the gateway, when you configure a VM network to use the gateway, you can choose among multiple connectivity settings for the VM network. You can choose the setting for a connection through a virtual private network (VPN) tunnel, with or without Border Gateway Protocol (BGP), or the setting for connecting directly to an additional logical network with network address translation (NAT). For descriptions and diagrams of these connectivity options for a gateway, see:
  - Windows Server Gateway as a site-to-site VPN gateway for hybrid cloud environments in the Windows Server Gateway topic
  - Multitenant Network Address Translation (NAT) for VM Internet access in the Windows Server Gateway topic
  - Multitenant remote access VPN connections in the Windows Server Gateway topic
- A forwarding gateway can bridge a single virtualized IP address space with a physical IP address space by using direct routing. To create a forwarding gateway, ensure that the connection string for the gateway includes **DirectRoutingMode=True**, as described in the procedure that follows. For a description and diagram of a forwarding gateway, see Windows Server Gateway as a forwarding gateway for private cloud environments.

  Important

  After you add a gateway configured with **DirectRoutingMode=True**, when you configure a VM network to use the gateway, choose the connectivity setting for connecting directly to an additional logical network, and do not choose the NAT setting.

For more information about the connectivity settings for VM networks, see Prerequisites for gateways in Configuring VM Networks and Gateways in VMM.

Prerequisites for adding a Windows Server Gateway

Before you can add a gateway that runs Windows Server 2012 R2 to your configuration in VMM, you must perform the tasks in this section.

Preparatory task: Download the compressed file (with a .zip extension) for the Windows Server Gateway from the Microsoft website at http://go.microsoft.com/fwlink/p/?LinkId=329037. Extract the files contained within the download. These files include a Quick Start Guide, two service templates, and a custom resource folder (a folder with a .cr extension) that contains files required for the service templates. You will choose one of the two service templates for your gateway. The template with 2NIC in the filename is designed for a host cluster configured with two network adapters, and the template with 3NIC in the filename is designed for a host cluster configured with three network adapters.

Review the Quick Start Guide, especially the network requirements and the gateway architecture diagram near the beginning of the guide. However, do not try to import a service template into VMM yet. Instead, proceed with the following tasks, which are also described in the Quick Start Guide.

1. Review your domain structure, and choose the domain location that you will use for the host cluster. This domain will also be the domain for the gateway virtual machines that run on the host cluster. If the gateway will be facing untrusted networks, such as the public Internet, we recommend that you place the host cluster and the VMM server in two different domains that do not have a trust relationship.
2. Ensure that the logical networks (and the associated network sites) that will be connected to the gateway have been configured in VMM. If you want to configure network settings on the host cluster by using a port profile and logical switch, also create those now.

   Important
   Review both the list and the table that follow before creating the logical networks.

   The following list outlines the actions that are required for all three of the logical networks:

   - Create at least one network site on each of the logical networks.
   - The network virtualization logical network should be created as a connected network.
   - Configure IP address pools on each of the logical networks, unless you want to use DCHP on the "Infrastructure" (management) network—if so, omit the IP address pool for that network.

   The following table outlines the logical networks and the specific requirements for each logical network:

Example name	Logical network description	Settings
Network Virtualization	The back end network. This is the logical network on which VM networks using network virtualization will be created. On this network, encapsulated packets will be sent to and received from the tenant virtual machines. This network must be used for network virtualization only.	**One connected network** **Allow new VM networks created on this logical network to use network virtualization**
External	The front end network. This is the network through which your virtual networks can access outside networks. If you will use your gateway for site-to-site VPN, this network must have an Internet-routable IP address space.	**One connected network** **Create a VM network with the same name to allow virtual machines to access this logical network directly**
Infrastructure	The management network. This is the network that connects the VMM server with the host cluster and the gateway (virtual machines). There must be a domain controller and a DNS server available on this network. You can configure a static IP address pool for this network, or use a DHCP server to provide IP addresses.	**One connected network** **Create a VM network with the same name to allow virtual machines to access this logical network directly**

After you have finished creating the logical networks, network sites, and IP address pools, review the following:

- If you added an IP address pool on the "Infrastructure" (management) network, determine whether the "Infrastructure" network and the “External” (front end) network route to the same network at any point. If they do, for each IP address pool, right-click the pool and then click **Properties**. On the **Gateway** tab, review the value in the **Metric** column. Ensure that the **Metric** for the "Infrastructure" network is set to a higher value than the **Metric** for the “External” network.

- If you added an IP address pool on the "Infrastructure" (management) network, right-click the pool and then click **Properties**. On the **IP address range** tab, under **IP addresses to be reserved for other uses**, specify an IP address that is within the range of addresses in the IP address pool. Record this IP address. You will use it later when you deploy the gateway.
- If you want to configure networking settings on the host cluster by using a port profile and a logical switch, create an uplink port profile that contains the three logical networks that you created. In the port profile, when you review the setting of the **Enable Hyper-V Network Virtualization** check box, note that network virtualization is always enabled on hosts running Windows Server 2012 R2, and therefore the check box has no effect on those hosts. After you create the uplink port profile, the next step is to create a logical switch and add the port profile to the logical switch.

  For information about uplink port profiles and logical switches, see How to Create a Port Profile for Uplinks in VMM and How to Create a Logical Switch in VMM.

3. Ensure that your VMM resources include a Scale-Out File Server. Also ensure that the Scale-Out File Server contains a share.
   - For background information about a Scale-Out File Server, see Scale-Out File Server for Application Data Overview.
   - If you already have a Scale-Out File Server in your datacenter, ensure that it has been added to VMM. For more information, see How to Add Windows File Server Shares in VMM.
   - For information about using Windows Server 2012 R2 to deploy a Scale-Out File Server, see Deploy Scale-Out File Server. For information about adding the Scale-Out File Server to VMM, see How to Add Windows File Server Shares in VMM.
   - For information about using VMM to deploy a Scale-Out File Server, see Adding Physical Computers as Hyper-V Hosts or as Scale-Out File Servers in VMM Overview.

   Important
   To confirm that the Scale-Out File Server has been added to VMM and the share is being managed in VMM, open the **Fabric** workspace, expand **Storage**, and then click **File Servers**. In the list, find the file server, and confirm that the **Type** is **Scale-Out File Server** and the **Status** is **OK**. Expand the listing for the Scale-Out File Server, right-click the share, and then click **Properties**. Ensure that the **File share managed by Virtual Machine Manager** check box is selected.
4. Create three virtual hard disks that will be used in your configuration:
   - Create a virtual hard disk containing the Windows Server 2012 R2 operating system. Ensure that the virtual hard disk has been generalized by using the Sysprep tool. The virtual hard disk can use the .vhd or .vhdx format. Copy the virtual hard disk into the VMM library, in the subfolder where you store virtual machine hard disk files. For more information, see How to Add File-Based Resources to the VMM Library.
   - Make two copies of the small blank .vhdx files that are included in the VMM library. Provide them with names that help identify them as the virtual hard disk files for a Cluster Shared Volume (CSV) and a quorum resource. In the VMM library, create a folder named **Windows Server Gateway**, and then copy the two blank .vhdx files into that folder.

5. Navigate to the resources that you downloaded, and locate the folder called **VMClusterSetup.cr**. The .cr filename extension is a standard extension in VMM that indicates a custom resource folder. Copy the entire folder and its contents into the **Windows Server Gateway** folder that you just created. Confirm that the **VMClusterSetup.cr** folder is a subfolder in the **Windows Server Gateway** folder.

   To confirm that the virtual hard disks and the custom resource folder for the gateway are in the VMM library, in VMM, open the **Library** workspace, right-click the library server or library share, click **Refresh**, and then review the items in the list.

6. Collect the following information:
   - The fully-qualified domain name (FQDN) of the domain that you chose in prerequisite 1. This is the domain that the host cluster and the virtual machines that comprise the gateway will join.
   - The name that you will give to the host cluster.
   - The name of the host groups for which the gateway should be available.
   - The name of the shared folder on the Scale-Out File Server that you will use with the gateway.
   - The name of a domain account that has permissions to add computers to the domain in the first item in this list. Also, from this domain account, create a Run As account in VMM, and record the name of the Run As account. For more information, see How to Create a Run As Account in VMM.

     Because this account will be used by VMM to manage the gateway, the service template will add this account to the local **Administrators** group on the virtual machines that together comprise the gateway.
   - The name of a domain user account. The service template will add this account to the local **Administrators** group on the virtual machines that comprise the gateway, to ensure that administrative access to the virtual machines is always available. Create a Run As account in VMM from this domain account also.
   - Product keys for the operating system on the virtual machines that comprise the gateway. If you have these product keys, have this information available as you configure the gateway.

     If you do not have product keys and you are creating an evaluation deployment, you must edit your chosen service template to remove the configurable service setting called **@ProductKey@**. Then, at the end of the deployment process, you must connect to the virtual machines that comprise the gateway, and, when prompted, select **Skip** to skip the product key and complete the deployment of the virtual machines.
   - The name that you will use for the gateway itself (the virtual machines that comprise the gateway and that run on the host cluster). Choose a new, valid NetBIOS name containing no more than 15 characters.
   - The IP address reserved for the gateway, if you added an IP address pool on the "Infrastructure" (management) network. This is the address that you specified in the properties of the IP address pool, under **IP addresses to be reserved for other uses**. However, if you are using DHCP for the "Infrastructure" network, make a note to avoid

entering a value for this setting, which in the service templates is called **VMClusterStaticIPAddress**.

- The name of the virtual switch to be used on the back end connection. However, ensure that you do not specify this information until you reach the last step of the procedure that follows.

To use a server running Windows Server 2012 R2 as a gateway with VMM

1. Open the Quick Start Guide that was included in the file that you downloaded in the preparatory step at the beginning of the Prerequisites. Follow instructions in the Quick Start Guide to import the appropriate service template into the VMM library. For more information, see How to Import a Service Template in VMM.

   When you import the template, ensure that you configure references to the following items:

   - The custom resource folder, called **VMClusterSetup.cr**.
   - The virtual hard disk containing the Windows Server 2012 R2 operating system.
   - The blank virtual hard disk that you added to the library for the CSV that the gateway will use.
   - The blank virtual hard disk that you added to the library for the quorum resource that the gateway will use.

   Also follow the instructions in the Quick Start Guide that describe how to customize the service template for your environment.
2. Create a two-node host cluster that runs Windows Server 2012 R2 with the Hyper-V role, and add it to VMM. As with any cluster, in the network infrastructure that connects the cluster nodes, avoid having single points of failure. Ensure that the host cluster is in an appropriate domain, as described in prerequisite 1. For information about the hardware requirements for the host cluster (the servers that run Hyper-V), see Windows Server Gateway Hardware and Configuration Requirements. When you deploy the host cluster, be sure to run the Validate a Configuration Wizard and confirm that the cluster passes the cluster validation tests.
   - For more information about using Windows Server 2012 R2 to deploy a host cluster, see Deploy a Hyper-V Cluster. Then, for more information about adding the host cluster to VMM, see How to Add Trusted Hyper-V Hosts and Host Clusters in VMM or How to Add Untrusted Hyper-V Hosts and Host Clusters in VMM.
   - For more information about using VMM to deploy a host cluster, see Adding Physical Computers as Hyper-V Hosts or as Scale-Out File Servers in VMM Overview.
3. Verify that the host cluster was successfully added by performing the following actions:
   a. Open the **Fabric** workspace.
   b. On the **Home** tab, in the **Show** group, ensure that **Fabric Resources** is selected.
   c. In the **Fabric** pane, click **Servers**.
   d. Expand the host group where you added the host cluster, click the host cluster, and then in the **Hosts** pane, verify that the host status is **OK**.
4. Associate the logical networks that you created with the appropriate physical adapters on

the nodes in the host cluster. In other words, ensure that the relevant virtual switches on both nodes of the new host cluster have been configured so that the switches specify the correct network sites. You can do this by using the port profile and logical switch that you created as prerequisites, or through direct configuration of the ports in the virtual switches. For more information about configuring these settings on a host cluster, see the following topics:

- How to Configure Network Settings on a Hyper-V Host in VMM
- How to Configure Network Settings on a Host by Applying a Logical Switch in VMM

5. Add a file share from the Scale-Out File Server to the host cluster. To add the file share, on the properties sheet for the host cluster, click the **File Share Storage** tab, and then click **Add**. Select the appropriate file share. If the file share does not appear, review prerequisite 2 in the list of prerequisites.

   After you close the properties sheet and the job completes, open the host cluster properties again, click the **File Share Storage** tab, and confirm that the share is listed with a check mark under **Access Status**.

6. Configure the hosts as dedicated network virtualization gateways. To do this, perform the following steps:

   a. In the **Hosts** pane, right-click one of the hosts (not the host cluster), and then click **Properties**.

   b. Click the **Host Access** tab and then select the check box labeled **This host is a dedicated network virtualization gateway, as a result it is not available for placement of virtual machines requiring network virtualization**. Then click **OK**.

   c. Repeat the process on the other host.

7. On the host cluster, deploy the service. To do this, follow the instructions in the Quick Start Guide that was included in the download. The result will be a pair of virtual machines that use a guest cluster internally for high availability, although they do not use the property in VMM called **Make this virtual machine highly available**. However, the pair of virtual machines together, when deployed on a host cluster, constitute a highly available gateway. The gateway runs Windows Server 2012 R2 and is configured with multiple virtual network adapters and with the necessary role, role services, and features.

8. Perform the following verification tasks to ensure that the service deployment was successful:

   - Confirm that the backend virtual network adapter on the gateway is not connected (it should not be connected yet). In VMM, in the **VMs and Services** workspace, on the **Home** tab, in the **Show** group, click **Services**. Expand **All Hosts** and then click the host group that the host cluster is in. In the **Services** pane, expand the service until you can see the gateway virtual machines, right-click a gateway virtual machine, click **Properties**, and then in the properties sheet, click the **Hardware Configuration** tab. Under **Network Adapters**, confirm that there are three network adapters, and that one of them is labeled **Not connected**.
   - Start the new service and confirm that the virtual machines enter the **Running** state.
   - With the virtual machines running, on the VMM server, open a command prompt as an administrator, and then type **ping** followed by the name or IP address of the

gateway itself. Press Enter and confirm that a response is received from the gateway. If a response is not received, review possible causes, such as DNS settings, firewall settings, and the state of the gateway cluster.

Important

- On the virtual machines that constitute a gateway, avoid directly specifying VLAN information for the virtual network adapters. The provider software requires this information to be supplied through network sites configured in VMM.
- On the virtual machines that constitute a gateway, if you must disable any integration services (which are all enabled by default), be sure that you do not disable the integration service called **Data Exchange**, which is a required service.

9. Open the **Fabric** workspace.
10. On the **Home** tab, in the **Show** group, ensure that **Fabric Resources** is selected.
11. In the **Fabric** pane, expand **Networking**, and then click **Network Service**.

    Network services include gateways, virtual switch extensions, network managers, and top-of-rack (TOR) switches.
12. On the **Home** tab, in the **Add** group, click **Add Resources**, and then click **Network Service**.

    The Add Network Service Wizard opens.
13. On the **Name** page, enter a name and optional description for the gateway, and then click **Next**.
14. On the **Manufacturer and Model** page, in the **Manufacturer** list, select **Microsoft**, and in the **Model** list, select **Microsoft Windows Server Gateway**. Then click **Next**.
15. On the **Credentials** page, specify the domain account that has permissions to add computers to the domain. This is the account that you specified for **DomainUserRAA** in the service template. To specify this account, click **Browse** and then on the **Select a Run As Account** dialog box, select the account. Then click **Next**.
16. On the **Connection String** page, in the **Connection string** box, type the connection string for the gateway to use, and then click **Next**. For a gateway running Windows Server 2012 R2, include the following items in the connection string, separated by semicolons (;).
    - **VMHost=** followed by the name of the host cluster.
    - **GatewayVM=** followed by the name of the virtual machine.
    - **BackendSwitch=** followed by the name of the virtual switch used on the back end connection. When you specify this, you complete the network connections in the correct way, which is to use the connection string to connect the third virtual network adapter to the correct virtual switch.

    You can also include one or more of the following items in the connection string, separated by semicolons:

    - **DirectRoutingMode=True** as the option that specifies a forwarding gateway (optional). If you include this option, configure only one VM network to use the gateway. When you configure that VM network, choose the connectivity setting for connecting directly to an additional logical network, and do not choose the NAT

setting. Using other connectivity settings will not work with a forwarding gateway.

If you include **DirectRoutingMode=True**, you must also include the following parameter:

- **FrontEndServerAddress=** followed by the IP address of this routing gateway on the external network. Network routing devices on the external network should point to this endpoint to get access to the VM network behind the gateway.

- **VPNServerAddress=** followed by the IP address of this VPN endpoint to report to tenants. This is only required if this gateway is behind an external load balancer.
- **MaxVMNetworksSupported=** followed by the number of VM networks that can be used with this gateway. If **DirectRoutingMode** is not specified or is not set to **True**, the default value is 50, and the maximum value is 100. If **DirectRoutingMode** is set to **True**, the default value is 1, and it cannot be set any higher.

For example, you might enter the following connection string. Note that this is a connection string for a gateway that does not use forwarding:

VMHost=GatewayHost1.contoso.com;GatewayVM=GatewayVM1.contoso.com;BackendSwitch=VirtualSwitch1

17. On the **Certificates** page, click **Next**.
18. On the **Provider** page, in the **Configuration provider** list, ensure that **Microsoft Windows Server Gateway Provider** is selected, and then click **Test** to use the selected provider to run basic validation tests against the gateway. If tests indicate that the provider works correctly for the gateway, click **Next**.

    Results that say **Passed** or **Failed** indicate whether the provider works as expected. One possible cause of failure is insufficient permissions in the Run As account. Results that say **Implemented** and **Not implemented** are informational only, and indicate whether the provider supports a particular API.
19. On the **Host Group** page, select one or more host groups to which the gateway will be available. Ensure that you include the host groups that are associated with the network sites that you plan to connect to the gateway.
20. On the **Summary** page, review and confirm the settings, and then click **Finish**.
21. After the gateway is created, under **Network Services**, find the listing for the gateway. Right-click the listing, click **Properties**, click **Connectivity**, and then specify the following:
    - Select the **Enable front end connection** check box, and then select the virtual network adapter and the network site that provides connectivity outside the hosting-provider or enterprise datacenter. If you will allow VPN connections, the network site needs to be routable to and from the Internet. Also, the network site must have a static IP address pool.
    - Select the **Enable back end connection** check box, and then select the **BackEnd** virtual network adapter and a network site in a logical network within the hosting-provider or enterprise datacenter. The logical network must have Hyper-V network virtualization enabled. Also, the network site must have a static IP address pool.

    Note

    If you do not see the network sites that you expect, ensure that the network

settings of the host cluster have been configured as intended. Also, in the gateway properties, on the **Host Group** tab, confirm that you have added all the host groups that are associated with the network sites that you want to select.

A variety of network diagnostic tools are available for reviewing the state of the gateway. For information about tools such as the Windows PowerShell cmdlet Test-VMNetworkAdapter, see New Networking Diagnostics with PowerShell in Windows Server 2012 R2.

When you are ready to configure the VM network that uses the newly added gateway, first obtain IP address and authentication details provided by your tenant, customer, or client, as described in the Prerequisites for gateways section in Configuring VM Networks and Gateways in VMM. Specify those settings in the wizard or property sheet for the VM network. Also, in the same wizard or property sheet, on the **Connectivity** page or tab, choose the appropriate setting for the connectivity of the gateway. The settings are described in the bulleted list under Gateway configuration and options earlier in this topic.

See Also

Configuring VM Networks and Gateways in VMM

Windows Server Gateway

Windows Server Gateway Hardware and Configuration Requirements

Configuring Networking in VMM

How to Create a VM Network in VMM in System Center 2012 R2

How to Add a Gateway in VMM in System Center 2012 R2

How to Add a Gateway in VMM in System Center 2012 SP1

How to Create a VM Network in VMM in System Center 2012 SP1

With VMM in System Center 2012 Service Pack 1 (SP1) and System Center 2012 R2, you can configure virtual machine networks (VM networks) on top of your logical networks. This topic describes how you can create a VM network in VMM in System Center 2012 SP1 only. For information about how to create a VM network in VMM in System Center 2012 R2, see How to Create a VM Network in VMM in System Center 2012 R2.

VM networks make use of network virtualization or other network configuration options. Network virtualization extends the concept of server virtualization to allow you to deploy multiple virtual networks (VM networks) on the same physical network. VM networks can also be configured in other ways, as described in Configuring VM Networks and Gateways in VMM.

Important

- For more information about the ways that you can use VM networks and other networking options to support your virtual machine configurations, see Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2.
- For illustrations of VM network configurations, see Configuring VM Networks in VMM Illustrated Overview.
- To understand the configuration of VM networks that use network virtualization, it can be useful to review the illustrations and descriptions (especially the first illustration) of Hyper-V

network virtualization in Network Virtualization technical details. Hyper-V network virtualization is found in Windows Server 2012 and Windows Server® 2012 R2.

In the following table, identify the VM network option that you want, based on the descriptions in Configuring VM Networks and Gateways in VMM. After you identify the VM network option, confirm that your logical network has been configured correctly, and then go to the appropriate procedure within this topic. For more information about configuring logical networks, see How to Create a Logical Network in VMM.

Intended VM network option	Correct setting for the logical network on which you will add the VM network	Procedure within this topic
Hyper-V network virtualization (in other words, using isolation)	Select the check box to enable network virtualization.	Create a VM network on a logical network where network virtualization is enabled
VLAN-based configuration	Select **Network sites within this logical network are not connected**. If you are using private VLAN technology, also select the check box for private VLANs. Otherwise, do not select it.	Create a VM network on a logical network that uses VLANs for isolation
One VM network that gives direct access to a logical network (by using "no isolation")	Either leave all check boxes cleared, or select the check box to enable network virtualization.	Create a VM network that gives direct access to a logical network (no isolation)
Using external networks that are implemented through a vendor network-management console	Do not create the logical network manually from within VMM. Instead, follow the steps in the next column to the right. The logical network settings will be imported from the database in the vendor network-management console.	Add the virtual switch extension manager that is associated with your vendor network-management console, as described in How to Add a Virtual Switch Extension Manager in System Center 2012 SP1.

Create a VM network on a logical network where network virtualization is enabled

Important

- For information about prerequisites and options for VM networks and gateways, see Configuring VM Networks and Gateways in VMM.
- If you want to create a VM network and configure it with a gateway at the same time, you must first add the gateway to your VMM configuration. You can also add a gateway later,

then open the property sheet of an existing VM network and configure the VM network to use the gateway. For more details, see How to Add a Gateway in VMM in System Center 2012 SP1.

To create a VM network on a logical network where network virtualization is enabled

1. Open the **VMs and Services** workspace.
2. On the **Home** tab, in the **Show** group, click **VM Networks**.
3. In the **VMs and Services** pane, click **VM Networks**.
4. On the **Home** tab, in the **Create** group, click **Create VM Network**.

   The **Create VM Network Wizard** opens.
5. On the **Name** page, enter a name and optional description, and then in the **Logical network** list, select the logical network on which you want to create the VM network. (This must be a logical network on which network virtualization is enabled.) Then click **Next**.

   Note

   The wizard pages and VM network properties that you can configure will vary depending on the properties of the logical network that you selected.
6. On the **Isolation** page, select **Isolate using Hyper-V network virtualization**. (If you do not want to use network virtualization, return to the table at the beginning of this topic and choose a procedure that matches your networking goals.) If needed, change the settings for the IP address protocol for the logical network and the IP address protocol for the VM network. Then click **Next**.
7. On the **VM Subnets** page, click **Add**, enter a name for the IP subnet and specify the subnet by using CIDR notation. Add more VM subnets as needed, and then click **Next**.
8. On the **Gateway** page, select one of the following options, and then click **Next**.
   - **No connectivity:** Select this if option if the virtual machines on this VM network will communicate only with other virtual machines on this VM network. (You can also select this option if you plan to configure the gateway properties of this VM network later.)
   - **Remote networks:** Select this option if the virtual machines on this VM network will communicate with other networks through a VPN tunnel, and then, on the **VPN gateway device** list, select the VPN gateway device that you want to use.

     If you select **Remote networks** and select a **VPN gateway device**, the **VPN Connection** and **VPN Settings** pages of the wizard appear. Fill in these pages based on information that you obtain from the administrator of that VPN gateway, for example, information about authentication and certificates. For more details, see “Prerequisites for gateways” in Configuring VM Networks and Gateways in VMM. After you fill in the settings on each page, click **Next**.
   - **Local networks:** Select this option if the virtual machines on this VM network will communicate with other networks in this data center, and then, on the **Gateway device** list, select the gateway device that you want to use.

9. On the **Summary** page, review and confirm the settings, and then click **Finish**.
10. Verify that the VM network appears in the **VM Networks and IP Pools** pane.

Create a VM network on a logical network that uses VLANs for isolation

Important
For information about prerequisites and options for VM networks, see Configuring VM Networks and Gateways in VMM.

To create a VM network on a logical network that uses VLANs for isolation

1. Open the **VMs and Services** workspace.
2. On the **Home** tab, in the **Show** group, click **VM Networks**.
3. In the **VMs and Services** pane, click **VM Networks**.
4. On the **Home** tab, in the **Create** group, click **Create VM Network**.

   The **Create VM Network Wizard** opens.
5. On the **Name** page, enter a name and optional description, in the **Logical network** list, select a logical network, and then click **Next**.

   Note
   The wizard pages and VM network properties that you can configure will vary depending on the properties of the logical network that you selected.
6. On the **Isolation** page, select one of the following, and then click **Next**. If you do not see these options, confirm that you selected the logical network that you intended, and review the table at the beginning of this topic.
   - **Automatic:** Select this option to have VMM automatically configure the isolation of the VM network. VMM will select a network site and subnet VLAN, based on the ones that are available on the logical network.
   - **Specify a VLAN:** Select this option to manually configure the isolation of the VM network, and then, in the **Logical network definition** list, select a network site (which is also called a logical network definition) and, in the **Subnet VLAN** list, select a VLAN.

     Note
     This option is available only to Administrators and Fabric Administrators (Delegated Administrators). Tenant Administrators can select only the **Automatic** option.
7. On the **Summary** page, review and confirm the settings, and then click **Finish**.
8. Verify that the VM network appears in the **VM Networks and IP Pools** pane.

Create a VM network that gives direct access to a logical network (no isolation)

Important
For information about prerequisites and options for VM networks, see Configuring VM Networks and Gateways in VMM.

To create a VM network that gives direct access to a logical network (no isolation)

1. Open the **VMs and Services** workspace.
2. On the **Home** tab, in the **Show** group, click **VM Networks**.
3. In the **VMs and Services** pane, click **VM Networks**.
4. On the **Home** tab, in the **Create** group, click **Create VM Network**.

   The **Create VM Network Wizard** opens.
5. On the **Name** page, enter a name and optional description, in the **Logical network** list, select a logical network, and then click **Next**.

   Note

   The wizard pages and VM network properties that you can configure will vary depending on the properties of the logical network that you selected.
6. On the **Isolation** page, select **No isolation** (or confirm that it is selected), and then click **Next**. If you do not see this option, confirm that you selected the logical network that you intended, and review the table at the beginning of this topic.

   The **No isolation** option is the only available option if the logical network was configured without network virtualization being enabled.

   Note

   Only one VM network with **No isolation** can be created per logical network.
7. On the **Summary** page, review and confirm the settings, and then click **Finish**.
8. Verify that the VM network appears in the **VM Networks and IP Pools** pane.

See Also

How to Create a Logical Network in VMM

Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2

Configuring VM Networks in VMM Illustrated Overview

Configuring VM Networks and Gateways in VMM

How to Create a VM Network in VMM in System Center 2012 R2

Configuring Networking in VMM

How to Create a VM Network in VMM in System Center 2012 R2

With VMM in System Center 2012 R2 and System Center 2012 Service Pack 1 (SP1), you can configure virtual machine networks (VM networks) on top of your logical networks. This topic describes how you can create a VM network in VMM in System Center 2012 R2 only. For information about how to create a VM network in VMM in System Center 2012 SP1, see How to Create a VM Network in VMM in System Center 2012 SP1.

VM networks make use of network virtualization or other network configuration options. Network virtualization extends the concept of server virtualization to allow you to deploy multiple virtual networks (VM networks) on the same physical network. VM networks can also be configured in other ways, as described in Configuring VM Networks and Gateways in VMM.

Important

- For more information about the ways that you can use VM networks and other networking options to support your virtual machine configurations, see Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2.
- For illustrations of VM network configurations, see Configuring VM Networks in VMM Illustrated Overview.
- To understand the configuration of VM networks that use network virtualization, it can be useful to review the illustrations and descriptions (especially the first illustration) of Hyper-V network virtualization in Network Virtualization technical details. Hyper-V network virtualization is found in Windows Server 2012 and Windows Server 2012 R2.

In the following table, identify the VM network option that you want to use, based on the descriptions in Configuring VM Networks and Gateways in VMM. After you identify the VM network option, confirm that your logical network has been configured correctly, and then go to the appropriate procedure within this topic. For more information about configuring logical networks, see How to Create a Logical Network in VMM.

Intended VM network option	Correct setting for the logical network on which you will add the VM network	Procedure to follow
Hyper-V network virtualization (that is, using isolation)	Select **One connected network**, and select the check box to enable network virtualization.	Create a VM network on a logical network where network virtualization is enabled
VLAN-based configuration	In most cases, select **VLAN-based independent networks**. However, if you are using private VLAN technology, select **Private VLAN (PVLAN) networks**.	Create a VM network on a logical network that uses VLANs for isolation
One VM network that gives direct access to a logical network (by using "no isolation")	The VM network might already have been created when the logical network was created, depending on the options that were selected at that time. For more information, see the link in the column to the right.	Create a VM network that gives direct access to a logical network (no isolation)
Using external networks that are implemented through a virtual switch extension or network manager (vendor	Follow the procedure in the topic listed in the next column. Also be sure to review the capabilities of your virtual switch extension or network	How to Add a Virtual Switch Extension or Network Manager in System Center 2012 R2.

Intended VM network option	Correct setting for the logical network on which you will add the VM network	Procedure to follow
network-management console)	manager to determine if you can configure setting information in the virtual switch extension or network manager, or if you have the option to configure it directly in VMM.	

Create a VM network on a logical network where network virtualization is enabled

Important

- For information about prerequisites and options for VM networks and gateways, see Configuring VM Networks and Gateways in VMM.
- If you want to create a VM network and configure it with a gateway at the same time, you must first add the gateway to your VMM configuration. You can also add a gateway later, then open the property sheet of an existing VM network and configure the VM network to use the gateway. For more details, see How to Add a Gateway in VMM in System Center 2012 R2 or How to Use a Server Running Windows Server 2012 R2 as a Gateway with VMM.

To create a VM network on a logical network where network virtualization is enabled

1. Open the **VMs and Services** workspace.
2. On the **Home** tab, in the **Show** group, click **VM Networks**.
3. In the **VMs and Services** pane, click **VM Networks**.
4. On the **Home** tab, in the **Create** group, click **Create VM Network**.

   The Create VM Network Wizard opens.
5. On the **Name** page, type a name and an optional description, and then in the **Logical network** list, select the logical network on which you want to create the VM network. (This must be a logical network on which network virtualization is enabled.) Then click **Next**.

   Note

   The wizard pages and VM network properties that you can configure will vary depending on the properties of the logical network that you selected.
6. On the **Isolation** page, select **Isolate using Hyper-V network virtualization**. (If you do not want to use network virtualization, return to the table earlier in this topic and choose a procedure that matches your networking goals.) If needed, change the settings for the IP address protocol for the logical network and the IP address protocol for the VM network. Then click **Next**.
7. On the **VM Subnets** page, click **Add**, type a name for the IP subnet, and specify the subnet by using CIDR notation. Add more VM subnets as needed, and then click **Next**.

8. On the **Connectivity** page, if you see the message **No network service that specifies a gateway has been added to VMM**, proceed to the next step. Otherwise, configure connectivity (gateway) properties according to the following guidelines:
   - **No connectivity** Leave all check boxes cleared if the virtual machines on this VM network will communicate only with other virtual machines on this VM network. You can also leave the check boxes cleared if you plan to configure the gateway properties of this VM network later.
   - **Connect to another network through a VPN tunnel** Select this option if the virtual machines on this VM network will communicate with other networks through a VPN tunnel. If the device will use the Border Gateway Protocol, also select the check box to enable this protocol. In the **Gateway device** list, select the VPN gateway device that you want to use. Confirm that the capabilities that are listed for the device are as expected.

     If you select **Connect to another network through a VPN tunnel** and select a **Gateway device**, the **VPN Connections** page of the wizard appears. If you selected the check box for Border Gateway Protocol, the **Border Gateway Protocol** page also appears. Fill in these pages based on information that you obtain from the administrator of that VPN gateway, for example, information about the VPN endpoint and the bandwidth. For more details, see Prerequisites for gateways in Configuring VM Networks and Gateways in VMM.
   - **Connect directly to an additional logical network** Select this option if the virtual machines on this VM network will communicate with other networks in this data center. Also select either **Direct routing** or **Network address translation (NAT)**. In the **Gateway device** list, select the gateway device that you want to use. Confirm that the capabilities that are listed for the device are as expected.
9. After you complete the options on each page that is related to connectivity, click **Next**.
10. On the **Summary** page, review and confirm the settings, and then click **Finish**.
11. Verify that the VM network appears in the **VM Networks and IP Pools** pane.

Create a VM network on a logical network that uses VLANs for isolation

Important
For information about prerequisites and options for VM networks, see Configuring VM Networks and Gateways in VMM.

To create a VM network on a logical network that uses VLANs for isolation

1. Open the **VMs and Services** workspace.
2. On the **Home** tab, in the **Show** group, click **VM Networks**.
3. In the **VMs and Services** pane, click **VM Networks**.
4. On the **Home** tab, in the **Create** group, click **Create VM Network**.

   The Create VM Network Wizard opens.
5. On the **Name** page, type a name and an optional description, and then in the **Logical network** list, select a logical network. Click **Next**.

Note
The wizard pages and VM network properties that you can configure will vary depending on the properties of the logical network that you selected.

6. On the **Isolation Options** page, select one of the following options, and then click **Next**. If you do not see these options, confirm that you selected the logical network that you intended, and review the table earlier in this topic.
   - **Automatic** Select this option to have VMM automatically configure the isolation of the VM network. VMM will select a network site and subnet VLAN, based on those that are available on the logical network.
   - **Specify a VLAN** Select this option to manually configure the isolation of the VM network, and then select the **Network site** and **Subnet VLAN**.

     Note
     This option is available only to Administrators and Fabric Administrators (Delegated Administrators). Tenant Administrators can select only the **Automatic** option.
7. On the **Summary** page, review and confirm the settings, and then click **Finish**.
8. Verify that the VM network appears in the **VM Networks and IP Pools** pane.

Create a VM network that gives direct access to a logical network (no isolation)

In VMM in System Center 2012 R2, when you create a logical network as one connected network, you have the option to create a VM network at the same time. If the logical network was created with the following two options selected, a VM network was also created:

- **One connected network**
- **Create a virtual network with the same name to allow virtual machines to access this logical network directly**

Therefore, before you try to create a VM network that gives direct access to a logical network, check for a VM network with the same name as the logical network. If you are viewing the logical network in VMM, you can perform this check by right-clicking the logical network and then clicking **View Dependent Resources**. Another way to check for a VM network and view details about that network is described in the following procedure.

Important
For information about prerequisites and options for VM networks, see Configuring VM Networks and Gateways in VMM.

To create a VM network that gives direct access to a logical network (no isolation)

1. Open the **VMs and Services** workspace.
2. On the **Home** tab, in the **Show** group, click **VM Networks**.
3. In the **VMs and Services** pane, click **VM Networks**.
4. In the **VM Networks and IP Pools** pane, check for a VM network that has the same name as the logical network that you want to give direct access to. If one exists, it is likely

that the VM network was created at the same time as the logical network and gives direct access to the logical network. To determine whether a VM network provides direct access, right-click it, click **Properties**, and look at the tabs that are visible in the property sheet. If **Name** and **Access** are the only tabs, then the VM network provides direct access to the logical network listed on the **Name** tab.

If there is already a VM network that provides direct access to the logical network, skip the rest of this procedure.

5. On the **Home** tab, in the **Create** group, click **Create VM Network**.

   The Create VM Network Wizard opens.

6. On the **Name** page, type a name and an optional description, and then in the **Logical network** list, select a logical network. Click **Next**.

   Note
   The wizard pages and VM network properties that you can configure will vary depending on the properties of the logical network that you selected.

7. Review the page or pages that appear. If the pages that you see are not as expected, confirm that you selected the logical network that you intended, and review the table earlier in this topic. Proceed through the wizard as follows:
   - If the logical network that you selected is configured as **One connected network** without network virtualization, the **Summary** page appears. Proceed to the last step of this procedure.
   - If the logical network that you selected is configured with network virtualization enabled, the **Isolation** page appears. Select **No isolation**, and then click **Next**.

     Note
     Only one VM network with **No isolation** can be created per logical network.

8. On the **Summary** page, review and confirm the settings, and then click **Finish**. Verify that the VM network appears in the **VM Networks and IP Pools** pane.

See Also

How to Create a Logical Network in VMM

Common Scenarios for Networking in System Center 2012 SP1 and System Center 2012 R2

Configuring VM Networks in VMM Illustrated Overview

Configuring VM Networks and Gateways in VMM

How to Create a VM Network in VMM in System Center 2012 SP1

Configuring Networking in VMM

How to Create IP Address Pools for VM Networks in VMM

You can use the following procedure to create a static IP address pool for a VM network in VMM in System Center 2012 Service Pack 1 (SP1) or System Center 2012 R2. When you create a static IP address pool for a VM network, VMM can assign static IP addresses to Windows-based virtual machines (running on any supported hypervisor platform) that use the VM network. By

using static IP address pools, IP address management for the virtual environment is brought within the scope of the VMM administrator.

Important
For guidelines about when IP pools are necessary on a VM network, when they are optional, and when to create an IP pool in a logical network rather than a VM network, see “Static IP Address Pools” in Configuring Logical Networking in VMM Overview.

Account requirements To complete this procedure, you must be a member of the Administrator or Delegated Administrator user role.

Prerequisites

Perform this procedure only after all the other networking elements have been configured for your virtual machines, including the logical network (which is used as a foundation for VM networks), the network sites for the logical network, and the VM network for which you want to create IP address pools. For more information, see Configuring VM Networks and Gateways in VMM.

To create static IP address pools for VM networks in VMM

1. Open the **VMs and Services** workspace.

   Note
   Because this IP address pool is for virtual machines, it is created in the **VMs and services** workspace, not in the **Fabric** workspace.
2. In the **VMs and Services** pane, click **VM Networks**.
3. On the **Home** tab, in the **Show** group, click **VM Networks**.

   The **VM Network** tab appears.
4. Click the **VM Network** tab.
5. In the **VM Networks and IP Pools** pane, click the VM network where you want to create the IP pool.
6. On the **VM Network** tab, in the **Create** group, click **Create IP Pool**.

   The Create Static IP Address Pool Wizard opens.
7. On the **Name** page, do the following, and then click **Next**.
   a. Enter a name and optional description for the IP address pool.
   b. In the **VM network** list, make sure that the correct VM network is selected.
   c. In the **VM subnet** list, make sure that the correct VM subnet is selected.
8. On the **IP address range** page, do the following, and then click **Next**:
   a. Under **IP address range**, enter the starting and ending IP addresses from the subnet that will make up the managed IP address pool. The starting and ending IP addresses must be contained within the subnet.

      Note
      Be aware that you can create multiple IP address pools within a subnet. If you create multiple IP address pools within a subnet, the ranges cannot

overlap.

Tip
The **Total addresses** field displays the total number of IP addresses in the specified IP address range.

b. Under **Reserved IP addresses**, specify the IP address ranges that you want to reserve for other purposes. The IP addresses that you want to reserve must fall within the IP address range that you specified in step 8a.

9. Optionally, on the **Gateway** page, click **Insert**, and then specify one or more default gateway addresses and the metric. The default gateway address must fall within the same subnet range as the IP address pool. It does not have to be part of the IP address pool range.

Note
The metric is a value that is assigned to an IP route for a particular network interface that identifies the cost that is associated with using that route. If you use the automatic metric, the metric is automatically configured for local routes based on the link speed.

10. Optionally, on the **DNS** page, specify Domain Name System (DNS)-related information, such as the list of DNS servers and their order, the default DNS suffix for the connection, and the list of DNS search suffixes.

Important
For virtual machines that will join an Active Directory domain, we recommend that you use Group Policy to set the primary DNS suffix. This will ensure that when a Windows-based virtual machine is set to register its IP addresses with the primary DNS suffix, a Windows-based DNS server will register the IP address dynamically. Additionally, the use of Group Policy enables you to have an IP address pool that spans multiple domains. In this case, you would not want to specify a single primary DNS suffix.

11. Optionally, on the **WINS** page, click **Insert**, and then enter the IP address of a Windows Internet Name Service (WINS) server. You can also select the check box that indicates whether to enable NetBIOS over TCP/IP. Be aware that enabling NetBIOS over TCP/IP is not recommended if the address range consists of public IP addresses.
12. On the **Summary** page, confirm the settings, and then click **Finish**.

    The **Jobs** dialog box appears. Make sure that the job has a status of **Completed**, and then close the dialog box.
13. To verify that the IP address pool was created, in the **VM Networks and IP Pools** pane, expand the VM network where you created the pool.

    The IP address pool appears under the VM network.
14. Optionally, repeat this procedure to create additional IP address pools for VM networks.

Note
You can use the Windows PowerShell cmdlets, Get-SCIPAddress and Get-

SCStaticIPAddressPool, to view the states of the IP addresses in an IP address pool. Use the cmdlets with the following syntax, where `<StaticIPAddressPool>` is the name of your static IP address pool:

```
$ippool=Get-SCStaticIPAddressPool -Name <StaticIPAddressPool>

Get-SCIPAddress -StaticIPAddressPool $ippool | Format-Table -property
Address,AssignedToType,State
```

From time to time, you might need to release IP addresses that are in the pool but that are marked by VMM as “inactive.” Releasing them makes them available for reassignment. For more information, see How to Release Inactive IP Addresses for VM Networks in VMM.

As of System Center 2012 R2, after a virtual machine has been deployed in VMM, you can view the IP address or addresses assigned to that virtual machine. To do this, right-click the listing for the virtual machine, click **Properties**, click the **Hardware Configuration** tab, click the network adapter, and in the results pane, click the **Connection details** button.

See Also

How to Release Inactive IP Addresses for VM Networks in VMM

Configuring VM Networks and Gateways in VMM

How to Create a VM Network in VMM in System Center 2012 SP1

How to Create a VM Network in VMM in System Center 2012 R2

Configuring Logical Networking in VMM Overview

How to Create IP Address Pools for Logical Networks in VMM

How to Release Inactive IP Addresses for VM Networks in VMM

With Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1) or System Center 2012 R2, you can use the following procedure to release inactive IP addresses that are in an IP address pool on a VM network. When you release an inactive address, VMM returns the address to the static IP address pool, and considers it available for reassignment. An IP address is considered inactive when either of the following conditions is true:

- A host that was assigned a static IP address through the bare-metal deployment process is removed from VMM management. When you remove the host, any IP and MAC addresses that were statically assigned to virtual machines on the host are also marked as inactive.
- A virtual machine goes into a missing state because it was removed outside VMM.

To release inactive IP addresses for VM networks

1. Open the **VMs and Services** workspace.

   Note
   Because this IP address pool is for virtual machines, it is located in the **VMs and services** workspace, not in the **Fabric** workspace.

2. In the **VMs and Services** pane, click **VM Networks**.
3. On the **Home** tab, in the **Show** group, click **VM Networks**.

The **VM Network** tab appears.

4. Click the **VM Network** tab.
5. In the **VM Networks and IP Pools** pane, expand the VM network.
6. Right-click the desired IP address pool, and then click **Properties**.
7. Click the **Inactive addresses** tab.
8. Select the check box next to each inactive IP address that you want to release, or select the check box in the table header row to select all the addresses, and then click **Release**.

See Also

Configuring Networking in VMM

How to Release Inactive IP or MAC Addresses in VMM

How to Create a VM Network in VMM in System Center 2012 SP1

How to Create a VM Network in VMM in System Center 2012 R2

How to View VMM Network Configuration Diagrams in VMM

With Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1) and System Center 2012 R2, you can view diagrams that show the relationships among networking objects, such as logical networks and VM networks, that you have configured. You can view a diagram of the networking objects on a particular host system or the networking objects on a cloud. A diagram provides a graphical view of network configurations, which supplements the text-based views that are available in the properties sheet for the host or the cloud.

To view VMM network configuration diagrams

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, expand **All Hosts**, and then locate and click the host group that contains a host for which you want to view the network configuration.
3. In the **Hosts** pane, select one of the hosts for which you want to view network diagrams.
4. On the **Host** tab, in the **Window** group, click **View Networking**.
5. As needed, select or clear check boxes for hosts, host groups, or clouds, until the items that you want to view are selected.
6. In the **Show** group, click a view:
   - **VM Networks**: This view shows VM networks and the virtual machines that are connected to them.
   - **Host Networks**: This view shows the logical networks that are configured on the network adapters on the hosts.
   - **Host/VM Networks**: This view shows the logical networks that are configured on the network adapters on the hosts, plus the VM networks on each logical network and the virtual machines on the hosts.
   - **Network Topology**: This view provides an overview of the logical networks, network sites, and VM networks that have been configured on the hosts.
7. In the **Zoom** group and the **Orientation** group, adjust options for the display.

To see information about an element in the diagram, hover over that item.

8. If you want to document the configuration, you can capture the information in the display using one of the following methods:
   - Press the **Print Screen** key, paste the screen image into a graphics application, and then save it.
   - Use your preferred screen capture application.
   - If Microsoft Visio is available for you to use, click the **File** tab (in the upper corner), and then click **Export to Visio**. Specify a path and file name for the Visio file, and then click **Save**.

See Also

Configuring Networking in VMM

Configuring VM Networks in VMM Illustrated Overview

How to Configure Network Settings on a Hyper-V Host in VMM

How to Configure Network Settings on a Citrix XenServer Host

How to Configure Network Settings on a VMware ESX Host

Configuring Ports and Switches in VMM Illustrated Overview

Configuring Storage in VMM

Virtualized workloads in System Center 2012 – Virtual Machine Manager (VMM) require storage resources to meet capacity and performance requirements. VMM recognizes local and remote storage. Local storage represents the storage capacity that is available on a server or that is directly attached to a server. Local storage is typically used for low-cost virtualization solutions. Remote storage offloads work from the server to an external storage device where the storage hardware provides scaling and capacity.

VMM supports the following storage solutions:

- **Block storage**—VMM supports the use of block-level storage devices that expose logical unit numbers (LUNs) for storage, by using Fibre Channel, iSCSI, and Serial Attached SCSI (SAS) connection mechanisms. For more information about Fibre Channel, see Managing Virtual Fibre Channel in VMM.
- **File storage**—VMM supports the use of network shares for storage. Network shares that support the Server Message Block (SMB) 3.0 Protocol can reside on a Windows-based file server or on a network-attached storage (NAS) device from storage vendors such as EMC and NetApp.

VMM introduces a number of new changes for storage provider and automation support that include:

- Support for the Windows Storage Management API (SMAPI). SMAPI was introduced in Windows Server 2012 for the management of directly attached storage and external storage arrays. SMAPI is combined with a Storage Management Provider (SMP), or the Microsoft Standards-Based Storage Management Service and an SMI-S provider. SMAPI supersedes the Virtual Disk Service (VDS) application programming interface (API) in Windows Server 2012. For more information, see An Introduction to Storage Management in Windows Server.

- VMM uses SMAPI to manage external storage by using SMP, or uses SMAPI together with the Microsoft Standards-based Storage Management Service to communicate with storage that is compliant with the Storage Management Initiative Specification (SMI-S). The new Windows Standards-Based Storage Management service replaces the Microsoft Storage Management Service in System Center 2012 – Virtual Machine Manager (VMM), and is an optional server feature that enables communication with SMI-S storage providers. It is enabled during the installation of System Center 2012.
- Storage area network (SAN) migration, which uses the legacy Virtual Disk Service (VDS) hardware provider interface, is not supported after the System Center 2012 release. When you upgrade from System Center 2012, you must remove the VDS hardware provider software from the VMM server and enable the SMI-S or native Windows Management Infrastructure (WMI) SMP provider by using instructions from the storage vendors.
- In addition to discovery and management of iSCSI arrays with static targets, VMM adds support for the discovery and management of iSCSI target arrays that support dynamic and manual targets, for example, Starwind, HP P2000, Dell EqualLogic, and Microsoft iSCSI Software Target.
- VMM supports creation of a thin provisioning logical unit (LU). VMM adds support for the creation of a thin provisioned logical unit on a storage pool. Thin provisioning makes it possible for you to allocate more capacity to specific applications or users than is physically available. The storage array must support thin provisioning, and the storage administrator must enable thin provisioning for a storage pool.
- VMM provides support for the Microsoft iSCSI Software Target by using an SMI-S provider. Microsoft iSCSI is now fully integrated into Windows Server 2012. The installation file (.msi) for the SMI-S provider for Microsoft iSCSI Target Server is included in the installation, in the path of CDLayout.EVAL\amd64\Setup\msi\iSCSITargetPRov\iSCSITargetSMISProvider.msi. For more information about the Microsoft iSCSI Software Target, see:
  - **Configuring an SMI-S Provider for iSCSI Target Server**
  - Introduction of iSCSI Target in Windows Server 2012
  - Six Uses for the Microsoft iSCSI Software Target
- Windows Server 2012 provides support for using Server Message Block (SMB) 3.0 file shares as shared storage for Hyper-V. By using VMM, you can assign SMB file shares to stand-alone servers that are running Hyper-V and clusters. For more information, see How to Assign SMB 3.0 File Shares to Hyper-V Hosts and Clusters in VMM.
- As of System Center 2012 R2, VMM provides support for creating and managing Scale-Out File Servers with Storage Spaces. For more information, see How to Create a Storage Pool from Physical Disks in VMM and How to Create a File Share from a Storage Pool in VMM.

Deploying and managing storage resources

VMM enables you to model, deploy, and manage the following storage resources:

- **Storage discovery**—Administrators often have a limited understanding of underlying storage infrastructures. By using System Center 2012 – Virtual Machine Manager (VMM), you can automatically discover local and remote storage that includes storage arrays, pools, and logical units, such as storage volumes or logical unit numbers (LUNs), disks, volumes, and virtual disks.

- **Storage classification**—You can classify discovered storage by using friendly descriptive names to create and expose a simplified storage model.
- **Storage provisioning**—VMM can create new logical units from available capacity to provision to a server that is running Hyper-V or a host cluster. New logical units can be provisioned by using any of the following methods. The method that you use depends on the type of storage array and the virtualization workload that you must deploy.
    - From available capacity—Create a new logical unit from available capacity is useful when you have a pool of storage available, which lets you control the number of logical units that you create and the size of each logical unit.
    - From a writeable snapshot of an existing logical unit—Create a writeable snapshot of an existing logical unit enables you to rapidly create many copies of an existing virtual disk. You can provision multiple virtual machines in a short amount of time, with minimal load on the hosts. Depending on the array, snapshots use space very efficiently and can be created almost instantaneously.
    - From a clone of a logical unit—Create a clone of an existing logical unit offloads the work of creating a full copy of a virtual disk to the array. Depending on the array, clones typically do not use space efficiently and can take some time to create.
    - From file shares on Windows-based file servers—You can provision new file shares on Windows-based file servers and on NAS devices.
- **Storage allocation**—You can allocate available storage pools and LUNs to defined host groups that can represent, for example, business groups and locations. Resources typically must be allocated on the host group level before they can be assigned to hosts. If you allocate a storage pool, you can create and assign logical units directly from managed hosts in the host group that can access the storage array. In addition, VMM can automatically create logical units from the storage pool, if you use rapid provisioning to provision virtual machines with SAN snapshots or cloning.
- **Storage decommissioning**—VMM can decommission the storage that it manages. This capability is important to avoid running out of storage capacity over time.

Usage scenarios

Typical usage scenarios for storage features include the following:

- **Assigning and adding storage to hosts or clusters**—A host group that requires new storage looks up the storage that allocated it and assigns it to servers that are running Hyper-V or clusters, as required. This automatic assignment of storage works in SAN-based rapid provisioning scenarios in which logical unit numbers are cloned. VMM exposes the storage to the virtual machine hosts, initializes the disks, and formats new volumes. For cluster deployments, VMM creates the required Cluster Shared Volumes (CSV) and physical disk resources, and maps the volume to all cluster hosts so that it is shared across a cluster. VMM can also assign additional storage to a host or cluster that already has storage assigned. VMM automates the unmasking and preparation of the volume. For a cluster, VMM also creates the cluster resources. For instructions, see **How to Configure Storage on a Hyper-V Host**.
- **Cluster creation**—VMM can create a cluster with up to 64 Hyper-V nodes and can automate the assignment of cluster-shared storage as part of the same workflow. To simplify the

creation of new clusters with shared storage is important in a private cloud deployment. For more information, see Creating a Hyper-V Host Cluster in VMM Overview.

- **Scale-Out File Server**— As of System Center 2012 R2, VMM can create a Scale-Out File Server and manage its storage. For more information see Adding Physical Computers as Hyper-V Hosts or as Scale-Out File Servers in VMM Overview.
- **Rapid Provisioning**—Storage arrays can create copies of virtual disks very efficiently with minimal load on the virtual machine host. VMM can leverage this capability to rapidly create virtual machines. VMM recognizes the capabilities of the storage array, when a logical unit contains a file system and a virtual disk, and you can create a template with a virtual disk on a logical unit. VMM can instruct the array to create a copy of a virtual disk by provisioning new storage on the array, by using a snapshot, or by cloning. VMM then exposes the storage to the host by mounting the file system and by associating the virtual disk with the virtual machine. In the VMM console, you use rapid provisioning to create stand-alone virtual machines or service-based machines. You can also integrate rapid provisioning into your own provisioning tools by using Windows PowerShell. For more information, see Rapid Provisioning a Virtual Machine by Using SAN Copy Overview.

Configuring storage automation

Before you begin

Before you begin to configure storage settings, note the following:

- Storage automation with VMM is only supported for servers that are running Hyper-V.
- Do not install the SMI-S provider on the VMM management server. This configuration is not supported.
- WMI SMP providers from Dell EqualLogic and Nexsan must be installed on the VMM management server.
- Check the list in Supported storage arrays to verify that a storage array is supported. Note that VMM recognizes storage on storage arrays that do not appear in this list. However, there is no guarantee that you can perform active management operations, such a logical unit provisioning, masking and unmasking, cloning, and taking snapshots on those storage arrays through VMM. If a storage array is not on this list, we recommend that you contact your storage vendor to determine VMM support.
- If the SMI-S provider type for the storage array is a "proxy" provider that must be installed on a separate server, obtain and install the latest version of the SMI-S provider from your storage vendor on a server that the VMM management server can access over the network by IP address or by the fully qualified domain name (FQDN).
- Notify your storage administrator, when VMM manages the assignment of logical units, that, by default, it creates one storage group or masking set per host that can include the initiators for that host. In a cluster configuration, VMM creates one storage group per cluster node by using all the initiators from that cluster node. A storage group can contain one or more of the host's initiator IDs, such as an iSCSI Qualified Name (IQN) or a World Wide Name (WWN).

  For some storage arrays, it is preferable to use one storage group for the entire cluster, where host initiators for all cluster nodes are contained in that group. To support this configuration, you must set the `CreateStorageGroupsPerCluster` property to `$true` by using the `Set-SCStorageArray` cmdlet in the VMM command shell.

Note

In VMM, a storage group is defined as an object that binds together host initiators, target ports, and logical units. A storage group has one or more host initiators, one or more target ports, and one or more logical units. Logical units are exposed to the host initiators through the target ports.

Storage automation workflow

The following list describes the workflow to discover, to classify, and to assign storage by using VMM:

1. **Discover storage**—From the VMM console, start the Add Storage Devices Wizard, and select the required provider type, Windows-based file server, SMI-S, or WMI SMP. The Windows-based file server and SMI-S providers require an IP address or FQDN. For SMI-S, you connect to the SMI-S storage provider to discover storage. For WMI SMP providers, you select the required provider from a drop-down list box. For instructions, see How to Add and Classify SMI-S and SMP Storage Devices in VMM.
2. **Classify storage**—The process of classifying storage assigns a meaningful classification to storage pools. For example, you might assign a classification of GOLD to a storage pool that resides on the fastest, most redundant storage array. For instructions, see How to Create Storage Classifications in VMM.
3. **Select a method for creating logical units**—Specify how logical units are to be created during virtual machine rapid provisioning. Note that, by default, new logical units are created from available capacity. You only have to modify this default setting if you want to use rapid provisioning with SAN copy technology, such as cloning or snapshots. For instructions, see How to Select a Method for Creating Logical Units in VMM.
4. **Provision storage**—Create logical units of storage. For instructions, see How to Provision Storage Logical Units in VMM. Alternatively, you can create logical units out-of-band by using your array vendor's management tools. If you use this method, it takes some time for VMM to refresh and reflect the changes.
5. **Allocate storage to a host group**—From the Storage node of the VMM console or in the **Properties** dialog box of the target host group, allocate pre-created logical units or storage pools to specific host groups. For instructions, see How to Allocate Storage Logical Units to a Host Group in VMM, and How to Allocate Storage Pools to a Host Group in VMM.

   Note

   If you allocate a storage pool, you can create and assign logical units directly from managed hosts in the host group that can access the storage array. In addition, VMM can automatically create logical units from the storage pool if you use rapid provisioning to provision virtual machines by using SAN snapshots or cloning. During the rapid provisioning process, logical units are automatically created and assigned.
6. **Assign the storage to hosts and clusters**—After you configure storage and assign storage to host groups, you can assign the storage to servers that are running Hyper-V and host clusters as shared via a Cluster Shared Volume (CSV) or available storage. Note that all nodes in the cluster should have access to the storage array by using host bus adapters (HBA) or iSCSI. If you allocated a storage pool to a host group, you can create and optionally

assign logical units directly in the **Properties** dialog box of a host or host cluster. If the storage array supports iSCSI host connectivity, you can create iSCSI sessions to the storage array in the **Properties** dialog box of a host. For instructions, see:

a. How to Configure Storage on a Hyper-V Host in VMM

b. How to Configure Storage on a Hyper-V Host Cluster in VMM

Note

The hosts must be able to access the storage array. For example, if you use a Fibre Channel SAN, each host must have a host bus adapter (HBA) and must be zoned correctly. For more information about Fibre Channel, see Managing Virtual Fibre Channel in VMM.

7. Configured storage can also be decommissioned, if required. For instructions, see How to Remove Storage Logical Units in VMM.

Supported storage arrays

For the latest version of supported storage arrays, see Supported storage arrays for System Center 2012 VMM on the TechNet Wiki.

Managing Virtual Fibre Channel in VMM

Virtual Fibre Channel enables Hyper-V virtual machines (VMs) on host computers to have direct access to Fibre Channel storage area network (SAN) array resources. In this way, applications and workloads that require direct access to SAN logical unit numbers (LUNs) can be virtualized. Using Virtual Fibre Channel, VM failover clusters can also access Fibre Channel SAN arrays.

Glossary of terms

The following terms represent the most important elements of a Virtual Fibre Channel environment:

Fabric. A fabric is one or more Fibre Channel switches that are connected together using Fibre Channel cables. Fabrics are used to access Fibre Channel storage devices. Although the term fabric is generally used to indicate multiple switches, a fabric can be comprised of a single switch.

Switch. A Fibre Channel switch is a network switch comprised of multiple ports and that supports the Fibre Channel (FC) transport protocol.

Classification. A friendly name used to designate a fabric for use in templates. Fabrics can be classified according to availability or service level, for example.

HBA. Host Bus Adapters (HBAs) are network cards installed in host computers and are used to provide connectivity to Fibre Channel devices. Every HBA card is assigned a World Wide Node Name (WWNN), which is shared among each port on the HBA. In turn, each HBA port is assigned a World Wide Port Name (WWPN). HBA ports are referred to as initiator ports.

NPIV. N_Port ID Virtualization (NPIV) is a standard used to create and map multiple virtual Fibre Channel (vHBA) ports to a single physical Fibre Channel N_port.

vHBA. The virtualized HBA. Multiple vHBAs can be mapped to a single HBA. The vHBA uses NPIV to address a VM's WWN within a host HBA.

Virtual SAN. In the context of VMM, a virtual SAN (vSAN) defines a group of physical Fibre Channel ports that are connected to a physical SAN array. Not to be confused with the vSAN product by VMware.

WWNN. World Wide Node Name (WWNN) is a globally unique number assigned to a Fibre Channel switch, HBA card, storage drive or other endpoint device.

WWPN. World Wide Port Number (WWPN) is a globally unique number assigned to a Fibre Channel port, similar to that of an Ethernet MAC address. The WWPN allows the storage fabric to recognize a particular HBA port.

Zone. A collection of Fibre Channel ports that are permitted to communicate with each other on a storage fabric

Zoning. A method of subdividing a storage area network into separate zones, or subsets of nodes on the network.

Zone alias. Several zone members that are grouped together and designated with a friendly name.

Zone members. Any device with a WWNN that is attached to a storage fabric and belongs to a zone.

Zone set. A database of zone definitions that fabrics use to determine traffic routes. All Fibre Channel switches keep a copy of the zone set. An active zone set refers to all the zones that are available to the fabric. An inactive zone set refers to those zones whose information has not yet been propagated to the fabric and hence are not available to the fabric. Zone information is always changed or updated in an inactive zone set first; such information cannot be changed in an active zone set.

Supported Configurations

The following configurations are supported for Virtual Fibre Channel:

- Single storage array connected a single fabric (comprised of single or multiple switches) connected to a single vSAN.
- Single storage array connected to multiple fabrics (comprised of single or multiple switches per fabric) connected to a single vSAN.
- Multiple storage arrays connected to a single fabric (comprised of single or multiple switches) connected to a single vSAN.
- Multiple storage arrays connected to multiple fabrics (comprised of single or multiple switches per fabric) connected to multiple vSANs. This configuration provides dual-redundant paths to storage arrays.

Note

A vSAN can only include HBAs from a single fabric

Prerequisites

In order to successfully deploy Virtual Fibre Channel in your network environment, the following prerequisites must be met:

- Ensure that the latest firmware and drivers are installed for storage arrays, switches and HBAs.

- Ensure that storage arrays can present logical units (LUs).
- Enable NPIV on Fibre Channel switches and HBAs.
- Host computers must be running Windows Server 2012 or newer release.
- Ensure that an SMI-S provider is installed. VMM manages Fibre Channel fabrics and SAN devices using the SMI-S provider.

Steps to Deploy Virtual Fibre Channel

Complete the following tasks to deploy Virtual Fibre Channel in your environment:

- Discover Fibre Channel fabrics and assign classifications to each fabric. For step-by-step instructions, see Adding and Classifying Virtual Fibre Channel Fabrics.
- For each host computer that is managed, create vSANs by grouping host HBA ports. For step-by-step instructions, see Managing Virtual SANs.
- Create zones and activate any inactive zone sets. Zones connect each host or VM vHBA to a storage array. For step-by-step instructions, see Managing Virtual Fibre Channel Zones.
- Create storage array LUNs and register (unmask) them for a host, VM, or service tier as needed. For step-by-step instructions, see Managing Storage LUNs for Virtual Fibre Channel.
- Create a VM template, and for each virtual Fibre Channel adapter (vHBA) that is created, specify dynamic or static WWN assignments and select the fabric classification. The fabric classification is used to connect a vHBA to a storage fabric. For more information, see Creating a VM for Virtual Fibre Channel,
- Create a VM, select the destination host to deploy the VM to, zone a Fibre Channel array to the VM, add a disk to the VM, create a LUN, and then register (unmask) the LUN to theVM. For more information, see Creating a VM for Virtual Fibre Channel,
- Create a service template, add VM templates to it, and for each virtual Fibre Channel adapter (vHBA) that is created, specify dynamic or static WWN assignments and select the fabric classification. For more information, see Creating a Service Tier for Virtual Fibre Channel,
- Create and deploy the service tier, zone a Fibre Channel array to the service tier, add a disk to the service tier, create a LUN, and register (unmask) the LUN to the service tier. For more information, see Creating a Service Tier for Virtual Fibre Channel,

See Also

Hyper-V Virtual Fibre Channel Troubleshooting Guide

Configuring Storage in VMM

Adding and Classifying Virtual Fibre Channel Fabrics

You can discover and add Fibre Channel storage fabrics to manage in Virtual Machine Manager (VMM) for System Center 2012 R2. You can also assign classifications for the added fabrics.

Before you begin, verify the following prerequisites:

- Ensure you are a member of the Administrator user role, or a member of the Delegated Administrator user role.
- Ensure you have installed the SMI-S provider for the device on a server that the VMM management server can access over the network by IP address or FQDN. For information about how to obtain SMI-S providers, see Configuring Storage in VMM.

Note

Do not install the SMI-S provider on the VMM management server. This configuration is not supported.

You can create a Run As account before running the Add Storage Devices Wizard, or during the wizard. The Run As account must have permissions to access the SMI-S provider. You can create a Run As account in the **Settings** workspace. For more information about Run As accounts, see How to Create a Run As Account in VMM.

How to add and classify Fibre Channel fabrics

Use the following procedures to discover and classify Fibre Channel storage fabrics.

To discover and classify Fibre Channel fabrics

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, click **Storage**.
3. On the **Home** tab, click **Add Resources**, and then click **Storage Devices** to start the **Add Storage Devices Wizard**.
4. On the **Select Provider Type** page, select **Fibre Channel fabric discovered and managed by a SMI-S provider**.
5. On the **Specify Discovery Scope** page, do the following:
   a. In the **Provider IP address or FQDN** box, enter either the IP address or the FQDN of the storage provider.
   b. In the **TCP/IP port** box, enter the port number that is used to connect to the provider.
   c. If required, select **Use Secure Sockets Layer (SSL) connection** to enable HTTPS for communicating with the provider.
   d. Next to the **Run As account** box, click **Browse**, and select a Run As account that can access the storage provider. If you do not have an account. click **Browse**, and then in the **Select a Run As Account** dialog box, click **Create Run As Account** and follow the instructions.
6. On the **Gather Information** page, VMM automatically discovers and imports the Fibre Channel fabric information. If the discovery process succeeds, the discovered fabric name, switches and fabric World Wide Node Names (WWNN) are listed on the page. When the process successfully completes, click **Next**. To retry the discovery process for an unsuccessful attempt, click **Scan Provider**.

   Note

   If you selected the SSL connection, the following occurs:

   a. During discovery the **Import Certificate** dialog box appears. Review the certificate information for the storage provider, and then click **Import**.
   b. By default, when you import a certificate for a storage provider, verification of the common name (CN) that is used in the certificate occurs. However, this may cause an issue where storage discovery fails when the certificate does not contain a CN

value, or the CN value does not match the expected format of NetBIOS name, FQDN or IP address that VMM uses.

7. On the **Fibre Channel Fabrics** page, do the following for each storage fabric that requires a classification:
   a. In the **Storage Device** column, select the check box next to a Fibre Channel fabric that you want VMM to manage.
   b. In the **Classification** column, select the classification that you want to assign to the fabric. For instructions on creating a new fabric classification, see How to [How to Create Storage Classifications in VMM](). When finished, click **Next**.
8. On the **Summary** page, confirm the settings, and then click **Finish**.

Note

The fabric classification task is separate from that for storage classification, although the concept is similar.

See Also

[Managing Virtual Fibre Channel in VMM]()

[Configuring Storage in VMM]()

Managing Virtual Fibre Channel Zones

Zones are used to connect a Fibre Channel array to a host computer or virtual machine (VM). Specifically, the storage array target ports are mapped to the HBA ports on the host or to the virtual HBA (vHBA) ports for the VM. The HBA and vHBA ports are referred to as initiator ports. The zoning process is also known as onboarding.

You can create zones for a host, a VM, or both. For Hyper-V failover clusters, a zone is needed for each host computer in the cluster.

Zones are grouped into zonesets, which use common Fibre Channel fabric devices. When all zones in a zone set have been added, modified, or removed as needed, the zoneset must be activated. Zoneset activation pushes information for each zone down to the Fibre Channel switches in the selected fabric.

Only members of the same zone can communicate with each other.

Creating zones

Use the following procedures to create new zones and then activate the zoneset. If you want to add a storage array to a Hyper-V cluster, you need to zone the array to each host computer first. Similarly, if you want to add an array to a guest cluster, you need to zone the array to each VM first.

To create a new zone

1. Open the **VMs and Services** workspace.
2. In the **Services** pane, right-click the applicable VM, and then click **Properties**.
3. On the **Properties** page, click the **Storage** tab, click **Add**, and then click **Add Fibre Channel Array**.

4. On the **Create New Zone** dialog box, do the following:
    a. In the **Zone Name** box, enter a name for the zone.
    b. In the **Storage Array** box, select an array from the drop-down list.
    c. In the **Fabric** box, select a switch from the drop-down list.
    d. Under **Storage array target ports**, select the applicable WWPM port or ports.
    e. Under **Virtual machine initiator**, select the applicable WWPM port or ports.
    f. When complete, click **Create**.
    g. To view zone aliases in the user interface that are available for selection, click **Show aliases**.

Activating zonesets

Use the following procedures to activate an inactive zoneset.

Note
Activating a zoneset may cause some downtime in the fabric as information is propagated to all the switches.

To activate a zoneset

1. Open the **Fabric** workspace.
2. Under **Name**, click the applicable inactive zoneset and then on the **Home** tab, click **Activate Zoneset**.

Editing and viewing zones

Use the following procedures to edit zone information or remove a zone from a zoneset.

To edit zone name and description or to remove a zone

1. Open the **Fabric** workspace.
2. Under **Name**, right-click the applicable zoneset, and then click **Properties**.
3. On the **Properties** page, click the **Zones** tab.
4. To edit a zone in a zoneset, click **Edit**, and change the zone name and description as needed.
5. To remove a zone from a zoneset, click **Remove**, click **Yes**, and then click **OK**.

To edit storage array zoning

1. Open the **VMs and Services** workspace.
2. In the **VMs and Services** pane, right-click the applicable host, and then click **Properties**.
3. On the **Properties** page, click the **Storage** tab.
4. Under **Storage**, scroll down to **Fibre Channel Arrays**, click **Edit**, click the applicable array, and then do the following:
    a. Click **Modify zoning** to edit zoning information.
    b. Click **View existing zoning** to view zoning information.

c. Click **New** to assign the storage array to a new zone.

5. When complete, click **OK**.

Viewing zonesets in a fabric

Use the following procedures to view the zonesets associated with a fabric.

To view zonesets

1. Open the **Fabric** workspace, and then click **Fibre Channel Fabric**.
2. Under **Name**, right-click the applicable fabric, and then click **Properties**.
3. On the **Properties** page, click the **Zonesets** tab.

See Also

Managing Virtual Fibre Channel in VMM

Managing Virtual SANs

A virtual storage area network (vSAN) is a named group of physical Fibre Channel Host Bus Adapter (HBA) ports on a host computer that a VM connects to in order to access Fibre Channel storage devices. One or more vSANs can be created for each host computer. Each vSAN can only contain HBAs that are from the same fabric.

Virtual Host Bus Adapters (vHBAs) represent the virtualization of Fibre Channel HBAs, and are used by VMs to connect with vSANs. Each vHBA has a World Wide Node Name (WWNN), which is different than the host HBA WWNN.

Using NPIV, a host computer HBA can have multiple vHBAs associated with it. HBA ports assigned to a vSAN can be added or removed as needed.

Creating virtual SANs

Use the following procedure to create a new vSAN for a host computer.

To create a virtual SAN

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, right-click the applicable host, and then click **Properties**.
3. On the **Properties** page, click the **Hardware** tab, then click **New Virtual SAN**, and do the following:
   a. In the **Name** box, enter a name for the vSAN.
   b. In the **Description** box, enter a description for the vSAN.
   c. Under **Fibre Channel adapters**, select the check boxes next to the Fibre Channel adapters (HBAs) that you want to assign to the vSAN.
   d. When completed, click **OK**.

Editing vSAN port assignments

Use the following procedure to change the host computer HBA ports assigned to a vSAN.

To edit vSAN ports

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, right-click the applicable host, and then click **Properties**.
3. On the **Properties** page, click the **Hardware** tab, and then scroll down to **FC Virtual SAN**.
4. Under **Fibre Channel adapter details**, select or unselect the applicable check boxes next to the HBA ports listed.

Removing a vSAN

Use the following procedure to remove a vSAN from a host computer.

Note
Any vHBAs attached to a vSAN must first be removed before the vSAN can be removed.

To remove a vSAN

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, right-click the applicable host, and then click **Properties**.
3. On the **Properties** page, click the **Hardware** tab, and then scroll down to **FC Virtual SAN**.
4. Right-click the applicable vSAN, click **Delete**, and then click **OK**.

Adding a new vHBA

Use the following procedure to add a virtual Fibre Channel adapter (vHBA) and assign it to a vSAN.

To add a new vHBA

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, right-click the applicable host, and then click **Properties**.
3. On the **Properties** page, click the **Hardware Configuration** tab, click **New**, click **Fibre Channel Adapter**, and then do the following:
   a. In the **Virtual SAN name** box, select a vSAN from the drop-down list to assign to the vHBA.
   b. If you want to dynamically assign the range of port settings for the vHBA, click **Dynamically assign World Wide Names**.
   c. If you want to statically assign port settings for the vHBA, click **Statically assign World Wide Names**, and then enter primary and secondary WWNN and WWPN port settings for the vHBA.
   d. When completed, click **OK**.

Editing vHBA WWNN and WWPN Dynamic Settings

Use the following procedure to change the port settings that can be dynamically assigned to a virtual Fibre Channel adapter (vHBA).

To edit dynamic vHBA port settings

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, right-click the applicable host, and then click **Properties**.
3. On the **Properties** page, click the **Hardware** tab, and then scroll down to **Global FC settings**.
4. Under **Fibre Channel adapter details**, do the following:
   a. In the **Minimum** box, enter the lowest WWPN port setting.
   b. In the **Maximum** box, enter the highest WWPN port setting.
   c. In the **World Wide Node Name** box, enter a name.
   d. When completed, click **OK**.

Important

Changing these settings does not affect vHBA ports that have already been created. To apply a new setting to an existing vHBA port, recreate the port by removing it and then adding it again.

See Also

Managing Virtual Fibre Channel in VMM

Managing Storage LUNs for Virtual Fibre Channel

For a host computer, VM, or computer service tier to access storage array resources, Logical Units (LUs) and associated Number (LUNs) must be created and then registered (unmasked) to the host, VM, or tier.

Creating storage LUNs

Use the following procedures to create a new logical unit (LUN) for a storage array.

To create a LUN

1. Open the **Fabric** workspace.
2. In the **Fabrics** pane, click **Storage** and then click **Classifications and Pools**.
3. Under **Name**, click the applicable storage device, and then on the **Home** tab, click **Create Logical Unit**.
4. In the **Create Logical Unit** dialog box, do the following:
   a. In the **Storage pool** box, select a pool from the drop-down list.
   b. In the **Name** box, enter a name.
   c. In the **Description** box, enter a description.
   d. In the **Size** box, enter a storage value in GB.
   e. Click a radio button to create either a thin or fixed size logical unit.
   f. When complete, click **OK**.

Registering storage LUNs

Use the following procedure to register (unmask) a LUN to one or more host HBA initiator ports.

To register a storage LUN

1. Open the **VMs and Services** workspace.
2. In the **VMs and Services** pane, right-click the applicable VM and then click **Properties**.
3. On the **Properties** page, click the **Storage** tab.
4. Click **Add** and then click **Add Disk**.
5. On the **Create Logical Unit** page, do the following:
   - Next to **Storage pool**, select a pool from the drop-down list.
   - In **Name**, enter a name for the LUN.
   - In **Size**, enter a storage size in GB.
6. When complete, click **OK**. The LUN is now registered (unmasked).

See Also

Managing Virtual Fibre Channel in VMM

Creating a VM for Virtual Fibre Channel

The following is the high-level process for creating a virtual machine that can access Fibre Channel storage resources.

Virtual Host Bus Adapters (vHBAs), which represent the virtualization of Fibre Channel HBAs, are used by VMs to connect with vSANs. In order for vHBAs to connect to vSANs, they first must be added to the hardware profile of a VM template.

To create a VM for virtual Fibre Channel

1. Using the **Create Virtual Machine Wizard**, create a new VM, and then add a new Fibre Channel adapter (vHBA) to the **Configure Hardware** page of the VM template. For each vHBA that you create, specify dynamic or static WWPN assignments and select the fabric classification. For information, see How to Create and Deploy a Virtual Machine from a Template.
2. Still using the **Create Virtual Machine Wizard**, place and deploy the VM to a destination host. Make sure the host contains a virtual SAN that matches the storage fabric. For more information, see How to Create and Deploy a Virtual Machine from a Template.

Once the VM is deployed to a host, a Fibre Channel storage array can be zoned to the VM. For more information, see Managing Virtual Fibre Channel Zones. Lastly, a LUN is created for the array and registered (unmasked) to the VM. For more information, see Managing Storage LUNs for Virtual Fibre Channel.

See Also

Managing Virtual Fibre Channel in VMM

Creating a Service Tier for Virtual Fibre Channel

The following is the high-level process for creating a service tier to access Fibre Channel storage resources.

To create a service tier for Virtual Fibre Channel

1. Using the **Service Template Designer**, create a service template and add the applicable VM templates you previously created to the service template. For information on creating a service template, see How to Create a Service Template in VMM and How to Configure the Properties of a Service Template.
2. Add a new Fibre Channel adapter (vHBA) to the **Configure Hardware** page of the service template. For each vHBA that you create, specify dynamic or static WWPN port assignments and select the fabric classification.
3. Create service tier from the service template and assign the service tier to a computer tier.
4. Deploy the tier. For more information, see How to Deploy a Service in VMM.

Once the service tier is deployed, a Fibre Channel storage array can be zoned to the tier. For more information, see Managing Virtual Fibre Channel Zones. Lastly, a LUN is created for the array and registered (unmasked) to the tier. For more information, see Managing Storage LUNs for Virtual Fibre Channel.

See Also

Managing Virtual Fibre Channel in VMM

How to Add and Classify SMI-S and SMP Storage Devices in VMM

Use the following procedure to add remote storage devices in System Center 2012 – Virtual Machine Manager (VMM). You can add and discover external storage arrays that are managed by Storage Management Initiative – Specification (SMI-S) or Store Management Provider (SMP) providers. You can assign friendly-name classifications for the added storage. For example, you can assign a Gold classification to solid-state drive (SSD) storage and a Bronze classification to slower drives.

Account requirements To complete this procedure, you must be a member of the Administrator user role, or a member of the Delegated Administrator user role.

Before you begin this procedure, verify the following prerequisites:

- Ensure that you are using a supported storage array. For a list of supported arrays, see the "Supported Storage Arrays" section of the topic Configuring Storage in VMM.
- To add an SMI-S storage device, ensure that you have installed the SMI-S provider for the array on a server that the VMM management server can access over the network by IP address or by fully qualified domain name (FQDN). For information about how to obtain SMI-S providers, see Configuring Storage in VMM.

  Note

  Do not install the SMI-S provider on the VMM management server. This configuration is not supported.

  WMI SMP providers from Dell EqualLogic and NexSan must be installed on the VMM server.
- You can create a Run As account before or while you are run the Add Storage Devices Wizard to discover storage. The Run As account must have permissions to access the SMI-S

provider. You can create a Run As account in the **Settings** workspace. For more information about Run As accounts, see How to Create a Run As Account in VMM.

Adding and classifying block storage devices

Use the following procedures to add, discover, and classify block storage devices.

To discover storage devices

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, click **Storage**.
3. On the **Home** tab, click **Add Resources**, and then click **Storage Devices** to start the Add Storage Devices Wizard.
4. On the **Select Provider Type** page, select one of the following:
   a. Select the **Add a storage device that is managed by an SMI-S provider** check box to specify and discover a storage device or an array that is supported by the SMI-S protocol.
   b. Select **Add a storage device that is managed by an SMP provider** to specify and discover a storage device or an array that is supported by the SMP protocol.
5. On the **Specify Discovery Scope** page, do the following:
   a. If you are adding an SMI-S provider storage device, do the following:
      i. In the **Protocol** list, select one of the following:
         - **SMI-S CIMXML** Choose this option to specify the SMI-S CIMXML-based storage provider that can be used to manage the storage devices.
         - **SMI-S WMI WMI** Choose this option to specify the SMI-S WMI-based storage provider that can be used to manage the storage devices.
      ii. In the **Provider IP address or FQDN** box, enter either the IP address or the FQDN of the storage provider.
      iii. In the **TCP/IP port** box, enter the port number that is used to connect to the provider.
      iv. Select the **Use Secure Sockets Layer (SSL) connection** check box to enable HTTPS for communicating with the SMI-S CIMXML provider. This setting is not available for the SIM-S WMI protocol.
      v. Next to the **Run As account** box, click **Browse**, and select a Run As account that can access the storage provider. If you do not have an account, click **Browse**, and then in the **Select a Run As Account** dialog box, click **Create Run As Account**.
   b. To add an SMP provider, select it from the **Provider** list. If the SMP provider is not in the list, click **Import** to refresh the list.
6. On the **Gather Information** page, VMM automatically tries to discover and import the storage device information. To retry discovery, click **Scan Provider**. Note the following if you selected the option to use an SSL connection for an SMI-S provider:
   a. During discovery, the **Import Certificate** dialog box appears. Review the certificate information for the storage provider, and then click **Import**.

b. By default, when you import a certificate for a storage provider, verification of the common name (CN) that is used in the certificate occurs. However, this process might cause an issue where storage discovery fails when the certificate does not contain a CN value, or the CN value does not match the expected format of NetBIOS name, FQDN, or IP address that VMM uses.

c. If you receive the error messages "SSL certificate common name is invalid" or "Certificate Authority not recognized", you must disable CN verification for the storage provider certificate in the registry. To do this, follow these steps on the VMM management server:

> **Warning**
> This task contains steps that indicate how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, ensure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up the registry, which is included in the system state, see Windows Server Backup.

i. Click **Start**, type **regedit** in the **Search programs and files** box, and then press ENTER.

ii. In the **User Account Control** dialog box, click **Yes** to continue.

iii. In Registry Editor, locate, and then click the following registry subkey:

HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Storage Management/

iv. On the **Edit** menu, point to **New**, and then click **DWORD (32-bit) Value**.

v. Type **DisableHttpsCommonNameCheck**, and then press ENTER.

vi. Double-click **DisableHttpsCommonNameCheck**.

vii. In the **Value data** box, type a value of **1**, and then click **OK**.

viii. Close Registry Editor.

If the discovery process succeeds, the discovered storage arrays, storage pools, manufacturer, model, and capacity are listed on the page. When the process finishes, click **Next**.

7. On the **Select Storage Devices** page, do the following for each storage pool that requires a classification:

a. Select the check box next to a storage pool that you want VMM to manage.

b. In the **Classification** column, select the storage classification that you want to assign. For instructions about how to create a new classification, see How to Create Storage Classifications in VMM. Then click **Next**.

8. On the **Summary** page, confirm the settings, and then click **Finish**.

The **Jobs** dialog box appears. Ensure that the job has a status of **Completed**, and then close the dialog box.

9. To verify the newly discovered storage information, in the **Fabric** workspace, on the **Home** tab, click **Fabric Resources**. In the **Fabric** pane, expand the **Storage** node, and

then do any of the following:

- To view the storage pools that are assigned to a classification, click **Classifications and Pools**, and then expand the classification where you added storage. Expand a storage pool to view logical unit information for the pool.
- To view storage provider information, click **Providers**. You can view the storage provider name, management address, managed arrays, and the provider status.
- To view discovered storage arrays, click **Arrays**. You can view the name of the array, total and used capacity, the number of managed storage pools, the provider name, and the provider status.

To change the storage classification for a storage pool

1. In the **Fabric** workspace, expand **Storage**, and then click **Classification and Pools**.
2. In the **Classifications, Storage Pools and Logical Units** pane, expand the storage classification that contains the storage pool that you want to reclassify.
3. Right-click the storage pool that you want to reclassify, and then click **Properties**.
4. In the **Classification** list, click the classification that you want to assign, and then click **OK**.

See Also

Configuring Storage in VMM

How to Add Windows File Server Shares in VMM

Use the following procedure to add remote Windows-based file servers as storage devices in System Center 2012 – Virtual Machine Manager (VMM).

Account requirements To complete this procedure, you must be a member of the Administrator user role or a member of the Delegated Administrator user role.

Before you begin this procedure, you can create a Run As account before or while you use the Add Storage Devices Wizard to discover storage. The Run As account must have administrator permissions on the file server. VMM uses this account to perform administrative operations, for example, to create shares and to modify share permissions on the server. For more information about Run As accounts, see How to Create a Run As Account in VMM.

Adding the file server

When you add a file server, VMM automatically discovers all the shares that are currently present on the server.

To add a file server

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, click **Storage**.
3. On the **Home** tab, click **Add Resources**, and then click **Storage Devices** to start the Add Storage Devices Wizard.
4. On the **Select Provider Type** page, select **Add a Windows-based file server as**

managed storage device to manage a single or clustered file server in the VMM console.

5. On the **Specify Discovery Scope** page, do the following:
   a. In the **Provider IP address or FQDN** box, specify the address or name of the file server.
   b. If the file server resides in a domain that is not trusted by the domain in which the virtual machine hosts are located, select **This computer is in an untrusted Active Directory domain**. The virtual machine hosts use the file server storage.
   c. Next to the **Run As account** box, click **Browse**, and select a Run As account that can access the storage provider. If you do not have an account. click **Browse**, and then, in the **Select a Run As Account** dialog box, click **Create Run As Account**.
6. On the **Gather Information** page, VMM automatically tries to discover and import information about the shares on the file server. If the discovery process succeeds, information about the file server is displayed. When the process finishes, click **Next**.
7. On the **Select Storage Devices** page, select the check box next to a file share that you want VMM to manage.
8. On the **Summary** page, confirm the settings, and then click **Finish**.

   The **Jobs** dialog box appears. Ensure that the job has a status of **Completed**, and then close the dialog box.
9. To verify the newly discovered storage information, in the **Fabric** workspace, on the **Home** tab, click **Fabric Resources**. In the **Fabric** pane, expand the **Storage** node.

After adding and discovering the file server storage, you can assign SMB 3.0 file shares to hosts and host clusters. For more information, see How to Assign SMB 3.0 File Shares to Hyper-V Hosts and Clusters in VMM.

How to Assign SMB 3.0 File Shares to Hyper-V Hosts and Clusters in VMM

In Windows Server 2012, Server Message Block (SMB) 3.0 file shares can be used as shared storage for Hyper-V hosts, so that Hyper-V can store virtual machine files, which include configuration, virtual hard disk (.vhd and .vhdx) files, and snapshots on SMB file shares. By using Virtual Machine Manager (VMM), you can assign SMB file shares to stand-alone servers that are running Hyper-V and host clusters. This topic describes the required procedures to deploy this configuration:

1. **Add a storage device**—As a first step, add a storage device or Windows-based file server to the VMM console. As part of the Add operation, VMM discovers all the storage of shares that are available on the device. For instructions, see How to Add Windows File Server Shares in VMM, and How to Add and Classify SMI-S and SMP Storage Devices in VMM.
2. **Create a file share**—Create a file share on the Windows-based file server. For example, create a file share that is named **\\fileserver1\smbfileshare**. When you create the share, you do not have to assign specific permissions at the share or file system level. VMM automatically assigns the required permissions. For instructions, see Creating a File Share.
3. **Assign the share**—Assign the share to a virtual machine host or cluster. VMM automatically modifies the share to assign the necessary permissions for the server that is running Hyper-V

or cluster to access the storage. For instructions, see Assigning a file share. Note the following prerequisites to create and assign the share:

- We recommend that you use a dedicated file server.
- The Windows-based file server should be in the same Active Directory Domain Services domain as the virtual machine hosts.
- Files shares that are assigned to hosts and clusters should not be added as VMM library shares.
- For SMB 3.0 file shares to work correctly with VMM, the file server must not be a server that is running Hyper-V. This rule also applies to a highly available file server. Do not add the file server, whether stand-alone or in a cluster, as a managed host in VMM.
- The VMM service account must have local administrative credentials on the file server where the SMB 3.0 share resides. You must assign these permissions outside of VMM.

Creating a file share

Create the file share on the file server, or optionally, create the file share by using the VMM console.

To create a file share by using VMM

1. Open the **Fabric** workspace.
2. Click **Storage**, and then click **Providers**.
3. In the **Providers** pane, select the file server, and then click **Create File Share**.
4. In the **Create File Share** dialog box, specify the absolute path where you want to create the share. If the share does not exist, VMM creates it.
5. Optionally, select **Continuously Available File Server** if you are using the Hyper-V Scale-Out File Server feature. For more information, see Scale-Out File Server for Application Data Overview .

Assigning a file share

After you create a host, you must assign the file share to any host or cluster on which you want to create virtual machines that use storage on the file server.

To configure a stand-alone host for SMB 3.0 file share access

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then expand **All Hosts**.
3. Click the host that you want to configure. Then, on the **Host** tab, in the **Properties** group, click **Properties**.
4. In the **Properties** dialog box, click the **Host Access** tab.
5. In the **Run As account** box, configure the account settings. Note the following:
   - By default, the Run As account that was used to add the host to VMM is listed. If you want to change the Run As account, click **Browse**, and then select an existing Run As account, or click **Create Run As Account** to create a new account. You cannot use the same account that you used for the VMM service account.

- If you used a domain account for the VMM service account, add the domain account to the local Administrators group on the file server.
- If you used the local system account for the VMM service account, add the computer account for the VMM management server to the local Administrators group on the file server. For example, for a VMM management server that is named **VMMServer01**, add the computer account **VMMServer01$**.
- Any host or host cluster that accesses the SMB 3.0 file share must have been added to VMM by using a Run As account. VMM automatically uses this Run As account to access the SMB 3.0 file share.

  Note
  If you specified explicit user credentials when you added a host or host cluster, you can remove the host or cluster from VMM, and then add it again by using a Run As account.

6. In the *Host Name* **Properties** dialog box, click the **Storage** tab.
7. On the toolbar, click **Add File Share**.
8. In **File share path**, select the required SMB 3.0 file share, and then click **OK**.

   Tip
   To confirm that the host has access, open the **Jobs** workspace to view the job status. Or, open the host properties again, and then click the **Storage** tab. Under **File Shares**, click the SMB 3.0 file share. Verify that a green check mark appears next to **Access to file share**.
9. Repeat this procedure for any stand-alone host that you want to access the SMB 3.0 file share.

To configure a host cluster for SMB 3.0 file share access

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then expand **All Hosts**.
3. Locate and right-click the cluster node that you want to configure, and then click **Properties**.
4. In the *Host Name* **Properties** dialog box, click the **Host Access** tab.
5. In the **Run As account** box, configure the account settings. Note the following:

   Note
   By default, the Run As account that was used to add the host to VMM is listed. If you want to change the Run As account, click **Browse**, and then select an existing Run As account, or click **Create Run As Account** to create a new account. Do not use the same account that you used for the VMM service account. You must use the same Run As account on all cluster nodes.
6. Repeat steps 3 through 5 on each node of the host cluster.
7. After you have verified the host management Run As account on each cluster node, click the host cluster that contains the nodes. Then, on the **Host Cluster** tab, in the

Properties group, click **Properties**.

8. In the *Cluster Name* **Properties** dialog box, click the **File Share Storage** tab.
9. In the **File share storage** pane, click **Add**.
10. In **File share path**, select the required SMB 3.0 file share, and then click **OK**.
11. Click **OK** to apply the changes and to close the dialog box.

    Tip
    To confirm that the cluster has access, open the **Jobs** workspace to view the job status. To view the access status, free space, and total capacity for the share, open the host cluster properties again, and then click the **File Share Storage** tab.
12. Repeat this procedure for any other host cluster to access the SMB 3.0 file share.

See Also

Configuring Storage in VMM

How to Add and Classify SMI-S and SMP Storage Devices in VMM

How to Create Storage Classifications in VMM

You can use the following procedure to create storage classifications in System Center 2012 – Virtual Machine Manager (VMM). Storage classifications enable you to assign user-defined storage classifications to discovered storage pools, typically by quality of service (QoS). For example, you could assign a classification of GOLD to storage pools that have the highest performance and availability.

Account requirements To complete this procedure, you must be a member of the Administrator user role or a member of the Delegated Administrator user role.

To create storage classifications

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Storage**, right-click **Classification and Pools**, and then click **Create Classification**.
3. In the **New Classification** dialog box, enter a name and description for each classification that you want to create. Click **Add** to add each newly created classification.

   As an example, you can create the following classifications.

   Note
   This information is provided only as an example. Use classifications and descriptions that make sense for your environment.

Name	Description
GOLD	**Storage pool based on solid-state drives (SSDs) that delivers high performance for I/O intensive**

	applications
SILVER	**Fibre Channel Serial Attached SCSI (SAS) storage (RAID 5)**
BRONZE	**iSCSI Serial ATA (SATA) storage (RAID 5)**

See Also

Configuring Storage in VMM

How to Select a Method for Creating Logical Units in VMM

You can use the following procedure to configure the preferred capacity allocation method for a managed storage array in System Center 2012 – Virtual Machine Manager (VMM). This setting defines how new logical units are allocated when you rapid provision virtual machines by using storage area network (SAN) copy technology. You can either create logical units by using the snapshot capability or by using the cloning capability.

Note

The storage array must support the selected allocation method, and the functionality for the selected method must be enabled on the array. Also, realize that the selected allocation method might require additional licensing from your storage vendor.

To configure the allocation method for a storage array

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Storage**, and then click **Arrays**.
3. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
4. In the **Arrays** pane, right-click the array that you want to configure, and then click **Properties**.
5. In the **Properties** dialog box, click the **Settings** tab.
6. Under **Storage array settings**, click one of the following options, and then click **OK**:
   - **Use snapshots** (the default)
   - **Clone logical units**

See Also

Configuring Storage in VMM

How to Provision Storage Logical Units in VMM

You can use the following procedure to create logical units from storage pools that are managed by System Center 2012 – Virtual Machine Manager (VMM).

Note

If you allocate a storage pool to a host group, you can also create and assign logical units directly from managed servers that are running Hyper-V in the host group. For more

information, see How to Configure Storage on a Hyper-V Host in VMM and How to Configure Storage on a Hyper-V Host Cluster in VMM.

Before you begin this procedure, ensure that one or more storage pools are defined in VMM management. For more information, see Configuring Storage in VMM and How to Add and Classify SMI-S and SMP Storage Devices in VMM.

Account requirements To complete this procedure, you must be member of the Administrator user role or a member of the Delegated Administrator user role.

To create logical units

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, click **Storage**.
3. Right-click **Classification and Pools**, and then click **Create Logical Unit**.
4. To create a logical unit, in the **Create Logical Unit** dialog box, do the following:
   a. In the **Storage pool** list, click the storage pool that you want to use.
   b. In the **Name** box, enter a name for the logical unit. Use only alphanumeric characters.
   c. Optionally, in the **Description** box, enter a description for the logical unit.
   d. In the **Size (GB)** box, enter the size of the logical unit, in gigabytes.
   e. When you are finished, click **OK**.

   To view the job status, open the **Jobs** workspace.
5. To verify that the logical unit was created, follow these steps:
   a. In the **Fabric** workspace, expand **Storage**, and then click **Classifications and Pools**.
   b. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
   c. In the **Classifications, Storage Pools, and Logical Units** pane, expand the storage classification for the pool where you created the logical unit, and then expand the storage pool.
   d. In the list of logical units, verify that the new logical unit appears.

You can now assign the logical unit to a host group. For more information, see How to Allocate Storage Logical Units to a Host Group in VMM.

See Also

Configuring Storage in VMM

How to Allocate Storage Logical Units to a Host Group in VMM

You can use the following procedure to allocate storage logical units to a host group in the System Center 2012 – Virtual Machine Manager (VMM) console. After you make the logical units available to a host group, if servers that are running Hyper-V are configured to access the storage, you can assign the logical units to servers that are running Hyper-V and host clusters that reside in the host group and any child host groups.

Tip

You can also allocate logical units to a host group through the host group properties.

Prerequisites

Before you begin this procedure, ensure that:

- The storage pools where the logical units reside have been discovered by VMM. For more information, see How to Add and Classify SMI-S and SMP Storage Devices in VMM.
- Unassigned logical units must exist in the storage pools from which you want to allocate storage capacity. For information about creating logical units by using VMM, see How to Provision Storage Logical Units in VMM. Alternately, you can create logical units by using your storage array vendor's management tools or by using a server that you use to manage Hyper-V. This server must be able to access the storage array, and a storage pool must have been allocated to the host group where the server that is running Hyper-V resides. For more information, see How to Allocate Storage Pools to a Host Group in VMM.

Account requirements To complete this procedure, you must be a member of the Administrator user role or a member of the Delegated Administrator user role where the management scope includes the target host group.

To allocate logical units to a host group

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, click **Storage**.
3. On the **Home** tab, click **Allocate Capacity** to open the **Allocate Storage Capacity** dialog box.
4. In the **Host groups** list, click the host group to which you want to allocate storage capacity.

   Total and available storage capacity information is displayed for the host group. This information includes the total and available capacity for both local and remote storage, and total and available allocated storage.
5. To allocate logical units to the host group, click **Allocate Logical Units** to open the **Allocate Logical Units** dialog box.
6. Optionally, select the **Display as available only storage arrays that are visible to any host in the host group** check box.
7. For each logical unit that you want to add, under **Available logical units**, click a logical unit that you want to allocate to the host group, and then click **Add**.
8. When you are finished, click **OK**.

After you have allocated logical units to a host group, you can assign logical units to servers that are running Hyper-V and host clusters in the host group that can access the storage array. For more information, see the topics How to Configure Storage on a Hyper-V Host in VMM and How to Configure Storage on a Hyper-V Host Cluster in VMM.

See Also

Configuring Storage in VMM

How to Allocate Storage Pools to a Host Group in VMM

You can use the following procedure to allocate one or more storage pools to a host group in System Center 2012 – Virtual Machine Manager (VMM). After you allocate a storage pool to a host group, you can do either of the following:

- Create logical units from servers that are running Hyper-V in the host group that can access the storage array where the storage pool resides.

  Note
  For more information, see How to Configure Storage on a Hyper-V Host in VMM and How to Configure Storage on a Hyper-V Host Cluster in VMM.

- Use the storage pool for the rapid provisioning of virtual machines. During rapid provisioning by using storage area network (SAN) cloning or snapshots, VMM requests a copy of an existing logical unit through a SAN copy-capable storage array. Therefore, you do not have to create logical units beforehand. For more information, see Rapid Provisioning a Virtual Machine by Using SAN Copy Overview.

Note
You can also allocate storage pools to a host group through the host group properties.

Account requirements To complete this procedure, you must be a member of the Administrator user role or a member of the Delegated Administrator user role where the management scope includes the target host group.

To allocate storage pools to a host group

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, click **Storage**.
3. On the **Home** tab, click **Allocate Capacity**.

   The **Allocate Storage Capacity** dialog box opens.

   Note
   To allocate storage capacity if you are a delegated administrator, where your management scope is restricted to specific host groups, you must right-click a host group that is included in your scope, click **Properties**, and then click the **Storage** tab. Then, continue to step 5.
4. In the **Host groups** list, click the host group to which you want to allocate storage capacity.

   Total and available storage capacity information is displayed for the host group. The storage capacity information includes the total and available capacity for both local and remote storage, and total and available allocated storage.
5. To allocate storage pools to the host group, click **Allocate Storage Pools** to open the **Allocate Storage Pools** dialog box.
6. Optionally, select the **Display as available only storage arrays that are visible to any host in the host group** check box.

7. For each storage pool that you want to add, under **Available storage pools**, click a storage pool that you want to allocate to the host group, and then click **Add**. When you are finished, click **OK**.

See Also

Configuring Storage in VMM

How to Remove Storage Logical Units in VMM

Use the following procedure to delete a logical unit that is under System Center 2012 – Virtual Machine Manager (VMM) management.

Prerequisites

Ensure that the logical unit that you want to delete is not currently assigned to a server that is running Hyper-V or is assigned as storage to a virtual machine. For information about how to remove an assigned logical unit from a server that is running Hyper-V or a server in a host cluster, see How to Configure Storage on a Hyper-V Host in VMM and How to Configure Storage on a Hyper-V Host Cluster in VMM.

Account requirements You must be a member of the Administrator user role or a member of the Delegated Administrator user role to complete this procedure.

To delete a logical unit

1. Open the **Fabric** workspace.
2. In the **Fabric** workspace, expand **Storage**, and then click **Classifications and Pools**.
3. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
4. In the **Classifications, Storage Pools, and Logical Units** pane, expand the storage classification that is assigned to the storage pool where the logical unit resides. Expand the storage pool, and then click the logical unit that you want to remove.
5. On the **Home** tab, in the **Remove** group, click **Remove**.
6. Review the warning message.

   Caution
   If you continue, the data on the logical unit is permanently deleted.
7. Click **OK** to continue and delete the logical unit. Open the **Jobs** workspace to view the job status.

   If removal is successful, the logical unit is deleted and is removed from the list in the **Classifications, Storage Pools, and Logical Units** pane.

See Also

Configuring Storage in VMM

How to Create a Storage Pool from Physical Disks in VMM

As of System Center 2012 R2 Virtual Machine Manager, you can use the Virtual Machine Manager (VMM) to create storage pools from physical disks on Scale-Out File Servers.

To create a new storage pool from physical disks

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, click **Storage**, and then click **File Servers**.
3. In the **File Servers, File Shares** pane, select the file server on which you want to create the pool.
4. On the **Home** tab, click **Manage Pools**.
5. In the **Manage Pools of File Server <file server>** dialog box, click **New**.
6. In the New Storage Pool Wizard, type a **Name** and select a **Classification** for the pool.

   The **Disk** list includes non-local physical disks that you can add to the pool. This includes Serial Attached SCSI (SAS) storage disks that are not in the pool yet. Select the disks that you want to include in the pool, and then click **Create**.
7. In **the Manage Pools of File Server <file server>** dialog box, click **OK** to create the pool.

How to Create a File Share from a Storage Pool in VMM

As of System Center 2012 R2, you can use Virtual Machine Manager (VMM) to create storage pools from physical disks, and then use these storage pools to create file shares on Scale-Out File Server clusters. When you create the file share on a Scale-Out File Server running Windows Server 2012 R2, the storage type for a file share can be a storage pool, a local path, or a volume.

Use the following procedure to create a new file share from a storage pool by using the VMM console. You can set **Resiliency** and **Redundancy** values to configure these file shares as follows:

- Configure as two-way mirror (or single parity), which can tolerate the failure of one disk
- Configure as three-way mirror (or dual parity), which requires more resources, but it can tolerate the failure of two disks

The default settings for a new file share use the NTFS file system format and a three-way mirror configuration. The file share is supported by a cluster shared volume that is formatted with NTFS (referred to as a CSV file system or CSVFS).

To create a file share from a storage pool

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, click **Storage**, and then on the **Home** tab, click **Create File Share**.
3. In the **Create File Share** dialog box, select the **File server** where you want to add the file share. Enter the remaining necessary information for creating the file share as follows:
   - In **Storage type**, click **Storage pool**, and then select one of the storage pools that you previously created.
   - Click **Resiliency**, and then choose **Redundancy** options as follows:
     - For **Parity**, you can select **Single** or **Dual**.

- For **Mirror**, you can select **Two-way** or **Three-way**.

4. Click **Create**.

How to Set a Disk Witness for a File Server Cluster Quorum in VMM

Starting with Virtual Machine Manager (VMM) in System Center 2012 R2, you can select a disk witness, specifically a node and disk majority, for a Scale-out File Server failover cluster quorum configuration. There is also support for 2-way and 3-way mirror for resiliency, as well as single parity and dual parity for redundancy.

Selecting a disk witness for a Scale-out File Server cluster quorum

Use the following procedure to node and disk majority for a Scale-out File Server failover cluster quorum configuration.

To select a disk witness for a Scale-out File Server cluster quorum

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, click **Storage**, right-click the applicable file server, and then click **Properties**.
3. On the **General** page, select the checkbox next to **Use disk witness for this file server from the specified pool.**
4. In the **Pools** box, select a storage pool from the drop-down list.
5. When complete, click **OK**.

See Also

Configuring Storage in VMM

Using Infrastructure Servers in VMM

Infrastructure server support has been added to System Center 2012 R2 Virtual Machine Manager. This feature allows you to add servers (that are not VMM host servers) as managed computers that support hosting services to support your infrastructure. For example, you can add managed servers that support services such as Active Directory, DNS, DCHP, Operations Manager, Service Manager, and File Servers. So, where VMM servers are listed by roles such as Host or Library, the additional servers that can be added as managed servers will be listed under the role of **Infrastructure**.

Note

All managed servers must be running Windows Server 2012 R2.

You can perform the following procedures on infrastructure servers:

- Create baselines for infrastructure nodes using existing VMM baseline tools and processes.
- Apply baselines to all infrastructure nodes once they are added as managed computers.
- View compliance status of infrastructure nodes after baselines have been applied.

- Orchestrate remediation to the infrastructure nodes using existing baseline tools and procedures.

In This Section

Follow these procedures to when using infrastructure servers in VMM.

Procedure	Description
How to View Infrastructure Servers	Describes how to view a list of infrastructure servers.
How to Add an Infrastructure Server to VMM	Describes how to add an infrastructure server.
How to Remove an Infrastructure Server from VMM	Describes how to remove an infrastructure server.
How to View the Properties of an Infrastructure Server in VMM	Describes how to view the properties of an infrastructure server.

How to View Infrastructure Servers

Use the following procedure to view a list of infrastructure servers

To view a list of infrastructure servers

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then click **Infrastructure**.
3. The list of infrastructure servers will be displayed.

How to Add an Infrastructure Server to VMM

Use the following procedure to add an Infrastructure Server to VMM 2012 R2.

To add an infrastructure server

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then expand **Infrastructure**.
3. In the ribbon, click **Add Resources**, and then click **Infrastructure Server**.
4. In the **Add Infrastructure Server** wizard, perform the following:
   a. In the **Computer name** field, enter the FQDN of the computer that you want to add.
   b. In the **Description** field, enter a description of the services provided by the computer.
   c. In the **Run As account** field, click **Browse**.
   d. In the **Select a Run As account** wizard, select the run as account that has sufficient

permissions to install the computer, and then click **OK**.

e. In the **Add Infrastructure Server** wizard, click **Add**.

How to Remove an Infrastructure Server from VMM

Use the following procedure to remove an infrastructure server.

To remove an infrastructure server

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then expand **Infrastructure**.
3. In **Infrastructure server** list, select the server that you want to remove.
4. In the ribbon, click **Remove**.
5. In the **Remove <computer name>** wizard, select an existing Run As account or enter credentials for an account that has sufficient permissions to remove the computer, and then click **OK**.

How to View the Properties of an Infrastructure Server in VMM

Use the following procedure to view the properties of an infrastructure server.

To view the properties of an infrastructure server

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then expand **Infrastructure**.
3. In the **Infrastructure servers** pane, select the server whose properties you want to view.
4. In the ribbon, click **Properties**.

Adding and Managing Hyper-V Hosts and Scale-Out File Servers in VMM

This section shows how to do the following in Virtual Machine Manager:

- Add existing Hyper-V hosts and Hyper-V host clusters to VMM, and configure host and host cluster properties.
- Convert a physical computer without an operating system installed to a managed Hyper-V host.

Note

A physical computer without an operating system installed is often referred to as a "bare-metal computer."

- Create a Hyper-V host cluster, add or remove nodes, and uncluster a host cluster directly through the VMM console.
- As of System Center 2012 R2 Virtual Machine Manager, convert physical computers without an operating system installed to a managed Scale-Out File Server cluster.
- Modify a Scale-Out File Server cluster through the VMM console.

Note

This section focuses on how to add Hyper-V hosts and Hyper-V host clusters. Be aware that VMM also enables you to add VMware ESX hosts and Citrix XenServer hosts to VMM management. For more information, see Managing VMware ESX and Citrix XenServer in VMM.

In This Section

Adding Hyper-V Hosts and Host Clusters, and Scale-Out File Servers to VMM

Describes how to add an existing Windows Server computer or a Windows Server failover cluster as one or more managed Hyper-V hosts in VMM. Covers adding Hyper-V hosts that are in a trusted domain, an untrusted domain, a disjointed namespace, and in a perimeter network. Additionally, this section covers how to convert a physical computer without an operating system installed, or a computer where you want to overwrite an existing operating system installation, to a managed Hyper-V host.

Creating and Modifying Hyper-V Host Clusters in VMM

Describes how to create a Hyper-V host cluster through the VMM console by using the Create Cluster Wizard. This section also includes procedures about how to use the VMM console to add and remove cluster nodes, and to uncluster a Hyper-V host cluster.

Modifying a Scale-Out File Server in VMM

Describes how to modify a Scale-Out File Server cluster. This section includes procedures about how to use the VMM console to add and remove cluster nodes, and to uncluster a Scale-Out File Server cluster.

Adding Hyper-V Hosts and Host Clusters, and Scale-Out File Servers to VMM

This section shows how to add Hyper-V hosts, Hyper-V host clusters, and as of System Center 2012 R2 Scale-Out File Server clusters, to Virtual Machine Manager (VMM). This section also

includes information about how to configure Hyper-V host properties, such as networking and storage settings.

You can add the following types of servers as managed Hyper-V hosts:

- Windows Server computers or Windows Server failover clusters in an Active Directory domain that is trusted by the domain of the VMM management server

  Note
  This includes Windows Server computers in a disjointed namespace.
- Windows Server computers or Windows Server failover clusters in an Active Directory domain that is untrusted by the domain of the VMM management server
- Windows Server computers in a perimeter network or in a workgroup (stand-alone computers only)
- Physical computers that do not have an operating system installed

  Note
  Through the VMM console, you can deploy an operating system to the physical computers, and add the computers as managed Hyper-V hosts. You can also use this method to overwrite an existing operating system on a physical computer.

The topics in this section are organized according to the different methods that you can use to add Hyper-V hosts, Hyper-V host clusters, or as of System Center 2012 R2 Scale-Out File Server clusters. The topics include example scenarios that will help guide you through the process. The example scenarios refer to a fictitious organization, contoso.com.

Important
When adding hosts or host clusters, you must perform all procedures in this section as a member of the Administrator user role, or as a Delegated Administrator whose management scope includes the host groups where you add the hosts or host clusters.

Advantages of Managing Scale-out File Server with VMM

With Windows Server 2012 Hyper-V, you can deploy virtual machines to block storage using Serial Attached SCSI (SAS), iSCSI, or Fibre Channel protocols. If there are Scale-out File Servers in your environment, Hyper-V supports VM virtual hard disks (VHDs) deployed to a continuously available file share using SMB3 protocol. With Virtual Machine Manager (VMM), you can manage the Scale-out File Server and create new file shares and set permissions on the file shares so that the Hyper-V servers can access the share. In System Center 2012 R2 Virtual Machine Manager, if the Scale-out File Server is connected to shared SAS disks, then disk pooling is possible using Windows Server Storage Spaces and VMM.

This section describes additional advantages of managing Scale-Out File Server with VMM.

Storage Spaces

When you add a new Scale-out File Server to VMM, the Spaces provider discovers all SAS physical disks that are available. You can list the physical disks that are available for pooling, and then select a subset or all of the physical disks that are on that list. You can also create a new pool. VMM also supports adding new disks to the storage pool. If the Scale-out File Server

already has storage pools, then VMM discovers them and automatically brings them under management.

Storage Classification

Storage pools managed by VMM must have a storage classification. Storage classification is used to differentiate between storage types based on either performance or guarantees offered by the underlying storage device. You can create a storage pool with all solid-state drives (SSDs) and associate that with a “MaximumPerformance” classification. A separate pool can have SSD and hard disk drive (HDD) from multiple enclosures which you can associate with a “MaximumResiliency” classification. Storage pools that are discovered by VMM are automatically classified as “RemoteStorage”. You can modify that classification at any time in the file server properties, or in the storage pool properties. VMM uses storage classification for VHD placement (which is defined in a templates or at creation time), and for scoping self-service users consuming cloud to specific storage.

File shares inherit the storage classification that is set for the underlying storage pool. If you need to further differentiate between two shares on the same pool, you can set storage classification at the file share level. In this case, if the storage pool is “Gold,” then one share can inherit from the storage pool so it will also be classified as “Gold”, and another file share can have a “Silver” classification.

Storage File Shares

VMM supports creation of file shares from a storage pool from a volume, or by using specific paths. In the case of creation from a storage pool, VMM uses the Storage Management API to create a new Cluster Shared Volume (CSV) from a Spaces storage pool. This operation consists of creating the disk, attaching the disk to a cluster, initializing, partitioning, formatting the volume, and finally converting the volume to CSV. VMM then calls File Server SMB3 APIs to create the Scale-Out file share.

If the CSV already exists, then all you need to do is select the volume; VMM will create the file folder structure and file share. Finally, VMM can create a file share using a specific path. For example, if the file share was accidently deleted, you can recreate the file share using an existing folder path.

File Share Permissions

Setting up permissions on folder and file shares is required before Hyper-V servers can access VM files stored on a file share. VMM automates setting permissions on the file system folder and share with the computer account from each Hyper-V server. This works for standalone Hyper-V servers and Hyper-V clusters. In addition, when you use VMM to add and remove Hyper-V nodes from a cluster, VMM modifies the permissions on the file share and the file system.

Library Storage

You can use file shares that are managed by VMM for library storage or for Hyper-V storage. You cannot use the same file share for both.

File Share Placement

VMM associates the share with the host/cluster so placement can consider file storage when evaluating its rating (similar to block storage). Placement looks at available capacity and whether a specific storage classification is required (based on the intent that is expressed in the template).

File Share Deployment

VMM offloads data transfers using CopyFile APIs. The Library server and Hyper-V host management accounts need to be set for this feature to work. If the accounts are not specified properly, VMM defaults to BITS transfer. After registering the file share with the Hyper-V server or cluster, you can deploy a new VM, the data copy is automatically offload. With a SAN, the Offloaded Data Transfer (ODX) feature handles the file transfer within the array. With a Scale-out File Server, CopyChunk support offloads the file copy and helps avoid the network roundtrip. If no offloads are available, the copy APIs reverts back to a regular SMB copy over the network. If that transfer fails for any reason (for example due to a network issue), VMM restarts the file copy job using BITS.

Cloud Storage Capacity

You can use storage classification to expose storage capacity to clouds. Self-service users do not need to pass in a share name or a mount point. Templates created by self-service users can specify a storage classification; for example if they want to use a specific VHD on gold storage. Or, the template might have no storage classification, in which case any storage that is available to the cloud can be used.

Overview Topics

Before you begin the procedures, review the information in the overview topic that applies to the type of servers that you plan to add as managed Hyper-V hosts, host clusters, or Scale-Out File Server cluster.

Topic	Description
Adding Windows Servers as Hyper-V Hosts in VMM Overview	Provides an overview, links to the operating system requirements, and links to the procedures for adding existing Windows Server computers and failover clusters as managed Hyper-V hosts.
Adding Physical Computers as Hyper-V Hosts or as Scale-Out File Servers in VMM Overview	Provides an overview, describes the Baseboard Management Controller (BMC) requirements, and links to the procedures for how to discover physical computers and convert them to managed Hyper-V hosts, or to a Scale-Out File Server cluster.
Configuring Hyper-V Host Properties in VMM	Describes the different host properties that you can configure in VMM. Includes detailed information about how to configure storage, networking and baseboard management

Topic	Description
	controller (BMC) settings on a Hyper-V host.

Adding Windows Servers as Hyper-V Hosts in VMM Overview

The procedures in this section describe how to add an existing Windows Server computer or a Windows Server failover cluster as one or more managed Hyper-V hosts in VMM. You can add Windows Server computers that are in a trusted or untrusted Active Directory domain, in a disjointed namespace, and in a perimeter network (also known as DMZ, demilitarized zone, and screened subnet). Realize that you can add only stand-alone hosts in a perimeter network. VMM does not support managing a host cluster in a perimeter network. If you want to manage a stand-alone host that is in a workgroup and not part of a domain, you can use the method to add a host in a perimeter network.

Note

New in System Center 2012 – Virtual Machine Manager, you can manage Hyper-V host clusters in untrusted Active Directory domains.

Operating System Requirements

The computers that you want to add as Hyper-V hosts must be running one of the operating systems that is listed in **Preparing your environment for System Center 2012 R2 Virtual Machine Manager**.

Important

If the Windows Server computer that you want to add does not already have the Hyper-V role installed, make sure that the BIOS on the computer is configured to support Hyper-V. If the Hyper-V role is not already installed on the server, VMM automatically adds and enables the Hyper-V role when you add the server. For more information, see Hyper-V Installation Prerequisites.

Example Scenario Overview

The example scenarios that are used in this section assume that you have the basic VMM infrastructure in place, such as a VMM management server and a library server. The examples in this section build on example scenarios from the Preparing the Fabric in VMM section, and uses the same example host group structure.

Note

The example resource names and configuration are used to help demonstrate the concepts. You can adapt them to your test environment.

The example scenarios walk you through how to add a Hyper-V host in a trusted Active Directory domain, an untrusted Active Directory domain, in a disjointed namespace, and in a perimeter network.

The following table summarizes the example resources that are used.

Resource	Resource Name
Windows Server in a trusted Active Directory domain	**HyperVHost01.contoso.com**
Windows Server in an untrusted Active Directory domain	**HyperVHost02.fabrikam.com**
Windows Server in a disjointed namespace	**HyperVHost03.contosocorp.com**
Windows Server in a perimeter network	**HyperVHost04**
Host groups	• **HyperVHost01.contoso.com** is added to the host group **Seattle\SEA_Tier0** • **HyperVHost02.fabrikam.com** is added to the host group **New York\NY_Tier2** • **HyperVHost03** is added to the host group **New York\NY_Tier1** • **HyperVHost04** is added to the host group **Seattle\SEA_Tier2**
Run As accounts	• **Trusted Hyper-V Hosts**  **Note** This Run As account is optional, as you can also specify a user name and password. • **Untrusted Hyper-V Hosts**

In This Section

Follow these procedures to add Windows Server computers as managed Hyper-V hosts.

Procedure	Description
How to Add Trusted Hyper-V Hosts and Host Clusters in VMM	Describes how to add Hyper-V hosts and host clusters that are in a trusted Active Directory domain.
How to Add Hyper-V Hosts in a Disjointed Namespace in VMM	Describes how to add Hyper-V hosts and host clusters that are in a disjointed namespace.
How to Add Untrusted Hyper-V Hosts and Host Clusters in VMM	Describes how to add Hyper-V hosts and host clusters that are in an untrusted Active Directory domain.
How to Add Hyper-V Hosts in a Perimeter Network in VMM	Describes how to add Hyper-V hosts that are in a perimeter network.

How to Add Trusted Hyper-V Hosts and Host Clusters in VMM

You can use the following procedure to add a trusted Windows Server–based computer or Windows Server–based failover cluster as one or more managed Hyper-V hosts in Virtual Machine Manager (VMM).

Prerequisites

Before you begin the procedure, review the following prerequisites:

- Make sure that the stand-alone server or the failover cluster is a member of an Active Directory domain that has a two-way trust with the domain of the VMM management server.
- The computers that you want to add must support Hyper-V. For more information, see the "Operating System Requirements" section of the topic Adding Windows Servers as Hyper-V Hosts in VMM Overview.
- If you want to add the VMM management server as a managed Hyper-V host, make sure that you enable the Hyper-V role on the VMM management server before you add the computer.

  Important
  You cannot add a highly available VMM management server as a managed Hyper-V host cluster.
- If you are adding a Hyper-V host cluster, this procedure assumes that you have an existing failover cluster that you created by using the Failover Cluster Management snap-in. For requirements for Hyper-V host operating systems, see the following:
  - For System Center 2012 – Virtual Machine Manager or for System Center 2012 SP1 see **System Requirements: Hyper-V Hosts in System Center 2012 and in System Center 2012 SP1**.
  - For System Center 2012 R2 Virtual Machine Manager see: **Preparing your environment for System Center 2012 R2 Virtual Machine Manager**.
- If you use Group Policy to configure Windows Remote Management (WinRM) settings, understand the following before you add a Hyper-V host to VMM management:
  - VMM supports only the configuration of WinRM Service settings through Group Policy, and only on hosts that are in a trusted Active Directory domain. Specifically, VMM supports the configuration of the **Allow automatic configuration of listeners**, **Turn On Compatibility HTTP Listener**, and **Turn on Compatibility HTTPS Listener** Group Policy settings. VMM does not support configuration of the other WinRM Service policy settings.
  - If you enable the **Allow automatic configuration of listeners** policy setting, you must configure it to allow messages from any IP address. To verify this configuration, view the policy setting and make sure that the IPv4 filter and IPv6 filter (depending on whether you use IPv6) are set to ***.
  - VMM does not support the configuration of WinRM Client settings through Group Policy. If you configure WinRM Client Group Policy settings, these policy settings may override client properties that VMM requires for the VMM agent to work correctly.

  If you enable any unsupported WinRM Group Policy settings, installation of the VMM agent may fail.

Note

The WinRM policy settings are located in the Computer Configuration\Administrative Templates\Windows Components\Windows Remote Management (WinRM) node of the Local Group Policy Editor or the Group Policy Management Console (GPMC).

- When you add a trusted host, you must specify account credentials for an account that has administrative rights on the computers that you want to add. You can enter a user name and password or specify a Run As account. If you want to use a Run As account, you can create the Run As account before you begin this procedure, or you can create it during the procedure.

  Important

  If you configured the VMM service to use a domain account when you installed the VMM management server, do not use the same domain account to add or remove Hyper-V hosts from VMM.

  For example, create a Run As account that is named **Trusted Hyper-V Hosts**.

  Note

  You can create Run As accounts in the **Settings** workspace. For more information about Run As accounts, see How to Create a Run As Account in VMM.

To add a trusted Hyper-V host or host cluster

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, click **Servers**.
3. On the **Home** tab, in the **Add** group, click **Add Resources**, and then click **Hyper-V Hosts and Clusters**.

   The Add Resource Wizard starts.
4. On the **Resource location** page, click **Windows Server computers in a trusted Active Directory domain**, and then click **Next**.
5. On the **Credentials** page, enter the credentials for a domain account that has administrative permissions on all hosts that you want to add, and then click **Next**.

   Important

   If you configured the VMM service to use a domain account when you installed the VMM management server, do not use the same domain account to add the hosts.

   You can specify an existing Run As account or manually enter user credentials in the format *domain_name\user_name*.

   Note

   If you do not already have a Run As account, click **Browse**, and then in the **Select a Run As Account** dialog box, click **Create Run As Account**.

   For example, if you created the example Run As account that is described in the

"Prerequisites" section of this topic, click **Browse**, and then click the **Trusted Hyper-V Hosts** Run As account.

6. On the **Discovery scope** page, do either of the following, and then click **Next**:
   - Click **Specify Windows Server computers by names**. In the **Computer names** box, enter the computers that you want to add, with each computer name or IP address on a new line. If you are adding a Hyper-V host cluster, you can either specify the cluster name or IP address, or specify the name or IP address of any cluster node.

     Tip
     Realize that you can also enter a partial computer name. For example, if you have several computers that start with the same prefix, such as "HyperVHost," you can enter **HyperVHost**, and then click **Next**. The next page of the wizard will then list all computers that have names that begin with "HyperVHost."

     For example, click **Specify Windows Server computer by names**, enter **HyperVHost01.contoso.com** as the computer name, and then click **Next**.
   - Click **Specify an Active Directory query to search for Windows Server computers**. Then, enter an Active Directory Domain Services (AD DS) query in the **Type your AD query** box, or click **Generate an AD query** to create the query.

     Note
     For information about query filters that you can use in Lightweight Directory Access Protocol (LDAP) queries, see the MSDN topic Creating a Query Filter.
7. On the **Target resources** page, select the check box next to each computer that you want to add, and then click **Next**. If you specified a cluster name or cluster node in step 6, select the check box next to the cluster name. (The cluster name is listed together with the associated cluster nodes.)

   For example, select the check box next to **HyperVHost01.contoso.com**, and then click **Next**.

   If the Hyper-V role is not enabled on a selected server, you receive a message that VMM will install the Hyper-V role and restart the server. Click **OK** to continue.
8. On the **Host settings** page, do the following:
   a. In the **Host group** list, click the host group to which you want to assign the host or host cluster.

      For example, click the host group **Seattle\Tier0_SEA**.
   b. If the host is already associated with a different VMM management server, select the **Reassociate this host with this VMM environment** check box.

      Note
      Realize that if the host was associated with a different VMM management server, it will stop working on that server.

c. If you are adding a stand-alone host, in the **Add the following path** box, enter the path on the host where you want to store the files for virtual machines that are deployed on the host, and then click **Add**. Repeat this step if you want to add more than one path. Note the following behavior:

- If you leave the box empty, the default path of %SystemDrive%\ProgramData\Microsoft\Windows\Hyper-V is used. Be aware that it is a best practice not to add default paths that are on the same drive as the operating system files.
- If you specify a path that does not already exist, the path is created automatically.

Note

When you add a host cluster, you do not specify default virtual machine paths, as you would for a stand-alone host. For a host cluster, VMM automatically manages the paths that are available for virtual machines based on the shared storage that is available to the host cluster.

d. When you are finished, click **Next**.

9. On the **Summary** page, confirm the settings, and then click **Finish**.

   The **Jobs** dialog box appears to show the job status. Make sure that the job has a status of **Completed**, and then close the dialog box.

10. To verify that the host or host cluster was successfully added, in the **Fabric** pane, expand the host group where you added the host or host cluster, click the host or host cluster. Then, in the **Hosts** pane, verify that the host status is **OK**.

Tip

To view detailed information about host status, right-click a host in the VMM console, and then click **Properties**. On the **Status** tab, you can view the health status for various areas such as overall health, VMM agent health, and Hyper-V role health. If there is an issue, you can click **Repair all**. VMM will try to automatically fix the issue.

See Also

Adding Windows Servers as Hyper-V Hosts in VMM Overview

Configuring Hyper-V Host Properties in VMM

How to Add Hyper-V Hosts in a Disjointed Namespace in VMM

You can use the following procedure to add Hyper-V hosts or Hyper-V host clusters that are in a disjointed name space as managed Hyper-V hosts in Virtual Machine Manager.

A disjointed name space occurs when the computer's primary Domain Name System (DNS) suffix does not match the domain of which it is a member. For example, a disjointed namespace occurs when a computer that has the DNS name of HyperVHost03.contosocorp.com is in a domain that has the DNS name of contoso.com. For more information about disjointed namespaces, see Naming conventions in Active Directory for computers, domains, sites, and OUs.

Prerequisites

Before you begin this procedure, make sure that the following prerequisites are met:

- The System Center Virtual Machine Manager service must be running as the local system account or a domain account that has permission to register a Service Principal Name (SPN) in Active Directory Domain Services (AD DS).
- Before you can add a host cluster that is in a disjointed namespace to a VMM management server that is not in a disjointed namespace, you must add the Domain Name System (DNS) suffix for the host cluster to the TCP/IP connection settings on the VMM management server.
- If you use Group Policy to configure Windows Remote Management (WinRM) settings, understand the following before you add a Hyper-V host to VMM management:
  - VMM supports only the configuration of WinRM Service settings through Group Policy, and only on hosts that are in a trusted Active Directory domain. Specifically, VMM supports the configuration of the **Allow automatic configuration of listeners**, the **Turn On Compatibility HTTP Listener**, and the **Turn on Compatibility HTTPS Listener** Group Policy settings. Configuration of the other WinRM Service policy settings is not supported.
  - If the **Allow automatic configuration of listeners** policy setting is enabled, it must be configured to allow messages from any IP address. To verify this, view the policy setting and make sure that the IPv4 filter and IPv6 filter (depending on whether you use IPv6) are set to "*".
  - VMM does not support the configuration of WinRM Client settings through Group Policy. If you configure WinRM Client Group Policy settings, these policy settings may override client properties that VMM requires for the VMM agent to work correctly.

  If any unsupported WinRM Group Policy settings are enabled, installation of the VMM agent may fail.

  Note
  The WinRM policy settings are located in the Computer Configuration\Administrative Templates\Windows Components\Windows Remote Management (WinRM) node of the Local Group Policy Editor or the Group Policy Management Console (GPMC).

To add a Hyper-V host in a disjointed namespace

1. Follow the steps in the topic How to Add Trusted Hyper-V Hosts and Host Clusters in VMM. Note the following:
   - On the **Credentials** page, enter credentials for a valid domain account.
   - On the **Discovery scope** page, enter the fully qualified domain name (FQDN) of the host. Also, select the **Skip AD verification** check box.
2. On the last page of the wizard, click **Finish** to add the host.

   When you use the Add Resource Wizard to add a computer that is in a disjointed namespace, VMM checks AD DS to see if an SPN exists. If it does not, VMM tries to create one. If the System Center Virtual Machine Manager service is running under an account that has permission to add an SPN, VMM adds the missing SPN automatically. Otherwise, host addition fails.

If host addition fails, you must add the SPN manually. To add the SPN, at the command prompt, type the following command, where <*FQDN*> represents the disjointed namespace FQDN, and <*NetBIOSName*> is the NetBIOS name of the host:

setspn -A HOST/<FQDN> <NetBIOSName>

For example, **setspn –A HOST/hypervhost03.contosocorp.com hypervhost03**.

Tip

To view a list of registered SPNs for the host, at the command prompt, type **setspn -l <NetBIOSName>**, where <*NetBIOSName*> is the NetBIOS name of the host.

See Also

Adding Windows Servers as Hyper-V Hosts in VMM Overview

How to Add Untrusted Hyper-V Hosts and Host Clusters in VMM

You can use the following procedure to add Hyper-V hosts or Hyper-V host clusters that are in an untrusted Active Directory domain as managed Hyper-V hosts in Virtual Machine Manager. During agent installation, VMM generates a certificate that is used to help secure communications with the host. When VMM adds the host, the certificate is automatically imported into the VMM management server's trusted certificate store.

Note

You cannot perform a local installation of the VMM agent on a computer that is in an untrusted domain. You must follow the procedure in this topic to perform a remote agent installation.

Prerequisites

Before you begin this procedure, review the following prerequisites:

- If you use Group Policy to configure Windows Remote Management (WinRM) settings, understand that VMM does not support the configuration of WinRM Group Policy settings (Service or Client) on hosts that are in an untrusted Active Directory domain. If WinRM Group Policy settings are enabled, installation of the VMM agent may fail.

  Note

  The WinRM policy settings are located in the Computer Configuration\Administrative Templates\Windows Components\Windows Remote Management (WinRM) node of the Local Group Policy Editor or the Group Policy Management Console (GPMC).

- Although it is not a required prerequisite, you can create a Run As account before you begin this procedure. (You can also create the account during the procedure.) The Run As account must have administrative rights on all hosts that you want to add.

  For example, create the Run As account **Untrusted Hyper-V Hosts**.

  Note

  You can create Run As accounts in the **Settings** workspace. For more information about Run As accounts, see How to Create a Run As Account in VMM.

To add a Hyper-V host that is in an untrusted Active Directory domain

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, click **Servers**.
3. On the **Home** tab, in the **Add** group, click **Add Resources**, and then click **Hyper-V Hosts and Clusters**.

   The Add Resource Wizard opens.
4. On the **Resource location** page, click **Windows Server computer in an untrusted Active Directory domain**, and then click **Next**.
5. On the **Credentials** page, next to the **Run As account** box, click **Browse**, click the Run As account that has administrative rights on the hosts that you want to add, click **OK**, and then click **Next**.

   Note

   If you do not already have a Run As account, click **Browse**, and then in the **Select a Run As Account** dialog box, click **Create Run As Account**.

   For example, if you created the example Run As account that is described in the Prerequisites section of this topic, click the **Untrusted Hyper-V Hosts** account, and then click **OK**.
6. On the **Target resources** page, in the **Fully qualified domain name (FQDN) or IP address** box, enter the FQDN or the IP address of the Hyper-V host or Hyper-V host cluster that you want to add, and then click **Add**.

   Note

   If you are adding a Hyper-V host cluster, you can either specify the cluster name or the name of one of the cluster nodes.

   If discovery succeeds, the host is listed under **Computer Name**.

   Repeat this step to add multiple hosts. When you are finished, click **Next**.

   For example, enter the name **HyperVHost02.fabrikam.com**, where *fabrikam.com* is the name of the untrusted domain.
7. On the **Host settings** page, do the following:
   a. In the **Host group** list, click the host group to which you want to assign the host or host cluster.

      For example, assign the host to the **New York\Tier2_NY** host group.
   b. In the **Add the following path** box, enter the path on the host where you want to store the files for virtual machines that are deployed on hosts, and then click **Add**. Repeat this step if you want to add more than one path. Note the following behavior:
      - If you leave the box empty, the default path of %SystemDrive%\ProgramData\Microsoft\Windows\Hyper-V is used. Be aware that it is a best practice not to add default paths that are on the same drive as the operating system files.
      - If you specify a path that does not already exist, the path is created

automatically.

- When you add a host cluster, you do not specify default virtual machine paths, as you would for a stand-alone host. For a host cluster, VMM automatically manages the paths that are available for virtual machines based on the shared storage that is available to the host cluster.

c. When you are finished, click **Next**.

8. On the **Summary** page, confirm the settings, and then click **Finish**.

   The **Jobs** dialog box appears to show the job status. Make sure that the job has a status of **Completed**, and then close the dialog box.

9. To verify that the host was successfully added, in the **Fabric** pane, expand the host group where you added the host, click the host, and then in the **Hosts** pane, verify that the host status is **OK**.

   Tip
   To view detailed information about host status, right-click a host in the VMM console, and then click **Properties**. On the **Status** tab you can view the health status for different areas such as overall health, host agent health, and Hyper-V role health. If there is an issue, you can click **Repair all**. VMM will to try to automatically fix the issue.

See Also

Adding Windows Servers as Hyper-V Hosts in VMM Overview

How to Add Hyper-V Hosts in a Perimeter Network in VMM

You can use the following procedure to add Hyper-V hosts that are in a perimeter network (also known as DMZ, demilitarized zone, and screened subnet) as managed Hyper-V hosts in Virtual Machine Manager. You can only add stand-alone hosts that are in a perimeter network. VMM does not support managing a host cluster in a perimeter network.

Note
You can also use this procedure to add a stand-alone Hyper-V host that is in a workgroup and not part of a domain.

Before you can add a host that is on a perimeter network to VMM, you must install an agent locally on the server that you want to add.

To install the VMM agent on the target host

1. On the VMM product media or network share, right-click **Setup.exe**, and then click **Run as administrator**.
2. On the Setup menu, under **Optional Installations**, click **Local Agent**.
3. On the **Welcome** page, click **Next**.
4. Review and accept the software license terms, and then click **Next**.
5. On the **Destination Folder** page, accept the default location or click **Change** to specify a different location, and then click **Next**.

6. On the **Security File Folder** page, do the following:
   a. Select the **This host is on a perimeter network** check box.
   b. In the **Security file encryption key** box, enter an encryption key, and then enter it again in the **Confirm encryption key** box.

      Security

      The encryption key is a value that you choose. We recommend that you enter an encryption key that contains a mix of uppercase and lowercase letters, numbers and symbols.

      Important

      Make note of the encryption key that you use to create the security file. You must enter this same key again when you add the host in the VMM console.
   c. Either accept the default location where the encrypted security file will be stored, or click **Change** to specify a different location to store the encrypted security file.

      Important

      Make note of the location where you stored the security file. In the “To ensure that the Security.txt file is available to VMM” procedure, you must transfer the security file to a location that is accessible to the computer on which a VMM console is installed.
   d. To use a certificate to encrypt communications between the VMM management server and the host, select the **Use a CA signed certificate for encrypting communications with this host** check box. In the **Thumbprint of the certificate** box, enter the thumbprint of the certificate.

      Note

      To obtain the thumbprint of a certificate, open the Certificates snap-in, and then select **Computer account**. In the Certificates snap-in, locate and then double-click the certificate that you want to use. On the **Details** tab, select the **Thumbprint** field. In the lower pane, highlight the thumbprint value, and then press Ctrl+C to copy the value to the clipboard.
   e. When you are finished, click **Next**.
7. On the **Host network name** page, specify how the VMM management server will contact the host, and then click **Next**. You can select either of the following options:
   - **Use local computer name**
   - **Use IP address**

   If you select **Use IP address**, click an IP address in the list.

   Important

   Make note of the computer name or IP address of the host. You must enter this same information again when you add the host in the VMM console.
8. On the **Configuration settings** page, accept the default port settings, or specify different ports, and then click **Next**.

Important

We recommend that you do not change the default port 5986 for agent communication. The port settings that you assign for the agent must identically match the port setting that the VMM management server uses. By default, the VMM management server uses port 5986 for agent communication with hosts in a perimeter network, and port 443 for file transfers.

9. On the **Ready to install** page, click **Install**.

To ensure that the SecurityFile.txt file is available to VMM

1. On the target host, navigate to the folder where the security file is stored. By default, the location is C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager. The name of the security file is SecurityFile.txt.
2. Transfer the security file to a location that is accessible to the computer on which a VMM console is installed. For example, transfer the file to the computer where the VMM console is installed, to an internal file share, or to a USB flash drive.

To add the Hyper-V host in the perimeter network

1. In the VMM console, open the **Fabric** workspace.
2. In the **Fabric** pane, click **Servers**.
3. On the **Home** tab, in the **Add** group, click **Add Resources**, and then click **Hyper-V Hosts and Clusters**.

   The Add Resource Wizard starts.
4. On the **Resource location** page, click **Windows Server computers in a perimeter network**, and then click **Next**.
5. On the **Target resources** page, do the following:
   a. In the **Computer name** box, enter the NetBIOS name or the IP address of the host in the perimeter network.
   b. In the **Encryption key** box, enter the encryption key that you created when you installed the agent on the target host.
   c. In the **Security file path** box, enter the path of the **SecurityFile.txt** file, or click **Browse** to locate the file.
   d. In the **Host group** list, click the host group where you want to add the host.

      For example, click the **Seattle\Tier2_SEA** host group.
   e. Click **Add**.

      The computer is listed under **Computer Name** in the lower pane.
   f. Repeat this step to add other hosts in the perimeter network. When you are finished, click **Next**.
6. On the **Host settings** page, in the **Add the following path** box, enter the path on the host where you want to store the files for virtual machines that are deployed on hosts, and then click **Add**. If you leave the box empty, the default path of

%SystemDrive%\ProgramData\Microsoft\Windows\Hyper-V is used. Be aware that it is a best practice not to add default paths that are on the same drive as the operating system files.

Repeat this step if you want to add more than one path. When you are finished, click **Next**.

Note

You can ignore the **Reassociate this host with this Virtual Machine Manager environment** check box. This setting does not apply to hosts in a perimeter network.

7. On the **Summary** page, confirm the settings, and then click **Finish**.

   The **Jobs** dialog box appears to show the job status. Make sure that the job has a status of **Completed**, and then close the dialog box.

8. To verify that the host was successfully added, in the **Fabric** pane, expand **Servers**, expand **All Hosts**, expand the host group where you added the host, and then click the host. In the **Hosts** pane, verify that the host status is **OK**.

Tip

To view detailed information about host status, right-click the host in the VMM console, and then click **Properties**. On the **Status** tab you can view the health status for different areas such as overall health, host agent health, and Hyper-V role health. If there is an issue, you can click **Repair all**. VMM will to try to automatically fix the issue.

See Also

Adding Windows Servers as Hyper-V Hosts in VMM Overview

Adding Physical Computers as Hyper-V Hosts or as Scale-Out File Servers in VMM Overview

The procedures in this section describe how to use Virtual Machine Manager (VMM) to discover physical computers on the network, automatically install one of the operating systems listed in this topic, and provision the computers into one of the followings:

- Managed Hyper-V hosts
- As of System Center 2012 R2 - Scale-out File Server cluster

To integrate with Windows Server 2012 R2, as of System Center 2012 R2 Virtual Machine Manager you can provision physical computers as file servers, and then create a Scale-Out File Server cluster that consists of these computers. You can then manage and monitor these clusters in VMM. This integrated management of file servers in System Center 2012 R2 Virtual Machine Manager ensures that administrators have an efficient management of Windows based storage. To create a Scale-Out File Server cluster, you need to use a physical computer profile that is configured with the Windows File Server role.

Operating system requirements

The operating system image that you use must be a server operating system that supports the boot from virtual hard disk (VHD) option. The operating system choices are as follows:

- **If you are using System Center 2012:**

  Windows Server 2008 R2

  Windows Server 2008 R2 with Service Pack 1 (SP1)
- **If you are using System Center 2012 with Service Pack 1 (SP1):**

  Windows Server 2008 R2

  Windows Server 2008 R2 with SP1

  Windows Server 2012
- **If you are using System Center 2012 R2 for Hyper-V Hosts:**

  Windows Server 2008 R2

  Windows Server 2008 R2 with SP1

  Windows Server 2012

  Windows Server 2012 R2
- **If you are using System Center 2012 R2 for Scale-Out File Servers:**

  Windows Server 2012 R2

For more information, see Understanding Virtual Hard Disks with Native Boot.

BMC requirements

To support discovery, the physical computer must have a baseboard management controller (BMC) installed that enables out-of-band management. The BMC must support one of the following out-of-band management protocols:

- Intelligent Platform Management Interface (IPMI) versions 1.5 or 2.0
- Data Center Management Interface (DCMI) version 1.0
- System Management Architecture for Server Hardware (SMASH) version 1.0 over WS-Management (WS-Man)

  Note

  If you use SMASH, make sure you are using the latest version of firmware for the BMC model.

Through a BMC, an administrator can access the computer remotely, independent of the operating system, and control system functions such as the ability to turn the computer off or on.

Workflow and deployment process

The following sequence describes the workflow and deployment process for provisioning physical computers into managed Hyper-V hosts, or into clustered Scale-Out File Servers (As of System Center 2012 R2 Virtual Machine Manager only).

Note

Links are provided to specific procedures in the last section of this topic.

1. Perform initial configuration of the physical computers. This includes configuring the basic input/output system (BIOS) to support virtualization, setting the BIOS boot order to boot from a Pre-Boot Execution Environment (PXE)-enabled network adapter as the first device, and configuring the logon credentials and IP address settings for the BMC on each computer.
2. Create Domain Name System (DNS) entries and Active Directory computer accounts for the computer names that will be provisioned, and allow time for DNS replication to occur. This step is not required, but it is strongly recommended in an environment where you have multiple DNS servers, where DNS replication may take some time.
3. Prepare the PXE server environment, and add the PXE server to VMM management.
4. Add the required resources to the VMM library. These resources include a generalized virtual hard disk with an appropriate operating system (as listed in Operating system requirements, earlier in this topic) that will be used as the base image, and optional driver files to add to the operating system during installation.
5. In the library, create one or more host profile, or as of Virtual Machine Manager (VMM) physical computer profile. These profiles include configuration settings, such as the location of the operating system image, and hardware and operating system configuration settings.
6. To create a Hyper-V host, run the Add Resources Wizard to discover the physical computers, to configure settings such as the host group and the host or physical computer profile to use, to configure custom deployment settings, and to start the operating system and Hyper-V deployment.

   To create a Scale-Out File Server cluster (As of System Center 2012 R2 Virtual Machine Manager only), run the Create Clustered File Server Wizard to discover the physical computers, to configure settings such as the cluster name, provisioning type, and discovery scope, and to start the Scale-Out File Server cluster deployment.
7. During deployment, the VMM management server restarts the physical computers by issuing “Power Off” and “Power On” commands to the BMC through out-of-band management. When the physical computers restart, the PXE server responds to the boot requests from the physical computers.
8. The physical computers boot from a customized Windows Preinstallation Environment (Windows PE) image on the PXE server. The Windows PE agent prepares the computer, configures the hardware when it is necessary, downloads the operating system image (.vhd or .vhdx file) together with any specified driver files from the library, and applies the drivers to the operating system image.

   Roles are then enabled as follows:

   - For Hyper-V host: Hyper-V role
   - For Scale-Out File Server (As of System Center 2012 R2 Virtual Machine Manager only): Failover cluster and file server roles are enabled. Then, after the cluster is created, the Scale-Out File Server role is enabled in the cluster.

   The computer is then restarted.

Example scenario overview

The example scenario demonstrates how to convert a bare-metal computer to a managed Hyper-V host. To complete the scenario, you must have one or more physical computers that have a

BMC installed, with a supported out-of-band management protocol. Also, the computers must support Hyper-V.

The example assumes that you have already configured the fabric as described in the Preparing the Fabric in VMM topic. If you intend to assign the host a static IP address from a pool that is managed by VMM, a logical network must exist with an associated network site and a configured static IP address pool. If you are using Dynamic Host Configuration Protocol (DHCP), you do not need to have a logical network with a static IP address pool configured.

Note
This example uses one bare-metal computer. In a more advanced scenario, you could convert more than one physical computer and then continue on to create a Hyper-V host cluster through the VMM console. To do this, after you complete this scenario, use the procedures in the Creating a Hyper-V Host Cluster in VMM Overview section to cluster the hosts.

The following table summarizes the example resources that are used in this scenario. These example resources are mentioned where they are relevant in procedures in this section, which means they are mentioned in the following topics:

- How to Add a PXE Server to VMM
- How to Create a Host or a Physical Computer Profile to Provision a Hyper-V Host in VMM
- How to Discover Physical Computers and Deploy as Hyper-V Hosts in VMM

Note
The example resource names and configuration are intended to demonstrate the concepts. We recommend that you adapt them to your test environment.

Resource	Resource names
Host names that are assigned to the physical computers	**HyperVHost05.contoso.com** **HyperVHost06.contoso.com** (if you want to deploy two hosts that you will then cluster)
Target host group	**New York\Tier0_NY** **Note** This host group structure is based on the example that is used in the Preparing the Fabric in VMM section.
PXE server (provided through Windows Deployment Services)	**PXEServer01.constoso.com**
Run As accounts	• **PXE Administrator** • **Add Physical Host** • **BMC Administrator**

Resource	Resource names
Logical network	**BACKEND** (for use with a network site that defines a static IP pool) **Note** You can also use DHCP.
Host profiles or Physical computer profiles	• **WS08R2Ent Hyper-V Hosts - Static** • **WS08R2Ent Hyper-V Hosts - DHCP**

In This Section

Follow the procedures listed here to discover physical computers and convert them to managed Hyper-V hosts.

Procedure	Description
Prepare the Physical Computers in VMM	Describes how to prepare the physical computers for discovery. Includes information about configuring the BIOS to support Hyper-V and PXE boot, and configuring BMC settings.
How to Add a PXE Server to VMM	Describes the PXE server requirements and how to add a PXE server to VMM management.
How to Add Driver Files to the VMM Library (optional)	Describes how to add driver files to the library and how to add driver tags.
How to Create a Host or a Physical Computer Profile to Provision a Hyper-V Host in VMM	Describes how to create a host profile or as of System Center 2012 R2 Virtual Machine Manager a physical computer profile. that contains hardware and operating system configuration settings.
How to Create a Physical Computer Profile to Provision File Servers in VMM	Describes how to create physical computer profile to provision computers into a Scale-Out File Server cluster.
How to Discover Physical Computers and Deploy as Hyper-V Hosts in VMM	Describes how to use the Add Resources Wizard to discover the physical computers and deploy them as managed Hyper-V hosts.
How to Create a Scale-Out File Server Cluster in VMM	Describes how to use a physical computer profile to discover computers and provision them into a Scale-Out File Server cluster.

Prepare the Physical Computers in VMM

Before you can begin the provisioning process through Virtual Machine Manager (VMM), you must prepare the physical computers for discovery.

Hyper-V Support

To support the Hyper-V role, the computers must use x64-based processors and have the appropriate basic input/output system (BIOS) settings enabled. For more information, see Hyper-V Installation Prerequisites.

PXE Boot

On each computer, set the BIOS boot order to boot from a Pre-Boot Execution Environment (PXE)-enabled network adapter as the first device.

Out-of-Band Management

To discover the physical computers through out-of-band management, the following conditions must be true:

- The baseboard management controllers (BMCs) must be configured with logon credentials and either a static IP address or an IP address that is assigned through Dynamic Host Configuration Protocol (DHCP). If you use DHCP, we recommend that you configure DHCP to assign a constant IP address to each BMC, for example by using DHCP reservations.
- The VMM management server must be able to access the network segment on which the BMCs are configured.

Note

The BMCs must use a supported out-of-band management protocol, and have the management protocol enabled in the BMC settings. For more information about supported out-of-band management protocols, see the “BMC Requirements” section of the topic Adding Physical Computers as Hyper-V Hosts or as Scale-Out File Servers in VMM Overview.

DNS Configuration

If your environment has multiple Domain Name System (DNS) servers, where DNS replication may take some time, we strongly recommend that you create DNS entries for the computer names that will be assigned to the physical computers, and allow time for DNS replication to occur. Otherwise, host deployment may fail.

See Also

Adding Physical Computers as Hyper-V Hosts or as Scale-Out File Servers in VMM Overview

How to Add a PXE Server to VMM

You can use the following procedure to add a pre-boot execution environment (PXE) server to Virtual Machine Manager (VMM). The PXE server is used to initiate the operating system installation on the physical computer.

Account requirements: You must perform this procedure as a member of the Administrator user role.

Prerequisites

Before you begin this procedure, make sure that the following prerequisites are met:

- You must have a PXE server that is provided through Windows Deployment Services. If you have an existing PXE server in your environment that is provided through Windows Deployment Services, you can use that. VMM will only respond to requests from computers that have been designated as new virtual machine hosts by VMM. All other requests will continue to be handled by the PXE server according to how it is configured.

  If you do not have an existing PXE server, you can deploy the Windows Deployment Services role on a server running a supported operating system. The operating system can be as follows:

  - In System Center 2012: Windows Server 2008 R2
  - In System Center 2012 SP1: Windows Server 2008 R2, or Windows Server 2012
  - In System Center 2012 R2: Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2

  For information about how to deploy Windows Deployment Services, including the required permissions, see the Windows Deployment Services Getting Started Guide for Windows Server 2008 and Windows Server 2008 R2, or the Windows Deployment Services Getting Started Guide for Windows Server 2012.

  When you install Windows Deployment Services, consider the following:

  - During installation of the Windows Deployment Services role, install both the **Deployment Server** and the **Transport Server** options.
  - When you configure Windows Deployment Services, you do not have to add images to Windows Deployment Services. During host deployment, VMM uses a virtual hard disk that you have created and stored in the VMM library.
  - You do not have to configure the settings on the **PXE Response** tab in Windows Deployment Services. VMM ignores these settings because VMM uses its own PXE provider.
- The PXE server must be in the same subnet as the physical computers that you want to provision.
- When you add a PXE server, you must specify account credentials for an account that has local administrator permissions on the PXE server. You can enter a user name and password or specify a Run As account. If you want to use a Run As account, you can create the Run As account before you begin this procedure, or create it during the procedure.

  For example, create a Run As account that is named **PXE Administrator**.

  Note
  You can create Run As accounts in the **Settings** workspace. For more information about Run As accounts, see How to Create a Run As Account.

To add the PXE server to VMM

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, click **Servers**.

3. On the **Home** tab, in the **Add** group, click **Add Resources**, and then click **PXE Server**.
4. In the **Add PXE Server** dialog box, do the following:
   a. In the **Computer name** box, enter the computer name of the PXE server.

      For example, enter **PXEServer01.contoso.com**.

   b. Enter the credentials for an account that has local administrator permissions on the PXE server.

      You can specify an existing Run As account or manually enter user credentials in the format *domain_name**user_name*.

      Note
      If you do not already have a Run As account, click **Browse**, and then in the **Select a Run As Account** dialog box, click **Create Run As Account**.

      For example, if you created the example **PXE Administrator** Run As account that is described in the Prerequisites section of this topic, you would click **Browse**, click the **PXE Administrator** Run As account, and then click **OK**.

   c. Click **Add**.

      The **Jobs** dialog box opens. Verify that the job has a status of **Completed**, and then close the dialog box. The job sets up the new PXE server, installs the VMM agent on the PXE server, imports a new Windows Preinstallation Environment (Windows PE) image, and adds the machine account for the PXE server to VMM.
5. To verify that the PXE server was added, perform these steps:
   d. .a. In the **Fabric** pane, expand **Servers**, and then click **PXE Servers**.
   b. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
   c. In the **PXE Servers** pane, verify that the PXE server appears with an agent status of **Responding**.

See Also

Adding Physical Computers as Hyper-V Hosts or as Scale-Out File Servers in VMM Overview

How to Add Driver Files to the VMM Library

You can use the following procedures to add driver files to the library in VMM, and to assign tags to the drivers. By adding driver files to the library and configuring a host profile, or a physical computer profile (as of System Center 2012 R2 Virtual Machine Manager) to add the driver files to the operating system during deployment, VMM can install the drivers during the installation of the operating system on a physical computer.

In the host profile or physical computer profile, you can select to filter the drivers by tags, or you can select to filter drivers with matching Plug and Play (PnP) IDs on the physical computer. If you select to filter the drivers by tags, VMM determines the drivers to apply by matching the tags that you assign to the drivers in the library to the tags that you assign in the profile. If you select to filter drivers with matching PnP IDs, you do not have to complete the “To assign custom tags to the driver files” procedure in this topic.

Note

These procedures are optional.

Account requirements To add driver files to the library, you must be a member of the Administrator user role, or a member of the Delegated Administrator user role where the management scope includes the library server where the library share is located.

To add driver files to the library

1. Locate a driver package that you want to add to the library.

   For example, you may want to add a driver package for a network adapter driver.

2. In the library share that is located on the library server that is associated with the group where you want to deploy the physical computers, create a folder to store the drivers, and then copy the driver package to the folder.

   For example, create a folder that is named **Drivers** in the library share, and then copy the driver package for a network adapter driver (in its own folder) to the **Drivers** folder.

   Important
   We strongly recommend that you create a separate folder for each driver package, and that you do not mix resources in the driver folders. If you include other library resources such as .iso images, .vhd files or scripts with an .inf file name extension in the same folder, the VMM library server will not discover those resources. Also, when you delete an .inf driver package from the library, VMM deletes the entire folder where the driver .inf file resides.

3. In the VMM console, open the **Library** workspace.
4. In the **Library** pane, expand **Library Servers**, expand the library server where the share is located, right-click the share, and then click **Refresh**.

   After the library refreshes, the folder that you created to store the drivers appears.

To assign custom tags to the driver files

1. In the **Library** pane, expand the folder that you created to store the drivers in the previous procedure, and then click the folder that contains the driver package.

   For example, expand the **Drivers** folder, and then click the folder that you created for the network adapter driver package.

   The driver .inf file of type **Driver Package** is listed in the **Physical Library Objects** pane.

2. In the **Physical Library Objects** pane, right-click the driver .inf file, and then click **Properties**.
3. In the *Driver File Name* **Properties** dialog box, in the **Custom tags** box, enter custom tags separated by a semi-colon, or click **Select** to assign available tags or to create and assign new ones. If you click **Select**, and then click **New Tag**, you can change the name of the tag after you click **OK**.

   For example, if you added a network adapter driver file, you could create a tag that is named *ServerModel NetworkAdapterModel*, where *ServerModel* is the server model and *NetworkAdapterModel* is the network adapter model.

4. When you are finished, click **OK**.

See Also

Adding Physical Computers as Hyper-V Hosts or as Scale-Out File Servers in VMM Overview

How to Create a Host or a Physical Computer Profile to Provision a Hyper-V Host in VMM

How to Associate a VMM Library Server with a Host Group

How to Create a Host or a Physical Computer Profile to Provision a Hyper-V Host in VMM

As of System Center 2012 R2, physical computer profiles replace host profiles. You can use physical computer profiles to provision computers into Hyper-V hosts, in the same manner that you use host profiles. The following procedure describes how to create a host profile—or for System Center 2012 R2, a physical computer profile—in the Virtual Machine Manager (VMM) library. You can then use the profile to provision computers into Hyper-V hosts. These profiles include configuration settings such as the location of the operating system image to use during host deployment, together with configuration settings for the hardware and operating system.

Important

Be sure to determine whether the computers that you want to add use Extensible Firmware Interface (EFI) or basic input/output system (BIOS). If you have computers of each type, you must create a separate profile for each type.

Prerequisites

Before you begin this procedure, be sure to meet the following prerequisites:

- A generalized virtual hard disk that has an appropriate operating system must exist in a library share.

  As of VMM in System Center 2012 Service Pack 1 (SP1), the format of the virtual hard disk file can be .vhd or .vhdx. For VMM in System Center 2012, the format must be .vhd. Because the profile is for a host system, the operating system on the virtual hard disk must be compatible with the file format, as follows.

Possible operating systems on a .vhd file	Possible operating systems on a .vhdx file (for System Center 2012 SP1 or System Center 2012 R2)
Windows Server 2012 Windows Server 2008 R2 with SP1 Windows Server 2008 R2	Windows Server 2012 Windows Server 2012 R2

  You must use an operating system edition that supports Hyper-V and is supported by VMM. For more information, see the following:

  - For System Center 2012 – Virtual Machine Manager or for System Center 2012 SP1 see: **System Requirements: Hyper-V Hosts in System Center 2012 and in System Center 2012 SP1**.

- For System Center 2012 R2 Virtual Machine Manager see: **Preparing your environment for System Center 2012 R2 Virtual Machine Manager**.

  Tip

  If you use Remote Desktop to manage servers, we recommend that you enable Remote Desktop connections in the image. You can also enable Remote Desktop by using an answer file in the host profile or physical computer profile, or by running a post-installation script after the host is deployed.

  To create the virtual hard disk, you can create a virtual machine, install the guest operating system, and then use Sysprep with the **/generalize** and the **/oobe** options to generalize the associated virtual hard disk. For more information about Sysprep, see Sysprep Command-Line Options. Another method that you can use is to follow the prerequisites and steps 1 and 2 of the article Walkthrough: Deploy a Virtual Hard Disk for Native Boot.

  For more information about virtual hard disks with native boot, see Understanding Virtual Hard Disks with Native Boot.

  Important

  We recommend that for production servers, you use a fixed-disk .vhd or .vhdx file to increase performance and to help protect user data. When you create the host profile or the physical computer profile, by default, VMM converts a dynamic disk to a fixed disk. If desired, you can change this setting when you create the profile.

- If you plan to assign custom drivers, the driver files must exist in the library. If you want to filter the drivers by tags, you must tag the driver files appropriately. For more information, see How to Add Driver Files to the VMM Library.
- If you are running VMM in System Center 2012 SP1 or System Center 2012 R2, and you plan to use a physical network adapter that uses a logical switch, or you plan to use a virtual network adapter, prepare your network configuration as follows.

For a physical network adapter	For a virtual network adapter
If you want to use a physical network adapter that uses a logical switch, before you create the host profile or the physical computer profile, make sure that you have installed the intended number of network adapters on the host computer or computers. In addition, before you create the host profile or the physical computer profile in VMM, create the uplink port profile and the logical switch. For more information, see: How to Create a Port Profile for Uplinks in VMM How to Create a Logical Switch in VMM	If you want to create a virtual network adapter, before you create the host profile or the physical computer profile, make sure that you have installed the intended number of physical network adapters on the host computer or computers. In addition, before you create the host profile or the physical computer profile, on the VMM management server, install all necessary virtual switch extensions and extension providers, create a logical switch, and create at least one virtual machine network. If you will use a port classification with the virtual network adapter, create the port classification before you create the host profile or the physical computer profile. For more information, see: Configuring Ports and Switches for VM Networks in VMM How to Create a VM Network in VMM in System Center 2012 SP1 How to Create a VM Network in VMM in System Center 2012 R2

- If you want to assign static IP addresses through VMM, the logical network that you want the host to use must have an associated network site and static IP address pool that are managed by VMM. The network site must be available to the host group or to a parent host group where you want to assign the hosts. For more information, see Configuring Logical Networking in VMM Overview.

  In this example scenario, the host uses the **BACKEND** logical network.
- If you want to use an answer file to specify additional host settings that are common to all hosts that will use this profile, create an Unattend.xml file that has the appropriate settings and add it to a VMM library share. For example, you may want to perform additional configuration steps, such as assigning static IP addresses to other physical network adapters on the host besides the management adapter, and enabling Remote Desktop. (Note that during the host deployment process, VMM automatically enables the Hyper-V role and the Multipath I/O [MPIO] feature.) You can select the answer file to use when you configure the profile.

  Tip

You can also run scripts on a Hyper-V host after the host is deployed. To do this, right-click the host in the **Fabric** workspace, and then click **Run Script Command**.

In the advanced settings for script commands, note that the **Restart the computer or virtual machine if the specified exit code is returned** setting is ignored when you run the script on a host.

- You must have a Run As account that you can use to join the target hosts to the domain.

  For example, create the Run As account **Add Physical Host**.

  Security

  Use an account that has very limited permissions. You should use the account only to join computers to the domain.

  Note

  You can create a Run As account in the **Settings** workspace. For more information about Run As accounts, see How to Create a Run As Account in VMM.

To create a host profile or a physical computer profile

1. Open the **Library** workspace.
2. On the **Home** tab, in the **Create** group, click **Create**, and then click **Host Profile** or **Physical Computer Profile**.

   The New Host Profile Wizard, or as of System Center 2012 R2 the New Physical Computer Profiles Wizard, opens.
3. On the **Profile Description** page, type a name and description for the profile.

   When you are creating a physical computer profile (for System Center 2012 R2), select **VM Host**.

   For example, if you want to assign an IP address through Dynamic Host Configuration Protocol (DHCP), type the name **WS08R2Ent Hyper-V Hosts - DHCP** and the description **Windows Server 2008 R2 Enterprise Hyper-V Hosts – DHCP address allocation**, and then click **Next**.
4. On the **OS Image** page, do the following:
   a. Next to the **Virtual hard disk file** box, click **Browse**, click the generalized virtual hard disk file that you added to the library share, and then click **OK**.

      Important

      Make sure that the file meets the requirements that are defined in the "Prerequisites" section of this topic.

      For the virtual hard disk file that you selected, VMM displays the virtual hard disk type, the expanded size (if dynamic), the current size, and the minimum partition size that you need.

   b. By default, if the disk type is dynamic, VMM will automatically convert the disk to a fixed disk type during host deployment. We strongly recommend that for production servers, you use a fixed disk type to increase performance and to help protect user

data. If you do not want to use a fixed disk, select the **Do not convert the virtual hard disk type to fixed during deployment** check box.

c. Click **Next** to continue.

5. On the **Hardware Configuration** page, configure the following options, and then click **Next**.

Management NIC (under **Network Adapters**)	• **For System Center 2012 – Virtual Machine Manager:** For the network adapter that you will use to communicate with the VMM management server, select whether to obtain an IP address through DHCP or to allocate a static IP address from the logical network that you specify. For example, if you are configuring a host profile or a physical computer profile for the **WS08R2Ent Hyper-V Hosts – DHCP** profile, click **Obtain an IP address through the DHCP service**. • **For VMM in System Center 2012 SP1 or in System Center 2012 R2**: For the network adapter that you will use to communicate with the VMM management server, choose between configuring a physical network adapter and creating a virtual network adapter. (The latter choice has certain requirements, as described in the list before this procedure). To provide a Consistent Device Naming (CDN) name for the adapter, or to configure logical switch and port information for the adapter, click **Physical Properties**. For more information about switches and ports, see Configuring Ports and Switches for VM Networks in VMM. To select whether to obtain an IP address through DHCP or to

	allocate a static IP address from the logical network that you specify, click **IP Configuration**. (If this is a physical network adapter that you have connected to a logical switch, the **IP Configuration** options will be disabled.) For example, if you are configuring a host profile or a physical computer profile for the **WS08R2Ent Hyper-V Hosts – DHCP** profile that is intended for use with physical adapters that use a CDN of Blue, first select the physical adapter option, and then click **Physical Properties** to specify the CDN. Next, click **IP Configuration**, and then click **Obtain an IP address through the DHCP service**. You can also click the **Add** button and add a physical network adapter or a virtual network adapter. Or you can remove an adapter by selecting it and clicking the **Remove** button.
Disk (under **Disk and Partitions**)	Specify the partitioning scheme for the first disk. You can select either of the following options: • **Master Boot Record (MBR)** • **GUID Partition Table (GPT)** **Note** If the host profile or the physical computer profile is for computers that use EFI, select **GUID Partition Table (GPT)** as the partitioning scheme. Under **Disk**, click the default partition name **OS**. In the **Partition information** pane, configure the following options: • Select the volume label. • Select whether to use all remaining free disk space or to use a specific

	size (in gigabytes). • Select whether to designate the partition as the boot partition. By default, the **Make this the boot partition** check box is selected for the operating system partition.  **Note** During deployment, VMM will copy the .vhd or .vhdx file to the boot partition and automatically create a system partition on the same disk where the boot partition is located. To add a new disk or partition, for System Center 2012, click either **Add Disk** or **Add Partition** on the toolbar. For System Center 2012 SP1 or System Center 2012 R2, click **Add**, and then select **Disk** or **Partition**. The new disk or partition appears under the **Disk and Partitions** section. Configure the settings for the new disk or partition.
Driver filter (under **Driver Options**)	You can filter the driver files that will be applied to the operating system during host deployment. You can select either of the following options: • **Filter drivers with matching PnP IDs**. By default, drivers that match the Plug and Play (PnP) IDs on the target physical computer are used. • **Filter drivers with all matching tags specified below**. If you select this option, enter the tags by which you want to filter, separated by semicolons, or click **Select** to view and assign the available tags. If you click **New Tag**, you can change the name of the tag after you click **OK**.  **Note** If you select the **Filter drivers with all matching tags specified below** option, you

	must add driver files to the library and assign corresponding tags to the drivers in the library share before you deploy the host. For information about how to add driver files to the library, see How to Add Driver Files to the VMM Library.

6. On the **OS Configuration** page, configure the following options, and then click **Next**.

Domain (under **General Settings**)	In the **Domain** box, specify the domain that the Hyper-V host should join. For example, type **contoso.com**. Next to the **Run As account** box, click **Browse**, and then select the Run As account that will be used to join the host to the domain. For example, if you created the Run As account that is described in the "Prerequisites" section of this topic, click **Add Physical Host**. **Security** Use an account that has very limited privileges. You should use the account only to join computers to the domain.
Admin Password (under **General Settings**)	Under **Specify the credential for the local administrator account**, type the password that you want to assign to the local administrator account on the physical computer. You cannot specify a blank password.
Identity Information (under **General Settings**)	Complete the information in the **Full name** and **Organization name** boxes.
Product Key (under **General Settings**)	Type the product key. For multiple computers, you must use a volume licensing key. **Note** If you do not enter a product

	key, the standard activation grace period applies.
Time Zone (under **General Settings**)	Select the time zone for the computer.
Answer File (under **Scripts**)	To use an answer file to specify additional settings, click **Browse**, click the Unattend.xml file that you want to use, and then click **OK**.
[GUIRunOnce] Commands (under **Scripts**)	To specify one or more commands to run the first time that a user logs on to the computer, type a command in the **Command to add** box, and then click **Add**. Repeat this procedure to add multiple commands. This action adds the commands to the [GuiRunOnce] section of the Sysprep file.

7. On the **Host settings** page, specify the path on the host to store the files that are associated with virtual machines that are placed on the host, click **Add**, and then click **Next**. Do not specify a location on the drive C because drive C is not available for placement.

   By default, if you do not specify a path, placement determines the most suitable location.

   Note
   You can accept the default path, specify a new path, or change the path after you deploy the host.

8. On the **Summary** page, confirm the settings, and then click **Finish**.

   The **Jobs** dialog box appears. Make sure that the job has a status of **Completed**, and then close the dialog box.

9. To verify that the host profile or the physical computer profile was created, in the **Library** pane, expand **Profiles**, and then click **Host Profiles** or **Physical Computer Profiles**.

   The new host profile or physical computer profile appears in the **Profiles** pane.

See Also

Adding Physical Computers as Hyper-V Hosts or as Scale-Out File Servers in VMM Overview

Configuring Networking in VMM

How to Discover Physical Computers and Deploy as Hyper-V Hosts in VMM

You can use the following procedure to create a fully-managed Hyper-V host from a physical computer through Virtual Machine Manager (VMM). The physical computer can either be a “bare-metal computer”, which means a computer without an operating system installed, or a computer

with an installed operating system that will be overwritten during this process. In this procedure, you use the **Add Resource Wizard** to do the following:

1. Discover the physical computer through out-of-band management
2. Deploy an operating system image on the computer through the host profile or the physical computer profile
3. Enable the Hyper-V role on the computers
4. Bring the computer under VMM management as a managed Hyper-V host

Note

As of System Center 2012 R2 Virtual Machine Manager host profiles are replaced by physical computer profiles. Physical computer profiles are used in the same manner as host profiles to discover physical computers and to deploy them as Hyper-V hosts.

Prerequisites

Before you begin this procedure, make sure that the following prerequisites are met:

- The physical computers must be correctly configured, a PXE server must exist and must be added to VMM management, a host profile or as of System Center 2012 R2 a physical computer profile must exist, and any needed driver files must be added to the library. For more information, see Prepare the Physical Computers in VMM, How to Add a PXE Server to VMM, How to Create a Host or a Physical Computer Profile to Provision a Hyper-V Host in VMM, and How to Add Driver Files to the VMM Library.

  Important

  As described in Prepare the Physical Computers in VMM, if your environment has multiple Domain Name System (DNS) servers, where DNS replication may take some time, we strongly recommend that you create DNS entries for the computer names that will be assigned to the physical computers, and allow time for DNS replication to occur. Otherwise, host deployment may fail.

- If you are running VMM in System Center 2012 and you plan to assign static IP addresses to the hosts, then for each physical computer, obtain and note the MAC address of the network adapter that you want to use for management. The management adapter is the network adapter that the host will use for communication with the VMM management server. Typically, you can obtain the MAC address of the installed network adapters from the BIOS or EFI settings, or from the invoice sheet that you receive from the OEM.

  If you are running VMM in System Center 2012, and the computers that you want to deploy as hosts contain multiple network adapters or disk volumes, it is a best practice to collect detailed information about the adapters (for example, MAC addresses) and the volumes (for example, disk sizes) before you begin the deployment process. Collecting this information can help you to create the intended configuration during deployment.

- If you are running VMM in System Center 2012 Service Pack 1 (SP1) or in System Center 2012 R2, and the computers that you want to deploy as hosts contain multiple network adapters or disk volumes, you do not have to collect detailed information about the adapters and volumes before beginning the deployment process. Instead, you can view this information during host deployment, through a process called deep discovery.

- Although it is not a required prerequisite, you can create a Run As account before you begin this procedure. (You can also create the account during the procedure.) The Run As account must have permissions to access the Baseboard Management Controller (BMC) that is used for out-of-band management on the computers that you want to discover.

  For example, create a Run As account that is named **BMC Administrator**.

  Note
  You can create a Run As account in the **Settings** workspace. For more information about Run As accounts, see How to Create a Run As Account in VMM.

To discover the physical computer and deploy it as a managed Hyper-V host

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, click **Servers**.
3. On the **Home** tab, in the **Add** group, click **Add Resources**, and then click **Hyper-V Hosts and Clusters**.

   The Add Resource Wizard opens.
4. On the **Resource location** page, click **Physical computers to be provisioned as virtual machine hosts**, and then click **Next**.
5. On the **Credentials and protocol** page, do the following:
   a. Next to the **Run As account** box, click **Browse**, click a Run As account that has permissions to access the BMC, and then click **OK**.

      Note
      If you do not already have a Run As account, click **Browse**, and then in the **Select a Run As Account** dialog box, click **Create Run As Account**.

      For example, if you created the Run As account that is described in the Prerequisites section of this topic, click the **BMC Administrator** account, and then click **OK**.

   b. In the **Protocol** list, click the out-of-band management protocol that you want to use for discovery, and then click **Next**.

      Note
      - If you want to use Data Center Management Interface (DCMI), click **Intelligent Platform Management Interface (IPMI)**. Although DCMI 1.0 is not listed, it is supported.
      - If you use SMASH, make sure that you use the latest version of firmware for the BMC model.
6. On the **Discovery scope** page, specify the IP address scope that includes the IP addresses of the BMCs, and then click **Next**. You can enter a single IP address, an IP subnet, or an IP address range.
7. If you specified an IP subnet or an IP address range, the **Target resources** page will list the discovered computers. Select the check box next to each computer that you want to convert to a Hyper-V host. If you are running VMM in System Center 2012 SP1 or System Center 2012 R2, and you do not need the information that is provided through

deep discovery (for example, MAC addresses of network adapters), then you can decrease the time that is needed for deployment by clearing the **Skip deep discovery for the selected computers** check box.

Caution

If you select a computer that already has an operating system installed, and later in this procedure you select the option to skip the Active Directory Domain Services (AD DS) check for the computer name, the operating system will be overwritten during the deployment process. Make sure that you select the correct computers. Keep careful records of the IP addresses of the BMCs, or verify the computers by using the System Management BIOS (SMBIOS) GUID or the serial number.

8. Click **Next**.
9. On the **Provisioning options** page, do the following, and then click **Next**:
   a. In the **Host group** list, click the host group that you want to assign as the target location for the new Hyper-V hosts.

      For example, click **New York\Tier0_NY**.

   b. Choose whether the Hyper-V hosts will obtain their network settings through DHCP, or whether to assign static IP addresses from an IP address pool that is managed by VMM. For either option, in the **Host profile** list, you must select a profile that contains these predefined network settings. Only the profiles with an IP address setting that matches the selected assignment type will appear in the list.

      For example, if you want to obtain network settings through DHCP, click **Obtain IP addresses and other network settings through a DHCP service**, in the **Host profile** list, click the **WS08R2Ent Hyper-V Hosts – DHCP** profile, and then click **Next**. If you want to specify static IP addresses, click **Specify static IP addresses and customize deployment settings for each host**, in the **Host profile** list, click the **WS08R2Ent Hyper-V Hosts - Static** profile, and then click **Next**.
10. If you are running VMM in System Center 2012 SP1 or System Center 2012 R2, follow this step. Otherwise, skip to the next step.

    Select a computer, allow time for deep discovery, and click items in the list on the left to review information about the computer. As needed, adjust settings.

    For example, to configure specific switch or port settings for a network adapter (different from the settings that you configured in the host profile or the physical computer profile), click **Network adapters**, locate a network adapter in the list, and for that adapter, click the ellipsis button **(…)**. A dialog box with advanced configuration settings opens. For more information about switch and port settings, see the links at the end of this procedure. As another example, to specify the disk volume on which the operating system should be installed, click **Disks**, and then select the appropriate volume.

    As a best practice, with a new or changed host profile or physical computer profile, or new computers, review the information in this wizard page carefully.

Important

If the number of physical network adapters in a computer does not match the number of physical network adapters that are defined in the host profile or the physical computer profile, you must specify any missing information for the adapters. Also, if you decide not to deploy a computer at this time, for example, if it requires physical hardware to be installed or uninstalled on it, you can remove the computer from the list of those that are to be deployed. To do this, select the BMC IP address of the computer that you want to remove, and then click the **Remove** button.

11. On the **Deployment customization** page, the steps vary, depending on whether you selected a profile that uses DHCP or a profile that uses static IP addresses.

    Note
    Until you type a computer name for each computer, a **Missing settings** warning appears.

    - **For a profile that uses DHCP**: If in step 9b you selected a host profile or a physical computer profile that uses DHCP, do the following:
        i. Click a BMC IP address in the list.
        ii. In the **Computer name** box, enter a computer name for the selected entry. The computer name cannot include any wildcard characters. Also, the computer name must be unique.

        For example, enter **HyperVHost05.contoso.com**.

        iii. Decide whether to select the **Skip Active Directory check for this computer name** check box based on the following information:

        If the check box is clear, deployment will fail if the computer account already exists in Active Directory Domain Services (AD DS). This check helps to prevent you from accidentally overwriting the operating system on an existing computer.

        If you select the check box, deployment will continue if the computer account already exists in AD DS.

        Caution
        If you select the **Skip Active Directory check for this computer name** check box, and the computer exists in AD DS and has an existing operating system, deployment will overwrite the existing operating system installation.

        Note that if there is an existing computer account in AD DS that was created by a user other than the Run As account that was specified in the host profile or the physical computer profile, and you skip Active Directory verification, the deployment process will fail to join the computer to the domain.

        iv. If multiple BMC IP addresses are listed, for each one, click the entry, and then

enter a computer name.

For example, for a second computer, enter **HyperVHost06.contoso.com**.

v. When you complete this step, and there are no more **Missing settings** warnings, click **Next**.

vi. Review the warning message, and then click **OK** to continue.

Note

Until you complete all required settings for a computer, a **Missing settings** warning or **Invalid MAC address** error appears.

- **For a profile that uses static IP addresses**: If in step 9b you selected a host profile or a physical computer profile that uses static IP addresses, do the following for each BMC IP address in the list:

  i. In the **Computer name** box, enter the name of the computer. The computer name cannot include any wildcard characters. Also, the computer name must be unique.

  For example, enter **HyperVHost05.contoso.com**.

  ii. Decide whether to select the **Skip Active Directory check for this computer name** check box based on the following information:

  If the check box is clear, deployment will fail if the computer account already exists in Active Directory Domain Services (AD DS). This check helps to prevent you from accidentally overwriting the operating system on an existing computer.

  If you select the check box, deployment will continue if the computer account already exists in AD DS.

  Caution

  If you select the **Skip Active Directory check for this computer name** check box, and the computer exists in AD DS and has an existing operating system, deployment will overwrite the existing operating system installation.

  Note that if there is an existing computer account in AD DS that was created by a user other than the Run As account that was specified in the host profile or in the physical computer profile, and you skip Active Directory verification, the deployment process will fail to join the computer to the domain.

  iii. In the **MAC address** box, enter the MAC address of the management network adapter on the selected computer.

  Note

  The management adapter is the network adapter that will be used to

communicate with the VMM management server. This is not the MAC address of the BMC.

iv. In the **Logical network** list, click the logical network that you want to use. The default logical network is what is defined in the host profile or in the physical computer profile. The list of available logical networks matches what is available to the host group that you selected in step 9.

v. In the **IP subnet** list, click the IP subnet that you want to use. The list of subnets is scoped to what is defined for the logical network in the associated network sites.

Important
Make sure that you select the correct IP subnet that corresponds to the physical location where you are deploying the hosts. Otherwise, deployment will fail.

vi. To assign an IP address, do either of the following:

To automatically assign an IP address from the selected IP subnet, make sure that the **Obtain an IP address corresponding to the selected subnet** check box is selected. VMM will assign an IP address from the first available static IP address pool.

Note
If the **Obtain an IP address corresponding to the selected subnet** check box is selected, the **IP range** and **IP address** settings do not apply.

To assign a specific IP address from the selected IP subnet, clear the **Obtain an IP address corresponding to the selected subnet** check box. In the **IP range** list, click the IP address range that you want. In the **IP address** box, enter an available IP address that falls in the range.

Note
The list of IP address ranges is scoped to the static IP address pools that are available for the selected subnet.

vii. When you complete this step, and there are no more warnings or error messages, click **Next**.

viii. Review the warning message, and then click **OK** to continue.

12. On the **Summary** page, confirm the settings, and then click **Finish** to deploy the new Hyper-V hosts and bring them under VMM management.

    The **Jobs** dialog box appears. Make sure that all steps in the job have a status of **Completed**, and then close the dialog box.

13. To confirm that the host was added, follow these steps:

    a. Open the **Fabric** workspace.

b. In the **Fabric** pane, expand **Servers**, expand **All Hosts**, and then expand the host group that you specified in step 9a.

c. Verify that the new Hyper-V hosts appear in the host group.

Tip

To run any post-deployment scripts on a specific Hyper-V host, right-click the host, and then click **Run Script Command**.

In the advanced script command settings, note that the **Restart the computer or virtual machine if the specified exit code is returned** setting is ignored when you run the script on a host.

See Also

Adding Physical Computers as Hyper-V Hosts or as Scale-Out File Servers in VMM Overview

Configuring Hyper-V Host Properties in VMM

Creating and Modifying Hyper-V Host Clusters in VMM

Configuring Hyper-V Host Properties in VMM

After you add Hyper-V hosts to VMM, you can configure the host properties. You can configure the settings that are described in the following table.

Tab	Settings
General	• View identity and system information for the host. This includes information such as processor information, total and available memory and storage, the operating system, the type of hypervisor, and the VMM agent version. • Enter a host description. • Configure whether the host is available for placement. • Configure the remote connection port. By default, the port is set to 2179.
Hardware	View or modify settings for CPU, memory, graphics processing units (GPUs), storage (including whether the storage is available for placement), floppy drives, network adapters, DVD/CD-ROM drives and Baseboard Management Controller (BMC) settings. • For more information about how to configure network settings, see How to Configure Network Settings on a Hyper-V Host in VMM.

Tab	Settings
	As of System Center 2012 Service Pack 1 (SP1), you can also configure network settings as described in How to Configure Network Settings on a Host by Applying a Logical Switch in VMM. As of System Center 2012 R2, you can also add a top-of-rack switch for a host, as described in How to Add a Top-of-Rack Switch in VMM in System Center 2012 R2. • For more information about how to configure BMC settings, see How to Configure Host BMC Settings in VMM.
Status	Lists health status information for the host. Includes areas such as overall health, Hyper-V role health and VMM agent health. In the **Status** pane, you can also do the following: • View error details. • Refresh the health status. • Click **Repair all**. VMM will try to automatically fix any errors.
Virtual Machine Paths/Virtual Machines	Shows the virtual machines that reside on the host, together with status information. Also enables you to register virtual machines on the host.
Reserves	Enables you to override host reserve settings from the parent host group, and configure reserved resources for the host. Configurable resources include CPU, memory, disk space, disk I/O and network capacity.
Storage	Shows storage allocated to a host, and enables you to add and remove storage logical units that are managed by VMM. For more information, see How to Configure Storage on a Hyper-V Host in VMM. **Note** For information about how to configure storage for a Hyper-V host cluster, see How to Configure Storage on a Hyper-

Tab	Settings
	V Host Cluster in VMM.
Virtual Switches/Virtual Networks	Enables you to configure virtual switches (which are called “virtual networks” in VMM in System Center 2012). For more information about how to configure network settings, see How to Configure Network Settings on a Hyper-V Host in VMM. As of System Center 2012 Service Pack 1 (SP1), you can also configure network settings as described in How to Configure Network Settings on a Host by Applying a Logical Switch in VMM.
Placement Paths/Placement	Enables you to configure the default virtual machine paths, and as of System Center 2012 R2, also default parent disk paths that will be used during virtual machine placement on the host.
Servicing Windows	Enables you to select servicing windows.
Custom Properties	Enables you to assign and manage custom properties.

In This Section

This section includes detailed information about how to configure storage, network, and Baseboard Management Controller (BMC) settings on a managed Hyper-V host or host cluster.

Topic	Description
How to Configure Storage on a Hyper-V Host in VMM	Describes how to create, assign, and remove storage logical units that are under VMM management on a Hyper-V host. Also describes how to create an iSCSI session to a new or existing array.
How to Configure Network Settings on a Hyper-V Host in VMM	Describes how to configure network settings on a Hyper-V host, and how to view compliance information for physical network adapters on the host.
How to Configure Host BMC Settings in VMM	Describes how to configure BMC settings for a managed host. If a computer is configured for

Topic	Description
	out-of-band management through a BMC, you can power the host on and off from the VMM console.
How to Configure Network Settings on a Host by Applying a Logical Switch in VMM	Describes how to apply a logical switch to a network adapter on a host. This brings together the network settings that you previously configured for the logical switch (and associated port profiles) and applies them to the network adapter. By applying logical switches, you can consistently configure identical capabilities for network adapters across multiple hosts.
How to Add a Top-of-Rack Switch in VMM in System Center 2012 R2	Describes how to add a top-of-rack (TOR) switch as a resource in VMM. This helps you keep the settings in the TOR switch synchronized with the settings that you see in VMM.
How to View Compliance Information for a Physical Network Adapter on a Host in VMM	Describes how to see whether the settings on physical network adapters on a host are consistent with the configuration in VMM. For example, you can see whether all the IP subnets and VLANs that are included in a network site in a logical network are assigned to a physical network adapter.

How to Configure Storage on a Hyper-V Host in VMM

You can use the following procedures to configure storage on a Hyper-V host in System Center 2012 – Virtual Machine Manager (VMM). The procedures show the following:

- How to create and assign a logical unit from a managed Hyper-V host
- How to assign an existing logical unit to a Hyper-V host
- How to remove an assigned logical unit from a Hyper-V host
- How to create an iSCSI session on a host

Account requirements To complete this procedure, you must be a member of the Administrator user role or a member of the Delegated Administrator user role where the management scope includes the host group where the Hyper-V host is located.

Prerequisites

Before you begin these procedures, make sure that the following prerequisites are met:

- You must have completed the procedures in the Configuring Storage in VMM section on a supported storage array to discover, classify and provision storage through the VMM console. When you provision the storage to a host group, consider the following:
  - If you want to create logical units from a managed host, you must allocate a storage pool to the host group where the host resides. For more information, see How to Allocate Storage Pools to a Host Group in VMM.
  - If you want to assign pre-created logical units to a host, allocate logical units to the host group where the host resides. For more information, see How to Allocate Storage Logical Units to a Host Group in VMM.

    Note
    Be aware that if you create a logical unit from a host as described in the previous bullet, and then you do not assign the logical unit to the host, the logical unit is available to other hosts in the host group.
- Make sure that the host is correctly configured to access the storage array. Configuration will vary depending on your storage hardware. Configuration typically includes the following:

  Note
  For specific configuration information, see your storage array vendor's documentation.
  - The Multipath I/O (MPIO) feature must be added on each host that will access the Fibre Channel or iSCSI storage array. You can add the MPIO feature through Server Manager. If the MPIO feature is already enabled before you add a host to VMM management, VMM will automatically enable MPIO for supported storage arrays by using the Microsoft provided Device Specific Module (DSM). If you already installed vendor-specific DSMs for supported storage arrays, and then add the host to VMM management, the vendor-specific MPIO settings will be used to communicate with those arrays.

    If you add a host to VMM management before you add the MPIO feature, you must add the MPIO feature, and then manually configure MPIO to add the discovered device hardware IDs. Or, you can install vendor-specific DSMs.

    Note
    For more information, including information about how to add the MPIO feature, see Support for Multipath I/O (MPIO).
  - If you are using a Fibre Channel storage area network (SAN), each host that will access the storage array must have a host bus adapter (HBA) installed. Additionally, make sure that the hosts are zoned accordingly so that they can access the storage array.
  - If you are using an iSCSI SAN, make sure that the Microsoft iSCSI Initiator Service on each host is started and set to Automatic. This topic includes a procedure to ensure that iSCSI portals have been added and that the iSCSI initiator is logged into the array.

To create a logical unit and assign it to a host

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then click **All Hosts**.

3. In the **Hosts** pane, right-click the host that you want to configure, and then click **Properties**.
4. In the *Host Name* **Properties** dialog box, click the **Storage** tab.
5. To create a logical unit, follow these steps:
   a. On the toolbar, next to **Disk**, click **Add**.
   b. Next to the **Logical unit** list, click **Create Logical Unit**.

      The Create Logical Unit dialog box opens.
   c. In the **Storage pool** list, click the desired storage pool.
   d. In the **Name** box, enter a name for the logical unit. Use only alphanumeric characters.
   e. Optionally, in the **Description** box, enter a description for the logical unit.
   f. In the **Size (GB)** box, enter the size of the logical unit, in gigabytes.
   g. When you are finished, click **OK**.

   The new logical unit is listed in the **Logical unit** list. At this point, the logical unit is created, but not assigned to any host. To assign the logical unit to the host, continue with this procedure.
6. In the **Logical unit** list, verify that the logical unit that you just created is selected.
7. In the **Format new disk** area, if you want to format the disk, select the **Format this volume as NTFS volume with the following settings** check box, and then do the following:
   a. In the **Partition style** list, click **MBR** (Master Boot Record) or **GPT** (GUID Partition Table).
   b. In the **Volume label** box, enter a volume label, for example **Finance Data**.
   c. In the **Allocation unit size** list, either accept the default, or click a specific allocation unit size. (Note that the values 512, 1024, 2048, 4096 and 8192 are in bytes.)
   d. Select or clear the **Quick format** check box. By default, the check box is selected. To prevent data loss, quick format formats the disk only if the disk is unformatted.
   e. If desired, select the **Force format even if a file system is found** check box. By default, the check box is clear.

      Warning
      If you select this option, any existing data on the volume will be overwritten.
8. In the **Mount point** area, select one of the following options:
   - **Assign the following drive letter** (the default). If you select this option, click the desired drive letter.
   - **Mount in the following empty NTFS folder**. If you select this option, click **Browse**, and then select the empty destination folder.
   - **Do not assign a drive letter or drive path**
9. When you are finished, click **OK**.

   VMM registers the storage logical unit to the host and mounts the storage disk. To view the associated job information, open the **Jobs** workspace.

10. To verify that the logical unit was assigned, view the information on the **Storage** tab in the *Host Name* **Properties** dialog box. The newly assigned logical unit appears under **Disk**. Click the new disk to view the disk details.

    Tip

    If the **Array** field is populated in the disk details, this indicates that the storage array is under VMM management.

11. To perform further configuration of the disk, open Disk Management on the host. (To open Disk Management, click **Start**, type **diskmgmt.msc** in the search box, and then press ENTER.)

    The new disk appears in the list of disks as a basic disk. If you chose to format the disk, the disk is already formatted and online. You can right-click the disk to see the available options, such as **Format** and **Change Drive Letter and Paths**.

To assign an existing logical unit to a host

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then click **All Hosts**.
3. In the **Hosts** pane, right-click the host that you want to configure, and then click **Properties**.
4. In the *Host Name* **Properties** dialog box, click the **Storage** tab.
5. To assign an existing logical unit to the host, on the toolbar, next to **Disk**, click **Add**.
6. In the **Logical unit** list, click the logical unit that you want to assign to the host.
7. Configure the format and mount point options, and then click **OK** to assign the logical unit to the host. For more information about these options and how to verify that the logical unit was assigned, see steps 7 through 12 of the “To create a logical unit and assign it to a host” procedure in this topic.

    Note

    If the logical unit has existing data, and you do not use the **Force Format** option, the VMM job to assign the logical unit will complete with a warning. VMM assigns the logical unit to the host. You can format the disk later.

To remove a logical unit from a host

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then click **All Hosts**.
3. In the **Hosts** pane, right-click the host that you want to configure, and then click **Properties**.
4. In the *Host Name* **Properties** dialog box, click the **Storage** tab.
5. Under **Disk**, click the logical unit that you want to remove, and then on the toolbar, click **Remove**.

    Note

For the Remove button to be enabled, the logical unit must be under VMM management.

6. Review the warning message, and then click **Yes** to remove the logical unit.

   Note
   When you remove a logical unit, the volume and any data on the logical unit are not modified.

7. Click **OK** to commit the changes.

   VMM unregisters the logical unit from the host. To view the associated job information, open the **Jobs** workspace.

To create an iSCSI session on a host

1. On the target host, in the Services snap-in, make sure that the Microsoft iSCSI Initiator Service is started and set to Automatic.
2. In the VMM console, open the **Fabric** workspace.
3. In the **Fabric** pane, expand **Servers**, and then click **All Hosts**.
4. In the **Hosts** pane, right-click the host that you want to configure, and then click **Properties**.
5. In the *Host Name* **Properties** dialog box, click the **Storage** tab.
6. Under **iSCSI Arrays**, see if the storage array is already listed. If it is not, on the toolbar, next to **iSCSI Array**, click **Add**.

   The Create New iSCSI Session dialog box opens.
7. In the **Array** list, click the desired iSCSI storage array.
8. To create an iSCSI session with the default settings, click **Create**.

   To create an iSCSI session with customized settings, select the **Use advanced settings** check box, and then do the following:

   a. In the **Target portal** list, click the IP address and port number for the connection to the storage array.
   b. In the **Target name** list, click the iSCSI Qualified Name (IQN) of the storage array.
   c. In the **Initiator IP** list, click the IP address of the network card on the host that you want to use. The associated logical networks are also listed.
   d. When you are finished, click **Create**.

   The array that you added appears under **iSCSI Arrays**. Click the array to view more details.
9. To create additional iSCSI sessions to the array, click **Create session**. In the **Create New iSCSI Session** dialog box, do either of the following:

   a. Click **Create** to have VMM automatically determine the connection information. VMM creates the iSCSI session by matching the host initiator IP address subnets with the iSCSI target portal IP subnets.
   b. Click **Use advanced settings** to manually select the target portal, target name and

the initiator IP address, and then click **Create**.

See Also

Configuring Storage in VMM

How to Configure Network Settings on a Hyper-V Host in VMM

After you design and configure logical networks for your environment, for example, a “Backend,” “Frontend,” and “Backup” network, you must take at least one more step before anyone can use those logical networks for connecting to or from virtual machines. That step is to assign the logical networks to physical network adapters on one or more hosts. This topic describes one way to take that step in Virtual Machine Manager (VMM), but there’s another topic that describes a different way, as outlined in the following table:

If you have...	And you want to...	Follow steps in...
System Center 2012	Assign logical networks to a physical network adapter	This topic
System Center 2012 Service Pack 1 (SP1) or System Center 2012 R2	Assign logical networks manually to each physical network adapter	This topic
System Center 2012 SP1 or System Center 2012 R2	Assign the same logical networks and other network settings consistently to multiple physical network adapters across multiple hosts	How to Configure Network Settings on a Host by Applying a Logical Switch in VMM

Do the tasks in this topic in this order:

1. Assign logical networks to a physical network adapter on a host
2. Configure settings for external, internal, and private virtual networks

Assign logical networks to a physical network adapter on a host

This procedure describes how to open host properties and configure a network adapter with the **Logical network connectivity** setting.

To assign logical networks to a physical network adapter on a host

1. Make sure that you have already created the logical networks that you want to assign to one or more physical network adapters. Also make sure that the network sites within your logical networks are configured to use the host group of the host you want to assign them to. Both of these steps are described in How to Create a Logical Network in VMM.
2. In the VMM console, open the **Fabric** workspace.
3. In the **Fabric** pane, expand **Servers**, expand **All Hosts**, and then locate and click the host group that contains the host.
4. In the **Hosts** pane, click the host that you want to configure.

5. On the **Host** tab, in the **Properties** group, click **Properties**.
6. In the *Host Name* **Properties** dialog box, click the **Hardware** tab.
7. Under **Network Adapters**, click the physical network adapter that you want to configure. If you want to use this network adapter for virtual machines, ensure that **Available for placement** is checked. If you want to use this network adapter for communication between the host and the VMM management server, ensure that **Used by management** is checked.

   Important
   You must make sure that you have at least one network adapter available for communication between the host and the VMM management server. Make sure that **Used by management** is checked for this network adapter.
8. View or click **Logical network connectivity**:

With System Center 2012	View **Logical network connectivity** in the pane on the right.
With System Center 2012 SP1 or System Center 2012 R2	Under the physical network adapter, click **Logical network connectivity**. Notice the various kinds of information displayed, such as the list of IP subnets and VLANs that are available. With System Center 2012 R2, if you've added a top-of-rack (TOR) switch as a network service, port information that is provided by the switch might also be displayed.

9. Review the list of logical networks, and take note of the following:
   - You might have to look fairly carefully at the entries in the list, because some of them might not actually be available for this host. The list is not limited to the logical networks with network sites that include the host group of this host. Instead, the list includes all the logical networks.
   - You might see some logical networks that appear to have been created automatically—this means that you added a host to VMM and the host didn't already have logical networks assigned to its network adapters. However, automatic creation of logical networks depends on your global settings, as described in How to Configure Global Network Settings in VMM.
10. Check the box next to each logical network that you want to assign to the physical adapter. For example, if you configured the BACKEND logical network in the Preparing the Fabric in VMM section, and the BACKEND logical network is available to the host group of your host, check the box next to **BACKEND**.
11. If you're running System Center 2012, to configure advanced settings, click **Advanced**, and view or modify the following:
    - The mode. Make sure you use the same mode that's used by the physical switch port

that the network adapter is connected to:

Trunk mode	In trunk mode, the different virtual machines that use the network adapter can use different VLAN IDs. Make sure that trunk mode is configured consistently across your hardware and software, including: • The port on the physical switch that the physical network adapter on the host is connected to • The port of the virtual switch When you configure trunk mode in VMM, either specify the VLAN IDs that the different virtual machines are using, or specify that you want to allow all VLAN IDs to be used.
Access mode	Use access mode when the physical network adapter is connected to a switch port that is also in access mode. Make sure the virtual machines that use the network adapter all use the same VLAN ID (the VLAN ID expected by the switch port).

- The IP subnets and VLANs that are available for a given logical network on the network adapter. By default, for a selected logical network, the IP subnets and VLANs assigned to the network adapter are the ones that are configured to use that host group or are inherited through the parent host group.

  To select the available IP subnets and VLANs, click a logical network in the **Logical network** list. Then, use the **Add** and **Remove** buttons to configure which IP subnets and VLANs are assigned to the adapter.

  Note
  If no IP subnets or VLANs appear in the **Available** or **Assigned** columns, this tells you that for the selected logical network, there is no network site that is configured to use the host group or inherited by the host group. For more information about network sites, see Configuring Logical Networking in VMM Overview and How to Create a Logical Network in VMM.

  In the **Logical network** list, if the **Unassigned** option is available, you can view any VLANs that the physical network adapter is connected to, but are not included in a network site. You can either remove these VLANs from the network adapter, or you

can include them in a network site.

Configure settings for external, internal, and private virtual networks

Use the following procedure to control the types of connectivity available to virtual machines by using **External**, **Internal**, or **Private** settings (more details about these settings are in the procedure). Also use this procedure to configure host access through VLANs. You configure these settings through a host property that in System Center 2012 is called a virtual network and in System Center 2012 SP1 and System Center 2012 R2 is called a virtual switch.

To configure settings for external, internal, and private virtual networks

1. If you plan to apply the External setting, make sure you've done the steps in Assign logical networks to a physical network adapter on a host, earlier in this topic.
2. In the VMM console, open the **Fabric** workspace.
3. In the **Fabric** pane, expand **Servers**, expand **All Hosts**, and then locate and click the host group that contains the host.
4. In the **Hosts** pane, click the host that you want to configure.
5. On the **Host** tab, in the **Properties** group, click **Properties**.
6. In the *Host Name* **Properties** dialog box, do the following:

With System Center 2012	Click the **Virtual Networks** tab. Then, under **Virtual Networking**, click the virtual network that you want to configure, or click **Add** to add a new virtual network.
With System Center 2012 SP1 or System Center 2012 R2	Click the **Virtual Switches** tab. Then click an existing virtual switch, or click **New Virtual Switch** and then click **New Standard Switch**. If you do not want to apply each setting individually (that is, you do not want to use a standard switch), and you instead want to apply a logical switch to the network adapter, see the procedures in How to Configure Network Settings on a Host by Applying a Logical Switch in VMM.

7. In the **Name** box, enter a name, or accept the default.
8. In the **Network binding** list, click the network type. You can configure the following types:

External	Allows virtual machines to communicate with each other and with externally located

	servers, and optionally with the host operating system. You might use this setting to allow virtual machines to access a perimeter network and not expose the host operating system. An **External** network is bound to a physical network adapter.
Internal	Allows communication between virtual machines on the same host and between the virtual machines and the host. This setting is often used to build a test environment where virtual machines are connected to the host operating system, but not connected to external networks. An **Internal** network is not bound to a physical network adapter.
Private	Allows communication between virtual machines on the same host but not with the host or with external networks. This setting is often used to isolate virtual machines from network traffic in the host operating system and in the external networks. A **Private** network does not have a virtual network adapter in the host operating system, and is not bound to a physical network adapter.

9. If you click **External**, do the following:
   a. In the **Network adapter** list, click the physical network adapter that you want to associate with the external virtual switch (or external virtual network, as it is called in System Center 2012).
   b. Review the **Logical network** field, which tells you which logical networks are assigned to the network adapter. To assign logical networks to a physical network adapter, see Assign logical networks to a physical network adapter on a host, earlier in this topic.
   c. If you're running System Center 2012 SP1 or System Center 2012 R2, skip this step. Otherwise, to enable the host to use the virtual network to communicate with virtual machines and also with the external network, check **Host access**.

      Warning
      If you clear the **Host access** check box for the physical network adapter that is used for management, you may lose connectivity to the host.

d. To access the host through a VLAN, check **Access host through a VLAN** (if available), and then select a VLAN number. The list that you see shows the VLANs that are included in the logical network and are assigned to the network adapter.

Warning
If you specify a VLAN for a single network connection to the host, network connectivity may be lost and you may lose the ability to manage the host. We recommend that you always use at least two physical network adapters on a host: one network adapter dedicated to remote management and communication between the host and the VMM server, and one or more network adapters dedicated to the external virtual networks that are used by virtual machines.

The following tips may also be useful:

Tip
Network optimizations: VMM can detect whether the operating system on your host provides the network optimizations called Virtual Machine Queue (VMQ) or TCP Chimney Offload. If VMM detects either of them, it displays a message saying **Network optimization is available**. Look for the message in the **Host Properties** dialog box, on the **Virtual Networks** tab (in System Center 2012) or the **Virtual Switches** tab (in System Center 2012 SP1 or System Center 2012 R2).

For more information, see Using TCP Chimney Offload and Using Virtual Machine Queue. For information about these network optimizations in the context of VMM, see the "Network Optimization Support" section in Configuring Virtual Networks in VMM (which describes the optimizations in an earlier version of VMM).

Tip
Compliance of network settings: You can use VMM to check on "compliance," that is, whether the settings you configured on the host by using VMM are as expected, or whether they've been changed through some other interface. For example, you can see whether all the IP subnets and VLANs that are included in a network site in a logical network are assigned to a network adapter. For more information, see How to View Compliance Information for a Physical Network Adapter on a Host in VMM. If you have System Center 2012 SP1 or System Center 2012 R2, you might also want to see How to View Host Network Adapter Settings and Increase Compliance with Logical Switch Settings in VMM.

See Also

Configuring Networking in VMM

Configuring Hyper-V Host Properties in VMM

How to Configure Network Settings on a Host by Applying a Logical Switch in VMM

How to View Compliance Information for a Physical Network Adapter on a Host in VMM

How to Configure Host BMC Settings in VMM

You can use the following procedure to configure Baseboard Management Controller (BMC) settings for a managed host in System Center 2012 – Virtual Machine Manager (VMM). If a computer is configured for out-of-band management through a BMC, you can power the host on and off by using the VMM console. The BMC settings are also used for power optimization.

Note
For more information about power optimization, see Configuring Dynamic Optimization and Power Optimization in VMM.

Prerequisites

To complete this procedure, the host must have a BMC installed that supports one of the following out-of-band management protocols:

- Intelligent Platform Management Interface (IPMI) versions 1.5 or 2.0
- Data Center Management Interface (DCMI) version 1.0
- System Management Architecture for Server Hardware (SMASH) version 1.0 over WS-Management (WS-Man)

Although it is not a required prerequisite, you can create a Run As account before you begin this procedure. (You can also create the account during the procedure.) The Run As account must have permissions to access the BMC.

For example, create a Run As account that is named **BMC Administrator**.

Note
You can create Run As accounts in the **Settings** workspace. For more information about Run As accounts, see How to Create a Run As Account in VMM.

To configure BMC settings

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then click **All Hosts**.
3. In the **Hosts** pane, click the host that you want to configure.
4. On the **Host** tab, in the **Properties** group, click **Properties**.
5. In the *Host Name* **Properties** dialog box, click the **Hardware** tab.
6. Under **Advanced**, click **BMC Setting**.
7. To enable out-of-band management, do the following:
   a. Select the **This physical machine is configured for OOB management with the following settings** check box.
   b. In the **This computer supports the specified OOB power management configuration provider** list, click the out-of-band management protocol that the BMC supports.
   c. In the **BMC address** box, enter the IP address of the BMC.
   d. In the **BMC port** box, accept the default. VMM automatically populates the box with the port number for the selected out-of-band management protocol.
   e. Next to the **Run As account** box, click **Browse**, click a Run As account that has

permissions to access the BMC, and then click **OK**.

Note

If you do not already have a Run As account, click **Browse**, and then in the **Select a Run As Account** dialog box, click **Create Run As Account**.

For example, if you created the Run As account that is described in the Prerequisites section of this topic, click **BMC Administrator**.

f. When you are finished, click **OK**.

To power a computer on or off through VMM

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then click **All Hosts**.
3. In the **Hosts** pane, click the host that you want to configure.
4. On the **Host** tab, in the **Host** group, click **Power On** or **Power Off**. (Additional options that are available with out-of-band power management include **Shutdown** and **Reset**.)

Note

- If BMC settings are not configured, these settings will not be available.
- Information about power on and power off events is available in the BMC logs. To view BMC log information for a host, open the host properties, click the **Hardware** tab, and then under **Advanced**, click **BMC Logs**.
- On HP computers, after the System Even Log is full, logging of new events stop and BMC logs display older events only.

How to Configure Network Settings on a Host by Applying a Logical Switch in VMM

You can use the procedures in this topic to configure network adapters on Hyper-V hosts in System Center 2012 Service Pack 1 (SP1) or System Center 2012 R2, by applying a logical switch and port profiles to the adapters. Before you use the procedures, you must configure the logical switch and port profiles that you will apply. The network adapters that you configure can be physical network adapters or virtual network adapters on the hosts.

This topic describes one way of configuring network adapters on hosts, but there are other topics that describe different ways, as outlined in the following table:

If you have...	And you want to...	Follow steps in...
System Center 2012 SP1 or System Center 2012 R2	Assign the same logical networks and other network settings consistently to multiple network adapters across multiple hosts by using the VMM console	This topic

If you have...	And you want to...	Follow steps in...
System Center 2012 SP1 or System Center 2012 R2	Assign the same logical networks and other network settings consistently to multiple network adapters during bare-metal provisioning of hosts by using Windows PowerShell	Bare Metal Deploy through VMM PowerShell (Part 1) Bare Metal Deploy through VMM PowerShell (Part 2) Hyper-V Host Network Settings through VMM PowerShell (Part 3) For background, see End-to-End Bare-Metal Provisioning with SCVMM 2012 SP1/R2
System Center 2012	Assign logical networks to a physical network adapter	How to Configure Network Settings on a Hyper-V Host in VMM
System Center 2012 SP1 or System Center 2012 R2	Assign logical networks manually to each physical network adapter	How to Configure Network Settings on a Hyper-V Host in VMM

Do the tasks in this topic in this order:

1. Specify whether a network adapter is used for virtual machines, host management, neither, or both
2. Configure network settings on a host by applying a logical switch

After you perform the procedures in this topic, as a best practice, review the procedures in How to View Host Network Adapter Settings and Increase Compliance with Logical Switch Settings in VMM.

Specify whether a network adapter is used for virtual machines, host management, neither, or both

Regardless of any port profiles and logical switches you are using in your network configuration, you must specify whether a network adapter in a host is used for virtual machines, host management, neither, or both. (The host must already be under management in VMM.)

To specify whether a network adapter is used for virtual machines, host management, neither, or both

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, expand **All Hosts**, and then locate and click the host group where the host resides.
3. In the **Hosts** pane, click the host that you want to configure.
4. On the **Host** tab, in the **Properties** group, click **Properties**.
5. In the *Host Name* **Properties** dialog box, click the **Hardware** tab.
6. Under **Network adapters**, click the physical network adapter that you want to configure.

If you want to use this network adapter for virtual machines, ensure that **Available for placement** is checked. If you want to use this network adapter for communication between the host and the VMM management server, ensure that **Used by management** is checked.

Important

- You must make sure that you have at least one network adapter available for communication between the host and the VMM management server. Make sure that **Used by management** is checked for this network adapter.
- If you have already applied a logical switch and an uplink port profile to a network adapter, if you click **Logical network connectivity**, you can see the resulting connectivity. However, if you plan to apply a logical switch and an uplink port profile, do not make individual selections in **Logical network connectivity**. Instead, use the following procedure.

Configure network settings on a host by applying a logical switch

Before you begin the following procedure, make sure you have configured the building blocks that are needed in the procedure, including logical networks, port profiles, and logical switches. For more information, see Configuring Ports and Switches for VM Networks in VMM. If you want to configure single-root I/O virtualization (SR-IOV) for network adapters on the host, it's especially important to review the "Settings" section in that topic, because SR-IOV has specific requirements.

To configure network settings on a host by applying a logical switch

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, expand **All Hosts**, and then locate and click the host group that contains the host.
3. In the **Hosts** pane, click the host that you want to configure.
4. On the **Host** tab, in the **Properties** group, click **Properties**.
5. In the *Host Name* **Properties** dialog box, click the **Virtual Switches** tab.
6. On the **Virtual Switches** tab, do the following:
   a. Select an existing logical switch from the list, or click **New Virtual Switch** and then click **New Logical Switch**.
   b. In the **Logical switch** list, select the logical switch that you want to use.
   c. Under **Adapter**, select the physical adapter that you want to apply the logical switch to.
   d. In the **Uplink Port Profile** list, select the uplink port profile that you want to apply. The list contains the uplink port profiles that have been added to the logical switch that you selected. If a profile seems to be missing, review the configuration of the logical switch and then return to this property tab.
   e. As needed, repeat the steps for applying a new logical switch.

      Important

If you apply the same logical switch and uplink port profile to two or more adapters, the two adapters might be teamed, depending on a setting in the logical switch. To find out if they will be teamed, open the logical switch properties, click the **Uplink** tab, and view the **Uplink mode** setting. If the setting is **Team**, the adapters will be teamed. The specific mode in which they will be teamed is determined by a setting in the uplink port profile.

f. When you have finished configuring settings, click **OK**.

Caution
While VMM creates the virtual switch, the host may temporarily lose network connectivity. This may have an adverse effect on other network operations in progress.

The following tips may also be useful:

Tip
Network optimizations: VMM can detect whether the operating system on your host provides the network optimizations called Virtual Machine Queue (VMQ) or TCP Chimney Offload. If VMM detects either of them, it displays a message saying **Network optimization is available**. Look for the message in the **Host Properties** dialog box, on the **Virtual Switches** tab.

For more information, see Using TCP Chimney Offload and Using Virtual Machine Queue. For information about these network optimizations in the context of VMM, see the “Network Optimization Support” section in Configuring Virtual Networks in VMM (which describes the optimizations in an earlier version of VMM).

Tip
Compliance of network settings: After you apply logical switches, you can later check to see if the network adapter settings on a host are still in compliance with the logical switch settings. If they’re not, you can use VMM to bring them back into compliance. For more information, see How to View Host Network Adapter Settings and Increase Compliance with Logical Switch Settings in VMM.

See Also

Configuring Ports and Switches for VM Networks in VMM

Configuring Ports and Switches in VMM Illustrated Overview

Configuring Networking in VMM

Adding Hyper-V Hosts and Host Clusters, and Scale-Out File Servers to VMM

Managing VMware ESX and Citrix XenServer in VMM

How to Configure Network Settings on a Hyper-V Host in VMM

How to Add a Top-of-Rack Switch in VMM in System Center 2012 R2

How to Configure Global Network Settings in VMM

How to Add a Top-of-Rack Switch in VMM in System Center 2012 R2

With System Center 2012 R2, you can add a top-of-rack (TOR) switch as a resource in Virtual Machine Manager (VMM). This helps you keep the settings in the TOR switch synchronized with the settings that you see in VMM.

To do this, you must first ensure that you have the necessary provider software on the VMM management server. If your switch is based on the Common Information Model (CIM) network switch profile, you can use the provider that is included in VMM in System Center 2012 R2. Otherwise, you must obtain the provider software that is provided by the switch vendor and install it on the VMM management server. Then you can add the TOR switch to VMM.

Important
This topic describes how you can add a TOR switch to the list of resources in VMM in System Center 2012 R2 only. For information about how to add a virtual switch extension manager to the list of resources in VMM in System Center 2012 SP1, see How to Add a Virtual Switch Extension Manager in System Center 2012 SP1.

Prerequisites

If you want to add a TOR switch to your configuration in VMM, you must first perform the following actions:

1. Ensure that you have the necessary provider software on the VMM management server. If your switch is based on the Common Information Model (CIM) network switch profile, you can use the provider that is included in VMM in System Center 2012 R2. Otherwise, you must obtain the provider software that is provided by the switch vendor and install it on the VMM management server. After you install the provider software, restart the System Center Virtual Machine Manager service.

   If you have installed a high availability VMM management server on a cluster, ensure that the provider is installed on all nodes of the cluster.

   For more information about installing provider software, refer to the manufacturer's documentation.
2. For your TOR switch, make sure that you know the manufacturer and model, the name of an account that has configuration permissions, the connection string, and the host groups to include. If certificates are used for the provider software, make sure you know how to view the thumbprint information for those certificates.

To add a top-of-rack switch in System Center 2012 R2

1. If you installed provider software as part of fulfilling the "Prerequisites" that are listed before this procedure, confirm that the provider is listed in VMM. To do this, open the **Settings** workspace, and in the **Settings** pane, click **Configuration Providers**. In the **Configuration Providers** pane, review the list of installed provider software.

2. Open the **Fabric** workspace.
3. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
4. In the **Fabric** pane, expand **Networking**, and then click **Network Service**.

   Network services include gateways, virtual switch extensions, network managers, and TOR switches.
5. On the **Home** tab, in the **Add** group, click **Add Resources**, and then click **Network Service**.

   The **Add Network Service Wizard** opens.
6. On the **Name** page, enter a name and optional description, and then click **Next**.
7. On the **Manufacturer and Model** page, make selections as follows:
   - To use the provider software that is included in VMM, in the **Manufacturer** list, click **Microsoft**, and in the **Model** list, click **Microsoft Network Switch Profile Switch**.
   - To use provider software that is provided by the switch vendor, click the appropriate **Manufacturer** and **Model** for your switch.

   Then click **Next**.
8. On the **Credentials** page, either click **Browse** and then on the **Select a Run As Account** dialog box, select an account, or click **Create Run As Account** and create a new account. Then click **Next**.
9. On the **Connection String** page, in the **Connection string** box, type the connection string that is used by the TOR switch, and then click **Next**.

   For example, you might enter the following connection string:

   https://TORswitch1.contoso.com:5986

   Important
   If you are not using the provider software that is included in VMM, when you enter the connection string, use the syntax that is defined by the manufacturer of your TOR switch. For more information about the required syntax, refer to the manufacturer's documentation.
10. On the **Certificates** page, if certificates are listed, verify that the thumbprints of those certificates match the thumbprints of the certificates that are installed on the TOR switch. Then select the box to confirm that the certificates can be imported to the trusted certificate store. Click **Next**.

    Note
    If no certificates are listed, the connection string that was provided probably does not require a certificate, and you can continue to the next page of the wizard. However, if no certificates are listed but your TOR switch requires them, confirm that the certificates were installed correctly on your device.
11. On the **Provider** page, in the **Configuration provider** list, select an available provider, and then click **Test** to run basic validation against the TOR switch by using the selected provider. If tests indicate that the provider software works as expected, click **Next**.
12. On the **Host Group** page, select one or more host groups to which the TOR switch will

be available.

13. On the **Summary** page, review and confirm the settings, and then click **Finish**.

See Also

Configuring Hyper-V Host Properties in VMM

How to Add a Virtual Switch Extension or Network Manager in System Center 2012 R2

Configuring Networking in VMM

How to Add an IPAM Server in VMM in System Center 2012 R2

How to Add a Virtual Switch Extension Manager in System Center 2012 SP1

How to View Compliance Information for a Physical Network Adapter on a Host in VMM

Compliance information lets you see whether the settings on physical network adapters on a host are consistent with the configuration in Virtual Machine Manager (VMM). For example, you can see whether all the IP subnets and VLANs that are included in a network site in a logical network are assigned to a physical network adapter.

If you have System Center 2012 Service Pack 1 (SP1) or System Center 2012 R2 and you want more detail about compliance information for logical switches, see How to View Host Network Adapter Settings and Increase Compliance with Logical Switch Settings in VMM instead.

To view compliance information for a physical network adapter

1. In the VMM console, open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Networking**, and then click **Logical Networks**.
3. On the **Home** tab, in the **Show** group, click **Hosts**.
4. In the **Logical Network Information for Hosts** pane, expand the host, and then click a physical network adapter.
5. In the **Network Compliance** column, view the compliance.

Fully compliant	All IP subnets and VLANs that are included in the network site are assigned to the network adapter.
Partially compliant	If you compare the IP subnets and VLANs that are included in the network site with those that are assigned to the network adapter, there is only a partial match. In the details pane, the **Logical network**

	information section lists the assigned IP subnets and VLANs for the physical network adapter. If an adapter is partially compliant, you can view the reason in the **Compliance errors** section.
Non compliant	None of the IP subnets and VLANs that are defined for the logical network are assigned to the physical network adapter.

Tip
In addition to the compliance information, you can also view detailed information about the physical network adapter, such as the assigned IP address and MAC address, and the associated virtual networks.

See Also

Configuring Logical Networking in VMM Overview

How to Configure Network Settings on a Hyper-V Host in VMM

How to Configure Network Settings on a Host by Applying a Logical Switch in VMM

How to Create a Logical Network in VMM

How to View Host Network Adapter Settings and Increase Compliance with Logical Switch Settings in VMM

Creating and Modifying Hyper-V Host Clusters in VMM

This section explains how to create, add, or remove nodes, and how to uncluster Hyper-V host clusters in Virtual Machine Manager (VMM). If you manage clustered Hyper-V hosts through VMM, you can support highly available virtual machines, along with features such as dynamic optimization and power optimization.

As of System Center 2012, VMM provides several new improvements that simplify the creation and management of Hyper-V host clusters. These improvements include the following:

- A new Create Cluster Wizard that you can use to cluster managed Hyper-V hosts that are in a trusted domain by using the VMM console.

  Note
  In VMM 2008 R2, you had to create the cluster outside VMM, and then bring it under VMM management. Be aware that this functionality is still supported. For more

information, see the topics How to Add Trusted Hyper-V Hosts and Host Clusters in VMM and How to Add Untrusted Hyper-V Hosts and Host Clusters in VMM.

- The ability to add nodes to, or remove nodes from, a Hyper-V host cluster through the VMM console.
- The ability to uncluster a Hyper-V host cluster into stand-alone hosts from the VMM console.

Note
You cannot create a Windows Server 2012 R2 Hyper-V cluster by using System Center 2012 R2 Virtual Machine Manager when VMM is installed on Windows Server 2012. In this environment, you must first create the Hyper-V cluster by using Failover Cluster Manager. You can then manage the cluster by using VMM.

In this section

Use the information in the following topics to create or modify a Hyper-V host cluster through VMM.

Topic	Description
Creating a Hyper-V Host Cluster in VMM Overview	Provides an overview of the cluster creation process in VMM. Links to prerequisites and a procedure that shows how to create a Hyper-V host cluster.
Modifying a Hyper-V Host Cluster in VMM	Links to procedures that show how to add a node to a Hyper-V host cluster, how to remove a node, and how to uncluster a Hyper-V host cluster.
Configuring Hyper-V Host Cluster Properties in VMM	Describes the properties of Hyper-V host clusters. Links to more detailed information about how to configure storage for a Hyper-V host cluster.

Creating a Hyper-V Host Cluster in VMM Overview

The procedure in this section describes how to create a Hyper-V host cluster in the VMM console by using the Create Cluster Wizard. Through the wizard, you can select which Hyper-V hosts to cluster, and configure the networking and storage resources that are used during cluster creation.

During the cluster creation process, System Center 2012 – Virtual Machine Manager (VMM) does the following:

- Validates that all hosts meet the prerequisites, such as required operating system and domain membership
- Enables the Failover Clustering feature on each host
- Unmasks the selected storage logical units to each host
- Creates the configured external virtual networks
- Runs the cluster validation process
- Creates the cluster with quorum and enables Cluster Shared Volumes (CSV)
- For each logical unit that is designated as a CSV, assigns the logical unit as a CSV on the cluster

Example Scenario Overview

The example scenario that is used in this section assumes that you have completed the procedures in the Preparing the Fabric in VMM section to configure fabric resources such as host groups, storage, and networking resources. Additionally, you must have completed the procedures in the Adding Hyper-V Hosts and Host Clusters, and Scale-Out File Servers to VMM section to add stand-alone Hyper-V hosts that you want to cluster to VMM management.

The example scenario uses the example resources that are used in the Preparing the Fabric in VMM section, such as the fictitious domain name contoso.com, the same example host group structure, and the BACKEND logical network.

Note
The example resource names and configuration are used to help demonstrate the concepts. You can adapt them to your test environment.

The example scenario walks you through how to create a two-node Hyper-V host cluster from two stand-alone Hyper-V hosts. The following table summarizes the examples that are used in this example scenario.

Resource	Resource Name
Stand-alone Hyper-V hosts	**HyperVHost05** and **HyperVHost06**
Domain	**contoso.com**
Cluster name	**HyperVClus01.contoso.com**
Host group where added	**New York\Tier0_NY**
Logical network	**BACKEND**

In This Section

The topics in this section describe the prerequisites and the procedure to create a Hyper-V host cluster through VMM.

Topic	Description
Creating a Hyper-V Host Cluster in VMM Prerequisites	Describes the host and fabric prerequisites that are required to complete the procedure.
How to Create a Hyper-V Host Cluster in VMM	Describes how to create a Hyper-V host cluster by using the Create Cluster Wizard.

Creating a Hyper-V Host Cluster in VMM Prerequisites

Before you run the Create Cluster Wizard in Virtual Machine Manager (VMM) to create a Hyper-V host cluster, there are several prerequisites that must be met. These include prerequisites for host configuration and for fabric configuration.

Host Prerequisites

Make sure that the hosts that you want to cluster meet the following prerequisites:

- You must have two or more stand-alone Hyper-V hosts that are managed by VMM. For more information, see How to Add Trusted Hyper-V Hosts and Host Clusters in VMM.
- The Hyper-V hosts must meet the requirements for failover clustering and must be running a supported operating system.

  For more information, see the followings:

  - About supported operating systems, see as follows:
    - For System Center 2012 – Virtual Machine Manager or for System Center 2012 SP1 see: **System Requirements: Hyper-V Hosts in System Center 2012 and in System Center 2012 SP1**.
    - For System Center 2012 R2 Virtual Machine Manager see: **Preparing your environment for System Center 2012 R2 Virtual Machine Manager**.
  - About hardware requirements for Windows Server 2008 R2, see Understanding Requirements for Failover Clusters.
  - About hardware requirements for Windows Server 2012, see Failover Clustering Hardware Requirements and Storage Options.

  Important
  If the cluster will have three or more nodes, and the nodes are running Windows Server 2008 R2 with SP1, you must install the hotfix that is described in the article Validate SCSI Device Vital Product Data (VPD) test fails after you install Windows Server 2008 R2 SP1. Install the hotfix on each node before you run the Create Cluster Wizard. Otherwise, cluster validation may fail.

- The Hyper-V hosts that you want to add as cluster nodes must be located in the same Active Directory domain. The domain must be trusted by the domain of the VMM management server.
- The Hyper-V hosts must belong to the same host group in VMM.

Fabric Prerequisites

Make sure that fabric configuration meets the following prerequisites:

- To use shared storage that is under VMM management, storage must already be discovered and classified in the Fabric workspace of the VMM console. Additionally, logical units that you want to use as available or shared storage must be created and allocated to the host group or parent host group where the Hyper-V hosts are located. The logical units must not be assigned to any host.

  Note

  For information about how to discover, classify and allocate storage, and the specific hardware and storage provider requirements, see the Configuring Storage in VMM section.

- To use shared storage that is not under VMM management, disks must be available to all nodes in the cluster before you can add them. Therefore, you must provision one or more logical units to all hosts that you want to cluster, and mount and format the storage disks on one of the hosts.

  Important

  VMM is agnostic regarding the use of asymmetric storage, where a workload can use disks that are shared between a subset of the cluster nodes. VMM does not support or block this storage configuration. Note that to work correctly with VMM, each cluster node must be a possible owner of the cluster disk. (Support for asymmetric storage was introduced in Windows Server 2008 R2 Service Pack 1.)

- Each host that you want to cluster must have access to the storage array.
  - The Multipath I/O (MPIO) feature must be added on each host that will access the Fibre Channel or iSCSI storage array. You can add the MPIO feature through Server Manager. If the MPIO feature is already enabled before you add a host to VMM management, VMM will automatically enable MPIO for supported storage arrays by using the Microsoft provided Device Specific Module (DSM). If you already installed vendor-specific DSMs for supported storage arrays, and then add the host to VMM management, the vendor-specific MPIO settings will be used to communicate with those arrays.

    If you add a host to VMM management before you add the MPIO feature, you must add the MPIO feature, and then manually configure MPIO to add the discovered device hardware IDs. Or, you can install vendor-specific DSMs.
  - If you are using a Fibre Channel storage array network (SAN), each host must have a host bus adapter (HBA) installed, and zoning must be correctly configured. For more information, see your storage array vendor's documentation.

- If you are using an iSCSI SAN, make sure that iSCSI portals have been added and that the iSCSI initiator is logged into the array. Additionally, make sure that the Microsoft iSCSI Initiator Service on each host is started and set to Automatic. For more information about how to create an iSCSI session on a host when storage is managed through VMM, see How to Configure Storage on a Hyper-V Host in VMM.

  Important

  By default, when VMM manages the assignment of logical units, VMM creates one storage group per host. In a cluster configuration, VMM creates one storage group per cluster node. A storage group can contain one or more of the host's initiator IDs (iSCSI Qualified Name (IQN) or a World Wide Name (WWN)).

  For some storage arrays, it is preferable to use one storage group for the entire cluster, where host initiators for all cluster nodes are contained in a single storage group. To support this configuration, you must set the `CreateStorageGroupsPerCluster` property to `$true` by using the `Set-SCStorageArray` cmdlet in the VMM command shell.

  In VMM, a storage group is defined as an object that binds together host initiators, target ports and logical units. A storage group has one or more host initiators, one or more target ports and one or more logical units. Logical units are exposed to the host initiators through the target ports.

- For all Hyper-V hosts that you want to cluster, if the hosts are configured to use static IP addresses, make sure that the IP addresses on all hosts are in the same subnet.
- One or more logical networks that are common across all of the Hyper-V hosts that you want to cluster must be configured in the Fabric workspace of the VMM console. If a logical network has associated network sites, a network site must be scoped to the host group where the host cluster will reside. Additionally, the logical networks must be associated with physical network adapters on each Hyper-V host.

  You do not have to create external virtual networks on the Hyper-V hosts beforehand. When you run the Create Cluster Wizard, you can configure the external virtual networks that VMM will automatically create on all cluster nodes. You can also configure virtual network settings for the cluster after cluster creation. For more information, see Configuring Hyper-V Host Cluster Properties in VMM.

  - For information about how to create logical networks, see How to Create a Logical Network in VMM.
  - For information about how to assign logical networks to physical network adapters, see How to Configure Network Settings on a Hyper-V Host in VMM.

  Important

  If the external virtual networks that you want to use for the cluster are already defined on each host, make sure that the names of the virtual networks are identical, and that the logical networks that are associated with each physical network adapters are identical. Otherwise, the virtual network will not be considered highly available by VMM.

See Also

Creating and Modifying Hyper-V Host Clusters in VMM

How to Create a Hyper-V Host Cluster in VMM

How to Create a Hyper-V Host Cluster in VMM

You can use the following procedure to create a Hyper-V host cluster from the VMM console in System Center 2012 – Virtual Machine Manager (VMM).

Important

Before you begin this procedure, make sure that your configuration meets the prerequisites that are described in the Creating a Hyper-V Host Cluster in VMM Prerequisites topic.

To create a Hyper-V host cluster through VMM

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, click **Servers**.
3. On the **Home** tab, in the **Create** group, click **Create**, and then click **Hyper-V Cluster**.

   The Create Cluster Wizard opens.
4. On the **General** tab, do the following, and then click **Next**:
   a. In the **Cluster name** box, enter the name of the cluster.

      For example, enter the cluster name **HyperVClus01.contoso.com**.

   b. Enter the credentials that will be used to create the cluster. You can specify a Run As account or manually enter user credentials in the format *domain_name\user_name*.

      Note

      To create a Run As account, next to the **Use an existing Run As account** box, click **Browse**, and then in the **Select a Run As Account** dialog box, click **Create Run As Account**.

      The account that you use must have administrative permissions on the servers that will become cluster nodes, and must belong to the same domain as the Hyper-V hosts that you want to cluster. Also, the account requires **Create Computer objects** and **Read All Properties** permissions in the container that is used for Computer accounts in the domain. For more information, see the Failover Cluster Step-by-Step Guide: Configuring Accounts in Active Directory.
5. On the **Nodes** page, do the following:
   a. In the **Host group** list, click the host group that contains the Hyper-V hosts that you want to cluster.

For example, click the **New York\Tier0_NY** host group.

Any available Hyper-V hosts that meet the operating system prerequisites from the selected host group appear under **Available hosts**.

b. Under **Available hosts**, click a Hyper-V host that you want to cluster, and then click **Add**. (To select multiple hosts, press and hold the CTRL key, and then click each host. To select a range, click the first host in the range, press and hold the SHIFT key, and then click the last host in the range.)

The hosts that you added move to the **Hosts to cluster** column.

For example, add the hosts **HyperVHost05** and **HyperVHost06**.

c. If desired, select the **Skip cluster validation tests** check box.

Warning
Select this check box only if you do not require support from Microsoft for the host cluster.

d. When you are finished, click **Next**.

6. If at least one host that you selected in the previous step has a physical network adapter that is configured to use a static IPv4 address instead of DHCP, and there is a physical network adapter on all other hosts that is assigned to the same subnet, the **IP Address** page of the wizard appears. VMM detects and lists the associated networks for the discovered static IPv4 addresses.

Note
A static IP address is not required if a physical network adapter on any host is configured to use DHCP for the same subnet. If DHCP is available, you can click **Next** to skip this page of the wizard.

In the **Network** column, select the check box next to each network from which you want to assign a static cluster IP address, and then do the following depending on the selection:

- If there are no static IP address pools that are associated with the subnet, in the **IP Address** column, enter the static IP address that you want to use from the selected network.
- If there are static IP address pools that are associated with the subnet, and you want VMM to automatically assign a static IP address from a pool, in the **Static IP Pool** column, select which IP address pool to use.
- If there are static IP address pools that are associated with the subnet, but you want to specify the IP address to use, in the **Static IP Pool** column, make sure that no IP address pool is selected. Then, in the **IP Address** column, enter an available IP address from the selected network.

Note
The IP address does not have to be part of an available IP address pool range. However, it does have to fall within the subnet range. If you do specify an IP address that falls within a static IP address pool range, VMM

recognizes this and will not assign the same static IP address to another virtual device.

When you are finished, click **Next**.

7. On the **Storage** page, select the check box next to each disk that you want to cluster, and then configure the various options. The list of available disks represents the logical units that are associated with the host group that you selected in step 5. If you assigned storage out-of-band, disks that are not managed by VMM are displayed and selected as available disks, with the check box next to each disk dimmed and unavailable.

   Important
   If you are using a third-party clustered file system (CFS) solution, make sure you are aware which disks are CFS disks. Do not select those disks for the cluster. If you do, cluster creation will fail.

   Note
   If the number of selected hosts for the cluster is even, the smallest disk that is larger than 500 megabytes (MB) is automatically chosen as the witness disk and is unavailable for selection.

   The options include the following.

Classification	The storage classification value is pre-assigned in the VMM console, and is non-editable in the wizard.
Partition Style	Click **MBR** or **GPT**. **Note** This setting is ignored if the disk is already initialized.
File System	Click **NTFS** or **Do not format**. By default, the file system is NTFS.
Volume Label	Enter a volume label.
Quick Format	Select the check box to perform a quick format of the disk. Available only if NTFS is selected. Quick format formats the disk only if the disk is unformatted.
CSV	Select the check box to convert the disk to a Cluster Shared Volume (CSV). Available only if NTFS is selected.

   Note
   The **Force Format** option is available if you right-click the column header, and

then click **Force Format**. Use this setting with caution, as any existing data on the disk will be overwritten during cluster creation.

8. On the **Virtual Networks** page, configure the external virtual networks that VMM will automatically create on all cluster nodes. To do this, follow these steps:
   a. Select the check box next to a logical network. The selected logical network will be automatically associated with the external virtual network that is created on each host.

      Note
      For a logical network to appear in the list, the following conditions must be true:

   - The logical network must be associated with a physical network adapter on each host.
   - The logical networks that are associated with a physical network adapter on each host must be identical. (This includes any associated VLAN IDs.) For example, if you associated a network adapter on one host to the BACKEND logical network, and a network adapter on another host to the BACKEND and the CORP logical networks, the logical networks will not be listed. If both network adapters are associated with only BACKEND, or both network adapters are associated with BACKEND and CORP, the logical networks will be listed.

     Realize that logical networks for external virtual networks that have already been configured on the hosts do not appear in the list.

   b. In the **Name** and **Description** boxes, enter a name and description for the external virtual network.
   c. To allow hosts to access virtual machines through the external virtual network, select the **Allow hosts to access VMs through this virtual network** check box.
   d. To access the hosts through a VLAN, select the **Hosts can access the VLAN ID** check box, and then click the desired VLAN. The list of available VLANs is scoped to the VLANs that are configured as part of the logical network.

   When you are finished, click **Next**.
9. On the **Summary** page, confirm the settings and then click **Finish**.

   The **Jobs** dialog box appears to show the job status. Verify that the job has a status of **Complete**, and then close the dialog box.
10. When the job completes, verify the cluster status. To do this, in the **Fabric** pane, expand **Servers**, expand **All Hosts**, and then locate and click the new host cluster. In the **Hosts** pane, in the **Host Status** column, verify that the host status for each node in the cluster is **OK**.

    Tip
    To view detailed status information for the host cluster, including a link to the cluster validation test report, right-click the host cluster, and then click **Properties**. View the information on the **Status** tab. For more information, see Configuring Hyper-V Host Cluster Properties in VMM.

Also, realize that you can perform an on-demand cluster validation. To do this, click the host cluster. Then, on the **Host Cluster** tab, click **Validate Cluster**. Cluster validation begins immediately.

See Also

Creating a Hyper-V Host Cluster in VMM Overview

Creating a Hyper-V Host Cluster in VMM Prerequisites

Modifying a Hyper-V Host Cluster in VMM

The procedures in this section describe how to add or remove a node in a Hyper-V host cluster that is managed by System Center 2012 – Virtual Machine Manager (VMM), and how to uncluster a managed Hyper-V cluster into stand-alone hosts.

Note
For information about how to add and remove storage that is under VMM management from an existing Hyper-V host cluster, see How to Configure Storage on a Hyper-V Host Cluster in VMM.

In This Section

Use the following procedures to modify a Hyper-V host cluster in VMM.

Procedure	Description
How to Add a Node to a Hyper-V Host Cluster in VMM	Describes how to add a node to an existing Hyper-V host cluster through the VMM console.
How to Remove a Node from a Hyper-V Host Cluster in VMM	Describes how to remove a node from an existing Hyper-V host cluster through the VMM console.
How to Uncluster a Hyper-V Host Cluster in VMM	Describes how to uncluster a Hyper-V host cluster into stand-alone Hyper-V hosts.

How to Add a Node to a Hyper-V Host Cluster in VMM

You can use the following procedure to add one or more nodes to a managed Hyper-V host cluster by using the VMM console in Virtual Machine Manager (VMM).

Note

This procedure shows how to add a managed Hyper-V host to a managed Hyper-V host cluster. If you have added an unmanaged node to a managed Hyper-V cluster out-of-band by using Failover Cluster Manager, then open the **Fabric** workspace, expand **Servers**, expand **All Hosts**, and then locate and expand the host cluster. Right-click the host with a status of **Pending**, and then click **Add to Host Cluster**.

Prerequisites

Before you begin this procedure, make sure that the following prerequisites are met for the Hyper-V host that you want to add as a cluster node:

- The host must already be managed by VMM.
- The host must meet the requirements for failover clustering and must be running a supported operating system:

  For more information, see the followings:

  - About supported operating systems, see as follows:
    - For System Center 2012 – Virtual Machine Manager or for System Center 2012 SP1: **System Requirements: Hyper-V Hosts in System Center 2012 and in System Center 2012 SP1**.
    - For System Center 2012 R2 Virtual Machine Manager: **Preparing your environment for System Center 2012 R2 Virtual Machine Manager**.
  - About hardware requirements for Windows Server 2008 R2, see Understanding Requirements for Failover Clusters.
  - About hardware requirements for Windows Server 2012, see Failover Clustering Hardware Requirements and Storage Options.

  For information about hardware requirements, see Understanding Requirements for Failover Clusters (for Windows Server 2008 R2) or Failover Clustering Hardware Requirements and Storage Options (for Windows Server 2012).

  Important

  If the cluster will have three or more nodes, and the nodes are running Windows Server 2008 R2 with SP1, you must install the hotfix that is described in the article Validate SCSI Device Vital Product Data (VPD) test fails after you install Windows Server 2008 R2 SP1. Install the hotfix on each node before you run the Create Cluster Wizard. Otherwise, cluster validation may fail.
- The host must be located in the same host group as the target host cluster.

- The host must be in the same domain as the target host cluster.
- If the cluster uses static IP addresses, the host must be configured to use static IP addresses with a subnet that matches the other nodes in the cluster.
- Physical network adapters on the host must be configured with logical networks that match the existing cluster virtual networks on the target host cluster. You do not have to create the external virtual network on the host that you want to add. You only have to associate the logical networks for all existing cluster virtual networks with physical network adapters on the host. To view the virtual networks on the target host cluster, right-click the cluster, and then in the *Cluster Name* **Properties** dialog box, click the **Virtual Networks** tab.

  Also, the logical networks that are associated with a network adapter on the host must exactly match what is configured for an existing virtual network on the cluster. (This includes any associated VLAN IDs.) For example, if a virtual network on the cluster is associated with the BACKEND and the CORP logical networks, a physical network adapter on the host must be associated with both the BACKEND and CORP logical networks.

  Note
  For more information, see How to Configure Network Settings on a Hyper-V Host in VMM.
- If the cluster has available or shared volumes with logical units that are managed by VMM, the host that you want to add must have access to the same storage array. Any storage logical units that are not managed by VMM must already be provisioned to the host.

Additionally, the target host cluster must be located in a domain that is trusted by the domain of the VMM management server.

To add a Hyper-V host as a cluster node

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then expand **All Hosts**.
3. Do one of the following:
   - Drag the host that you want to add as a cluster node to the host cluster name. Continue to step 5.
   - Locate and then click the host cluster on which you want to add the node. On the **Host Cluster** tab, in the **Host Cluster** group, click **Add Cluster Node**. Continue to the next step.

     Note
     If you use this method, you can add multiple hosts at one time.
4. In the **Add Host Cluster Nodes** dialog box, do the following:
   a. In the **Available hosts** column, click a host that you want to add as a cluster node, and then click **Add**. (To select multiple hosts, press and hold the CTRL key, and then click each host. To select a range, click the first host in the range, press and hold the SHIFT key, and then click the last host in the range.)
   b. If desired, select the **Skip cluster validation** check box.

Warning
Select this check box only if you do not require support from Microsoft for the host cluster.

c. When you are finished, click **Add** in the lower-right of the dialog box.

5. In the **Enter Credentials** dialog box (or the **Add Node to Cluster** dialog box if you used the drag-and-drop method to add a node), enter the credentials for a user account that has administrative permissions on the host that you want to add, and then click **OK**. You can specify a Run As account, or enter the credentials in the format *domain_name\user_name*.

Note
To create a Run As account, next to the **Use an existing Run As account** box, click **Browse**, and then in the **Select a Run As Account** dialog box, click **Create Run As Account**.

VMM adds the node to the cluster. To view the job status, open the **Jobs** workspace.

Note
As part of the job, VMM automatically registers shared storage for the cluster that is managed through VMM.

6. To verify that the cluster node was added, in the **Fabric** pane, expand **Servers**, expand **All Hosts**, and then locate and click the host cluster.

   In the **Hosts** pane, verify that the new node appears as part of the host cluster, and that the host status is **OK**.

Tip
To view detailed status information for the host cluster, including a link to the cluster validation test report, right-click the host cluster, and then click **Properties**. View the information on the **Status** tab. For more information, see Configuring Hyper-V Host Cluster Properties in VMM.

Also, note that you can perform an on-demand cluster validation. To do this, click the host cluster. Then, on the **Host Cluster** tab, click **Validate Cluster**. Cluster validation begins immediately.

See Also

Creating and Modifying Hyper-V Host Clusters in VMM

How to Remove a Node from a Hyper-V Host Cluster in VMM

You can use the following procedure to remove one or more nodes from a managed Hyper-V host cluster by using the VMM console in Virtual Machine Manager (VMM). After you remove a node from a cluster, that node becomes a stand-alone managed host.

Prerequisites

Before you begin this procedure, make sure that the following prerequisites are met:

- The managed Hyper-V host must be located in a domain that is trusted by the domain of the VMM management server.
- The host cluster that you want to remove the node from must have more than one node.
- The node that you want to remove must be in maintenance mode. To start maintenance mode, in the **Fabric** workspace, expand **Servers**, and then expand **All Hosts**. Locate and then right-click the cluster node that you want to remove, and then click **Start Maintenance Mode**. In the **Start Maintenance Mode** dialog box, click **Move all virtual machines to other hosts in the cluster**, and then click **OK**.

To remove a node from a Hyper-V host cluster

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, expand **All Hosts**, expand the host group where the cluster is located, expand the host cluster, and then click the node that you want to remove.

   Note
   The node that you want to remove must be in maintenance mode. In the **Hosts** pane, verify that the host status is **In Maintenance Mode**.
3. On the **Host** tab, in the **Cluster** group, click **Remove Cluster Node**.
4. When prompted whether you want to remove the node, click **Yes**.

   VMM removes the node from the cluster. Open the **Jobs** workspace to view the job status.
5. To verify that the node was removed, in the VMM console, make sure that it is no longer listed as part of the cluster.

   Note
   As part of the job, any shared storage that is managed through VMM is unregistered from the node that is being removed. If you allocated storage to the cluster that is not managed by VMM, we recommend that you unregister the shared storage from that node by using your storage array vendor's management tools.

See Also

Modifying a Hyper-V Host Cluster in VMM

How to Uncluster a Hyper-V Host Cluster in VMM

You can use the following procedure to uncluster a managed Hyper-V host cluster through the VMM console in Virtual Machine Manager (VMM). When you uncluster a host cluster, the nodes in the cluster become stand-alone managed hosts.

Prerequisites

Before you begin this procedure, make sure that the following prerequisites are met.

- The host cluster must be a managed host cluster that is located in a domain that is trusted by the domain of the VMM management server.
- The host cluster must have no highly-available virtual machines or any other clustered services or applications.

Note
You do not have to put the cluster nodes in maintenance mode.

To uncluster a Hyper-V host cluster

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, expand **All Hosts**, and then locate and click the host cluster.
3. On the **Host Cluster** tab, in the **Host Cluster** group, click **Uncluster**.
4. Review the warning message, and then click **Yes** to continue.
5. Open the **Jobs** workspace to monitor the job status.

   When the job is completed, the hosts appear as stand-alone hosts in the **Fabric** workspace.

   Note
   As part of the job, VMM unregisters the shared storage that is managed through VMM from the cluster nodes. If the cluster had shared storage assigned that was not managed by VMM, we recommend that you unregister the shared storage by using your storage array vendor's management tools.

See Also

Creating and Modifying Hyper-V Host Clusters in VMM

How to Remove a Node from a Hyper-V Host Cluster in VMM

Configuring Hyper-V Host Cluster Properties in VMM

After you add a Hyper-V host cluster to System Center 2012 – Virtual Machine Manager (VMM), you can view and configure the host cluster properties that are described in the following table.

Tab	Settings
General	View the name, host group and description for the cluster. You can also configure the **Cluster reserve (nodes)** setting, and view the cluster reserve state and any cluster reserve details. The **Cluster reserve (nodes)** setting specifies the number of node failures a cluster must be able to sustain while still supporting all virtual machines deployed on the host cluster. If the cluster cannot withstand the specified number of node failures and still keep all of the virtual machines running, the cluster is placed in an over-committed state. When over-committed, the clustered hosts receive a zero rating during virtual machine placement. An administrator can override the rating and place a highly-available virtual machine on an over-committed cluster during a manual placement.
Status	View detailed status information for the host cluster. You can view the following information: • Whether a cluster validation test was run, and whether it succeeded. If you ran a cluster validation test, there is a link to the report. **Note** To access the report, you must have administrative permissions on the cluster node where the report is located. **Tip** You can perform an on-demand

Tab	Settings
	cluster validation through VMM. To do this, in the **Fabric** workspace, locate and click the host cluster. Then, on the **Host Cluster** tab, click **Validate Cluster**. Cluster validation begins immediately. • Whether cluster core resources are online. • Whether the disk witness in quorum is online. • Whether the cluster service on each node is online.
Available Storage	Shows available storage that is allocated to the host cluster. Available storage is considered the storage logical units that are assigned to the host cluster that are not Cluster Shared Volumes (CSV). You can also do the following: • Add and remove storage logical units that are managed by VMM. • Convert available storage to shared storage (CSV). For information about how to configure storage for a Hyper-V host cluster, see How to Configure Storage on a Hyper-V Host Cluster in VMM.
Shared Volumes	Shows the shared volumes (CSVs) that are allocated to the host cluster. You can also do the following: • Add and remove CSVs that are managed by VMM. • Convert CSVs to available (non-CSV) storage. For information about how to configure storage for a Hyper-V host cluster, see How to Configure Storage on a Hyper-V Host Cluster in VMM.
Virtual Networks	Shows the external virtual networks that are common across all cluster nodes. From the Virtual Networks tab, you can also

Tab	Settings
	create and edit external virtual networks that are common across all nodes. To create an external virtual network that is common across all cluster nodes, make sure that the logical networks that you want to use are associated with physical network adapters on each Hyper-V host. The logical networks that are associated with a physical network adapter on each node must be identical. (This includes any associated VLAN IDs.) Then, click **Create**, select a logical network, enter a name for the virtual network, configure whether to enable host access, and then click **Create**. Click **OK** to commit the changes. **Note** For information about logical network association, see the “Prerequisites” section and the “To associate logical networks with a physical network adapter (for an external virtual network)” procedure in How to Configure Network Settings on a Hyper-V Host in VMM.
Custom Properties	Enables you to assign and manage custom properties.

In This Section

This section includes detailed information about how to configure storage on a managed Hyper-V host cluster.

Topic	Description
How to Configure Storage on a Hyper-V Host Cluster in VMM	Describes how to create, assign, and remove shared and available storage that is under VMM management on a Hyper-V host cluster.

See Also

Creating and Modifying Hyper-V Host Clusters in VMM

How to Configure Storage on a Hyper-V Host Cluster in VMM

You can use the following procedures to configure storage on a managed Hyper-V host cluster in Virtual Machine Manager (VMM). The procedures show the following:

- How to add available storage to a managed Hyper-V host cluster
- How to convert available storage to shared storage (Cluster Shared Volumes or CSV)
- How to add shared storage to a managed Hyper-V host cluster
- How to convert shared storage to available storage
- How to remove available or shared storage from a managed Hyper-V host cluster

Note
Windows Server 2008 with Service Pack 2 (SP2) does not support CSV. Therefore, procedures in this topic that apply to shared storage are not supported on a Windows Server 2008 with SP2-based Hyper-V host cluster.

Important
VMM is agnostic regarding the use of asymmetric storage, where a workload can use disks that are shared between a subset of the cluster nodes. VMM does not support or block this storage configuration. Note that to work correctly with VMM, each cluster node must be a possible owner of the cluster disk. (Support for asymmetric storage was introduced in Windows Server 2008 R2 Service Pack 1.)

Account requirements To complete this procedure, you must be a member of the Administrator user role or a member of the Delegated Administrator where the management scope includes the host group where the Hyper-V host cluster is located.

Prerequisites

Before you begin these procedures, make sure that the following prerequisites are met:

- You must have completed the procedures in the Configuring Storage in VMM section to discover, classify and provision storage through the VMM console.
- You must have allocated logical units or storage pools to the host group (or parent host group) where the Hyper-V host cluster resides. For more information, see How to Allocate Storage Logical Units to a Host Group in VMM and How to Allocate Storage Pools to a Host Group in VMM.

Note

Realize that you can create logical units during the procedures to add available or shared storage to a Hyper-V host cluster. To do this, you must have allocated one or more storage pools to the host group (or parent host group) where the Hyper-V host cluster resides.

- Make sure that each node of the cluster is correctly configured to access the storage array. Configuration will vary depending on your storage hardware. Configuration typically includes the following:

  Note
  For specific configuration information, see your storage array vendor's documentation.

  - The Multipath I/O (MPIO) feature must be added on each host that will access the Fibre Channel or iSCSI storage array. You can add the MPIO feature through Server Manager. If the MPIO feature is already enabled before you add a host to VMM management, VMM will automatically enable MPIO for supported storage arrays by using the Microsoft provided Device Specific Module (DSM). If you already installed vendor-specific DSMs for supported storage arrays, and then add the host to VMM management, the vendor-specific MPIO settings will be used to communicate with those arrays.

    If you add a host to VMM management before you add the MPIO feature, you must add the MPIO feature, and then manually configure MPIO to add the discovered device hardware IDs. Or, you can install vendor-specific DSMs.

    Note
    For more information, including information about how to install MPIO, see Support for Multipath I/O (MPIO).

  - If you are using a Fibre Channel storage area network (SAN), each host that will access the storage array must have a host bus adapter (HBA) installed. Additionally, make sure that the hosts are zoned accordingly so that they can access the storage array.
  - If you are using an iSCSI SAN, make sure that iSCSI portals have been added and that the iSCSI initiator is logged into the array. Additionally, make sure that the Microsoft iSCSI Initiator Service on each host is started and set to Automatic. For information about how to create an iSCSI session on a host through VMM, see How to Configure Storage on a Hyper-V Host in VMM.

  Important
  By default, when VMM manages the assignment of logical units, VMM creates one storage group per host. In a cluster configuration, VMM creates one storage group per cluster node. A storage group can contain one or more of the host's initiator IDs (iSCSI Qualified Name (IQN) or a World Wide Name (WWN)).

  For some storage arrays, it is preferable to use one storage group for the entire cluster, where host initiators for all cluster nodes are contained in a single storage group. To support this configuration, you must set the `CreateStorageGroupsPerCluster` property to `$true` by using the `Set-SCStorageArray` cmdlet in the VMM command shell.

In VMM, a storage group is defined as an object that binds together host initiators, target ports and logical units. A storage group has one or more host initiators, one or more target ports and one or more logical units. Logical units are exposed to the host initiators through the target ports.

- Before you remove storage, make sure that there are no virtual machines on the cluster that use the storage for their associated .vhd or .vhdx files. If there are, the Remove option is disabled.
- Before you convert available to shared storage, or convert shared to available storage, make sure that there are no virtual machines on the cluster that have their associated .vhd or .vhdx files located on the storage that you want to convert.

Warning

If you convert shared to available storage, and there are virtual machines on the storage that you convert, this can cause serious data loss.

To add available storage for a Hyper-V host cluster

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then expand **All Hosts**.
3. Locate and then click the Hyper-V host cluster that you want to configure.
4. On the **Host Cluster** tab, in the **Properties** group, click **Properties**.
5. In the *Host Cluster Name* **Properties** dialog box, click the **Available Storage** tab.
6. To assign available logical units to the host cluster, follow these steps:
   a. Click **Add**.

      Logical units that are available for assignment through VMM are listed.

   b. To create a new logical unit, click **Create Logical Unit**. The Create Logical Unit dialog box opens. In the **Storage pool** list, click a storage pool. Enter a name, description and size (in gigabytes) for the logical unit, and then click **OK**.

      Note

      For the logical unit name, use only alphanumeric characters.

   c. In the **Add Cluster Disk** dialog box, select the check box next to each logical unit that you want to add.
   d. For each logical unit, configure the partition style (**MBR** or **GPT**) and the file system (**NTFS** or **Do not format**), enter a volume label, and then select or clear the **Quick Format** check box.

      Note

      If the disk has already been initialized, the option to change the partition style is unavailable. Also, if the disk is not newly created, VMM does not format the disk.

   e. When you are finished, click **OK**.
7. In the *Host Cluster Name* **Properties** dialog box, click **OK** to commit the changes.

Note

When a virtual machine is placed on an available logical unit, the logical unit no longer appears as available storage.

To convert available storage to shared storage (CSV)

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then expand **All Hosts**.
3. Locate and then click the Hyper-V host cluster that you want to configure.
4. On the **Host Cluster** tab, in the **Properties** group, click **Properties**.
5. In the *Host Cluster Name* **Properties** dialog box, click the **Available Storage** tab.
6. Select a volume that you want to convert to shared storage, and then click **Convert to CSV**.

   When you click **Convert to CSV**, the logical unit disappears from the **Available Storage** tab.

   Note

   If you want to convert multiple volumes, you must convert them one at a time.
7. When you are finished, click **OK** to commit the changes.

   Verify that the logical unit appears on the **Shared Volumes** tab.

To add shared storage (CSVs) to a Hyper-V host cluster

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then expand **All Hosts**.
3. Locate and then click the Hyper-V host cluster that you want to configure.
4. On the **Host Cluster** tab, in the **Properties** group, click **Properties**.
5. In the *Host Cluster Name* **Properties** dialog box, click the **Shared Volumes** tab.

   To assign Cluster Shared Volumes (CSVs) to the host cluster, follow these steps:

   a. Click **Add**.

      Logical units that are available for assignment through VMM are listed.

   b. To create a new logical unit, click **Create Logical Unit**. The Create Logical Unit dialog box opens. In the **Storage pool** list, click a storage pool. Enter a name, description and size (in gigabytes) for the logical unit, and then click **OK**.

   c. In the **Add Cluster Shared Volume** dialog box, select the check box next to each logical unit that you want to add.

   d. For each logical unit, configure the partition style (**MBR** or **GPT**) and the file system (**NTFS** or **Do not format**), enter a volume label, and then select or clear the **Quick Format** check box.

   e. When you are finished, click **OK**.
6. In the *Host Cluster Name* **Properties** dialog box, click **OK** to commit the changes.

To convert shared storage (CSV) to available storage

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then expand **All Hosts**.
3. Locate and then click the Hyper-V host cluster that you want to configure.
4. On the **Host Cluster** tab, in the **Properties** group, click **Properties**.
5. In the *Host Cluster Name* **Properties** dialog box, click the **Shared Volumes** tab.
6. Select one or more volumes that you want to convert to available storage, and then click **Convert to Available Storage**.

   When you click **Convert to Available Storage**, the logical unit disappears from the **Shared Volumes** tab.
7. When you are finished, click **OK** to commit the changes.

   Verify that the logical unit appears on the **Available Storage** tab.

To remove available or shared storage

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then expand **All Hosts**.
3. Locate and then click the Hyper-V host cluster that you want to configure.
4. On the **Host Cluster** tab, in the **Properties** group, click **Properties**.
5. In the *Host Cluster Name* **Properties** dialog box, click the **Available Storage** tab or the **Shared Volumes** tab.
6. Select one or more volumes that you want to remove, and then click **Remove**.

   Note
   If there are virtual machines on the cluster that use the volume for their associated .vhd or .vhdx files, the Remove option is disabled.
7. When you are finished, click **OK** to commit the changes.

See Also

Configuring Storage in VMM

How to Configure Storage on a Hyper-V Host in VMM

Modifying a Scale-Out File Server in VMM

This section describes how to add or remove nodes, from Scale-Out File Server clusters in Virtual Machine Manager (VMM).

In This Section

Topic	Description
How to Add a Node to a Scale-Out File Server in VMM	Describes how to add a node to a Scale-Out File Server in VMM.
How to Remove a Node From a Scale-Out File Server in VMM	Describes how to remove a node from a Scale-Out File Server in VMM.
How to Remove and Uncluster a Scale-Out File Server in VMM	Describes how to remove a Scale-Out File Server so that it is no longer managed by VMM.

How to Add a Node to a Scale-Out File Server in VMM

You can use the following procedure to add one or more nodes to a Scale-Out File Server cluster by using the Virtual Machine Manager (VMM) console.

Prerequisites

Before you begin this procedure, make sure that the following prerequisites are met:

- The Windows Server 2012 R2 operating system is installed on the computers that you want to add as a cluster node.
- The computer is located in the same domain as the target cluster.
- The target computer must be located in a domain that has two-way trust relations with the domain of the VMM management server.

To add a file server as a cluster node

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Storage**, and then click **File Servers**.
3. In the **File Servers** pane, right-click the name of the Scale-Out File Server cluster to which you want to add a node, and click **Properties**.
4. In the **Properties** dialog box, skip to the **Cluster Nodes** page.
5. On the **Nodes in the cluster** page, click **Add** to open the **Add File Server Nodes** dialog box. Enter the necessary information to identify the computers that you want to add to the cluster. Enter one computer per line.

   If you already added nodes to the cluster without using VMM (for example, by using Windows), although these nodes are included in the cluster, the VMM agent was not installed on them. These nodes will be listed under **Computer name** , and you need to

add them to the cluster prior to adding other nodes. This allows VMM to install the VMM agent on these nodes, so that they are properly managed by VMM as part of the cluster.

Click **Add** to close the **Add File Server Nodes** dialog box.

6. Verify that the computers you want to add to the cluster are listed in the **File server nodes** area, with the status of **Pending cluster addition**, and then click **OK**.
7. After the jobs for adding the nodes complete, you can verify that a cluster node was added. In the **Fabric** pane, expand **Storage**, click **File Servers**, and then locate and expand the Scale-Out File Server cluster.

   In the **File Servers** pane, verify that the new node appears as part of the cluster, and that the status of the nodes is **OK**.

How to Remove a Node From a Scale-Out File Server in VMM

You can use the following procedure to remove one or more nodes from a Scale-Out File Server cluster by using the Virtual Machine Manager (VMM) console.

Prerequisites

Before you begin this procedure, make sure that the following prerequisites are met:

- The node must be located in a domain that has two-way trust with the domain of the VMM management server.
- The cluster that you want to remove the node from must have more than one node.
- All the nodes in the cluster must have the VMM agent installed.

To remove a node from a Scale-Out File Server cluster

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Storage**, and click **File Servers**.
3. In the **File Servers** pane, right-click the file server that the node is part of, and then click **Properties**.
4. In the **Properties** dialog box, skip to the **Cluster Nodes** page. In the **File server nodes** list, select the nodes that you want to remove, and click **Remove**.
5. Open the **Jobs** workspace to view the job status. To verify that VMM removed the node from the cluster, in the VMM console, make sure that it is no longer listed as part of the file server.

   Note

   A file server cluster can have storage logical units from a storage area network (SAN) unmasked to it. When you remove a node from the cluster, VMM does not

mask the storage in that scenario. If the array is managed by VMM, you can open the **Properties** dialog box of the storage logical unit to remove the initiators that the storage is unmasked to. If the array is not managed by VMM, you can mask the storage by using the vendor's management tools for your storage array.

How to Remove and Uncluster a Scale-Out File Server in VMM

You can use the following procedure to remove a managed Scale-Out File Server by using the Virtual Machine Manager (VMM) console. When you remove a Scale-Out File Server, it still exists; however, it is no longer managed by VMM. To uncluster a Scale-Out File Server, you can use the Uninstall-SCStorageFileServer cmdlet.

To remove a Scale-Out File Server

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Storage**, and expand **Providers**.
3. In the **Providers** pane, locate the storage provider that is associated with the Scale-Out File Cluster you want to remove.
4. On the **Home** tab, click **Remove**.

Configuring Dynamic Optimization and Power Optimization in VMM

The procedures in this section explain how to configure Dynamic Optimization and Power Optimization in System Center 2012 – Virtual Machine Manager (VMM), and how to run Dynamic Optimization on demand for a host cluster.

VMM can perform load balancing within host clusters that support live migration. Dynamic Optimization migrates virtual machines within a cluster according to settings you enter.

Note
In System Center 2012 – Virtual Machine Manager, Dynamic Optimization replaces the host load balancing that is performed for Performance and Resource Optimization (PRO) by the PRO CPU Utilization and PRO Memory Utilization monitors in System Center Virtual Machine Manager (VMM) 2008 R2.

VMM can help to save power in a virtualized environment by turning off hosts when they are not needed and turning the hosts back on when they are needed.

VMM supports Dynamic Optimization and Power Optimization on Hyper-V host clusters and on host clusters that support live migration in managed VMware ESX and Citrix XenServer environments. For Power Optimization, the computers must have a baseboard management controller (BMC) that enables out-of-band management.

Dynamic Optimization in VMM

During Dynamic Optimization, VMM migrates virtual machines within a host cluster to improve load balancing among hosts and to correct any placement constraint violations for virtual machines.

Dynamic Optimization can be configured on a host group, to migrate virtual machines within host clusters with a specified frequency and aggressiveness. Aggressiveness determines the amount of load imbalance that is required to initiate a migration during Dynamic Optimization. By default, virtual machines are migrated every 10 minutes with medium aggressiveness. When configuring frequency and aggressiveness for Dynamic Optimization, an administrator should factor in the resource cost of additional migrations against the advantages of balancing load among hosts in a host cluster. By default, a host group inherits Dynamic Optimization settings from its parent host group.

Dynamic Optimization can be set up for clusters with two or more nodes. If a host group contains stand-alone hosts or host clusters that do not support live migration, Dynamic Optimization is not performed on those hosts. Any hosts that are in maintenance mode also are excluded from Dynamic Optimization. In addition, VMM only migrates highly available virtual machines that use shared storage. If a host cluster contains virtual machines that are not highly available, those virtual machines are not migrated during Dynamic Optimization.

On demand Dynamic Optimization also is available for individual host clusters by using the **Optimize Hosts** action in the **VMs and Services** workspace. On demand Dynamic Optimization can be performed without configuring Dynamic Optimization on host groups. After Dynamic Optimization is requested for a host cluster, VMM lists the virtual machines that will be migrated for the administrator's approval.

Power Optimization in VMM

Power Optimization is an optional feature of Dynamic Optimization, and it is only available when a host group is configured to migrate virtual machines through Dynamic Optimization. Through Power Optimization, VMM helps to save energy by turning off hosts that are not needed to meet resource requirements within a host cluster and turns the hosts back on when they are needed again.

By default, VMM performs power optimization all of the time when the feature is turned on. However, you can schedule the hours and days during the week when power optimization is performed. For example, you might initially schedule power optimization only on weekends, when

you anticipate low resource usage on your hosts. After observing the effects of power optimization in your environment, you might increase the hours.

Power Optimization ensures that the cluster maintains a quorum if an active node fails. For clusters created outside VMM and added to VMM, Power Optimization requires more than four nodes. For each additional one or two nodes in a cluster, one node can be powered down. For instance:

- One node can be powered down for a cluster of five or six nodes.
- Two nodes can be powered down for a cluster of seven or eight nodes.
- Three nodes can be powered down for a cluster of nine or ten nodes.

When VMM creates a cluster, it creates a quorum disk and uses that disk as part of the quorum model. For clusters created by VMM, Power Optimization can be set up for clusters of more than three nodes. This means that the number of nodes that can be powered down is as follows:

- One node can be powered down for a cluster of four or five nodes.
- Two nodes can be powered down for a cluster of six or seven nodes.
- Three nodes can be powered down for a cluster of eight or nine nodes.

For more information about quorum configurations, see Understanding Quorum Configurations in a Failover Cluster.

Before turning off a host for Power Optimization, VMM migrates all virtual machines to other hosts in the host cluster. When a host is needed again, VMM turns on the host and then performs Dynamic Optimization to migrate virtual machines and balance load within the host cluster. When Power Optimization is disabled on a host group, or when a scheduled period of Power Optimization ends, the same process occurs with all hosts that were turned off by Power Optimization.

Resource thresholds for Dynamic Optimization and Power Optimization

The following settings in the host group properties determine the actions that VMM takes on host clusters:

- Dynamic Optimization settings specify thresholds of resource usage beyond which VMM attempts to migrate virtual machines to improve load balancing. You can specify Dynamic Optimization settings for the following resources: CPU, memory, disk I/O, and network I/O.
- Power Optimization settings specify resource capacity that must be maintained after VMM turns off a host during power optimization. These settings provide a buffer of available resources to ensure that fluctuations in resource usage during normal operations do not result in VMM turning hosts on and off needlessly. Power Optimization settings include CPU, memory, disk space, disk I/O, and network I/O.

When Power Optimization is enabled on a host group, Dynamic Optimization and Power Optimization are performed in concert. Hosts that VMM has turned off to conserve energy can be turned on to balance load or to meet virtual machine requirements.

For more information about configuring Dynamic Optimization levels and placement levels for a host group, see How to Configure Dynamic Optimization and Power Optimization.

Prerequisites

To use Dynamic Optimization and Power Optimization, ensure that the following requirements are met:

- To use Dynamic Optimization, VMM must be managing a host cluster that supports live migration. For information about configuring Hyper-V host clusters in VMM, see Adding and Managing Hyper-V Hosts and Host Clusters in VMM. For information about adding VMware ESX and Citrix XenServer environments to VMM, see Managing VMware and Citrix XenServer in VMM.

  Note
  You can configure Dynamic Optimization and Power Optimization on any host group. However, the settings will not have any effect unless the host group contains a host cluster.

- To use Power Optimization, the host computers must have a BMC that enables out-of-band management. For more information about the BMC requirements, see How to Configure Host BMC Settings.
- To view Dynamic Optimization and Power Optimization in action, you must deploy and run virtual machines on the host cluster. For more information, see Creating and Deploying Virtual Machines in VMM.

In This Section

Use the procedures in this section to perform the following tasks.

Procedure	Description
How to Configure Dynamic Optimization and Power Optimization	Describes how to configure Dynamic Optimization and Power Optimization for a host group.
How to Run Dynamic Optimization on a Host Cluster	Describes how to initiate Dynamic Optimization on demand within a host cluster by using the **Optimize Hosts** action in the **Fabric** workspace.

How to Configure Dynamic Optimization and Power Optimization

Use the following procedures to enable Dynamic Optimization and Power Optimization for a host group in System Center 2012 – Virtual Machine Manager (VMM) and to configure resource Power Optimization usage on a host group.

For more information about Dynamic Optimization and Power Optimization, see Configuring Dynamic Optimization and Power Optimization in VMM.

Account requirements Administrators and delegated administrators can configure Dynamic Optimization. Delegated administrators can configure Dynamic Optimization on host groups that are within the scope of their user role.

To turn on Dynamic Optimization and Power Optimization for a host group

1. In the **Fabric** workspace, expand **Servers**, expand **All Hosts**, navigate to the host group that you want to configure.
2. With the host group selected, on the **Folder** tab, in the **Properties** group, click **Properties**.
3. In the host group properties, click **Dynamic Optimization** to open the **Specify dynamic optimization settings** page.
4. To configure different settings than those of the parent host group, clear the **Use Dynamic Optimization settings from the parent host group** check box.
5. In **Aggressiveness**, select **High**, **Medium**, or **Low**.

   Aggressiveness determines the amount of imbalance in virtual machine load on the hosts that is required in order to initiate a migration during Dynamic Optimization. When you configure frequency and aggressiveness for Dynamic Optimization, you should try to balance the resource cost of additional migrations against the advantages of balancing load among hosts in a host cluster. Initially, you might accept the default value of **Medium**. After you observe the effects of Dynamic Optimization in your environment, you can increase the aggressiveness.

   To help conserve energy by having VMM turn off hosts when they are not needed and turn them on again when they are needed, configure Power Optimization for the host group. Power Optimization is only available when virtual machines are being migrated automatically to balance load.
6. To periodically run Dynamic Optimization on qualifying host clusters in the host group, enter the following settings:
   a. Select the **Automatically migrate virtual machines to balance load** check box.
   b. In **Frequency (minutes)**, specify how often to run Dynamic Optimization. You can enter any value between 10 minutes (the default frequency) and 1440 minutes (24 hours).
7. To turn on Power Optimization on the host group, select the **Enable power optimization**

check box.

8. Click **OK** again to save your changes to the dynamic optimization settings.

Use the following procedure to change the thresholds for CPU, memory, disk I/O, and network I/O on hosts that govern how VMM performs Dynamic Optimization and Power Optimization within a host group. You do not need to perform this procedure unless you want to change the default thresholds.

To configure settings for Power Optimization

1. In the **Fabric** workspace, navigate to the host group and open its properties.
2. Click **Dynamic Optimization** and, on the **Specify dynamic optimization settings** page, click **Settings**.
3. In the **Customize Power Optimization Schedule** dialog box, change the settings for any of these resources: CPU, memory, disk input/output (I/O), or network I/O.
4. Under **Schedule**, select the hours when you want power optimization to be performed. Click a box to turn power optimization on or off for that hour.

   VMM applies the Power Optimization schedule locally according to the time zone of each host.
5. Click **OK** to close the dialog box and **OK** again to close the group **Properties**.

How to Run Dynamic Optimization on a Host Cluster

Use the following procedure to run Dynamic Optimization on demand on a host cluster in System Center 2012 – Virtual Machine Manager (VMM). Through Dynamic Optimization, VMM can balance load among hosts by migrating virtual machines within a host cluster. VMM only performs Dynamic Optimization on host clusters that support live migration. On demand Dynamic Optimization does not require that Dynamic Optimization be configured on the parent host group.

For more information about Dynamic Optimization, see Configuring Dynamic Optimization and Power Optimization in VMM.

Account requirements Administrators can run Dynamic Optimization on a host cluster. Delegated administrators can run Dynamic Optimization on host clusters that are within the scope of their Delegated Administrator user role.

How to run Dynamic Optimization on a host cluster

1. Open the **Fabric** workspace.
2. On the **Fabric** pane, expand **Servers**, expand **Host Groups**, and navigate to the host cluster on which you want to run Dynamic Optimization. Then click the host cluster to select it.

3. On the **Folder** tab, in the **Optimization** group, click **Optimize Hosts**.

   VMM performs a Dynamic Optimization review to determine whether virtual machines can be migrated to improve load balancing in the host cluster. If migrating virtual machines can improve load balancing, VMM displays a list of virtual machines that are recommended for migration, with the current and target hosts indicated. The list excludes any hosts that are in maintenance mode in VMM and any virtual machines that are not highly available.
4. To perform Dynamic Optimization on the host cluster, click **Migrate**.

Managing VMware ESX and Citrix XenServer in VMM

The topics in this section explain how to add and manage VMware ESX hosts and Citrix XenServer hosts from the VMM console in System Center 2012 – Virtual Machine Manager (VMM).

In This Section

Managing VMware ESX Hosts Overview

Describes the key differences in ESX host management from VMM 2008 R2, provides information about the supported ESX host versions and features, and links to procedures for how to add and manage ESX hosts.

Managing Citrix XenServer Overview

Describes the benefits of managing Citrix XenServer through VMM, provides information about the supported XenServer host versions and features, and links to procedures for how to add and manage XenServer hosts.

Managing VMware ESX Hosts Overview

System Center 2012 – Virtual Machine Manager (VMM) enables you to deploy and manage virtual machines and services across multiple hypervisor platforms, including VMware ESX and ESXi hosts. In VMM, support for ESX is optimized for virtual machine and service management. VMM enables you to manage and provide resources from multiple hypervisors and make the

resources available to private cloud deployments, all from a common user interface and common command-line interface (CLI).

VMM integrates directly with VMware vCenter Server. Through the VMM console, you can manage the day-to-day operations of VMware ESX hosts and host clusters, such as the discovery and management of ESX hosts, and the ability to create, manage, store, place and deploy virtual machines on ESX hosts. However, we expect you to perform more advanced fabric management through vCenter Server, such as the configuration of port groups, standard and distributed virtual switches (or “vSwitches”), vMotion and Storage vMotion. By integrating with vCenter Server to manage ESX hosts, VMM can recognize and support these VMware features.

Key Differences in VMware ESX Management from VMM 2008 R2

The following list summarizes the key differences in VMware ESX management from VMM 2008 R2.

- When you add a vCenter Server, VMM no longer imports, merges and synchronizes the VMware tree structure with VMM. Instead, after you add a vCenter Server, you can add selected ESX servers and hosts to any VMM host group. Therefore, there are fewer issues with synchronization.
- When you import a VMware template to the VMM library, the .vmdk file is no longer copied to the library. Instead, VMM only copies the metadata that is associated with the template. The .vmdk file remains in the ESX datastore. Because of this relationship, you can deploy virtual machines by using the template much more quickly. Also, when you import a VMware template, VMM no longer deletes the source template. It is important to realize that there is now a dependency on the VMware template on the vCenter Server.
    - If you delete the template in vCenter Server, the VMM template will go into a missing state.
    - In vCenter Server, you can convert the template to a virtual machine, make changes, and then convert it back to a template. Because the ID of the template is the same, VMM will mark the template as OK instead of Missing.

  Another behavioral change in VMM is that when you delete a VMware template from the VMM library, it is no longer deleted from the VMware datastore.
- VMM uses HTTPS for all file transfers between ESX hosts and the VMM library. VMM no longer supports Secure File Transfer Protocol (SFTP) for file transfers.
- VMM now supports VMware distributed virtual switch functionality. You must configure distributed virtual switches through vCenter Server.
- Because VMM no longer supports SFTP for file transfers, you do not have to enable root Secure Shell (SSH) access to ESX hosts. In System Center 2012 – Virtual Machine Manager, the use of a virtual machine delegate is not supported.
- VMM no longer automatically creates port groups on ESX hosts for network equivalency. For example, if you deploy a new virtual machine to an ESX host cluster, and you select a virtual network that is not available on all nodes of the cluster, VMM will not automatically create a port group. You must perform all port group configuration in vCenter Server.

VMware Support

For information about the supported versions of vCenter Server and ESX/ESXi hosts, see as follows.

- For System Center 2012 – Virtual Machine Manager or for System Center 2012 SP1 see: **System Requirements: VMware ESX Hosts in System Center 2012 and in System Center 2012 SP1**.
- For System Center 2012 R2 Virtual Machine Manager see: **Preparing your environment for System Center 2012 R2 Virtual Machine Manager**.

Supported Features

The following tables shows the VMM and VMware features that are supported when VMM manages ESX hosts through vCenter Server.

Feature	Notes
VMM command shell	The VMM command shell is common across all hypervisors.
Placement	VMM offers virtual machine placement based on host ratings during the creation, deployment, and migration of VMware virtual machines. This includes concurrent virtual machine deployment during service deployment.
Services	You can deploy VMM services to ESX hosts. **Note** VMM services use a different model than VMware vApp. Therefore, the two methods can coexist. However, you cannot use VMM to deploy vApps.
Private clouds	You can make ESX host resources available to a private cloud by creating private clouds from host groups where ESX hosts reside, or by creating a private cloud from a VMware resource pool. You can configure quotas for the private cloud and for self-service user roles that apply to the private cloud. **Note** VMM does not integrate with VMware vCloud.

Feature	Notes
Dynamic Optimization and Power Optimization	You can use the new Dynamic Optimization features with ESX hosts. For example, VMM can load balance virtual machines on ESX host clusters by using Live Migration. Through Power Optimization, you can configure VMM to turn ESX hosts on and off for power management. **Note** For power optimization, you can use the Dynamic Optimization feature in VMM or the VMware Dynamic Resource Scheduler.
Migration	Supported VMware transfer types include the following: • Live Migration between hosts within cluster (uses vMotion) • Live Storage Migration (uses Storage vMotion) Supported VMM transfer types include the following: • Network migration to and from the library **Note** VMware thin provision disks become thick when a disk is migrated to the VMM library. • Network migration between hosts
Maintenance mode	You can place an ESX host that is managed by VMM in and out of maintenance mode by using the VMM console.
Library	You can organize and store VMware virtual machines, .vmdk (VMDK) files, and VMware templates in the VMM library. VMM supports creating new virtual machines from templates and converting stored VMware virtual machines to Hyper-V. **Important** If you want to use VMDK files that were

Feature	Notes
	created in VMware Server or VMware Workstation, realize that System Center 2012 – Virtual Machine Manager does not support older VMDK disk types. Supported VMDK disk types include the following: • Regular VMDK files: VMFS and monolithicFlat • VMDK files that are used to access physical disks: vmfsPassthroughRawDeviceMap • Snapshots: vmfssparse If you want to copy a VMDK file that uses an unsupported disk type to the VMM library, you must use VMware conversion tools such as VMware Virtual Disk Manager to update the disk type to a supported type.
Templates	Supports the creation of templates using .vmdk files that are stored in the library. In this case, all physical files are stored in the VMM library. You can also import templates that are stored on ESX hosts. When you import a template from vCenter Server, VMM only imports template metadata. The .vmdk file is not copied to the VMM library.
Networking	VMM supports both standard and distributed vSwitches and port groups. Be aware that you must perform all vSwitch and port group configuration by using vCenter Server. VMM recognizes and uses existing configured vSwitches and port groups for virtual machine deployment. The new VMM networking management features are supported on ESX hosts, such as the assignment of logical networks, and the assignment of static IP addresses and MAC addresses to Windows-based virtual machines that are running on ESX hosts.

Feature	Notes
	Important VMM does not automatically create port groups on VMware ESX hosts. Therefore, for logical networks to work correctly for managed ESX hosts, you must use VMware vCenter Server to configure port groups with the necessary VLANs that correspond to the logical network sites.
Storage	VMM supports and recognizes VMware Paravirtual SCSI (PVSCSI) storage adapters. For example, when you use VMM to create a new virtual machine on an ESX host, you can add a SCSI adapter of type “VMware Paravirtual.” **Note** VMM does not support VMware virtual machines with virtual hard disks that are connected to an integrated drive electronics (IDE) bus. VMM supports VMware thin provision virtual hard disks through the dynamic disk type. Note the following behavior: • If you create and deploy a virtual machine to an ESX host that is configured to use a dynamic disk, the disk is created as a thin provisioned disk. • If a virtual machine uses a thin provisioned disk that was created out of band, VMM displays the disk as a dynamic disk. • If you save a thin provision virtual hard disk to the library, VMM converts the disk to a fixed thick disk. If you then create a virtual machine from the virtual hard disk that is on the library, and deploy it to an ESX host, the disk remains a thick fixed disk. VMM supports the hot add and hot removal of virtual hard disks on VMware virtual machines. **Note**

Feature	Notes
	The new VMM storage automation features are not supported for ESX hosts. All storage must be added to ESX hosts outside VMM.
Conversion	Converting a VMware-based virtual machine to a Hyper-V based virtual machine is supported by using the virtual to virtual (V2V) process. **Note** VMM does not support VMware virtual machines with virtual hard disks that are connected to an integrated drive electronics (IDE) bus. Therefore, you cannot perform a V2V conversion of a VMware virtual machine that is on an IDE bus.
Performance and Resource Optimization (PRO)	Monitoring and alerting for ESX hosts is possible through VMM with the integration of Operations Manager and PRO.

Additional Support Information

- VMM supports up to 255 GB of RAM for virtual machines that are deployed on ESX/ESXi 4.0 hosts.
- VMM supports up to 8 virtual CPUs (vCPUs) for virtual machines that are deployed on ESX/ESXi 4.0 hosts.
- VMM recognizes VMware fault tolerant virtual machines. In the VMM console, VMM shows only the virtual machine that is designated as the primary on the vCenter Server. If there is a failure, VMM recognizes the new primary.
- Update management through VMM is not supported for ESX hosts. You must use your existing solution to update VMware ESX hosts.
- The conversion of a bare-metal computer to a virtual machine host, and cluster creation through VMM is not supported for ESX hosts.
- The Dynamic Memory feature is not supported on ESX hosts. Dynamic Memory is only supported on Hyper-V hosts that are running an operating system that supports Dynamic Memory.

In This Section

Follow these procedures to manage VMware ESX hosts through VMM.

Procedure	Description
How to Add a VMware vCenter Server to VMM	Describes how to add a VMware vCenter server to VMM management.
How to Add VMware ESX Hosts to VMM	Describes how to add ESX and ESXi hosts to VMM management.
How to Configure Network Settings on a VMware ESX Host	Describes how to configure ESX host network settings to support the new logical network feature in VMM.
How to Configure Host BMC Settings in VMM	Describes how to configure Baseboard Management Controller (BMC) settings on a host to support power management through VMM.
How to Import VMware Templates	Describes how to import a VMware template to the VMM library.
How to Convert VMware Virtual Machines to Hyper-V	Describes how to convert a VMware virtual machine to a Hyper-V virtual machine through the virtual-to-virtual (V2V) machine conversion process.

How to Add a VMware vCenter Server to VMM

You can use the following procedure to add a VMware vCenter Server to System Center 2012 – Virtual Machine Manager (VMM). You must add the vCenter Server before you can add VMware ESX hosts.

Prerequisites

Before you begin this procedure, make sure that the following prerequisites are met:

- The server that you want to add must be running a supported version of vCenter Server. For more information, see as follows:
  - For System Center 2012 – Virtual Machine Manager or for System Center 2012 SP1 see: **System Requirements: VMware ESX Hosts in System Center 2012 and in System Center 2012 SP1**.
  - For System Center 2012 R2 Virtual Machine Manager see: **Preparing your environment for System Center 2012 R2 Virtual Machine Manager**.

- For communications between the VMM management server and the vCenter Server, encryption using Secure Sockets Layer (SSL) requires a certificate to verify the identity of the vCenter Server. You can either use a self-signed certificate for the vCenter Server, or a third-party, verified certificate. If you are using a self-signed certificate, you can manually import the certificate to the Trusted People certificate store on the VMM management server before you add the vCenter Server, or you can import the certificate during this procedure when you are prompted to do this.

  Note
  If you are using a third-party, verified certificate, you do not have to import the certificate to the Trusted People certificate store.

- Although it is not a required prerequisite, as you can create a Run As account when you add the vCenter Server, you can create a Run As account beforehand. The credentials that you specify for the Run As account must have administrative permissions on the vCenter Server. You can use a local account or an Active Directory domain account, as long as the account has local administrative rights on the operating system of the vCenter Server.

  For example, create a Run As account that is named **VMware vCenter**.

  Note
  You can create a Run As account in the **Settings** workspace. For more information about Run As accounts, see How to Create a Run As Account in VMM.

To add a vCenter Server

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then click **vCenter Servers**.
3. On the **Home** tab, in the **Add** group, click **Add Resources**, and then click **VMware vCenter Server**.

   The Add VMware vCenter Server dialog box opens.
4. In the **Add VMware vCenter Server** dialog box, do the following:
   a. In the **Computer name** box, enter the fully qualified domain name (FQDN), NetBIOS name, or IP address of the vCenter Server.
   b. In the **TCP/IP port** box, enter the port to use to connect to the vCenter Server. By default, VMM uses TCP/IP port 443 to connect to the server through Secure Socket Layer (SSL).
   c. Next to the **Run As account** box, click **Browse**, click the Run As account that has administrative access to the vCenter Server, and then click **OK**.

      For example, if you created the Run As account that is described in the Prerequisites section of this topic, click the **VMware vCenter** Run As account.

      Note
      If you do not already have a Run As account, click **Browse**, and then in the **Select a Run As Account** dialog box, click **Create Run As Account**.
   d. In the **Security** area, select or clear the **Communicate with VMware ESX hosts in**

secure mode check box. By default, this check box is selected (recommended). If selected, a certificate and public key are required for each ESX or ESXi host that is managed by the vCenter Server. If you clear the check box, only Run As account credentials are required for communication.

e. When you are finished, click **OK**.

5. If you are using a self-signed certificate for the vCenter Server, and you have not manually copied the certificate into the Trusted People certificate store on the VMM management server, the **Import Certificate** dialog box appears. In the **Import Certificate** dialog box, review the VMware certificate information, and then click **Import** to add the certificate to the Trusted People certificate store.

   Note
   This step is not required if the certificate is a third-party, verified certificate.

   The **Jobs** dialog box appears. Make sure that the job to add the vCenter Server has a status of **Completed**, and then close the dialog box.

6. To verify that the vCenter Server was added, in the **Fabric** workspace, expand **Servers** and then click **vCenter Servers**.

   In the **vCenter Servers** pane, verify that the vCenter Server is listed, with a status of **Responding**.

See Also

Managing VMware ESX Hosts Overview

How to Add VMware ESX Hosts to VMM

How to Add VMware ESX Hosts to VMM

You can use the following procedure to add a VMware ESX or ESXi host or host cluster to System Center 2012 – Virtual Machine Manager (VMM).

Prerequisites

Before you begin this procedure, make sure that the following prerequisites are met:

- The VMware vCenter Server that manages the ESX hosts that you want to add must already be under VMM management. For more information, see the topic How to Add a VMware vCenter Server to VMM.
- The hosts that you want to add must be running a supported version of ESX. For more information, see as follows:
  - For System Center 2012 – Virtual Machine Manager or for System Center 2012 SP1: **System Requirements: VMware ESX Hosts in System Center 2012 and in System Center 2012 SP1**.

- For System Center 2012 R2 Virtual Machine Manager: **Preparing your environment for System Center 2012 R2 Virtual Machine Manager**.

- If when you added the vCenter Server you selected the option to communicate with the ESX hosts in secure mode, VMM requires a certificate and public key for each managed ESX/ESXi host. This enables all supported management tasks. You can either use the self-signed certificate that VMware created when ESX was installed on the hosts, or a certificate from a trusted certification authority. If you are using the self-signed certificate, you can import the certificate from each ESX host to the VMM management server beforehand, or you can import the certificate during this procedure. If you are using a certificate from a trusted certification authority, you do not have to manually retrieve the certificate from each host.
- Although it is not a required prerequisite, as you can create a Run As account when you add the ESX hosts, you can create a Run As account beforehand. The Run As account need not have root credentials on the ESX hosts that you want to add. The Run As account must be a local account on the ESX host that has administrator permissions on the ESX host. Domain accounts are not supported.

  For example, create a Run As account that is named **ESX Hosts**.

  Note
  You can create Run As accounts in the **Settings** workspace. For more information about Run As accounts, see How to Create a Run As Account in VMM.

  Note
  In System Center 2012 – Virtual Machine Manager, you do not have to enable Secure Shell (SSH) root login on each ESX host. Also, realize that in System Center 2012 – Virtual Machine Manager, the use of a virtual machine delegate is not supported.

To add an ESX host or host cluster

1. Open the **Fabric** workspace.
2. On the **Home** tab, in the **Add** group, click **Add Resources**, and then click **VMware ESX Hosts and Clusters**.

   The Add Resource Wizard opens.
3. On the **Credentials** page, next to the **Run As account** box, click **Browse**, click the Run As account credentials on the ESX hosts that you want to add, click **OK**, and then click **Next**.

   For example, if you created the Run As account that is described in the Prerequisites section of this topic, click the **ESX Hosts** Run As account.

   Note
   If you do not already have a Run As account, click **Browse**, and then in the **Select a Run As Account** dialog box, click **Create Run As Account**.
4. On the **Target resources** page, in the **VMware vCenter Server** list, click the vCenter

Server that manages the ESX hosts that you want to add.

The available ESX hosts for the selected vCenter Server are listed. If the ESX hosts are clustered, the cluster name is listed together with the cluster nodes.

5. In the **Computer Name** column, select the check box next to each ESX host or host cluster that you want to add, or click **Select all**. When you are finished, click **Next**.
6. On the **Host settings** page, in the **Location** list, click the host group where you want to assign the ESX hosts, and then click **Next**.

   Note
   You do not have to add virtual machine placement paths.
7. On the **Summary** page, confirm the settings, and then click **Finish**.

   The **Jobs** dialog box opens to indicate the job status. Verify that the job has a status of **Completed**, and then close the dialog box.
8. To verify that the ESX host or host cluster was added, in the **Fabric** workspace, expand **Servers**, expand **All Hosts**, and then expand the host group where you added the ESX host or host cluster. Click the host or host cluster, and then verify in the **Hosts** pane that each host has a status of either **OK** or **OK (Limited)**.

   If each host has a status of **OK**, you do not have to complete the rest of this procedure.
9. If the host status is **OK (Limited)**, you must provide security information for the host to enable all supported management tasks in VMM. The host status indicates **OK (Limited)** if you enabled secure mode, but have not yet imported a certificate and public key. To update the host status to **OK**, follow these steps:

   Tip
   To view or change the secure mode setting, in the **Fabric** pane, expand **Servers**, and then click **vCenter Servers**. In the **vCenter Servers** pane, right-click the vCenter Server, and then click **Properties**. The secure mode setting is under **Security**.

   a. Right-click an ESX host that has a status of **OK (Limited)**, and then click **Properties**.
   b. In the *Host Name* **Properties** dialog box, click the **Management** tab.
   c. To retrieve the certificate and public key for the host, click **Retrieve**.
   d. To view the thumbprint details, click **View Details**.
   e. To accept the certificate and public key, select the **Accept the certificate for this host** check box.
   f. When you are finished, click **OK**.
   g. In the **Hosts** pane, verify that the host status is **OK**.

Repeat this step for each host that has a status of **OK (Limited)**.

See Also

Managing VMware ESX Hosts Overview

How to Add a VMware vCenter Server to VMM

How to Configure Network Settings on a VMware ESX Host

You can use the following procedures to configure logical network settings on a VMware ESX host in System Center 2012 – Virtual Machine Manager (VMM), and to view compliance information for physical network adapters on the host.

To make logical networks available to virtual machines on an external virtual network, you must associate logical networks with physical network adapters on the ESX host. Compliance information indicates whether all IP subnets and VLANs that are included in the network site that is associated with a logical network are assigned to the physical network adapter.

Prerequisites

Before you begin these procedures, make sure that the following prerequisites are met:

- In the VMM console, you must have already configured the logical networks that you want to associate with the physical network adapter. For more information, see How to Create a Logical Network in VMM.

  Note
  By default, when you add a host to VMM management, VMM automatically creates logical networks on host physical network adapters that do not have logical networks defined. For an ESX host, the default behavior is to create logical networks that match the virtual network switch name. For more information about the default behavior, see How to Configure Global Network Settings in VMM.
- If the logical network has associated network sites, one or more of the network sites must be scoped to the host group where the ESX host resides.

Important
In System Center 2012 – Virtual Machine Manager, VMM does not automatically create port groups on ESX hosts. Therefore, for logical networks and associated network sites, you must use vCenter Server to configure port groups with the necessary VLANs that correspond to the network sites.

To associate logical networks with a physical network adapter (for an external virtual network)

1. Open the **Fabric** workspace.

   Note
   The term fabric is used to denote the infrastructure - the software, servers, high-speed connections and switches that enable access to storage devices in a network.
2. In the **Fabric** pane, expand **Servers**, expand **All Hosts**, and then click the host group

where the host resides.

3. In the **Hosts** pane, click the ESX host that you want to configure.
4. On the **Host** tab, in the **Properties** group, click **Properties**.
5. In the *Host Name* **Properties** dialog box, click the **Hardware** tab.
6. Under **Network Adapters**, click the physical network adapter that you want to configure.
7. Under **Logical network connectivity**, select the check box next to each logical network that you want to associate with the physical network adapter.

   Note
   Be aware that all logical networks are listed here; not just the logical networks that are available to the host group where the host resides.

   For example, if you configured the BACKEND logical network in the Preparing the Fabric in VMM section, and the BACKEND logical network is available to the host group where the host resides, select the check box next to **BACKEND**.
8. To view advanced settings, click **Advanced**. In the **Advanced Network Adapter Properties** dialog box for an ESX host, you can view the IP subnets and VLANs that are available for a given logical network on the network adapter. By default, for a selected logical network, the IP subnets and VLANs that are scoped to the host group or inherited through the parent host group are assigned to the network adapter.

   Note
   If no IP subnets or VLANs appear in the **Available** or **Assigned** columns, this indicates that no network site exists for the selected logical network that is scoped to the host group or inherited by the host group.

   To view the available IP subnets and VLANs, click a logical network in the **Logical network** list. As mentioned earlier, you must use vCenter Server to configure port groups with the necessary VLANs that correspond to the network sites.

   In the **Logical network** list, if the **Unassigned** option is available, you can view any VLANs that the physical network adapter is connected to, but are not included in a network site. If desired, you can define them in a network site.

To verify virtual networking settings

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, expand **All Hosts**, and then click the host group where the host resides.
3. In the **Hosts** pane, click the host where you want to verify the virtual network settings.
4. On the **Host** tab, in the **Properties** group, click **Properties**.
5. In the *Host Name* **Properties** dialog box, click the **Virtual Networks** tab.
6. Under **Virtual Networking**, click the virtual network that you want to view the properties of.
7. Next to **Logical network**, verify that the logical network that you associated with the

physical network adapter in the previous procedure is listed.

Tip
For a graphical overview of the networking configuration on a host, right-click the host, and then click **View networking**. Hover over an item to view additional information.

To view compliance information for a physical network adapter

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Networking**, and then click **Logical Networks**.
3. On the **Home** tab, in the **Show** group, click **Hosts**.
4. In the **Logical Network Information for Hosts** pane, expand the host, and then click a physical network adapter.
5. In the **Compliance** column, view the compliance status.
   - A value of **Fully compliant** indicates that all subnets and VLANs that are included in the network site are assigned to the network adapter.
   - A value of **Partially compliant** indicates that there is only a partial match between the IP subnets and VLANs that are included in the network site and what is assigned to the network adapter.

     In the details pane, the **Logical network information** section lists the assigned IP subnets and VLANs for the physical network adapter. If an adapter is partially compliant, you can view the reason why in the **Compliance errors** section.
   - A value of **Non compliant** indicates that there are no corresponding IP subnets and VLANs that are defined for the logical network that are assigned to the physical adapter.

See Also

Managing VMware ESX Hosts Overview

Configuring Networking in VMM

How to Configure Host BMC Settings in VMM

You can use the following procedure to configure Baseboard Management Controller (BMC) settings for a managed host in System Center 2012 – Virtual Machine Manager (VMM). If a computer is configured for out-of-band management through a BMC, you can power the host on and off by using the VMM console. The BMC settings are also used for power optimization.

Note
For more information about power optimization, see Configuring Dynamic Optimization and Power Optimization in VMM.

Prerequisites

To complete this procedure, the host must have a BMC installed that supports one of the following out-of-band management protocols:

- Intelligent Platform Management Interface (IPMI) versions 1.5 or 2.0
- Data Center Management Interface (DCMI) version 1.0
- System Management Architecture for Server Hardware (SMASH) version 1.0 over WS-Management (WS-Man)

Although it is not a required prerequisite, you can create a Run As account before you begin this procedure. (You can also create the account during the procedure.) The Run As account must have permissions to access the BMC.

For example, create a Run As account that is named **BMC Administrator**.

Note
You can create Run As accounts in the **Settings** workspace. For more information about Run As accounts, see How to Create a Run As Account in VMM.

To configure BMC settings

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then click **All Hosts**.
3. In the **Hosts** pane, click the host that you want to configure.
4. On the **Host** tab, in the **Properties** group, click **Properties**.
5. In the *Host Name* **Properties** dialog box, click the **Hardware** tab.
6. Under **Advanced**, click **BMC Setting**.
7. To enable out-of-band management, do the following:
   a. Select the **This physical machine is configured for OOB management with the following settings** check box.
   b. In the **This computer supports the specified OOB power management configuration provider** list, click the out-of-band management protocol that the BMC supports.
   c. In the **BMC address** box, enter the IP address of the BMC.
   d. In the **BMC port** box, accept the default. VMM automatically populates the box with the port number for the selected out-of-band management protocol.
   e. Next to the **Run As account** box, click **Browse**, click a Run As account that has permissions to access the BMC, and then click **OK**.

      Note
      If you do not already have a Run As account, click **Browse**, and then in the **Select a Run As Account** dialog box, click **Create Run As Account**.

      For example, if you created the Run As account that is described in the Prerequisites section of this topic, click **BMC Administrator**.
   f. When you are finished, click **OK**.

To power a computer on or off through VMM

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then click **All Hosts**.
3. In the **Hosts** pane, click the host that you want to configure.
4. On the **Host** tab, in the **Host** group, click **Power On** or **Power Off**. (Additional options that are available with out-of-band power management include **Shutdown** and **Reset**.)

   Note
   - If BMC settings are not configured, these settings will not be available.
   - Information about power on and power off events is available in the BMC logs. To view BMC log information for a host, open the host properties, click the **Hardware** tab, and then under **Advanced**, click **BMC Logs**.
   - On HP computers, after the System Even Log is full, logging of new events stop and BMC logs display older events only.

How to Import VMware Templates

You can use the following procedure to import a VMware template to the System Center 2012 – Virtual Machine Manager (VMM) library.

When you import a VMware template to the VMM library, VMM no longer copies the .vmdk file to the library. Instead, VMM copies only the metadata that is associated with the template. Therefore, the VMware template is now dependent on the server that is running VMware vCenter Server. For more information about the new template behavior in VMM, see the “Key Differences in VMware ESX Management from VMM 2008 R2” section of the topic Managing VMware ESX Hosts Overview.

For you to complete this procedure, a VMware template must exist. Make sure that the server that is running vCenter Server, and that contains the template, is under VMM management. For more information, see How to Add a VMware vCenter Server to VMM.

Note
You cannot install VMware Tools through VMM. Therefore, we recommend that you install the tools for Windows-based guest operating systems on the virtual machine before you use vCenter Server to create the template.

To import a template from vCenter Server

1. Open the **Library** workspace.
2. On the **Home** tab, in the **Import** group, click **Import VMware Template**.
3. In the **Import VMware Templates** dialog box, select the check box next to each VMware

template that you want to import, and then click **OK**.

4. To verify that the template was added, in the **Library** pane, expand **Templates**, and then click **VM Templates**.

   In the **Templates** pane, verify that the template appears.

How to Convert VMware Virtual Machines to Hyper-V

You can use the following procedure to convert a VMware virtual machine to a Hyper-V virtual machine through the virtual-to-virtual (V2V) machine conversion process in System Center 2012 – Virtual Machine Manager (VMM). The source virtual machine can be stored in the VMM library or managed by a VMware ESX host.

Before you begin

Before you begin, there are several things you need to be aware of concerning V2V conversions:

- VMM does not support converting VMware Workstations.
- VMM does not support converting VMware virtual machines with virtual hard disks that are connected to an integrated drive electronics (IDE) bus.
- Online V2V conversions are not supported. This means VMware virtual machines must be offline (powered off).
- You must stop any anti-virus applications that are running.
- You must uninstall VMware Tools on the guest operating system of the virtual machine. For information about VMWare Tools, see Overview of VMware Tools.

VMM in System Center 2012 supports the V2V machine conversion of virtual machines that are running on the following versions of VMware ESX:

- ESX/ESXi 3.5 Update 5
- ESX/ESXi 4.0
- ESX/ESXi 4.1
- ESXi 5.1

VMM in System Center 2012 Service Pack 1 (SP1) and in System Center 2012 R2 supports the V2V machine conversion of virtual machines that are running on the following versions of VMware ESX:

- ESX/ESXi 4.1
- ESXi 5.1

You can perform V2V conversions using Microsoft Virtual Machine Converter (MVMC) or by using the Convert Virtual Machine Wizard in VMM. For more information about MVMC, see Microsoft Virtual Machine Converter. To download the MVMC tool, go to Microsoft Virtual Machine

Converter Solution Acceleratorand follow the instructions. To use the Convert Virtual Machine Wizard, complete the following procedure.

For a list of common V2V conversion issues, error messages and resolutions, see Troubleshooting Virtual Machine Conversion Issues

To convert VMware virtual machines to Hyper-V using the Convert Virtual Machine Wizard

1. Open the **VMs and Services** workspace.
2. On the **Home** tab, in the **Create** group, click the **Create Virtual Machine** drop-down arrow, and then click **Convert Virtual Machine**.

   The Convert Virtual Machine Wizard opens.
3. On the **Select Source** page, next to the **Select the virtual machine that you would like to convert** box, click **Browse**.
4. In the **Select Virtual Machine Source** dialog box, click the VMware virtual machine that you want to convert, and then click **OK**.

   Tip

   Verify that the **Virtualization Platform** column indicates **VMware ESX Server**.
5. On the **Select Source** page, click **Next**.
6. On the **Specify Virtual Machine Identity** page, either keep or change the virtual machine name, enter an optional description, and then click **Next**.

   Note

   The virtual machine name identifies the virtual machine to VMM. The name does not have to match the computer name of the virtual machine. However, to avoid confusion, we recommend that you use the same name as the computer name.
7. On the **Virtual Machine Configuration** page, configure the number of processors and assign the amount of memory in megabytes or gigabytes, and then click **Next**.
8. On the **Select Host** page, select a Hyper-V host for placement, and then click **Next**.
9. On the **Select Path** page, do the following, and then click **Next**:
   a. In the **Storage location** box, configure the storage location on the host for virtual machine files. By default, the default virtual machine paths on the target host are listed. To select a different location, click **Browse**, click a folder, and then click **OK**.

      Note

      As a best practice, do not specify a path that is on the same drive as the operating system files.
   b. To add the path to the list of storage locations on the virtual machine host, select the **Add this path to the list of default storage locations on the host** check box.
10. On the **Select Networks** page, select the logical network, the virtual network, and the virtual LAN (VLAN), if applicable, to use for the virtual machine, and then click **Next**.

    Note

The list of available logical networks, virtual networks, and VLANs matches what is configured on the host physical network adapters.

11. On the **Add Properties** page, configure the settings that you want, and then click **Next**.
12. On the **Summary** page, review the settings. Optionally, select the **Start the virtual machine after deploying it** check box. To start the conversion process, click **Create**.

    The **Jobs** dialog box appears to indicate the job status. Verify that the job has a status of **Completed**, and then close the dialog box.
13. To verify that the virtual machine was converted, do the following:
    a. In the **VMs and Services** workspace, locate and then click the Hyper-V host which you selected during placement.
    b. On the **Home** tab, in the **Show** group, click **VMs**.
    c. In the **VMs** pane, verify that the virtual machine appears.

Managing Citrix XenServer Overview

Virtual Machine Manager (VMM) enables you to deploy and manage virtual machines and services across multiple hypervisors, including Citrix XenServer hosts. Through VMM, you can manage the day-to-day operations of XenServer hosts and XenServer pools. These operations include the discovery and management of XenServer hosts and pools, and the ability to create, manage, store, place and deploy virtual machines and services on XenServer hosts. Managing XenServer hosts through VMM also gives you more choice with regard to Linux-based guest operating systems than if you were only managing Hyper-V.

In addition, VMM enables you to make resources from Hyper-V, XenServer and VMware ESX hosts available to private cloud deployments, all from a common user interface and common command-line interface (CLI).

Operating System Requirements

The computers that you want to add as XenServer hosts must meet the requirements that are outlined as follows:

- For System Center 2012 – Virtual Machine Manager or for System Center 2012 SP1 see: **System Requirements: Citrix XenServer Hosts in System Center 2012 and in System Center 2012 SP1**.
- For System Center 2012 R2 Virtual Machine Manager see: **Preparing your environment for System Center 2012 R2 Virtual Machine Manager**.

Note
Through VMM, the XenServer hosts are directly managed. Therefore, there is no interaction between the VMM management server and the Citrix XenCenter server.

Additional Requirements

Make sure that the following additional requirements are met:

- You must have a Dynamic Host Configuration Protocol (DHCP) server available to automatically assign IP addresses for Citrix TransferVMs. The addresses that are assigned by the DHCP server must be accessible from the XenServer host management network.

  Note
  A TransferVM is a template for paravirtual virtual machines that contains Background Intelligent Transfer Service (BITS) and iSCSI servers. The virtual machine is temporary. A TransferVM is created and destroyed on the XenServer host during each transfer and mount operation in XenServer. For example, TransferVMs are used for disk transfers over HTTP.

- If the VMM library servers that the XenServers will use are running Windows Server 2008, you must do the following:

  a. Install Windows Management Framework Background Intelligent Transfer Service 4.0 (BITS 4.0) on each library server. To download BITS 4.0, see Windows Management Framework (Windows PowerShell 2.0, WinRM 2.0, and BITS 4.0).

  b. After you install BITS 4.0, enable the **BITS Compact Server** feature in Server Manager.

  You must have the BITS Compact Server feature enabled to successfully create a new XenServer virtual machine from an existing template or virtual hard disk, or to create a VMM virtual machine template from a XenServer virtual machine.

Supported Features

The following table shows the VMM and XenServer features that are supported when VMM manages XenServer hosts.

Feature	Notes
VMM command shell	The VMM command shell is common across all hypervisors.
Adding XenServer hosts and pools	VMM supports the addition of stand-alone XenServer hosts and XenServer clusters (known as pools) to VMM management. Realize that you must install and configure XenServer before you add the hosts to VMM management. Also, you must create and configure XenServer pools in Citrix XenCenter.
Placement	VMM offers virtual machine placement based on host ratings during the creation, deployment, and migration of XenServer virtual machines. This includes concurrent virtual machine

Feature	Notes
	deployment during service deployment.
Services	You can deploy VMM services to XenServer hosts.
Private clouds	You can make XenServer host resources available to a private cloud by creating private clouds from host groups where XenServer hosts reside. You can configure quotas for the private cloud and for self-service user roles that are assigned to the private cloud. For more information, see Creating a Private Cloud in VMM Overview.
Dynamic Optimization and Power Optimization	You can use the new Dynamic Optimization features with XenServer hosts. For example, VMM can load balance virtual machines on XenServer pools by using Live Migration. Through Power Optimization, you can configure VMM to turn XenServer hosts on and off for power management.
Migration	Supported migration types include the following: • Live Migration between hosts in a managed pool (through Citrix XenMotion) • LAN migration between a host and the library through BITS **Note** TransferVM is used for each virtual hard disk.
Maintenance mode	You can place a XenServer host that is managed by VMM in and out of maintenance mode by using the VMM console.
Library	You can organize and store XenServer virtual machines, virtual hard disks, and VMM templates in the VMM library. VMM supports creating new virtual machines from templates. **Tip** If you store virtual hard disks for XenServer in the VMM library, we

Feature	Notes
	recommend that you open the properties of the .vhd or .vhdx file, and then on the **General** tab, in the **Virtualization platform** list, click **Citrix XENServer Server**. This will help you distinguish which files are for XenServer.
XenServer Templates	XenServer templates are not used by VMM. However, you can use XenCenter to create a virtual machine, and then create a VMM template from the virtual machine.  **Note** To retain paravirtualization properties of a virtual machine, you must create a virtual machine with paravirtualization properties on the XenServer host, and then create a VMM virtual machine template from the virtual machine.
VMM Templates	VMM virtual machine templates are supported with XenServer, with the following restrictions: • The generalization and customization of virtual machines is supported for Windows-based virtual machines only. • You must manually install XenServer Tools (Citrix Tools for Virtual Machines). • When you create a VMM virtual machine template from a XenServer virtual machine, you cannot modify any associated disk images. Although you can modify the settings in the VMM console, when you deploy the template the original images will be attached. You can modify all other properties.
Networking	The new VMM networking management features are supported on XenServer hosts, such as the assignment of logical networks, and the assignment of static IP addresses and MAC addresses to Windows-based virtual machines that are running on XenServer hosts. Be aware that you must create external virtual

Feature	Notes
	networks through XenCenter. VMM recognizes and uses the existing external networks for virtual machine deployment. **Note** VMM uses a single virtual switch to represent all XenServer switches with different VLAN IDs that are bound to a single physical network adapter.
Storage	VMM supports all virtual disk storage repositories that XenServer does. These include the following: • Software iSCSI, Network File System (NFS) virtual hard disk, Hardware host bus adapters (HBAs), and Advanced StorageLink technology • Shared and local storage In addition, VMM supports ISO repositories on an NFS or a Windows File Sharing (Common Internet File System (CIFS)) share. Note the following: • If you want to deploy ISO images from the library to the XenServer host, you must set the permissions on the ISO repository to Read-Write. • You can only attach ISO images from the VMM library. Therefore, in XenCenter, connect to the XenServer host, and then specify a Read-Write share location in the VMM library as the ISO storage repository. **Note** The new VMM storage automation features are not supported for XenServer hosts. All storage must be added to XenServer hosts outside VMM.
Virtual machine management	VMM supports paravirtual (PV) and hardware-assisted virtualization (HVM) virtual machines, with the following restrictions: • Windows-based operating systems will only

Feature	Notes
	run on HVM virtual machines. • If you create a new virtual machine through the VMM console, you can only create HVM virtual machines. • To create a virtual machine with paravirtualization properties from VMM, you must first clone a virtual machine with paravirtualization properties to the library, and then clone and deploy the virtual machine. You cannot create a virtual machine with paravirtualization properties by using the New Virtual Machine wizard to create a virtual machine from an existing virtual hard disk. Typical virtual machine management options are available, such as the use of virtual hard disks and the ability to attach ISO image from the library through an NFS or CIFS share. You can also control the state of the virtual machine, such as start, stop, save state, pause and shut down.
Conversion	In VMM in System Center 2012 and System Center 2012 Service Pack 1 (SP1) only, converting a XenServer virtual machine to a Hyper-V virtual machine is supported by using the physical-to-virtual machine conversion process (P2V conversion). You do not have to remove the Citrix Tools for Virtual Machines before you start the conversion. Realize that VMM only supports the conversion of virtual machines that are running supported Windows-based guest operating systems. To start the P2V process, in the **VMs and Services** workspace, on the **Home** tab, in the **Create** group, click the **Create Virtual Machine** drop-down arrow, and then click **Convert Physical Machine**. **Important** As of System Center 2012 R2, you can no longer convert a XenServer virtual machine to a Hyper-V virtual machine

Feature	Notes
	or perform other P2V conversions in VMM.
Performance and Resource Optimization (PRO)	Monitoring and alerting for XenServer hosts is possible through VMM with the integration of Operations Manager and PRO.

Additional Support Information

- VMM does not support the host-to-host migration of stopped virtual machines (LAN migration) between XenServer and other hosts.
- The Dynamic Memory feature only applies to Hyper-V hosts that are running an operating system that supports Dynamic Memory.
- Update management through VMM is not supported for XenServer hosts. You must use your existing solution to update XenServer hosts.
- The conversion of a bare-metal computer to a virtual machine host, and cluster creation through VMM is not supported with XenServer.

In This Section

Follow these procedures to manage XenServer hosts through VMM.

Procedure	Description
How to Add XenServer Hosts to VMM	Describes how to add a XenServer host or pool to VMM management.
Configuring XenServer Host Properties	Describes the settings that are available in the XenServer host properties. Includes the following subtopics: • How to Configure Network Settings on a Citrix XenServer Host Describes how to configure XenServer host network settings, including how to configure logical network settings. • How to Configure Host BMC Settings in VMM Describes how to configure Baseboard Management Controller (BMC) settings on a host to support power management through VMM.

How to Add XenServer Hosts to VMM

You can use the following procedure to add a Citrix XenServer computer or XenServer pool to System Center 2012 – Virtual Machine Manager (VMM) as one or more managed hosts or host clusters.

Prerequisites

Before you begin this procedure, review the following prerequisites:

- The computers that you want to add must meet the requirements that are outlined as follows:
  - For System Center 2012 – Virtual Machine Manager or for System Center 2012 SP1 see: **System Requirements: Citrix XenServer Hosts in System Center 2012 and in System Center 2012 SP1**.
  - For System Center 2012 R2 Virtual Machine Manager see: **Preparing your environment for System Center 2012 R2 Virtual Machine Manager**.
- If you want to add a XenServer pool, this procedure assumes that you have an existing XenServer pool that you created by using Citrix XenCenter or some other external method.
- When you add a XenServer host, you must specify a Run As account, where the associated account has root credentials on the computers that you want to add. Although it is not a required prerequisite, you can create a Run As account before you begin this procedure. (You can also create the account during the procedure.)

  For example, create a Run As account that is named **XenServer Hosts**.

  Note
  You can create Run As accounts in the **Settings** workspace. For more information about Run As accounts, see How to Create a Run As Account in VMM.

To add a XenServer host or pool

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, click **Servers**.
3. On the **Home** tab, in the **Add** group, click **Add Resources**, and then click **Citrix XenServer Hosts and Clusters**.

   The Add Resource Wizard starts.
4. On the **Server Settings** page, do the following:
   a. In the **Computer name** box, enter the fully qualified domain name, the NetBIOS name or the IP address of the XenServer host. To add a pool of hosts, enter the name or IP address of any XenServer host in the pool. If you specify a name, it must be resolvable by Domain Name System (DNS).

      Note
      If you add a pool, the node that you specify does not have to be the master.

   b. Unless you have changed it on the XenServer host, accept the default TCP port of

5989.

c. Make sure that the **Use certificates to communicate with this host** check box is selected.

d. Next to the **Run As account** box, click **Browse**, click the Run As account that has root credentials on the XenServer, and then click **OK**. (If you do not already have a Run As account, click **Browse**, and then click **Create Run As Account**.)

   For example, if you created the Run As account that is described in the Prerequisites section of this topic, click the **XenServer Hosts** Run As account.

e. In the **Host group** list, click the host group where you want to add the XenServer host or pool.

f. When you are finished, click **Add**.

   VMM discovers the servers and lists them in the lower pane. If you added a pool, the name of the pool is listed together with each host in the pool.

   Note
   The server name that is listed will match the name that the associated certificate is issued to.

g. Verify that the certificate for each host is valid. To do this, click a host, and then click **View certificate**. If you find a host with a certificate that is not valid, click **Remove** to remove it from the list.

h. If all hosts have valid certificates, select the **These certificates have been reviewed and can be imported to the trusted certificate store** check box, and then click **Next**.

5. On the **Summary** page, confirm the settings, and then click **Finish**.

   The **Jobs** dialog box appears to indicate the job status. Make sure that the job has a status of **Completed**, and then close the dialog box. If the job fails, perform the following troubleshooting steps:

   a. Make sure that you can ping the host by the computer name or IP address that you specified in step 4a. If you specified a computer name, make sure that the computer name is resolvable by DNS.

   b. Verify that the supplemental pack is installed correctly on the XenServer host. To do this, open a command prompt with Administrator privileges on the VMM management server, type the following command, where <*HOSTNAME*> is the name of the host, <*ROOT USER*> is the root user on the XenServer host, and <*PASSWORD*> is the password of the root user, and then press ENTER:

      winrm enum http://schemas.citrix.com/wbem/wscim/1/cim-schema/2/Xen_HostComputerSystem -r:https://<HOSTNAME>:5989 -encoding:utf-8 -a:basic -u:<ROOT USER> -p:<PASSWORD> -skipcacheck –skipcncheck

      If it is successful, the command returns information about the host computer. If the command is unsuccessful, the supplemental pack is either not installed or is not functioning correctly.

6. To verify that the host was successfully added, in the **Fabric** pane, expand **Servers**, expand the host group where you added the host, and then click the XenServer host. In the **Hosts** pane, verify that the host status is **OK**.

   Tip
   To view detailed information about host status, right-click a host in the VMM console, and then click **Properties**. On the **Status** tab you can view the health status for the overall health of the host, and the network and XenServer Common Information Model (CIM) state health. Realize that the **Repair all** option does not apply to XenServer hosts.

Configuring XenServer Host Properties

After you add Citrix XenServer hosts to System Center 2012 – Virtual Machine Manager (VMM), you can configure the host properties. You can configure the settings that are described in the following table.

Tab	Settings
General	• View identity and system information for the host. This includes information such as processor information, total and available memory and storage, the operating system, and the type of hypervisor. • Enter a host description. • Configure whether the host is available for placement. • View or change the remote connection port.
Status	Lists health status information for the host. Includes areas such as overall health, network health, and XenServer Common Information Model (CIM) state health. In the **Status** pane, you can also do the following: • View error details. • Refresh the health status. **Note** The **Repair all** option does not apply to XenServer hosts.

Tab	Settings
Management	Enables you to change the credentials that VMM uses to connect to the XenServer host, and to retrieve or view the host certificate. **Note** The account that you specify must have root credentials on the XenServer host.
Hardware	View or modify settings for CPU, memory, storage (including whether the storage is available for placement), network adapters, DVD/CD-ROM drives and Baseboard Management Controller (BMC) settings. • For more information about how to configure network settings, see How to Configure Network Settings on a Citrix XenServer Host. • For more information about how to configure BMC settings, see How to Configure Host BMC Settings in VMM.
Virtual Machine Paths	Shows the virtual machines that reside on the host, together with status information. **Note** The **Add** option to register virtual machines is not supported on a XenServer host.
Reserves	Enables you to override host reserve settings from the parent host group, and configure reserved resources for the host. Configurable resources include CPU, memory, disk space, disk I/O and network capacity.
Storage	Shows storage that is allocated to the host.
Virtual Networks	Enables you to configure virtual networks. For more information about how to configure network settings, see How to Configure Network Settings on a Citrix XenServer Host.
Placement	Enables you to view the virtual machine paths that will be used during virtual machine

Tab	Settings
	placement on the host.
Servicing Windows	Enables you to select servicing windows.
Custom Properties	Enables you to assign and manage custom properties.

In This Section

This section includes detailed information about how to configure network and Baseboard Management Controller (BMC) settings on a managed XenServer host.

Topic	Description
How to Configure Network Settings on a Citrix XenServer Host	Describes how to configure network settings on a XenServer host, and how to view compliance information for physical network adapters on the host.
How to Configure Host BMC Settings in VMM	Describes how to configure BMC settings for a managed host. If a computer is configured for out-of-band management through a BMC, you can power the host on and off from the VMM console.

How to Configure Network Settings on a Citrix XenServer Host

You can use the following procedures to configure network settings on a Citrix XenServer host in System Center 2012 – Virtual Machine Manager (VMM), and to view compliance information for physical network adapters on the host.

To make logical networks available to virtual machines on an external virtual network, you must configure virtual network settings and associate logical networks with the physical network adapter. Compliance information indicates whether all IP subnets and VLANs that are included in the network site that is associated with a logical network are assigned to the physical network adapter.

Prerequisites

Before you begin these procedures, make sure that the following prerequisites are met:

- You must create external virtual networks through Citrix XenCenter. VMM recognizes and uses the existing external virtual networks for virtual machine deployment.

  Note
  VMM uses a single virtual switch to represent all XenServer switches with different VLAN IDs that are bound to a single physical network adapter.
- In the VMM console, you must have already configured the logical networks that you want to associate with the physical network adapter. If the logical network has associated network sites, one or more of the network sites must be scoped to the host group where the XenServer host resides. For more information, see How to Create a Logical Network in VMM.

Note
By default, when you add a host to VMM management, VMM automatically creates logical networks on host physical network adapters that do not have logical networks defined. For a XenServer host, the default behavior is to create logical networks that match the virtual network switch name. For more information about the default behavior, see How to Configure Global Network Settings in VMM.

To associate logical networks with a physical network adapter (for an external virtual network)

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, expand **All Hosts**, and then click the host group where the host resides.
3. In the **Hosts** pane, click the XenServer host that you want to configure.
4. On the **Host** tab, in the **Properties** group, click **Properties**.
5. In the *Host Name* **Properties** dialog box, click the **Hardware** tab.
6. Under **Network Adapters**, click the physical network adapter that you want to configure.
7. Under **Logical network connectivity**, select the check box next to each logical network that you want to associate with the physical network adapter.

   Note
   Be aware that all logical networks are listed here; not just the logical networks that are available to the host group where the host resides.

   For example, if you configured the BACKEND logical network in the Preparing the Fabric in VMM section, and the BACKEND logical network is available to the host group where the host resides, select the check box next to **BACKEND**.
8. To configure advanced settings, click **Advanced**. In the **Advanced Network Adapter Properties** dialog box, you can view and modify the IP subnets and VLANs that are available for a given logical network on the network adapter. By default, for a selected logical network, the IP subnets and VLANs that are scoped to the host group or inherited through the parent host group are assigned to the network adapter.

   Note
   If no IP subnets or VLANs appear in the **Available** or **Assigned** columns, this

indicates that no network site exists for the selected logical network that is scoped to the host group or inherited by the host group. For more information about network sites, see How to Create a Logical Network in VMM and How to Modify or Delete a Logical Network in VMM.

To modify the available IP subnets and VLANs, click a logical network in the **Logical network** list. Then, use the **Add** and **Remove** buttons to configure which IP subnets and VLANs are assigned to the adapter.

Important
Before you enable logical networks with VLANs (other than VLAN 0) on the network adapter, make sure that you have at least one other network adapter that is available for communication between the host and the VMM management server.

In the **Logical network** list, if the **Unassigned** option is available, you can view any VLANs that the physical network adapter is connected to, but are not included in a network site. You can either remove these VLANs from the network adapter, or you can define them in a network site.

9. When you are finished, click **OK** to apply any changes.

To verify or configure virtual networking settings

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, expand **All Hosts**, and then click the host group where the host resides.
3. In the **Hosts** pane, click the host on which you want to verify the virtual network settings.
4. On the **Host** tab, in the **Properties** group, click **Properties**.
5. In the *Host Name* **Properties** dialog box, click the **Virtual Networks** tab.
6. Under **Virtual Networking**, do either of the following:
   - Click an external virtual network that you want to view the properties of. To verify the logical network settings, next to **Logical network**, verify that the logical networks that you associated with the physical network adapter in the previous procedure are listed.
   - Click **Add** to add a new private virtual network. In the **Name** box, enter a name for the virtual network or accept the default, enter an optional description, and then click **OK**.

     Note
     A private virtual network allows communication between virtual machines on the same host but not with the host or with external networks. A private virtual network does not have a virtual network adapter in the host operating system, nor is it bound to a physical network adapter. You can use a private virtual network when you want to isolate virtual machines from network traffic in the host operating system and in the external networks.

Tip

For a graphical overview of the networking configuration on a host, right-click the host, and then click **View networking**. Hover over an item to view additional information.

To view compliance information for a physical network adapter

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Networking**, and then click **Logical Networks**.
3. On the **Home** tab, in the **Show** group, click **Hosts**.
4. In the **Logical Network Information for Hosts** pane, expand the host, and then click a physical network adapter.
5. In the **Compliance** column, view the compliance status.
   - A value of **Fully compliant** indicates that all subnets and VLANs that are included in the network site are assigned to the network adapter.
   - A value of **Partially compliant** indicates that there is only a partial match between the IP subnets and VLANs that are included in the network site and what is assigned to the network adapter.

     In the details pane, the **Logical network information** section lists the assigned IP subnets and VLANs for the physical network adapter. If an adapter is partially compliant, you can view the reason why in the **Compliance errors** section.
   - A value of **Non compliant** indicates that there are no corresponding IP subnets and VLANs that are defined for the logical network that are assigned to the physical adapter.

See Also

Configuring Networking in VMM

How to Configure Host BMC Settings in VMM

You can use the following procedure to configure Baseboard Management Controller (BMC) settings for a managed host in System Center 2012 – Virtual Machine Manager (VMM). If a computer is configured for out-of-band management through a BMC, you can power the host on and off by using the VMM console. The BMC settings are also used for power optimization.

Note

For more information about power optimization, see Configuring Dynamic Optimization and Power Optimization in VMM.

Prerequisites

To complete this procedure, the host must have a BMC installed that supports one of the following out-of-band management protocols:

- Intelligent Platform Management Interface (IPMI) versions 1.5 or 2.0

- Data Center Management Interface (DCMI) version 1.0
- System Management Architecture for Server Hardware (SMASH) version 1.0 over WS-Management (WS-Man)

Although it is not a required prerequisite, you can create a Run As account before you begin this procedure. (You can also create the account during the procedure.) The Run As account must have permissions to access the BMC.

For example, create a Run As account that is named **BMC Administrator**.

Note
You can create Run As accounts in the **Settings** workspace. For more information about Run As accounts, see How to Create a Run As Account in VMM.

To configure BMC settings

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then click **All Hosts**.
3. In the **Hosts** pane, click the host that you want to configure.
4. On the **Host** tab, in the **Properties** group, click **Properties**.
5. In the *Host Name* **Properties** dialog box, click the **Hardware** tab.
6. Under **Advanced**, click **BMC Setting**.
7. To enable out-of-band management, do the following:
   a. Select the **This physical machine is configured for OOB management with the following settings** check box.
   b. In the **This computer supports the specified OOB power management configuration provider** list, click the out-of-band management protocol that the BMC supports.
   c. In the **BMC address** box, enter the IP address of the BMC.
   d. In the **BMC port** box, accept the default. VMM automatically populates the box with the port number for the selected out-of-band management protocol.
   e. Next to the **Run As account** box, click **Browse**, click a Run As account that has permissions to access the BMC, and then click **OK**.

      Note
      If you do not already have a Run As account, click **Browse**, and then in the **Select a Run As Account** dialog box, click **Create Run As Account**.

      For example, if you created the Run As account that is described in the Prerequisites section of this topic, click **BMC Administrator**.
   f. When you are finished, click **OK**.

To power a computer on or off through VMM

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then click **All Hosts**.

3. In the **Hosts** pane, click the host that you want to configure.
4. On the **Host** tab, in the **Host** group, click **Power On** or **Power Off**. (Additional options that are available with out-of-band power management include **Shutdown** and **Reset**.)

   Note
   - If BMC settings are not configured, these settings will not be available.
   - Information about power on and power off events is available in the BMC logs. To view BMC log information for a host, open the host properties, click the **Hardware** tab, and then under **Advanced**, click **BMC Logs**.
   - On HP computers, after the System Even Log is full, logging of new events stop and BMC logs display older events only.

Managing Fabric Updates in VMM

The procedures in this scenario explain how to set up update management in System Center 2012 – Virtual Machine Manager (VMM) and how to perform updates on physical servers that are managed by VMM.

For information about Windows Server Update Service (WSUS) requirements, see the followings:

- For System Center 2012 – Virtual Machine Manager or for System Center 2012 SP1: **System Requirements: Update Management in System Center 2012 and in System Center 2012 SP1**.
- For System Center 2012 R2 Virtual Machine Manager: **Preparing your environment for System Center 2012 R2 Virtual Machine Manager**.

Why should you manage fabric updates through VMM?

Fabric servers include the following physical computers managed by VMM: Hyper-V hosts and Hyper-V clusters, library servers, Pre-Boot Execution Environment (PXE) servers, the Windows Server Update Management (WSUS) server, and the VMM management server.

VMM supports on demand compliance scanning and remediation of the fabric. Administrators can monitor the update status of the servers. They can scan for compliance and remediate updates for selected servers. Administrators also can exempt resources from installation of an update.

VMM supports orchestrated updates of Hyper-V host clusters. When a VMM administrator performs update remediation on a host cluster, VMM places one cluster node at a time in maintenance mode and then installs updates. If the cluster supports live migration, intelligent placement is used to migrate virtual machines off the cluster node. If the cluster does not support live migration, VMM saves state for the virtual machines.

Managing the update server

After you add a WSUS server to VMM, you should not manage the WSUS using the WSUS console. In VMM, an administrator updates the properties of the update server to configure a proxy server for synchronizations and to change the update categories, products, and supported languages that are synchronized by the WSUS server.

If you add the update server to VMM in Single Sockets Layer (SSL) mode, you can update proxy server credentials for synchronization in the update server properties. If the update server is not added to VMM in SSL mode, proxy server credentials are managed in the WSUS Administration Console.

For more information, see How to Update WSUS Settings in VMM.

User roles and update management

In VMM, administrators and delegated administrators manage fabric updates. Only administrators can manage the update server and synchronize updates. Delegated administrators can scan and remediate updates on computers that are within the scope of their user roles. Delegated administrators can use baselines created by administrators and other delegated administrators. But delegated administrators cannot modify or delete baselines created by others.For more information about user roles, see Creating User Roles in VMM.

In This Section

Follow these procedures to install a WSUS update server, add the update server to VMM, configure update baselines, scan computers for compliance, and perform update remediations. The final procedure demonstrates how to orchestrate updates within a Hyper-V host cluster.

Procedure	Description
How to Install a WSUS Server for VMM	Describes requirements for installing a dedicated WSUS server to use with VMM.
How to Add an Update Server to VMM	Describes how to enable update management in VMM by adding a WSUS server to VMM.
How to Configure Update Baselines in VMM	Describes how to edit a built-in update baseline and how to create new updates baselines for your VMM environment.
How to Scan for Update Compliance in VMM	Describes how to scan managed computers for update compliance in **Compliance** view of the VMM console.
Performing Update Remediation in VMM	Describes how to perform update remediations on stand-alone Hyper-V hosts that are

Procedure	Description
	managed by VMM and how to orchestrate updates on a Hyper-V host cluster in VMM.
How to Create and Remove Update Exemptions for Resources in VMM	Describes how to create an update exemption to prevent installation of an update on a resource and how to remove an update exemption and then return the resource to update compliance.
How to Perform On-Demand WSUS Synchronizations in VMM	Describes how to use the **Synchronize** action in the **Fabric** workspace to synchronize updates in VMM.
How to Update WSUS Settings in VMM	Describes how to configure a proxy server for synchronization and how to change the update classifications, products, and supported languages that WSUS synchronizes by updating the properties of the update server in VMM.
How to Integrate Fabric Updates with Configuration Manager	Describes how to configure VMM to use a WSUS server that is part of a Microsoft System Center Configuration Manager environment.
Using Infrastructure Servers in VMM	Describes how to add servers (that are not VMM host servers) as managed computers that support hosting services to support your infrastructure.

How to Install a WSUS Server for VMM

To manage updates in Virtual Machine Manager (VMM), you must either set up a dedicated Windows Server Update Services (WSUS) server or use an existing WSUS server.

Note
To use an existing WSUS server that is deployed in a System Center Configuration Manager environment, see How to Integrate Fabric Updates with Configuration Manager.

You can set up the WSUS server on the VMM management server. However, we recommend setting up the WSUS server on separate system, especially if the VMM management server is managing a large number of computers. If you set up WSUS on a remote server, you must install a WSUS Administration Console on the VMM management server and then restart the VMM service.

If you are using a highly available VMM management server, we recommend that you use a remote WSUS server. With a highly available VMM management server, you must install a WSUS Administration Console on each node of the cluster to enable the VMM service to continue to support update management. Update management in VMM requires a WSUS Administration Console, which includes the respective WSUS Class Library Reference.

This topic covers either a local or remote WSUS server without Secure Sockets Layer (SSL).

Installing WSUS server role on Windows Server 2012 or Windows Server 2012 R2

To set up WSUS on Windows Server 2012 or Windows Server 2012 R2, you need to install the WSUS server role that is integrated with the operating system. When you select the WSUS server role to be installed, Windows automatically selects any other server roles that are required such as Internet Information Services (IIS).

To install the WSUS server role for VMM

1. Decide whether to install WSUS on the VMM management server or on a remote server.
2. Install the WSUS server role on that server. For more information, see Install the WSUS Server Role.

Installing WSUS 3.0 SP2

Before you install the WSUS 3.0 SP2 server, ensure that the server meets all necessary prerequisites as described on the Windows Server Update Services 3.0 SP2 download page.

You must install the Web Server (IIS) role in Windows Server. In addition to the roles services that are added by default, WSUS requires the role services in the following table.

Category	Required role service
Application Development	ASP.NET
Security	Windows Authentication
Performance	Dynamic Content Compression
Management Tools	IIS 6 Management Compatibility

To install a WSUS 3.0 SP2 for VMM

1. Install Windows Server Update Services (WSUS) 3.0 64 Bit with Service Pack 2 (SP2), either on the VMM management server or on a remote server. Download WSUS 3.0 SP2 from the Windows Server Update Services 3.0 SP2 download page.

   In the Windows Server Update Services 3.0 SP2 Setup Wizard, make the following

selections:

- **Full server installation including Administration Console**
- **Create a Windows Server Update Services SP2 Web site**

In the Windows Server Update Services Configuration Wizard, VMM requires the settings in the following table.

Option	Entry
Microsoft Report View 2008	This option is not needed if you install the WSUS server on your VMM management server.
Choose Upstream Server	**Synchronize with Microsoft Update**
Choose Languages **Choose Products** **Choose Classifications**	To limit WSUS synchronization time, you can limit languages, products, and classifications. **Products:** Limit products to the supported range for Hyper-V hosts, library servers, and the VMM management server in VMM. **Classifications:** You can limit classifications as desired, but consider keeping at least **Critical Updates** and **Security Updates**.
Configure Sync Schedule	**Synchronize manually**
Use a proxy server when synchronizing	To be used when synchronizing updates.

2. If you installed the WSUS server on a remote server:
   a. For System Center 2012 – Virtual Machine Manager only: Install a WSUS Administration Console on the VMM management server.
   b. Restart the VMM service on the VMM management server.

   Important
   If you are using a highly available VMM management server with a remote WSUS server, you must install a WSUS Administration Console on each node of the cluster. To avoid an interruption in service while you perform the WSUS Administration Console installation, move the VMM service to another cluster node before you begin installing the console on a cluster node. You can then install the console and restart the computer without any temporary loss of service.
3. For System Center 2012 SP1 only: If the WSUS server is running

Windows Server 2008 R2, then to allow management of VMM servers that are running Windows Server 2012, install the update for Windows Server Update Services 3.0 Service pack 2 (KB2734608).

4. To verify that the WSUS server was installed successfully:
   a. On the WSUS server, click **Start**, click **Administrative Tools**, and then click **Windows Server Update Services**.
   b. In the navigation pane, click the server name to expand it, and then click **Synchronizations**. You can verify that the initial synchronization succeeded.

How to Add an Update Server to VMM

In order to use VMM to manage updates, you can either install a dedicated Windows Server Update Services (WSUS) server or use an existing WSUS server. For instructions on how to install a WSUS server, see How to Install a WSUS Server for VMM. To use an existing WSUS server that is deployed in a System Center Configuration Manager environment, see How to Integrate Fabric Updates with Configuration Manager.

This procedure describes how to add a WSUS server to your VMM environment.

Account requirements To enable update management, you must be a member of the Administrator user role in VMM. You will need an account that has local administrator rights on the WSUS server.

To add a Windows Server Update Server to VMM

1. In the VMM console, open the **Fabric** workspace.
2. On the **Home** tab, in the **Add** group, click **Add Resources**, and then click **Update Server**.

   The **Add Windows Server Update Services Server** dialog box opens.
3. Type in the **Computer name** of the WSUS server.
4. Specify the TCP/IP port that the WSUS website listens on for connections. For WSUS on a computer with Windows Server 2012 or later, use port 8530 (non-SSL) or 8531 (SSL). For earlier versions of Windows, use port 80.
5. Enter credentials for connecting to the WSUS server. The account must have administrator rights on the WSUS server. You can use an existing Run As Account, or create a new one.
6. If necessary, select the **Use Secure Socket Layer (SSL) to communicate with the WSUS server and clients** check box.
7. Click **Add**.

The WSUS server will be added to VMM, followed by initial synchronization of the updates catalog. Depending on how many update classifications and products you chose when you configured the WSUS server, this operation can take a long time, depending on such factors

as network traffic and the load on the WSUS server. To find out the status of the operation, monitor the status of the **Add Update Server** and **Synchronize Update Server** jobs in the **Jobs** window or in the **Jobs** workspace.

Note
After you enable update management in VMM, you can manage the WSUS server through VMM. If you use the WSUS Administrator Console to update WSUS configuration, then these updates will be visible in VMM only after WSUS synchronization.

To verify that the WSUS server was added to VMM successfully:

1. In the **Fabric** workspace, on the **Fabric** pane, expand **Servers**, in System Center 2012 R2 Virtual Machine Manager click **Infrastructure Servers**, and then click **Update Server**. The results pane displays the update server.
2. In the **Library** workspace, on the **Library** pane, expand **Update Catalog and Baselines**, and then click **Update Catalog**. The results pane displays all the available WSUS updates.

After you add the update server to VMM, you can configure a proxy server for synchronization and change the update categories, products, and supported languages that WSUS synchronizes by updating the properties of the update server in VMM. For more information, see How to Update WSUS Settings in VMM.

How to Configure Update Baselines in VMM

After you add a Windows Server Update Services (WSUS) server to VMM, you can prepare to manage updates for the VMM fabric by configuring update baselines. An update baseline contains a set of required updates that is then scoped to an assignment such as a host group, a stand-alone host, a host cluster, a VMM management server, or an infrastructure server (as of System Center 2012 R2 Virtual Machine Manager). Update baselines can be assigned to host groups and to individual computers based on their role in VMM. Update baselines that are assigned to a host group are applied to all stand-alone hosts and host clusters in the host group, as well as the stand-alone hosts and host clusters in child host groups.

During a compliance scan, computers that are assigned to a baseline are graded for compliance with their assigned baselines. After a computer is found noncompliant, an administrator brings the computer into compliance through update remediation.

If a host is moved from one host group to another, the baselines for the new host group are applied to the host, and the baselines for the preceding host group no longer apply - that is, unless the baseline is assigned to both host groups. Explicit baseline assignments to a managed host stay with the host when it is moved from one host group to another. It is only when the baseline is assigned to a host group that baseline assignments get revoked during the move.

You can use two methods to prepare update baselines for remediation:

- Use one of the built-in update baselines that VMM provides: **Sample Baseline for Critical Updates** and **Sample Baseline for Security Updates**.
- Create your own update baseline.

Important
To help you get started with update management, the built-in security and critical baselines provide a starter set of updates in those categories. If you choose to use the built-in baselines, you must maintain them. They are not continuously updated.

The following procedures explain both methods. We recommend that you use the first procedure to update the built-in security baseline before you create your own baseline.

Account requirements To create or configure update baselines, you must be an administrator or delegated administrator in VMM. Delegated administrators can only assign the update baselines to computers that are within the scope of their user role.

Assign Computers to a Built-in Update Baseline

VMM provides two sample built-in updates baselines that you can use to apply security updates and critical updates to the computers in your VMM environment. Before you can use a baseline, you must specify an assignment scope which contains the host groups, host clusters, individual managed computers, or infrastructure servers (as of System Center 2012 R2 Virtual Machine Manager) to which the baseline is applied to. The following procedure explains how to assign computers to the sample security baseline.

To assign computers to a built-in update baseline

1. Open the **Library** workspace.
2. On the **Library** pane, expand **Update Catalog and Baselines**, and then click **Update Baselines**.

   The **Baselines** pane displays the two built-in baselines: **Sample Baseline for Security Updates** and **Sample Baseline for Critical Updates**.
3. On the **Baselines** pane, click **Sample Baseline for Security Updates**.
4. On the **Home** page, in the **Properties** group, click **Properties**.

   The **Properties** dialog box for the **Sample Baseline for Security Updates** opens.

   Note
   On the left of the dialog box, click **Updates** to open the **Updates** page.
5. On the **Updates** page, optionally add or remove update baselines from the baselines that are listed. The **Sample Baseline for Security Updates** includes all security updates. To ensure that all security updates are remediated, do not remove any updates from this baseline.
6. Click **Assignment Scope** to open the **Assignment Scope** page and then, select host groups, host clusters, computers, and infrastructure servers (as of System Center 2012 R2 Virtual Machine Manager) to add to the baseline.

Computers are represented by the roles they perform in VMM. When you select a computer with a role, such as **VMM server**, all the other roles that the computer performs in VMM are selected. For example, if your VMM management server is also a library server, selecting your VMM management server under **VMM Server** causes the same computer under **Library Servers** to be selected.

To apply a baseline to all hosts, select the **All Hosts** root host group.

7. Click **OK** to save your changes.

Create a New Update Baseline

Now that you have experience assigning computers to a built-in update baseline in VMM, try creating a new baseline by using the following procedure.

To create an update baseline in VMM

1. Open the **Library** workspace.
2. On the **Library** pane, expand **Update Catalog and Baselines**, and then click **Update Baselines**.
3. On the **Home** page, in the **Create** group, click **Baseline**.

   The **Update Baseline Wizard** starts.
4. On the **General** page, enter a name (for example, **Critical Updates for Hyper-V Hosts**) and a description for the update baseline. Click Next to proceed to the **Updates** page.
5. On the **Updates** page, add the updates that you want to include in the baseline.

   For example, to add critical updates for your Hyper-V hosts:

   a. Click **Add**.

   b. In the search box, type **critical updates** to filter the selection.

   c. Select each critical update that you want to apply to your Hyper-V hosts.

   Tip
   To select more than one update, hold down the CTRL key while you click the updates. To select a set of consecutive updates, click the first update, press and hold down the Shift key, and then click the last update in the set.

   d. Click **Add**.

   Click **Next** to proceed to the **Assignment Scope** page.
6. On the **Assignment Scope** page, expand **Host Groups** and **Infrastructure** (as of System Center 2012 R2 Virtual Machine Manager). **Host Groups** lists all host groups, standalone hosts and clusters. **Infrastructure** lists all VMM role servers and any infrastructure servers. Select the items that you want to apply the baseline to. You can apply a baseline to computers that are performing any of the following roles in VMM:
   - Host groups or individual hosts
   - Library servers

- PXE servers
- Update server
- VMM management server

Click Next to proceed to the **Summary** page.

7. On the **Summary** page, review your settings, and then click **Finish**.

   If any of the selected updates require that you accept a Microsoft license agreement, the **Microsoft License Terms** dialog box opens.

8. To start installing the updates, after you review the license terms, click **Accept** if you accept the license terms.

   Note
   If multiple updates require a license agreement, VMM prompts for acceptance of each license.

To verify that the update baseline was created successfully, on the **Library** pane, expand **Updates and Baselines Catalog**, and then click **Baselines**. The results pane should display the new baseline.

See Also

Using Infrastructure Servers in VMM

How to Scan for Update Compliance in VMM

After you assign computers to an update baseline in VMM, you can scan the computers to determine their compliance status for the baselines.

When a computer is scanned for compliance, WSUS checks each update in the assigned update baselines to determine whether the update is applicable and, if the update is applicable, whether the update has been installed. After a compliance scan, for every computer, each update has a compliance status of **Compliant**, **Non Compliant**, **Error**, **Pending Reboot**, or **Unknown**. You can view compliance properties for additional information.

The compliance scan focuses only on the updates that the administrator has identified as important by adding them to a baseline. That enables organizations to monitor for compliance for what is deemed important for their organization.

The following changes can cause an **Unknown** update status for a computer, and should be followed by a scan operation to access the computer's compliance status:

- A host is moved from one host group to another host group.
- An update is added to or removed from a baseline that is assigned to a computer.
- The computer is added to the scope of a baseline.

Important

You should perform all updates in **Compliance** view. The **Scan** and **Remediate** actions also are available in **Fabric Resources** view. However, if you scan and remediate updates in **Fabric Resource** view, you cannot see the results of the operations.

To display Compliance view in the Fabric workspace

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, click **Servers**.
3. On the **Home** tab, in the **Show** group, click **Compliance**.

   The results pane displays the compliance status of the computers in the VMM fabric. Because you have not yet scanned the computers for compliance, the computers that you added to a baseline have a compliance status of **Unknown** and an operational status of **Pending Compliance Scan**.

To scan computers for compliance

1. In **Compliance** view of the **Fabric** workspace, select the computers that you want to scan.
2. On the **Home** tab, in the **Compliance** group, click **Scan**.

   While the scan is in progress, the compliance status changes to **Unknown**. After the compliance scan completes, the computer's compliance status of each update is **Compliant**, **NonCompliant**, or **Error**. To bring noncompliant computers into compliance, you will perform update remediations in VMM.

Performing Update Remediation in VMM

The operation of bringing a managed computer into compliance is known as *update remediation*. In System Center 2012 – Virtual Machine Manager (VMM), you can choose to remediate all update baselines that are assigned to a computer, all noncompliant updates in a single update baseline, or a single update.

The procedures in this section describe how to perform update remediation on virtual machine hosts by using VMM. The first procedure remediates all updates on a single stand-alone host. The second procedure describes how to orchestrate rolling updates of the cluster nodes.

Account requirements To perform update remediation, you must be an administrator or a delegated administrator in VMM. Delegated administrators can only remediate updates for computers that are within the scope of their user role.

Prerequisites

Before you can perform these procedures, you must have set up update management in VMM. For more information, see Managing Fabric Updates in VMM.

In This Section

Follow these procedures to perform updates on stand-alone Hyper-V hosts and on a Hyper-V host cluster.

Procedure	Description
How to Remediate Updates on a Stand-Alone Hyper-V Host in VMM	Describes how to install updates on noncompliant Hyper-V hosts.
How to Perform Rolling Updates on a Hyper-V Host Cluster in VMM	Describes how to perform rolling orchestrate update remediation on a Hyper-V host cluster.
How to Remediate Updates on Infrastructure Servers in VMM	Describes how to install updates on infrastructure servers in System Center 2012 R2 Virtual Machine Manager.

How to Remediate Updates on a Stand-Alone Hyper-V Host in VMM

Use the following procedure to remediate updates for stand-alone Hyper-V hosts that are managed by VMM. You can also orchestrate updates of a managed Hyper-V host cluster in VMM. For information, see How to Perform Rolling Updates on a Hyper-V Host Cluster in VMM.

Note

The **Remediate** action is only available after you install a WSUS server for VMM, enable update management, create and assign update baselines for computers managed by VMM, and scan the computers for compliance. For more information, see Managing Fabric Updates in VMM.

To remediate updates for a Hyper-V host in VMM

1. Display **Compliance** view for the managed computers:
   a. Open the **Fabric** workspace.
   b. In the **Fabric** pane, click **Servers**.
   c. On the **Home** tab, in the **Show** group, click **Compliance**.
2. Select the computers that you want to remediate. Click a computer to display all the baselines checked for that computer.

   The system may be compliant for some baselines and not complaint for others.You can select a single update baseline or a single update within a baseline.
3. On the **Home** tab, in the **Compliance** group, click **Remediate**. (The **Remediate** task is only available when the selected objects are noncompliant.)

The **Update Remediation** dialog box opens.

4. Optionally select or clear update baselines or individual updates to determine which updates to remediate. If you selected a computer to remediate, all updates are initially selected.
5. If you prefer to restart the computers manually after remediation completes instead of letting the wizard do that, select the **Do not restart the servers after remediation** check box.

   By default, the wizard restarts the computer after installing updates if any of the updates requires a restart. If you choose not to restart the servers after remediation, and any updates require a restart, the operational status of the computer changes to **Pending Machine Reboot** after the remediation. The updates will not be activated until you restart the computer.

   Note
   If you choose to manually restart computers after installing updates, that status of the computers will remain **Pending Reboot** until after you scan the computer for updates again. VMM does not scan computers to assess their update compliance status during refreshes.
6. Click **Remediate** to start update remediation.

How to Perform Rolling Updates on a Hyper-V Host Cluster in VMM

Use the following procedure to orchestrate rolling updates of a Hyper-V host cluster that is managed by System Center 2012 – Virtual Machine Manager (VMM). VMM rolls through the host cluster, remediating one cluster node at a time. If a cluster node is compliant, VMM bypasses that node.

Before VMM begins remediating a host in a cluster, it places the host in maintenance mode. You have the option of migrating all virtual machines to other hosts in the cluster. If you do not select this option, VMM saves state and does not migrate virtual machines.

Note
The **Remediate** action is only available after you install a WSUS server for VMM, enable update management, create update baselines for computers managed by VMM, and scan the computers for compliance. For more information, see Managing Fabric Updates in VMM.

To perform rolling update remediation on a Hyper-V host cluster

1. Display **Compliance** view for the managed computers:

a. Open the **Fabric** workspace.
b. In the **Fabric** pane, click **Servers**.
c. On the **Home** tab, in the **Show** group, click **Compliance**.

2. On the **Home** tab, in the **Compliance** group, click **Remediate**. (The **Remediate** task is only available when the selected objects are noncompliant.)

   The **Update Remediation** dialog box opens.

3. In the resource list, select the host cluster by its cluster name.

   If you select the cluster by its cluster name, VMM assumes you want to orchestrate remediation of the hosts in the cluster, and displays cluster remediation options. If you select individual hosts in the cluster, VMM assumes that you want to update them as you would a stand-alone host, and does not display cluster remediation options.

4. If you prefer to restart the computers manually after remediation completes if any updates require a restart, select the **Do not restart the servers after remediation** check box.

   Note
   If you choose to manually restart computers after installing updates, that status of the computers will remain **Pending Reboot** until after you scan the computer for updates again. VMM does not scan computers to assess their update compliance status during refreshes.

5. Select the **Allow remediation of clusters with nodes already in maintenance mode check box** if you want to bypass maintenance mode.

   By default, VMM places each host in maintenance mode before it remediates updates on the host.

6. Specify **Live migration** to remove virtual machines from a host before performing update remediation or **Save state** to shut down virtual machines and proceed with remediation.
7. Click **Remediate** to start update remediation on the host cluster.

You can watch the status of the remediation in the **Jobs** window or the **Jobs** workspace.

After the remediation completes successfully, and no reboot is pending for any machine, the compliance status of each node in the host cluster changes to **Compliant**.

Note
If any computer has a **Machine Reboot Pending** status, restart the computer to complete the update installation and bring the computer into compliance.

How to Remediate Updates on Infrastructure Servers in VMM

Use the following procedure to remediate updates for infrastructure servers that are managed by System Center 2012 R2 Virtual Machine Manager.

Note

The **Remediate** action is only available after you install a WSUS server for VMM, enable update management, create and assign update baselines for computers managed by VMM, and scan the computers for compliance. For more information, see Managing Fabric Updates in VMM.

To remediate updates for infrastructure in VMM

1. Display the **Compliance** view for the managed computers:
   a. Open the **Fabric** workspace.
   b. In the **Fabric** pane, click **Servers**.
   c. On the **Home** tab, in the **Show** group, click **Compliance**.
2. Select the computers that you want to remediate. Click a computer to display all the baselines checked for that computer.

   The system may be compliant for some baselines and not complaint for others.You can select a single update baseline or a single update within a baseline.
3. On the **Home** tab, in the **Compliance** group, click **Remediate**. (The **Remediate** task is only available when the selected objects are noncompliant.)

   The **Update Remediation** dialog box opens.
4. Optionally select or clear update baselines or individual updates to determine which updates to remediate. If you selected a computer to remediate, all updates are initially selected.
5. If you prefer to restart the computers manually after remediation completes instead of letting the wizard do that, select the **Do not restart the servers after remediation** check box.

   By default, the wizard restarts the computer after installing updates if any of the updates requires a restart. If you choose not to restart the servers after remediation, and any updates require a restart, the operational status of the computer changes to **Pending Machine Reboot** after the remediation. The updates will not be activated until you restart the computer.

   Note

   If you choose to manually restart computers after installing updates, that status of the computers will remain **Pending Reboot** until after you scan the computer for updates again. VMM does not scan computers to assess their update compliance status during refreshes.
6. Click **Remediate** to start update remediation.

How to Create and Remove Update Exemptions for Resources in VMM

The procedures in this topic explain how to create an update exemption that prevents an update from being installed on a server in VMM and how to remove the exemption so that the update can be installed in the next update remediation.

When an administrator creates an update exemption for a managed computer, the computer remains accountable to an assigned baseline while it is exempted from a particular update in the baseline.

The most common reason for creating an update exemption is that a specific update has placed a managed computer in an unhealthy state. The administrator uninstalls the update, which returns the computer to a healthy state, and wants to prevent the update from being reinstalled until the issues can be identified and resolved so that the update can be installed without placing the computer in an unhealthy state.

Because the update was removed out of band, the computer's update status in VMM remains **Compliant** until the computer is again scanned for update compliance. The next scan will change the computer's status to **Non Compliant**. To prevent an accidental reinstallation of that update before the issues are resolved, and to provide a valid business justification, the administrator adds an update exemption to the baseline. After the issues are resolved on the computer, the administrator removes the exemption so that the update will be installed during the next update remediation.

To create an update exemption for a resource

1. Open the **Fabric** workspace.
2. Display **Compliance** view of the VMM fabric. To display **Compliance** view, on the **Home** tab, in the **Show** group, click **Compliance**.
3. On the **Fabric** pane, expand **Servers**, navigate to the server that is to be exempted from the update, and click the server to select it.

   The results pane displays the update baselines that have been assigned to the server.
4. In the results pane, expand the update baseline that contains the update from which you want to exempt the server. Then click the update to select it.
5. On the **Home** tab, in the **Compliance** group, click **Compliance Properties**.

   The **Compliance Properties** dialog box opens.
6. Select the update or updates to include in the exemption and then click **Create** to open the **Create Exemption** dialog box.
7. In **Notes**, enter information about the reason, intended duration of the exemption, contact person, and so forth. For example, you might enter the following notes: "Exempt through 03/15/2012 to resolve issues with MyService.exe interactions."
8. Click **Create**.

   In **Compliance Properties** dialog box, the status of the update or updates changes to

Exempt. The update will not be applied to the resource during update remediations until the exemption is removed.

After you remove an update exemption from a resource, you should scan the resource for compliance and then perform update remediation to bring the resource back into a compliant state. The following procedure explains how to perform this process.

To remove an update exemption from a resource

1. Open the **Fabric** workspace.
2. On the **Home** tab, in the **Show** group, click **Compliance**.
3. On the **Fabric** pane, expand **Servers**, navigate to the server for which the exemption was created.
4. In the results pane, expand the update baseline that contains the exemption, and then in the **Compliance** group, click **Compliance Properties**.
5. In the **Compliance Properties** dialog box, select the exemption or exemptions to be removed and click **Delete** and then click **Yes** to confirm.

   After the exemption is removed, the status of the update changes to **Unknown**. You should perform a compliance scan on the resource to update the compliance status, and then perform update remediation to bring the resource into compliance.
6. Click **OK** to close the **Compliance Properties** dialog box.
7. To perform a compliance scan on a server, in the results pane, click the server to select it. Then, on the **Home** tab, in the **Compliance** group, click **Scan**.

   The statuses of the update, the update baseline, and the server change to **Non Compliant**.
8. To return the server to a **Compliant** state, in the results pane, select the update, the update baseline, or the server that is in a **Non Compliant** state. Then, on the **Home** tab, in the **Compliance** group, click **Remediate**. For more information about performing an update remediation, see Performing Update Remediation in VMM.

How to Perform On-Demand WSUS Synchronizations in VMM

Use this procedure to perform on-demand update synchronization for a Windows Server Update Services (WSUS) server in VMM. To get updates, the WSUS server contacts Microsoft Update. WSUS determines if any new updates have been made available since the last synchronization. WSUS then downloads the new metadata. Then VMM imports the changes into the VMM update catalog.

When the update server is added to VMM, an initial synchronization is performed. VMM does not perform automatic synchronizations after that. You should perform on-demand synchronizations

on a schedule that meets your organization's needs. Typically an organization synchronizes updates at least every 15-30 days, in accordance with Microsoft security and update release cycles.

Important
After you add a WSUS server to VMM, you should only manage the WSUS server in VMM. VMM does not synchronize settings that are entered in the WSUS Administration Console with those that are entered in the update server properties. In VMM, update the properties of the update server to configure a proxy server for synchronizations and to change the update categories, products, and supported languages that are synchronized by the WSUS server. For more information, see How to Update WSUS Settings in VMM.

How to Synchronize Updates in VMM

1. Open the **Fabric** workspace.
2. On the **Fabric** pane, expand **Servers**, and then click **Update Server**.
3. On the **Update Server** tab, in the **Update Server** group, click **Synchronize**.

After the synchronization is completed, you can view all new updates in the **Library** workspace under **Update Catalog and Baselines**; you can add any update to baselines. To find out how many new updates were downloaded, how many updates expired, and how many updates were revised during synchronization, view job details for the **Synchronize Update Server** job in the **Jobs** workspace or the **Jobs** window.

How to Update WSUS Settings in VMM

Use the following procedure to update the properties of the Windows Server Update Services (WSUS) server that is used for fabric updates in VMM. In VMM, you update the properties of the update server to configure a proxy server for use during synchronizations and to change the update categories, products, and supported languages that are synchronized by the WSUS server.

Important
After you add a WSUS server to VMM, you should only manage the WSUS server in VMM.

To update the properties of the Windows Server Update Server in VMM

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Servers**, and then click **Update Server** to display the **Update Server** tab on the ribbon.
3. On the **Update Server** tab, in the **Properties** group, click **Properties**.

4. On the **Proxy Server** tab, configure WSUS to use a proxy server when synchronizing updates, or update the port for a proxy server that is already in use.
5. On the **Update Classifications** tab, select each update classification that you want to synchronize.
6. On the **Products** tab, select each product to include in update synchronizations.
7. On the **Languages** tab, select each supported language to include in update synchronizations.
8. Click **OK** to apply any changes you make.

Tip

To manually synchronize updates in VMM, in the **Fabric** workspace, on the **Fabric** pane, expand **Servers**, and then click **Update Server**. Then, on the **Update Server** tab, in the **Update Server** Group, click **Synchronize**.

How to Integrate Fabric Updates with Configuration Manager

VMM supports using a WSUS server that is part of a Configuration Manager environment. This will also enable you to use the reporting capabilities of Configuration Manager to provide compliance information.

If you use an existing WSUS server from a Configuration Manager environment, changes to configuration settings for the WSUS server (for example, update classifications, languages, and proxy settings) should only be made from Configuration Manager. The VMM administrator can view the configuration settings from the VMM console, but cannot make changes.

Note

For VMM, the synchronization schedule is always on-demand, regardless of the setting specified in Configuration Manager.

Before you perform any configuration steps for update management in VMM, you should first configure the Configuration Manager environment.

The following procedure contains an overview of the steps you need to perform in Configuration Manager. For more information, refer to the following Configuration Manager documentation:

- For Configuration Manager 2007 R2:
  - Software Updates in Configuration Manager
  - Reporting in Configuration Manager
- For System Center 2012 Configuration Manager:
  - Software Updates in Configuration Manager
  - Reporting in Configuration Manager

To configure Configuration Manager to share a WSUS server with VMM

1. In Configuration Manager, create a collection. This collection will contain all the computers that VMM will manage.
2. To the collection, add the computers that VMM will manage. This includes all computers for which VMM will perform update management. This includes computers such as the following:
   - Virtual machine hosts
   - Library servers
   - VMM management server
   - PXE servers
   - The WSUS server
3. Exclude this collection from any software update deployments delivered by Configuration Manager to ensure that VMM controls update management of those computers.

   Note

   You will still be able to view compliance information for this collection in Configuration Manager reports.
4. If you want to include VMM compliance information in Configuration Manager reports, create an update group in Configuration Manager that contains all the updates against which you want to measure compliance for the computers managed by VMM.

   Important

   You are creating this update group only to provide reporting capabilities. Do not deploy this update group to the computers managed by VMM.

To configure VMM to use a WSUS server shared with Configuration Manager

1. Add the WSUS server to VMM by following the steps in How to Add an Update Server to VMM.
2. After you have added the WSUS server to VMM, open the Fabric workspace, expand **Servers**, and click **Update Server**, and then select the update server.
3. On the **Update Server** tab, in the **Properties** group, click **Properties**.
4. On the **General** page, ensure that the **Allow Update Server configuration changes** check box is not selected, and then click **OK**.

For more information about configuring update management, see Managing Fabric Updates in VMM.

Creating and Deploying Virtual Machines and Services in VMM

The following topics provide information to help you create, deploy, and manage private clouds, virtual machines, and services in System Center 2012 – Virtual Machine Manager (VMM).

- Creating a Private Cloud in VMM Overview
- Configuring Self-Service in VMM Overview
- Creating and Deploying Virtual Machines in VMM
- Creating Profiles and Templates in VMM
- Creating and Deploying Services in VMM
- Rapid Provisioning of Virtual Machines Using SAN Copy Overview
- Configuring Virtual Machine Settings in VMM
- Creating Virtual Machine Role Templates by Using VMM and Windows Azure Pack

For an overview of VMM, see Overview of System Center 2012 - Virtual Machine Manager.

Creating a Private Cloud in VMM

A private cloud is a cloud that is provisioned and managed on-premises by an organization. The private cloud is deployed by using an organization's own hardware to leverage the advantages of the private cloud model. By using VMM, an organization can manage the private cloud definition and can manage access to the private cloud and the underlying physical resources. This section provides an overview of a private cloud architecture, and procedures for creating a private cloud from one or more host groups from a VMware resource pool in System Center 2012 – Virtual Machine Manager (VMM). Use the following procedures to create and manage a private cloud:

- How to Create a Private Cloud from Host Groups
- How to Create a Private Cloud from a VMware Resource Pool
- How to Increase the Capacity of a Private Cloud
- How to Delete a Private Cloud

Creating a Private Cloud in VMM Overview

A private cloud is a cloud that is provisioned and managed on-premises by an organization. The private cloud is deployed by using an organization's own hardware to leverage the advantages of the private cloud model. By using VMM, an organization can manage the private cloud definition and can manage access to the private cloud and the underlying physical resources.

In VMM, a private cloud provides the following benefits:

- **Self service**—Administrators can delegate management and usage of the private cloud while they retain the opaque usage model. Self-service users do not have to ask the private cloud provider for administrative changes except to request increase capacity and quotas as their requirements change.
- **Resource pooling**—Through the private cloud, administrators can collect and present an aggregate set of resources, such as storage and networking resources. Resource usage is limited by the capacity of the private cloud and by user role quotas.
- **Opacity**—Self-service users have no knowledge of the underlying physical resources.
- **Elasticity**—Administrators can add resources to a private cloud to increase the capacity.
- **Optimization**—Usage of the underlying resources is continually optimized without affecting the overall private cloud user experience.

You can create a private cloud from either of the following sources:

- Host groups that contain resources from Hyper-V hosts, VMware ESX hosts and Citrix XenServer hosts
- A VMware resource pool

During private cloud creation, you select the underlying fabric resources that will be available in the private cloud, configure library paths for private cloud users, and set the capacity for the private cloud. Therefore, before you create a private cloud, you should configure the fabric resources, such as storage, networking, library servers and shares, host groups, and hosts. For information about how to configure the fabric and add hosts to VMM management, see the following sections:

- Preparing the Fabric in VMM
- Adding and Managing Hyper-V Hosts and Host Clusters in VMM
- Managing VMware ESX and Citrix XenServer in VMM

Example Scenario Overview

In the example scenarios, a private cloud that is named **Finance** is created from resources in configured host groups. A private cloud that is named **Marketing** is created from a VMware resource pool.

The following table summarizes the examples that are used.

Note

The example resource names and configuration are used to help demonstrate the concepts. The examples build from examples that are used in the "Preparing the Fabric in VMM" section. You can adapt them to your test environment.

Private cloud	Resource
Finance (Private cloud that is created from host groups)	Host groups: **Seattle\Tier0_SEA**, **Seattle\Tier1_SEA**, **New York\Tier0_NY**, **New York\Tier1_NY**

Private cloud	Resource
	Logical network: **BACKEND** Load balancer: **LoadBalancer01.contoso.com** Virtual IP profile: **Web tier (HTTPS traffic)** Storage classification: **GOLD** and **SILVER** Read-only library shares: **SEALibrary** and **NYLibrary** Stored virtual machine path: **VMMServer01\Finance\StoredVMs** Capability profile: **Hyper-V**
Marketing (Private cloud that is created from a VMware resource pool)	VMware resource pool: **Resource pool 1** Logical network: **BACKEND** Load balancer: **LoadBalancer01.contoso.com** Virtual IP profile: **Web tier (HTTPS traffic)** Read-only library shares: **SEALibrary** and **NYLibrary** Stored virtual machine path: **VMMServer01\Marketing\StoredVMs** Capability profile: **ESX Server**

How to Create a Private Cloud from Host Groups

You can use this procedure to create a private cloud from resources in one or more host groups in System Center 2012 – Virtual Machine Manager (VMM). You can create a private cloud from host groups that contain a single type of host, or from host groups that contain a mix of Hyper-V, VMware ESX, and Citrix XenServer hosts.

Note
You can also create a private cloud from a VMware resource pool. For more information, see How to Create a Private Cloud from a VMware Resource Pool.

Account requirements You must perform this procedure as a member of the Administrator user role or as a member of the Delegated Administrator user role where the administrative scope includes the host groups that you want to use for the private cloud.

Prerequisites

Before you create a private cloud, make sure that the following prerequisites are met:

- Configure the fabric and add hosts to VMM management by using the procedures in the following sections:
  - Preparing the Fabric in VMM

    Note
    The fabric resource examples in this procedure use examples from the "Preparing the Fabric in VMM" section.
  - Adding and Managing Hyper-V Hosts and Host Clusters in VMM
  - Managing VMware ESX and Citrix XenServer in VMM
- If you want to provide self-service users the ability to store virtual machines to the VMM library, create a library share, or create a folder in a library share that will serve as the storage location. Realize that self-service users must have the **Store and re-deploy** permission to store their virtual machines.

  Important
  The library share location that you designate for stored virtual machines must be different from the shares that you designate as read-only resource locations for the private cloud. Also, the path or part of the path must be unique when compared to the user role data path that is specified for a self-service user role. For example, if the user role data path for a self-service user role is \\VMMServer01\Finance, you cannot create a stored virtual machine path of \\VMMServer01\Finance\StoredVMs. However, if the user role data path is \\VMMServer01\Finance\FinanceUserRoleData, you could specify \\VMMServer01\Finance\StoredVMs as the stored virtual machine path, as the full path is unique. You could also create entirely separate library shares.

  Realize that you configure the stored virtual machine path and read-only library shares when you run the Create Cloud Wizard. The self-service user role data path is specified when you create a self-service user role or modify the properties of a self-service user role.

  For example, outside VMM, create the **\\VMMServer01\Finance\StoredVMs** path, and then add the **VMMServer01\Finance** library share to the VMM library.
- If you want to assign read-only shares to the private cloud, where administrators can store read-only resources such as .iso files that they want to make available to self-service users, make sure that one or more library shares exists that you can assign as the read-only library shares. Realize that self-service users must have the **Author** permission to access the resources.

  Important
  The library shares that you designate as read-only resource locations for the private cloud must be unique when compared to the library share or shares that are used for stored virtual machines and for the user role data path that is specified for a self-service user role.

For example, you can use the **SEALibrary** and the **NYLibrary** library shares.

Note

For more information about self-service user permissions, see How to Create a Self-Service User Role in VMM.

To create a private cloud from host groups

1. Open the **VMs and Services** workspace.
2. On the **Home** tab, in the **Create** group, click **Create Cloud**.

   The Create Cloud Wizard opens.
3. On the **General** page, enter a name and optional description for the private cloud, and then click **Next**.

   For example, enter the name **Finance**, and the description **Private cloud for virtual machines and services in the finance department**.
4. On the **Resources** page, do the following:
   a. Click **Host groups**.
   b. Select the check box next to each host group that you want to add, and then click **Next**.

      For example, select the check boxes next to **Seattle\Tier0_SEA**, **Seattle\Tier1_SEA**, **New York\Tier0_NY** and **New York\Tier1_NY**, and then click **Next**.
5. On the **Logical Networks** page, select the check box next to each logical network that you want to make available to the private cloud, and then click **Next**. Only logical networks that are associated with physical network adapters on hosts in the selected host groups appear in the list.

   For example, select the check box next to **BACKEND**, and then click **Next**.
6. On the **Load Balancers** page, select the check box next to each load balancer that you want to make available to the private cloud, and then click **Next**. Only load balancers that are associated with the selected host groups appear in the list.

   For example, select the check box next to **LoadBalancer01.contoso.com**, and then click **Next**.

   Tip

   In the Create Cloud Wizard, if you do not have a fabric resource configured, you can click **Next** to move to the next page. Realize that you can add or remove private cloud resources and modify other private cloud settings after you complete the wizard. To do this, right-click the private cloud, and then click **Properties**.
7. On the **VIP Profiles** page, select the check box next to each VIP template that you want to make available to the private cloud, and then click **Next**.

   For example, select the check box next to **Web tier (HTTPS traffic)**, and then click **Next**.
8. On the **Storage** page, select the check box next to each storage classification that you

want to make available to the private cloud, and then click **Next**. Only storage classifications for storage pools that are assigned to the selected host groups appear in the list.

For example, select the check boxes next to **GOLD** and **SILVER**, and then click **Next**.

Note

If you do not have storage that is managed by VMM, click **Next**.

9. On the **Library** page, do the following:
   a. Next to the **Stored VM path** box, click **Browse**. In the **Select Destination Folder** dialog box, expand the library server, click the library share or the folder in a library share that you want to use as the location for self-service users to store virtual machines, and then click **OK**.

      For example, if you created the folder that is described in the Prerequisites section of this topic, click the **StoredVMs** folder in the **VMMServer01\Finance** library share.
   b. In the **Read-only library shares** area, click **Add**, select the check box next to one or more library shares where administrators can provide read-only resources to cloud users, click **OK**, and then click **Next**.

      For example, select the check box next to the **SEALibrary** library share and the **NYLibrary** library share.
10. On the **Capacity** page, set capacity limits for the private cloud, and then click **Next**. You can either accept the default values, or clear the **Use Maximum** check boxes and set quotas for the following resources:

Quota Type	Description
Virtual CPUs	Sets a limit on processing capacity within the private cloud that is equivalent to the capacity that can be provided by a specified number of CPUs. Applied against running virtual machines. Setting a CPU quota does not guarantee contiguous capacity; it only guarantees total CPU capacity available among hosts in the private cloud.
Memory	Sets a quota on memory (in gigabytes) that is available for virtual machines that are deployed on the private cloud. Applied against running virtual machines only. Setting a memory quota does not guarantee contiguous capacity. For example, the private cloud might have available 2 GB of memory on one host and 2 GB of memory on another.

Storage	Sets a quota on storage capacity (in gigabytes) that is available to virtual machines that are deployed on the private cloud. For dynamic virtual hard disks, quota calculations are based on maximum size.
Custom quota (points)	Sets a quota on virtual machines that are deployed on the private cloud based on total quota points that are assigned to the virtual machines through their virtual machine templates. Quota points are an arbitrary value that can be assigned to a virtual machine template based on the anticipated size of the virtual machines. Custom quotas are provided for backward compatibility with self-service user roles that were created in VMM 2008 R2.
Virtual machines	Limits the total number of virtual machines that can be deployed on the private cloud.

11. On the **Capability Profiles** page, select the check box next to each virtual machine capability profile that you want to add, and then click **Next**. Select the capability profiles that match the type of hypervisor platforms that are running in the selected host groups. The built-in capability profiles represent the minimum and maximum values that can be configured for a virtual machine for each supported hypervisor platform.

    For example, select the check box next to **Hyper-V**, click **OK**, and then click **Next**.

    Tip

    In the Library workspace, you can also create custom capability profiles to limit the resources that are used by virtual machines that are created in the private cloud. To view the settings that are associated with a built-in capability profile or to create a custom capability profile, open the **Library** workspace, expand **Profiles**, and then click **Capability Profiles**. You can view the properties of a capability profile, or on the **Home** tab, in the **Create** group, click **Create**, and then click **Capability Profile** to create a new one.

12. On the **Summary** page, confirm the settings, and then click **Finish**.

    The **Jobs** dialog box appears. Make sure that the job has a status of **Completed**, and then close the dialog box.

13. To verify that the private cloud was created, in the **VMs and Services** workspace, expand **Clouds**.

    The private cloud that you created should appear.

Tip

To view information about used and available resources in the private cloud, in the **VMs and Services** workspace, expand **Clouds**, and then click the private cloud. On the **Home** tab, in the **Show** group, click **Overview**. In the **Show** group, you can also click **VMs** or **Services** to view information about virtual machines and services that are deployed to the private cloud.

14. To verify that the private cloud library was created, open the **Library** workspace, and then expand **Cloud Libraries**. A private cloud library is listed that matches the private cloud name. If you expand the private cloud library, depending on what you configured, the read-only library shares are listed together with a **Stored Virtual Machines and Services** node.

After you create a private cloud, you can assign the private cloud to one or more user roles. To assign the private cloud to an existing user role, or to assign the private cloud and create a user role at the same time, in the **VMs and Services** workspace, click the private cloud that you want to assign. Then, on the **Home** tab, in the **Cloud** group, click **Assign Cloud** to open the **Assign Cloud** dialog box. If you select an existing user role, you can modify the properties of the user role. If you select **Create a user role and assign this cloud**, the Create User Role Wizard opens.

For information about how to create a self-service user role, see How to Create a Self-Service User Role in VMM.

See Also

Creating a Private Cloud in VMM Overview

How to Create a Private Cloud from a VMware Resource Pool

You can use this procedure to create a private cloud from a VMware resource pool in System Center 2012 – Virtual Machine Manager (VMM).

Account requirements You must perform this procedure as a member of the Administrator user role or as a member of the Delegated Administrator user role where the administrative scope includes the host group where the ESX host or host cluster that contains the VMware resource pool resides.

Prerequisites

Before you create a private cloud from a VMware resource pool, make sure that the following prerequisites are met:

- Configure the fabric by using the procedures in Preparing the Fabric in VMM. The fabric resource examples in this procedure use examples from the “Preparing the Fabric in VMM” section.

  Note
  You cannot discover and manage storage for VMware ESX hosts through VMM.

- In VMware vCenter Server, one or more resource pools must be configured. A vCenter Server and the VMware ESX host or host cluster that contains the VMware resource pool must be under VMM management. For information about how to add vCenter Server and ESX hosts to VMM management, see Managing VMware ESX Hosts Overview.
- If you want to provide self-service users the ability to store virtual machines to the VMM library, create a folder in an existing library share that will serve as the storage location. Realize that self-service users must have the **Store and re-deploy** permission to store their virtual machines.

  Important
  The library share location that you designate for stored virtual machines must be different from the shares that you designate as read-only resource locations for the private cloud. Also, the path or part of the path must be unique when compared to the user role data path that is specified for a self-service user role. For example, if the user role data path for a self-service user role is \\VMMServer01\Marketing, you cannot create a stored virtual machine path of \\VMMServer01\Marketing\StoredVMs. However, if the user role data path is \\VMMServer01\Marketing\MarketingUserRoleData, you could specify \\VMMServer01\Marketing\StoredVMs as the stored virtual machine path, as the full path is unique. You could also create entirely separate library shares.

  Realize that you configure the stored virtual machine path and read-only library shares when you run the Create Cloud Wizard. The self-service user role data path is specified when you create a self-service user role or modify the properties of a self-service user role.

  For example, create the **VMMServer01\Marketing\StoredVMs** path.

- If you want to assign read-only shares to the private cloud, where administrators can store read-only resources such as .iso files that they want to make available to self-service users, make sure that one or more library shares exists that you can assign as the read-only library shares. Realize that self-service users must have the **Author** permission to access the resources.

  Important
  The library shares that you designate as read-only resource locations for the private cloud must be unique when compared to the library share or shares that are used for stored virtual machines and for the user role data path that is specified for a self-service user role.

  For example, you can use the **SEALibrary** and the **NYLibrary** library shares.

Note

For more information about self-service user permissions, see How to Create a Self-Service User Role in VMM.

How to create a private cloud from a VMware resource pool

1. Open the **VMs and Services** workspace.
2. On the **Home** tab, in the **Create** group, click **Create Cloud**.

   The Create Cloud Wizard opens.
3. On the **General** page, enter a name and description for the private cloud, and then click **Next**.

   For example, enter the name **Marketing**, and the description **Private cloud for virtual machines and services in the marketing department**.
4. On the **Resources** page, click **VMware resource pools**, click an available VMware resource pool, and then click **Next**.

   Note

   For the resource pool to be available for selection, the VMware ESX host or host cluster that contains the VMware resource pool must be under VMM management.
5. On the **Logical Networks** page, select the check box next to each logical network that you want to make available to the private cloud, and then click **Next**.

   For example, select the check box next to **BACKEND**, and then click **Next**.
6. On the **Load Balancers** page, select the check box next to each load balancer that you want to make available to the private cloud, and then click **Next**.

   For example, select the check box next to **LoadBalancer01.contoso.com**, and then click **Next**.

   Tip

   When you complete the wizard, if you do not have a fabric resource configured, you can click **Next** to move to the next page. Realize that you can add or remove private cloud resources and modify other private cloud settings after you complete the wizard. To do this, right-click the private cloud, and then click **Properties**.
7. On the **VIP Profiles** page, select the check box next to each VIP template that you want to make available to the private cloud, and then click **Next**.

   For example, select the check box next to **Web tier (HTTPS traffic)**, and then click **Next**.
8. On the **Storage** page, click **Next**.

   Note

   You cannot use VMM to manage or assign storage classifications for storage that is assigned to ESX hosts.

9. On the **Library** page, do the following:
   a. Next to the **Stored VM path** box, click **Browse**. In the **Select Destination Folder** dialog box, expand the library server, click the library share or the folder in a library share that you want to use as the location for self-service users to store virtual machines, and then click **OK**.

      For example, click the **StoredVMs** folder that you created in the **VMMServer01\Marketing** library share.
   b. In the **Read-only library shares** area, click **Add**, select the check box next to one or more library shares to use as the location where administrators can store read-only resources that they want to make available to self-service users, click **OK**, and then click **Next**.

      For example, select the check box next to the **SEALibrary** library share and the **NYLibrary** library share.
10. On the **Capacity** page, set capacity limits for the private cloud, and then click **Next**. You can either accept the default values, or clear the **Use Maximum** check boxes and set quotas for the following resources:

Quota Type	Description
Virtual CPUs	Sets a limit on processing capacity within the private cloud that is equivalent to the capacity that can be provided by a specified number of CPUs. Applied against running virtual machines. Setting a CPU quota does not guarantee contiguous capacity; it only guarantees total CPU capacity available among hosts in the private cloud.
Memory	Sets a quota on memory (in gigabytes) that is available for virtual machines that are deployed to the private cloud. Applied against running virtual machines only. Setting a memory quota does not guarantee contiguous capacity. For example, the private cloud might have available 2 GB of memory on one host and 2 GB of memory on another.
Storage	Sets a quota on storage capacity (in gigabytes) that is available to virtual machines that are deployed to the private cloud. For dynamic virtual hard disks, quota calculations are based on maximum

	size.
Custom quota (points)	Sets a quota on virtual machines that are deployed to the private cloud based on total quota points that are assigned to the virtual machines through their virtual machine templates. Quota points are an arbitrary value that can be assigned to a virtual machine template based on the anticipated size of the virtual machines. Custom quotas are provided for backward compatibility with self-service user roles that were created in VMM 2008 R2.
Virtual machines	Limits the total number of virtual machines that can be deployed to a private cloud.

11. On the **Capability Profiles** page, select the check box next to **ESX Server**, and then click **Next**. The built-in capability profiles represent the minimum and maximum values that can be configured for a virtual machine for each supported hypervisor platform.

    Tip
    In the **Library** workspace, you can also create custom capability profiles to limit the resources that are used by virtual machines that are created in the private cloud. To view the settings that are associated with a built-in capability profile or to create a custom capability profile, open the **Library** workspace, expand **Profiles**, and then click **Capability Profiles**. You can view the properties of a capability profile, or on the **Home** tab, in the **Create** group, click **Create**, and then click **Capability Profile** to create a new one. If you do create a custom capability profile for ESX, make sure that fabric compatibility is set to **ESX Server**.

12. On the **Summary** page, confirm the settings, and then click **Finish**.

    The **Jobs** dialog box appears. Make sure that the job has a status of **Completed**, and then close the dialog box.

13. To verify that the private cloud was created, in the **VMs and Services** workspace, expand **Clouds**.

    The private cloud that you created should appear.

    Tip
    To view information about used and available resources in the private cloud, in the **VMs and Services** workspace, expand **Clouds**, and then click the private cloud. On the **Home** tab, in the **Show** group, click **Overview**. In the **Show** group, you can also click **VMs** or **Services** to view information about virtual machines and services that are deployed to the private cloud.

14. To verify that the private cloud library was created, open the **Library** workspace, and

then expand **Cloud Libraries**. A private cloud library is listed that matches the private cloud name. If you expand the private cloud library, depending on what you configured, the read-only library shares are listed together with a **Stored Virtual Machines and Services** node.

After you create a private cloud, you can assign the private cloud to one or more user roles. To assign the private cloud to an existing user role, or to assign the private cloud and create a user role at the same time, in the **VMs and Services** workspace, click the private cloud that you want to assign. Then, on the **Home** tab, in the **Cloud** group, click **Assign Cloud** to open the **Assign Cloud** dialog box. If you select an existing user role, you can modify the properties of the user role. If you select **Create a user role and assign this cloud**, the Create User Role Wizard opens.

For information about how to create a self-service user role, see How to Create a Self-Service User Role in VMM.

See Also

Creating a Private Cloud in VMM Overview

How to Increase the Capacity of a Private Cloud

You can use this procedure to increase the capacity of a private cloud in System Center 2012 – Virtual Machine Manager (VMM).

Note

If the capacity of the private cloud already equals the capacity of the underlying fabric, you must first add hosts or other fabric resources, make them available to the private cloud, and then increase private cloud capacity. To modify any private cloud resource settings, open the private cloud properties (as described in the following procedure), and then click the desired tab.

To increase the capacity of a private cloud

1. Before you increase private cloud capacity, you can view used and available resource information for private clouds and host groups. To do this, follow these steps:
   a. Open the **VMs and Services** workspace.
   b. In the **VMs and Services** pane, locate and then click a private cloud or host group for which you want to view usage information.
   c. On the **Home** tab, in the **Show** group, click **Overview**.

      Usage information is displayed in the **Overview** pane.
2. To increase capacity, in the **VMs and Services** pane, expand **Clouds**, and then click the

private cloud for which you want to increase the capacity.

3. On the **Folder** tab, click **Properties**.
4. In the *Cloud Name* **Properties** dialog box, click the **Capacity** tab.
5. Under **Cloud capacity**, modify the desired capacity settings, and then click **OK**.

See Also

Creating a Private Cloud in VMM Overview

How to Delete a Private Cloud

You can use this procedure to delete a private cloud in System Center 2012 – Virtual Machine Manager (VMM).

Important
Before you can delete a private cloud, there must be no objects that reference the private cloud, such as services, service deployment configurations, and deployed or stored virtual machines.

To delete a private cloud

1. Open the **VMs and Services** workspace.
2. In the **VMs and Services** pane, expand **Clouds**. Locate and then click the private cloud that you want to delete.
3. In the **VMs** pane, verify that there are no objects related to that cloud.
4. On the **Folder** tab, click **Delete**.
5. When you are prompted whether you want to remove the private cloud, click **Yes**.

   Open the **Jobs** workspace to view the job status.

See Also

Creating a Private Cloud in VMM Overview

Configuring Self-Service in VMM

The procedures in this section explain how to create a self-service user role that can create, deploy, and use virtual machines and services on one or more private clouds in Virtual Machine Manager (VMM). The procedures also explain how to share VMM resources as a self-service user, if permissions have been set up for you to share these resources with other self-service users.

Important
As of System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed. If you need a self-service portal solution, we recommend that you use App Controller. For more information, see App Controller.

Procedure	Description
Configuring Self-Service in VMM Overview	Provides an overview of self-service features in VMM.
How to Create a Self-Service User Role in VMM	Describes how to create a self-service user role that can create and deploy virtual machines and services on a private cloud.
How to Open a New Session While You Are Logged On to the VMM Console	Describes how to open a new connection to the VMM console under a different user role.
How to Enable Self-Service Users to Share Resources in VMM	Describes how to enable resource sharing between self-service user roles.
How to Share Resources as a Self-Service User in VMM	Describes how to share resources as a self-service user in VMM.
Configuring the Library to Support Self-Service Users	Describes new methods that are available in VMM for sharing resources with self-service users
How to Configure the Library to Support Self-Service Users	Describes how to create read-only library shares and user role data paths
How to Import and Export Physical Resources To and From the Library	Describes how to import and export file-based resources between library servers and library shares.

See Also

Creating User Roles in VMM

Configuring Self-Service in VMM Overview

As of Virtual Machine Manager (VMM) in System Center 2012, self-service user roles were redesigned to provide a richer environment for creating, deploying, and managing virtual machines as well as services in a private cloud.

As of System Center 2012, multiple self-service features were added or enhanced in VMM. These features fall into the following categories:

- Actions That Self-Service Users Can Take: Self-service users now deploy their virtual machines and services to private clouds. They can create their own templates and profiles. They can also create virtual machines from building blocks such as virtual hard disks (VHDs) rather than just templates.
- Ways That Self-Service Users Can Work with the Interface: Self-service users can use the VMM console or the VMM command shell (instead of having to use a portal). Also, a person who is a member of more than one user role can open a second VMM session to operate under a different user role, and then switch between sessions as needed.
- Ways That Resources and Run As Accounts Can Be Made Available to Self-Service Users: More types of library resources, including virtual machine templates, service templates, and multiple types of profiles, can be assigned to a self-service user role. Resources can be shared between self-service user roles if an administrator assigns the Share and Receive actions to self-service users. Also, an administrator can assign Run As accounts (to provide credentials) to the user role of a self-service user.

The following sections provide more details about these additions and enhancements.

Actions That Self-Service Users Can Take

As of VMM in System Center 2012, self-service users can take additional actions, compared to previous versions. The following list provides details:

- As of VMM in System Center 2012, self-service users deploy their virtual machines and services to private clouds. This is a change from earlier versions of VMM, in which self-service user roles are assigned host groups, and virtual machines are deployed automatically (and transparently) to the most suitable host in the host group. A private cloud consists of one or more host groups that provide computing capacity and disk resources to self-service user roles. A private cloud can be assigned to multiple self-service user roles. Role-level quotas on each self-service user role that has the private cloud within its scope are used to allocate computing capacity and other storage within the cloud. Member-level quotas set individual limits for self-service user role members.

  During virtual machine and service deployment in VMM, self-service users view a simplified placement map that shows the private cloud that their virtual machine or service will be deployed to. If the self-service user role has more than one private cloud within its scope, users select the appropriate cloud before placement runs.
- Self-service users can create their own templates and profiles. The **Author** action for a self-service user role grants self-service users authoring rights. Users with authoring rights can create hardware profiles, guest operating system profiles, application profiles, SQL Server profiles, virtual machine templates, and service templates.
- Self-service users can create virtual machines from building blocks such as virtual hard disks (VHDs) rather than just templates. In VMM 2008 R2, self-service users were allowed to create virtual machines only from existing templates that an administrator assigned to their self-service user role. As of VMM in System Center 2012, you can require users to use templates by granting the **Deploy (From template only)** action. However, to enable self-

service users to create virtual machines from building blocks such as VHDs, you can add the **Deploy** action to the self-service user role. That action allows self-service users to create virtual machines from the VHDs that they have access to. Both the **Deploy** action and the **Deploy (From template only)** action extend the virtual machine creation capabilities for self-service users to include service creation.

Ways That Self-Service Users Can Work with the Interface

As of VMM in System Center 2012, self-service users can work with the interface in the following ways:

- Self-service users can use the VMM console or the VMM command shell to create and manage their own virtual machines and services. In the VMM console, self-service users can view status, resource usage, jobs, and PRO tips (by permission only) for their own virtual machines and services. They can view available capacity and quota usage within their assigned private clouds, but they cannot see host groups, hosts, library servers and shares, or network and storage configurations.

  Note

  For customers who are using self-service in VMM 2008 R2 and who migrate to System Center 2012 – Virtual Machine Manager, System Center 2012 – Virtual Machine Manager provides backward compatibility for existing self-service user accounts through an updated version of the VMM Self-Service Portal. The updated portal supports capabilities provided in the legacy self-service user roles but will not support new self-service capabilities in System Center 2012 – Virtual Machine Manager.

  As of System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed. If you need a self-service portal solution, we recommend that you use App Controller. For more information, see App Controller.

- While working in the VMM console, a person who is a member of more than one user role can open another VMM session to operate under a different user role by using the **Open New Connection** action, and can then switch between VMM sessions by using the Taskbar or CTRL+TAB.

  As of VMM in System Center 2012, a self-service user who belongs to more than one self-service user role must choose one self-service user role for each VMM session. This is different than in VMM 2008 R2, which allows a self-service user who belongs to more than one self-service user role to choose which self-service user role to use when creating or deploy a virtual machine within a VMM session.

Ways That Resources and Run As Accounts Can Be Made Available to Self-Service Users

As of VMM in System Center 2012, resources and Run As accounts can be made available to self-service users in the following ways:

- To support application deployment and the additional profiles and templates associated with service creation, more types of library resources can be assigned to a self-service user role as of VMM in System Center 2012. Self-service user roles can be assigned hardware profiles, guest operating system profiles, virtual machine templates, application profiles, SQL Server profiles, and service templates.
- In VMM, resources can be shared between self-service user roles. The **Share** action allows user role members to share resources that they own with members of self-service user roles that allow the **Receive** action. Sharable resources include hardware profiles, guest operating system profiles, virtual machine templates, application profiles, SQL Server profiles, service templates, virtual machines, and services.
- In VMM, the credentials for application, virtual machine, and service deployment are provided by Run As accounts. An administrator assigns Run As accounts to the user role of self-service users to provide the credentials that the users need to deploy their virtual machines and services.

See Also

Configuring Self-Service in VMM

Creating User Roles in VMM

How to Create a Self-Service User Role in VMM

As of Virtual Machine Manager (VMM) in System Center 2012, you can use this procedure to create a Self-Service User role.

Account requirements Administrators and delegated administrators can create Self-Service User roles. Delegated administrators can create Self-Service User roles for private clouds that are in the scope of their user role.

To create a Self-Service User role

1. In the **Settings** workspace, on the **Home** tab, in the **Create** group, click **Create User Role**.
2. In the **Create User Role Wizard** on the **Name and description** page, enter a name and optional description of the Self-Service User role, and then click **Next**.
3. On the **Profile** page, click **Self-Service User**, and then click **Next**.

4. On the **Members** page, add user accounts and Active Directory groups to the role, and then click **Next**.

   Note

   If you want all role members to share ownership of all virtual machines that any member creates, create a security group in Active Directory and assign that group to the user role. An alternate method for sharing resources among Self-Service User role members is to use the **Share** and **Receive** actions, discussed later, which enable resource owners who are self-service users to share individual resources with one or all members of a Self-Service User role.

   If you plan to use this user role to test deploying virtual machines and services to a private cloud, be sure to add yourself as a member.

5. On the **Scope** page, select at least one private cloud for the Self-Service User role, and then click **Next**.
6. On the **Quotas** page, set quotas for each private cloud that is in the scope of the user role, and then click **Next**. If multiple private clouds are assigned to a Self-Service User role, you will see a **Quotas** page for each private cloud.

   Note

   Each quota sets an individual limit for each member of the user role. If you want all role members to share overall quotas, create a security group in Active Directory and assign that group to the user role.

Quota Types Supported for Self-Service in VMM

Quota Type	Description
Virtual CPUs	Limits the total number of virtual machine CPUs that can be consumed from the private cloud.
Memory (MB)	Limits the amount of virtual machine memory (in megabytes) that can be consumed from the private cloud.
Storage (GB)	Limits the amount of virtual machine storage (in Gigabytes) that can be consumed from the private cloud.
Custom quota (points)	Sets a quota on virtual machines deployed on the private cloud based on total quota points assigned to the virtual machines via their virtual machine templates. Quota points are an arbitrary value that can be assigned to a virtual machine template based on the anticipated "size" of

	the virtual machines. Custom quotas are provided for backward compatibility with self-service user roles created in VMM 2008 R2.
Virtual machines	Limits the total number of virtual machines that can be deployed on a private cloud.

Quotas only apply to deployed virtual machines. If a Self-Service User role has permission to store virtual machines, the quota does not apply to virtual machines that are stored in the library.

7. On the **Resources** page, click **Add** to open the **Add Resources** dialog box. Assign hardware profiles, operating system profiles, virtual machine templates, application profiles, SQL server profiles, and service templates for the self-service users to use during virtual machine creation.

8. Under **Specify user role data path**, use the **Browse** button to select a path on a library share where user role members can upload and share their own resources. The user data path also is a good place to store prepared resources that should be shared only with members of this Self-Service User role.

   Click **Next** to continue.

9. On the **Actions** page, select the actions that the self-service users need to perform on their own virtual machines and services, and then click **Next**. To select all actions, click **Select all**.

Actions Available to Self-Service User Roles in VMM

Action	Description
Author	Grants members permission to author templates and profiles. Users with authoring rights can create hardware profiles, operating system profiles, application profiles, SQL Server profiles, virtual machine templates and service templates.
Checkpoint	Grants members permission to create, edit, and delete checkpoints for their own virtual machines and to restore their virtual machine to a previous checkpoint. **Note** VMM does not support checkpoint actions on services.

Checkpoint (Restore only)	Grants members permission to restore their own virtual machines to a checkpoint but not to create, edit, and delete checkpoints.
Deploy	Grants members permission to deploy virtual machines and services from templates and virtual hard disks that are assigned to their user role. However, they do not have the right to author templates and profiles. (Expanded in VMM to include creation of services)
Deploy (From template only)	Grants members permission to deploy virtual machines and services from templates that are assigned to their user role. However, they do not have any authoring rights. (Expanded in VMM to include creation of services)
Local Administrator	Grants members permission to serve as a local Administrator on their own virtual machines. **Important** Be sure to select the **Local Administrator** action on any Self-Service User role that has the **Deploy (From Template)** action selected. This action enables those users to set the local Administrator password during virtual machine and service deployment. Self-service users who are granted the **Deploy** action do not need this action to be able to set local Administrator credentials.
Pause and resume	Grants members permission to pause and resume their own virtual machines and services.
Receive	Allows members to receive resources that are shared by members of other Self-Service User roles.

Remote connection	Grants members permission to connect to their virtual machines from the VMM console, the VMM Self-Service Portal, or App Controller. **Note** As of System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed. If you need a self-service portal solution, we recommend that you use App Controller. For more information, see App Controller.
Remove	Grants members permission to remove their own virtual machines and services.
Save	Grants members permission to save their own virtual machines and services.
Share	Allows members to grant resources that they own to other Self-Service User roles. Sharable resources include hardware profiles, operating system profiles, application profiles, SQL Server profiles, virtual machine templates, virtual machines, service templates, and services. A self-service user must be the owner of a resource to share it. The Self-Service User role that receives the shared resource must be assigned the **Receive** action.
Shut down	Grants members permission to perform an orderly shutdown of their own virtual machines and services.
Start	Grants members permission to start their own virtual machines and services.
Stop	Grants members permission to stop their own virtual machines and services.
Store and re-deploy	Grants members permission to store their own virtual machines in the VMM library, and re-deploy those virtual machines.

	Virtual machines stored in the library do not count against a user's virtual machine quotas. **Note** VMM does not support storing services.

10. If you selected the **Author** action, the **Run As accounts** page opens. Select Run As accounts for the Self-Service User role to use in the templates and profiles that they use to create virtual machines and services, and then click **Next**.
11. Review the settings you have entered on the **Summary** page, and then click **Finish**.

After you create a Self-Service User role, you can change settings using the **Properties** dialog box for the user role.

See Also

Configuring Self-Service in VMM

Creating User Roles in VMM

How to Open a New Session While You Are Logged On to the VMM Console

To create services and deploy services to a private cloud as a self-service user, you must use the VMM console. If you are logged on to the VMM console as an administrator, and you also are a member of a self-service user role, you can open a new session under the self-service user role. The following procedure explains how to open a new session while you are logged on to the VMM console.

To open a new VMM session while you are logged on to the VMM console

1. From any workspace in the VMM console, click the down arrow at the top left corner of the ribbon, and then click **Open New Connection**.
2. In the **Connect to Server** dialog box, click **Connect** to start a second session with the current VMM instance.
3. In the **Select User Role** dialog box, select the user role you want to log on under, and then click **OK**.

   A new instance of the VMM console opens, and the previous VMM session remains open. You can determine which session you are using by viewing the title bar, because the title bar contains the name of the user role that is being used.

How to Enable Self-Service Users to Share Resources in VMM

Use the following procedures if you are an administrator and you want to enable resource sharing between self-service user roles in Virtual Machine Manager (VMM). For a list of other procedures related to configuring self-service, see Configuring Self-Service in VMM.

If you are a self-service user, see **How to Share Resources as a Self-Service User in VMM**.

In VMM, a member of a self-service user role can share the resources that she owns with other members of her self-service user role, with another self-service user role, or with an individual member of another self-service user role. For example, a member of an Application Developers self-service user role might share his service template with an Application Testers self-service user role for pre-production testing.

To share a resource with a member of another self-service user role, the following conditions must be met:

- The self-service user who shares the resource must be the owner of the resource.
- The resource owner must belong to a self-service user role that has been assigned the **Share** action.
- The resource receiver must belong to a self-service user role that has been assigned the **Receive** action.

To enable self-service user roles to share resources

1. Open the **Settings** workspace.
2. In the **Settings** pane, expand **Security**, and click **User Roles**.
3. In the **User Roles** pane, click the self-service user role for which you want to enable the sharing of resources.
4. On the **Home** tab, in the **User Role** group, click **Properties**.

   The user role **Properties** dialog box opens.
5. On the **Actions** tab, select **Share**, and then click **OK**.

   Members of this self-service user role can now share their own resources with members of any self-service user role that has the **Receive** action assigned to it. Now, configure the other self-service user role to receive resources.
6. Open the properties of the other self-service user role. (In the **User Roles** pane, right-click the user role and click **Properties**.)
7. On the **Actions** tab, select **Receive**, and then click **OK**.

See Also

Configuring Self-Service in VMM

How to Share Resources as a Self-Service User in VMM

Configuring the Library to Support Self-Service Users

This topic provides guidance on new methods that are available for sharing resources with self-service users in Virtual Machine Manager (VMM) and describes the self-service user's view of the **Library** workspace. If you already understand the background information and want detailed steps for configuring the library, see How to Configure the Library to Support Self-Service Users.

To enable self-service users to create their own virtual machines and services and deploy them to private clouds, VMM provides additional ways for administrators to make resources available to self-service users. As of VMM in System Center 2012, self-service users can use the VMM console, and can see their logical and physical resources in the **Library** workspace. In earlier releases of VMM, self-service users who were assigned the **Create** action had to use virtual machine templates that were created by an administrator and assigned to their self-service user role to create their virtual machines. Those self-service users had no access to the library. Assigned templates were available only in selection lists.

As of VMM in System Center 2012, self-service users who are assigned the **Author** action can create their own templates and profiles, and can share their service templates and virtual machine templates with other self-service users. A user data path is provided to the self-service user role to enable those users to upload and share their own resources. Read-only library paths are provided on private clouds to enable the administrator to share resources among all cloud users. Lastly, the design of the **Library** workspace in VMM has been updated to meet the needs of those self-service users.

Providing Resources for Self-Service Users

Use the following methods to provide resources to self-service users who deploy services and virtual machines in private clouds:

- **Read-only library shares for private clouds** Use the read-only library shares for private clouds to share resources that should be widely available to self-service users who deploy services to a cloud. For example, an administrator might store the Application Frameworks resources that are provided with VMM on a read-only library share for a private cloud so that cloud users can use the resources to sequence and deploy their own applications. For more information about the Application Frameworks resources, see Application Framework Resources in VMM.
- **Self-service user data paths** Configure user data paths on self-service user roles to provide a place where members of a self-service user role can upload and share their own

resources. The user data path also is the best place for administrators to store resources that only members of a self-service user role need to use. For example, a user data path might store the application packages for services that a self-service user role deploys. Permissions on the user data path are controlled through the file system. VMM discovers all files that the current self-service user has access to. Access control permissions determine whether the users have Read/Write or Read/only access.

To enable administrators to audit and manage resources on users' data paths, the data paths must be on a library share.

Note
Only self-service users whose user role has the **Author** action or the **Deploy** action can actually use these physical resources in VMM. The **Author** action enables members to create templates and profiles for their own virtual machines and services. The **Deploy** action enables members to deploy virtual machines by using VHDs as well as virtual machine templates that are assigned to or shared with their user role. For more information, see How to Create a Self-Service User Role in VMM.

- **Assigned resources** To make virtual machine templates and service templates available to the self-service users who will deploy virtual machines and services in a private cloud, assign the templates to the self-service user roles. In addition, self-service users with the **Author** action can benefit from using standard guest operating system profiles, hardware profiles, application profiles, SQL Server profiles, and virtual machine templates that an administrator provides. Self-service users do not need access to the physical resources that are referenced by templates and by profiles assigned to their self-service user role.

  Important
  When you create templates for self-service users, be aware of the following changes in VMM:

  - In VMM, the concept of a "self-service owner" for a template no longer exists. A template that is to be shared by members of a self-service user role should have no owner assigned. When a template with no owner is assigned to a self-service user role that has the **Author**, **Deploy**, or **Deploy (Template Only)** action assigned to it, all members can use the template. However, when an owner is assigned to the template, only the owner can use the template.
  - VMM provides new types of quotas for self-service users' deployed virtual machines. The quota points that are assigned to virtual machine templates in earlier releases of VMM still are supported as "custom quotas." Administrators also can place individual- or role-level quotas on virtual CPU, memory, storage, and the total number of virtual machines deployed in each private cloud that is in the scope of a self-service user role. For more information, see How to Create a Self-Service User Role in VMM.

- **Shared resources** Allow self-service users to share their resources with other self-service users. You can configure self-service user roles to allow the owners of virtual machine templates and service templates to share their resources with other members of their own self-service user role, with another self-service user role, or with an individual member of another self-service user role. For example, members of a **Service Developers** self-service user role might share their fully tested service templates with a **Service Manager** self-service

user role for deployment into a production environment. The **Share** action enables a self-service user role to share resources; the **Receive** action enables a self-service user role to receive resources that are shared by another self-service user role. For more information, see How to Enable Self-Service Users to Share Resources in VMM.

A Self-Service User's View of the VMM Library

In System Center 2012 – Virtual Machine Manager, the following changes were made to the **Library** workspace to accommodate self-service users' new capabilities:

- Instead of the **Library Servers** node that administrators see, self-service users see a **Cloud Libraries** node, which displays physical resources that are available to self-service users through private clouds. The **Cloud Libraries** node displays a node for each of the private cloud that is in the scope of the self-service user role. Each private cloud node displays physical resources on read-only library shares that have been configured for the private cloud.

  Note
  Administrators see both the **Library Servers** node and the **Cloud Libraries** node. Delegated administrators see only the library servers and cloud libraries that are in the scope of their user roles.
- In the new **Self-Service User Data** node, self-service users see physical resources that they have access to on the user data path for their self-service user role. Access control permissions in the file system determine what the users see.
- In the **Templates** and **Profiles** nodes, self-service users see only templates and profiles that they own, that are assigned to their self-service user roles, or that are shared with them by other self-service users.

See Also

Configuring Self-Service in VMM

How to Configure the Library to Support Self-Service Users

How to Configure the Library to Support Self-Service Users

Use the following procedures to prepare the library to enable self-service users to deploy virtual applications to a private cloud in Virtual Machine Manager (VMM). To give all private cloud users access to prepared resources that are used widely in service deployment, create library shares to add as read-only library shares on private clouds. To enable members of a self-service user role to upload and share the physical resources that they use to create service templates and to deploy services, configure a user data path for their self-service user role. For background

information about configuring the library, see Configuring the Library to Support Self-Service Users.

Account requirements All of these procedures must be performed by a VMM administrator. Delegated administrators can add library shares on library servers that are in the scope of their user role, can configure read-only library shares on private clouds that they created, and can configure user data paths on self-service user roles that they created. Only members of the local Administrators group can grant access permissions on their user data paths.

Sharing Physical Resources with Private Cloud Users

To share physical resources with self-service users who deploy virtual machines and services to private clouds, you can add the resources to read-only library shares for the private clouds. The resources on read-only library shares for a private cloud are available to members of all self-service user roles that have the private cloud in their scope. The resources can be used in VMM, but the files cannot be accessed directly through the file system and modified by self-service users.

Use the read-only library shares on private clouds to make prepared resources widely available. For example, VHDs, ISO images, and other resources that are assigned to self-service user roles must be stored either on a read-only library share for a private cloud that is associated with the self-service user role or on the user data path for the self-service user role. You might also store resources such as the Application Frameworks resources on these shares to enable self-service users to configure templates and profiles with scripts that install the Microsoft Web Deployment tool and a Server App-V client on a tier to enable installation of virtual applications during service deployment. (To enable the users to sequence their own applications, you would need to either grant access permission to the Server App-V Sequencer through the file system or store it on the user data path for their self-service user role.)

To create shares for read-only resources for users

1. In Windows Explorer, create a shared folder to store all resources that will be used by self-service users who deploy services to private clouds. This folder will include read-only library shares for private clouds, and it will include user data paths for self-service user roles. For convenience, you can create the folder near your default library share so that it is easy to access when you manage library resources. For example, create the following folder:

   C:\ApplicationData\Virtual Machine Manager Cloud Resources

2. Within that folder, create a folder to store the \ApplicationFrameworks resources. Then share the folder so that you can add it as a library share. For example, create and share the following folder:

   C:\ApplicationData\Virtual Machine Manager Cloud Resources\ApplicationFrameworks

   Important

The shared folder cannot be in the path of the default library share. You cannot add a library share that is in the path of an existing library share.

3. Copy the ApplicationFrameworks folder from your default library share to the share that you created for private cloud resources.
4. Add the share to the VMM library:
   a. In the VMM console, open the **Library** workspace.
   b. On the **Library** pane, expand **Library Servers**, and click the library server that contains the default library share.
   c. On the **Library Server** tab, in the **Library Server** group, click **Add Library Shares**.

      The **Add Library Shares Wizard** opens.
   d. On the **Add Library Shares** page, select each shared folder that you want to add to the library. For example, select ApplicationFrameworks, on the C:\VMM Cloud Resources path.
   e. On the **Summary** pane, click **Add Library Shares**.
5. After the **Add library shares** job completes, on the **Library** pane, expand **Library Servers**, and then expand the node for the library server that contains your default library share. The node should display the new library share. You can expand the share node to see resources stored on the share.

To add read-only library shares to a private cloud in VMM

1. Open the **VMs and Services** workspace.
2. On the **VMs and Services** pane, expand clouds, and click the private cloud that you want to update.
3. On the **Folder** tab, in the **Properties** group, click **Properties**.
4. In the **Properties** dialog box, open the **Library** tab.
5. By **Read-only library shares**, click **Add**.
6. In the **Add Library Shares** dialog box, select each library share that you want to add to the read-only library share for the private cloud, and tehn click **OK**.
7. Click **OK** a second time to save the updates to the private cloud properties.

Providing a Place for Self-Service Users to Store and Share Their Resources

Use the following procedure to set up a user data path for a self-service user role. The user data path enables members of a self-service user role to upload and share the physical resources that they use to create service templates and to deploy services. Each self-service user role has only one user data path for all private clouds that are in the scope of the user role. The user data path must be in a library share.

Access to the physical resources on a user data path is controlled through the file system. To enable members of a self-service user role to use and share their own resources in VMM, grant Read/Write permission on the folder to all role members.

In the **Library** workspace, self-service users can see any resources for which they have permissions on the **Library** pane, in the **Self-Service User Data** node. However, only members of a self-service user role that has the **Author** action assigned to it can use the resources to create profiles and templates in VMM.

To enable members of a self-service user role to use their own application packages to create service templates and deploy services in VMM, configure a user data path for the self-service user role and grant Read/Write permission on the folder.

To create a folder for resources owned by a self-service user role

1. In Windows Explorer, create a folder to store all shared resources that will be used by self-service users who deploy virtual machines and services to private clouds. For example, create the following folder:

   C:\ProgramData\Virtual Machine Manager Cloud Resources\Self-Service User Data
2. Within that folder, create a subfolder to store resources for the self-service user role. For example, create the following folder:

   C:\ProgramData\Virtual Machine Manager Cloud Resources\Self-Service User Data\Finance Service Managers
3. Within that folder, create a subfolder to store the application packages for all releases of the virtual application that you will use in this scenario; within that folder, create a subfolder to store the application package for the first release of the service. Each time you update and re-sequence an application by using Server App-V, you will need to store the new application package in a separate folder. For example, create the following folder, where <MyApplication> is the name of the application that is being developed and managed through self-service:

   C:\ProgramData\Virtual Machine Manager Cloud Resources\Self-Service User Data\Finance Service Managers\<MyApplication>\MyApplication v1>
4. To enable members of the self-service user role to access the resources and upload their own resources to the folder, grant all members Read/Write permission on the folder.
5. If needed, share the folder that contains user data for all self-service user roles, and then add the share to the VMM library.

   To be assigned to a self-service user role, a user data path must be on a library share.

To configure a user role data path for a self-service user role

1. Open the **Settings** workspace.
2. On the **Settings** pane, expand **Security**, and click **User Roles**.
3. On the **User Roles** pane, click the self-service user role. For example, click Finance Service Managers.
4. On the **Home** tab, in the **User Role** group, click **Properties**.

5. In the user role properties, open the **Resource** tab.
6. In **Data path**, use the **Browse** button to select the folder that you created to store shared resources for members of the self-service user role. For example, for the Finance Service Manager user role, you would select the following folder:

   C:\ProgramData\Virtual Machine Manager Cloud Resources\Self-Service User Data\Finance Service Managers
7. Click **OK** to store the updates to the self-service user role.

   After you save the user role, the data path is added to the **Library** workspace.
8. To verify that the new data path has been added:
   a. Open the **Library** workspace.
   b. On the **Library** pane, expand **Self-Service User Content**.

      You should see a node with the name of the self-service user role - for example, Finance Service Managers. Unless you have added yourself to the self-service user role, you will not be able to see the physical resources that are stored in the folder.

See Also

Configuring Self-Service in VMM

Configuring the Library to Support Self-Service Users

How to Import and Export Physical Resources To and From the Library

You can use the following procedures to import and export file-based resources between library servers and library shares in Virtual Machine Manager (VMM). This functionality also enables you to transfer files between library servers that are associated with different VMM management servers.

This is the recommended method for self-service users to import and export physical resources to and from the VMM library. This is especially true if the self-service user does not have permissions set outside VMM to access private cloud library shares or their user role data path through Windows Explorer.

Account requirements You must be a member of the Administrator, Delegated Administrator, or Self-Service user role with the **Author** permission to complete these procedures. Delegated administrators can only import and export resources to and from library locations that are within the scope of their user role. Self-service users can only import resources to their user role data path in the Self Service User Content node of the VMM library. Self-service users can export resources that are available in their user role data path and in their private cloud library shares.

To import physical resources

1. Open the **Library** workspace.
2. On the **Home** tab, in the **Import** group, click **Import Physical Resource**.
3. In the **Import Library Resources** dialog box, click either of the following:
   - **Add custom resource**

     This option enables you to import a folder and its contents. You can select a folder that has a .CR extension to import the folder as a custom resource package. Or, you can select a folder without a .CR extension that contains one or more files of a supported file type. If you select a folder without a .CR extension, only the files of a supported file type will appear in the VMM library. However, if you use Windows Explorer to access the library share, you can access all files in the folder depending on the file and share permissions that are configured outside VMM.

     Tip
     If the folder with .CR extension contains more than one hundred file to be imported, it is recommended that you zip the files before the import. This will improve performance.
   - **Add resource**

     This option enables you to import one or more files of a supported type to another library location. For information about the supported file types, see the table in the "File-based resources" section of Configuring the Library Overview.
4. If you are an administrator or a delegated administrator, after you have selected the desired resources, under **Select library server and destination for the imported resources**, click **Browse**. Then, click the desired library server, the library share, and optionally, the desired folder location, and then click **OK**.
5. When you are finished, click **Import**.

   To verify that the resources were imported, if you are an administrator or a delegated administrator, under **Library Servers**, locate and then click the target location. In the **Physical Library Objects** pane, make sure that the resources are listed.

   If you are a self-service user, expand **Self Service User Content**, and then click the user role data path. In the **Self Service User Objects** pane, make sure that the resources are listed.

To export physical resources

1. Open the **Library** workspace.
2. On the **Home** tab, in the **Export** group, click **Export Physical Resource**.
3. In the **Export Library Resources** dialog box, click **Add**.

   All physical library resources in the VMM library that the user has access to are listed.

   Tip
   You can right-click the column header to select which columns appear.
4. Select the physical resources that you want to export, and then click **OK**. (To select

multiple resources, press and hold the CTRL key, and then click each resource. To select a range, click the first resource in the range, press and hold the SHIFT key, and then click the last resource in the range.)

5. Under **Specify a destination for the export files**, click **Browse**. In the **Browse for Folder** dialog box, click a destination folder, and then click **OK**.
6. When you are finished, click **Export**.

See Also

How to Add File-Based Resources to the Library

Creating and Deploying Virtual Machines in VMM

The following topics describe how to create and deploy virtual machines in Virtual Machine Manager (VMM):

- Creating and Deploying Virtual Machines Overview
- Understanding Virtual Machine Placement and Ratings in VMM
- Understanding Generation 1 and Generation 2 Virtual Machines in VMM
- Requirements for Linux-Based Virtual Machines
- How to Create and Deploy a Virtual Machine from a Blank Virtual Hard Disk
- How to Create and Deploy a Virtual Machine from an Existing Virtual Hard Disk
- How to Create and Deploy a Virtual Machine from an Existing Virtual Machine
- How to Create and Deploy a Virtual Machine from a Template
- How to Deploy a Virtual Machine by Converting a Physical Computer (P2V)
- How to Deploy a Virtual Machine by Converting a Virtual Machine (V2V)
- How to Deploy a Virtual Machine Stored in the VMM Library
- How to View and Modify Properties of a Deployed Virtual Machine in VMM

Creating and Deploying Virtual Machines Overview

Virtual Machine Manager (VMM) provides a number of methods for creating and deploying virtual machines, and for applying standard configuration settings to those virtual machines. This section provides information about these methods, and about other concepts that are related to virtual machines.

Methods for Creating and Deploying Virtual Machines

- **Create and deploy a stand-alone virtual machine**—You can manually create a stand-alone virtual machine as follows:
  - **Create and deploy a virtual machine from a blank virtual hard disk**—After creating the virtual machine using this method you can install an operating system from an .iso image, CD or DVD, or from a network boot if a Pre-Boot Execution Environment (PXE) server is available. For instructions, see How to Create and Deploy a Virtual Machine from a Blank Virtual Hard Disk.
  - **Create and deploy a virtual machine from an existing virtual hard disk**—Using this method you can create a virtual machine from an existing virtual hard disk stored in the VMM library. We recommend that you use a virtual hard disk that has been generalized using Sysprep, otherwise the new virtual machine will have the same identity as the source machine. For instructions, see How to Create and Deploy a Virtual Machine from an Existing Virtual Hard Disk.
  - **Create and deploy a virtual machine from an existing virtual machine**—Using this method you can clone an existing virtual machine in the VMM library to create a new one. We recommend that you clone virtual machine that has been generalized using Sysprep, so that the virtual machines do not have the same identity. As of System Center 2012 R2, when you use this method to create a virtual machine, Virtual Machine Manager automatically uses differencing disk if a base disk is detected on the host on which the cloned virtual machine is being created on.
- **Create and deploy a virtual machine using a virtual-to-virtual (V2V) conversion**—Use this method to copy an existing Citrix XenServer or VMware virtual machine and create a Hyper-V virtual machine. For more information, see How to Convert Citrix XenServer Virtual Machines to Hyper-V, and How to Convert VMware Virtual Machines to Hyper-V.
- **Create and deploy a virtual machine using a physical-to-virtual machine (P2V) conversion**—Use this method to convert an existing physical computer into a virtual machine, if you are running VMM in System Center 2012 or System Center 2012 Service Pack 1 (SP1). As of System Center 2012 R2, you can no longer perform P2V conversions in VMM. P2V conversions are done on a best effort basis. For more information about P2V, see How to Deploy a Virtual Machine by Converting a Physical Computer (P2V).
- **Create and deploy a virtual machine using a virtual machine template**—Use this method to create virtual machines with consistent configuration settings taken from a template. Virtual machine templates are preconfigured XML objects stored in the VMM library. Templates can be used to control and restrict the virtual machine configurations available for selection by self-service users. Templates have a number of properties associated with them, including a guest operating system profile, a hardware profile, and one or more VHDs which can be used to create a new virtual machine. To create virtual machine templates, you first create the required profiles, and then create templates based on those profiles. Templates can be created from an existing template, from a virtual hard disk stored in the library, or from an existing virtual machine deployed on a host.

As of System Center 2012 R2, when using this method to create and deploy a virtual machine, usage of differencing disk is optimized, allowing for a more efficient process.

- For information on creating profiles, see Creating Profiles and Templates in VMM.
- For information on creating templates, see How to Create a Virtual Machine Template.
- For information on creating a virtual machine based on a template, see How to Create and Deploy a Virtual Machine from a Template.

- **Create and deploy virtual machines in a service deployment**—System Center 2012 – Virtual Machine Manager introduced the concept of a service, which is a logical grouping of virtual machines that are configured and deployed together, and managed as a single entity. Services can be single-tier or multi-tier. A single-tier service consists of a single virtual machine that provides additional configuration settings to those provided by a virtual machine template. A multi-tiered service contains multiple virtual machines. For example a multi-tier service might consist of a SQL server tier, a Server App-V tier, and a Web App tier. You define a service by configuring a service template, which includes information about virtual machines that are deployed in the service. You can create a new service templates, or create a service template based on an existing virtual machine template. For more information, see the following resources:

  As of System Center 2012 R2, when using templates in this method to create and deploy a virtual machine, usage of differencing disk is optimized, allowing for a more efficient process.

  - For general information about deploying services, see Creating and Deploying Services in VMM.
  - For instructions on creating service templates, see How to Create a Service Template in VMM.
  - For instructions on deploying virtual machines as part of a service template, see How to Add a Tier to a Service Template.
- **Rapid provisioning of virtual machines** In VMM, you can rapidly provision virtual machines by using storage area network (SAN) copy technology such as snapshot and clone. Rapid provisioning is available for stand-alone virtual machines and for virtual machines that are deployed as a service. For more information, see Rapid Provisioning of Virtual Machines Using SAN Copy Overview.

Using Differencing Disks for Creating and Deploying Virtual Machines

In System Center 2012 R2, usage of differencing disks has been optimized. You can use differencing disks when you create virtual machines using a virtual machine template, or when you use a service. Using a differencing disk is associated with a virtual hard disk that serves as a base virtual disk, and which does not change. This base disk is combined with a differencing disk that contains any modifications to the base disk. This allows you to isolate the changes to the base disk, and to optimize several operations in VMM that are related to virtual machines. Using a small set of initial virtual disks, you can use differencing disks so that a large percentage of the disk data is shared among multiple virtual disks.

VMM optimizes support for differencing disks to provide the following benefits:

- Optimized migration of storage that utilizes differencing disks. During a migration, VMM does not migrate base disks unless it is necessary.
- Optimize virtual machine deployment time by utilizing differencing disks. VMM will attempt to identify and utilize differencing disks on the target computer.
- When differencing disks is utilized, deployment of the base virtual disk is optimized by taking advantage of the Windows Offloaded Data Transfers (ODX) capability to copy files to the guest machine during service deployment.
- Optimize time and storage of cloning of virtual machines by utilizing differencing disks. VMM provides the option to create and utilize differencing disks during a cloning operation.

When using differencing disks, administrators should pay attention to the following:

- Ensure that unused base virtual disks on hosts are removed.
- If a base virtual disk becomes corrupted, or unavailable for any other reason, all virtual disks that depend on the lost disk are lost too. As with any critical data, to mitigate that risk, you should follow a backup plan that will ensure the high availability of the base virtual disks.

Fast File Copy

During virtual machine deployment Virtual Machine Manager needs to move and copy large files, such as VHD's, between two locations. Fast file copy in System Center 2012 R2 Virtual Machine Manager improves the performance of file transfers, mostly by leveraging the Windows Offloaded Data Transfers (ODX) feature introduced in Windows Server 2012 R2. In System Center 2012 R2 Virtual Machine Manager, background intelligent transfer (BITS) is still used as a mechanism for file transfers. However, when possible (for example when copying files to SANs that support ODX), Virtual Machine Manager leverages ODX for that task, greatly improving the time performance of virtual machine deployments. For information about Windows ODX, see Windows Offloaded Data Transfers Overview.

Understanding Virtual Machine Placement and Ratings in VMM

When you deploy or migrate a virtual machine to a host, Virtual Machine Manager (VMM) uses virtual machine placement (also known as intelligent placement) to evaluate the suitability of available hosts. The placement algorithm analyzes performance data for the workload and the host, and then rates hosts on a scale of one to five stars to indicate the best placement choice. The VMM placement process for a number of deployment scenarios is used as summarized in the following table.

Deployment scenario	Details
Create a new virtual machine from a disk, existing virtual machine, or template.	When you create a new virtual machine the host rating is used to offer suggestions for

Deployment scenario	Details
	selecting a host. If a self-service user creates a virtual machine, or you use drag-and-drop to move a virtual machine to a host group, the host will be assigned automatically by VMM, based on the highest rating.
Convert a physical or non-Hyper-V virtual machine	The conversion wizards provide ratings for hosts so that you can select the most appropriate host.
Migrate a virtual machine	During migration (offline, quick migration, live migration) VMM provides host ratings to help you select appropriate hosts.

Placement Improvements as of System Center 2012 SP1

As of System Center 2012 SP1, VMM includes the following:

- A number of performance enhancements for placement. In particular, as of System Center 2012 SP1, VMM displays hosts as they are rated, and you can select a suitable host before host rating is complete. With System Center 2012 – Virtual Machine Manager, a host cannot be selected until all hosts have been rated.
- Placement on clusters was improved with the following features:
    - Preferred Owners: This feature allows you to specified prioritized hosts for the virtual machine. This property is a Failover Cluster Manager setting which is used at the time of failover. When a virtual machine needs to be failed over, VMM tries to use the preferred owners first.
    - Possible Owners: This feature allows you to specify possible host owners for a virtual machine. If a host is not included in the possible owners, both VMM and Failover Cluster Manager will not allow the virtual machine to be placed on that host.
    - Availability sets: This feature allows you to identify virtual machines that should be kept on separate hosts. If you create an availability set, automatic placement will place virtual machines in line with availability set settings.
- Placement now considers defined storage classifications. Clouds can be scoped to restrict virtual machine deployment to specific storage classifications only.

Calculating Host Ratings

VMM evaluates all hosts within a selected host group and any hosts contained in child host groups. Host ratings are calculated on a scale from 0 to 5 stars, where 5 stars indicate the

highest rating. The ratings are based on default criteria. Note that host rating criteria do not include all information. For example, network connection speed is not taken into account. Ratings are based on individual hosts and not on the relative suitability of all available hosts. Ratings for one host do not change based on the ratings for other hosts. VMM calculates host ratings according to specific formulas, described in the following table.

Rating	Formula
CPU	[1 – (CPU Utilization / (100 – CPU Reserve))] x CPU Weight
Memory (RAM)	[1 – (Memory Used / (Total Memory – Memory Reserve))] x Memory Weight
Disk I/O capacity	[1 – (Disk IOPS / Maximum Disk IOPS] x Disk Weight
Network	[1 – (Network Utilization / (100 – Network Reserve))] x Network Weight

A host is rated only when a virtual machine needs to be placed. The information gathered about a host is compared to the information about the resources required by the virtual machine, and a rating is assigned to the host. During automatic placement, VMM attempts to use the host assigned the highest rating. During manual placement the host rating is shown so that you can select the appropriate host. As of System Center 2012 SP1, you can select a host in VMM even if not all hosts have been rated. The selected host must have a positive number of stars.

VMM measures CPU, memory, disk, and network usage approximately every 10 minutes to recalculate an average rating that is an average of all the measurements taken that the last action that reset the host rating. Host ratings are reset when the following happens:

- A new virtual machine is created
- A virtual machine is deployed, stored, migrated or deleted
- A virtual machine is turned on, off, or moved into a stopped, paused, or saved state.

Zero Rating

A host might be assigned a zero rating if it does not meet conditions to receive a non-zero rating. To receive a non-zero rating the following criterion are required:

- The host must have at least one hard disk with enough storage to hold the total hard disk space required by the virtual machine. With dynamic hard disks, the current hard disk size is used, not the maximum hard disk size.
- The memory required for the virtual machine must be less than the current amount of memory available on the host. A host must also have sufficient memory available to start the virtual machine.
- If dynamic memory is enabled note the following:

    - If the virtual machine (including any one of its checkpoints) is configured to use Dynamic Memory, the host should also have Dynamic Memory enabled. If it does not the placement of the virtual machine will be blocked during creation or migration.
    - For placement of a new or stopped virtual machine, the host must meet at least the startup memory requirement for the virtual machine.
    - For placement of a running virtual machine the host must meet at least the current memory requirement for the virtual machine.
    - For placement of a virtual machine in a saved state, the last known memory usage value of the virtual machine will be compared to the startup memory of the virtual machine.
- The host must contain all of the virtual networks required for the virtual machine. If you use network tags, the network location tags for the virtual machine and host must be identical.
- A host in maintenance mode automatically receives a zero rating.
- If Microsoft RemoteFX 3D video adapter is enabled on the virtual machine, note the following conditions. If these conditions are not met placement is blocked during creation or migration of the virtual machine:
    - The host must support RemoteFX.
    - The host must have one or more RemoteFX-capable graphics processing units (GPUs) with sufficient available memory. If the virtual machine is running placement will be blocked. If it is stopped or in a saved state a zero rating with a warning will be issued, but placement will not be blocked.
- Highly available virtual machines must be placed on clustered hosts. VMM assigns zero stars to hosts that are not clustered but manual placement is not blocked. If you migrate a highly-available virtual machine to a non-clustered host, the virtual machine will no longer be highly available after the migration.
- VMM blocks migration of Hyper-V hosts to hosts running different virtualization software. Migration of a virtual machine with specific features not allowed by the virtualization software that is running on a host will be blocked. For example, Hyper-V hosts do not allow booting up from a SCSI hard disk.

Understanding Generation 1 and Generation 2 Virtual Machines in VMM

In Virtual Machine Manager (VMM) in System Center 2012 R2, on a host running Windows Server 2012 R2, you can create and manage two types of virtual machines, including the newer type supported in Hyper-V in Windows Server 2012 R2, called “generation 2 virtual machines.” Before generation 2 virtual machines existed, virtual machines were all of one type, which are now referred to as “generation 1 virtual machines.” For more information, see Generation 2 Virtual Machine Overview.

A virtual machine must be either a generation 1 virtual machine or a generation 2 virtual machine. In VMM, you can use the wizards and property sheets to choose options for either a generation 1 virtual machine or a generation 2 virtual machine, but not both together.

Important

Services in VMM in System Center 2012 R2 do not support generation 2 virtual machines. When you create a service template in VMM, if you have created virtual machine templates (VM templates) that specify generation 2 virtual machines, you cannot add those templates to the service template. You can only add virtual machine templates that specify generation 1 virtual machines. Also, within a service template, in the virtual machine (tier) properties sheet, properties for a generation 1 virtual machine appear, but properties that are unique to generation 2 virtual machines do not appear.

Host requirements for generation 2 virtual machines

Generation 2 virtual machines can only run on a host with a host operating system that supports them. Windows Server 2012 R2 is an operating system that supports generation 2 virtual machines, and VMM will avoid placing generation 2 virtual machines on hosts that are running earlier operating systems. For example, VMM will avoid placing a generation 2 virtual machine on a host running Windows Server 2012.

Customizing the startup order for a generation 2 virtual machine

Because of underlying differences between generation 1 and generation 2 virtual machines, the startup order (boot order) for different devices (such as a hard disk or CD) is not handled the same way in the two generations. To customize the startup order for a generation 2 virtual machine in System Center 2012 R2, you must use a Windows PowerShell command that specifies the first boot device, rather than an ordered list of boot devices. The following list outlines the differences in the methods for customizing the startup order.

- **Customizing the startup order for generation 1 virtual machines**

  One way to customize the startup order for generation 1 virtual machines is by using the VMM console. To use the VMM console, in the wizards for adding a hardware profile, virtual machine, or virtual machine template, on the page where you configure hardware settings, under **Advanced**, in the **Firmware** section, you can modify the order of items in the **Startup order** list. Another way to customize the startup order is to use Windows PowerShell commands with the **BootOrder** parameter, which is described in more detail in TechNet topics for cmdlets such as Set-SCVirtualMachine, Set-SCVMTemplate, or Set-SCHardwareProfile.

- **Customizing the startup order for generation 2 virtual machines**

  To customize the first boot device for generation 2 virtual machines, you must use Windows PowerShell commands with the **FirstBootDevice** parameter. By default, the first boot device is set to a virtual hard disk—either the virtual hard disk marked as **Contains the operating**

system for the virtual machine, or the only virtual hard disk, if the virtual machine has only one.

The **FirstBootDevice** parameter is described in more detail in TechNet topics for cmdlets, such as Set-SCVirtualMachine, Set-SCVMTemplate, or Set-SCHardwareProfile. For example, you could run the following command to configure an existing virtual machine template called **Generation2template** so that the first boot device is the first network adapter. This command is based on the assumption that the network adapter supports the Pre-Boot Execution Environment (PXE):

```
Set-SCVMTemplate -Template "Generation2template" –
FirstBootDevice "NIC,0"
```

Creating a virtual machine or virtual machine template and specifying the generation

When you use a wizard to create a new virtual machine or virtual machine template in VMM in System Center 2012 R2, VMM responds to your selections as follows:

- If you use a virtual hard disk in .vhd format (the older format) as the starting point for a virtual machine or virtual machine template, it automatically becomes generation 1, because generation 2 virtual machines support only the .vhdx format. In this situation, you do not see the **Generation** list box on the second page of the wizard, and you cannot select the generation.
- If you use a virtual hard disk in .vhdx format (the newer format) as the starting point for the virtual machine or virtual machine template, when you reach the second page of the wizard (the **Identity** page), you have two choices for the virtual machine or virtual machine template: **Generation 1** or **Generation 2**. By default, **Generation 1** is selected.

  This guideline also applies if you create a virtual machine and choose **Create the new virtual machine with a blank virtual hard disk**. With this option, the blank disk uses the .vhdx format.
- If you use an existing virtual machine or virtual machine template as the starting point for a new virtual machine or virtual machine template, the generation is determined by the existing virtual machine or virtual machine template.
- If you create a hardware profile (to make it easier to consistently apply the same hardware settings to multiple virtual machines or virtual machine templates), on the first page of the New Hardware Profile Wizard, you must choose between **Generation 1** or **Generation 2**. By default, **Generation 1** is selected.

  When you later incorporate the hardware profile into a virtual machine or virtual machine template, in the respective wizard, the generation of the virtual machine or virtual machine template is determined on the first or second page (as described earlier in this list). Then, on the wizard page that contains the **Hardware profile** list box, the only hardware profiles that appear are those of the same generation as the virtual machine or virtual machine template that you are creating.

After the generation has been determined for a hardware profile, virtual machine, or virtual machine template, as you progress through a wizard, the capabilities that do not apply to that generation are either absent or they appear dimmed. For example, if you select **Generation 1** on the **Identity** page, when you advance to the **Configure Hardware** page, under **Bus Configuration**, **IDE Devices** appears. IDE devices are found only in generation 1 virtual machines. In contrast, if you select **Generation 2** on the **Identity** page, when you advance to the **Configure Hardware** page, under **Bus Configuration**, **IDE Devices** does not appear. Instead, for the **SCSI Adapters** that appear, attached devices are shown, which reflects the unique capability in generation 2 virtual machines to boot from a SCSI-attached virtual hard disk.

Similarly, with a Windows PowerShell command, if you try to combine the unique capabilities of both generations into one virtual machine or virtual machine template, the command does not succeed, and an error message is displayed. Also, if you try to modify an existing virtual machine or virtual machine template by adding options from the other generation, the command does not succeed, and an error message is displayed. For more information about the unique capabilities in generation 2 virtual machines, see Generation 2 Virtual Machine Overview.

See Also

Creating and Deploying Virtual Machines in VMM

How to Create a Virtual Machine Template

How to Create a Hardware Profile

Generation 2 Virtual Machine Overview

Requirements for Linux-Based Virtual Machines

As of System Center 2012 Service Pack 1 (SP1), Virtual Machine Manager supports virtual machines that contain Linux as the guest operating system. There are two requirements when creating such virtual machines, as follows:

- Linux Integration Services (LIS) must be installed on the virtual machine. By default, LIS is included with some distributions of Linux. If LIS is not included in the distribution of Linux that you are using for the virtual machine, then you must manually install it.
  - For more information about installing LIS for Hyper-V on Windows 2008 R2, see About Virtual Machines and Guest Operating Systems.
  - For more information about installing LIS for Hyper-V on Windows Server 2012, see Hyper-V Overview and the section titled ‘Software requirements (for supported guest operating systems)’ in the Introduction to the Linux Integration Components blog.
- The VMM guest agent for Linux must be installed on the virtual machine. It is required for service template integration, and it allows you to modify properties on the Linux computer such as the host name. For instructions on how to accomplish that, see How to Install the VMM Agent for Linux

VMM does not verify that the virtual machine meets these requirements. However, if these requirements are not met, the virtual machine will fail to deploy.

See Also

Create a Linux-Based Virtual Machine Template Scenario

How to Install the VMM Agent for Linux

When creating a virtual machine with Linux as the guest operating system, you must install the VMM agent for Linux on that virtual machine. Use the following procedure to perform that task.

To install the VMM agent for Linux on a virtual machine

1. On the VMM management server, open a command prompt session, with administrative rights.
2. Go to the 'c:\Program Files\Microsoft System Center 2012\Virtual Machine Manager\agents\Linux' folder.
3. Copy all the agent installation files from that folder to a new folder on the virtual machine, and then, on the virtual machine on which Linux is running as a guest operating system, open the new folder.
4. Run the following command:

   ```
   chmod +x install
   ```

5. Run either of the following commands, as appropriate:

   ```
   ./install scvmmguestagent.1.0.0.544.x64.tar
   ./install scvmmguestagent.1.0.0.544.x86.tar
   ```

   The following folders and files are created on the virtual hard disk during the installation of the VMM agent for Linux:

   - A default installation folder - /opt/microsoft/scvmmguestagent
   - A default log files folder - /var/opt/microsoft/scvmmagent/log
   - An installation log file - scvmm-install.log
   - A specialization log file - scvmm.log. This file is created when the virtual machine is deployed and specialized.
   - A configuration file - scvmm.conf. This file contains the location of the log file and is used to control logging during deployment and specialization.

How to Create and Deploy a Virtual Machine from a Blank Virtual Hard Disk

Use the following procedure to create a virtual machine from a blank virtual hard disk in Virtual Machine Manager. After you create the virtual machine, you can install an operating system from an .iso image, from a CD or DVD, or from a network boot if a Pre-Boot Execution Environment (PXE) server is available.

Before you complete this procedure, note the following:

- To complete the procedure, you must be a member of the Administrator or Delegated Administrator user role, or you must be a self-service user who has the **Deploy** action in the scope of their user role.
- For a self-service user to store a virtual machine in the library, the following is required:
  - The self-service user role must have the **Store and re-deploy** action assigned.
  - The self-service user must first deploy the virtual machine to a private cloud, and then store it in the library.
- Static IP address settings can only be customized when you create a virtual machine from a virtual machine template.
- As of System Center 2012 Service Pack 1 (SP1), you can use VMM to configure the availability settings for the virtual machine. For more information, see Configuring Availability Options for Virtual Machines Overview.

Creating a Virtual Machine

Use the following procedure to create a virtual machine from a blank virtual hard disk.

To create a virtual machine from a blank virtual hard disk

1. Open the **VMs and Services** workspace.
2. On the **Home** tab, click the **Create Virtual Machine** drop-down arrow, and then click **Create Virtual Machine**.

   The **Create Virtual Machine Wizard** opens.
3. On the **Select Source** page, click **Create the new virtual machine with a blank virtual hard disk**, and then click **Next**.
4. Specify identity options as follows, and then click **Next**:
   - With VMM in System Center 2012 SP1 or System Center 2012, on the **Specify Virtual Machine Identity** page, enter the virtual machine name and optional description.
   - With VMM in System Center 2012 R2, on the **Identity** page, enter the virtual machine name and an optional description. In the **Generation** box, select **Generation 1** or **Generation 2**. For more information, see Understanding Generation 1 and Generation 2 Virtual Machines in VMM.

5. On the **Configure Hardware** page, either select the profile that you want to use from the **Hardware profile** list, or configure the hardware settings manually, and then click **Next**. Note the following:
   - In **Compatibility**, if you want to deploy the virtual machine to a private cloud, select a capability profile that is available to the private cloud.
   - With VMM in System Center 2012 R2, the hardware profiles and hardware options that are available are those of the generation that you selected in the previous step. For more information, see Understanding Generation 1 and Generation 2 Virtual Machines in VMM.
   - In **Bus Configuration**, if you want to install an operating system from a DVD or an .iso image, ensure there is a virtual DVD drive that is configured to use an available option such as the **Existing ISO image file** option. If you want to use an ISO image file, the file must be present in the VMM library.
   - If you want to store the virtual machine in the VMM library before you deploy it to a host, use of one of the blank virtual hard disks that by default are provided in the VMM library. Do this as follows:
     i. In **Bus Configuration**, click the virtual hard disk.
     ii. In the details pane, click **Use an existing virtual hard disk**. Then click **Browse**. Click one of the blank disk choices, and then click **OK**.
   - If you are running VMM in System Center 2012 SP1 or System Center 2012, and if the virtual machine starts from the network to install an operating system, in **Network Adapters**, ensure to use the legacy network adapter type. This type is indicated by the network adapter name, for example, **Legacy Network Adapter 1**.
   - If you are running VMM in System Center 2012 R2, and if the virtual machine is a generation 1 virtual machine that will boot from the network to install an operating system, in **Network Adapters**, use the legacy network adapter type. This type is indicated by the network adapter name, for example, **Legacy Network Adapter 1**.
6. On the **Select Destination** page, specify how the virtual machine should be deployed:
   - Select **Deploy the virtual machine to a private cloud** to place the virtual machine in an existing private cloud. Then follow the instructions in Deploying the virtual machine in a private cloud.
   - Select **Place the virtual machine on a host** to place the virtual machine on an existing virtual machine host. Then follow the instructions in Deploying the virtual machine on a host.
   - Select **Store the virtual machine in the library** to store the virtual machine. Then follow the instructions in Storing the virtual machine in the library.

Deploying the virtual machine in a private cloud

Use the following procedure to deploy the virtual machine in a private cloud.

To deploy the virtual machine in a private cloud

1. On the **Select Cloud** page, select the private cloud on which you want to place the virtual

machine. If you are connected as an Administrator, you can select the host on which the virtual machine should be deployed in the private cloud. The cloud suggestions are based on a 0-5 star rating. For more information, see Understanding Virtual Machine Placement and Ratings in VMM. Verify the settings and modify if required:

- **Expected utilization**—For a virtual machine that is created from a blank hard disk, the expected utilization is based on standard defaults. For a virtual machine that is created from an existing virtual machine, the default settings are based on past performance of the existing machine. VMM updates host suggestions and ratings in response to modifications made to the expected virtual machine utilization.
- **Make this VM highly available**—With this option selected, only hosts that are located in a cluster are available for selection.
- **Details**—Indicates the status of the host, the operating system, and the type and status of the virtualization software.
- **Rating Explanation**—Provides an explanation if a host received a zero rating.
- **SAN Explanation** or **Deployment and Transfer Explanation**—Lists any factors that make a storage area network (SAN) transfer unavailable. VMM does not recognize a virtual machine that is stored on a SAN as available for deployment by using SAN transfer if the virtual machine was stored directly in the library when it was created or was added to the library during a library refresh. To avoid this issue, deploy the virtual machine to a host by using a LAN transfer, and then store the virtual machine in the same VMM library, library share, and logical unit number (LUN).

  In addition, in System Center 2012 R2 Virtual Machine Manager, the **Deployment and Transfer Explanation** tab provides an explanation if fast file copy could not be used. Fast file copy is a new feature in System Center 2012 R2 Virtual Machine Manager that is based on the Windows Offloaded Data Transfers (ODX) feature, which is introduced in Windows Server 2012 R2. For information about ODX, see Windows Offloaded Data Transfers Overview.

2. On the **Configure Settings** page, review the virtual machine settings:
   a. In **Locations**, either accept the default virtual machine path on the host to store the virtual machine files, or click **Browse** to specify a different location. Optionally, select the **Add this path to the list of default virtual machine paths on the host** check box.
   b. In **Machine Resources**, click **Virtual Hard Disk**. Accept the default values, or select a different destination path on the host for the virtual hard drive file (.vhd or .vhdx file). To change the file name, enter a new name in the **File name** box.

   Tip
   To prevent placement from choosing a different value for these settings, click the pin icon next to the setting. Note that self-service users do not see this option.
3. On the **Select Networks** page, if the page appears, optionally, select the virtual machine network that you want to use, the virtual network, and the virtual LAN (VLAN) ID, if applicable, and then click **Next**.
4. On the **Add Properties** page, configure the action to take when the host starts or stops,

and the operating system that you will install on the virtual machine. Click **Next.**

5. On the **Summary** page, confirm the settings, and then click **Create**. To confirm that the virtual machine was created, in the **VMs and Services** workspace, in the **VMs and Services** pane, expand **Clouds**, and then click the private cloud where you deployed the virtual machine. On the **Home** tab, in the **Show** group, click **VMs**. The virtual machine appears in the **VMs** pane.

Deploying the virtual machine on a host

Use the following procedure to deploy the virtual machine on a host.

To deploy the virtual machine on a host

1. On the **Select Host** page, view the ratings, click the host on which you want to deploy the virtual machine, and then click **Next**. The host suggestions are based on a 0-5 star rating. For more information, see Understanding Virtual Machine Placement and Ratings in VMM. Note the following settings:
   - **Expected utilization**—For a virtual machine that is created from a blank hard disk, the expected utilization is based on standard defaults. For a virtual machine that is created from an existing virtual machine, the default settings are based on past performance of the existing machine. VMM updates host suggestions and ratings in response to modifications that are made to the expected virtual machine utilization.
   - **Make this VM highly available**—With this option selected, only hosts in a cluster are available for selection.
   - **Details**—Indicates the status of the host, the operating system, and the type and status of the virtualization software.
   - **Rating Explanation**—Provides an explanation if a host received a zero rating.
   - **SAN Explanation** or **Deployment and Transfer Explanation**—Lists any factors that make a SAN transfer unavailable. VMM does not recognize a virtual machine that is stored on a SAN as available for deployment by using SAN transfer if the virtual machine was stored directly in the library when it was created or was added to the library during a library refresh. To avoid this issue, deploy the virtual machine to a host by using a LAN transfer, and then store the virtual machine in the same VMM library, library share, and logical unit number (LUN).

     In addition, in System Center 2012 R2 Virtual Machine Manager, the **Deployment and Transfer Explanation** tab provides an explanation if fast file copy could not be used. Fast file copy is a new feature in System Center 2012 R2 Virtual Machine Manager that is based on the Windows Offloaded Data Transfers (ODX) feature, which is introduced in Windows Server 2012 R2. For information about ODX, see Windows Offloaded Data Transfers Overview.
2. On the **Configure Settings** page, review the settings for the virtual machine:
   a. In **Locations**, either accept the default virtual machine path on the host to store the virtual machine files, or click **Browse** to specify a different location. Optionally, select the **Add this path to the list of default virtual machine paths on the host** check

box.

b. In **Machine Resources**, click **Virtual Hard Disk**. Accept the default values, or select a different destination path on the host for the virtual hard drive file (.vhd or .vhdx file). To change the file name, enter a new name in the **File name** box.

Tip
To prevent placement from choosing a different value for these settings, click the pin icon next to the setting. Note that self-service users do not see this option.

3. On the **Select Networks** page, if the page appears, optionally, select the virtual machine network that you want to use, the virtual network, and the virtual LAN (VLAN) ID, if applicable, and then click **Next**.
4. On the **Add Properties** page, configure the action to take when the host starts or stops, and the operating system to install on the virtual machine. Then click **Next**.
5. On the **Summary** page, confirm the settings, and then click **Create**.

Storing the virtual machine in the library

Use the following procedure to store the virtual machine in the library.

To store the virtual machine in the library

1. On the **Select Library Server** page, click the library server that you want to use, and then click **Next**.
2. On the **Select Path** page, specify the library share location to store the virtual machine. Click **Browse** to select a library share and an optional folder location, click **OK**, and then click **Next**.
3. On the **Summary** page, confirm the settings, and then click **Create**.
4. To confirm that the virtual machine was created, in the **Library** workspace, in the **Library** pane, expand **Library Servers**, expand the library server where you stored the virtual machine, and then click **Stored Virtual Machines and Services**. The stored virtual machine appears in the **Physical Library Objects** pane.

See Also

Configuring Virtual Machine Settings in VMM

How to Create and Deploy a Virtual Machine from an Existing Virtual Hard Disk

Use the following procedure in to create a virtual machine from an existing virtual hard disk that is stored in the Virtual Machine Manager (VMM) library.

Before you complete this procedure, note the following:

- To complete this procedure, you must be a member of the Administrator or Delegated Administrator user role, or a self-service user who has the **Deploy** action in the user role scope.
- For a self-service user to store a virtual machine in the library, the following is required:
  - The self-service user role must have the **Store and re-deploy** action assigned.
  - The self-service user must first deploy the virtual machine to a private cloud, and then store it in the VMM library.
- The virtual hard disk that you want to use must be stored in the VMM library. If the virtual hard disk currently exists on another computer or device, copy it to the VMM library. For instructions, see How to Add File-Based Resources to the VMM Library.
- Use a virtual hard disk that has been generalized by using the Sysprep tool. If you do not use a generalized virtual hard disk, the identity of the new virtual machine will be the same as the source. Issues might occur if you turn on two virtual machines with the same identity at the same time.

Creating a virtual machine

Use the following procedure to create a virtual machine from an existing virtual hard disk.

To create a virtual machine from an existing virtual hard disk

1. Open the **VMs and Services** workspace.
2. On the **Home** tab, click the **Create Virtual Machine** drop-down arrow, and then click **Create Virtual Machine**.

   The **Create Virtual Machine Wizard** opens.
3. On the **Select Source** page, click **Use an existing virtual machine, VM template, or virtual hard disk**, and then click **Browse**.
4. In the **Select Virtual Machine Source** dialog box, select an existing virtual hard disk file, and then click **OK**.
5. On the **Select Source** page, click **Next**.
6. Specify identity options as follows, and then click **Next**:
   - With VMM in System Center 2012 SP1 or System Center 2012, on the **Specify Virtual Machine Identity** page, enter the virtual machine name and an optional description.
   - With VMM in System Center 2012 R2, on the **Identity** page, enter the virtual machine name and an optional description.

     If the virtual hard disk file that you selected on the previous page uses the .vhdx file format, the **Generation** box also appears. In the **Generation** box, select **Generation 1** or **Generation 2**. For more information, see Understanding Generation 1 and Generation 2 Virtual Machines in VMM.
7. On the **Configure Hardware** page, either select the profile that you want to use from the **Hardware profile** list, or configure the hardware settings manually. Then click **Next**. In **Compatibility**, if you want to deploy the virtual machine to a private cloud, select a

capability profile that is available to the private cloud.

8. On the **Select Destination** page, specify how the virtual machine should be deployed:
   - Select **Deploy the virtual machine to a private cloud** to place the virtual machine in an existing private cloud. Then follow the instructions in Deploying the virtual machine in a private cloud.
   - Select **Place the virtual machine on a host** to place the virtual machine on an existing virtual machine host. Then follow the instructions in Deploying the virtual machine on a host.
   - Select **Store the virtual machine in the library** to store to virtual machine. Then follow the instructions in Storing the virtual machine in the library.

Deploying the virtual machine in a private cloud

Use the following procedure to deploy the virtual machine in a private cloud.

To deploy the virtual machine in a private cloud

1. On the **Select Cloud** page, select the private cloud on which you want to place the virtual machine. If you are connected as an administrator, you can select the host on which the virtual machine should be deployed in the private cloud. The private cloud suggestions are based on a 0-5 star rating. For more information, see Understanding Virtual Machine Placement and Ratings in VMM. Verify the settings and modify if required:
   - **Expected utilization**—For a virtual machine that is created from a blank hard disk, the expected utilization is based on standard defaults. For a virtual machine that is created from an existing virtual machine, the default settings are based on past performance of the existing machine. VMM updates host suggestions and ratings in response to modifications that are made to the expected virtual machine utilization.
   - **Make this VM highly available**—With this option selected, only hosts located in a cluster available for selection.
   - **Details**—Indicates the status of the host, the operating system, and the type and status of virtualization software.
   - **Rating Explanation** or **Deployment and Transfer Explanation**—Provides an explanation if a host received a zero rating.
   - **SAN Explanation** or **Deployment and Transfer Explanation**—Lists any factors that make a storage area network (SAN) transfer unavailable. VMM does not recognize a virtual machine that is stored on a SAN as available for deployment using SAN transfer if the virtual machine was stored directly in the VMM library when it was created, or was added to the library during a library refresh. To avoid this issue, deploy the virtual machine to a host by using a LAN transfer, and then store the virtual machine in the same VMM library, library share, and logical unit number (LUN).

     In addition, in System Center 2012 R2 Virtual Machine Manager, the **Deployment and Transfer Explanation** tab provides an explanation if fast file copy cannot be used. Fast file copy is a new feature in System Center 2012 R2 Virtual Machine

Manager that is based on the Windows Offloaded Data Transfers (ODX) feature that is introduced in Windows Server 2012 R2. For information about ODX, see Windows Offloaded Data Transfers Overview.

2. On the **Configure Settings** page, review the virtual machine settings:
   a. In **Locations**, either accept the default virtual machine path on the host to store the virtual machine files, or click **Browse** to specify a different location. Optionally, select the **Add this path to the list of default virtual machine paths on the host** check box.
   b. Under **Machine Resources**, click **Virtual Hard Disk**. Accept the default values or select a different destination path on the host for the virtual hard drive file (.vhd or .vhdx file). To change the file name, enter a new name in the **File name** box.

   Tip
   To prevent placement from choosing a different value for these settings, click the pin icon next to the setting. Note that self-service users do not see this option.
3. On the **Add Properties** page, configure the action to take when the host starts or stops. If you are an administrator, to prevent the virtual machine from being migrated by Performance and Resource Optimization (PRO) or dynamic optimization, select the **Exclude virtual machine from optimization actions** check box. When you have finished this step, click **Next**.
4. On the **Summary** page, confirm the settings, and then click **Create**.
5. To confirm that the virtual machine was created, in the **VMs and Services** workspace, in the **VMs and Services** pane, expand **Clouds**, and then click the private cloud where you deployed the virtual machine. On the **Home** tab, in the **Show** group, click **VMs**. The virtual machine appears in the **VMs** pane.

Deploying the virtual machine on a host

Use the following procedure to deploy the virtual machine on a host.

To deploy the virtual machine on a host

1. On the **Select Host** page, view the ratings, click the host on which you want to deploy the virtual machine, and then click **Next**. The host suggestions are based on a 0-5 star rating. For more information, see Understanding Virtual Machine Placement and Ratings in VMM. Note the following settings:
   - **Expected utilization**—For a virtual machine that is created from a blank hard disk, the expected utilization is based on standard defaults. For a virtual machine that is created from an existing virtual machine, the default settings are based on past performance of the existing virtual machine. VMM updates the host suggestions and ratings in response to modifications that are made to the expected virtual machine utilization.
   - **Make this VM highly available**—With this option selected, only hosts that are located in a cluster are available for selection.

- **Details**—Indicates the status of the host, the operating system, and the type and status of virtualization software.
- **Rating Explanation**—Provides an explanation if a host received a zero rating.
- **SAN Explanation** or **Deployment and Transfer Explanation**—Lists any factors that make a SAN transfer unavailable. VMM does not recognize a virtual machine that is stored on a SAN as available for deployment using SAN transfer if the virtual machine was stored directly in the VMM library when it was created, or if it was added to the VMM library during a library refresh. To avoid this issue, deploy the virtual machine to a host by using a LAN transfer, and then store the virtual machine in the same VMM library, library share, and logical unit number (LUN).

  In addition, in System Center 2012 R2 Virtual Machine Manager, the **Deployment and Transfer Explanation** tab provides an explanation if fast file copy could not be used. Fast file copy is a new feature in System Center 2012 R2 Virtual Machine Manager that is based on the Windows Offloaded Data Transfers (ODX) feature that is introduced in Windows Server 2012 R2. For information about ODX, see Windows Offloaded Data Transfers Overview.

2. On the **Configure Settings** page, review the settings for the virtual machine:
   a. In **Locations**, either accept the default virtual machine path on the host for storing the virtual machine files, or click **Browse** to specify a different location. Optionally, select the **Add this path to the list of default virtual machine paths on the host** check box.
   b. In **Networking**, click a network adapter to view the configured network settings.
   c. In **Machine Resources**, click **Virtual Hard Disk**. Accept the default values, or select a different destination path on the host for the virtual hard drive file (.vhd or .vhdx file). To change the file name, enter a new name in the **File name** box.

   Tip
   To prevent placement from choosing a different value for these settings, click the pin icon next to the setting. Note that self-service users do not see this option.
3. On the **Select Networks** page, if it appears, optionally select the logical network that you want to use, the virtual network, and the virtual LAN (VLAN) ID, if applicable, and then click **Next**.
4. On the **Add Properties** page, configure the action to take when the host starts or stops, and the operating system that you will install on the virtual machine. To prevent the virtual machine from being migrated by Performance and Resource Optimization (PRO) or dynamic optimization, select the **Exclude virtual machine from optimization actions** check box. When you have finished this step, click **Next**.
5. On the **Summary** page, confirm the settings, and then click **Create**.

Storing the virtual machine in the library

Use the following procedure to store the virtual machine in the VMM library.

To store the virtual machine in the library

1. On the **Select Library Server** page, click the library server that you want to use, and then click **Next**.
2. On the **Select Path** page, specify the library share location to store the virtual machine. Click **Browse** to select a library share and optional folder location, click **OK**, and then click **Next**.
3. On the **Summary** page, confirm the settings, and then click **Create**.

To confirm that the virtual machine was created, in the **Library** workspace, in the **Library** pane, expand **Library Servers**, expand the library server where you stored the virtual machine, and then click **Stored Virtual Machines and Services**. The stored virtual machine appears in the **Physical Library Objects** pane.

See Also

Configuring Virtual Machine Settings in VMM

How to Create and Deploy a Virtual Machine from an Existing Virtual Machine

Use the following procedure to use Virtual Machine Manager (VMM) to create a virtual machine by *cloning* an existing virtual machine. You can also use cloning to create backups of existing virtual machines.

Note the following:

- You must be a member of the Administrator or Delegated Administrator user role, or a self-service user who has the **Deploy** action in the scope of the role to complete this procedure.
- When you clone a virtual machine, the existing virtual machine source is not deleted. We recommend that you clone a virtual machine that has been prepared and generalized with the Sysprep tool. If you do not use a generalized virtual hard disk, the identity of the new virtual machine will be the same as the source. Issues might occur if you turn on two virtual machines with the same identity at the same time.
- You can clone a virtual machine that is deployed on a host, or a virtual machine that is stored in the VMM library. In VMM in System Center 2012 SP1 and System Center 2012, to clone a virtual machine that is deployed on a host, the virtual machine must either be stopped or be in a saved state. As of System Center 2012 R2, for Hyper-V hosts that are running Windows Server 2012 R2, the virtual machine can either be online, be stopped, or be in a saved state.
- In System Center 2012 R2, the option to use differencing disk optimizations is automatically applied when you deploy the virtual machine on a host, and when a base disk exists on that host.
- For a self-service user to store a virtual machine in the VMM library, the following is required:

a. The self-service user role must have the **Store and re-deploy** action assigned.
b. The self-service user must first deploy the virtual machine to a private cloud, and then store it in the VMM library.

Creating a virtual machine

Use the following procedure to create a virtual machine from an existing virtual machine.

To create a virtual machine from an existing virtual machine

1. Open the **VMs and Services** workspace.
2. On the **Home** tab, in the **Create** group, click the **Create Virtual Machine** drop-down arrow, and then click **Create Virtual Machine**.

   The **Create Virtual Machine Wizard** opens.
3. On the **Select Source** page, ensure that **Use an existing virtual machine, VM template, or virtual hard disk** is selected, click **Browse**, click the existing virtual machine, and then click **OK**.
4. On the **Select Source** page, click **Next**.
5. On the **Identity/Specify Virtual Machine Identity** page, enter a new name for the virtual machine name and an optional description.
6. On the **Configure Hardware** page, optionally configure any available settings, and then click **Next**.
7. On the **Select Destination** page, select one of the following:
   - Select **Deploy the virtual machine to a private cloud** to place the virtual machine in an existing private cloud. Then follow the instructions in Deploying the virtual machine in a private cloud.
   - Select **Place the virtual machine on a host** to place the virtual machine on an existing virtual machine host. Then follow the instructions in Deploying the virtual machine on a host.
   - Select **Store the virtual machine in the library** to store the virtual machine before deployment. Then follow the instructions in Storing the virtual machine in the library.

Deploying the virtual machine in a private cloud

1. On the **Select Cloud** page, select the private cloud on which you want to place the virtual machine. If you are connected as an administrator, you can select the host on which the virtual machine should be deployed in the private cloud. The cloud suggestions are based on a 0-5 star rating. For more information, see Understanding Virtual Machine Placement and Ratings in VMM. Verify the settings and modify them if required:
   - **Expected utilization**—For a virtual machine that is created from a blank hard disk, the expected utilization is based on standard defaults. For a virtual machine created that is created from an existing virtual machine, the default settings are based on past performance of the existing virtual machine. VMM updates host suggestions and ratings in response to modifications that are made to the expected virtual machine utilization.

- **Make this VM highly available**—With this option selected, only hosts that are located in a cluster are available for selection.
- **Details**—Indicates the status of the host, the operating system, and the type and status of virtualization software.
- **Rating Explanation**—Provides an explanation if a host received a zero rating.
- **SAN Explanation** or **Deployment and Transfer Explanation**—Lists any factors that make a storage area network (SAN) transfer unavailable. VMM does not recognize a virtual machine that is stored on a SAN as available for deployment using SAN transfer if the virtual machine was stored directly in the VMM library when it was created, or was added to the library during a library refresh. To avoid this issue, deploy the virtual machine to a host by using a LAN transfer, and then store the virtual machine in the same VMM library, library share, and logical unit number (LUN).

  In addition, in System Center 2012 R2 Virtual Machine Manager, the **Deployment and Transfer Explanation** tab provides an explanation if fast file copy cannot be used. Fast file copy is a new feature in System Center 2012 R2 Virtual Machine Manager that is based on the Windows Offloaded Data Transfers (ODX) feature that is introduced in Windows Server 2012 R2. For information about ODX, see Windows Offloaded Data Transfers Overview.

2. On the **Configure Settings** page, review the virtual machine settings:
   a. In **Locations**, either accept the default virtual machine path on the host for storing the virtual machine files, or click **Browse** to specify a different location. Optionally, select the **Add this path to the list of default virtual machine paths on the host** check box.
   b. In **Machine Resources**, click **Virtual Hard Disk**. Accept the default values or select a different destination path on the host for the virtual hard drive file (.vhd or .vhdx file). To change the file name, enter a new name in the **File name** box.

   Tip
   To prevent placement from choosing a different value for these settings, click the pin icon next to the setting. Note that self-service users do not see this option.
3. On the **Select Networks** page, if the page appears, optionally select the logical network that you want to use, the virtual network, and the virtual LAN (VLAN) ID, if applicable, and then click **Next**.
4. On the **Add Properties** page, configure the action to take when the host starts or stops, and then click **Next**.
5. On the **Summary** page, confirm the settings, and then click **Create**. To confirm that the virtual machine was created, in the **VMs and Services** workspace, in the **VMs and Services** pane, expand **Clouds**, and then click the private cloud where you deployed the virtual machine. On the **Home** tab, in the **Show** group, click **VMs**. The virtual machine appears in the **VMs** pane.

Deploying the virtual machine on a host

1. On the **Select Host** page, review the placement ratings and transfer type, click a host, and then click **Next**. Note the following settings:

- **Expected Utilization**—For a virtual machine that is created from a blank hard disk, the expected utilization is based on standard defaults. For a virtual machine that is created from an existing virtual machine, the default settings are based on past performance of the existing virtual machine. VMM updates host suggestions and ratings in response to modifications that are made to the expected virtual machine utilization.
- **Make this VM highly available**—With this option selected, only hosts in a cluster available for selection.
- **Details**—Indicates the status of the host, the operating system, and the type and status of virtualization software.
- **Rating Explanation**—Provides an explanation if a host received a zero rating.
- **SAN Explanation** or **Deployment and Transfer Explanation**—Lists any factors that make a storage area network (SAN) transfer unavailable. VMM does not recognize a virtual machine that is stored on a SAN as available for deployment using SAN transfer if the virtual machine was stored directly in the VMM library when it was created, or was added to the library during a library refresh. To avoid this issue, deploy the virtual machine to a host by using a LAN transfer, and then store the virtual machine in the same VMM library, library share, and logical unit number (LUN).

  In addition, in System Center 2012 R2 Virtual Machine Manager, the **Deployment and Transfer Explanation** tab provides an explanation if fast file copy cannot be used. Fast file copy is a new feature in System Center 2012 R2 Virtual Machine Manager that is based on the Windows Offloaded Data Transfers (ODX) feature that is introduced in Windows Server 2012 R2. For information about ODX, see Windows Offloaded Data Transfers Overview.

2. On the **Configure Settings** page, review the settings for the virtual machine:
   a. In **Locations**, either accept the default virtual machine path on the host for storing the virtual machine files, or click **Browse** to specify a different location. Optionally, select the **Add this path to the list of default virtual machine paths on the host** check box.
   b. In **Machine Resources**, click **Virtual Hard Disk**. Accept the default values, or select a different destination path on the host for the virtual hard drive file (.vhd or .vhdx file). To change the file name, enter a new name in the **File name** box.

   Tip
   To prevent placement from choosing a different value for these settings, click the pin icon next to the setting. Note that self-service users do not see this option.
3. On the **Select Networks** page, accept or change the logical network, virtual network, or VLAN ID if applicable, and then click **Next**.
4. On the **Add Properties** page, configure the action to take when the host starts or stops. Then click **Next**.
5. On the **Summary** page, confirm the settings, and then click **Create**.

Storing the virtual machine in the library

1. On the **Select Library Server** page, click the library server that you want to use, and then click **Next**.

2. On the **Select Path** page, specify the library share location to store the virtual machine. Click **Browse** to select a library share and optional folder location, click **OK**, and then click **Next**.
3. On the **Summary** page, confirm the settings, and then click **Create**.

   To confirm that the virtual machine was created, in the **Library** workspace, in the **Library** pane, expand **Library Servers**, expand the library server where you stored the virtual machine, and then click **Stored Virtual Machines and Services**. The stored virtual machine appears in the **Physical Library Objects** pane.

See Also

Configuring Virtual Machine Settings in VMM

How to Create and Deploy a Virtual Machine from a Template

Use the following procedure to create a virtual machine from a virtual machine template in Virtual Machine Manager (VMM). You can use a virtual machine template to create new stand-alone virtual machines or to create tiers in a service template. For more information about service templates, see Creating Service Templates in VMM.

Note the following:

- Server roles and features, application installation, and settings on an instance of Microsoft SQL Server apply only when a virtual machine template is used for service deployments. For stand-alone virtual machine creation, these settings are not used and are not visible when you use a template with these settings to create a virtual machine.
- To configure a virtual machine to use static IP addresses from an IP address pool that is managed by VMM, you must use a virtual machine template as the source.
- To complete this procedure, you must be a member of the Administrator, the Delegated Administrator, or the self-service user role.
- For a self-service user to deploy a virtual machine from a template, the following is required:
  - The self-service user role must have the **Deploy** or **Deploy (From template only)** actions in their user role scope.
  - The template must be available to the self-service user role as an assigned resource, or the self-service user role must be granted access in the template properties.

  For information about how to assign resources to a self-service role, see How to Create a Self-Service User Role in VMM. For information about how self-service users can share resources between self-service user roles, see How to Enable Self-Service Users to Share Resources in VMM.
- As of System Center 2012 Service Pack 1 (SP1), if you are a member of an Administrator or Delegated Administrator role, you can use VMM to configure availability settings for the

virtual machine. For more information, see Configuring Availability Options for Virtual Machines Overview.

Creating a virtual machine

Use the following procedure to create a virtual machine from a template.

To create a virtual machine from a template

1. Open the **VMs and Services** workspace.
2. On the **Home** tab, in the **Create** group, click the **Create Virtual Machine** drop-down arrow, and then click **Create Virtual Machine**.

   The Create Virtual Machine Wizard opens.
3. On the **Select Source** page, ensure that **Use an existing virtual machine, VM template, or virtual hard disk** is selected, and then click **Browse**.
4. In the **Select Virtual Machine Source** dialog box, click the appropriate virtual machine template, and then click **OK**.

   Note
   If the template contains Windows Server roles and features, application deployment, or SQL Server deployment settings, you receive a message that these settings will be ignored for stand-alone virtual machine deployment. Click **OK** to continue.
5. On the **Select Source** page, click **Next**.
6. On the **Identity/Specify Virtual Machine Identity** page, enter the virtual machine name and optional description, and then click **Next**.
7. On the **Configure Hardware** page, either select the profile that you want to use from the **Hardware profile** list, or configure the hardware settings manually. After you have configured the hardware settings, click **Next**. Note the following:
   - In **Capability**, you must select a capability profile that is supported by the private cloud.
   - In **Network Adapters**, if you configure a network adapter to use static IP addresses, you must also set the MAC address to **Static**.

     Warning
     In System Center 2012 (without Service Pack 1), the **Enable spoofing of MAC addresses** check box is inaccurate and does not actually change the setting. However, this setting is required to deploy a service to a Hyper-V host running Windows Server 2008 R2 (with or without Service Pack 1) that has Network Load Balancing enabled. Enable MAC spoofing by using the VMM command shell to update either the virtual machine template or the hardware profile that you plan to use in templates. To update a virtual machine template, type the following on the Windows PowerShell command line, where *VMTemplate01* represents the name of the virtual machine

template:

```
PS C:\> $VMTemplate = Get-SCVMTemplate -Name "VMTemplate01"
PS C:\> $VirtNetworkAdapter = Get-SCVirtualNetworkAdapter -
VMTemplate $VMTemplate
PS C:\> Set-SCVirtualNetworkAdapter -VirtualNetworkAdapter
$VirtNetworkAdapter -EnableMACAddressSpoofing $True
```

For more information, see How to Configure NLB for a Service Tier.

- In **Network Adapters**, for a virtual machine that uses a virtual hard disk in the VMware .vmdk format, be sure to include a legacy network adapter in the template. To add a legacy network adapter, at the top, in the **New** bar, click **Network Adapter**, and then, in the drop-down box, click **Legacy network adapter**. If you do not include a legacy network adapter when you use the .vmdk format, when you deploy the virtual machine, the virtual machine might not be able to start in a domain, although it can start in a workgroup.
- On the **Configure Operating System** page, configure the guest operating system settings. If you have an existing guest operating system profile that you want to use, in the **Guest OS profile** list, click the guest operating system profile that you want to use. After you configure the guest operating system settings, click **Next**.

8. On the **Select Destination** page, specify how to deploy the virtual machine:
   - Select **Deploy the virtual machine to a private cloud** to place the virtual machine in an existing private cloud. Then follow the instructions in Deploying the virtual machine in a private cloud.
   - Select **Place the virtual machine on a host** to place the virtual machine on an existing virtual machine host. Then follow the instructions in Deploying the virtual machine on a host.
   - Select **Store the virtual machine in the library** to store the virtual machine. Then follow the instructions in Storing the virtual machine in the library.

Deploying the virtual machine in a private cloud

1. On the **Select Cloud** page, select the private cloud on which you want to place the virtual machine. If you are connected as an administrator, you can select the host on which the virtual machine should be deployed in the private cloud. The cloud suggestions are based on a 0-5 star rating. For more information, see Understanding Virtual Machine Placement and Ratings in VMM. Verify the settings and modify them if required:
   - **Expected utilization**—For a virtual machine that is created from a blank hard disk, the expected utilization is based on standard defaults. For a virtual machine that is created from an existing virtual machine, the default settings are based on past performance of the existing virtual machine. VMM updates host suggestions and ratings in response to modifications that are made to the expected virtual machine utilization.
   - **Make this VM highly available**—With this option selected, only hosts that are located in a cluster are available for selection.

- **Details**—Indicates the status of the host, the operating system, and the type and status of virtualization software.
- **Rating Explanation**—Provides an explanation if a host received a zero rating.
- **SAN Explanation** or **Deployment and Transfer Explanation**—Lists any factors that make a storage area network (SAN) transfer unavailable. VMM does not recognize a virtual machine that is stored on a SAN as available for deployment using SAN transfer if the virtual machine was stored directly in the VMM library when it was created, or was added to the library during a library refresh. To avoid this issue, deploy the virtual machine to a host by using a LAN transfer, and then store the virtual machine in the same VMM library, library share, and logical unit number (LUN).

  In addition, in System Center 2012 R2 Virtual Machine Manager, the **Deployment and Transfer Explanation** tab provides an explanation if fast file copy cannot be used. Fast file copy is a new feature in System Center 2012 R2 Virtual Machine Manager that is based on the Windows Offloaded Data Transfers (ODX) feature that is introduced in Windows Server 2012 R2. For information about ODX, see Windows Offloaded Data Transfers Overview.

2. On the **Configure Settings** page, confirm or change the computer name, and then click **Next**.
3. On the **Add Properties** page, configure the action to take when the host starts or stops. If you are a VMM administrator, to prevent the virtual machine from being migrated by Performance and Resource Optimization (PRO) or dynamic optimization, select the **Exclude virtual machine from optimization actions** check box. Then click **Next**.
4. On the **Summary** page, confirm the settings, and then click **Create**.

   To confirm that the virtual machine was created, in the **VMs and Services** workspace, in the **VMs and Services** pane, expand **Clouds**, and then click the private cloud where you deployed the virtual machine. On the **Home** tab, in the **Show** group, click **VMs**. The virtual machine appears in the **VMs** pane.

Deploying the virtual machine on a host

Use the following procedure to deploy the virtual machine on a host.

1. On the **Select Host** page, view the ratings, click the host on which you want to deploy the virtual machine, and then click **Next**. The host suggestions are based on a 0-5 star rating. For more information, see Understanding Virtual Machine Placement and Ratings in VMM. Note the following settings:
   a. **Expected utilization**—For a virtual machine that is created from a blank hard disk, the expected utilization is based on standard defaults. For a virtual machine that is created from an existing virtual machine, the default settings are based on past performance of the existing virtual machine. VMM updates the host suggestions and ratings in response to modifications that are made to the expected virtual machine utilization.
   b. **Make this VM highly available**—With this option selected, only hosts that are located in a cluster are available for selection.

c. **Details**—Indicates the status of the host, the operating system, and the type and status of virtualization software.

d. **Rating Explanation**—Provides an explanation if a host received a zero rating.

e. **SAN Explanation** or **Deployment and Transfer Explanation**—Lists any factors that make a SAN transfer unavailable. VMM does not recognize a virtual machine that is stored on a SAN as available for deployment using SAN transfer if the virtual machine was stored directly in the VMM library when it was created, or if it was added to the VMM library during a library refresh. To avoid this issue, deploy the virtual machine to a host by using a LAN transfer, and then store the virtual machine in the same VMM library, library share, and logical unit number (LUN).

   In addition, in System Center 2012 R2 Virtual Machine Manager, the **Deployment and Transfer Explanation** tab provides an explanation if fast file copy could not be used. Fast file copy is a new feature in System Center 2012 R2 Virtual Machine Manager that is based on the Windows Offloaded Data Transfers (ODX) feature that is introduced in Windows Server 2012 R2. For information about ODX, see Windows Offloaded Data Transfers Overview.

2. On the **Configure Settings** page, review the settings for the virtual machine:

   a. In **Locations**, either accept the default virtual machine path on the host for storing the virtual machine files, or click **Browse** to browse to a different location. Optionally, select the **Add this path to the list of default virtual machine paths on the host** check box.

   b. In **Operating System Settings**, click **Identity Information**. You can either accept or change the computer name.

   c. In **Networking**, you can click a network adapter to view the configured network settings.

   d. In **Machine Resources**, click **Virtual Hard Disk**, then review or modify the settings.

      In VMM in System Center 2012 R2, under **Method to deploy the virtual hard disk to the host**, the option to **Use differencing disk optimizations** has been added.

      Click **Next**.

   Tip
   To prevent placement from choosing a different value for these settings, click the pin icon next to the setting. Note that self-service users do not see this option.

3. On the **Add Properties** page, configure the action to take when the host starts or stops. To prevent the virtual machine from being migrated by Performance and Resource Optimization (PRO) or dynamic optimization, select the **Exclude virtual machine from optimization actions** check box. When you have finished this step, click **Next**.

4. On the **Summary** page, confirm the settings, and then click **Create**.

Storing the virtual machine in the library

1. On the **Select Library Server** page, click the library server that you want to use, and then click **Next**.

2. On the **Select Path** page, specify the library share location to store the virtual machine. Click **Browse** to select a library share and optional folder location, click **OK**, and then click **Next**.

3. On the **Summary** page, confirm the settings, and then click **Create**.

   To confirm that the virtual machine was created, in the **Library** workspace, in the **Library** pane, expand **Library Servers**, expand the library server where you stored the virtual machine, and then click **Stored Virtual Machines and Services**. The stored virtual machine appears in the **Physical Library Objects** pane.

See Also

Configuring Virtual Machine Settings in VMM

How to Create a Virtual Machine Template

How to Deploy a Virtual Machine by Converting a Physical Computer (P2V)

In VMM in System Center 2012 and System Center 2012 Service Pack 1 (SP1) only, you can convert existing physical computers into virtual machines through a process known as physical-to-virtual (P2V) conversion. VMM simplifies P2V conversion by providing a task-based wizard to automate much of the conversion process.

Important
As of System Center 2012 R2, you can no longer perform P2V conversions in VMM. For information about how to use an earlier version of Virtual Machine Manager to mitigate this change, see the How to perform a P2V in a SCVMM 2012 R2 environment blog.

The following topics describe converting physical systems to virtual machines.

- P2V Prerequisites in VMM
- How to Convert Physical Computers to Virtual Machines by Using VMM

P2V Prerequisites in VMM

VMM requirement

Check the version of VMM that you have. You can perform P2V conversions with VMM in System Center 2012 and System Center 2012 Service Pack 1 (SP1).

Important
As of System Center 2012 R2, you can no longer perform P2V conversions in VMM. For information about how to use an earlier version of Virtual Machine Manager to mitigate this change, see the How to perform a P2V in a SCVMM 2012 R2 environment blog.

Requirements on the source machine

The physical computer to be converted must meet the following requirements:

- Must have at least 512 MB of RAM.
- Cannot have any volumes larger than 2040 GB.
- Must have an Advanced Configuration and Power Interface (ACPI) BIOS. Vista WinPE will not install on a non-ACPI BIOS.
- Must be accessible by VMM and by the virtual machine host.
- Cannot be in a perimeter network.

  Note

  A perimeter network, which is also known as a screened subnet, is a collection of devices and subnets that are placed between an intranet and the Internet to help protect the intranet from unauthorized Internet users. The source computer for a physical-to-virtual (P2V) conversion can be in any other network topology in which the VMM management server can connect to the source machine to temporarily install an agent and can make Windows Management Instrumentation (WMI) calls to the source computer.
- The source computer should not have encrypted volumes.

  Warning

  If the source computer has encrypted volumes, an offline P2V conversion may render the computer unbootable.

Supported operating systems

The following restrictions apply to P2V operating system support:

- VMM does not support P2V conversion for computers with Itanium architecture–based operating systems.
- VMM does not support P2V on source computers that are running Windows NT Server 4.0.
- VMM does not support converting a physical computer running Windows Server 2003 with Service Pack 1 (SP1) to a virtual machine that is managed by Hyper-V. Hyper-V does not support Integration Components on computers running Windows Server 2003 with SP1. As a result, there is no mouse control when you use Remote Desktop Protocol (RDP) to connect to the virtual machine. To avoid this issue, update the operating system to Windows Server 2003 with Service Pack 2 (SP2) before you convert the physical computer.

Note

Some products listed are no longer supported or are in Extended support. After extended support ends, integration services for these operating systems will not be updated and support will not be available for any issues arising from using these operating systems in virtual machines. For more information about the end of support, see the Microsoft Support Lifecycle Index.

The following table lists the supported operating systems for P2V conversion:

Operating System	Supported
Windows XP Professional with Service Pack 3 (SP3)	Yes in System Center 2012 – Virtual Machine Manager No in VMM in System Center 2012 SP1
Windows XP 64-Bit Edition SP3	Yes in System Center 2012 – Virtual Machine Manager No in VMM in System Center 2012 SP1
Windows Server 2003 Standard Edition (32-bit x86)	Yes (Requires SP2 or later.)
Windows Server 2003 Enterprise Edition (32-bit x86)	Yes (Requires SP2 or later.)
Windows Server 2003 Datacenter Edition (32-bit x86)	Yes (Requires SP2 or later.)
Windows Server 2003 x64 Standard Edition	Yes (Requires SP2 or later.)
Windows Server 2003 Enterprise x64 Edition	Yes (Requires SP2 or later.)
Windows Server 2003 Datacenter x64 Edition	Yes (Requires SP2 or later.)
Windows Server 2003 Web Edition	Yes
Windows Small Business Server 2003	Yes
Windows Vista with Service Pack 1 (SP1)	Yes
64-bit edition of Windows Vista with Service Pack 1 (SP1)	Yes
Windows Server 2008 Standard 32-Bit	Yes
Windows Server 2008 Enterprise 32-Bit	Yes
Windows Server 2008 Datacenter 32-Bit	Yes
64-bit edition of Windows Server 2008 Standard	Yes
64-bit edition of Windows Server 2008 Enterprise	Yes
64-bit edition of Windows Server 2008 Datacenter	Yes
Windows Web Server 2008	Yes

Operating System	Supported
Windows 7	Yes
64-bit edition of Windows 7	Yes
64-bit edition of Windows Server 2008 R2 Standard	Yes
64-bit edition of Windows Server 2008 R2 Enterprise	Yes
64-bit edition of Windows Server 2008 R2 Datacenter	Yes
Windows Web Server 2008 R2	Yes
64-bit edition of Windows 8	Yes
64-bit edition of Windows Server 2012 Standard	Yes
64-bit edition of Windows Server 2012 Enterprise	Yes
64-bit edition of Windows Server 2012 Datacenter	Yes
Windows Web Server 2012	Yes

Requirements for the destination virtual machine host

In VMM, a host is a physical computer on which you can deploy one or more virtual machines. To run P2V conversion, you need a host on which to place the image of the source computer.

Requirements for the host server include the following:

- The destination host during a P2V conversion must be running a supported operating system. For a list of supported operating systems, see the followings:
  - For System Center 2012 – Virtual Machine Manager or for System Center 2012 SP1: **System Requirements: Virtual Machine Hosts in System Center 2012 and in System Center 2012 SP1**.
  - For System Center 2012 R2 Virtual Machine Manager: **Preparing your environment for System Center 2012 R2 Virtual Machine Manager**.
- The destination host cannot be in a perimeter network.
- As in any virtual machine creation or migration, the destination host for a P2V conversion must have sufficient memory for the virtual machine in addition to memory that is reserved for the host operating system. By default, the amount of memory that is reserved for the host

operating system is 256 MB in System Center 2012 – Virtual Machine Manager. If the host does not have enough memory, you will receive a placement error in the Convert Physical Server (P2V) Wizard.

Online and offline conversions

VMM can do an *online conversion* or an *offline conversion*.

Note
With both online and offline P2V conversion, VMM temporarily installs an agent on the physical source computer to be converted.

The following table lists some of the differences between the online and offline P2V conversions.

Category	Online P2V Conversion	Offline P2V Conversion
Source computer availability	The source computer continues to perform normal operations during the conversion.	The source computer is taken offline during the conversion.
Process	VMM creates a copy of local NTFS volumes and data of VSS-aware applications. VMM leverages the Volume Shadow Copy Service (VSS) to ensure that data is backed up consistently while the server continues to service user requests. VMM uses this read-only snapshot to create a VHD.	The source computer restarts into the Windows Preinstallation Environment (Windows PE), and then VMM clones the volume to a VHD. Finally, VMM restarts the source computer into the original operating system.
Compatibility	Online P2V conversion is the default for the operating systems on most physical computers.	Offline P2V conversion is the only method to reliably migrate FAT volumes, and the recommended method for converting domain controllers.
Advantages	Source computer is available throughout the conversion.	Offline P2V conversion can be the most reliable way to ensure data consistency and is the only option in certain situations (see above).

See Also

How to Convert Physical Computers to Virtual Machines by Using VMM

How to Convert Physical Computers to Virtual Machines by Using VMM

Before you begin a physical-to-virtual (P2V) conversion in VMM, we recommend that you do the following:

- Check the version of VMM that you have. You can perform P2V conversions with VMM in System Center 2012 and System Center 2012 Service Pack 1 (SP1).

  Important
  As of System Center 2012 R2, you can no longer perform P2V conversions in VMM. For information about how to use an earlier version of Virtual Machine Manager to mitigate this change, see the How to perform a P2V in a SCVMM 2012 R2 environment blog.

- If you have not already reviewed the prerequisites for P2V, see P2V Prerequisites in VMM.
- Run the System Center Virtual Machine Manager Configuration Analyzer (VMMCA) on the VMM management server, the destination hosts, and the source computers.

  The VMMCA scans the hardware and software configurations of the computers that you specify, evaluates them against a set of predefined rules, and then provides you with error messages and warnings for any configurations that are not optimal for the VMM role or other VMM function that you have specified for the computer.
- To prevent disruptions to the conversion, configure the source computer to not go into standby power mode.
- To help minimize the time required, perform a disk defragmentation on the source computer. Also, ensure that you have a fast network connection between the source computer and the virtual machine host.
- Use dynamic virtual hard disks (VHDs) to conserve disk space on the destination host. For example, if you convert 5 GB of data on a 40 GB hard drive, VMM will create a dynamically expanding 40 GB VHD that occupies approximately 5 GB of disk space and can expand up to 40 GB. The actual size depends on fragmentation of the original volume plus some VHD format overhead.

  Note
  It is not possible to shrink the size of a disk.
- For an online P2V conversion, make sure that all critical applications that are running on the source computer have VSS-aware writers or that they are stopped.
- For an offline P2V, be prepared to supply NIC and mass storage drivers that are compatible with the source computer. Make sure the Driver Import folder (%SYSTEMDRIVE%\Program Files\Microsoft System Center 2012\Virtual Machine Manager\Driver Import) on the VMM

management server contains all necessary drivers to support the drives that are emulated by the target virtualization software. VMM will evaluate the source physical computer and compare it with the drivers that are included in Windows PE, and will provide instructions on adding drivers on the source computer.

To convert a physical system to a virtual machine

1. Open the **VMs and Services** workspace.
2. On the **Home** tab, in the **Create** group, click the **Create Virtual Machine** drop-down arrow, and then click **Convert Physical Machine**.

   The Convert Physical Server (P2V) Wizard opens.
3. On the **Select Source** page, do the following:
   - In the **Computer name or IP address** box, specify a physical computer to convert. You can identify the computer by name or by IPv4 or IPv6 address.
   - In the **Administrative account** section, enter credentials for an administrator to connect to the physical computer, and then click **Next**.
4. On the **Specify Virtual Machine Identity** page, enter a virtual machine name and optional description, and then click **Next**.
5. On the **System Information** page, click **Scan System** to gather information about the physical computer. VMM temporarily installs a VMM agent on the computer to gather system information.

   Warning

   Review the warning about encrypted volumes. We strongly recommend that you do not convert a source computer that has encrypted volumes.

   When the scan is complete, click **Next** to continue.
6. On the **Volume Configuration** page, do the following:
   a. If desired, clear the check box next to any additional volumes. By default, VMM creates a virtual hard disk for each volume. You cannot clear the check box next to the system or system reserve volume.
   b. Accept or modify the **VHD Size (MB)**, **VHD Type**, or **Channel** settings.
   c. Click the chevron icon next to **Conversion Options**.
   d. In the **Conversion Options** area, click **Online conversion** or **Offline conversion**.
   e. If desired, select the **Turn off source computer after conversion** check box.
   f. Click **Next** to continue.
7. If you selected offline conversion, on the **Offline Conversion Options** page, select whether to obtain an IP address automatically, or to use a specific IPv4 or IPv6 address.

   If you selected an IPv4 or IPv6 address, enter the relevant information and, if necessary, select the network adapter to bind the address to. Then, click **Next**.
8. For either offline or online conversion, do the following:
   a. On the **Virtual Machine Configuration** page, configure the number of virtual processors and the amount of memory for the new virtual machine, and then click

Next.

b. On the **Select Host** page, review the virtual machine host placement ratings, click the desired host, and then click **Next**.

c. On the **Select Path** page, specify a storage location on the host for the virtual machine files, and then click **Next**.

d. On the **Select Networks** page, configure which logical network, virtual network and VLAN (if applicable) to assign to each virtual network adapter, and then click **Next**.

e. On the **Add Properties** page, configure the action to take when the virtual machine host stops or starts, and then click **Next**.

f. On the **Conversion Information** page, verify that no issues are detected, and then click **Next**.

   If there are issues, click each issue to view the associated error and suggested resolution information. Resolve any issues before you continue.

g. On the **Summary** page, review the settings. If desired, select the **Start the virtual machine after deploying it** check box, and then click **Create** to continue with the conversion.

   Tip
   You can click **View Script** to create a PowerShell script.

See Also

P2V Prerequisites in VMM

How to Deploy a Virtual Machine by Converting a Virtual Machine (V2V)

Virtual Machine Manager (VMM) enables you to copy existing Citrix XenServer or VMware virtual machines to create Hyper-V virtual machines. This process is known as V2V. Note that V2V is a read-only operation that does not delete or affect the original source virtual machine. Use the following procedures for conversions:

- How to Convert Citrix XenServer Virtual Machines to Hyper-V
- How to Convert VMware Virtual Machines to Hyper-V
- Using OVF Packages to Create Virtual Machines in System Center Virtual Machine Manager 2012

How to Convert Citrix XenServer Virtual Machines to Hyper-V

In VMM in System Center 2012 and System Center 2012 Service Pack 1 (SP1) only, converting a Citrix XenServer virtual machine to a Hyper-V virtual machine is supported by using the physical-to-virtual machine (P2V) conversion process. You do not have to remove the Citrix Tools for Virtual Machines before you start the conversion. Realize that VMM only supports the conversion of virtual machines that are running supported Windows-based guest operating systems.

Important
As of System Center 2012 R2, you can no longer convert a XenServer virtual machine to a Hyper-V virtual machine or perform other P2V conversions in VMM. For information about how to use an earlier version of Virtual Machine Manager to mitigate this change, see the How to perform a P2V in a SCVMM 2012 R2 environment blog.

For more information about the P2V conversion process, see How to Deploy a Virtual Machine by Converting a Physical Computer (P2V).

See Also

Managing Citrix XenServer Overview

How to Convert VMware Virtual Machines to Hyper-V

You can use the following procedure to convert a VMware virtual machine to a Hyper-V virtual machine through the virtual-to-virtual (V2V) machine conversion process in System Center 2012 – Virtual Machine Manager (VMM). The source virtual machine can be stored in the VMM library or managed by a VMware ESX host.

Before you begin

Before you begin, there are several things you need to be aware of concerning V2V conversions:

- VMM does not support converting VMware Workstations.
- VMM does not support converting VMware virtual machines with virtual hard disks that are connected to an integrated drive electronics (IDE) bus.
- Online V2V conversions are not supported. This means VMware virtual machines must be offline (powered off).
- You must stop any anti-virus applications that are running.
- You must uninstall VMware Tools on the guest operating system of the virtual machine. For information about VMWare Tools, see Overview of VMware Tools.

VMM in System Center 2012 supports the V2V machine conversion of virtual machines that are running on the following versions of VMware ESX:

- ESX/ESXi 3.5 Update 5
- ESX/ESXi 4.0
- ESX/ESXi 4.1
- ESXi 5.1

VMM in System Center 2012 Service Pack 1 (SP1) and in System Center 2012 R2 supports the V2V machine conversion of virtual machines that are running on the following versions of VMware ESX:

- ESX/ESXi 4.1
- ESXi 5.1

You can perform V2V conversions using Microsoft Virtual Machine Converter (MVMC) or by using the Convert Virtual Machine Wizard in VMM. For more information about MVMC, see Microsoft Virtual Machine Converter. To download the MVMC tool, go to Microsoft Virtual Machine Converter Solution Acceleratorand follow the instructions. To use the Convert Virtual Machine Wizard, complete the following procedure.

For a list of common V2V conversion issues, error messages and resolutions, see Troubleshooting Virtual Machine Conversion Issues

To convert VMware virtual machines to Hyper-V using the Convert Virtual Machine Wizard

1. Open the **VMs and Services** workspace.
2. On the **Home** tab, in the **Create** group, click the **Create Virtual Machine** drop-down arrow, and then click **Convert Virtual Machine**.

   The Convert Virtual Machine Wizard opens.
3. On the **Select Source** page, next to the **Select the virtual machine that you would like to convert** box, click **Browse**.
4. In the **Select Virtual Machine Source** dialog box, click the VMware virtual machine that you want to convert, and then click **OK**.

   Tip

   Verify that the **Virtualization Platform** column indicates **VMware ESX Server**.
5. On the **Select Source** page, click **Next**.
6. On the **Specify Virtual Machine Identity** page, either keep or change the virtual machine name, enter an optional description, and then click **Next**.

   Note

   The virtual machine name identifies the virtual machine to VMM. The name does not have to match the computer name of the virtual machine. However, to avoid confusion, we recommend that you use the same name as the computer name.
7. On the **Virtual Machine Configuration** page, configure the number of processors and

assign the amount of memory in megabytes or gigabytes, and then click **Next**.

8. On the **Select Host** page, select a Hyper-V host for placement, and then click **Next**.
9. On the **Select Path** page, do the following, and then click **Next**:
   a. In the **Storage location** box, configure the storage location on the host for virtual machine files. By default, the default virtual machine paths on the target host are listed. To select a different location, click **Browse**, click a folder, and then click **OK**.

      Note
      As a best practice, do not specify a path that is on the same drive as the operating system files.

   b. To add the path to the list of storage locations on the virtual machine host, select the **Add this path to the list of default storage locations on the host** check box.
10. On the **Select Networks** page, select the logical network, the virtual network, and the virtual LAN (VLAN), if applicable, to use for the virtual machine, and then click **Next**.

    Note
    The list of available logical networks, virtual networks, and VLANs matches what is configured on the host physical network adapters.
11. On the **Add Properties** page, configure the settings that you want, and then click **Next**.
12. On the **Summary** page, review the settings. Optionally, select the **Start the virtual machine after deploying it** check box. To start the conversion process, click **Create**.

    The **Jobs** dialog box appears to indicate the job status. Verify that the job has a status of **Completed**, and then close the dialog box.
13. To verify that the virtual machine was converted, do the following:
    a. In the **VMs and Services** workspace, locate and then click the Hyper-V host which you selected during placement.
    b. On the **Home** tab, in the **Show** group, click **VMs**.
    c. In the **VMs** pane, verify that the virtual machine appears.

Using OVF Packages to Create Virtual Machines in System Center Virtual Machine Manager 2012

The Open Virtualization Format (OVF) is a packaging standard from Distributed Management Task Force, Inc., designed to facilitate portability and deployment of virtual appliances. In Virtual Machine Manager (VMM), you can use an OVF package to create a virtual machine. In System Center 2012 – Virtual Machine Manager (VMM), you can use the *OVF Import/Export* tool to perform these tasks. However, as of Virtual Machine Manager in System Center 2012 Service Pack 1 (SP1), the OVF tool is not supported.

When you work with OVF packages, the name of the virtual hard disk that is specified in the .ovf file must match the actual path and name of the virtual hard disk. If you convert a file from, for example, .vmdk to .vhd, or if you rename the virtual hard disk file, you must also edit the .ovf file to update the name.

Note the following:

- If you plan to convert a virtual hard disk from one format to another, such as from .vhd to .vmdk or from .vmdk to .vhd, we recommend that you use the fixed size disk format. A fixed size disk is also known as a "thick disk."
- The virtual hard disk name appears more than once in the .ovf file. Ensure that you update all instances of the name.
- The current version of the OVF tool supports a single virtual machine. The import and export of VMM service templates containing more than one virtual machine or with deployment customizations are not currently supported.

Creating Virtual Machines from OVF Packages

As of Virtual Machine Manager in System Center 2012 Service Pack 1 (SP1), the OVF tool is not supported. Instead, to import an OVF package to a Hyper-V host, you can use the Microsoft Virtual Machine Converter (MVMC), which converts the .vmdk file to a .vhd file. By using MVMC, the metadata in the OVF package is lost, so you must capture information, such as the virtual machine hardware configuration, before you create a new virtual machine from the converted virtual hard disk. For more information about MVMC, see Microsoft Virtual Machine Converter on TechNet.

To convert an OVF package into a virtual machine

1. Open the descriptor in the OVF package and note the virtual machine metadata, such as the virtual machine hardware configuration.
2. Use Microsoft Virtual Machine Converter (MVMC) to convert the .vmdk file to a .vhd file.
3. Use VMM to create a virtual machine from the virtual hard disk; use the original metadata that you noted from the OVF package, as applicable. For more information, see How to Create and Deploy a Virtual Machine from an Existing Virtual Hard Disk.

Using the OVF Tool to Import and Export Virtual Machines

The OVF Import/Export tool consists of Windows PowerShell cmdlets that enable users of System Center 2012 – Virtual Machine Manager (VMM) to import and export virtual machines that are packaged in the OVF format. You can use the OVF tool to import a virtual machine from other virtualization platforms (currently, these are VMware vCenter and Citrix XenServer) or to export a virtual machine for use on another platform.

The OVF format uses an XML file with the extension .ovf together with one or more virtual disks. The OVF Import/Export tool does not convert virtual hard disk file formats. You might require third-party tools to convert a virtual hard disk format.

Installing the OVF Import/Export tool

You can download the OVF Import/Export tool from the Microsoft Download Center. The OVF Import/Export tool is distributed as a Windows Installer package. You must install the tool on an existing VMM management server that has the VMM console installed. The package installs a Windows PowerShell snap-in that contains the following cmdlets:

- **Export-SCVirtualMachine**
- **Import-SCVirtualMachine**

To install the OVF Import/Export tool, double-click the Windows Installer package **SC2012_VMM_OVFImport-Export.msi**. You must accept the license terms and select an installation folder. Complete the installation.

Before you use the cmdlets in the VMM command shell, you must add the Windows PowerShell snap-in to your current Windows PowerShell session. To add the snap-in, run the cmdlet **Add-PSSnapin OVFToolSnapIn**.

If you start a new Windows PowerShell session by opening a new instance of the VMM command shell, you must run the Windows PowerShell cmdlet in that session before you can use the OVF Import/Export cmdlets.

Note
If you use a profile, add the cmdlet **Add-PSSnapin OVFToolSnapIn** to your profile to load the Windows PowerShell snap-in automatically. For more information, type **get-help about_profiles**.

Importing a virtual machine

Use the **Import-SCVirtualMachine** cmdlet to create a new virtual machine for VMM by using the .ovf file and virtual hard disks in a specified location. The cmdlet creates a new virtual machine with the referenced virtual hard disk and stores it in a VMM library share. Self-service users must specify a writable share for the virtual machine. Note the following:

- Before you import an OVF package to VMM with the OVF Import/Export tool, verify that the virtual hard disk format is .vhd or .vhdx, or convert it to be .vhd or .vhdx. Ensure that you use the fixed size disk format.
- If the original virtual machine is joined to a logical network, the import process tries to join the imported virtual machine to a logical network with the same name, if such a network exists. Otherwise, the virtual machine is not joined to a network.

The **Import-SCVirtualMachine** cmdlet has several key parameters.

Import parameter	Required?	Description
ImportVMPath	Yes	Specifies the path of the OVF descriptor file to be imported.
LibraryServerObject	Yes	Specifies the library server object that is associated with the library share.
VMMServerObject	Yes	Specifies the VMM management server.
LibrarySharePath	Yes	Specifies the library share.
VHDSourcePath	Yes	Specifies a local path for the virtual hard disk. Specify multiple instances for virtual machines with more than one virtual hard disk.
VMName	Yes	Specifies a name for the new virtual machine.
AllowUnencryptedTransfer	Switch	Specifies whether Unencrypted Bits transfer is allowed.
Overwrite	Switch	Specifies whether export files overwrite existing files.

The following example commands create and store a virtual machine that is named **MyVirtualMachine**.

```
$vmm = get-scvmmserver -ComputerName "MyVMM"

$ls = Get-SCLibraryServer -ComputerName "MyLibraryServer"

Import-SCVirtualMachine -ImportVMPath "C:\Test\MyVirtualMachineOVF.ovf" -
LibraryServerObject $ls -VMMServerObject $vmm -LibrarySharePath
"\\MyLibraryServerFQDN\MSSCVMMLibrary\Import\" -VHDSourcePath
"C:\ImportInVMM\MyVirtualMachineVHD.vhd" -VMName "MyVirtualMachine"
```

The first command gets the VMM management server. The second command gets the library server. The third command creates a virtual machine with the specified name by using the specified .ovf file and disk, and then stores it in the specified library share.

Exporting a virtual machine

Use the **Export-SCVirtualMachine** cmdlet to create an OVF package together with the virtual hard disk for a virtual machine. The virtual machine that you want to export must be stored in the library. The cmdlet saves the exported files in a specified local directory.

The **Export-SCVirtualMachine** cmdlet has several key parameters.

Export parameter	Required	Description
ExportPath	Yes	Specifies a local path for exporting the OVF files.
StoredVMObject	Yes	Specifies the stored virtual machine object to be exported.
TargetVirtualizationPlatform	Yes	Specifies the platform for export: vmm, vcenter, or xen.
VMMServerObject	Yes	Specifies the VMM management server.
AllowUnencryptedTransfer	Switch	Specifies whether Unencrypted Bits transfer is allowed.
Overwrite	Switch	Specifies whether export files overwrite existing files.
ExportOnlyOVF	Switch	Specifies whether to export only the .ovf file without a virtual hard disk file.

The following example commands export a virtual machine that is named **MyVirtualMachine**.

```
$vmm = get-scvmmserver -ComputerName "MyVMM"

$vm = get-scvirtualmachine -name "MyVirtualMachine"

Export-SCVirtualMachine -ExportPath "C:\ExportDir" -StoredVMObject $vm -
TargetVirtualizationPlatform ”<supportedPlatform>”  -VMMServerObject $vmm
```

The first command gets the VMM management server. The second command gets the virtual machine object. The third command exports the virtual machine in the form of an OVF package to the local export path.

How to Deploy a Virtual Machine Stored in the VMM Library

Use the following procedure to deploy a virtual machine that is stored in the Virtual Machine Manager (VMM) library. For information about creating a virtual machine and storing it in the library, see Creating and Deploying Virtual Machines in VMM.

To deploy a virtual machine stored in the VMM library

1. In the VMM console, in the **Library** workspace, in the navigation pane, navigate to the library server on which the virtual machine is stored, and then click **Stored Virtual Machines and Services**.
2. In the results pane, select the virtual machine.
3. On the **Virtual Machine** tab, in the **Actions** group, click **Deploy**.

   The Deploy Virtual Machine Wizard opens.
4. On the **Select Host** page, select a host on which to deploy the virtual machine. In the list of hosts, all available hosts are given a rating of 0–5 stars, based on their suitability to host the virtual machine. The host rating levels are recommendations. You can select any host that has the required disk space, even if the host has a zero host rating. For more information, see Understanding Virtual Machine Placement and Ratings in VMM.

   Network optimization If a host has network optimization enabled, a green check mark appears in the **Network Optimization** column. Network optimization capabilities apply to Hyper-V hosts running Windows Server 2008 R2. For information about network optimization and the hardware that supports it, see the Windows Server 2008 R2 topics, Using Virtual Machine Chimney and Using Virtual Machine Queue.

   Highly available virtual machines To make a virtual machine a highly available virtual machine (HAVM), you can migrate the virtual machine to a host that is in a host cluster, even if the virtual machine has not been configured as highly available. The wizard also enables you to migrate a highly available virtual machine to a stand-alone host. Because of the resulting change to the virtual machine's highly available setting, either of these actions requires confirmation.

   Note
   For more information about environmental factors and settings that affect virtual machine placement in VMM, see Understanding Virtual Machine Placement and Ratings in VMM.

   - To get additional information about the host, select the host, and view the tabs in the **Details** area.

     Details—Indicates the status of the host, the operating system, and the type and status of virtualization software. Lists the virtual machines on the host.

     Rating Explanation—Lists the factors that resulted in a rating, if the host received a zero rating.

SAN Explanation or **Deployment and Transfer Explanation**— Lists factors that make a SAN transfer unavailable.

In addition, in System Center 2012 R2 Virtual Machine Manager, the **Deployment and Transfer Explanation** tab provides an explanation if fast file copy cannot be used. Fast file copy is a new feature in System Center 2012 R2 Virtual Machine Manager that is based on the Windows Offloaded Data Transfers (ODX) feature that is introduced in Windows Server 2012 R2. For information about ODX, see Windows Offloaded Data Transfers Overview.

- To change the host rating criteria for the current virtual machine, click **Customize Ratings**. You can change the placement goal and the relative importance that is placed on the availability of CPU, memory, disk I/O capacity, and network capacity for the current virtual machine. For more information, see Understanding Virtual Machine Placement and Ratings in VMM.

5. On the **Select Path** page, do the following:
   a. In **Save Path**, click **Browse**, navigate to the folder in which you want to store the configuration files for the virtual machine, and then click **OK**.
   b. If you selected a path other than a default virtual machine path, and you want to store other virtual machines on that path, select the **Add this path to the list of host default paths** check box to add the path to the default paths on the host.
   c. If SAN transfers are enabled for this deployment, by default, the virtual machine is transferred to the host over the storage area network (SAN). If you do not want to perform a SAN transfer, select the **Transfer over the network even if a SAN transfer is available** check box. If SAN transfers are not available for this deployment, this option is not available.
6. On the **Select Networks** page, select the network settings for the virtual machine to use.
7. On the **Summary** page, review your settings. To change settings, click **Previous**.

   To start the virtual machine after it is deployed, select the **Start the virtual machine immediately after deploying it to the host** check box.
8. To begin deploying the virtual machine, click **Deploy**.

   To review the progress and results of the operation, open the **Jobs** workspace. By default, the workspace opens when the wizard closes. To view this workspace at any time, click **Jobs** on the taskbar in the results pane of the VMM console.

See Also

Creating and Deploying Virtual Machines in VMM

How to View and Modify Properties of a Deployed Virtual Machine in VMM

After a virtual machine has been deployed in VMM, you can view the properties of the virtual machine. You can modify some of the properties that you view in the properties dialog box. However, for some properties, the state of the virtual machine must be off to allow modifications.

As of System Center 2012 R2, the properties of IP addresses have been enhanced to include all addresses on a vNIC, not just the addresses that are in an IP pool.

To view and to modify properties of a deployed virtual machine in VMM

1. Open the **VMs and Services** workspace.
2. Expand **All Hosts**, expand the host group that the virtual machine is deployed on, and then select the host that the virtual machine is deployed on.
3. Under **VMs**, right-click the name of the virtual machine, and then click **Properties**.
4. In the virtual machine's properties dialog box, click on the various tabs to view the properties of the virtual machine.

   For example:

   - To view IP addresses: Click the **Hardware Configuration** tab, click the network adapter, and in the results pane, click the **Connection details** button.
   - To view processor and memory: Click the **Hardware Configuration** tab, and in the results pane, under **General**, click **Processor** or **Memory** respectively. If you need to, you can modify the number of processors and the amount of memory that is allocated.

See Also

Creating and Deploying Virtual Machines in VMM

How to Create IP Address Pools for VM Networks in VMM

Creating Profiles and Templates in VMM

Virtual Machine Manager (VMM) profiles contain configuration settings that you can apply to a new virtual machine template or virtual machine. You can create, view, and modify profiles in the **Library** workspace. The following topics provide information about how to create profiles and virtual machine templates:

- Creating Profiles and Templates in VMM Overview
- How to Create a Hardware Profile
- How to Create a Guest Operating System Profile
- How to Create an Application Profile in a Service Deployment

- How to Create a SQL Server Profile in a Service Deployment
- How to Create a Virtual Machine Template

Note
VMM also includes host profiles, and as of System Center 2012 R2 Virtual Machine Manager, physical computer profiles. These profiles are not used for virtual machine creation. They are used during the conversion of a bare-metal computer to a server that is running Hyper-V.

For more information about service deployments, see the following:

- Creating and Deploying Services Overview
- Creating Service Templates in VMM
- How to Configure the Properties of a Service Template
- How to Create a Guest Cluster by Using a Service Template in VMM

Creating Profiles and Templates in VMM Overview

In Virtual Machine Manager (VMM), a profile is a library resource that contains specifications that can be applied to a new virtual machine or a virtual machine template. Templates encapsulate a standard set of configuration settings that you can use to create a virtual machine. Templates help you to quickly create virtual machines with consistent hardware and operating system settings. Templates can also be used to restrict the virtual machine settings that are available to self-service users who create new virtual machines. You can use profiles to simplify the process of creating templates. A virtual machine template typically consists of a hardware profile, an operating system profile, and a virtual hard disk, which will be used by the virtual machine that is created from the template. The virtual hard disk might be stored in the VMM library, or it might be a disk from an existing virtual machine.

Profiles

VMM provides the following profiles for virtual machine templates:

- **Hardware profile**—A hardware profile defines hardware configuration settings, such as CPU, memory, network adapters, a video adapter, a DVD drive, and the priority that is given to the virtual machine when resources are allocated on a virtual machine host.
- **Guest operating system profile**—A guest operating system profile defines operating system configuration settings that will be applied to a virtual machine that is created from the template. It defines common operating system settings, such as the type of operating system, the computer name, administrator password, domain name, product key, time zone, answer file, and RunOnce file.

Virtual machine templates

Templates are database objects that are stored in the library catalog of the VMM database. Templates are not represented by physical configuration files. Virtual machine templates can be created as follows:

- From an existing virtual hard disk or virtual machine template that is stored in the library
- From an existing virtual machine that is deployed on a host

Note that creating a virtual machine template can destroy the virtual machine that is used as the template's source because Sysprep strips the virtual machine of its computer identity. If you want to continue to use the source virtual machine, clone it before you create the template.

Services Profiles and Templates

System Center 2012 – Virtual Machine Manager (VMM) introduced the concept of services, which includes a new template type—a service template—and a number of new profiles. Service templates include capabilities not available in virtual machine templates. The following list describes these capabilities:

- Service templates can be used to deploy multiple virtual machines. Virtual machine templates can be used to deploy a single virtual machine only.
- Service templates can include settings for installing Windows Server roles and features on virtual machines. If a virtual machine template includes settings for installing roles and features, these settings are only used when the virtual machine is deployed as part of a service.
- In addition to the standard building blocks of virtual hard disks, hardware profiles, and operating system profiles, service templates can leverage additional profiles that include:
    - **Application profile**—Application profiles provide instructions that are necessary for installing an application. VMM supports multiple mechanisms for application deployment. Three of these mechanisms are for specific application packaging technologies: Microsoft Server Application Virtualization (Server App-V), data-tier applications (DAC), and WebDeploy, also known as MSDeploy. As of System Center 2012 R2 Virtual Machine Manager, a fourth mechanism enables you to install any application by running a script. You can use scripts that are created for Windows Installer (MSI), Setup.exe installation programs, Windows PowerShell Desired State Configuration (DSC), Puppet software, and Chef software.
    - **SQL Server profile**—SQL Server profiles provide instructions for customizing an instance of Microsoft SQL Server for a SQL Server DAC when a virtual machine is deployed as part of a service.

For more information about service profiles and templates, see Creating and Deploying Services Overview.

See Also

Creating Profiles and Templates in VMM

How to Create a Hardware Profile

You can use the following procedure to create a hardware profile in Virtual Machine Manager (VMM). A hardware profile specifies the hardware settings that you want the virtual machine to use when the virtual machine is created and deployed.

To create a hardware profile

1. Open the **Library** workspace.
2. On the **Home** tab, in the **Create** group, click **Create**, and then click **Hardware Profile**.

   The New Hardware Profile dialog box opens.
3. On the **General** tab, in the **Name** box, enter a name for the hardware profile. For example, enter **8 GB 2 processor server**.

   If you are running VMM in System Center 2012 R2, in the **Generation** box, select **Generation 1** or **Generation 2**. (For more information, see Understanding Generation 1 and Generation 2 Virtual Machines in VMM.)
4. Click the **Hardware Profile** tab, and then configure the desired settings. For example, you can configure the following settings:
   - The number of processors
   - The amount of static or Dynamic memory
   - The logical network
   - Whether to make the virtual machine highly available
   - Which capability profiles to use

   Note
   - If you want to deploy the virtual machine to a private cloud, you must select a capability profile that is supported by the private cloud. For more information about capability profiles, see How to Create a Private Cloud from Host Groups.
   - With VMM in System Center 2012 R2, the hardware options that are available are those of the generation that you selected in the previous step.

   After you have made your selections, click **OK**.
5. To verify that the profile was created, in the **Library** pane, expand **Profiles**, and then click **Hardware Profiles**.

   The hardware profile appears in the **Profiles** pane.

See Also

Creating Profiles and Templates in VMM

How to Create a Guest Operating System Profile

You can use the following procedure to create a guest operating system profile in Virtual Machine Manager (VMM). A guest operating system profile specifies the operating system settings that you want the virtual machine to use when the virtual machine is created and deployed.

To create a guest operating system profile

1. Open the **Library** workspace.
2. On the **Home** tab, in the **Create** group, click **Create**, and then click **Guest OS Profile**.

   The **New Guest OS Profile** dialog box opens.
3. On the **General** tab, in the **Name** box, enter a name for the guest operating system profile. For example, enter **Domain-joined Windows Server 2008 R2 Enterprise**.
4. Click the **Guest OS Profile** tab, and then configure the desired settings. For example, you can configure the following settings:
   - **Computer name**

     For the computer name, you can provide a pattern to generate computer names. For example, if you type **server####**, the computer names that are created are server0001, server0002, and so on. Using a pattern ensures that when you add additional virtual machines to a service, unique computer names are created, and these computer names are related and identifiable. If you use this method to specify the computer name, you cannot use it in combination with a name prompt parameter (@<name>@). You can use one method or the other, but not both.
   - Local administrator account password

     Note
     If you want to use the guest operating system profile in a virtual machine template that is used in a service template, under **Admin Password**, do not select the **No local administrator credential required** option. You can either specify the password of the local administrator account, or select a Run As account. This setting does not apply to Linux-based profiles.
   - **Product key**

     If applicable, enter the product key to use for the virtual machine.
   - Operating system to install

     Note
     This setting lets you choose a Windows-based or a Linux-based operating system. If you choose an edition of the Windows Server 2003 operating system, you must ensure that the .NET Framework 2.0 or later is installed on the virtual hard disk before you attempt to deploy the virtual machine as part of a service. The agent that VMM uses requires the .NET Framework.

- Domain to join

  For System Center 2012, if you want to use the guest operating system profile in a virtual machine template to be used in a service template, under **Networking**, you must configure Active Directory domain settings. Use the fully qualified domain name (FQDN). For example, enter *contoso.com* as the domain name. The domain must have a two-way trust relationship with the domain of the VMM management server. This setting does not apply to Linux-based profiles.

  Note

  As of System Center 2012 SP1, this setting does not apply. You do not need to have the virtual machine join a domain, nor do you need to have a two-way trust relationship with the VMM management server.

- Windows Server roles or features to install

  The settings for roles or features apply only if you deploy the virtual machine as part of a service and only for Windows-based profiles. Also, the virtual machine must use a guest operating system that supports these settings, as listed in the following table:

Product version of VMM	Guest operating systems that support settings for roles or features
System Center 2012	Windows Server 2008 R2
System Center 2012 Service Pack 1 (SP1)	Windows Server 2008 R2 or Windows Server 2012
System Center 2012 R2	Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2

- RunOnce commands

  This setting applies only to Linux-based profiles. These commands run in the specified order during deployment after the operating system has been configured. If shell conventions such as pipes are used, we recommend wrapping each command with an explicit invocation of the shell, for example, `/bin/sh –c "<your command>"`. In this example, double quotes in the command must be escaped.

- Public SSH key

  Under **Root Credentials**, **Public SSH key** is a Linux-specific option. This option sets the content of a specified public Secure Shell (SSH) key as an authorized key for authentication of the root user. Enter the name of a public key file that is stored in the VMM library, and that has the extension .sshkey.

After you have made your selections, click **OK**.

5. To verify that the profile was created, in the **Library** pane, expand **Profiles**, and then click **Guest OS Profiles**.

The guest operating system profile appears in the **Profiles** pane.

See Also

Creating Profiles and Templates in VMM

How to Create an Application Profile in a Service Deployment

You can use the following procedure to create an application profile in Virtual Machine Manager (VMM). An application profile provides instructions for installing Microsoft Server Application Virtualization (Server App-V) applications, Microsoft Web Deploy applications, and Microsoft SQL Server data-tier applications (DACs), and instructions for running scripts when a virtual machine is deployed as part of a service. Application profiles are not supported for Linux operating systems because application profiles are designed for technologies that are specific to Windows operating systems.

Important
You can only use an application profile when you deploy a virtual machine as part of a service.

To create an application profile

1. Confirm that your application components, such as packages, scripts, and so on, have been copied to the VMM library share. For example, if you plan to create a profile for a SQL Server application host, confirm that your SQL Server DAC packages and SQL Server scripts have been copied to the VMM library share.
2. Open the **Library** workspace.
3. On the **Home** tab, in the **Create** group, click **Create**, and then click **Application Profile**.

   The **New Application Profile** dialog box opens.
4. On the **General** tab, in the **Name** box, enter a name for the application profile. For example, enter **Corporate Finance Application**.
5. On the **General** tab, in the **Compatibility** list, choose an appropriate option:
   - For deployment of any application type or combination of application types that are listed at the beginning of this topic, keep the default selection, **General**.
   - For deployment of SQL Server DAC packages or SQL Server scripts to an existing instance of SQL Server in your environment, click **SQL Server Application Host**. If you click **SQL Server Application Host**, you can add only SQL Server DAC packages and SQL Server scripts to the application profile.
   - As of System Center 2012 Service Pack 1 (SP1), for deployment of web applications to a server that is runs Internet Information Services (IIS), click **Web Application Host**. If you click **Web Application Host**, you can add only Web Deploy packages

and associated scripts to the application profile.

6. Click the **Application Configuration** tab, and then do the following:
   a. Click **OS Compatibility**, and then select the guest operating systems on which the application is supported.
   b. Click **Add**, and then click the type of application or script that you want to add to the application profile.
      - You can add more than one of each type of application. For example, you can add three virtual applications.
      - If you kept the **Compatibility** option (described in the previous step) set to the default option, **General**, you can add more than one type of application or script to the application profile. For example, you can add a virtual application and a web application.
      - In VMM in System Center 2012 R2, if you kept the **Compatibility** option (described in the previous step) set to the default option, **General**, you can add an application that will be deployed by running a script, such as a script based on a Setup.exe installation program. To add such an application, select **Script Application**.
      - After you add an application, you can select **Application script** to add application scripts. You can add one application script that will run before the application is installed or uninstalled, and one application script that will run after the application is installed or uninstalled.
      - Regardless of whether you add an application, if you kept the **Compatibility** option set to **General**, you can select **Scripts** to add a script.

      In VMM in System Center 2012, for this option, you can specify one script that will run before the process of installing or uninstalling an application begins, and one script that will run after that process is completed.

      As of VMM in System Center 2012 SP1, the number of scripts is not limited, and you can specify the order in which the scripts will run.

      In VMM in System Center 2012 R2, you can specify scripts that create a guest cluster out of multiple virtual machines that are all deployed as part of a VMM service. For example, you can specify that one script will run at **Creation: First VM** (to form the cluster on the first virtual machine) and a different script will run at **Creation: VMs After First** (to add additional virtual machines to the cluster). For more information, see How to Create a Guest Cluster by Using a Service Template in VMM.

   c. For each application or script that you add, configure the appropriate settings. Some of the settings that you can configure are as follows:
      - For application packages, you can specify settings such as certificate, port, or folder settings for the application. To specify a setting, under **Applications**, select the application, select the setting, and then click **Properties**. Type the value, and then click **OK**.

Note
An application package can contain settings to be entered when you configure the service for deployment. To format this type of setting, enter the parameter in the **Value** field, in this format: @<SettingLabel>@. For example, you might prompt for the instance name of a SQL Server for a SQL Server database tier application by using the parameter @SQLServerInstanceName@.

- For scripts, as of System Center 2012 SP1, you can configure a variety of settings, such as parameters, the security account under which the script should run, time-out, failure, and restart policies that specify what to do if there is an error, and other settings. To configure these settings, under **Scripts**, select the script and review or change the parameters, deployment order, time-out, or other settings. As needed, click **Advanced** and view or configure advanced settings such as failure and restart policies.

After you have made your selections, click **OK**.

7. To verify that the profile was created, in the **Library** pane, expand **Profiles**, and then click **Application Profiles**.

   The application profile appears in the **Profiles** pane.

See Also

Creating Profiles and Templates in VMM

Preparing to Create Services in VMM

Creating Service Templates in VMM

How to Create a Guest Cluster by Using a Service Template in VMM

How to Create a SQL Server Profile in a Service Deployment

You can use the following procedure to create a SQL Server profile in Virtual Machine Manager (VMM). The SQL Server profile provides instructions for installing an instance of Microsoft SQL Server on a virtual machine.

Important
You can only use a SQL Server profile when you want to deploy a virtual machine as part of a service. In addition, you must use a virtual hard disk that contains a prepared instance of SQL Server (generalized by using the Sysprep tool), as described in the following list:

- **For VMM in System Center 2012**: SQL Server 2008 R2.

- **For VMM in System Center 2012 Service Pack 1 (SP1)**: SQL Server 2008 R2 or SQL Server 2012.
- **For VMM in System Center 2012 R2**: SQL Server 2008 R2 or SQL Server 2012.

To create a SQL Server profile

1. Open the **Library** workspace.
2. On the **Home** tab, in the **Create** group, click **Create**, and then click **SQL Server Profile**.

   The **New SQL Server Profile** dialog box opens.
3. On the **General** tab, in the **Name** box, enter a name for the SQL Server profile. For example, enter **Corporate Finance SQL Server**.
4. Click the **SQL Server Configuration** tab, and then, next to **Add**, click **SQL Server Deployment**.

   Note

   A SQL Server deployment corresponds to the configuration of one instance of SQL Server. If you want to configure multiple instances of SQL Server on the same virtual machine, you must add and configure a SQL Server deployment for each instance.
5. Under **SQL Server Deployment**, do the following:
   a. Click **SQL Server Deployment, Deployment 1**. In the results pane, enter the required configuration information.

      Required information includes the name of this SQL Server deployment (for which you can choose to enter a more meaningful name than "Deployment 1"), the SQL Server instance name, and the SQL Server instance ID (the instance ID specified during installation of SQL Server). The installation Run As account is optional and uses the VMM Service account unless you specify otherwise. For more information about Run As accounts, see Configuring Run As Accounts in VMM.
   b. Click **Configuration**. In the results pane, enter the required configuration information.

      Required information includes the media source (the path to the SQL Server installation media folder where Setup.exe is located) and the SQL Server administrators.
   c. Click **Service Accounts**. In the results pane, enter the Run As accounts to use.

   After you have made your selections, click **OK**.
6. To verify that the profile was created, in the **Library** pane, expand **Profiles**, and then click **SQL Server Profiles**.

   The SQL Server profile appears in the **Profiles** pane.

See Also

Creating Profiles and Templates in VMM

How to Create a Virtual Machine Template

You can use the following procedure to create a virtual machine template in Virtual Machine Manager (VMM). Virtual machine templates help you create new virtual machines and configure tiers in a service template. For more information about service templates, see Creating Service Templates in VMM.

You can create a virtual machine template based on an existing virtual machine template or based on an existing virtual hard disk that is stored in a library. Alternatively, you can create a virtual machine template based on an existing virtual machine that is deployed on a host. This option requires that the existing machine has been stopped.

If you base your new virtual machine template on an existing virtual machine template or on a virtual hard disk that is stored in the library, you can configure hardware settings, guest operating system settings, application installations, and the installation of instances of Microsoft SQL Server. You can configure each of these settings manually, or you can import the settings from an existing profile. For more information about creating profiles, see Creating Profiles and Templates in VMM.

If you create a virtual machine template that is based on the Linux operating system, some of the Linux-specific settings, such as operating system specialization, work only if you deploy the Linux-based virtual machine on a Hyper-V host. Also, the option to create a virtual machine template that is based on an existing virtual machine that is deployed on a host is not applicable for Linux-based virtual machine templates. For more information about creating Linux-based virtual machines, see Requirements for Linux-Based Virtual Machines.

Before you create a virtual machine template, note the following:

- When you create a virtual machine template, you can customize IP address settings. Static IP address settings are available only when you deploy a virtual machine from a virtual machine template.
- Application deployment, SQL Server deployment, and configurable service settings apply only when you deploy the virtual machine as part of a service.
- If you grant rights for a particular template to a user that does not have rights to the Run As account that is specified in the template, then the user can potentially extract the credentials for the Run As account from the template during deployment.
- Make sure the template has the correct operation system specified.
- You must create a new local administrator account on the virtual machine before creating a template. Using the default built-in administrator account will cause Sysprep to fail.
- Make sure the virtual machine is not joined to a domain before creating a template, otherwise Sysprep will fail. For more information, see SCVMM create virtual machine error 66.
- When creating a template for a Windows XP or Windows Server 2003 system, the Sysprep.exe and Setupcl.exe files must be copied to the appropriate directory under

`C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager\Sysprep` on the VMM server. For more information, see Creating a System Center 2012 Virtual Machine Manager template for a Windows XP or Windows Server 2003 system fails with error 678.

Note

For Sysprep best practices, see Sysprep, SkipRearm, and Image Build Best Practices.

To create a virtual machine template that is based on an existing virtual hard disk or virtual machine template

1. Open the **Library** workspace.
2. On the **Home** tab, in the **Create** group, click **Create VM Template**.

   The Create VM Template Wizard opens.
3. On the **Select Source** page, click **Use an existing VM template or a virtual hard disk stored in the library**, and then click **Browse**.
4. In the **Select VM Template Source** dialog box, click the appropriate virtual hard disk or virtual machine template, click **OK**, and then click **Next**.
5. Specify identity options as follows, and then click **Next**:
   - With VMM in System Center 2012 SP1 or System Center 2012, on the **VM Template Identity** page, provide a name and optional description for the virtual machine template.
   - With VMM in System Center 2012 R2, on the **Identity** page, enter the virtual machine name and an optional description.

     If the VM template source that you selected on the previous page was a virtual hard disk in VHDX format, the **Generation** box also appears. In the **Generation** box, select **Generation 1** or **Generation 2**. (For more information, see Understanding Generation 1 and Generation 2 Virtual Machines in VMM.)
6. On the **Configure Hardware** page, configure the hardware settings. If you have an existing hardware profile that you want to use, in the **Hardware profile** list, click the desired hardware profile. After you have configured the hardware settings, click **Next**.

   When you configure hardware settings, consider the following:
   - If you intend to deploy the virtual machine to a private cloud, under **Capability**, you must select a cloud capability profile that is supported by the private cloud.
   - With VMM in System Center 2012 R2, if you selected **Generation 1** or **Generation 2** in the previous step, the hardware profiles and hardware options that are available are those of the generation that you selected. For more information, see Understanding Generation 1 and Generation 2 Virtual Machines in VMM.
   - If you configure a network adapter to use static IP addresses, you must also set the media access control (MAC) address to static.
   - In System Center 2012 (without Service Pack 1), it is a known issue that the **Enable spoofing of MAC addresses** check box does not actually change the setting. You must enable spoofing of MAC addresses if you want to deploy a service to a Windows Server 2008 R2–based Hyper-V host (regardless of the version of VMM)

with Network Load Balancing (NLB) enabled. To enable MAC spoofing, you must first create the template and then use the Virtual Machine Manager (VMM) command shell to configure the setting either in the template or in the hardware profile that you use for the template. For more information, see the Windows PowerShell commands in How to Configure NLB for a Service Tier.

- As of System Center 2012 SP1, if the virtual machine will be on a host cluster, you can use VMM to configure virtual machine priority for the virtual machine. For more information, see How to Configure Priority in VMM for a Virtual Machine on a Host Cluster.
- As of System Center 2012 R2, you can use VMM to create virtual machines that will work together as a guest cluster. For more information, see How to Create a Guest Cluster by Using a Service Template in VMM.

7. On the **Configure Operating System** page, open the **Guest OS profile** list and either select a guest operating system profile, or select the type of operating system for which you want to create customized settings—Windows, Linux, or none. Your selection from the list determines the settings that are displayed on the wizard page. Your selection also determines whether additional wizard pages are displayed.

   Configure the guest operating system settings, and then click **Next**.

   When you configure operating system settings, consider the following:

   - Under **Identity Information**:
     - For the **Computer name**, you can provide a pattern to generate computer names. For example, if you enter **server####**, the computer names that are created are server0001, server0002, and so on. The use of a pattern ensures that when you add additional virtual machines to a service, the computer names that are generated are related and identifiable. If you use this method to specify the computer name, you cannot use it in combination with a name prompt parameter (@<name>@). You can use one method or the other, but not both.
     - **DNS domain name** is a Linux-specific option. Enter the domain name portion of the fully qualified domain name (FQDN).
   - The **Roles and Features** settings apply only for Windows, and only if you use the virtual machine template in a service template. Also, the virtual machine must use a guest operating system that supports these settings, as listed in the following table:

Product version of VMM	Guest operating systems that support settings for roles or features
System Center 2012	Windows Server 2008 R2
System Center 2012 Service Pack 1 (SP1)	Windows Server 2008 R2 or Windows Server 2012
System Center 2012 R2	Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2

- The **RunOnce commands** apply only to Linux-based virtual machine templates. These commands run in the specified order during deployment after the operating system has been configured. If shell conventions, such as pipes, are used, we recommend wrapping each command with an explicit invocation of the shell, for example, `/bin/sh –c "<your command>"` . In this example, double quotes in the command must be escaped.
- Under **Root Credentials**, **Public SSH key** is a Linux-specific option. This option sets the content of a specified public Secure Shell (SSH) key as an authorized key for authentication of the root user. Enter the name of a public key file that is stored in the VMM library and has the extension .sshkey.
- To use the virtual machine template in a service template, under **Networking**, configure the settings as follows:

  Note
  Active Directory domain settings do not apply to Linux-based templates.

  - **With VMM in System Center 2012**: You must configure Active Directory domain settings. Use the FQDN. For example, enter **contoso.com** as the domain name. The domain must have a two-way trust relationship with the domain of the VMM management server.

  To use the virtual machine template in a service template, under **Admin Password**, do not select the **No local administrator credential required** option. You can either specify the password of the local administrator account, or select a **Run As account** option.

  - **With VMM as of System Center 2012 SP1**: You can specify Active Directory domain settings by using the FQDN or by using at signs (@) before and after, for example, by entering @Domain@. By using the at signs (@) in this way, the necessary information can be entered when the virtual machine is deployed as part of a service. A trust relationship is not necessary between the domain where the service is deployed and the domain of the VMM management server.

  You can use the virtual machine template in a service template regardless of which option you select under **Admin Password**.

8. If the **Configure Applications** page appears, as needed, configure the applications to install. If you have an existing application profile with settings that you want to use, select that application profile from the **Application profile** list. After you have configured the application settings, click **Next**.

   Note
   Application deployment settings do not apply if you use the template for stand-alone virtual machines that are not part of a service.

9. If the **Configure SQL Server** page appears, as needed, configure the installation of an instance of SQL Server. If you have an existing SQL Server profile that you want to use, in the **SQL Server profile** list, click the SQL Server profile. After you have configured the

SQL Server settings, click **Next**.

> **Note**
> SQL Server settings do not apply if you use the template for stand-alone virtual machines that are not part of a service.

10. On the **Summary** page, confirm the settings, and then click **Create**.

To create a virtual machine template from an existing virtual machine that is deployed on a host

1. Open the **Library** workspace.
2. On the **Home** tab, in the **Create** group, click **Create VM Template**.

   The Create VM Template Wizard opens.
3. On the **Select Source** page, click **From an existing virtual machine that is deployed on a host**, and then click **Browse**.
4. In the **Select VM Template Source** dialog box, click the desired virtual machine, click **OK**, and then click **Next**.
5. On the **VM Template Identity** page, provide a name for the virtual machine template, and then click **Next**.

   > **Warning**
   > A warning message advises you that creating a template will destroy the source virtual machine, and that any user data on the source virtual machine may be lost. To continue, click **Yes**.
6. On the **Configure Hardware** page, click **Next**.
7. On the **Configure Operating System** page, configure the guest operating system settings. If you have an existing guest operating system profile that you want to use, in the **Guest OS profile** list, click the desired guest operating system profile. After you have configured the guest operating system settings, click **Next**.
8. On the **Select Library Server** page, click the library server for the virtual machine, and then click **Next**.
9. On the **Select Path** page, click **Browse**, click a library share and optional folder path, click **OK**, and then click **Next**.
10. On the **Summary** page, confirm the settings, and then click **Create**.

See Also

Configuring Virtual Machine Settings in VMM

How to Create and Deploy a Virtual Machine from a Template

Creating Service Templates in VMM

Creating and Deploying Services in VMM

In VMM, a service is a set of virtual machines that are configured and deployed together and are managed as a single entity. For example, a deployment of a multi-tier line-of-business application.

The following topics provide an overview of services and examples of how you might use services in your VMM environment:

- Creating and Deploying Services Overview
- Common Scenarios for Services

The following topics provide information to help you create, deploy, and manage services in VMM:

- Preparing to Create Services in VMM
- Creating Service Templates in VMM
- Deploying Applications with Services in VMM
- Deploying Services in VMM
- Scaling Out a Service in VMM
- Updating a Service in VMM
- Exporting and Importing Service Templates in VMM

Creating and Deploying Services Overview

In System Center 2012 – Virtual Machine Manager (VMM), a service is a set of virtual machines that are configured and deployed together and are managed as a single entity. For example, a deployment of a multi-tier line-of-business application.

In the VMM console, you use the Service Template Designer to create a service template, which defines the configuration of the service. The service template includes information about the virtual machines that are deployed as part of the service, which applications to install on the virtual machines, and the networking configuration needed for the service (including the use of a load balancer). The service template can make use of existing virtual machine templates or you can define the service without using any existing virtual machine templates.

After the service template is created, you can then deploy the service to a private cloud or to virtual machine hosts. After the service is deployed, you can update the service template and then deploy those updated changes to the already deployed service. Or you can deploy additional virtual machines to an existing service in order to provide additional resources for the service.

Why use services?

Description	Example
Allows you to configure and manage multi-tier applications as a single entity.	You may have a line-of-business application that is comprised of a web server, an application server, and a database server.
Enables you to handle fluctuations in capacity for your application, allowing you to easily add or remove virtual machines needed to support the application.	During the holiday shopping season, your website may need additional web servers deployed to handle the increase in traffic to your site.
Provides the capability to separate the operating system configuration from the application installation, allowing you to manage fewer operating system images. This also makes updating the application or the underlying operating system easier.	You may need to deploy a new version of an application or apply a service pack to the operating system.

For more examples of how to use services, see Common Scenarios for Services.

For a walkthrough of the steps for creating a service, see Test Lab Guide for Creating a Service in VMM.

Common tasks for creating and deploying services

Task	Description	For more information
Prepare to create services	Ensure that the resources you need to create the service (for example, virtual machine templates or sequenced applications) are available before you start	Preparing to Create Services in VMM
Create service templates	Use the Service Template Designer to create service templates to deploy services	Creating Service Templates in VMM
Deploy services	Deploy services to private clouds or hosts by using a service template	Deploying Services in VMM
Scale out a service	Add additional virtual machines to a deployed service	Scaling Out a Service in VMM

Task	Description	For more information
Update a service	Make changes to a deployed service	Updating a Service in VMM
Export and import service templates	Backup service templates or copy service templates to another VMM environment	Exporting and Importing Service Templates in VMM

See Also

Test Lab Guide for Creating a Service in VMM

Common Scenarios for Services

The following are some common scenarios when using services in VMM. These scenarios only apply to virtual machines that are deployed as part of service.

Scenario	Key information	For more information
Deploy a virtual machine with Windows Server roles or features installed	• Must be using at least Windows Server 2008 R2 • Virtual machine must be joined to a domain • Specify the roles or features to install in a guest operating system profile	How to Create a Guest Operating System Profile
Deploy an updated version of the guest operating system (for example, with the latest service pack) to a virtual machine	• Create a new virtual hard disk with the updated operating system • Create an updated service template • Update the service by deploying the new virtual machine with the updated settings	Updating a Service in VMM
Deploy a Microsoft Server Application Virtualization (Server App-V) application	• Sequence the application by using Server App-V • Create an application profile	Server App-V documentation How to Create an Application Profile in a Service Deployment

Scenario	Key information	For more information
Deploy an instance of SQL Server to a virtual machine	• Create a virtual hard disk that contains a sysprepped version (prepared instance) of Microsoft SQL Server. For information about supported versions of Microsoft SQL Server, see How to Create a SQL Server Profile in a Service Deployment. • Create a SQL Server profile.	How to Create a SQL Server Profile in a Service Deployment

See Also

Test Lab Guide for Creating a Service in VMM

Preparing to Create Services in VMM

Before you begin creating service templates to be used to deploy services in VMM, you should review and document all the elements that make up the service that you want to deploy. For example:

- What computers (physical and virtual) need to be deployed to support the service?
- What applications need to be deployed?
- What networking components are used?
- Who will use the service?

You also need to ensure that the VMM resources needed to deploy the service have been created, configured, and are available. For example:

Task	For more information
VMM library resources (such as virtual hard disks)	Configuring the VMM Library
Networking components (such as logical networks and load balancers)	Configuring Networking in VMM
Virtual machine hosts and host groups	Creating Host Groups in VMM Adding and Managing Hyper-V Hosts and

Task	For more information
	Scale-Out File Servers in VMM Managing VMware ESX and Citrix XenServer in VMM
Private clouds	Creating a Private Cloud in VMM Overview
Hardware profiles, guest operating system profiles, application profiles, and SQL Server profiles	Creating Profiles and Templates in VMM
Virtual machine templates	How to Create a Virtual Machine Template
Monitoring and reporting	Configuring Operations Manager Integration with VMM

- If you plan to install applications, ensure that you have all the necessary installation files, scripts, and configuration information available for the applications.
- If you are using Microsoft Server Application Virtualization (Server App-V), ensure that you have sequenced the applications.
- If you plan to deploy an instance of SQL Server on to a virtual machine, ensure that you have a virtual hard drive that contains a sysprepped version (prepared instance) of Microsoft SQL Server. For information about supported versions of Microsoft SQL Server, see How to Create a SQL Server Profile in a Service Deployment.

See Also

Test Lab Guide for Creating a Service in VMM

Creating Service Templates in VMM

A service template defines the configuration of a service. In the VMM console, you use the Service Template Designer to create a service template. The service template includes information about the virtual machines that are deployed as part of the service, which applications to install on the virtual machines, and the networking configuration needed for the service (including the use of a load balancer).

Before creating a service template, review the information in Preparing to Create Services in VMM.

The following topics provide information to help you create a service template in VMM:

- How to Create a Service Template in VMM
- How to Add a Tier to a Service Template
- How to Add Networking Components to a Service Template

- How to Configure the Properties of a Service Template
- How to Create a Guest Cluster by Using a Service Template in VMM

For an overview of services, see Creating and Deploying Services Overview.

See Also

Test Lab Guide for Creating a Service in VMM

How to Create a Service Template in VMM

You can create a service template by using the Service Template Designer in System Center 2012 – Virtual Machine Manager (VMM). After you create the service template, you can add tiers and networking components to the service template.

Create a new service template

Use the following procedure to create and save a new service template.

Account requirements: Services templates can be created by administrators, by delegated administrators, and by members of self-service user roles that have the **Author** action in their scope.

To create a new service template by using the Service Template Designer

1. In the VMM console, open the **Library** workspace.
2. On the **Home** tab, in the **Create** group, click **Create Service Template**.
3. In the **New Service Template** dialog box, do the following:
   - In the **Name** text box, provide a name for the service template. For example, type **Finance Application**.
   - In the **Release** text box, provide a value to indicate the version of the service template. For example, type **1.0** or type **Beta**.

     The release value is important for when you update a service. The release value helps you to identify the version of the service template. For more information about updating a service, see Updating a Service in VMM.
   - Under **Patterns**, select the pattern on which you want to base your service template. For example, if you select **Two Tier Application**, your service template will begin with two tiers.

   After you complete your selections, click **OK**.

   Depending on the pattern that you selected, the canvas area of the Service Template Designer may be empty or may contain some default tiers. For information about adding tiers and networking components to the service template, see the following topics:
   - How to Add a Tier to a Service Template

- How to Add Networking Components to a Service Template

4. On the **Home** tab, in the **Service Template** group, click **Save and Validate** to save the service template.

   If there are any validation errors, a warning icon will appear on the element of the service template that caused the validation error and a message that describes the issue will appear in the properties pane in the Service Template Designer window.

   After you save the service template, it is added to the Service Templates node in the Library workspace. To open an existing service template in the Service Template Designer, select the service template in the Library workspace, and then on the **Service Template** tab, in the **Actions** group, click **Open Designer**.

   Important
   If you try to save changes to a service template that is used as the basis for a deployed service, you need to save the service template with a new release value. The name of the service template will remain the same. In the Service Templates node in the Library workspace, you will see separate entries for the two versions of the service template.

After you create the service template and add the necessary tiers and network components, you can configure the properties of the elements of the service template. For more information, see How to Configure the Properties of a Service Template.

See Also

How to Configure the Properties of a Service Template

Creating Service Templates in VMM

How to Add a Tier to a Service Template

You can add a tier to a service template by doing either of the following:

- By dragging a virtual machine template on to the canvas area
- By using the Create Machine Tier Template wizard

The simplest way to add a tier to a service template is to drag a virtual machine template on to the canvas area. In the Service Template Designer, a list of available virtual machine templates appears in the left pane. Select the virtual machine template that you want to use to create a tier, and then drag the virtual machine template on to the canvas. A tier is created using the properties of the virtual machine template that you selected.

If you created a service template with a pattern that created default tiers for you, you can drag the virtual machine template on to one of those default tiers. The tier will be configured with the properties of that virtual machine template.

Important

No link or relationship is created between the virtual machine template and the tier that you create. Any subsequent changes that you make to the virtual machine template in VMM are not also made to the tier in the service template. And any configuration settings that you make to the tier are not also made to the virtual machine template.

For more information about creating a virtual machine template, see How to Create a Virtual Machine Template.

Creating a tier by using a wizard

You can also use the Create Machine Tier Template wizard to add a tier to a service template. The wizard allows you to create a tier based on one of the following:

- A copy of an existing virtual machine template
- A customized copy of an existing virtual machine template
- A virtual hard disk stored in the VMM library

To add a tier by using the Create Machine Tier Template wizard

1. In the Service Template Designer, on the **Home** tab, in the **Service Template Components** group, click **Add Machine Tier**.
2. On the **Select Source** page of the Create Machine Tier Template wizard, choose the source for your tier.

   If you are using a copy of an existing virtual machine template as the basis for your new tier, do the following:

   a. Click **Browse**, select the virtual machine template you want to use, click **OK**, and then click **Next**.

   b. On the **Additional Properties** page, configure the properties appropriate for this tier, and then click **Next**. For more information about configuring the properties of a tier, see How to Configure the Properties of a Service Template.

   c. On the **Summary** page, review your settings, and then click **Create**. A new tier based on that virtual machine template is added to the canvas of the Service Template Designer.

   If you are using a customized copy of an existing virtual machine template or you are using a virtual hard disk stored in the VMM library as the basis for your new tier, do the following:

   a. Click **Browse**, select the virtual machine template you want to use, click **OK**, and then click **Next**.

   b. On the **Additional Properties** page, configure the properties appropriate for this tier, and then click **Next**. For more information about configuring the properties of a tier, see How to Configure the Properties of a Service Template.

   c. On the **Configure Hardware** page, configure the hardware properties appropriate for

this tier, and then click **Next**. For more information about configuring hardware properties, see How to Create a Hardware Profile.

d. On the **Configure Operating System** page, configure the operating system properties appropriate for this tier, and then click **Next**. For more information about configuring operating system properties, see How to Create a Guest Operating System Profile.

e. On the **Configure Applications** page, if necessary, configure the application that you want to install for this tier, and then click **Next**. For more information about configuring application installations, see How to Create an Application Profile in a Service Deployment.

f. On the **Configure SQL Server** page, if necessary, configure the installation of an instance of SQL Server for this tier, and then click **Next**. For more information about installing an instance of SQL Server, see How to Create a SQL Server Profile in a Service Deployment.

g. On the **Summary** page, review your settings, and then click **Create**. A new tier is added to the canvas of the Service Template Designer.

See Also

Test Lab Guide for Creating a Service in VMM

How to Add Networking Components to a Service Template

You can add the following networking components to a service template:

- Logical network
- Load balancer

For information about adding a load balancer to a service template, see the following topics:

- How to Configure a Hardware Load Balancer for a Service Tier
- How to Configure NLB for a Service Tier
- How to Determine the Virtual IP Address for a Service

Important
You must configure a load balancer for a tier before you deploy a service. After you deploy a service, you cannot add a load balancer by updating the service.

To add a logical network to a service template

1. In the Service Template Designer, on the **Home** tab, in the **Service Template Components** group, click **Add Logical Network**. An element representing the logical network is added to the canvas.

2. Select the logical network element on the canvas, and then in the properties pane at the bottom of the Service Template Designer window, select the appropriate logical network from the **Network** list.
3. To connect the logical network to the network adapter of a tier, on the **Home** tab, in the **Tools** group, click **Connector**. Then on the canvas, drag from the logical network element to the network adapter element of the tier. A connecting line will appear to join the two elements.

How to Configure a Hardware Load Balancer for a Service Tier

Use the following procedures to configure a hardware load balancer for one or more tiers of a service template in System Center 2012 – Virtual Machine Manager (VMM). For example, you might configure a load balancer for a Web tier and for a middle business logic tier.

Note

A load balancer must be configured before you deploy a service. After a service is deployed, you cannot add a load balancer by updating the service.

Account requirements To configure the fabric prerequisites, you must be an administrator or a delegated administrator. Delegated administrators can only configure the prerequisites that are within the scope of their user role. To add a load balancer to a service template, you must be an administrator, a delegated administrator, or a member of a self-service user role that has the **Author** action in their scope.

Fabric Prerequisites

Before you begin this procedure, make sure that the following prerequisites are met:

- Create the desired logical networks, with one or more associated network sites. Ensure that the network sites where users will deploy the service have one or more associated IP subnets that you can create static IP address pools from. Also, ensure that you associate each network site with the host group or one of its parent host groups where the service may be deployed. For more information, see How to Create a Logical Network.
- Create static IP address pools that are associated with the network sites where users will deploy the service. The IP address pool must contain a reserved range of virtual IP addresses that can be assigned to the load balancer. You must set up the static IP address pools for the load balancer and for the virtual machines that will be placed behind the load balancer. These can be from the same pool or from different pools, but the environment must have both virtual IP addresses and IP addresses for the virtual machines. For more information, see How to Create IP Address Pools.
- Configure a hardware load balancer in VMM. You must have a supported hardware load balancer, and you must have installed the load balancer provider on the VMM management server. When you configure the load balancer, you must select the host group or one of its

parent host groups where the service may be deployed. Also, when you configure logical network affinity, make sure that you select the logical networks from which the load balancer can obtain its virtual IP address as the front-end, and the logical networks to which you want to make the load balancer available for connections from the virtual machines that make up a service tier as the back-end. For more information, see How to Add Hardware Load Balancers.

- Create a virtual IP (VIP) template for the hardware load balancer. For more information, see How to Create VIP Templates for Hardware Load Balancers.
- Ensure that the hosts where the service may be deployed can access the load balancer. Therefore, the host group where the load balancer is available must be the host group of the virtual machine host or one of its parent host groups.
- On each host where the service may be deployed, ensure that a physical network adapter on the host is configured to use the same logical network that the service tier will use. For example, if the tier will use the BACKEND logical network, the BACKEND logical network must be associated with a physical adapter on the host. For more information, see How to Configure Network Settings on a Hyper-V Host, How to Configure Network Settings on a VMware ESX Host, and How to Configure Network Settings on a Citrix XenServer Host.

Note

For an overview of the load balancer workflow, see the "Load Balancer Integration" section of Configuring Networking Overview.

To add a load balancer to a service tier

1. Open the service template in the **Virtual Machine Manager Service Template Designer**. To do this, follow these steps:
   a. Open the **Library** workspace.
   b. In the **Library** pane, expand **Templates**, and then click **Service Templates**.
   c. In the **Templates** pane, click the service template that you want to open.
   d. On the **Service Template** tab, in the **Actions** group, click **Open Designer**.

      The **Virtual Machine Manager Service Template Designer** opens with the service template displayed.
2. On the **Home** tab, in the **Service Template Components** group, click **Add Load Balancer**.

   Note

   This action is only available if VIP templates are defined in the Fabric workspace. Only a full administrator or delegated administrator can configure VIP templates.
3. Click the load balancer object (identifiable by the VIP template name) that is added to the service map. In the load balancer details, select a different VIP template if needed.
4. Configure the load balancer connection to a virtual network adapter for the service tier.
   a. On the **Home** tab, in the **Tools** group, click the **Connector** tool to select it.
   b. On the service map, click the **Server connection** object that is associated with the load balancer, and then click a **NIC** object (for example, click the network adapter for

the BACKEND logical network). This connects the load balancer to the network adapter.

c. Click the **NIC** object to display its properties in the detail area. Verify that the IPv4 address type, the IPv6 address type, or both types (depending on the logical network configuration) are static, and that the MAC address type is static.

5. Configure the client connection for the load balancer to use the correct logical network. With the Connector tool still selected, on the service map, click the **Client connection** object that is associated with the load balancer, and then click a logical network object. For example, click the BACKEND logical network. This connects the load balancer to the logical network.
6. Save the updated service template settings. On the **Home** tab, in the **Service Template** group, click **Save and Validate**.

Important
When the service is deployed, VMM automatically selects a virtual IP address from the reserved range that is defined in the static IP address pool, and assigns it to the load-balanced service tier. To enable users to connect to the service, the following must occur:

- A full administrator or delegated administrator must determine the virtual IP address that VMM assigned to the load balancer.
- After the virtual IP address is determined, a Domain Name System (DNS) administrator must manually create a DNS entry for the virtual IP address. The DNS entry for the virtual IP address should be the name that users will specify to connect to the service, for example *ServiceName.contoso.com*.

  For more information, see How to Determine the Virtual IP Address for a Service.

See Also

How to Add Networking Components to a Service Template

How to Configure NLB for a Service Tier

How to Deploy a Service in VMM

How to Configure NLB for a Service Tier

Use the following procedure to configure Microsoft Network Load Balancing (NLB) for one or more tiers of a service template in Virtual Machine Manager (VMM). For example, you might configure a load balancer for a Web tier and for a middle business logic tier.

Note
NLB cannot be used with service tiers running Linux. To load balance service tiers that are running Linux, you must use hardware load balancers. For more information, see Configuring Load Balancing in VMM Overview.

To support NLB, there are several prerequisites that must be met. These include fabric-related prerequisites, and specific operating system requirements and configuration settings that are required for the virtual machines that you want to load balance.

Important
You must configure a load balancer for a tier before you deploy a service. After you deploy a service, you cannot add a load balancer by updating the service.

Account requirements To configure the fabric prerequisites, you must be an administrator or a delegated administrator. Delegated administrators can only configure the prerequisites that are within the scope of their user role. To add a load balancer to a service template, or to complete the virtual machine template prerequisites, you must be an administrator, a delegated administrator, or a member of a self-service user role that has the **Author** action in their scope.

Fabric Prerequisites

Before you begin this procedure, make sure that the following prerequisites are met:

- Create a virtual IP (VIP) template for NLB. For more information, see How to Create VIP Templates for Network Load Balancing (NLB).
- Create a logical network, with one or more associated network sites. Ensure that the network sites where users will deploy the service have one or more associated IP subnets that you can create static IP address pools from. Also, ensure that you associate each network site with the host group or one of its parent host groups where the service may be deployed.

  For more information, see How to Create a Logical Network.
- Create static IP address pools that are associated with the network sites where users will deploy the service. The pools must be associated with the network sites where users will deploy the service. The IP address pools must contain a reserved range of virtual IP (VIP) addresses that can be assigned to the load balancer, and a range for the virtual machines that will be placed behind the load balancer.

  Important
  The addresses for the VIPs and the dedicated IP addresses for the virtual machines can be from the same pool or from different pools. However, the VIP address and the dedicated virtual machine IP addresses must all be in the same subnet.

  For more information, see How to Create IP Address Pools.
- On each host where the service may be deployed, ensure that a physical network adapter on the host is configured to use the same logical network that the service tier will use. For example, if the tier will use the BACKEND logical network, the BACKEND logical network must be associated with a physical adapter on the host. For more information, see How to Configure Network Settings on a Hyper-V Host.

Virtual Machine Template Prerequisites

When you use the Create VM Template wizard to create a virtual machine template for a service tier that you want to load balance by using NLB, or if you have an existing virtual machine template that you want to use, verify that the following prerequisites are met:

Note

The following table lists only the required settings for NLB. Configure other settings according to your virtual machine requirements. For information about how to create a virtual machine template for a service tier, see How to Create a Virtual Machine Template.

NLB Requirements	More Information
Ensure that the operating system for the virtual hard disk is an appropriate version, as listed under “More information.”	One of the requirements is that you install the NLB feature in the guest operating system. To install features through VMM, for System Center 2012, the guest operating system must be set to Windows Server 2008 R2. For System Center 2012 SP1, it can be set to Windows Server 2008 R2 or Windows Server 2012. For System Center 2012 R2, it can be set to Windows Server 2008 R2, Windows Server 2012, or Windows Server® 2012 R2. **Note** The NLB feature is included with all editions of Windows Server 2008 R2 except for HPC Edition. It is included with all editions of Windows Server 2012 and Windows Server 2012 R2.
Configure the network adapter to use a logical network with static IP address assignment, static MAC addresses, and, depending on the hypervisor that you want to deploy the service to, enable MAC address spoofing.	On the **Configure Hardware** page of the Create VM Template wizard (or the **Hardware Configuration** tab in the properties of an existing virtual machine template), click a network adapter, and then do the following: **Note** If you are using a hardware profile, configure these settings in the hardware profile. 1. Under **Connectivity**, click **Connected to**, and then select the desired logical network that meets the requirements that are outlined in the “Fabric Requirements” section of this topic. 2. Click **Static IP (from a static IP pool)** to configure the network adapter to use a static IP address. In the **IP protocol version** list, select the correct IP protocol version, for example, **IPv4 only**.

NLB Requirements	More Information

	3. Under **MAC Address**, click **Static**.
	
	Important
	If you want to deploy the service to a Windows Server 2008 R2-based Hyper-V host (with or without Service Pack 1), you must also enable MAC address spoofing for NLB to work correctly. If you do not, service deployment will fail. However, in System Center 2012 (without Service Pack 1) you cannot use the **Enable spoofing of MAC addresses** check box in the virtual machine template or the associated hardware profile to configure this setting. Instead, you must use the VMM command shell to configure this setting after you create the template, or in the hardware profile that you use for the template.
	
	To update a virtual machine template, use the following syntax, where *VMTemplate01* represents the name of the virtual machine template:
	
	`PS C:\> $VMTemplate = Get-SCVMTemplate -Name "VMTemplate01"`
	
	`PS C:\> $VirtNetworkAdapter = Get-SCVirtualNetworkAdapter -VMTemplate $VMTemplate`
	
	`PS C:\> Set-SCVirtualNetworkAdapter -VirtualNetworkAdapter $VirtNetworkAdapter -EnableMACAddressSpoofing $True`
	
	To update a hardware profile, use the following syntax, where *HWProfile01* represents the name of the virtual hardware profile:
	
	`PS C:\> $HWProfile = Get-SCHardwareProfile | where { $_.Name -eq "HWProfile01" }`
	
	`PS C:\> $VirtNetworkAdapter = Get-SCVirtualNetworkAdapter -HardwareProfile`

NLB Requirements	More Information

	`$HWProfile`
	`PS C:\> Set-SCVirtualNetworkAdapter -VirtualNetworkAdapter $VirtNetworkAdapter -EnableMACAddressSpoofing $True`
	  **Note**
	Do not enable MAC address spoofing for a virtual machine template or an associated hardware profile that will be used to deploy a service to a Windows Server 2008 with Service Pack 2-based Hyper-V host, a Citrix XenServer host, or a VMware ESX host.

Set the administrator password	On the **Configure Operating System** page of the Create VM Template wizard (or the **OS Configuration** tab in the properties of an existing virtual machine template), under **General Settings**, click **Admin Password**. Either specify the password of the local administrator account or select a Run As account for the local administrator account.  **Note** If you are using a guest operating system profile, configure the administrator account settings in the profile.
Configure the virtual machine to join a domain	On the **Configure Operating System** page of the Create VM Template wizard (or the **OS Configuration** tab in the properties of an existing virtual machine template), under **Networking**, configure the virtual machine to join a domain. This includes the credentials to join the domain.  **Note** If you are using a guest operating system profile, configure the domain settings in the profile.
Enable the Network Load Balancing feature	On the **Configure Operating System** page of the Create VM Template wizard (or the **OS**

NLB Requirements	More Information
	Configuration tab in the properties of an existing virtual machine template), do the following: **Note** If you are using a guest operating system profile, configure these settings in the profile. 1. Under **Roles and Features**, click **Features**. 2. Select the **Network Load Balancing** check box. 3. Optionally, under **Remote Server Administration Tools**, select the **Network Load Balancing Tools** check box. Network Load Balancing Tools include the Network Load Balancing Manager snap-in, Windows PowerShell tools for managing Network Load Balancing, and the Nlb.exe and Wlbs.exe command-line tools. **Important** The NLB tools are not available in a Server Core installation of the Windows Server 2008 R2 operating system or the Windows Server 2012 operating system. Therefore, do not select this option if you are using a Server Core installation, or service deployment will fail. (If you are using a Server Core installation, and you receive a validation error message saying that you must select NLB and the NLB tools feature, make sure that you have the NLB feature selected. You can ignore the part of the warning message about NLB tools as it is not required.)

After you have a virtual machine template that meets the virtual machine template prerequisites, create a service template that uses the virtual machine template. The following procedure

assumes you have an existing service template. For information about how to create a service template, see How to Create a Service Template in VMM.

To add an NLB load balancer to a service tier

1. Open an existing service template that meets the prerequisites that are outlined in the "Virtual Machine Template Prerequisites" section of this topic. To do this, follow these steps:
   a. Open the **Library** workspace.
   b. In the **Library** pane, expand **Templates**, and then click **Service Templates**.
   c. In the **Templates** pane, click the service template that you want to open.
   d. On the **Service Template** tab, in the **Actions** group, click **Open Designer**.

      The **Virtual Machine Manager Service Template Designer** opens with the service template displayed.
2. Click the virtual machine template that represents the tier that you want to load balance. In the virtual machine template details pane, select the **This computer tier can be scaled out** check box, and configure the number of instances.
3. On the **Home** tab, in the **Service Template Components** group, click **Add Load Balancer**.

   Note
   This action is only available if VIP templates are defined in the Fabric workspace. Only a full administrator or delegated administrator can configure VIP templates.
4. Make sure that the correct VIP template for NLB is selected. To do this, follow these steps:
   a. Click the load balancer object (identifiable by the VIP template name) that is added to the service map.
   b. In the load balancer details, in the **Load Balancer VIP Profile** list, select a different VIP template if needed.
   c. Verify that the **Load Balancer Model** field indicates **Network Load Balancing (NLB)**.
5. Configure the load balancer connection to a virtual network adapter for the service tier.
   a. On the **Home** tab, in the **Tools** group, click the **Connector** tool to select it.
   b. On the service map, click the **Server connection** object that is associated with the load balancer, and then click a **NIC** object (for example, click the network adapter for the BACKEND logical network). This connects the load balancer to the network adapter.
   c. Click the **NIC** object to display its properties in the detail area. Verify that the IPv4 address type, the IPv6 address type, or both types (depending on the logical network configuration) are static, and that the MAC address type is static.
6. Configure the client connection for the load balancer to use the correct logical network. With the Connector tool still selected, on the service map, click the **Client connection** object that is associated with the load balancer, and then click a logical network object.

For example, click the BACKEND logical network. This connects the load balancer to the logical network.

Important
For NLB deployments, the logical network that is associated with the client connection and the logical network of the NIC that is associated with the server connection in step 5 must be the same.

7. Save the updated service template settings. On the **Home** tab, in the **Service Template** group, click **Save and Validate**.

Important
When the service is deployed, VMM automatically selects a virtual IP address from the reserved range that is defined in the static IP address pool, and assigns it to the load-balanced service tier. To enable users to connect to the service, the following must occur:

- A full administrator or delegated administrator must determine the virtual IP address that VMM assigned to the load balancer.
- After the virtual IP address is determined, a Domain Name System (DNS) administrator must manually create a DNS entry for the virtual IP address. The DNS entry for the virtual IP address should be the name that users will specify to connect to the service, for example *ServiceName.contoso.com*.

  For more information, see How to Determine the Virtual IP Address for a Service.

See Also

How to Add Networking Components to a Service Template

How to Configure a Hardware Load Balancer for a Service Tier

How to Deploy a Service in VMM

How to Determine the Virtual IP Address for a Service

When you deploy a service that is configured to use a hardware load balancer or Microsoft Network Load Balancing (NLB), System Center 2012 – Virtual Machine Manager (VMM) automatically assigns a virtual IP (VIP) address to the load balancer from the static IP address pool. The virtual IP address is the address on the load balancer that users will connect to when they access a service.

To enable users to connect to a service, you must determine the virtual IP address that is assigned to the service, and then ask your Domain Name System (DNS) administrator to register the address in DNS. For example, the DNS administrator can register the name of

ServiceName.contoso.com, where *ServiceName* is the name that you want users to specify when they connect to the service.

Account requirements To perform this procedure, you must be a full administrator, a delegated administrator, or a read-only administrator.

To determine the virtual IP address that is assigned to a service

1. Open the **Fabric** workspace.
2. In the **Fabric** pane, expand **Networking**, and then click **Load Balancers**.
3. On the **Show** tab, click **Services**.
4. In the **Load Balancer Information for Services** pane, expand the service with the load-balanced tier to see which virtual IP address was assigned.
5. To view more information, click the virtual IP address, and then view the associated information in the details pane.

After you obtain the IP address, ask the DNS administrator to create a DNS entry for the virtual IP address on a DNS server.

See Also

How to Configure a Hardware Load Balancer for a Service Tier

How to Configure NLB for a Service Tier

How to Configure the Properties of a Service Template

You can configure the following settings in a service template:

- The service
- Each tier of the service
- Networking components (network adapters and load balancers)

Note
The following procedures assume that you have already started to create a service template and that you are working in the Service Template Designer. For information about creating a service template, see How to Create a Service Template in VMM.

To configure settings for the service template

1. On the canvas, select the service template object. The service template object contains the service template name and the release value.
2. The most common properties that you can change appear in the details pane in the Service Template Designer. To display all of the settings that you can configure, click

View All Properties in the details pane.

The following table lists some key settings that you can configure for the service template:

Setting	Description
Name	The name for the service template. This name will appear in the VMs and Services workspace if you deploy a service that is based on this service template.
Release	A value to indicate the version of the service template (for example, **1.0** or **Beta**). The release value is important for when you update a service. The release value helps you to identify the version of the service template. For more information about updating a service, see Updating a Service in VMM.
Access	The owner of the service template and a list of self-service users that can use this service template to deploy a service.

To configure settings for a tier

1. On the canvas, select the tier object.
2. The most common properties that you can change appear in the details pane in the Service Template Designer. To display all settings that you can configure, click **View All Properties** in the details pane.

   The following table lists some key settings that you can configure for a tier:

Setting	Description
Name	The name for the tier. This name will appear in the VMs and Services workspace if you deploy a service that is based on this service template.
Scale out	The ability to add additional virtual machines to a tier of a deployed service. For more information about scaling out a tier of a service, see Scaling Out a Service in VMM.

Upgrade domains	A group in which VMM automatically places instances of a tier of a service, so that when the service is updated, those instances are updated at the same time. For more information about updating a service, see Updating a Service in VMM.
Availability set	A set that contains the virtual machines that you want VMM to keep on separate hosts in order to improve service continuity. When it is possible, VMM will separate virtual machines that are in the same availability set, rather than placing them together on one host. For more information about availability sets, see How to Configure Availability Sets in VMM for Virtual Machines on a Host Cluster.
Hardware configuration	The hardware settings that you want a virtual machine that is deployed in this tier to use. For more information about hardware settings, see How to Create a Hardware Profile.
Guest operating system configuration	The settings of the guest operating system that you want a virtual machine that is deployed in this tier to use. For more information about guest operating system settings, see How to Create a Guest Operating System Profile.
Application configuration	The applications that you want to be installed on a virtual machine that is deployed in this tier. For more information about application installation settings, see How to Create an Application Profile in a Service Deployment.
SQL Server configuration	The instances of SQL Server that you want to be installed on a virtual machine that is deployed in this tier. For more information about installing an instance of SQL Server, see How to Create a SQL Server Profile in a Service Deployment.

To configure settings for a networking component

- On the canvas, select the networking object that you want to configure.

  For a network adapter, you can configure the following settings:

  - **IPv4 address type (dynamic or static)**
  - **IPv6 address type (dynamic or static)**
  - **MAC address type (dynamic or static)**
  - **Required bandwidth**

  For a load balancer, you can configure the virtual IP (VIP) profile that is being used and provide a description. For more information about adding a load balancer to a tier, see the following topics:

  - How to Configure a Hardware Load Balancer for a Service Tier
  - How to Configure NLB for a Service Tier

How to Create a Guest Cluster by Using a Service Template in VMM

This topic explains how to create a guest cluster by using a service template in Virtual Machine Manager (VMM) in System Center 2012 R2. A guest cluster can be configured to run a variety of applications, but one application that guest clusters often run is SQL Server.

Service templates can be built up from other profiles and templates. Regardless of how a service template is created for a guest cluster, it includes instructions that tell VMM to deploy multiple virtual machines together as a “tier” (in this case, the tier is the guest cluster). The service template also includes instructions that tell VMM how to run appropriate scripts to create a cluster from the virtual machines as they are deployed.

Important
The following procedures apply only to VMM in System Center 2012 R2. For information about creating profiles and templates in VMM in System Center 2012 SP1 or System Center 2012, see the list of topics in Creating Profiles and Templates in VMM.

Prerequisites

To prepare to create a guest cluster, review the following prerequisites:

- **Host cluster**: Virtual machines in a guest cluster can be deployed only to host clusters running Windows Server® 2012 R2. If you deploy a service from a service template that includes one or more guest clusters, and there are no host clusters running Windows Server 2012 R2 to which the guest cluster can be deployed, deployment of the guest cluster will fail. For information about host clusters, see Creating and Modifying Hyper-V Host Clusters in VMM.

- **Scripts**: Scripts that you will need for creating the guest cluster include:
  - A script to run on the first virtual machine so that it can form the cluster.
  - A script to run on the later virtual machines so that they can join the cluster.
  - Potentially, scripts that install your application correctly for a cluster. For example, to run SQL Server 2012, you might need a script that installs SQL Server 2012 correctly on the first node of the guest cluster, and another script to install it on later nodes. (You cannot use a sysprepped image of SQL Server for installation, because this does not work in the context of a cluster.)

  Note

  In VMM, script settings are specified as part of the “application” configuration—either in an application profile or on the application tab of a VM template or service-tier template.
- **Information about hardware settings**: You will need to know basic hardware settings, such as the amount of memory, that you want on the nodes (the virtual machines) in the guest cluster.
- **One or more virtual hard disks to be used by all nodes in the guest cluster**: Most clusters have one or more shared disks that are used by all nodes in the cluster, although this is not required. To configure shared disks for your guest cluster, use the following guidelines:
  - Install Update Rollup 2 for System Center 2012 R2 before using VMM to create a guest cluster that uses shared virtual hard disks (VHDX files).
  - Review the virtual hard disks (VHDX files) in your VMM library, and make sure that the VHDX files that will be shared by the cluster nodes are in the library.
  - Use new VHDX files. Do not reuse VHDX files from a previous cluster.
  - Identify a single location (path) in SCSI-based shared storage where all the VHDX files for the guest cluster will be placed at deployment time.

    You can use storage classifications to control the placement of the shared VHDX files, but within your storage classification, you must have at least one location with the capacity to contain all the shared VHDX files for your guest cluster. VMM will not deploy the shared VHDX files to multiple locations.

    You can vary the location of shared VHDX files at deployment time, even if you use the same service template to deploy a series of guest clusters. To do this, you must deploy your guest clusters to a host group (not a cloud). Then, at deployment time, you can specify a single location (path) for the shared VHDX file or files for that particular guest cluster. This will override the location that you specified in the virtual machine template.

  For background information about virtual hard disks that are used for a guest cluster, see Virtual Hard Disk Sharing Overview.

  Important

  If you want to manage a guest cluster by using VMM, and you want to use shared virtual hard disks for the guest cluster, be sure you’ve installed Update Rollup 2 for System Center 2012 R2. Also, for best results with managing the guest cluster in

VMM, we recommend that you create the guest cluster as a service in VMM, rather than creating the guest cluster by using Hyper-V.

- **Virtual hard disk for the operating system for each node of the guest cluster**: You will need a virtual hard disk file that contains the operating system (prepared with Sysprep) that you want the virtual machines in the guest cluster to use. (This is different from the virtual hard disk file that will be deployed to shared storage.) When each node is created, VMM will use a copy of this virtual hard disk file for the system disk of the node.

With these prerequisites in place, you can create a service template and connect all the configuration elements together.

This topic contains the following procedures:

1. Specify settings for scripts that run when a guest cluster is created
2. Create a virtual machine template and include it in a service tier for a guest cluster

Specify settings for scripts that run when a guest cluster is created

In the application settings in VMM in System Center 2012 R2, you can include scripts that will be run at specific times in relation to the creation of a guest cluster, such as **Creation: First VM** or **Creation: VMs After First**. The following procedure provides steps for specifying such settings.

To specify settings for scripts that run when a guest cluster is created

1. Confirm that your application components, especially your scripts, have been copied to the VMM library share. When you copy a script, place it in a folder in the library share and give the folder an extension of **.cr**, which indicates a “custom resource” in VMM.
2. Open the **Library** workspace.
3. On the **Home** tab, in the **Create** group, click **Create**, and then click **Application Profile**.

   The New Application Profile dialog box opens.
4. On the **General** tab, in the **Name** box, type a name and an optional description. For example, type the name **GuestSQL**.
5. On the **General** tab, in the **Compatibility** list, leave the default selection, **General**.

   You must use the **General** option for a profile in which you specify scripts that first form a cluster and then join nodes to the cluster.
6. Click the **Application Configuration** tab, click **OS Compatibility**, and then select one or more editions of the Windows Server 2012 R2 or Windows Server 2012 operating systems. For a guest cluster, do not select any of the earlier operating systems that are listed.
7. Still on the **Application Configuration** tab, add the scripts that you need for creating the first node of the cluster and for adding other nodes to the cluster. To add a script, click **Add** and then select **Script**. The number of scripts is not limited, and you can specify the order in which the scripts will run. Provide the following types of information for each script:

- For a script that will run on the first node of the cluster when it is created (and not on other nodes), for **Script command type**, select **Creation: First VM**.
- For a script that will run on later nodes of the cluster when they are created (and not on the first node), for **Script command type**, select **Creation: VMs After First**.
- For each script, specify the executable name and the parameters through which the script will run.

  Note

  A script can contain settings to be entered when you are configuring the service for deployment. To format this type of setting, type the parameter in the **Parameters** field in the following format: @<SettingLabel>@ (for example, type @ClusterName@).

  For example, consider a script that runs with the executable name **Cmd.exe** with the **/q** and **/c** parameters. Suppose that the script is called **FormCluster.cmd**, and it requires that the cluster name is supplied when the cluster is deployed. For this script, you could specify the following information:

  Executable program: **Cmd.exe**

  Parameters: **/q /c FormCluster.cmd @ClusterName@**
- For each script, provide the script location. Under **Script resource package**, click **Browse** and then select the folder with the **.cr** extension into which you copied the script. Click **OK**.
- For each script, provide a **Run As account**.
- Configure other settings as needed, such as how long the script should run before timing out, the failure and restart policies that specify what to do if there is an error, and other settings. To configure these settings, under **Scripts**, select the script and review or change the deployment order, timeout, or other settings. As needed, click **Advanced** and view or configure advanced settings such as failure and restart policies.

You can also add scripts that will delete the guest cluster in an orderly way. For such a script, select a **Script command type** of **Deletion: VMs Before Last** or **Deletion: Last VM**.

8. To add more scripts to the application profile, on the **Application Configuration** tab, click **Add**, select **Script**, and specify appropriate settings.

   You can add scripts that use a **Script command type** that was not mentioned in the previous step. For example, with a **Script command type** of **Pre-Install**, a script will run on the first virtual machine and also on later virtual machines that are created as part of the service tier.
9. After you have made all your selections, click **OK**.
10. To verify that the profile was created, in the **Library** pane, expand **Profiles**, and then click **Application Profiles**.

    The application profile appears in the **Profiles** pane.

Create a virtual machine template and include it in a service tier for a guest cluster

When you create a virtual machine template and you include it in a service tier for a guest cluster, in most cases, you will include settings for a shared VHDX file in the virtual machine template. This VHDX file must be deployed to shared storage that has SCSI channels available for each node of the cluster. This configuration provides each node of the guest cluster with access to the same VHDX file (disk).

Also, the service tier in which the virtual machine template is placed must have settings for scaling the tier out to multiple instances of the virtual machine. Each instance in the tier is one node in the guest cluster.

To create a virtual machine template and include it in a service tier for a guest cluster

1. Ensure that on the VMM library share, you have a virtual hard disk that contains the operating system (prepared with Sysprep) that you want the virtual machines in the guest cluster to use. This virtual hard disk cannot be blank. (This is different from the virtual hard disk file that will be deployed to shared storage.)
2. Open the **Library** workspace.
3. On the **Home** tab, in the **Create** group, click **Create VM Template**.

   The Create VM Template Wizard opens.
4. On the **Select Source** page, click **Use an existing VM template or a virtual hard disk stored in the library**, and then click **Browse**.
5. In the **Select VM Template Source** dialog box, click the virtual hard disk described in step 1 of this procedure, click **OK**, and then click **Next**.
6. On the **VM Template Identity** page, provide a name for the virtual machine template, and for the **Generation**, select **Generation 1**. Then click **Next**.

   Because the VM template must be added into a service template, you cannot choose **Generation 2**.
7. On the **Configure Hardware** page, configure the hardware settings. If you want to use a hardware profile, make sure it includes the settings in the list that follows, and then in the **Hardware profile** list, click the intended hardware profile.

   When you configure hardware settings, consider the following:

   - If you intend to deploy the virtual machine to a private cloud, under **Capability**, you must select a cloud capability profile that is supported by the private cloud.
   - To configure the guest cluster to use a shared virtual hard disk (in the VHDX format), under **Bus Configuration**, click **SCSI adapter 0**, and then near the top of the page, beside **New**, click **Disk**. The new disk appears as a listing under the SCSI adapter. Select that disk and then select **Share the disk across the service tier**. Ensure that the check box for **Contains the operating system for the virtual machine** is cleared. Click **Browse**, select the VHDX file that you want VMM to deploy to shared storage, and then click **OK**. Repeat this process for each additional node in the cluster—add the same disk each time, but ensure that the SCSI channel is unique for

each instance of that disk.

Important
For each node that you plan to have in the guest cluster, configure one instance of the same disk, and give that instance a unique SCSI channel.

You can repeat the process of adding disks that will be used by the cluster. However, be sure to review “Prerequisites,” earlier in this topic, for details about choosing the shared storage location. If you do add more shared disks, ensure that each additional disk is configured with the same number of SCSI channels as the number of nodes that you plan to have in the guest cluster.

- If you configure a network adapter to use static IP addresses, you must also set the media access control (MAC) address to static.
- Under **Network Adapters**, select the network adapter, and at the bottom of the details pane, select **Enable guest specified IP addresses**. This enables the nodes (virtual machines) in the guest cluster to specify IP addresses for the cluster itself, and for applications that you configure to run in the cluster.
- Under **Advanced**, click **Availability**, and then select **Make this virtual machine highly available**. When this is selected, the virtual machine is created as a clustered instance on the host cluster, so that if one host fails, the virtual machine will fail over to another host in the cluster.
- As a best practice, under **Advanced**, click **Availability**, and then click the **Manage availability sets** button. To create a new availability set, click the **Create** button, provide a name for the set, and then click **OK**. In the **Manage Availability Sets** dialog box, click **OK**.

  The availability set name that you specify will be used by all the nodes (virtual machines) in the guest cluster, which means that VMM will attempt to keep the virtual machines on separate hosts, so that if one host fails, a virtual machine on another host can provide service as needed. (If you have worked with failover clusters in other contexts, you might know this setting as **AntiAffinityClassNames**.)

After you have configured the hardware settings, click **Next**.

8. On the **Configure Operating System** page, open the **Guest OS profile** list and either select a guest operating system profile, or select **[Create new Windows operating system customization settings]**. Your selection from the list determines the settings that are displayed on the wizard page. Your selection also determines whether additional wizard pages are displayed.

   When you configure operating system settings, consider the following:

   - Under **Identity Information**, for the **Computer name**, you can provide a pattern to generate computer names. For example, if you enter **server####**, the computer names that are created are server0001, server0002, and so on. The use of a pattern ensures that when you add additional virtual machines to a service, the computer names that are generated are related and identifiable. If you use this method to specify the computer name, you cannot use it in combination with a name prompt parameter (@<name>@). You can use one method or the other, but not both.

- Under **Networking**, you can specify specify settings for Active Directory Domain Services by using the FQDN or by using at signs (@) before and after the domain name, for example, @Domain@. By using the at signs (@) in this way, the necessary information can be entered when the virtual machine is deployed as part of a service. A trust relationship is not necessary between the domain where the service is deployed and the domain of the VMM management server.

After you configure the guest operating system settings, click **Next**.

9. On the **Configure Applications** page, click **Next**. You will add these settings to your configuration later, as described in this procedure.
10. On the **Configure SQL Server** page, click **Next**.
11. On the **Summary** page, confirm the settings, and then click **Create**. Confirm that the virtual machine template was created.
12. In the **Library** workspace, on the **Home** tab, in the **Create** group, click **Create Service Template**.

    The **New Service Template** dialog box opens.
13. Specify a name, version, and pattern for the template. The patterns help you begin to create a service template, but you can change the number of tiers after you exit this dialog box. After you complete your selections, click **OK**.

    The pattern that you selected appears on the canvas. If you select a pattern with tiers, the tiers exist, but they do not have VM templates applied to them.
14. In the **VM Templates** pane (next to the canvas), click the virtual machine template that you just created and drag it onto a tier. If you do not yet have tiers on the canvas, drag the virtual machine template anywhere on the canvas.

    The label in the box (for the tier) changes to reflect the name of the virtual machine template. If the virtual machine template contains network settings, a connector might appear lower in the box. This connector shows a connection to a VM network.

    Dragging a virtual machine template onto the canvas is the basic process for building a service template. You can change the number of tiers as needed. You can add a tier by dragging an additional virtual machine template onto the canvas, or remove a tier by deleting a virtual machine template that is on the canvas.
15. On the canvas, right-click the tier that you just dragged the virtual machine template onto, click **Properties**, and then click **Application Configuration**. Near the top of the page, next to **Application profile**, click the drop-down list, and then click the application profile that you created in the procedure earlier in this topic. Then click **OK**.

    Because you have taken this step, when the service is deployed, the scripts that you specified in the application profile will run.
16. On the **Home** tab, in the **Service Template** group, click **Save and Validate** to save the service template.

    If there are any validation errors, a warning icon appears on the element of the service template that caused the validation error, and a message that describes the issue appears in the properties pane in the Service Template Designer window.
17. Right-click the box that represents the tier for the guest cluster, and then click

Properties. On the **General** tab, select **This machine tier can be scaled out**, and then specify values greater than 1 for **Default instance count** and **Maximum instance count**. The values that you specify control the number of nodes in the guest cluster. For example, **Default instance count** specifies the number of nodes that VMM will create when the cluster is created.

Important

Be sure that the **Maximum instance count** is less than or equal to the number of SCSI channels that you previously configured for the disk (under **Bus Configuration**). Be sure that the **Default instance count** is less than or equal to the **Maximum instance count**.

18. With the properties of the tier for the guest cluster still displayed (as in the previous step), for **Number of upgrade domains**, specify a value that is the same as the **Maximum instance count** that you specified in the previous step.

    For example, if you specified a **Default instance count** of **3** and a **Maximum instance count** of **3**, the guest cluster would have three nodes. When you updated the service, if you specified an incorrect value of **1** for the **Number of upgrade domains**, VMM would perform the update in one stage, which means it would update all three virtual machines at the same time. This would cause the cluster to lose quorum and stop running during the update process. However, if you specified an appropriate value of **3** for the **Number of upgrade domains**, VMM would perform the update in three stages, which means it would update one virtual machine at a time. This would leave two virtual machines in the guest cluster running at any given time, and the cluster would continue to run during the update process.

    For more information about upgrade domains, see Updating a Service in VMM.

19. On the **Home** tab, in the **Service Template** group, click **Save and Validate** to save the service template.

For information about deploying the service, see Deploying Services in VMM.

See Also

Creating Profiles and Templates in VMM

Preparing to Create Services in VMM

Deploying Services in VMM

Virtual Hard Disk Sharing Overview

Configuring Availability Options for Virtual Machines Overview

How to Configure Priority in VMM for a Virtual Machine on a Host Cluster

Using Guest Clustering for High Availability

Test Lab Guides: System Center 2012 SP1 - Virtual Machine Manager

Deploying Applications with Services in VMM

VMM supports the installation of Microsoft Server Application Virtualization (Server App-V) applications, Microsoft Web Deploy applications, and Microsoft SQL Server data-tier applications (DACs), and for running scripts when deploying a virtual machine as part of a service. VMM also supports installing an instance of SQL Server on to a virtual machine.

For more information, see the following topics:

- How to Create an Application Profile in a Service Deployment
- How to Create a SQL Server Profile in a Service Deployment
- Application Framework Resources in VMM

For more information about Server App-V, see Server App-V documentation.

Application Framework Resources in VMM

The Application Frameworks resources available in VMM can be used to install tools such as the Web Deployment Tool and a Microsoft Server Application Virtualization (Server App-V) client on a virtual machine and then install applications during service deployment. These resources are available in the VMM library.

The Application Frameworks resources that VMM provides include x86 and x64 versions of the Server App-V agent, the Server App-V Sequencer, Server App-V PowerShell cmdlets, and the Microsoft Web Deployment tool.

The resources also include scripts that can be added to application profiles in service templates to install virtual applications and Web applications during service deployment. The following table describes each script.

Script	Description
InstallSAV.cmd	Used to install the Server-App V agent and, optionally, the Server App-V PowerShell cmdlets and the Web Deployment tool. **Syntax:** `InstallSAV.cmd [/w] [/c]` **Parameters:** `/w`: Installs the Microsoft Web Deployment tool `/c`: Installs the Server App-V PowerShell cmdlets
InstallSAVSequencer.cmd	Used to install the Server-App V Sequencer application.

Script	Description
	Syntax: `InstallSAVSequencer.cmd` **Parameters:** None
InstallWebDeploy.cmd	Used to install the Microsoft Web Deployment tool. **Syntax:** `InstallWebDeploy.cmd` **Parameters:** None

Deploying Services in VMM

A service in System Center 2012 – Virtual Machine Manager (VMM) can be deployed to a private cloud or to a host group. Before you can deploy a service, you must create a service template. For more information about creating service templates, see Creating Service Templates in VMM.

The following topics provide information to help you deploy a service in VMM:

- How to Deploy a Service in VMM
- How to Configure Deployment Settings for a Service
- How to View and Manage a Deployed Service

For an overview of services, see Creating and Deploying Services Overview.

How to Deploy a Service in VMM

Use the following procedures to deploy a service to a private cloud or to a host group. You can initiate service deployment from the Library workspace, from the Service Template Designer, or from the VMs and Services workspace.

To deploy a service from the Library workspace

1. In the Library workspace, expand the **Templates** node, and then click **Service Templates**.
2. In the **Templates** pane that lists the available service templates, select the service template that you want to use to deploy the service.

   Note

For information about service templates, see Creating Service Templates in VMM.

3. On the **Service Template** tab, in the **Actions** group, click **Configure Deployment**.
4. In the **Select name and destination** dialog box, do the following:
   a. In **Name** box, enter a name for the service instance. For example, enter **Corporate Finance Application**.
   b. In **Destination**, select the host group or private cloud where you want to deploy the service.

   After you have made your selections, click **OK**.
5. VMM performs a placement check to determine the best location on which to deploy the service and then opens the **Deploy Service** window.

   The **Deploy Service** window contains the following areas:

   - In the left pane, the **Service Components** tab lists the tiers of the service and each instance of a tier that will be deployed.
   - In the left pane, the **Settings** tab displays the global settings that will be used during application deployment. The contents of the **Settings** tab varies depending on the scripts that are configured for the service.
   - In the center pane, a deployment map shows the recommended deployment location for each tier and each instance of a tier that will be deployed as part of the service. If you are deploying the service to a host group, the recommended host for each virtual machine to be deployed will be shown. If you are deploying the service to a private cloud, the host information is not shown.
   - In the right pane, the **Minimap** tab allows you to adjust the size of the contents in the deployment map. This is intended to help you navigate the deployment map for a service that is made up multiple tiers.

   Review the deployment configuration settings. For more information about making changes, see How to Configure Deployment Settings for a Service.
6. If the placement process encounters an issue, an icon (error, warning or informational) will appear on the element of the service that needs attention and a message will appear in the details pane. Resolve any errors that are identified in the deployment configuration, and review warnings to resolve any conditions that need attention. You cannot deploy a service until all errors are resolved.
7. To deploy the service, on the **Home** tab, in the **Service** group, click **Deploy Service**. Then, in the **Deploy service** dialog box, click **Deploy** to begin the deployment of the service.

   Note

   If you close the **Deploy Service** window before you deploy the service, you will be prompted whether you want to save your deployment configuration settings for the service. If you click **Save**, you can deploy the service at a later time with

the deployment configuration settings that you have already specified. To deploy the service at a later time, go to the Library workspace, expand the Templates node, and then click **Service Deployment Configurations**. Select the service that you saved, and then click **Configure Deployment**. The **Deploy Service** window will open.

8. You can track the progress of the service deployment in the Jobs window. A **Create service instance** job is created for a service deployment. For information about viewing a service after the service has been deployed, see How to View and Manage a Deployed Service.

Tip
Service deployment is a complex process that can take 15 minutes or longer. You can perform other tasks in the VMM console while you monitor the job.

To deploy a service from the Service Template Designer

1. In the Library workspace, expand the **Templates** node, and then click **Service Templates**.
2. In the **Templates** pane that lists the available service templates, select the service template that you want to use to deploy the service.
3. On the **Service Template** tab, in the **Actions** group, click **Open Designer**.
4. In the Service Template Designer, on the **Home** tab, in the **Service Template** group, click **Configure Deployment**.
5. Follow the steps described above for making selections in the **Select name and destination** dialog box, reviewing the deployment configuration settings, resolving any errors and warnings, and then deploying the service.

To deploy a service from the VMs and Services workspace

1. In the VMs and Services workspace, select the private cloud or host group to which you want to deploy the service.
2. On the **Home** tab, in the **Create** group, click **Create Service**.
3. In the **Create Service** dialog box, ensure **Use an existing service template** is selected, and then click **Browse**.
4. In the **Select Service Template** dialog box, select the service template that you want to use, and then click **OK**.
5. In the **Create Service** dialog box, enter the name for the service in the **Name** box, ensure that the correct location is specified in the **Destination** list, and then click **OK**.
6. VMM performs a placement check to determine the best location on which to deploy the service and then opens the **Deploy Service** window.
7. Follow the steps described above for reviewing the deployment configuration settings, resolving any errors and warnings, and then deploying the service.

How to Configure Deployment Settings for a Service

When you are configuring a service for deployment to a private cloud or to a host group, you can configure settings for the following:

- The service
- The virtual machines being deployed in each tier
- The applications that are being installed

Note
The procedures below assume that you have started the deployment process for a service and that you are working in the **Deploy Service** window. For information about starting the deployment process, see How to Deploy a Service in VMM.

To configure deployment settings for the service

1. On the deployment map, select the service object. The service object contains the name of the service template being used and the release value.
2. The details pane displays the settings that you can configure for the service. The following are some key settings that you can configure:

Setting	Description
Name	The name for the deployed service. This is the name that will appear in the VMs and Services workspace after the service is deployed.
Folder	The host group to which you want to deploy the service. This setting is only displayed if you are deploying the service to a host group.

To save your changes to the deployment settings, click the down arrow in the top left corner of the ribbon, and then click **Save**.

To configure deployment settings for a virtual machine in a tier

1. On the deployment map, select the virtual machine object in a tier.
2. The details pane displays the settings that you can configure for the virtual machine. The following are some key settings that you can configure:

Setting	Description

VM name	The name for the virtual machine. This is the name that will appear in the VMs and Services workspace after the service is deployed. We recommend that you set the value of **VM name** to match the value of **Computer name** to ensure consistent displays when monitoring the health and performance of the virtual machine with Operations Manager.
Computer name	The computer name to use for the guest operating system of the virtual machine. Ensure that this computer name is not already being used in your environment.
Folder	The host group to which you want to deploy the virtual machine. This setting is only displayed if you are deploying the service to a host group.
Host	The host to which you want to deploy the virtual machine. This setting is only displayed if you are deploying the service to a host group.

Tip
The pin icon next to a setting allows you to specify whether the value you enter can be changed when the virtual machine is created and deployed. When the pin is in a horizontal position, the setting will not be changed.

To save your changes to the deployment settings, click the down arrow in the top left corner of the ribbon, and then click **Save**.

To configure deployment settings for an application being installed

- In the left pane, the **Settings** tab displays the service settings that will be used during application deployment. The contents of the **Settings** tab varies depending on the application packages and scripts that are configured for the service.
- For more information about configuring application installations, see How to Create an Application Profile in a Service Deployment.

How to View and Manage a Deployed Service

Use the following procedures to view and manage a deployed service. For information about how to deploy a service, see How to Deploy a Service in VMM.

To view a deployed service

1. In the VMM console, open the VMs and Services workspace.
2. Select the private cloud or host group to which you deployed the service.
3. On the **Home** tab, in the **Show** group, click **Services**.
4. In the Services pane, select the service that you deployed. You can expand the service to show each tier that is deployed and you can expand each tier to show the virtual machines that are deployed as part of that tier. You can also expand each virtual machine to show the applications (and each application's settings) deployed to the virtual machine by VMM.

   The Service pane provides information about the status and configuration of the service; for example:

   - The **VM Status** column provides information about the state of the service, tiers, and virtual machines. For example, the **VM Status** column could show the following:
     - For a virtual machine, **Stopped** if the virtual machine is powered off.
     - For a tier, **Saved Stated** if all virtual machines in the tier are in a saved state.
     - For a service, **Mixed** if the tiers of the service are in different states.
   - The **Template Name** column displays the name of the service template that was used to deploy the service.
   - The **Template Release** column displays the version of the service template that the service is currently using.
   - The **Update Status** column displays **New Release Available** if there is a new version of the service template available with which to update the service.

   For information about updating a deployed service, see Updating a Service in VMM.

To manage a deployed service

1. In the VMM console, open the VMs and Services workspace.
2. Select the private cloud or host group to which you deployed the service.
3. On the **Home** tab, in the **Show** group, click **Services**.
4. In the Services pane, select the service that you want to manage, and then click the **Services** tab on the ribbon.

   The actions that you can perform on the entire service appear on the ribbon. For example, if you want to put all the virtual machines in the service into a saved state, in the **Service** group, click **Save State**. To view the properties of the service, such as which self-service users have access to the service, in the **Properties** group, click

Properties.

If you want to manage a tier in the service, in the Services pane, select the tier. A **Tier** tab appears on the ribbon. For example, if you want to deploy additional virtual machines to the tier, in the **Machine Tier** group, click **Scale Out**. For information about scaling out a tier, see Scaling Out a Service in VMM.

If you want to manage a virtual machine in the service, in the Services pane, expand the appropriate tier, and then select the virtual machine. A **Virtual Machine** tab appears on the ribbon with a list of actions that can be performed on the virtual machine. For example, if you want to connect to the virtual machine, in the **Window** group, click **Connect or View**, and then click **Connect via Console**.

Scaling Out a Service in VMM

After you have deployed a service in VMM and you need to deploy additional virtual machines to a tier of the service, you can use the scale out functionality of VMM. For example, during the holiday shopping season, your website may need additional web servers deployed to handle the increase in traffic to your site.

When you create a tier in a service template, you can specify whether that tier can be scaled out and the minimum and maximum number of virtual machines that you can deploy in the tier. For more information, see How to Configure the Properties of a Service Template.

If you try to scale out a tier beyond its maximum tier size, you will receive a warning, but VMM will not prevent you from scaling out the tier. However, after the virtual machine is deployed, the tier and the service will show a status of **Needs Attention** in the VMs and Services workspace.

To scale out a tier in a service, see the following topic: How to Scale Out a Service in VMM

How to Scale Out a Service in VMM

Use the following procedure to scale out a tier in a service that is deployed in VMM.

To scale out a service

1. In the VMM console, open the VMs and Services workspace.
2. Select the private cloud or host group to which you deployed the service.
3. On the **Home** tab, in the **Show** group, click **Services**.
4. In the Services pane, select the service that you want to scale out.
5. On the **Service** tab, in the **Update** group, click **Scale Out**.
6. In the Scale Out Tier wizard, on the **Select Tier** page, in the **Tier** list, select the tier that you want to scale out, and then click **Next**.

Tip

On the **Select Tier** page, under the **Tier details**, the number of virtual machines currently deployed in the tier and the maximum tier size is displayed.

7. On the **Specify Virtual Machine Identity** page, enter a name for the new virtual machine, and then click **Next**.
8. The next steps in the Scale Out Tier wizard depend on whether the service is deployed to a private cloud or to a host group:

   If the tier is part of a service that is deployed to a private cloud, do the following:

   a. On the **Configure Settings** page, in **Operating System Settings**, enter the computer name to use for the guest operating system of the new virtual machine. Ensure that this computer name is not already being used in your environment.
   b. After you have entered the computer name, click **Next**.

   If the tier is part of a service that is deployed to a host group, do the following:

   a. On the **Select Host** page, select a host on which to deploy the new virtual machine, and then click **Next**.
   b. On the **Configure Settings** page, in **Operating System Settings**, enter the computer name to use for the guest operating system of the new virtual machine. Ensure that this computer name is not already being used in your environment.

      Update any other virtual machine settings as needed, and then click **Next**.

   Tip

   The pin icon next to a setting allows you to specify whether the value you enter can be changed when the virtual machine is created and deployed. When the pin is in a horizontal position, the setting will not be changed.

9. On the **Add Properties** page, specify the actions to perform on the virtual machine when the host on which the virtual machine is deployed starts or stops, and then click **Next**.
10. On the **Summary** page, review your settings, and then click **Scale Out**.

    You can track the progress of the scale out operation in the Jobs window. A **Create virtual machine** job is created for a scale out operation.

    Tip

    Deploying a virtual machine can take 15 minutes or longer. You can perform other tasks in the VMM console while you monitor the job.
11. After the **Create virtual machine** job completes successfully, open the VMs and Services workspace and verify that the new virtual machine was added to the tier of the service. For information about viewing a service and its tiers, see How to View and Manage a Deployed Service.

Updating a Service in VMM

Updating a service is the process of making changes to a deployed service. Because System Center 2012 – Virtual Machine Manager (VMM) keeps track of which service template was used to deploy a service, you can make updates to the service template, and then use that updated service template to make changes to the deployed service.

VMM supports two different methods for making the updates to a deployed service:

- Applying updates to the existing (in-place) virtual machines
- Deploying new virtual machines with the updated settings

Applying updates to the existing virtual machines takes less time. Most configuration changes to virtual machines and application updates can be applied in this manner.

To minimize service interruptions when a tier is updated in-place, you can specify more than one upgrade domain in the tier properties. When the tier is updated, VMM updates the virtual machines in the tier according to the upgrade domain to which they belong. VMM upgrades one upgrade domain at a time, shutting down the virtual machines running within the upgrade domain, updating them, bringing them back online, and then moving on to the next upgrade domain. By shutting down only the virtual machines running within the current upgrade domain, VMM ensures that an upgrade takes place with the least possible impact to the running service. For more information about configuring an upgrade domain, see How to Configure the Properties of a Service Template.

Note

Upgrade domains have no connection to Active Directory domains. You can specify the number of upgrade domains you want to use, and then VMM arbitrarily assigns the virtual machines to an upgrade domain.

Deploying new virtual machines with the updated settings is a more time-consuming process, because you are replacing the existing virtual machines of the service with new virtual machines. Typically, this is how you would deploy operating system updates, such as deploying a service pack for the guest operating system on the virtual machine. If you have applications installed on these virtual machines, and your application has a method for saving and restoring application state, you can use a script in the application profile to save the application state before the existing virtual machines are removed and use a script to restore the application state after the new virtual machines have been deployed. Microsoft Server Application Virtualization (Server App-V) applications automatically support the saving and restoring of application state so no scripts are needed.

To update a deployed service in VMM, see the following topics:

- How to Create an Updated Service Template in VMM
- How to Update a Service Template to Use an Updated Resource in VMM
- How to Apply Updates to a Deployed Service in VMM

How to Create an Updated Service Template in VMM

To update a deployed service in VMM, you must first make a copy of the service template on which the deployed service is based. After you have made a copy of the service template, you will need to provide a new release value for the service template and you will need to make the necessary updates to the service template.

Use the following procedure to copy a service template for the purpose of updating an existing service.

To create an updated service template

1. In the VMM console, open the Library workspace, expand the **Templates** node, and then click **Service Templates**.
2. In the **Templates** pane that lists the available service templates, select the service template that you want to copy.

   Tip
   When you select a service template, the detail pane displays the services that have been deployed using that service template.
3. On the **Service Template** tab, in the **Create** group, click **Copy**.

   A copy of the service template is made and appears in the **Templates** pane. The new service template has the same name as the service template that you copied, but the release value is set to "Copy of <*original release value*>." For example, if the original service template had a release value of **1.0**, the release value of the new service template would be **Copy of 1.0**.
4. In the **Templates** pane, right-click the new service template, and then click **Properties**.
5. In the **Properties** dialog box, on the **General** page, enter a new release value (for example, type **2.0**), and then click **OK**.

At this point, make the necessary updates to the new service template by using the Service Template Designer. For more information about configuring a service template, see Creating Service Templates in VMM.

Note
If you are working in the Service Template Designer and you try to save changes to a service template that is being used as the basis for a deployed service, you will be prompted to save the service template with a new release value.

How to Update a Service Template to Use an Updated Resource in VMM

When a resource is updated in System Center 2012 – Virtual Machine Manager (VMM) and it is referenced by a service template, you must copy and update the service template so that it uses the updated resource.

Use the following procedure to update a service template when one of its dependent resources has been updated.

To update a service template to use an updated resource

1. In the VMM console, open the Library workspace, expand the **Templates** node, and then click **Service Templates**.
2. In the **Templates** pane that lists the available service templates, locate the service template that you want to update.

   Service templates referencing outdated resources display “Outdated” in the **Update Status** column.
3. Confirm the dependent resources that need updating by right-clicking the service template and then selecting **View Updated Resources**.

   Note

   This option is unavailable if dependent resources have not been updated.

   The **View Updated Resources** dialog box opens and displays the most recent version of resources used by this service template.
4. In the **Templates** pane of the Library workspace, right-click the service template that you want to update, and then select **Copy and Update**.

   Note

   This option is unavailable if dependent resources have not been updated.

   A copy of the current service template is created and the outdated resource is replaced with the most recent release from the same family.
5. Publish the updated service template and then apply the updated template to the deployed service. For instructions, see How to Apply Updates to a Deployed Service in VMM.

How to Apply Updates to a Deployed Service in VMM

Use the following procedures to publish an updated service template and then use that updated service template to apply updates to a deployed service.

To publish an updated service template

1. In the VMM console, open the Library workspace, expand the **Templates** node, and then click **Service Templates**.
2. In the **Templates** pane that lists the available service templates, select the service template that you want to publish.
3. On the **Service Template** tab, in the **Actions** group, click **Publish**.

   Note
   If you no longer want to make the service template available, click **Revoke**.
4. Open the VMs and Service workspace and find the service that you want to update with the updated service template. The **Update Status** column for the service should display **New Release Available**.

To apply updates to a deployed service by using an updated service template

1. In the VMs and Service workspace, select the service that you want to update with the updated service template.
2. On the **Service** tab, in the **Update** group, click **Set Template**.
3. In the Change Service Template wizard, on the **Updated Service Template** page, select **Replace the current template with an updated template for this service**.

   Note
   Use the **Modify application settings for this service** option if you only need to change the setting of an application installed in the service. For example, if you need to change the name of the SQL Server database that an application is using.
4. Click **Browse**, select the updated service template, click **OK**, and then click **Next**.
5. On the **Settings** page, configure any application settings that are listed, and then click **Next**.
6. On the **Update Method** page, select whether you want to make the updates in-place to the existing virtual machines or whether you want to deploy new virtual machines with the updated settings, and then click **Next**.

   Note
   For more information about these two update methods, see Updating a Service in VMM.

7. On the **Updates Review** page, review your selections, and then **Next**.

   Note
   If you want the updates to be made immediately, select the **Apply the changes to the service immediately after this wizard completes** check box.
8. On the **Summary** page, review the settings, and then click **Finish**.
9. When you are ready to apply the updates to the deployed service (for example, during a regularly scheduled maintenance windows), in the VMs and Service workspace, select the service that you want to update.
10. On the **Service** tab, in the **Upgrade** group, click **Apply Template**.
11. In the **Apply Service Template** dialog box, review the updates that will be made, and then click **OK**.

    You can track the progress of the service being updated in the Jobs window. A **Perform servicing on a service** job is created.
12. After the update job has completed, in the VMs and Services workspace, verify that the **Template Release** value for the service has been updated.

Exporting and Importing Service Templates in VMM

In VMM, you can export and import service templates. Exporting and importing service templates gives you the capability to back up service templates and share service templates between different VMM environments.

Note
You can also export and import virtual machine templates.

When you export a service template in VMM, tier definitions, hardware settings, guest operating system settings, application installation settings, and network configurations are saved to an .XML file. The export can optionally include sensitive data such as passwords, product keys, and application and global settings that are marked as secure. The sensitive settings can be encrypted. During a service template import, sensitive settings can be included or excluded. If sensitive settings are included, and they were encrypted during the service template export, the encryption password is required.

You can also choose to export some or all of the physical resources (for example, base virtual hard disks, scripts, or application packages) that are associated with the service template along with the .XML file for the exported service template. When you import a service template into VMM, VMM validates physical and logical resources that the service template references in the current environment and allows you to update references to missing resources, such as logical resources include logical networks and virtual hard disks.

You can export a service template to a file share or to a VMM library share. However, by storing the .XML file on a library share, you can ensure that administrators have access to the file for service template imports.

Account requirements In VMM, administrators can export and import all service templates. Self-service users whose user role is assigned the **Author** action can export and import service templates that they have access to, irrespective of the owner. When a self-service user imports a service template, that user becomes the service template owner.

To export and import service templates in VMM, see the following topics:

- How to Export a Service Template in VMM
- How to Import a Service Template in VMM

How to Export a Service Template in VMM

Use the following procedure to export a service template in VMM.

Account requirements Administrators and delegated administrators can export any template in VMM. Self-service users can export templates that they own.

To export a service template

1. In the VMM console, open the Library workspace.
2. In the Library pane, expand the **Templates** node, click **Service Templates**, and then in the **Template** pane, select the service template that you want to export.
3. On the **Service Template** tab, in the **Actions** group, click **Export**.
4. In the **Export Template Resources** dialog box, do the following:
   - To export physical resources associated with the service template (for example, a virtual hard disk or an application package), under the **Physical Resources** column, click **None**. In the **Select Resources** dialog box, select the physical resources that you want to export, and then click **OK**.
   - Select the **Overwrite the existing export files** check box if you want to overwrite an earlier export file for any of the selected templates.
   - Select the **Export any sensitive template settings** checkbox if you want to include sensitive data such as passwords, product keys, and application and global settings that are marked as secure. If you select this option, you can configure encryption for the sensitive settings. If you choose not to include sensitive settings, an administrator can provide the settings during template import or by updating the template after it is imported.
   - To configure encryption for sensitive settings in the template, select the **Encrypt template settings** check box, and then enter an encryption password for the .XML file.

     Important
     To protect sensitive data, if you choose to export sensitive template settings,

we strongly recommend that you use encryption.

- In the **Location** box, use the **Browse** button to select the folder where you want to store the exported service template. The location does not have to be a library share. However, we recommend that you store exported service templates in the library to ensure access for import. If you are a self-service user, you might store the template on the user data path for your self-service user role.

After you make your selections, click **OK**.

5. To verify that the service template export completed successfully, you can do the following:
   - In the Jobs workspace or the Jobs window, verify that the **Export service template** job completed successfully.
   - In **Windows Explorer**, verify that an .XML file with the name of the service template was saved in the folder that you specified.
   - If you stored the exported service template on a library share, you can verify that the .XML file was added to physical library objects in the Library workspace. On the **Library** pane, navigate to the library share where you stored the exported service template. You should see an .XML file with the name of the service template.

How to Import a Service Template in VMM

Use the following procedure to import a service template in VMM.

To import a service template

1. In the VMM console, open the Library workspace.
2. In the Library pane, expand the **Templates** node, and then click **Service Templates**.
3. On the **Home** tab, in the **Import** group, click **Import Template**.
4. In the Import Package wizard, on the **Select Package** page, do the following:
   a. In **Package path**, use the **Browse** button to select the .XML file for the exported service template that you want to import. The .XML file will have the name of the service template
   b. If you want to import sensitive settings such as passwords, product keys, and application and global settings that are marked as secure, select the **Import sensitive template settings** check box. If you do not want to import sensitive data, you can update the references during the template import.
5. After you have made your selections, click **Next**.

   If sensitive data was encrypted when the service template was exported, and you chose to import the sensitive data, a **Password** dialog box opens
6. In the **Password** box, enter the encryption password that was used to encrypt sensitive data when the service template was exported, and then click **OK**.

7. On the **Configure References** page, do the following:
   - In the **Name** box, enter a name for the service template. If you are restoring a service template, keep the same service template name.
   - In **Release** box, provide a release value for the service template. If you are restoring a service template, keep the same release value.
   - Review the list of logical and physical resources that the service template references to identify any missing resources.

     In the resource list, each missing resource has a **Current Mapping** value of **None**. The most common missing resources are logical networks and virtual hard disks.
   - If necessary, update missing logical or physical resources to a resource that is available in the current VMM environment.

     To update a resource, click the pencil icon at the right end of the resource entry to display a list of available resources. After you select a new resource, the **Current Mapping** for the resource displays the selected resource.

     Note
     You can import a template that references missing resources and update the resource references later.

   After you finish updating references, click **Next**.
8. If the name and the release value match those of an existing service template in the current VMM environment, you will be prompted to confirm whether you want to overwrite settings in the existing service template. Click **Yes** to continue, or cancel the operation and then change the service template name or release value.
9. On the **Summary** page, review your selections, and then click **Import**.
10. To verify that the service template was imported successfully, you can do the following:
    - In the Jobs workspace, verify that the **Import template** job completed successfully.
    - In the Library workspace, In the **Library** pane, expand **Templates**, and then click **Service Templates**. The **Templates** pane should display the new service template. The **Status** should be **OK**.

      Note
      If any unavailable resources were not mapped, the template status is **Missing**. To review errors in a service template, open the service template in the Service Template Designer.

Rapid Provisioning of Virtual Machines Using SAN Copy Overview

Rapid provisioning provides a method for deploying new virtual machines to storage arrays without the requirement for copying virtual machines over the network. Virtual Machine Manager (VMM) enables you to take advantage of your storage area network (SAN) infrastructure for cloning virtual machines, and use a VMM template to customize the guest operating system. You can use rapid provisioning to deploy stand-alone virtual machines and virtual machines that are deployed as part of a service.

Rapid provisioning through SAN copy enables you to quickly create virtual machines from a SAN copy-capable template. You can create a SAN copy-capable template from a virtual hard disk that resides on a storage logical unit that supports SAN copy through cloning or snapshots. When you create a new virtual machine by using the SAN copy-capable template, VMM quickly creates a read-write copy of the logical unit that contains the virtual hard disk, and places the virtual machine files on the new logical unit.

When VMM deploys a virtual machine by using rapid provisioning through SAN copy, VMM uses a SAN transfer instead of a network transfer. During a SAN transfer, a SAN copy of the logical unit that contains the virtual machine is created and is assigned to the destination host or host cluster. Because the files for a virtual machine are not actually moved over the network when you transfer a virtual machine over a SAN, it is much faster than a transfer over a standard network.

Caution

Any storage that is accessible by the provisioned computer may be partitioned during the provisioning process even if a specific disk is selected to be used as the operating system disk. In this case data will be lost. To guarantee the use of a specific boot volume, use deep discovery and do not restart the computer before the deployment of the operating system completes.

Methods for rapid provisioning using SAN copy

You can use either of the following methods to create a SAN copy-capable template.

Note

The outlined methods provide a high-level overview of the workflow, and assume that the prerequisites are met. Links to more detailed procedures for each method are provided. The prerequisites are described in Prerequisites for rapid provisioning using SAN copy, later in this topic.

Method 1: Create a SAN copy-capable template from a new virtual machine

1. From a storage pool that is managed by VMM and allocated to the host group where the target host resides, create and assign a storage logical unit to the host.

Note

You can also use your storage array vendor's management tools to create and assign the logical unit.

2. Create a virtual machine with a blank virtual hard disk file on the logical unit.
3. Install and customize the guest operating system and the applications that you want. Generalize the image by using Sysprep.exe with the **/generalize** and the **/oobe** options to generalize the associated virtual hard disk. For more information about Sysprep, see Sysprep Command-Line Options.
4. Use the Create VM Template Wizard to create a SAN-copy capable template from the virtual machine.

   When you create the template, VMM transfers the logical unit that includes the virtual hard disk file from the host to the library through a SAN transfer. The library indexes the virtual hard disk file during the next refresh.

You can then create and deploy new virtual machines by using the SAN copy-capable template. When you deploy a new virtual machine, VMM creates a clone or snapshot of the logical unit that contains the virtual hard disk file, by using a disk that is allocated from the managed storage pool. VMM automatically unmasks the new logical unit to the host.

For detailed steps, see How to Create a SAN Copy-Capable Template from a New Virtual Machine.

Method 2: Create a SAN copy-capable template from an existing virtual machine

1. Create a logical unit from a storage pool that is managed by VMM and allocated to the host group where the library server resides. Assign the logical unit to the library server.

   Note

   If you want to perform this procedure entirely within VMM, you must add the library server as a managed Hyper-V host. This action enables you to assign the logical unit to the library server. If you do not want to make the library server a managed Hyper-V host, you can use your array vendor's management tools to register the logical unit to the library server.
2. On the library server, mount the logical unit to a folder path in the library share.

   Note

   If the storage is managed by VMM, you can mount the logical unit to a folder path in the library share at the same time that you assign the logical unit to the library server.
3. Copy the existing virtual hard disk file (that has been generalized by using Sysprep) to the folder path where you mounted the logical unit.
4. Create a SAN-copy capable template by using the virtual hard disk file.

You can then create and deploy new virtual machines by using the SAN copy-capable template. When you do, VMM creates a clone or snapshot of the logical unit, which automatically creates a

new logical unit from the storage pool. VMM automatically unmasks the new logical unit to the host.

For detailed steps, see How to Create a SAN Copy-Capable Template from an Existing Virtual Machine.

Prerequisites for rapid provisioning using SAN copy

Before you begin, ensure that the following prerequisites are met:

- The storage array must support the new storage management features in VMM.
- The storage array must support cloning or snapshots, and the cloning or snapshots feature must be enabled.

  Note

  This might require additional licensing from your storage vendor.
- The storage pool that you want to use for rapid provisioning must be under VMM management. To meet this requirement, you must add the Storage Management Initiative Specification (SMI-S) provider for the array, discover storage pools, classify the storage, and set the preferred allocation method for the storage array to either snapshot or cloning.
- The storage pool that you want to use for rapid provisioning must be allocated to the host group where you want to use rapid provisioning of virtual machines.
- The Hyper-V hosts that you want to use as placement destinations must be members of the host group. Additionally, the following prerequisites must be met:
  - If you want to create a SAN-copy capable template from a new virtual machine, the host where you create the virtual machine must also be a member of this host group.
  - If you want to create a SAN-copy capable template from an existing virtual machine, and want to create and assign the logical unit from the library server, the library server must be a member of this host group. Therefore, the library server must be a Hyper-V host. (If you do not want to add the library server as a host, you can assign the logical unit out-of-band by using your storage array vendor's management tools.)
- With VMM in System Center 2012 R2, if you want to use rapid provisioning to deploy generation 2 virtual machines, you must choose a host with an operating system that supports these virtual machines. Windows Server 2012 R2 supports generation 2 virtual machines. Previous host operating systems do not support them.

  For more information about generation 2 virtual machines, see Understanding Generation 1 and Generation 2 Virtual Machines in VMM.
- All Hyper-V hosts that you want to use for rapid provisioning and the library server must have access to the storage array. Also, they must use the same type of SAN connectivity. For SAN migrations to succeed, you cannot have some hosts that connect to the array through Fibre Channel and others that connect through iSCSI. Configuration varies, depending on your storage hardware.

  Note

For specific configuration information, see your storage array vendor's documentation.

Configuration typically includes the following:

- The Multipath I/O (MPIO) feature must be added on each host that will access the Fibre Channel or iSCSI storage array. You can add the MPIO feature through Server Manager. If the MPIO feature is already enabled before you add a host to VMM management, VMM will automatically enable MPIO for supported storage arrays by using the Microsoft provided Device Specific Module (DSM). If you already installed vendor-specific DSMs for supported storage arrays, and then add the host to VMM management, the vendor-specific MPIO settings will be used to communicate with those arrays.

  If you add a host to VMM before you add the MPIO feature, you must manually configure MPIO to add the discovered device hardware IDs. Or, you can install vendor-specific DSMs.

  Note
  For more information, including information about how to install MPIO, see Support for Multipath I/O (MPIO).
- If you are using a Fibre Channel storage area network (SAN), each host that will access the storage array must have a host bus adapter (HBA) installed. Additionally, ensure that the hosts are zoned accordingly so that they can access the storage array.
- If you use an iSCSI SAN, ensure that iSCSI portals have been added and that the iSCSI initiator is logged into the array. Additionally, ensure that the Microsoft iSCSI Initiator Service on each host is started and set to **Automatic**. For information about how to create an iSCSI session on a host through VMM, see How to Configure Storage on a Hyper-V Host.

For information about supported storage arrays, how to bring storage under VMM management, how to configure the preferred capacity allocation method for a managed storage array, and how to allocate storage to a host group, see Configuring Storage Overview.

In This Section

Use the following steps to deploy a virtual machine by using rapid provisioning.

Task	Description
Step 1: Use either of the following instructions: • How to Create a SAN Copy-Capable Template from a New Virtual Machine • How to Create a SAN Copy-Capable Template from an Existing Virtual Machine	Describes how to create a SAN copy-capable template from either a new or existing virtual machine. Includes scenario-specific prerequisites.
Step 2: How to Deploy a New Virtual Machine from the SAN Copy-Capable Template	Describes how to create and deploy the new virtual machine by using the SAN copy-capable template.

How to Create a SAN Copy-Capable Template from a New Virtual Machine

You can use the procedures in this topic to create a SAN copy-capable template from a new virtual machine in Virtual Machine Manager (VMM). In these procedures, you create a new virtual machine on a logical unit that is assigned to a Hyper-V host, and then create a SAN-copy capable template from the virtual machine on the library server. When you create the template, the logical unit is automatically unregistered from the host and registered to the library server.

Prerequisites

Before you begin these procedures, make sure that the following prerequisites are met:

- Your configuration must meet all the prerequisites that are defined in the “Rapid Provisioning by Using SAN Copy Prerequisites” section of the Rapid Provisioning of Virtual Machines Using SAN Copy Overview topic. Note that the library server does not have to be a managed Hyper-V host. However, it must have access to the storage pool where the logical unit that you use for rapid provisioning resides.
- You must create a logical unit from the managed storage pool that you want to use for rapid provisioning, and assign it to the host where you want to create the new virtual machine. You must also format the logical unit with NTFS, and assign a drive letter. You can use any of the following methods:
  - Create and assign the logical unit through the VMM console from the Storage tab in the managed Hyper-V host’s properties. When you assign the logical unit, you can format and assign a drive letter to the logical unit at the same time. For information about how to create and assign a logical unit to a host through VMM, see How to Configure Storage on a Hyper-V Host.
  - Create a logical unit from the Storage node in the Fabric workspace. Then, allocate the logical unit to a host group, and assign the logical unit to the host from the managed Hyper-V host. When you assign the logical unit, you can format and assign a drive letter to the logical unit at the same time. For information about how to create a logical unit from the Storage node, see How to Create Logical Units Through VMM.
  - Use your storage array vendor’s management tools to create and assign the logical unit. You can use Disk Management (Diskmgmt.msc) to format the logical unit and assign a drive letter after the logical unit is assigned to the host.

  Note
  In the example scenario, drive L: is used to represent the drive letter that is assigned to the logical unit.
- The logical unit that you want to use for the new virtual machine must be empty.

To create a SAN copy-capable virtual hard disk on a host

1. Open the **VMs and Services** workspace.
2. On the **Home** tab, in the **Create** group, click the **Create Virtual Machine** drop-down arrow, and then click **Create Virtual Machine**.

   The Create Virtual Machine Wizard opens.
3. On the **Select Source** page, click **Create the new virtual machine with a blank virtual hard disk**, and then click **Next**.
4. Specify identity options as follows, and then click **Next**:
   - With VMM in System Center 2012 SP1 or System Center 2012, on the **Specify Virtual Machine Identity** page, enter the virtual machine name and optional description. For example, enter the name **Rapid Provision Base VM (WS08R2Ent)**.
   - With VMM in System Center 2012 R2, on the **Identity** page, enter the virtual machine name—for example, the name **Rapid Provision Base VM WS12**—and an optional description. In the **Generation** box, select **Generation 1** or **Generation 2**. (For more information, see Understanding Generation 1 and Generation 2 Virtual Machines in VMM.)
5. On the **Configure Hardware** page, configure the desired hardware settings for the virtual machine, and then click **Next**.

   Note
   Make sure that the **Create a new virtual hard disk** option is selected.
6. On the **Select Destination** page, accept the default setting of **Place the virtual machine on a host**, and then click **Next**.
7. On the **Select Host** page, select the host where you assigned the logical unit that you want to use for rapid provisioning, and then click **Next**.
8. On the **Configure Settings** page, do the following:
   a. Under **Locations**, click **Virtual Machine Location**. In the results pane, under the **Virtual machine path** box, click **Browse**. In the **Select Destination Folder** dialog box, click the drive that you created from the assigned logical unit, and then click **OK**.

      Note
      In the **Select Destination Folder** dialog box, verify that the text **SAN (Migration Capable)** appears next to the drive information.

      For example, click drive **(L:\) [9.92 GB free of 10.00 GB, SAN (Migration Capable)]**.

   b. Under **Machine Resources**, click **Virtual Hard Disk**. In the results pane, next to the **Destination path** box, click **Browse**. In the **Select Destination Folder** dialog box, click the same drive that you selected in step 8a (the drive that you created from the assigned logical unit), and then click **OK**.

      For example, click drive **L:**.

   c. Click **Next** to continue.
9. On the **Select Networks** page, select the desired logical network, virtual network, and

VLAN setting.

10. On the **Add Properties** page, configure the desired settings, and then click **Next**.
11. On the **Summary** page, review the settings, and then click **Create**.

    Open the **Jobs** workspace to view the job status. Verify that the job has a status of **Completed w/ Info**, and then close the dialog box.
12. In the **VMs and Services** workspace, under **All Hosts**, click the host where you placed the virtual machine. In the **VMs** pane, verify that the new virtual machine is listed.
13. On the new virtual machine, install and customize the guest operating system and any desired applications. Generalize the image by running Sysprep.exe.

    Note

    When you are finished, make sure that there are no .iso image files attached to the virtual DVD drive.

To create a SAN copy-capable template

1. Open the **Library** workspace.
2. On the **Home** tab, in the **Create** group, click **Create VM Template**.

   The Create VM Template Wizard opens.
3. On the **Select Source** page, click **From an existing virtual machine that is deployed on a host**, click **Browse**, click the virtual machine on the host that resides on the logical unit, and then click **OK**.

   For example, click a virtual machine name such as **Rapid Provision Base VM (WS08R2Ent)** or **Rapid Provision Base VM WS12**, and then click **OK**.
4. On the **Select Source** page, click **Next**.
5. Review the warning message, and then click **Yes** to continue.
6. On the **VM Template Identity** page, enter a name for the template in the **VM Template name** box, enter an optional description, and then click **Next**.

   For example, enter a name such as **Rapid Provision Template (WS08R2Ent)** or **Rapid Provision Template WS12**, and then click **Next**.
7. On the **Configure Hardware** page, click **Next**.

   Note

   Notice that a storage classification appears in the **Classification** list for the virtual hard disk. The classification matches what you assigned to the storage pool from which you created the logical unit.
8. On the **Configure Operating System** page, click **Next**.
9. On the **Select Library Server** page, click the library server where you want to create the template. Verify that the **Transfer Type** column for the selected library server indicates **SAN**, and then click **Next**.

   Important

The library server must have access to the same storage pool as the host.

10. On the **Select Path** page, next to the **Virtual machine path** box, click **Browse**. In the **Select Destination Folder** dialog box, select a location on the library server to store the virtual machine files, click **OK**, and then click **Next**.
11. On the **Summary** page, click **Create**.

    Open the **Jobs** workspace to view the job status. Verify that the job has a status of **Completed**.
12. To verify that the template was created, in the **Library** workspace, in the **Library** pane, expand **Templates**, and then click **VM Templates**.

    In the **Templates** pane, verify that the new template is listed, with a status of **OK**.

    Tip
    To add the SAN Copy Capable column to the Templates pane, right-click the column header, and then click **SAN Copy Capable**.

See Also

Rapid Provisioning of Virtual Machines Using SAN Copy Overview

How to Deploy a New Virtual Machine from the SAN Copy-Capable Template

How to Create a SAN Copy-Capable Template from an Existing Virtual Machine

You can use the procedures in this topic to create a SAN copy-capable template from an existing virtual machine in Virtual Machine Manager (VMM). In these procedures, you create and assign a logical unit to the library server, mount the logical unit to a folder in the library share, copy an existing virtual hard disk to the folder in the library share, and then create a SAN-copy capable template by using the virtual hard disk file as the template source.

Prerequisites

Before you begin these procedures, make sure that the following prerequisites are met:

- Your configuration must meet all the prerequisites that are defined in the “Rapid Provisioning by Using SAN Copy Prerequisites” section of the Rapid Provisioning of Virtual Machines Using SAN Copy Overview topic.
- If you want to perform this procedure entirely within VMM, you must add the library server as a managed Hyper-V host. This enables you to assign the logical unit to the library server through VMM. If you do not want to make the library a managed Hyper-V host, you can use your array vendor’s management tools to assign the logical unit to the library server.
- You must have an existing virtual hard disk (that was generalized by using Sysprep) that you want to use as a base image for rapid provisioning.

- Create a folder in the library share that you will use to mount the logical unit to, and to store the virtual hard disk.

  For example, create a folder in the **SEALibrary** library share that is named **Rapid Provision VHD**.

To create a SAN-copy capable virtual hard disk

1. Create a logical unit from a storage pool that is managed by VMM, assign it to the library server, format the logical unit, and mount the logical unit to the folder path that you created in the Prerequisites section of this topic.

   If the library server is a managed Hyper-V host, you can create and assign the logical unit from the library server. You can also format the disk with NTFS and mount the logical unit to the folder path in the library share at the same time. For information about how to create and assign a logical unit to a host through VMM, see the topic “How to Configure Storage on a Hyper-V Host” in Adding and Managing Hyper-V Hosts and Host Clusters in VMM.

   Important
   When you create the logical unit, choose the option **Mount in the following empty NTFS folder**, click **Browse**, and then click the folder that you created in the Prerequisites section. Do not assign a drive letter. Also, do not ever create multiple mount points to the folder.

   If the library server is not a managed Hyper-V host, use your array vendor’s management tools to create the logical unit, and to unmask the logical unit to the library server. Then, mount the logical unit to the folder path in the library share that you created in the Prerequisites section of this topic. To do this, follow these steps:

   a. Open Disk Management. To do this, click **Start**, type **diskmgmt.msc** in the search box, and then press ENTER.

   b. Rescan the disks, initialize the disk, and then format the disk. To rescan the disks, on the **Action** menu, click **Rescan Disks**. To initialize the disk, right-click the disk, and then click **Initialize Disk**.

      Important
      Do not assign a drive letter to the disk.

   c. Mount the partition using a folder path in the library share. To do this, right-click the disk, and then click **Change Drive Letter and Paths**. Click **Add**, and then click **Mount in the following empty NTFS folder**. Click **Browse**, locate and then click the empty library folder that you created in the Prerequisites section of this topic, and then click **OK**.

      Important
      Do not ever create multiple mount points to the folder.

      For example, mount the partition to the **Rapid Provision VHD** folder that you created in the SEALibrary library share.

d. Close Disk Management.

2. Copy the virtual hard disk that you want to use to the new folder in the library share.

   Important
   The logical unit that you use must not contain any data. The virtual hard disk that you copy to the logical unit in this procedure must be the only file on the logical unit.

3. In the VMM console, open the **Library** workspace, and then refresh the library share.

   The new folder that you created appears in the library share. To verify that the virtual hard disk is SAN copy-capable, click the new folder, and then in the **Physical Library Objects** pane, click the virtual hard disk file. In the details pane for the virtual hard disk file, make sure that the **SAN copy capable** field indicates a value of **Yes**.

To create a SAN copy-capable template

1. Open the **Library** workspace.
2. In the **Library** pane, expand **Library Servers**, expand the library share where you mounted the folder, and then click the SAN copy capable virtual hard disk that you created in the previous procedure.
3. On the **Home** tab, in the **Create** group, click **Create VM Template**.

   The Create VM Template Wizard opens.

4. On the **VM Template Identity** page, in the **VM Template name** box, enter a name for the template and an optional description, and then click **Next**.

   For example, enter the name **WS08R2 Rapid Provision**.

5. Complete the rest of the New VM Template Wizard. Note the following:
   - On the **Configure Hardware** page, specify the storage classification. Make sure that the field is empty, or that you select the classification that was assigned to the logical unit that you created. (To do this, under **Bus Configuration**, click the virtual hard disk. In the **Classification** list, specify the storage classification.)
   - Realize that if you plan to use the template for the rapid-provisioning of stand-alone virtual machines, any settings that you enter in the **Configure Applications** and the **Configure SQL Server** pages of the wizard are ignored. These settings are only used for virtual machines that are deployed as part of a service.

   After you complete the wizard, open the **Jobs** workspace to view the job status. Verify that the job to create the template has a status of **Completed**,.

6. To verify that the template was created, in the **Library** workspace, in the **Library** pane, expand **Templates**, and then click **VM Templates**.

   In the **Templates** pane, verify that the new template is listed.

   Tip
   To add the SAN Copy Capable column to the Templates pane, right-click the column header, and then click **SAN Copy Capable**.

See Also

Rapid Provisioning of Virtual Machines Using SAN Copy Overview

How to Deploy a New Virtual Machine from the SAN Copy-Capable Template

How to Deploy a New Virtual Machine from the SAN Copy-Capable Template

You can use this procedure to deploy a virtual machine from a SAN copy-capable template that you created for rapid provisioning in Virtual Machine Manager (VMM). You can use the SAN copy-capable template to deploy stand-alone virtual machines, and to deploy virtual machines as part of a service. This procedure shows how to deploy a new stand-alone virtual machine by using rapid provisioning. If you want to use the template during service creation, you can select an existing SAN clone-capable virtual machine template when you create a service.

Important

The hosts where you want to place the virtual machines must have access to the managed storage pool where the logical unit that is associated with the template resides. If you want to deploy the virtual machines to a private cloud, the storage classification that is assigned to the logical unit that was used to create the SAN clone-capable template must be available to the private cloud. Additionally, the host groups that are used to provide resources for the private cloud must contain the hosts that have access to the managed storage pool where the logical unit that is associated with the template resides.

To deploy a virtual machine through rapid provisioning

1. Open the **VMs and Services** workspace.
2. On the **Home** tab, in the **Create** group, click the **Create Virtual Machine** drop-down arrow, and then click **Create Virtual Machine**.

   The Create Virtual Machine Wizard opens.
3. On the **Select Source** page, make sure that **Use an existing virtual machine, VM template or virtual hard disk** is selected, and then click **Browse**.
4. In the **Select Virtual Machine Source** dialog box, under **Type: VM Template**, click the template that you created for rapid provisioning, and then click **OK**.

   Important

   Make sure that there is a value of **Yes** for the template in the **SAN Copy Capable** column.
5. On the **Select Source** page, click **Next**.
6. Complete the rest of the steps in the New Virtual Machine wizard to create and deploy the virtual machine. Note the following:

- On the **Configure Hardware** page, under **Bus Configuration**, leave the **Classification** list empty, or select the storage classification that matches the classification of the logical unit where the SAN copy capable virtual hard disk resides.
- On the **Select Host** page or the **Select Cloud** page, make sure that the **Transfer Type** column for the host or private cloud that you select indicates **SAN**.
- If you selected to place the virtual machine on a host, on the **Configure Settings** page, under **Machine Resources**, click the virtual hard disk to verify the deployment options. For rapid provisioning through SAN copy, make sure that the value in the **Method to deploy the virtual hard disk to the host** list is **Transfer the virtual disk by using the SAN**.

7. After you complete the wizard, open the **Jobs** workspace to view the job status. To view job details, click the **Create virtual machine** job.

   When you create a virtual machine from the SAN copy-capable template, a new logical unit is automatically provisioned from the same storage pool where the virtual hard disk that was used to create the SAN copy-capable template from resides. The logical unit is automatically registered and mounted on the target host.
8. To verify that the virtual machine was created, open the **VMs and Services** workspace. Expand **All Hosts** or **Clouds**, depending on where you deployed the virtual machine, and then locate and click the destination host or private cloud. In the **VMs** pane, verify that the new virtual machine appears. If you open Disk Management (Diskmgmt.msc) on the destination host, you can see the new disk that is assigned and registered to the host.

Migrating Virtual Machines and Storage Overview

Virtual Machine Manager (VMM) supports the following types of migration:

- **Network migration**—This is the slowest type of migration and performs a network copy of the virtual machine data using BITS. The amount of downtime is in direct proportion to the size of the data transfer.
- **Quick migration**—This type of migration is also known as cluster transfer, and can be used to migrate a highly available virtual machine. It leverages Windows Failover Cluster to migrate virtual machines between cluster nodes. The running state of the virtual machine is saved to disk (the virtual machine is hibernated), the disk is failed over to the other cluster node, and then the saved state is loaded to wake up the virtual machine. Downtime is minimal because quick migration takes a snapshot of the virtual machine and transfers data without requiring the virtual machine to be turned off.
- **Quick storage migration**—Quick storage migration allows you to move virtual machine storage from one location to another. For example, you can move the storage for a virtual machine from a Fibre Channel SAN to an iSCSI SAN. The virtual disks of a running virtual machine can be migrated independent of storage protocols (SCSI, Fibre Channel) or storage types (local, DAS, SAN). Downtime is minimal because quick storage migration takes a

snapshot of the virtual machine and transfers data without requiring the virtual machine to be turned off.

- **SAN migration**—This type of migration uses SAN transfer to migrate virtual machines, and highly available virtual machines, into and out of a cluster. It can be used when both the source and destination hosts have access to the same storage infrastructure (LUN), and the storage can be transferred from one host to another. For SAN migration, the files for a virtual machine are not copied from one server to another and thus downtime is minimized. SAN migration can be used to copy a virtual machine from one host to another, or copying a virtual machine to or from the library. Note the following:
    a. When you migrate a virtual machine into a cluster by using a SAN transfer, VMM checks that each node in the cluster can see the LUN, and automatically creates a cluster disk resource for the LUN.
    b. To migrate a virtual machine out of a cluster, the virtual machine must be on a dedicated LUN that is not using CSV.
    c. The following SAN infrastructures are supported for migration: Fiber Channel; iSCSI SANs; N_Port ID Virtualization (NPID).
- **Live migration**—This type of migration moves a virtual machine running as part of a failover cluster from one cluster to another with no noticeable downtime for users or network applications.

VMM automatically selects the type of transfer that will be used for migration. When you perform a migration in the VMM console using the Migrate VM Wizard, the migration type that will be used is displayed in the Transfer Type column.

Live migration new features

As of System Center 2012 SP1, VMM provides a number of additional live migration features, based on new migration capabilities in Windows Server 2012. These features include:

- Live migration outside a cluster—In addition to performing live migration within a cluster, you can perform live migration between two standalone computers that are not cluster nodes.
- Live migration between nodes in two different clusters— You can migrate between nodes within a cluster, or between nodes in different clusters.
- Live migration of virtual machine storage —You can migrate storage in order to update the physical storage that is available in Hyper-V, or to mitigate bottlenecks in storage performance. Storage can be added to either a stand-alone computer or to a Hyper-V cluster, and then virtual machines can be moved to the new storage while they continue to run.
- Live VSM—By using live system migration (live VSM), you can migrate virtual machines and their storage together in a single action.
- Concurrent live migration— You can perform multiple concurrent live migrations of virtual machines and storage. The concurrent limit can be configured manually. Any concurrent live migrations in excess of the limit will be queued.

VMM inspects and validates the configuration settings of a destination host before migration from a source host begins.

Business benefits

The new live migration features provide a number of business benefits:

- **Increased flexibility**—The new features can help to simplify the movement of virtual machines across hosts and clusters. Therefore, it becomes easier to manage a dynamic datacenter.
- **Ease-of-maintenance**—Live migration alleviates the need to take standalone hosts and cluster hosts offline for maintenance and migration purposes, which helps to avoid downtime. With the ability to perform concurrent migrations and maintenance, migration timeframes can become shorter, depending on the time that is required to perform the live migration. In addition, the planning process for Hyper-V mobility is simplified.
- **Better hardware utilization**—The distribution of virtual machines can be optimized across the infrastructure. Virtual machines and storage can be moved to stand-alone servers and clusters with spare capacity, without interrupting availability. Power consumption is reduced as virtual machines can be moved across hosts, and then hosts can be powered down to save energy.
- **Windows Server 2012 features**—As of System Center 2012 SP1, VMM takes advantage of the new failover clustering features that are available in the Windows Server 2012 release. These features include: new APIs to migrate virtual machines across cluster nodes, and improved attach/detach functionality that enables migration of virtual machines in and out of failover clusters without downtime.

Virtual machine live migration support

The following table summarizes the support matrix for live migration of virtual machines as of System Center 2012 SP1.

Source	**Destination**	
	Destination: Stand-alone	**Destination: Cluster node**
Source: Stand-alone	Supported	Supported
Source: Cluster node	Supported	Supported. Source and destination can be in the same cluster or in different clusters.

Live storage migration

With virtual machine storage migration you can move storage from one location to another without interrupting the workload of the virtual machine, if it is running. You can also use storage migration to move, service, or upgrade storage resources, or for migration of a standalone or

cluster virtual machine. The following table summarizes the support matrix for storage migration as of System Center 2012 SP1.

Source	Destination		
	Destination: Local disk (stand-alone)	**Destination: SMB 3.0 share (standalone or cluster)**	**Destination: CSV (cluster)**
Source: Local disk (stand-alone)	Supported	Supported. The virtual machine will be promoted to high availability.	Not supported.
Source: SMB 3.0 share	Supported. In a cluster configuration the virtual machine will be demoted, and will no longer be highly available after migration to the local disk.	Supported	Supported
Source: CSV (cluster)	In a cluster configuration the virtual machine will be demoted, and will no longer be highly available after migration to the local disk.	Supported. The SMB share must be available from the destination cluster node.	Supported. CSV must be available from the destination cluster node.

Live migration limitations

Note the following requirements and limitations when performing a live migration of virtual machines and storage:

- Live migration requires two or more servers that run Hyper-V, that support hardware virtualization, and use processors from the same manufacturer, such as all AMD processors or all Intel processors, for example.
- Live migration is supported for hosts that run Windows Server 2012. There is no backward compatibility to support migration between hosts that run Windows Server 2008 R2 and Windows Server 2012.

- Virtual machines must be configured to use virtual hard disks or virtual Fibre Channel disks, not physical disks.
- For live migration network traffic you should use a private network.
- Source and destination servers must belong to the same Active Directory domain, or to different trusted domains.
- If the source or destination virtual machine VHD has a base disk, the base disk must be in a share that is accessible (registered) from the destination host. Generally, live migration does not move the base disk.
- Migration between clusters is only supported on hosts that run versions of the Windows Server 2012 operating system that support the Windows Failover Cluster Service. Windows Failover Clustering and Cluster Shared Volume (CSV) storage should be enabled in the cluster.
- Live migration of a virtual machine does not migrate virtual machine storage, specifically meaning the location that stores the virtual machine images (VHD, ISO, VFD files). To handle storage requirements, you can use one of the following options:
    - Configure the virtual machine so that the storage files are available on a file share that is accessible by both the source and destination host of the migration.
    - Run a combined live virtual machine and storage migration (live VSM) in a single action.
    - Run a separate storage migration.
- If the source and destination hosts use shared storage, note the following:
    - All files that comprise a virtual machine, such as virtual hard disks, snapshots, and configuration, should be stored on an SMB share.
    - Permissions on the SMB share should be configured to grant access to the computer accounts of all servers that run Hyper-V.
- A storage migration moves virtual machine images (VHD, ISO, and VFD files), snapshot configurations, and data (saved state files).
- Storage migration is per virtual machine.
- Storage migration does not move base (parent) disks, with the exception of snapshot disks.

Live virtual machine and storage migration (live VSM)

You can perform a live VSM to migrate both a virtual machine, and the virtual machine storage in a single action.

- To use live VSM, the virtual machine LUN must be masked from the destination host.
- Live VSM is supported between two stand-alone hosts that run Hyper-V on Windows Server 2012. The transfer can occur between local disks or SMB 3.0 file shares.
- Live VSM is supported between two Hyper-V host clusters that run on Windows Server 2012. The virtual machine can be transferred to either a CSV or SMB 3.0 file share on the destination host cluster.

Configuring Virtual Machine Settings in VMM

The following topics provide information to help you configure virtual machine settings that were first introduced in Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1):

- Configuring Availability Options for Virtual Machines Overview
- Configuring Resource Throttling for VMM
- Deploying Virtual NUMA for VMM

Configuring Availability Options for Virtual Machines Overview

In System Center 2012 Service Pack 1 (SP1) or System Center 2012 R2, you can use Virtual Machine Manager (VMM) to configure availability options for virtual machines that are deployed on Hyper-V host clusters. By using VMM, you can configure the following availability options:

- **Virtual machine priority**: Based on these settings, the host cluster starts or places high-priority virtual machines before medium-priority or low-priority virtual machines. This ensures that the high-priority virtual machines are allocated memory and other resources first, for better performance. Also, after a node failure, if the high-priority virtual machines do not have the necessary memory and other resources to start, the lower priority virtual machines will be taken offline to free up resources for the high-priority virtual machines. Virtual machines that are preempted are restarted later in priority order.
- **Preferred and possible owners of virtual machines**: These settings influence the placement of virtual machines on the nodes of the host cluster. By default, there are no preferred owners (there is no preference), and the possible owners include all server nodes on the cluster.
- **Availability sets**: When you place multiple virtual machines in an availability set, VMM will attempt to keep those virtual machines on separate hosts and avoid placing them together on the same host whenever possible. This helps to improve continuity of service. Another way to configure this setting is to use Windows PowerShell commands for failover clustering. In this context, the setting appears in the Get-ClusterGroup listing and is called **AntiAffinityClassNames**.

The following topics describe how to configure availability options for virtual machines that are being managed with VMM in System Center 2012 SP1 or System Center 2012 R2:

- How to Configure Priority in VMM for a Virtual Machine on a Host Cluster
- How to Configure Preferred and Possible Owners for a Virtual Machine on a Host Cluster
- How to Configure Availability Sets in VMM for Virtual Machines on a Host Cluster

See Also

Creating a Hyper-V Host Cluster in VMM Overview

How to Configure Priority in VMM for a Virtual Machine on a Host Cluster

With System Center 2012 Service Pack 1 (SP1) or System Center 2012 R2, if you deploy or are planning to deploy virtual machines on a host cluster, you can use Virtual Machine Manager (VMM) to configure priority settings for the virtual machines. With these settings, the cluster starts or places high-priority virtual machines before medium-priority or low-priority virtual machines. This ensures that the high-priority virtual machines are allocated memory and other resources first, for better performance. Also, after a node failure, if the high-priority virtual machines do not have the necessary memory and other resources to start, the lower priority virtual machines will be taken offline to free up the necessary resources for the high-priority machines. Virtual machines that are preempted are later restarted in priority order.

You can also configure the virtual machine priority setting in a virtual machine template, so that any virtual machines that are created with that template will have the specified virtual machine priority. For virtual machines that have been deployed on a host cluster, you can also configure these settings by using Failover Cluster Manager.

For information about other settings related to availability of virtual machines on a host cluster, see Configuring Availability Options for Virtual Machines Overview.

Account requirements To complete this procedure you must be a member of the Administrator or Delegated Administrator user role, or a self-service user who has the **Deploy** action in the scope of your user role.

To configure priority for a virtual machine on a host cluster or in a virtual machine template designed for deployment on a host cluster

1. Configure a virtual machine or virtual machine template by using one of the following options:
   a. To configure a deployed virtual machine, in the **VMs and Services** workspace, navigate to the host on which the virtual machine is deployed. In the results pane, right-click the virtual machine, and then click **Properties**.
   b. To configure a stored virtual machine, in the **Library** workspace, navigate to the library server on which the virtual machine is stored. In the results pane, right-click the virtual machine, and then click **Properties**.
   c. To configure a virtual machine while you are creating it, follow an appropriate procedure under Configuring Virtual Machine Settings in VMM to open the **Create Virtual Machine Wizard** and to proceed to the **Configure Hardware** page.
   d. To configure a virtual machine template, in the **Library** workspace, under **Templates**, click **VM Templates**. In the results pane, right-click the virtual machine template, and then click **Properties**.
2. On the **Hardware Configuration** tab or (for the wizard) the **Configure Hardware** page, scroll down to **Advanced** and under it, click **Availability**.
3. Confirm that **Make this virtual machine highly available** is checked. (On a deployed

virtual machine, this setting cannot be changed, because it depends on whether the virtual machine is deployed on a host cluster.)

4. Under **Virtual machine priority**, select a priority of **High**, **Medium**, or **Low** for the virtual machine. If you want the virtual machine to always require a manual start and never pre-empt other virtual machines, select **Do not restart automatically**.
5. Click **OK** or complete the wizard.
6. To verify the setting, reopen the properties sheet.

See Also

How to Create and Deploy a Virtual Machine from a Blank Virtual Hard Disk

How to Create and Deploy a Virtual Machine from an Existing Virtual Hard Disk

How to Create a Virtual Machine Template

How to Create and Deploy a Virtual Machine from a Template

Configuring Availability Options for Virtual Machines Overview

How to Configure Availability Sets in VMM for Virtual Machines on a Host Cluster

With System Center 2012 Service Pack 1 (SP1) or System Center 2012 R2, if you deploy virtual machines on a host cluster, you can use Virtual Machine Manager (VMM) to configure availability sets for the virtual machines. When you place virtual machines in an availability set, VMM will attempt to keep those virtual machines on separate hosts and avoid placing them together on the same host whenever possible. This helps to improve continuity of service.

You can also configure availability sets in a service template, to specify how virtual machines that are created with that template should be placed on hosts. For more information, see How to Configure the Properties of a Service Template.

For virtual machines that have been deployed on a host cluster, another way to configure this setting is to use Windows PowerShell commands for failover clustering. In this context, the setting appears in the Get-ClusterGroup listing and is called **AntiAffinityClassNames**.

For information about other settings related to availability of virtual machines on a host cluster, see Configuring Availability Options for Virtual Machines Overview.

Account requirements To complete this procedure you must be a member of the Administrator or Delegated Administrator user role, or a self-service user who has the **Deploy** action in the scope of your user role.

To configure availability sets for a virtual machine on a host cluster

1. Open the properties sheet of the virtual machine by using one of the following actions:
   a. To configure a deployed virtual machine, in the **VMs and Services** workspace,

navigate to the host on which the virtual machine is deployed. In the results pane, right-click the virtual machine, and then click **Properties**.

b. To configure a stored virtual machine, in the **Library** workspace, navigate to the library server on which the virtual machine is stored. In the results pane, right-click the virtual machine, and then click **Properties**.

2. On the **Hardware Configuration** tab, scroll down to **Advanced** and under it, click **Availability**.
3. Confirm that **Make this virtual machine highly available** has the intended setting. (On a deployed virtual machine, the setting cannot be changed, because it depends on whether the virtual machine is deployed on a host cluster.)
4. Under **Availability sets**, click **Manage availability sets**.
5. Click the name of an availability set, and use the controls to add or remove the set. Repeat this action until all of the intended availability sets appear in the **Assigned properties** list. To create a new availability set, click the **Create** button, provide a name for the set, and then click **OK**.
6. In the **Manage Availability Sets** dialog box, click **OK**.
7. In the properties sheet, click **OK**.
8. To verify the setting for a deployed virtual machine, in the listing for the virtual machine, view the name under **Availability Set Name**.

See Also

Creating and Deploying Virtual Machines Overview

Configuring Availability Options for Virtual Machines Overview

How to Configure Preferred and Possible Owners for a Virtual Machine on a Host Cluster

In System Center 2012 Service Pack 1 (SP1) or System Center 2012 R2, if you deploy virtual machines on a host cluster, you can use Virtual Machine Manager (VMM) to configure preferred owners and possible owners for the virtual machines. By default, there are no preferred owners (there is no preference), and the possible owners include all nodes (servers) in the host cluster.

For information about other settings related to availability of virtual machines on a host cluster, see Configuring Availability Options for Virtual Machines Overview.

Account requirements To complete this procedure you must be a member of the Administrator or Delegated Administrator user role, or a self-service user who has the **Deploy** action in the scope of their user role.

To configure preferred and possible owners for a virtual machine

1. In the **VMs and Services** workspace, navigate to the host on which the virtual machine is deployed. In the results pane, right-click the virtual machine, and then click **Properties**.
2. Click the **Settings** tab and configure the options:
   - To control which nodes (servers) in the cluster will own the virtual machine most of the time, configure the preferred owners list.
   - To prevent a virtual machine from being owned by a particular node, configure the possible owners list, omitting only the nodes that should never own the virtual machine.
3. In the properties sheet, click **OK**.
4. To verify the settings, reopen the properties sheet.

See Also

Creating and Deploying Virtual Machines Overview

Configuring Availability Options for Virtual Machines Overview

Configuring Resource Throttling for VMM

System Center 2012 – Virtual Machine Manager (VMM) provided some rudimentary resource throttling features. VMM in System Center 2012 SP1 enhances these features with processor (CPU) and memory throttling capabilities. These additional features can help administrators and cloud hosters to ensure that CPU and memory resources are allocated and used effectively, and that incorrectly balanced resources do not cause virtual machines to run ineffectively.

Processor (CPU) throttling

You can set the weight of a virtual processor to provide the processor with a larger or smaller share of CPU cycles, using the following properties:

- **High, Normal, Low, Custom**—Specifies how the CPU is distributed when contention occurs. Higher priority virtual machines will be allocated CPU first.
- **Reserve CPU cycles (%)—**Specifies the percentage of CPU resources that are associated with one logical processor that should be reserved for the virtual machine. This is useful when a virtual machine runs applications that are particularly CPU-intensive and you want to ensure a minimal level of CPU resources. A zero setting indicates that no specific CPU percentage is reserved for the virtual machine. This setting is only supported for Windows Server 2012.
- **Limit CPU cycles (%)**—Specifies that the virtual machine should not consume more that the indicated percentage of one logical processor. This setting is only supported for Windows Server 2012.

The settings for these properties ensure that virtual machines can be prioritized or deprioritized when CPU resources are overcommitted. For highly intensive workloads, more virtual processors can be added, especially when a physical CPU is close to its upper limit.

Memory throttling and weight

Memory throttling helps to prioritize or deprioritize access to memory resources in scenarios where memory resources are constrained. When memory usage on a host is high, then the virtual machines with a higher memory priority are allocated memory resources before the virtual machines with a lower priority. If you specify a lower priority, it might prevent a virtual machine from starting when other virtual machines are running and the available memory is low. You can set the memory priority settings and thresholds as follows:

- **Static**—The amount of static memory that is assigned to a specific virtual machine
- **Dynamic**—Dynamic memory settings include:
    a. **Start-up memory**—The amount of memory that is allocated to the virtual machine when it starts up. It should at least be set to the minimum amount of memory that is required to run the operating system and applications on the virtual machine. Dynamic memory will adjust the memory amount as required.
    b. **Minimum memory**—The minimum amount of memory that is required for the virtual machine. It allows an idle machine to scale back the memory consumption below the start-up memory requirement. The available memory can then be used by other virtual machines.
    c. **Maximum memory**—The memory limit that is allocated to the virtual machine. The default value for Windows Server 2012 is 1 TB.
    d. **Memory Buffer Percentage**—Dynamic memory adds memory to a virtual machine as required, but there is a chance that an application might demand memory more quickly than dynamic memory allocates it. The memory buffer percentage specifies the amount of available memory that will be assigned to the virtual machine if needed. The percentage is based on the amount of memory that is actually needed by the applications and services that run on the virtual machine. It is expressed as a percentage because it changes depending on the virtual machine requirements.

    The percentage is calculated as follows: Amount of memory buffer = memory needed by the virtual machine/ (memory buffer value/100). For example, if the memory that is committed to the virtual machine is 1000 MB and the buffer is 20%, then an additional buffer of 20% (200 MB) will be allocated for a total of 1200 MB of physical memory allocated to the virtual machine.
    e. **Memory weight**—The priority that is allocated to a virtual machine when the memory resources are in full use. If you set a high priority value, it will prioritize a virtual machine when the memory resources are allocated. If you set a low priority, a virtual machine might be unable to start if memory resources are insufficient.

For information about how to configure processor and memory throttling, see How To Configure Processor and Memory Throttling for VMM.

How To Configure Processor and Memory Throttling for VMM

Virtual Machine Manager (VMM) provides processor throttling (CPU) and memory throttling capabilities. This topic describes how to configure the throttling values. You can set the values when you configure a virtual machine by using the Create Virtual Machine Wizard, on the property sheet of an existing virtual machine, or on a virtual machine template. This topic describes how to configure processor and memory throttling, and memory weight.

To configure processor throttling

1. In the **Advanced** section of the virtual machine or of the virtual machine template properties, click **CPU Priority**.
2. Select a priority value for the virtual machine. These values specify how the CPU resources are balanced between virtual machine, and correspond to the relative weight value in Hyper-V:
   - High—Relative weight value of 200
   - Normal—Relative weight value of 100
   - Low—Relative weight value of 50
   - Custom—Relative weight values that are supported are between 1 and 10000
3. In **Reserve CPU cycles (%)**, specify the percentage of the CPU resources on one logical processor that should be reserved for a virtual machine. This is useful when a virtual machine runs applications that are particularly CPU-intensive, and you want to ensure a minimal level of CPU resources. A zero setting indicates that no specific CPU percentage is reserved.
4. In **Limit CPU cycles (%)**, specify the maximum percentage of the CPU resources on one logical processor that the virtual machine should consume. The virtual machine will not be allocated more than this percentage.

To configure memory throttling

1. In the **General** section of the virtual machine or of the virtual machine template properties, click **Memory**.
2. Select **Static** to specify that a fixed amount of memory should be assigned to a virtual machine.
3. Select **Dynamic** to specify the dynamic memory settings for a virtual machine, as follows:
   a. In **Startup memory**, specify the amount of memory that is allocated to the virtual machine when it starts up. The memory value should be set at least to the minimum amount of memory that is required for the virtual machine operating system and applications to run.
   b. In **Minimum memory**, specify an amount of memory that allows an idle virtual machine to scale back the memory consumption below the startup memory requirement. This makes more memory available for use by other virtual machines.

c. In **Maximum memory**, specify the maximum amount of memory that is allocated to a virtual machine. The default setting for Windows Server 2012 is 1 TB.

d. In **Memory buffer percentage** specify the amount of available memory that will be assigned to a virtual machine if the need arises. The percentage should be based on the amount of memory that is actually needed by the applications and services that run on the virtual machine. The memory buffer percentage should be calculated as follows: Amount of memory buffer = memory that is needed by the virtual machine/ (memory buffer value/100). For example, if the memory that is committed to the virtual machine is 1000 MB and the buffer is 20%, then an additional buffer of 20% (200 MB) will be allocated for a total of 1200 MB of physical memory allocated to the virtual machine.

To configure memory weight

1. In the **Advanced** section of the virtual machine or of the virtual machine template properties, click **Memory Weight**.
2. Configure the priority that is used to allocate memory to a virtual machine when memory resources are in high usage. If you specify a low priority, the virtual machine might not be available to start when the memory resources are not sufficient.

Deploying Virtual NUMA for VMM

With Virtual Machine Manager (VMM) you can configure, deploy, and manage the virtual Non-Uniform Memory Access (NUMA) features that are introduced in Hyper-V™ in Windows Server 2012.

NUMA is a memory architecture that is used in multiprocessor systems, where the time that is required for a processor to access memory depends on the location of the memory relative to the processor. On a NUMA system, a processor can access the local memory (the memory that is directly attached to the processor) faster than the non-local memory (the memory that is attached to another processor). NUMA attempts to close the gap between the speed of processors and the memory that they use. To do so, NUMA provides separate memory on a per-processor basis, thus This helps to avoid the performance degradation that occurs when multiple processors try to access the same memory. Each block of dedicated memory is known as a NUMA node.

NUMA features in Hyper-V on Windows Server 2012

Hyper-V in Windows Server 2012 supports running on a host system with up to 320 logical processors. The number of virtual processors that can be configured in a virtual machine depends on the number of processors on the physical computers. For example, to configure a virtual machine with the maximum of 64 virtual processors, you must be running Hyper-V on a

virtualization host that has 64 or more logical processors. In order to support this scalability, Hyper-V in Windows Server 2012 provides virtual NUMA, a synthetic NUMA-like environment for virtual machines. Virtual processors and guest memory are grouped into virtual NUMA nodes, and the virtual machine presents a topology to the guest operating system based on the underlying physical topology.

By default, when a virtual machine is created, Hyper-V examines the underlying physical topology and automatically configures the virtual NUMA topology with optimal settings, based on a number of factors, which include: the number of logical processors and the amount of memory per NUMA node.

Virtual NUMA enables the deployment of larger and more mission-critical workloads that can be run without significant performance degradation in a virtualized environment, when compared to running non-virtualized computers with physical NUMA hardware. When a new virtual machine is created, by default Hyper-V uses values for the guest settings that are in sync with the Hyper-V host NUMA topology. For example, if a host has 16 cores and 64 GB divided evenly between two NUMA nodes with two NUMA nodes per physical processor socket, then a virtual machine that is created on the host with 16 virtual processors will have the maximum number of processors per node setting set to eight, maximum nodes per socket set to two, and maximum memory per node set to 32 GB.

In addition, NUMA spanning can be enabled or disabled. With spanning enabled, individual virtual NUMA nodes can allocate non-local memory, and an administrator can deploy a virtual machine that has more virtual processors per virtual NUMA node than the number of processors that are available on the underlying hardware NUMA node on the Hyper-V host. NUMA spanning for a virtual machine does incur a performance cost because virtual machines access memory on non-local NUMA nodes.

For information about how to configure virtual NUMA, see How to Configure Virtual NUMA for VMM.

How to Configure Virtual NUMA for VMM

With Virtual Machine Manager (VMM) you can configure the virtual Non-Uniform Memory Access (NUMA) features that are provided by Hyper-V™ in Windows Server 2012. This topic provides the following procedures for configuring virtual NUMA:

1. Configuring virtual NUMA settings—When a new virtual machine is created, Hyper-V specifies the default settings for virtual NUMA. These settings are in sync with the NUMA topology of the Hyper-V host. For example, if a host has 16 cores and 64 GB divided evenly between two NUMA nodes, with two NUMA nodes per physical processor socket, then by default, a virtual machine that was created on the host will have the **Maximum processors per virtual NUMA node** property set to 8, the **Maximum virtual NUMA nodes per socket** set to 2, and the **Maximum memory per virtual NUMA node (MB)** property set to 32 GB. You can modify the default values as required.

2. Enable virtual NUMA spanning—If virtual NUMA spanning is enabled, then individual virtual NUMA nodes can allocate non-local memory. If the setting is not enabled, each node uses memory from only one physical NUMA node. Note that whether spanning is enabled or not, virtual nodes can be allocated memory from the same or different underlying host NUMA nodes, based on the physical host topology. NUMA spanning is enabled by default.

Configuring virtual NUMA settings

Use this procedure to enable and configure virtual NUMA.

To configure virtual NUMA settings

1. In the **Advanced** section of the virtual machine or virtual machine template properties, click **Virtual NUMA**.
2. In **Maximum processors per virtual NUMA node**, specify the maximum number of virtual processors that belong to the same virtual machine and that can be used concurrently on a virtual NUMA node. Configure this setting to ensure maximum bandwidth. different NUMA virtual machines to use different NUMA nodes. The minimum limit is 1 and the maximum is 32.
3. In **Maximum memory per virtual NUMA node (MB)**, specify the maximum amount of memory (MB) that can be allocated to a single virtual NUMA node. The minimum limit is 8 MB and the maximum is 256 GB.
4. In **Maximum virtual NUMA nodes per socket**, specify the maximum number of virtual NUMA nodes that are allowed on a single socket. The minimum number is 1 and the maximum is 64.

Enable virtual NUMA spanning

Use this procedure to enable or disable virtual NUMA spanning.

To enable or disable virtual NUMA spanning

1. In the **Virtual NUMA** properties page, to enable spanning, select **Allow virtual machine to span hardware NUMA nodes**. Clear the check box to disable spanning.

Creating Virtual Machine Role Templates by Using VMM and Windows Azure Pack

As a hosting provider, you can use VMM in System Center 2012 R2 in combination with Windows Azure Pack to increase the range of capabilities that you can offer to tenants. To help tenants create virtual machines with specific operating systems and applications already installed, in a way that works flexibly with software licensing methods, you can create Virtual Machine Role

templates. Tenants can use these templates to create Virtual Machine Roles in both on-premises hosting environments and service-provider hosting environments.

Note
To use Virtual Machine Role templates, you must use VMM in System Center 2012 R2 with Windows Azure Pack.

To begin to create a Virtual Machine Role template, you can download and install one or more Windows Azure Pack Gallery Resources into your hosting environment. Windows Azure Pack Gallery Resources include two types of standard, reusable software packages:

- Resource Definition package: Forms the basis for creating a virtual machine.
- Resource Extension package: Forms the basis for installing applications on a virtual machine.

Each Windows Azure Pack Gallery Resource contains a Readme file that explains how to prepare your environment for that resource. Part of the process of installing the gallery resource into your hosting environment is to use Windows PowerShell commands to import the Resource Extension package into VMM.

To create a Virtual Machine Role template, you also need a virtual hard disk file that contains an operating system that has been prepared for deployment. For example, you could use a virtual hard disk file in .vhdx format that contains an operating system such as Windows Server 2012 that has been prepared with the Sysprep tool. After you create the virtual hard disk, you must add it to the VMM library and use the VMM console and Windows PowerShell to provide VMM with necessary information about the virtual hard disk. Examples of this information include the name of the operating system and the specific release number.

Use the following table to find more information about the process for creating a Virtual Machine Role template, and about items such as Windows Azure Pack Gallery Resources, and the Resource Definition and Resource Extension packages within them.

Type of information	Link
Information about Windows Azure Pack	Windows Azure Pack on the Microsoft website Windows Azure Pack for Windows Server on TechNet
Description of how to add file-based resources, such as virtual hard disk files, to the VMM library	How to Add File-Based Resources to the VMM Library on TechNet
Steps for creating a Virtual Machine Role template, including steps for downloading items from the Windows Azure Pack Gallery and steps for importing Resource Extension packages into VMM	Downloading and Installing Windows Azure Pack Gallery Resource on the TechNet wiki

Type of information	Link
A link for downloading the Web Platform Installer, with which you can download Windows Azure Pack Gallery Resources	Microsoft Web Platform Installer
Description and diagram of how Virtual Machine Role templates are created, with descriptions of Resource Definitions and Resource Extensions	System Center 2012 R2 Virtual Machine Role Authoring Guide on the TechNet wiki
Steps for creating a customized Virtual Machine Role template, including steps for creating Resource Definition and Resource Extension packages and installing them in your hosting environment	System Center 2012 R2 Virtual Machine Role Authoring Guide - Installing a Virtual Machine Role on the TechNet wiki

Migrating Virtual Machines and Storage in VMM

This section provides an overview of migration in Virtual Machine Manager (VMM) and includes procedures to migrate a virtual machine by using the Migrate Virtual Machine Wizard or a drag-and-drop operation, to perform a quick storage migration, and to run a live migration.

- Migrating Virtual Machines and Storage Overview
- How to Migrate a Virtual Machine in VMM
- How to Run a Quick Storage Migration in VMM
- How to Run a Live Migration in VMM

Migrating Virtual Machines and Storage Overview

Virtual Machine Manager (VMM) supports the following types of migration:

- **Network migration**—This is the slowest type of migration and performs a network copy of the virtual machine data using BITS. The amount of downtime is in direct proportion to the size of the data transfer.
- **Quick migration**—This type of migration is also known as cluster transfer, and can be used to migrate a highly available virtual machine. It leverages Windows Failover Cluster to migrate virtual machines between cluster nodes. The running state of the virtual machine is saved to disk (the virtual machine is hibernated), the disk is failed over to the other cluster

node, and then the saved state is loaded to wake up the virtual machine. Downtime is minimal because quick migration takes a snapshot of the virtual machine and transfers data without requiring the virtual machine to be turned off.

- **Quick storage migration**—Quick storage migration allows you to move virtual machine storage from one location to another. For example, you can move the storage for a virtual machine from a Fibre Channel SAN to an iSCSI SAN. The virtual disks of a running virtual machine can be migrated independent of storage protocols (SCSI, Fibre Channel) or storage types (local, DAS, SAN). Downtime is minimal because quick storage migration takes a snapshot of the virtual machine and transfers data without requiring the virtual machine to be turned off.
- **SAN migration**—This type of migration uses SAN transfer to migrate virtual machines, and highly available virtual machines, into and out of a cluster. It can be used when both the source and destination hosts have access to the same storage infrastructure (LUN), and the storage can be transferred from one host to another. For SAN migration, the files for a virtual machine are not copied from one server to another and thus downtime is minimized. SAN migration can be used to copy a virtual machine from one host to another, or copying a virtual machine to or from the library. Note the following:
    a. When you migrate a virtual machine into a cluster by using a SAN transfer, VMM checks that each node in the cluster can see the LUN, and automatically creates a cluster disk resource for the LUN.
    b. To migrate a virtual machine out of a cluster, the virtual machine must be on a dedicated LUN that is not using CSV.
    c. The following SAN infrastructures are supported for migration: Fiber Channel; iSCSI SANs; N_Port ID Virtualization (NPID).
- **Live migration**—This type of migration moves a virtual machine running as part of a failover cluster from one cluster to another with no noticeable downtime for users or network applications.

VMM automatically selects the type of transfer that will be used for migration. When you perform a migration in the VMM console using the Migrate VM Wizard, the migration type that will be used is displayed in the Transfer Type column.

Live migration new features

As of System Center 2012 SP1, VMM provides a number of additional live migration features, based on new migration capabilities in Windows Server 2012. These features include:

- Live migration outside a cluster—In addition to performing live migration within a cluster, you can perform live migration between two standalone computers that are not cluster nodes.
- Live migration between nodes in two different clusters— You can migrate between nodes within a cluster, or between nodes in different clusters.
- Live migration of virtual machine storage —You can migrate storage in order to update the physical storage that is available in Hyper-V, or to mitigate bottlenecks in storage performance. Storage can be added to either a stand-alone computer or to a Hyper-V cluster, and then virtual machines can be moved to the new storage while they continue to run.

- Live VSM—By using live system migration (live VSM), you can migrate virtual machines and their storage together in a single action.
- Concurrent live migration— You can perform multiple concurrent live migrations of virtual machines and storage. The concurrent limit can be configured manually. Any concurrent live migrations in excess of the limit will be queued.

VMM inspects and validates the configuration settings of a destination host before migration from a source host begins.

Business benefits

The new live migration features provide a number of business benefits:

- **Increased flexibility**—The new features can help to simplify the movement of virtual machines across hosts and clusters. Therefore, it becomes easier to manage a dynamic datacenter.
- **Ease-of-maintenance**—Live migration alleviates the need to take standalone hosts and cluster hosts offline for maintenance and migration purposes, which helps to avoid downtime. With the ability to perform concurrent migrations and maintenance, migration timeframes can become shorter, depending on the time that is required to perform the live migration. In addition, the planning process for Hyper-V mobility is simplified.
- **Better hardware utilization**—The distribution of virtual machines can be optimized across the infrastructure. Virtual machines and storage can be moved to stand-alone servers and clusters with spare capacity, without interrupting availability. Power consumption is reduced as virtual machines can be moved across hosts, and then hosts can be powered down to save energy.
- **Windows Server 2012 features**—As of System Center 2012 SP1, VMM takes advantage of the new failover clustering features that are available in the Windows Server 2012 release. These features include: new APIs to migrate virtual machines across cluster nodes, and improved attach/detach functionality that enables migration of virtual machines in and out of failover clusters without downtime.

Virtual machine live migration support

The following table summarizes the support matrix for live migration of virtual machines as of System Center 2012 SP1.

Source	**Destination**	
	Destination: Stand-alone	**Destination: Cluster node**
Source: Stand-alone	Supported	Supported
Source: Cluster node	Supported	Supported. Source and destination can be in the same

Source	Destination	
		cluster or in different clusters.

Live storage migration

With virtual machine storage migration you can move storage from one location to another without interrupting the workload of the virtual machine, if it is running. You can also use storage migration to move, service, or upgrade storage resources, or for migration of a standalone or cluster virtual machine. The following table summarizes the support matrix for storage migration as of System Center 2012 SP1.

Source	Destination		
	Destination: Local disk (stand-alone)	**Destination: SMB 3.0 share (standalone or cluster)**	**Destination: CSV (cluster)**
Source: Local disk (stand-alone)	Supported	Supported. The virtual machine will be promoted to high availability.	Not supported.
Source: SMB 3.0 share	Supported. In a cluster configuration the virtual machine will be demoted, and will no longer be highly available after migration to the local disk.	Supported	Supported
Source: CSV (cluster)	In a cluster configuration the virtual machine will be demoted, and will no longer be highly available after migration to the local disk.	Supported. The SMB share must be available from the destination cluster node.	Supported. CSV must be available from the destination cluster node.

Live migration limitations

Note the following requirements and limitations when performing a live migration of virtual machines and storage:

- Live migration requires two or more servers that run Hyper-V, that support hardware virtualization, and use processors from the same manufacturer, such as all AMD processors or all Intel processors, for example.
- Live migration is supported for hosts that run Windows Server 2012. There is no backward compatibility to support migration between hosts that run Windows Server 2008 R2 and Windows Server 2012.
- Virtual machines must be configured to use virtual hard disks or virtual Fibre Channel disks, not physical disks.
- For live migration network traffic you should use a private network.
- Source and destination servers must belong to the same Active Directory domain, or to different trusted domains.
- If the source or destination virtual machine VHD has a base disk, the base disk must be in a share that is accessible (registered) from the destination host. Generally, live migration does not move the base disk.
- Migration between clusters is only supported on hosts that run versions of the Windows Server 2012 operating system that support the Windows Failover Cluster Service. Windows Failover Clustering and Cluster Shared Volume (CSV) storage should be enabled in the cluster.
- Live migration of a virtual machine does not migrate virtual machine storage, specifically meaning the location that stores the virtual machine images (VHD, ISO, VFD files). To handle storage requirements, you can use one of the following options:
    - Configure the virtual machine so that the storage files are available on a file share that is accessible by both the source and destination host of the migration.
    - Run a combined live virtual machine and storage migration (live VSM) in a single action.
    - Run a separate storage migration.
- If the source and destination hosts use shared storage, note the following:
    - All files that comprise a virtual machine, such as virtual hard disks, snapshots, and configuration, should be stored on an SMB share.
    - Permissions on the SMB share should be configured to grant access to the computer accounts of all servers that run Hyper-V.
- A storage migration moves virtual machine images (VHD, ISO, and VFD files), snapshot configurations, and data (saved state files).
- Storage migration is per virtual machine.
- Storage migration does not move base (parent) disks, with the exception of snapshot disks.

Live virtual machine and storage migration (live VSM)

You can perform a live VSM to migrate both a virtual machine, and the virtual machine storage in a single action.

- To use live VSM, the virtual machine LUN must be masked from the destination host.
- Live VSM is supported between two stand-alone hosts that run Hyper-V on Windows Server 2012. The transfer can occur between local disks or SMB 3.0 file shares.
- Live VSM is supported between two Hyper-V host clusters that run on Windows Server 2012. The virtual machine can be transferred to either a CSV or SMB 3.0 file share on the destination host cluster.

How to Migrate a Virtual Machine in VMM

This procedure describes how to migrate a virtual machine in Virtual Machine Manager (VMM). To perform a migration, you can use any of the following actions:

- **Run the Migrate VM Wizard**—By using this wizard, you can select a destination virtual machine host for the migration, specify the path that stores the virtual machine files, attach the virtual machine to any of the virtual networks that are found on the selected host, and, if a storage area network (SAN) transfer is available, select a network transfer instead.
- **Run the Migrate Storage Wizard**— By using this wizard, you can move the files for a virtual machine to a different storage location on the same host.
- **Drag the virtual machine onto a host**—When you drag a virtual machine to a host, VMM uses automatic placement to place the virtual machine on the most suitable volume on the host. The placement is based on available space.
- **Drag the virtual machine onto a host group**—When you drag the virtual machine to a host group, VMM uses automatic placement to place the virtual machine on the most suitable host that is available in the host group, which is based on the virtual machine requirements and the host ratings. The virtual machine is placed on the most suitable volume on the host. The placement is based on available space. During automatic placement, the host rating process identifies the most suitable volume on each host. For more information, see Understanding Virtual Machine Placement and Ratings in VMM..

Note the following before you begin migration:

- If a correctly configured SAN is available, VMM automatically uses SAN to perform transfers. However, if you use the Migrate Virtual Machine Wizard to perform a transfer, you can override the SAN usage and perform a local area network (LAN) transfer.
- If you migrated a virtual machine that is connected to SAN storage, the virtual machine cannot reconnect to the SAN unless the destination host also has access to that SAN. VMM cannot detect if a virtual machine is connected to a SAN or if the destination host is connected to the same SAN, and therefore cannot provide a warning. You must ensure that the new host is configured to enable the virtual machine to reconnect to the SAN before you migrate the virtual machine.
- One method to convert a VMware ESX virtual machine to a Microsoft Hyper-V virtual machine is to migrate the virtual machine from ESX Server host to a Hyper-V host. Before

you migrate a virtual machine from a ESX server to a Hyper-V host, ensure that the source ESX Server host has the **OK** status in VMM, and that the virtual machine is turned off. If the host has **OK (Limited)** status, additional security configuration is required to enable file transfers to the Hyper-V host. You must provide credentials for the ESX Server host; in addition, if you manage your VMware infrastructure in secure mode, a certificate and public key might be required. Alternatively, you can perform a virtual-to-virtual (V2V) conversion on the virtual machine files to convert a VMware virtual machine to a Hyper-V virtual machine. For more information see How to Deploy a Virtual Machine by Converting a Virtual Machine (V2V).

- If you change the permissions for a virtual machine through the file system, and then migrate the virtual machine, VMM re-creates the access control list (ACL). All changes that were made outside VMM will be lost.
- If you attempt to migrate a virtual machine on a Hyper-V host soon after you have removed a checkpoint from the virtual machine, the migration might fail. If you attempt a migration before Hyper-V has finished deleting the checkpoint, the migration fails, and you must repair the virtual machine by using the **Undo** option. To avoid this issue, you can ensure that the checkpoint has been deleted, or you can wait for Hyper-V to delete it for you. To ensure that a checkpoint has been deleted, do the following:
  a. In the VMM console, in **Virtual Machines** view, click the virtual machine, and then click **Stop** in the **Actions** pane.
  b. On the host, open Hyper-V Manager. Click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
  c. In the **Status** column, **Merge in progress** indicates that the checkpoint has not been deleted. Wait until this operation has finished before you migrate the virtual machine.

Migrating a virtual machine

Use the following procedure to migrate a virtual machine by using the Migrate VM Wizard.

To migrate a virtual machine by using the wizard

1. In **Virtual Machines** view, browse to the host on which the virtual machine is deployed in the navigation pane.
2. In the results pane, select the virtual machine, and then click **Migrate Virtual Machine** in the **Actions** pane.
3. On the **Select Host** wizard page, select the destination host.
4. To get additional information about the host, select the host, and view the tabs in the details area:
   - **Details**—Indicates the status of the host, the operating system, and the type and status of virtualization software. Lists the virtual machines on the host.
   - **Rating Explanation**—Lists the factors that resulted in a 0 star rating.
   - **SAN Explanation** or **Deployment and Transfer Explanation**—Lists the factors that make a SAN transfer unavailable. In addition, in System Center 2012 R2 Virtual Machine Manager, the **Deployment and Transfer Explanation** tab provides an

explanation if fast file copy could not be used. Fast file copy is a new feature in System Center 2012 R2 Virtual Machine Manager, which is based on the Windows Offloaded Data Transfers (ODX) feature that is introduced in Windows Server 2012 R2. For information about ODX, see Windows Offloaded Data Transfers Overview.

5. In the **Select Path** page, accept the default path, or click **Browse** and browse to the folder in which you want to store the configuration files for the virtual machine, and then click **OK**. Note the following:
   a. If the target host is a part of a failover cluster that has Cluster Shared Volumes (CSV) enabled, you can store the virtual machine on a CSV Logical Units (LUs) and associated Number (LUN) that is already in use by other highly available virtual machines (HAVMs). With CSV, multiple HAVMs can share the same LUN. The migration of one HAVM does not affect others that are sharing the same LUN. VMM also supports multiple HAVMs per LUN for VMware environments that are configured with VMware VMFS LUNs.
   b. If you selected a path other than a default virtual machine path and want to store other virtual machines on that path, select the **Add this path to the list of host default paths** check box to add the path to the default paths on the host.

      As of System Center 2012 Service Pack 1 (SP1), if you use a network transfer, you have the option to specify separate storage locations for each virtual hard disk (.vhd or .vhdx) file for the virtual machine. By default, all .vhd or .vhdx files are stored in the same location that is specified for the virtual machine.
   c. If SAN transfers are enabled for this deployment, the virtual machine by default is transferred to the host over the SAN. If you do not want to perform a SAN transfer, select **Transfer over the network even if a SAN transfer is available**. If SAN transfers are not available for this deployment, that option is not available.
6. On the **Select Networks** wizard page, modify the networks, and then attach them to **None** or to any of the virtual networks that are found on the selected host.

   Note
   Networks area lists each of the virtual network adapters that are currently attached to the virtual machine. Network adapters default to **None** if you selected **None** in the hardware configuration or to the best matching virtual network according to the network matching rules.
7. On the **Select Virtual SAN** wizard page, select the applicable virtual SANs from the drop-down list for each listed virtual HBA. When you have finished, click **Next**.
8. On the **Summary** wizard page, review your settings. To change settings, click **Previous**.

   To start the virtual machine after you deployed it, select the **Start the virtual machine immediately after deploying it to the host** check box.

   Note
   Click **View Script** to view the Windows PowerShell cmdlets that perform the migration.
9. To begin deploying the virtual machine, click **Move**.

To review the progress and results of the operation, open the **Jobs** workspace. By default, the workspace opens when the wizard closes. To open this workspace at any time, click **Jobs** on the VMM console toolbar.

Use the following procedure to migrate a virtual machine by using a drag-and-drop operation.

To migrate a virtual machine by using a drag-and-drop operation

1. In **Virtual Machines** view, browse to the virtual machine's current host in the navigation pane.
2. In the results pane, click the virtual machine and, while you hold down the mouse button, drag the virtual machine to either the host of choice or to the host group of choice in the navigation pane.
3. When you release the mouse button, the system attempts to migrate the virtual machine by using one of the following methods:
   - If you dragged the virtual machine to a host, the system evaluates the host's suitability for the virtual machine and attempts to migrate the virtual machine if the host is found suitable.
   - If you dragged the virtual machine to a host group, the system rates each host in the host group and attempts to migrate the virtual machine to the most suitable of those hosts. For the migration to succeed, a virtual machine path must be configured on the host for the recommended volume.

Note

If you encounter difficulties using drag-and-drop, log out of VMM, and then log back in and try again. Also try restarting the virtual machine and then try again.

How to Run a Quick Storage Migration in VMM

Use the following procedure to run a *quick storage migration* in Virtual Machine Manager (VMM). Quick storage migration enables you to move the files of a virtual machine from one storage location to another on the same virtual machine host. If the virtual machine is running, you can perform a quick storage migration, which results in little or no service outage for users of the virtual machine. If the virtual machine has more than one virtual hard disk, you can specify a separate location for each virtual hard disk (.vhd or .vhdx) file.

Running a quick storage migration

Use the following procedure to run a quick storage migration.

To run a quick storage migration

1. In the VMM console, open the **VM's and Services** workspace. In the **VM's and Services** pane, expand **All Hosts**, and then select the host on which the virtual machine is deployed.
2. In the **VM's** pane, right-click the virtual machine, and then click **Migrate Storage**.

   The Migrate Storage Wizard opens at the **Select Path** page. It displays the current locations of the virtual machine's files. The current path to the location of the configuration files is displayed in the **Storage location for VM configuration** box, and the current path to the location of each virtual hard disk (.vhd) is displayed in the **Disks** list.
3. On the **Select Path** page, do the following:
   - Configure a storage location for the virtual machine configuration, by doing one of the following:
     - Click the **Browse** button next to **Storage location for VM configuration**, and then click an existing default virtual machine path on the list.
     - Click the **Browse** button next to **Storage location for VM configuration** and browse to a location on the host. VMM automatically changes the paths for all virtual disks to the same path that you specified for the configuration files.
     - Type a path. When you type a new path for the configuration files of the virtual machine, VMM does not automatically change the paths for the virtual disks until you click outside of the **Storage location for VM configuration** box.
   - Select the **Add this path to the list of default storage locations on the host** check box, if you selected a path other than an existing virtual machine path, and you want to add the path to the default paths on the host.
   - Specify the configuration file placement options, as follows:
     i. Select **Automatically place all VHDs with the configuration** to move all of the virtual machine files to the same location.
     ii. Select **Allow VHDs to be placed individually** to move one or more of the virtual machine files to a different location than the location of the configuration files. If you select this setting, in the **Disks** area, type the new path in the **Location** box for each virtual hard disk, or click **Browse** to browse to the location where you want to store the file. Note that if the virtual machine is running, and you change the path for any of the virtual hard drives, you also must specify a new path for the configuration files of the virtual machine, or the migration operation fails. You must enter the new path even if you want to leave the configuration files in their current location. In that case, you can create a new subfolder within the current location of the configuration files, and then select that new location in the **Storage location for VM configuration** box.
4. On the **Summary** page, click **Move** to begin moving the virtual machine files.
5. To review the progress and results of the operation, open the **Jobs** pane. By default, this pane opens after the wizard closes. To view this pane at any time, click **Jobs** on the VMM console toolbar.

How to Run a Live Migration in VMM

Virtual Machine Manager (VMM) provides live migration support between stand-alone Hyper-V hosts, or cluster hosts that have the Live Migration feature enabled. This topic describes the following migration procedures:

- Live migration of a virtual machine between two stand-alone hosts—This procedure describes how to migrate a virtual machine from one stand-alone Hyper-V host to another stand-alone Hyper-V host. Note that the virtual machine configuration files and virtual hard disk must be located on a Server Message Block (SMB) 3.0 file share.
- Live migration of a virtual machine between hosts in two clusters—This procedure describes how to migrate a virtual machine from a host that runs in one cluster to a host that runs in a different cluster. Note that when you run a live migration between two clusters, the virtual machine temporarily loses its high availability status. Therefore, a host failure during the migration causes the virtual machine to become unavailable. For live migration between clusters, you should use SMB 3.0 file shares as the storage location. Because the storage does not have to be migrated, the time in which high availability status cannot be guaranteed is very short.
- Live migration of storage between two locations on a stand-alone host—This procedure describes how to migrate storage only.
- Concurrent live migrations—This procedure provides an overview of how to run multiple concurrent migrations and describes how to verify that concurrent migrations run as expected.
- Faster live migrations—This procedure provides an overview of how to perform a faster live migration.

Live migration of a virtual machine between two stand-alone hosts

Use the following procedure to perform a live migration between two stand-alone hosts.

To perform live migration of a virtual machine between two stand-alone hosts

1. Open the **VMs and Services** workspace.
2. In the **VMs and Services** pane, expand **All Hosts**. Locate, and then click the stand-alone source host from which you want to migrate a virtual machine.

   For example, click the host **StandAlone1** in the host group **Stand-Alone HG**.
3. In the **VMs** pane, click the running virtual machine that you want to migrate. Start the machine if it is not running.

   For example, click the virtual machine **StandAloneVM1**.
4. On the **Virtual Machine** tab, in the **Virtual Machine** group, click **Migrate Virtual Machine** to start the **Migrate Virtual Machine Wizard**.
5. On the **Select Host** page, review the destination hosts and their associated transfer

types.

The **Live** transfer type appears if both hosts are configured to connect to the same SMB 3.0 file share.

6. Click the destination host where the transfer type is **Live**, and then click **Next**.

   For example, click the host **StandAlone2**.

7. On the **Summary** page, click **Move**.
8. To track the job status, open the **Jobs** workspace.
9. To verify that the virtual machine was migrated, in the **VMs and Services** workspace, in the **VMs and Services** pane, locate, and then click the destination host. In the **VMs** pane, verify that the virtual machine is listed with a status of **Running**.

Live migration of a virtual machine between hosts in two clusters

Use the following procedure to perform a live migration between two cluster hosts.

To perform live migration of a virtual machine between hosts in two clusters

1. Open the **VMs and Services** workspace.
2. In the **VMs and Services** pane, expand **All Hosts**. Locate, and then click the cluster node from which you want to try the live migration of a highly available virtual machine.

   For example, click the cluster node **Cluster1Node1**.

3. In the **VMs** pane, click the running virtual machine that you want to migrate. Start the machine if it is not running.

   For example, click the virtual machine **HAVM1**.

4. On the **Virtual Machine** tab, in the **Virtual Machine** group, click **Migrate Virtual Machine** to start the **Migrate Virtual Machine Wizard**.
5. On the **Select Host** page, review the destination hosts and their associated transfer types.

   The **Live** transfer type is available for any destination cluster nodes that are configured to connect to the same SMB 3.0 file share on which the virtual machine was originally created.

6. Click a cluster node that is in a different host cluster, and then click **Next**.

   For example, click the cluster node **Cluster2Node1**.

7. On the **Summary** page, click **Move**.
8. To track the job status, open the **Jobs** workspace.
9. To verify that the virtual machine was migrated, in the **VMs and Services** workspace, in the **VMs and Services** pane, locate, and then click the destination host. In the **VMs** pane, verify that the virtual machine is listed with a status of **Running**.

Live migration of storage between two locations on a stand-alone host

Use the following procedure to perform a live migration between locations on stand-alone hosts. You can move the entire virtual machine, which includes virtual hard disks (VHDs) and configuration information, or move only specific VHDs to a different location.

To perform live migration of storage between two locations on a stand-alone host

1. Open the **VMs and Services** workspace.
2. In the **VMs and Services** pane, expand **All Hosts**. Locate, and then click the stand-alone host where the virtual machine resides.

   For example, click the host **StandAlone2** in the host group **Stand-Alone HG**.
3. In the **VMs** pane, click the running virtual machine on which you want to try live storage migration. Start the virtual machine if it is not running.

   For example, click the virtual machine **StandAloneVM1**.
4. On the **Virtual Machine** tab, in the **Virtual Machine** group, click **Migrate Storage** to start the **Migrate Virtual Machine Wizard**.
5. On the **Select Path** page, in the **Storage location** list, click one of the default storage locations on the host. Or, click **Browse** to view all possible storage destinations, click the destination SMB 3.0 file share or location on the local hard disk, and then click **OK**.

   Important
   If you specify an SMB 3.0 file share in the **Storage location** list, ensure that you use the fully qualified domain name (FQDN) of the destination server in the share path. For example, instead of *fileserver1**smbshare*, use *fileserver1.contoso.com**smbshare*.
6. Optionally, select the **Add this path to the list of default storage locations on the host** check box, and then click **Next**.
7. On the **Summary** page, click **Move**.
8. To track the job status, open the **Jobs** workspace.

Concurrent live migrations

To run live migrations concurrently, perform any of the procedures in this topic on multiple virtual machines so that two migrations occur at the same time on the same host. In the user interface, you cannot multi-select virtual machines to perform live migrations. Instead, you must manually start each migration. You can specify how many concurrent migrations to run. The default setting is two, which is the number of simultaneous live migration and storage migrations that are enabled in Hyper-V. For example, a host can participate in one outgoing live migration plus one incoming, two outgoing live migrations, or two incoming live migrations. Live migrations and live storage migrations are independent. Therefore, you can perform two live migrations and two live storage migrations simultaneously. VMM considers live virtual machine and storage migration

(live VSM) as one live migration and one storage migration. Use the following procedure to view concurrent migrations.

To view concurrent migrations

1. Open Hyper-V Manager on the host, and then in the **Actions** pane, click **Hyper-V Settings**. Under **Server**, you can view **Live Migrations** and **Storage Migrations** settings.
2. In the **Jobs** workspace, verify that the migrations occur simultaneously.

Faster live migrations

As of System Center 2012 R2, you can perform faster live migrations for Hyper-V hosts. Live migration speed can be increased by using compression, by using SMB as the transport, or by using both. The compression method uses algorithms that reduce the data that is transmitted over the wire. The SMB method can allow for faster data transfer.

By default, faster live migration is enabled to use the compression method. You can disable, enable, or change the method of faster live migration by changing the live storage migration settings, either at the Hyper-V host level, or for each live migration instance.

To change live migration settings

1. Open Hyper-V Manager on the host, and then in the **Actions** pane, click **Hyper-V Settings**. Under **Server**, click **Live Migration**, and then click **Advanced Features**.
2. In the **Migration settings** page, under **Live migration settings**, do one of the following:
   - To disable faster live migration, click **Standard live migration**.
   - To use compression for faster live migration, click **Use compression**.
   - To use SMB for faster live migration, click **Use SMB as Transport**.

Monitoring and Reporting in VMM

The topics in this section provide information about how to integrate System Center 2012 – Virtual Machine Manager (VMM) with Operations Manager to monitor the health and performance of virtual machine hosts and their virtual machines, and to use the reporting functionality of Operations Manager.

Monitoring and reporting topics

- Configuring Operations Manager Integration with VMM

Provides procedures on how to create a connection between VMM and Operations Manager, how to enable Performance and Resource Optimization (PRO), and how to configure SQL Server Analysis Services (SSAS).

- Using Reporting in VMM

  Provides information about the reports that are available in VMM and how to view those reports.

Configuring Operations Manager Integration with VMM

You can connect Virtual Machine Manager (VMM) with Operations Manager to monitor the health and availability of the virtual machines and virtual machine hosts that VMM manages. You can also monitor health and availability of the VMM management server, the VMM database server, library servers, and VMM Self-Service Portal web servers, and see diagram views of the virtualized environment through the Operations console in Operations Manager.

Note

As of System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed.

For information about the versions of Operations Manager that VMM supports, see the followings:

- For System Center 2012 – Virtual Machine Manager or for System Center 2012 SP1: **System Requirements: Monitoring and Reporting in System Center 2012 and in System Center 2012 SP1**.
- For System Center 2012 R2 Virtual Machine Manager: **Preparing your environment for System Center 2012 R2 Virtual Machine Manager**.

When you integrate VMM with Operations Manager, the monitoring pack for VMM is automatically imported into Operations Manager, and in addition, the following features become available:

- Performance and Resource Optimization (PRO)
- Maintenance Mode integration
- Support for SQL Server Analysis Services (SSAS) and the reporting capabilities provided by SSAS

The following topics provide information about how to integrate VMM with Operations Manager:

- How to Connect VMM with Operations Manager
- How to Enable PRO Tips in VMM
- How to Configure SQL Server Analysis Services for VMM

How to Connect VMM with Operations Manager

You can connect Virtual Machine Manager (VMM) with Operations Manager so that they work in an integrated way. To connect VMM with Operations Manager, you must choose a version of Operations Manager that works with the version of VMM that you are using, as described in:

- For System Center 2012 – Virtual Machine Manager or for System Center 2012 SP1: **System Requirements: Monitoring and Reporting in System Center 2012 and in System Center 2012 SP1**.
- For System Center 2012 R2 Virtual Machine Manager: **Preparing your environment for System Center 2012 R2 Virtual Machine Manager**.

You must also configure the Operations Manager server to work with VMM.

Note

The version of the Operations Manager operations console that is installed on the VMM management server must match the version of Operations Manager with which you intend to integrate.

Prerequisites

Before you connect VMM with Operations Manager, perform the following actions:

1. Ensure that an appropriate version of Windows PowerShell is installed on all Operations Manager management servers:
   - **For System Center 2012**: Windows PowerShell 2.0
   - **For System Center 2012 SP1**: Windows PowerShell 3.0
   - **For System Center 2012 R2**: Windows PowerShell 3.0

   To determine which version of Windows PowerShell is on a server, run the following:

   Get-Host | Select-Object Version
2. Make sure that port 5724 is open between VMM and Operations Manager.
3. Install an Operations Manager Operations console on the VMM management server.
4. Install Operations Manager agents on the VMM management server and all hosts under management by VMM (managed hosts). For more information, see Operations Manager Agent Installation Methods.
5. Verify that the managed hosts on which you installed agents are visible in Operations Manager by performing the following actions:
   a. In the **Operations** console, click **Administration**.
   b. In the **Administration** pane, under **Device Management**, click **Agent Managed**. Verify that the expected hosts are listed.
   c. If you are running System Center 2012 SP1 or System Center 2012 R2, double-click a host in the list, click the **Security** tab, and then ensure that **Allow this agent to act as a proxy and discover managed objects on other computers** has been selected. Repeat this step for each of the hosts.

6. In Operations Manager, import the necessary management packs, as described in How to Import an Operations Manager Management Pack. Management packs, which in some cases are called “monitoring packs,” are available through the catalog at the Microsoft System Center Marketplace. The necessary management packs are as follows:
   - Windows Server Internet Information Services 2003
   - Management packs that are required by the management pack for Windows Server 2008 Internet Information Services 7:
     - Windows Server 2008 Operating System (Discovery)
     - Windows Server Operating System Library
   - Windows Server 2008 Internet Information Services 7
   - Windows Server Internet Information Services Library
   - SQL Server Core Library

Important

You can get the following three prerequisite management packs in one download from Windows Server Internet Information Services 7 Management Pack for System Center Operations Manager 2007:

- Microsoft.Windows.InternetInformationServices.2000.MP
- Microsoft.Windows.InternetInformationServices.2003.MP
- Microsoft.Windows.InternetInformationServices.2008.MP

These management packs allow you to maintain monitoring data from previous releases when you upgrade to System Center 2012 R2.

Note

After you connect to Operations Manager, if you are running System Center 2012 or System Center 2012 Service Pack 1 (SP1), and you update your VMM management packs, you must update the registry on your VMM management server. If you are running System Center 2012 R2, you do not need to update the registry.

Procedures in this topic

You can use procedures in this topic to perform the tasks appropriate for the software version that you are running. The following table provides details:

Software versions that the procedure applies to	Procedure link
System Center 2012, System Center 2012 SP1, System Center 2012 R2	Set up integration with Operations Manager
System Center 2012, System Center 2012 SP1	To enable storage monitoring and network monitoring
System Center 2012, System Center 2012 SP1	Update the registry on the VMM management server (for management pack updates with System Center 2012 or System Center 2012

Software versions that the procedure applies to	Procedure link
	SP1)
System Center 2012, System Center 2012 SP1, System Center 2012 R2	Update management packs
System Center 2012, System Center 2012 SP1, System Center 2012 R2	Remove an Operations Manager server connection

Account requirements You must be a member of the Administrator user role to set up and modify the connection to an Operations Manager server.

To set up integration with Operations Manager

1. In the VMM console, open the **Settings** workspace.
2. In the **Settings** pane, click **System Center Settings**, and then click **Operations Manager Server**.
3. On the **Home** tab, in the **Properties** group, click **Properties**.

   Note
   If the Operations Manager connection has already been established, clicking **Properties** opens the **Operation Manager Settings** dialog box. If this dialog box appears and does not describe the correct connection, remove the current connection before you enter the correct information.
4. Review the information in the **Introduction** page, and then click **Next**.
5. In the **Connection to Operations Manager** page, enter the **Server name** for your root management server (System Center Operations Manager 2007 R2) or a management server in the management group (System Center 2012 – Operations Manager), and select an account to use to connect. You can use the VMM server service account or specify a Run As account.

   Important
   This account must be a member of the Operations Manager Administrator role.
6. Select **Enable Performance and Resource Optimization (PRO)**, if desired.
7. Select **Enable maintenance mode integration with Operations Manager**, if desired.

   When hosts are placed in maintenance mode using the VMM management server, Operations Manager places them in maintenance mode as well. In this mode, the Operations Manager agent suppresses alerts, notifications, rules, monitors, automatic responses, state changes, and new alerts.

   Operations Manager automatically places virtual machines in maintenance mode when they are moved to the VMM library.

8. Click **Next**.
9. Enter credentials for Operations Manager to connect with the VMM management server, and then click **Next**.

   This account will be added to the Administrator user role in VMM.
10. Review the information in the **Summary** page, and click **Finish**.

    You can view the status of the new connection in the **Jobs** workspace.
11. With **System Center Settings** still selected, in the results pane, right-click **Operations Manager Server**, and then click **Properties**.

    The **Operation Manager Settings** dialog box opens.
12. Click the **Details** tab. Next to **Connection Status**, confirm that the connection is **OK**.

Verify that the integration is complete by opening the Operations console in Operations Manager and selecting the **Monitoring** workspace. In the navigation pane, review the following entries:

- **Virtual Machine Manager**

  Includes health and performance information for virtual machines, hosts, and VMM servers.
- **Virtual Machine Manager Views**

  Displays diagrams for managed systems.

  Note
  The diagrams themselves will not be available until several hours after you complete this procedure.

When you use the preceding procedure to set up integration with Operations Manager, the monitoring pack for Virtual Machine Manager is imported into Operations Manager. For more information about the monitoring pack, see Guide for System Center Monitoring Pack for System Center 2012 - Virtual Machine Manager.

If you are running System Center 2012 R2 and you set up integration with Operations Manager, the Fabric Health Dashboard is also imported into Operations Manager. For more information about the Fabric Health Dashboard, see Fabric Monitoring.

To enable storage monitoring and network monitoring

Note
The following procedures for enabling storage monitoring and network monitoring apply to System Center 2012 and System Center 2012 SP1 only. In System Center 2012 R2, storage monitoring and network monitoring are automatically enabled.

To enable storage monitoring in an English environment with System Center 2012 or System Center 2012 SP1

1. Open the Operations console.
2. Import the following management packs from the '\\<*Operations Manager installation*>\ManagementPacks' folder:
   - Microsoft.SystemCenter.VirtualMachineManager.Storage.Library
   - Microsoft.SystemCenter.VirtualMachineManager.Storage.2012.Discovery.mp
   - Microsoft.SystemCenter.VirtualMachineManager.Storage.2012.Monitoring.mp
   - Microsoft.SystemCenter.VirtualMachineManager.Storage.Dashboard.mpb

To enable storage monitoring in a non-English environment with System Center 2012 or System Center 2012 SP1

1. Open the Operations console.
2. Import the following management packs from the '\\<*Operations Manager installation*>\Setup\AMD64\MPLP' folder:
   - Microsoft.SystemCenter.VirtualMachineManager.Storage.Library.*.mp
   - Microsoft.SystemCenter.VirtualMachineManager.Storage.2012.Discovery.*.mp
   - Microsoft.SystemCenter.VirtualMachineManager.Storage.2012.Monitoring.*.mp
   - Microsoft.SystemCenter.VirtualMachineManager.Storage.Dashboard.*.mp

To enable network monitoring in a non-English environment with System Center 2012 or System Center 2012 SP1

1. Open the Operations console.

   Note
   The following steps apply to a non-English environment only. In an English environment, network monitoring is automatically enabled.
2. Import the following management pack from the Operations Manager installation folder:

   Setup\AMD64\MPLP\Microsoft.SystemCenter.VirtualMachineManager.Network.Dashboard.*.mp

To update the registry on the VMM management server in System Center 2012 or System Center 2012 SP1

1. To get the version number of the VMM management pack, check the most recent version of the Guide for System Center Monitoring Pack for System Center 2012 – Virtual Machine Manager.

   You can see the current version number of the monitoring pack in the Operations console. Open the **Administration** workspace. In the Administration pane, click **Management Packs**. Scroll down to find the VMM monitoring packs, such as **System Center 2012 Virtual Machine Manager Discovery**.

Note

If you are running VMM in System Center 2012 R2, this procedure is not necessary. Instead, follow the steps in Update management packs, later in this topic.

2. On the VMM management server, click **Start**, type **regedit** in the **Search programs and files** text box or in a Command Prompt window, and then press Enter.

   If the **User Account Control** dialog box appears, click **Yes** to continue.

   Caution

   Serious problems might occur if you modify the registry incorrectly. We recommend that you back up the registry before proceeding. Windows Server Backup can help you to perform backup tasks. For information about Windows Server Backup, see Backing Up Your Server.

3. In Registry Editor, locate the following registry key:

   `HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Microsoft System Center Virtual Machine Manager Server/Setup`

4. Under the key, if necessary, update the string value `CompatibleMPVersion` to the new version number, and then close Registry Editor.

To update management packs

1. If you are running VMM in System Center 2012 R2, skip to the next step. If you are running VMM in System Center 2012 or System Center 2012 SP1, on the VMM management server, follow the preceding procedure to update the registry to reflect the version number of the new management pack files. Then restart the System Center Virtual Machine Manager service.

   Note

   To obtain the version number of the monitoring pack, check the most recent version of the Guide for System Center Monitoring Pack for System Center 2012 – Virtual Machine Manager.

2. On the VMM management server, open the management packs directory. By default, the directory location is C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager\ManagementPacks.
3. Back up the existing .mp files.
4. Extract the new .mp files to the management pack directory, overwriting the existing .mp files.
5. If you have already integrated Operations Manager with VMM, in the VMM console, in the **Settings** workspace, remove the Operations Manager server by using the procedure in this topic.

6. Connect to the Operations Manager server, by using the procedure in this topic.

After the connection has been set up, open the **Settings** workspace. In the **Settings** pane, click **System Center Settings**. In the results pane, right-click **Operations Manager Server**, and then click **Properties**. On the **Management Pack** page, verify the installed version of the management packs.

To remove an Operations Manager server connection

1. In the VMM console, open the **Settings** workspace.
2. In the **Settings** pane, click **System Center Settings**, right-click **Operations Manager Server**, and then click **Remove**.

   When prompted, verify that you want to remove the server.

You can check the progress of the removal in the **Jobs** workspace.

Note
The VMM management packs are not removed from Operations Manager, but any Connectors that have been added are removed. (A Connector is a custom service or program that makes it possible for Operations Manager to communicate with other software.)

If you want to reconnect VMM to the Operations Manager server, see To set up integration with Operations Manager in this topic.

See Also

Configuring Operations Manager Integration with VMM

How to Enable PRO Tips in VMM

System Center 2012 – Virtual Machine Manager (VMM) supports Performance and Resource Optimization (PRO). To implement PRO, you need to establish a connection with a root management server (System Center Operations Manager 2007 R2) or a management server in the management group (System Center 2012 – Operations Manager), as detailed in How to Connect VMM with Operations Manager, and then enable PRO.

Note
In System Center 2012 – Virtual Machine Manager, Dynamic Optimization replaces the host load balancing that is performed for PRO by the PRO CPU Utilization and PRO Memory Utilization monitors in VMM 2008 R2. System Center 2012 –
Virtual Machine Manager includes default PRO monitors for dynamic memory to monitor

virtual machine dynamic memory allocation issues and maximum virtual machine memory aggregations on Hyper-V hosts. For more information, see Configuring Dynamic Optimization and Power Optimization in VMM and the VMM Management Pack documentation.

You can enable PRO when you first establish the connection with Operations Manager or use this procedure to enable it later.

Account requirements You must be a member of the Administrator user role to set up and modify the connection to an Operations Manager server.

To enable Performance and Resource Optimization

1. In the VMM console, open the **Settings** workspace.
2. In the **Settings** pane, click **System Center Settings**, and then click **Operations Manager Server**.
3. On the **Home** tab, in the **Properties** group, click **Properties**.
4. In the **Details** page, under **Connection Settings**, select **Enable Performance and Resource Optimization (PRO)**, and then click **OK**.

If you have an Operations Manager agent installed on the VMM management server, as recommended, you can test whether PRO Tips are working by clicking **Test PRO** in the **Operations Manager Settings** dialog box. Check on the result of your test PRO Tip either in the **Jobs** workspace in the VMM console or in the Operations console in Operations Manager.

Note
Allow up to ten minutes before using **Test PRO**.

How to Configure SQL Server Analysis Services for VMM

You can integrate Virtual Machine Manager (VMM) with SQL Server Analysis Service (SSAS) in order to provide forecasting reports. Be sure that SQL Analysis Services are installed on the Operations Manager Reporting server.

Before you enable SSAS, you need to connect to an Operations Manager management server, as described in How to Connect VMM with Operations Manager. Also, before you use SSAS, it is strongly recommended that you apply the latest Update Rollup for VMM that is available from Microsoft Support.

Important
SSAS requires Analysis Management Objects (AMO) be installed on the VMM management server. To download AMO, see the Microsoft SQL Server 2008 Feature

Pack, Microsoft SQL Server 2008 R2 Feature Pack, or Microsoft SQL Server 2012 Feature Pack.

Account requirements You must be a member of the Administrator user role to configure SSAS.

To configure SQL Server Analysis Service

1. In the VMM console, open the **Settings** workspace.
2. In the **Settings** pane, click **System Center Settings**, and then click **Operations Manager Server**.
3. On the **Home** tab, in the **Properties** group, click **Properties** to open the **Operations Manager Settings** dialog box.
4. On the **SQL Server Analysis Services** page, click **Enable SSAS**.
5. Enter the **SSAS server**, **SSAS instance**, and SSAS **Port**.

   The instance name must be the same as the SQL Server Reporting Services, by default MSSQLSERVER.

   The default port is 0.

   Important
   Make sure that SQL Server Reporting Services allows reports access using default port 80 and has HTTP access to reports.
6. Select either a Run As account or enter a user name and password, and then click **OK**.

   This user must belong to the Operations Manager Report Security Administrator profile.

Using Reporting in VMM

After you connect Virtual Machine Manager (VMM) with Operations Manager, you can create and view reports relating to VMM managed components, including virtual machine hosts, virtual machines, and VMM-related servers (for example, library servers.)

Note
For information about connecting VMM to Operations Manager, see How to Connect VMM with Operations Manager.

You can view reports in the **Reporting** workspace in Operations Manager, or by using a web browser and entering this address:

```
http[s]://<OpsMgrReportServer>[:<port>]/<reports>
```

- `<OpsMgrReportServer>` is the reporting server
- `<port>` is 80 for http and 443 for https, by default
- `<reports>` is the reporting server virtual directory, by default, `reports`

You can view the following preconfigured reports for VMM managed components.

Note

To use the forecasting reports, SQL Server Analysis Services must be installed on the Operations Manager Reporting server. For more information, see How to Configure SQL Server Analysis Services for VMM.

Report	Description
Capacity Utilization	Details usage for virtual machine hosts and other objects. This report provides an overview of how capacity is being used in your datacenter. This information can inform decisions about how many systems you need to support your virtual machines.
Chargeback	Provides information to calculate chargeback to cost centers for virtual machines. You can set up this report by Cost Center grouping to summarize CPU, memory, disk, and network usage for virtual machines within your cost centers. The cost center is a property of virtual machines, which can also be set on virtual machine templates. **Note** • This report is available in VMM in System Center 2012 Service Pack 1 (SP1) and System Center 2012 only. • In System Center 2012 R2 and System Center 2012 Service Pack 1 (SP1), other methods for creating chargeback reports are available. For more information, see Installing and Configuring Chargeback Reports in System Center 2012 - Service Manager and Chargeback: A scenario example.
Host Group Forecasting	Predicts host activity based on history of disk space, memory, disk IO, network IO, and CPU usage.
Host Utilization	Shows the number of virtual machines that are running on each host and average usage, along with total or maximum values for host processors, memory, and disk space.
Host Utilization Growth	Shows the percentage change in resource

Report	Description
	usage and the number of virtual machines that are running on selected hosts during a specified time period.
Power Savings	Shows how much power is saved through Power Optimization. You can view total hours of processor power saved for a date range and host group, as well as detailed information for each host in a host group. For more information about Power Optimization, see Configuring Dynamic Optimization and Power Optimization in VMM.
SAN Usage Forecasting	Predicts SAN usage based on history.
Virtual Machine Allocation	Provides information about allocation of virtual machines.
Virtual Machine Utilization	Provides information about resource utilization by virtual machines, including average usage and total or maximum values for virtual machine processors, memory, and disk space.
Virtualization Candidates	Helps identify physical computers that are good candidates for conversion to virtual machines. You can use the Virtualization Candidates report to identify little-used servers and display average values for a set of commonly requested performance counters for CPU, memory, and disk usage, along with hardware configurations, including processor speed, number of processors, and total RAM. You can limit the report to computers that meet specified CPU and RAM requirements, and you can sort the results by selected columns in the report.

You can also design your own reports.

See Also

Configuring Operations Manager Integration with VMM

Performing Maintenance Tasks in VMM

The procedures in this section describe how to perform common maintenance tasks in System Center 2012 – Virtual Machine Manager (VMM).

Maintenance topics

- How to Create and Assign a Servicing Window in VMM

  Describes how to create a user-defined time period to indicate when an object (for example, a host) is available to be taken offline for maintenance.
- How to Place a Host in Maintenance Mode in VMM

  Describes how to use maintenance mode to move or save virtual machines on a host before taking the host offline for maintenance.
- Back Up and Restore Virtual Machine Manager

  Describes how to backup and restore the VMM environment.

How to Create and Assign a Servicing Window in VMM

Servicing windows provide a method for scheduling servicing outside System Center 2012 – Virtual Machine Manager (VMM). In VMM, you can associate a servicing window with individual hosts, virtual machines, or services. Before using other applications to schedule maintenance tasks, you can use Windows PowerShell scripts or custom applications to query the object and determines if it is currently in a servicing window. Servicing windows do not interfere with the regular use and functionality of VMM.

To create a servicing window

1. In the **Settings** workspace, on the **Home** tab, in the **Create** group, click **Create Servicing Window**.
2. In the **New Servicing Window** dialog box, enter a name and optional description for the servicing window.
3. In **Category**, enter or select the category of servicing window.
4. In **Start time**, enter the date, time of day, and time zone for the maintenance window.
5. In **Duration**, specify the number of hours or minutes in the servicing window.
6. Under **Recurrence pattern**, select the frequency (**Daily**, **Weekly**, or **Monthly**), and then schedule the occurrences within that frequency.
   - To configure a daily servicing window, click **Daily**. Then, either click **Every** and enter the number of days between servicing, or click **Every weekday** to configure daily servicing.

- To configure a weekly servicing window, click **Weekly**. In **Recur every**, enter a number to specify the number of weeks between servicing. For example, enter 2 to configure servicing every other week. Finally, in **weeks on**, select each day on which to perform servicing.
- To configure a monthly servicing window, click **Monthly**, and then use one of the following methods to configure the monthly servicing window.

  Click **Day**, enter a number to indicate which day of the month, and in **of every**, enter a number to indicate the number of months between servicing. For example, you might configure a servicing window to be performed on the first day (day 1) of each quarter (every 3 months).

  Click second option (beginning with **The**). Select the week of the month (**first**, **second**, **third**, **fourth**, or **last**). Select a day of the week. Then, in **of every**, specify the number of months between servicing. For example, you might specify the second Tuesday of every month (every 1 months).

7. Click **OK** to save your servicing window.

   Note
   On the **Home** tab, in the **Properties** group, click **Properties** to modify a servicing window.

After you save the new servicing window, you can view it by clicking the **Servicing Windows** node on the **Settings** pane.

Use the following procedure to add a servicing window to a host. You can perform the same procedure on a virtual.

To add a servicing window to a host

1. In the **Fabric** workspace, on the **Fabric** pane, expand **Servers**, expand **All Hosts**, and optionally navigate to the host group that contains the host.
2. On the **Hosts** pane, click the host.
3. On the **Host** tab, in the **Properties** group, click **Properties**.

   The host properties dialog box opens.
4. On the **Servicing Windows** page, click **Manage**.

   The **Manage the list of Servicing Windows** dialog box opens.
5. Under **Available servicing windows**, click the servicing window that you want to add to the host, and then click **Add**.

   The selected servicing window moves to the **Selected servicing windows** list.
6. Click **OK** to add the servicing window and click **OK** again to save the updated host properties.

How to Place a Host in Maintenance Mode in VMM

In System Center 2012 – Virtual Machine Manager (VMM), you can start maintenance mode for a virtual machine host anytime that you need to perform maintenance tasks on the physical host, such as applying security updates or replacing hardware on the physical host computer. You can place Hyper-V hosts, VMware ESX hosts, and Citrix XenServer hosts that are managed by VMM into maintenance mode.

When you start maintenance mode on a host, you can do one of the following:

- Place all running virtual machines into a saved state.
- On a host cluster that is capable of live migration (including Citrix XenMotion and VMware vMotion), move all highly available virtual machines to other hosts in the cluster.

Caution

Placing a running virtual machine in a saved state causes a loss of service to any users of that virtual machine.

Note

For ESX hosts, if the VMware Distributed Resources Scheduler is not configured, all virtual machines on the host must be either manually shut down or moved to another host to successfully start maintenance mode on an ESX host.

When a host is in maintenance mode, the following restrictions are placed on the host:

- Virtual machines cannot be created on the host.
- Virtual machines cannot be moved to the host.
- The host has a zero rating and cannot be selected for placement.
- The host is excluded from Dynamic Optimization.

Note

If VMM is integrated with Operations Manager, when a host is placed in maintenance mode in VMM, Operations Manager also places the host into maintenance mode. In maintenance mode, the Operations Manager agent suppresses alerts, notifications, rules, monitors, automatic responses, state changes, and new alerts.

To start maintenance mode on a host

1. In the VMM console, open the **Fabric** workspace.
2. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
3. In the **Fabric** pane, expand **Servers**, and then expand **All Hosts**.
4. In the **Hosts** pane, locate and then click the host that you want to place in maintenance mode.
5. On the **Host** tab, in the **Host** group, click **Start Maintenance Mode**.
6. In the **Start Maintenance Mode** dialog box, select either of the following, and then click

OK.

- Move all virtual machines to other hosts in the cluster
- Place all running virtual machines into a saved state.

Tip
When a host is in maintenance mode, the **Host Status** for the host displays as **In Maintenance Mode** in the **Hosts** pane in the **Fabric** workspace.

To stop maintenance mode on a host

1. In the VMM console, open the **Fabric** workspace.
2. On the **Home** tab, in the **Show** group, click **Fabric Resources**.
3. In the **Fabric** pane, expand **Servers**, and then expand **All Hosts**.
4. In the **Hosts** pane, locate and then click the host that you want to bring out of maintenance mode.
5. On the **Host** tab, in the **Host** group, click **Stop Maintenance Mode**.

Important
When you bring a host out of maintenance mode, VMM does not automatically restart the virtual machines and does not automatically move any migrated virtual machines back on to the host.

Back Up and Restore Virtual Machine Manager

It is important to develop and implement a comprehensive backup plan for protecting all of your Virtual Machine Manager (VMM) data, including data on the VMM management server, hosts, virtual machines, and library servers. In case of a failure in the VMM environment, such as a failure of the management server, you have to restore that server, so that it regains the functionality that existed prior to the failure. Ideally, the important data in the VMM environment has been backed up, such as the VMM database, to minimize data loss. This section describes various backup processes and recommendations, and the data recovery process.

Important
Do not use checkpoints for disaster recovery. Checkpoints do not create full duplicates of the hard disk contents nor do they copy data to a separate volume. A checkpoint can serve as temporary backup before updating an operating system on a virtual machine so that you can roll back the update if the update has any adverse effects. You should use a backup application to back up and recover your data in case of catastrophic data loss.

If Data Protection Manager (DPM) is deployed in your environment and is used for backing up VMM, then you can use DPM to restore the data that was backed up. For more information about using DPM for backup and restore in VMM, see Data Protection Manager.

Data such as Remote Access Authorization (RAA) passwords and the product key can be entered when you re-install VMM. However, some encrypted data such as Virtual Machine Roles cannot be re-entered, and if VMM is using the Data Protection application programming interface (DPAPI) to store that data – it will be lost if the VMM management server fails.

Create a backup plan

The main goal of an effective backup plan is to be able to recover your environment quickly while minimizing data loss in case of a failure. Key candidates for protection are files that change frequently or that are accessed frequently. You must plan to back up the following:

- VMM management server
  - SQL Server database (user accounts, configuration data)
- Hosts
  - Virtual machines
  - Host configuration data (virtual networks)
- Library server data
  - Virtual hard disks (VHDs)
  - ISO images

How to back up Virtual Machine Manager

The following section describes how to back up your VMM environment.

Back up the VMM database

The VMM database contains information such as configurations, service templates, profiles, virtual machine templates, services, scale-out services, and other critical data that is required for VMM to function correctly. To back up the VMM database regularly is an important maintenance task.

The VMM database can be stored on the VMM management server itself or on a separate server running Microsoft SQL Server. To back up the VMM database, you can use one of the following, or use any other tools that are used in your environment:

- The VMM console
- A Windows PowerShell cmdlet
- SQL Server tools. For more information, see Create a Full Database Backup (SQL Server).
- The SCVMMRecover.exe tool (available on the VMM management server): For more information, see How to Back up and Restore the VMM Database (using the SCVMMRecover.exe tool).

Important

To back up the VMM database, you must be a member of the Administrator user role.

To back up the VMM database by using the VMM console

1. In the **Administration** view, in the **Actions** pane, click **Back up Virtual Machine Manager**.
2. Select a backup destination folder that is not a root directory and that SQL Server can access.

To back up the VMM database by using a cmdlet in Windows PowerShell

1. Start a Windows PowerShell session.
2. At the Windows PowerShell command prompt, enter the following cmdlet:

```
get-vmmserver <VMM management server name> | backup-vmmserver -Path
<BackupFileDir>
```

In addition to backing up the database, we recommend that you create a system state backup of the VMM management server so that you can re-create the server with the same security identifier (SID) in case of a catastrophic data loss. The SID is an integral part of how VMM is authorized on virtual machine hosts.

Back up hosts and virtual machines

Virtual machine hosts are Microsoft Hyper-V Servers, Hyper-V role in Windows Server, Citrix XenServer, VMware ESXi hosts, and host clusters on which virtual machines and services are deployed. To back up virtual machine hosts and clusters, use Microsoft System Center Data Protection Manager (DPM) or another backup application that takes advantage of Volume Shadow Copy Service (VSS) to copy host and virtual machine data to a remote file server share.

Important

We recommend that you back up virtual machine configuration files (.vmc) daily.

Inventory your hosts, and then back up all of the hosted virtual machines. To get the list of hosts that are being managed by VMM, run the following cmdlet from a Windows PowerShell command line:

```
$vmhost = get-vmmserver <VMM management server name> | get-vmhost
```

Back up all of the configuration and resource files on each VMM host by using backup software that supports the Virtual Server VSS writer. Backup software that supports Microsoft Virtual Server minimizes the number of steps required to archive and restore virtual servers, minimizes downtime, and ensures consistency of the data that is being archived or restored. For more information, see Backing up and Restoring Virtual Server and Planning to Back up and Restore Data.

Back up library servers

The VMM library is a catalog of resources that provides access to file-based resources, such as virtual hard disks, virtual floppy disks, ISO images, scripts, driver files, and application packages that are stored on library servers, and to resources, which are not file-based, such as virtual machine and service templates and profiles that reside in the VMM database.

To back up the data on library servers, use System Center Data Protection Manager (DPM) or another backup application that takes advantage of Volume Shadow Copy Service (VSS) to copy host and virtual machine data to a remote file server share. As with VMM hosts, begin by inventorying your library servers. To get the list of library servers that are managed by VMM, run the following cmdlet from the Windows PowerShell command line:

```
$libraryservers = get-vmmserver <VMM management server name> | get-libraryserver
```

Much of the library data is located in the VMM database. For example, templates, hardware profiles, and operating system profiles are not represented on the library server. Back up all files on library shares to a shared folder on a remote file server, including .vhd, .vfd, .iso, .inf, .vmx, .ps1, .vmc, and .vsv files.

Back up VMM private clouds

To back up VMM private clouds, you can use Windows Server 2012 Hyper-V Replica. System Center 2012 – Virtual Machine Manager (VMM) clouds can be protected through automating the replication of the virtual machines that compose them at a secondary location. Windows Server 2012 Hyper-V Replica provides the ongoing asynchronous replication of each virtual machine, and Hyper-V Recovery Manager monitors and coordinates the replication process.

Back up registry keys

VMM uses various registry keys to store settings that control the behavior of VMM functionality. Settings values are stored in the following registry key and its subkeys, such as PerformanceTuning, Debugging, Placement, ServiceCreation, Sql, and Library: **HKLM\Software\Microsoft\Microsoft System Center Virtual Machine Manager Server\Settings**. You should back up this entire section of the registry so you can later mirror the original configuration accurately.

To back up registry keys, you can use the Regedit **Export** function, or any other tool that is used in your environment to back up registry keys.

Back up encryption keys in Active Directory Domain Services

If distributed key management (DKM) is configured to store VMM-related encryption keys in Active Directory Domain Services (AD DS), then ensure that Active Directory is backed up on a regular basis in your environment.

Back up non-VMM managed credentials

Some credentials that are related to VMM are managed by the Windows Credential Manager on the VMM management server. To access the Credential Manager, in Control Panel, select **All Control Panel Items**, and then click **Credential Manager**. Click **Back up Credentials** to back up any VMM-related credentials.

Back up non-Microsoft user interface add-ins and other non-Microsoft applications

Non-Microsoft user interface (UI) add-ins can be integrated with the VMM console to extend the functionality of the console. The location of the data that is used by a UI add-in can vary. It might be stored on the local server or on a remote computer, and it might be configured with a specific set of permissions. Therefore, you have to consult the backup guidelines of your specific UI add-in.

For any other non-Microsoft applications, refer to the applications' specific backup guidelines.

How to restore the VMM environment

The following section describes the procedures that are necessary for data recovery and for reassociating servers in your VMM environment.

Restore a VMM management server

If you have regularly backed up important data in the VMM environment, then follow the general process to restore a VMM management server that has failed:

1. Ensure that the hardware on which you intend to re-install VMM meets all requirements as described in System Requirements for System Center 2012 – Virtual Machine Manager.
2. Perform a system state restore: If you restore the system state to the original hardware, the SID of the VMM server remains the same.
3. Restore the VMM database to the SQL Server database if necessary.
4. Install VMM while using the backed-up database.
5. Perform any post-restore tasks that are needed in the VMM deployment.

The steps that you must perform to restore a VMM management server depend on whether you restore the VMM management server to the same physical computer or to a different computer. The initial steps are similar. However, if you restore VMM to a new computer, then you must perform some additional steps.

Restore the VMM database

To restore the VMM database to the VMM environment, you have to point to the backed-up database during the re-installation of VMM. For more information about using an existing database during the VMM setup process, see How to Install a VMM Management Server.

If you must first restore the database to the SQL Server, then use the appropriate method depending on the method that you used to back up the database.

To restore the SQL Server database on a VMM management server, you can open an elevated command prompt, navigate to the <*VMM installation location*>\bin folder, and then run the **SCVMMRecover.exe** as follows.

```
SCVMMRecover [-Path <location>] [-Confirm]

[-Path <location>]      Location where VMM database backup resides.

[-Confirm]              VMM database recovery confirmation.
```

<location> refers to the folder or share location of the backup file that you created, and it must include the name of the backup file (including the .bak extension).

To use SQL Server to restore the VMM database, see Restore and Recovery Overview (SQL Server).

Or, use any other tool that is appropriate to the method that you used to back up the VMM databases.

Recover data on the same computer

If you restore a VMM management server onto the same physical computer with the same SID as before the data loss, you must perform the following manual steps:

1. Remove any hosts or virtual machines from the VMM console that were removed after the last backup. If a host has been removed after the last backup, then it appears as "Not Responding" and all virtual machines on the host appear as "Host Not Responding". If the host is present but a virtual machine has been removed after the last backup, then the virtual machine appears as "Missing."
2. Add any hosts or virtual machines that were added after the last backup.

Recover data on a different computer

If you restore a VMM management server onto a different physical computer with a different SID, then you must perform the steps described in the previous section, and in addition, you have to reassociate each of the hosts to the new VMM management server. Until you perform the following additional steps, the hosts remain mapped to the original computer's machine account.

To reassociate a host to the new VMM management server

1. Open the VMM console.
2. Click **Administration**, and then click **Managed Computers** to identify all of the managed computers that are marked as "Access Denied."
3. Right-click each managed computer, click **Reassociate**, and then provide the administrative credentials.
4. If you are restoring a VMM management server that was also a library server, then the new computer lists the original VMM server as the default library server. From the **Library** view, remove the original library server, and then add the new computer as a

library server.

5. If necessary, reassociate servers in the perimeter network (also known as DMZ, demilitarized zone, and screened subnet).

Reassociate servers in a perimeter network

Hosts on a perimeter network require additional recovery steps. Initially, servers on a perimeter network appear as "Not Responding." To reassociate servers on a perimeter network, you must perform the following steps.

To reassociate servers in a perimeter network

1. Sign in to each server on the perimeter network, and then locate the VMM account. The VMM account is a local administrator account with a 10-character user name of **scvmm** plus 5 random characters.
2. Change the password of the VMM account on each server.
3. On the VMM management server, in the **Host Properties** dialog box, click the **Options** tab, and then assign each server the same password that you created in step 2.

Restore hosts and library servers

To restore a host server after data loss, use the Virtual Server VSS writer to recover the server and all the virtual machines.

To restore a library server after data loss, restore the file server shares, and then restore the data back onto the shares. For more information, see Planning to Back Up and Restore Data.

After you restore the VMM management server, the VMM database, the operating system, and system state to either type of server, the library servers are listed in the VMM console. However, you must use the VMM console to reassociate them with the physical library servers as follows.

To reassociate library servers with physical computers

1. If the newly restored computer has the same name as the original computer, install the Virtual Machine Manager agent locally on that computer and then reassociate that computer with the VMM management server.
2. If the newly restored computer has a different name than the original computer, use the VMM console to remove the original computer from the list of hosts that are managed by VMM, and then add the new computer as a host.

For more information, see How to Reassociate a Managed Computer with Another Virtual Machine Manager Server.

Restore registry keys

To restore registry keys that were previously backed up, you can use the Regedit **Import** function or any other tool that is used in your environment to back up registry keys.

Restore Active Directory objects

If DKM is enabled in your VMM environment, then VMM stores some data in Active Directory, such as RAA passwords, product key information, and Virtual Machine Role data. After re-installing VMM, it is possible to re-enter some of the data that was stored in Active Directory, such as RAA passwords and product key information if needed. After you re-installed VMM and restored Active Directory if it was necessary, the data in Active Directory continues to be accessible to VMM.

Restore non-VMM managed credentials

Open the Windows Credential Manager. In Control Panel, select **All Control Panel Items**, and then click **Credential Manager**. Click **Restore Credentials** to restore any VMM-related credentials.

Post-restore tasks

Depending on your VMM configuration, you must do some or all of the following tasks after you restore the VMM data and re-install VMM.

Reassociate virtual machine hosts and library servers

In some restore scenarios, you must reassociate virtual machine hosts and VMM library servers with the VMM management server after restore is complete.

For more information, see How to Reassociate a Host or Library Server.

Restore non-Microsoft user interface add-ins

To restore any non-Microsoft user interface add-ins or any other non-Microsoft party applications, consult the respective application's restore guidelines.

Reinstall Windows Azure Pack

If Windows Azure Pack (WAP) was deployed in your environment to support tenants by using VMM, then you'll have to reinstall it after you restore the VMM environment. For more information about Windows Azure Pack for Windows Server, see Windows Azure Pack for Windows Server.

Install additional VMM consoles

If previously additional VMM consoles were installed, then you must re-install them on stand-alone servers.

For more information, see Installing and Opening the VMM Console.

Update Driver Packages

Driver packages that were previously added to the VMM library might have to be removed and be re-added to be discovered correctly.

For more information, see How to Add Driver Files to the VMM Library.

Update virtual machine templates

All virtual machine templates that were restored must correctly specify the virtual hard disk that contains the operating system.

To update a virtual machine template

1. In the VMM console, open the **Library** workspace, expand **Templates**, and then click **VM Templates**.
2. In the **Templates** pane, right-click the virtual machine template that you want to update, click **Properties**, and click the **Hardware Configuration** page to update the settings.

Restore Windows Azure Hyper-V Recovery Manager

If Windows Azure Hyper-V Recovery Manager is implemented in the VMM environment, then you must perform a few steps to restore the Windows Azure Hyper-V Recovery Manager Provider.

For more information, see How to Restore Windows Azure Hyper-V Recovery Manager Provider.

Update Certificates

Any VMM-related certificates on hosts must be updated with the information of the new VMM management server.

Account control lists

After re-installing VMM, VMM updates the account control lists (ACLs) that became outdated due to the failure. No further intervention is required.

Remote Console in System Center 2012 R2

Remote Console is a feature that was introduced in System Center 2012 R2. Remote Console provides tenants with the ability to access the console of their virtual machines in scenarios when other remote tools (or Remote Desktop) are unavailable. Tenants can use Remote Console to access virtual machines when the virtual machine is on an isolated network, an untrusted network, or across the Internet.

Remote Console needs the following to run:

- Microsoft® Hyper-V® Server 2012 R2
- System Center 2012 R2 Virtual Machine Manager
- System Center 2012 R2 Service Provider Foundation
- Windows Azure Pack for Windows Server

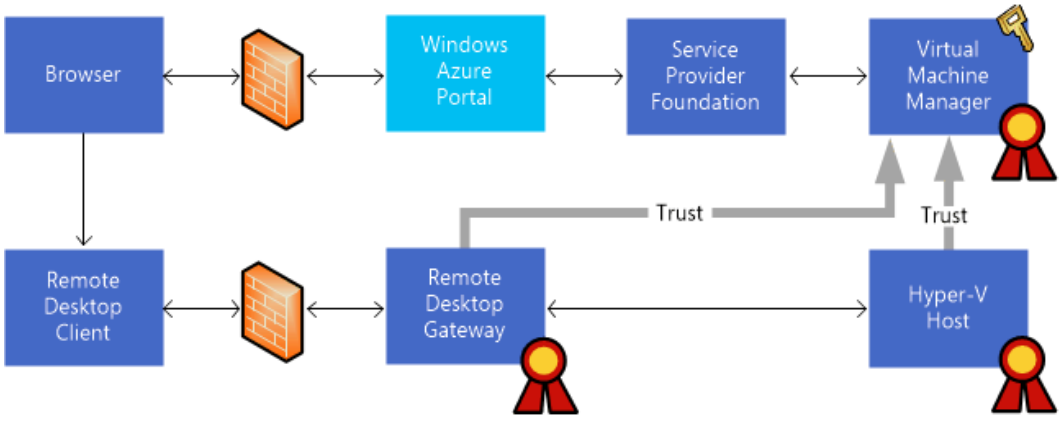
Note
Tenants need a client computer that supports Remote Desktop Protocol 8.1. For example, users who are running Windows 8 must upgrade to Windows 8.1. In addition, clients using Windows 7 SP1 must install KB2830477.

In this release, Remote Console supports limited functionality. Features such as the clipboard, sound, printer redirection, and drive mapping are not supported. Remote Console functions in a manner that is similar to the keyboard, video, and mouse (KVM) connection that is used by physical computers.

User authentication

Hyper-V in Windows Server 2012 R2 supports certificate-based authentication, which is used to make sure that tenants only access virtual machines that are assigned to them. The Windows Azure Pack for Windows Server web portal, Service Provider Foundation, and Virtual Machine Manager (VMM) authenticate and authorize access to virtual machines and provide a token that the Hyper-V host uses to grant access to a single virtual machine.

The following diagram illustrates the components that are needed for Remote Console access when tenants are accessing a virtual machine across an untrusted network such as the Internet. Remote Desktop Gateway (RD Gateway) is omitted if this environment is deployed in a corporate network.



The private and public keys for a certificate are used to establish a trust relationship. The following sections describe how to create the required certificates.

Creating a certificate for remote access

A certificate is used to create a trust relationship between RD Gateway server, the Hyper-V hosts, and VMM. The certificate allows RD Gateway and the Hyper-V hosts to accept claims tokens that are issued by VMMRD Gateway. It is possible to use the same or different certificates for validation on RD Gateway and the Hyper-V hosts. Valid certificates must meet the following requirements:

1. The certificate must not be expired.
2. The Key Usage field must contain a digital signature.
3. The Enhanced Key Usage field must contain the following Client Authentication object identifier: (1.3.6.1.5.5.7.3.2)
4. The root certificates for the certification authority (CA) that issued the certificate must be installed in the Trusted Root Certification Authorities certificate store.
5. The cryptographic service provider for the certificate must support SHA256.

You can obtain a valid certificate from a commercial Certification Authority, an Enterprise Certification Authority, or using a self-signed certificate.

Note
You can obtain a valid certificate from a commercial certification authority, an enterprise certification authority, or by using a self-signed certificate. When you use a self-signed certificate, you must place the public key of the certificate in the Trusted Root Certification Authorities certificate store in RD Gateway and the Hyper-V hosts.

Using the MakeCert tool to create a test certificate

For testing purposes, you can use the MakeCert tool to create a self-signed certificate. MakeCert is part of the Windows SDK.

- To download the SDK, see Windows SDK for Windows 7.
- For more information, see MakeCert on the Windows Dev Center.

The following code provides an example for how to create a self-signed certificate:

```
makecert -n "CN=Remote Console Connect" -r -pe -a sha256 -e <mm/dd/yyyy> -len 2048 -sky signature -eku 1.3.6.1.5.5.7.3.2 -ss My -sy 24 "<CertificateName>.cer"
```

where:

-sky signature	Use for signing
-r	Create self-signed certificate
-n “CN=Remote Console Connect”	Subject name (Remote Console Connect)
-pe	Private key is exportable
-a sha256	algorithm
-len 2048	Key length

-e <mm/dd/yyyy>	Expiry date
-eku 1.3.6.1.5.5.7.3.2	Enhanced Key Usage (Client Authentication object identifier)
-ss My	Store private key in certificate store My
-sy 24	Cryptographic provider type (supports SHA256)
“<CertificateName>.cer”	Name for the public key

Using a certification authority

When you request a certificate from a certification authority, a certificate template .inf file similar to the following can be used with the Certreq tool. For more information, seeCertreq.

```
[Version]

Signature="$Windows NT$"

[NewRequest]

; Change to your,country code, company name and common name

Subject = "C=US, O=Contoso, CN=wap-rdg.contoso.com"

; Indicates both encryption and signing

KeySpec = 1

; Length of the public and private key, use 2048 or higher

KeyLength = 2048

; Certificate will be put into the local computer store

MachineKeySet = TRUE

PrivateKeyArchive = FALSE

RequestType = PKCS10

UserProtected = FALSE

; Allow the key to be shared between multiple computers

Exportable = TRUE

SMIME = False

UseExistingKeySet = FALSE

; ProviderName and ProviderType must be for a CSP that supports SHA256

ProviderName = "Microsoft Enhanced RSA and AES Cryptographic Provider"

ProviderType = 24

; KeyUsage must include DigitalSignature. 0xA0 also includes Key Encipherment

KeyUsage = 0xa0
```

```
[EnhancedKeyUsageExtension]

OID=1.3.6.1.5.5.7.3.2
```

You can validate that a certificate in a .pfx file meets algorithm and Enhanced Key Usage requirements by running the following Windows PowerShell script:

```
$cert = Get-PfxCertificate <cert.pfx>

if ($cert.PrivateKey.CspKeyContainerInfo.ProviderName -ne "Microsoft Enhanced RSA and AES Cryptographic Provider")

{

       Write-Warning "CSP may not support SHA256"

}

if (! (Test-Certificate $cert -EKU "1.3.6.1.5.5.7.3.2") )

{

       Write-Warning "Certificate is not valid"

}
```

Installing the certificate

Once the certificate has been created, you must then install it and configure Virtual Machine Manager to use the certificate to issue claims tokens. The private key for the certificate is then imported into the Virtual Machine Manager database. To do this, use the **Set-SCVMMServer** Windows PowerShell cmdlet, for example:

```
PS C:\> $mypwd = ConvertTo-SecureString "password" -AsPlainText -Force

PS C:\> $cert = Get-ChildItem .\RemoteConsoleConnect.pfx

PS C:\> $VMMServer = VMMServer01.Contoso.com

PS C:\> Set-SCVMMServer -VMConnectGatewayCertificatePassword $mypwd -VMConnectGatewayCertificatePath $cert -VMConnectHostIdentificationMode FQDN -VMConnectHyperVCertificatePassword $mypwd -VMConnectHyperVCertificatePath $cert -VMConnectTimeToLiveInMinutes 2 -VMMServer $VMMServer
```

In this example, the same certificate is used for RD Gateway and for the Hyper-V hosts, and tokens have a lifetime of two minutes. You can select a lifetime for tokens of 1 to 60 minutes.

You identify the host server by its Fully Qualified Domain Name (FQDN). Alternatively, hosts can be identified by IPv4 address, IPv6 address, and host name. The host identity is included in the Remote Desktop Protocol (RDP) file that is sent to tenants.

Note

`VMMServer01.Contoso.com` is used as the example host server name. Change this to your actual server name.

`RemoteConsoleConnect.pfx` is used to import the PFX file where the certificate keys are stored to the VMM database.

When each host is refreshed in Virtual Machine Manager, it installs the certificate in the Personal certificate store of the Hyper-V host and configures the Hyper-V host to validate tokens by using the certificate. You can use the following Windows PowerShell command to force a refresh of all Hyper-V hosts:

```
PS C:\> Get-SCVMHost -VMMServer "VMMServer01.Contoso.com" | Read-SCVMHost
```

Hyper-V hosts

When authenticating tokens, Hyper-V only accepts tokens that are signed by using specific certificates and hash algorithms. Virtual Machine Manager performs the required configuration for the Hyper-V hosts. Only Hyper-V in Windows Server 2012 R2 supports Remote Console functionality.

When you use a self-signed certificate, you must import the public key of the certificate to the Trusted Root Certification Authorities certificate store for the Hyper-V host. The following script provides an example of how to use Windows PowerShell to import the public key:

```
PS C:\> Import-Certificate -CertStoreLocation cert:\LocalMachine\Root -Filepath
"<certificate path>.cer"
```

You must restart the Hyper-V Virtual Machine Management service if you install a certificate after you configure Virtual Machine Manager.

You can verify that the Hyper-V host is correctly configured for Remote Console as follows:

1. Check that the certificate is in the Personal certificate store of the Hyper-V host and that it is trusted.
2. Check the hash configuration for the trusted issuer certificate.

The following script provides an example of how to use Windows PowerShell to check that the certificate is installed in the Personal certificate store of the Hyper-V host:

```
PS C:\> dir cert:\localmachine\My\ | Where-Object { $_.subject -eq "CN=Remote Console
Connect" }
```

The following script provides an example of how to use Windows PowerShell to check the hash configuration for the trusted issuer certificate:

```
PS C:\> $TSData = Get-WmiObject -computername $Server -NameSpace "root\virtualization\v2"
-Class "Msvm_TerminalServiceSettingData"
```

The **TrustedIssuerCertificateHashes** array must contain the certificate thumbprint that is used to connect Remote Console. The **AllowedHashAlgorithms** array must be empty or contain the SHA256 algorithm. When the array is empty, it defaults to SHA256 or SHA512.

Note

Virtual Machine Manager generates SHA256 tokens.

Remote Desktop Gateway

Remote Desktop Gateway (RD Gateway) can only be used for console access to virtual machines. When you configure RD Gateway, a configuration change occurs, which makes the gateway unusable for other purposes. The following tasks are completed when you configure RD Gateway:

1. Deploy RD Gateway and install the authentication plug-in.
2. Install the certificate.
3. Configure trusted issuer certificates (by using WMI).
4. Create a certificate for RD Gateway.

To support federated authentication, it is necessary to install the Microsoft System Center Virtual Machine Manager Console Connect Gateway onto RD Gateway server. Start by creating a virtual machine, then enable Remote Desktop Services.

Then install the System Center Virtual Machine Manager Console Connect Gateway component. You will find the installation binaries for this component in the following Virtual Machine Manager installation media folder: **CDLayout.EVAL\amd64\Setup\msi\RDGatewayFedAuth**. For a high availability configuration, install multiple quantities of RD Gatewaywith the Console Connect Gateway component behind a load balancer.

Next, import the public key of the certificate into the Personal certificate store on each RD Gateway server. You can accomplish this by using Windows PowerShell as shown in the following example:

```
PS C:\> Import-Certificate -CertStoreLocation cert:\LocalMachine\My -Filepath
"<certificate path>.cer"
```

If you are using a self-signed certificate, you must import the public key of the certificate into the Trusted Root Certification Authorities certificate store for the machine account. You can accomplish this by using Windows PowerShell as shown in the following example:

```
PS C:\> Import-Certificate -CertStoreLocation cert:\LocalMachine\Root -Filepath
"<certificate path>.cer"
```

When authenticating tokens, RD Gateway accepts only tokens that are signed by using specific certificates and hash algorithms. This configuration is performed by setting the **TrustedIssuerCertificateHashes** and **AllowedHashAlgorithms** properties in the WMI **FedAuthSettings** class. You must have administrative credentials to set these properties.

The **TrustedIssuerCertificateHashes** property is an array of certificate thumbprints that are stored in the RD Gateway server. You can use the following Windows PowerShell command to set the **TrustedIssuerCertificateHashes** property:

```
$Server = "rdgw.contoso.com"
$Thumbprint = "95442A6B58EB5E443313C1B4AFD2665991D354CA"
```

```
$TSData = Get-WmiObject -computername $Server -NameSpace "root\TSGatewayFedAuth2" -Class
"FedAuthSettings"
$TSData.TrustedIssuerCertificates = $Thumbprint
$TSData.Put()
```

The last step is to select or create a self-signed certificate for RD Gateway. To accomplish this, open RD Gateway Manager, right-click **Remote Desktop Gateway**, and click **Properties**. In the **Properties** dialog box, click the **SSL Certificate** tab.

This certificate is used by tenant client computers to verify the identity of the RD Gateway server. The CN name for the certificate must match the FQDN of the RD Gateway server. Open RD Gateway Manager and assign or create a self-signed certificate.

Note

Use a self-signed certificate only for testing. A self-signed certificate should never be used in a production deployment. Using a self-signed certificate also requires that the certificate is installed on every tenant computer that is connecting through the RD Gateway.

You can verify the configuration of RD Gateway by performing the following steps:

1. Make sure that RD Gateway is configured to use the Console Connect Gateway for authentication and authorization. You can accomplish this by using Windows PowerShell as shown in the following example:

   ```
   PS C:\> Get-WmiObject -Namespace root\CIMV2\TerminalServices -
   Class Win32_TSGatewayServerSettings
   ```

   Verify that the **AuthenticationPlugin** and **AuthorizationPlugin** properties are set to **FedAuthorizationPlugin**.
2. Make sure that a certificate has been installed in the Personal certificate store for the machine account. You can accomplish this by using Windows PowerShell as shown in the following example:

   ```
   PS C:\> dir cert:\localmachine\My\ | Where-Object { $_.subject -
   eq "CN=Remote Console Connect" }
   ```
3. Check the configuration of the Console Connect Gateway. You can accomplish this by using Windows PowerShell as shown in the following example:

   ```
   PS C:\> Get-WmiObject -computername $Server -NameSpace
   "root\TSGatewayFedAuth2" -Class "FedAuthSettings"
   ```

   The **TrustedIssuerCertificates** array must contain the certificate thumbprint for Console Connect Gateway.

Windows Azure Pack for Windows Server for Remote Console

You can enable access to Remote Console on a per plan basis through the Virtual Machine Clouds service in Windows Azure Pack for Windows Server. In the dashboard of the plan, select

the **Virtual Machine Clouds** under plan services, and select **Connect to the console of virtual machines** under additional settings.

If you have installed a Remote Desktop Gateway, read the procedure How to Configure Windows Azure Pack to use the Remote Desktop Gateway.

Security recommendations

We recommend that you perform the following tasks to improve security:

Name	Threat	Recommendation
Token Access	Access to My certificate store can be used to generate access tokens for any virtual machine.	Use Active Directory security groups to restrict access to the Virtual Machine Manager server generating tokens.
Token lifetime	The Remote Desktop Protocol (RDP) file contains the **EndpointFedAuth** token and possession of the RDP file allows access to the console of a specific virtual machine.	Configure a short expiration time for the token. One minute is the recommended expiration time. Use the **SetSCVMMServer** Windows PowerShell cmdlet to set the token lifetime.
Shared access	Another user requests and accesses the console session, which ends the existing session. This includes a host that accesses the console of a user who is signed in, and then gains access to tenant resources. Console sessions are similar to KVM sessions for physical hosts. A virtual machine session is available to all users who have been granted the Console Read or Console Read/Write operations privilege in the authorization policy. By default, this is granted to any Administrator.	Tennant Users: Do not remain signed in to a console session when not actively working. Ensure that the operating system locks after a short period of inactivity. Hosting service providers: Use authorization policies to restrict read and write access.
Malicious users	Malicious users can attempt to connect to ports through the RD Gateway when they are not	Configure Remote Desktop resource authorization policies in the RD Gateway server to

Name	Threat	Recommendation
	authorized. For example, a malicious user might attempt to connect to the RDP port on a Hyper-V host to try user name and password combinations.	block users from connecting directly to port 3389 on the Hyper-V server. Connections are needed only to port 2179. For more information, see Manage Remote Desktop Resource Allocation Policies Policies.
Man-in–the-middle attack	One security issue that Hyper-V was designed to address is better protection against “man-in-the-middle” attacks(also referred to as MITM). Use of trusted certificates to identify the Hyper-V host can help protect against MITM attacks. Hyper-V uses a single-port listener that utilizes trusted certificates for server authentication. Under certain circumstances, Hyper-V issues a self-signed certificate that is then used for server authentication. As an alternative to this approach, you can configure Hyper-V to use a different certificate, such as one issued by a certification authority (CA).	Use a Hyper-V host certificate with a valid certificate chain that is connected to a trusted root certificate. This prevents an error message that says the identity of the remote computer cannot be verified. For more information, see Configuring Certificates for Virtual Machine Connection.
Session snooping	When a console connection is active, it is possible for host staff to take a snapshot of the virtual machine and export the virtual machine to another server, or to collect thumbnail images of the console.	Use authorization policies to restrict read and write access. Disclose to tenants the situations in which your staff could access console sessions.
Network configuration	A malicious user can use properties in the RDP file to gain insight about a network configuration.	Determine if the host name or IP address should be used to connect to a server running Hyper-V. This information is

Name	Threat	Recommendation
		included in the RDP file that is sent to the service consumer. It is also in the certificate that is presented by the server running Hyper-V when the console connection is initiated. Set the network configuration to ensure that servers running Hyper-V are not directly accessible from the Internet or from a user's virtual machine. An IP address (in particular, an IPv6 address) reduces the amount of information that is disclosed.

See Also

How to Configure Windows Azure Pack to use the Remote Desktop Gateway

How to Configure Windows Azure Pack to use the Remote Desktop Gateway

The following procedure will show you how to configure Windows Azure Pack to use the Remote Desktop Gateway (RD Gateway).

To configure Windows Azure Pack for the RD Gateway

1. Log into the WAP Service Management Portal with administrative credentials.
2. From the home page, select **VM Clouds**.
3. Select the **Clouds** tab.
4. Select your VMM server and then click **Edit**.
5. In the **Virtual machine cloud provider properties** page, do the following:
   a. Enter the fully qualified domain name in the **RMOTE DESKTOP GATEWAY FQDN** dialog box.

Configuring Security in System Center 2012 - Virtual Machine Manager

The following topics provide information to help you configure security for System Center 2012 – Virtual Machine Manager (VMM).

- Configuring Run As Accounts in VMM
- Creating User Roles in VMM
- Disable Support for SSL 2.0
- Ports and Protocols for VMM
- Clear Text Passwords in Unattend.xml

For an overview of VMM, see Overview of System Center 2012 - Virtual Machine Manager.

Configuring Run As Accounts in VMM

In System Center 2012 – Virtual Machine Manager, the credentials that a user enters for any process can be provided by a Run As account. A Run As account is a container for a set of stored credentials.

Only administrators and delegated administrators can create and manage Run As accounts. Read-only administrators can see the account names associated with Run As accounts that are in the scope of their user role.

The same restrictions on creating, managing, and viewing Run As accounts are in effect in both the VMM console and the VMM command shell. Delegated administrators and self-service users can only get objects that are in the scope of their user role and can only perform the actions that their user role allows.

Security for Run As accounts in VMM

System Center 2012 – Virtual Machine Manager uses the Windows Data Protection API (DPAPI) to provide operating system level data protection services during storage and retrieval of the Run As account credentials. DPAPI is a password-based data protection service that uses cryptographic routines (the strong Triple-DES algorithm, with strong keys) to offset the risk posed by password-based data protection. For more information about DPAPI architecture and security, see Windows Data Protection.

During the installation of a VMM management server, you can configure System Center 2012 – Virtual Machine Manager to use Distributed Key Management to store encryption keys in Active Directory Domain Services (AD DS). For more information, see Configuring Distributed Key Management in VMM.

In This Section

Use the procedures in this section to perform the following tasks.

Procedure	Task
How to Create a Run As Account in VMM	Describes how to create Run As accounts
How to Disable and Enable Run As Accounts in VMM	Describes how to disable and enable a Run As account to temporarily prevent its use.
How to Delete a Run As Account in VMM	Describes how to delete a Run As account.

How to Create a Run As Account in VMM

Use the following procedure to configure Run As accounts for use in System Center 2012 – Virtual Machine Manager (VMM).

A Run As account is a container for a set of stored credentials. For more information about Run As accounts, see Configuring Run As Accounts in VMM.

Account requirements Administrators and delegated administrators can create Run As accounts.

To create a Run As account

1. Open the **Settings** workspace.
2. On the **Home** tab, in the **Create** group, click **Create Run As Account**.

   The **Create Run As Account** dialog box opens.
3. Enter a name and optional description to identify the credentials in VMM.
4. Enter credentials for the Run As account in the **User name** and **Password** text boxes. The credentials can be a valid Active Directory user or group account or they can be local credentials.
5. Unselect **Validate domain credentials**, if desired.
6. Click **OK** to create the Run As account.

How to Disable and Enable Run As Accounts in VMM

To temporarily make a Run As account unavailable for use in System Center 2012 – Virtual Machine Manager (VMM), you can disable the account. To make the Run As account available for use again, enable the account.

Account requirements Administrators and delegated administrators can disable and enable Run As accounts. Delegated administrators can only disable and enable Run As accounts in the scope of their user role.

To disable a Run As account in VMM

1. Open the **Settings** workspace.
2. On the **Settings** pane, expand **Security**, and then click **Run As Accounts**.
3. On the **Run As Accounts** pane, select the Run As account.
4. On the **Home** tab, in the **Run As account** group, click **Disable**.

   The **Enabled** status of the Run As account changes to a red X. The account is not available until it is enabled.

To enable a disabled Run As account

1. Open the **Settings** workspace.
2. On the **Settings** pane, expand **Security**, and then click **Run As Accounts**.
3. On the **Run As Accounts** pane, select the disabled Run As account.
4. On the **Home** tab, in the **Run As account** group, click **Enable**.

How to Delete a Run As Account in VMM

Use the following procedure to delete a Run As account that is not being currently consumed by any process in System Center 2012 – Virtual Machine Manager (VMM). VMM blocks deletion of any Run As account being consumed by a process.

Account requirements Administrators can delete Run As accounts. Delegated administrators who have Run As accounts in the scope of their user role can delete those Run As accounts.

To delete a Run As account

1. Open the **Settings** workspace.
2. In the **Settings** pane, expand **Security**, and then click **Run As accounts**.
3. In the results pane, select the Run As account.

4. On the **Home** tab, in the **Delete** group, click **Delete**, and then click **Yes** to confirm.

The credentials are removed from the VMM database.

Creating User Roles in VMM

You can create user roles in Virtual Machine Manager (VMM) to define the objects that users can manage and the management operations that users can perform. The following table summarizes the capabilities of each user role in VMM.

User Role Descriptions for VMM

VMM User Role	Capabilities
Administrator	Members of the Administrators user role can perform all administrative actions on all objects that VMM manages. Administrators have sole responsibility for these features of VMM: • Only administrators can add stand-alone XenServer hosts and XenServer clusters (known as pools) to VMM management. • Only administrators can add a Windows Server Update Services (WSUS) server to VMM to enable updates of the VMM fabric through VMM. To change the members of the Administrator user role, see How to Add Users to the Administrator User Role in VMM.
Fabric Administrator (Delegated Administrator)	Members of the Delegated Administrator user role can perform all administrative tasks within their assigned host groups, clouds, and library servers, except for adding XenServer and adding WSUS servers. Delegated Administrators cannot modify VMM settings, and cannot add or remove members of the Administrators user role. To create a delegated administrator, see How to Create a Delegated Administrator User Role in VMM.
Read-Only Administrator	Read-only administrators can view properties,

VMM User Role	Capabilities
	status, and job status of objects within their assigned host groups, clouds, and library servers, but they cannot modify the objects. Also, the read-only administrator can view Run As accounts that administrators or delegated administrators have specified for that read-only administrator user role. To create a read-only administrator, see How to Create a Read-Only Administrator User Role in VMM.
Tenant Administrator	As of VMM in System Center 2012 Service Pack 1 (SP1), you can create Tenant Administrator user roles. Members of the Tenant Administrator user role can manage self-service users and VM networks. Tenant administrators can create, deploy, and manage their own virtual machines and services by using the VMM console or a web portal. Tenant administrators can also specify which tasks the self-service users can perform on their virtual machines and services. Tenant administrators can place quotas on computing resources and virtual machines. To create a tenant administrator, see How to Create a Tenant Administrator User Role in VMM.
Application Administrator (Self-Service User)	Members of the Self-Service User role can create, deploy, and manage their own virtual machines and services by using the VMM console or a Web portal. To create a self-service user, see How to Create a Self-Service User Role in VMM.

Caution

If you grant rights for a particular template to a user that does not have rights to the Run As account that the template is configured with, then the user can potentially extract the credentials for the Run As account from the template.

As of System Center 2012 R2, VMM administrators can use the **Create User Role Wizard** to configure user roles with a set of permitted actions on a per-cloud basis in addition to the global

settings. These settings apply only to the tenant administrator and the self-service user roles. With these settings, the user's effective permitted actions for a given cloud are the combination of their global permitted actions and cloud permitted actions.

See Also

Configuring Self-Service in VMM

How to Add Users to the Administrator User Role in VMM

The Administrator user role is created when you install Virtual Machine Manager (VMM). The user who performs the VMM installation and all domain users in the Local Administrators group are added to the Administrator user role.

Use this procedure to add users to the Administrator user role in VMM or remove users from the user role.

Account requirements Administrators can add new users to the Administrator user role or remove users from that user role.

To add users to the Administrator user role

1. In the **Settings** workspace, click **Security**, then click **User Roles**. Under **User Roles**, click the **Administrator** user role to select it.
2. In the **Home** tab, in the **Properties** group, click **Properties**
3. In the **Administrator Properties** dialog box, click **Members** to access the **Members** page, and then click **Add** to open the **Select Users, Computers, or Groups** dialog box.
4. Enter a user or Active Directory group of users and click **OK** to continue. The dialog box verifies that your selections are valid users.

   Note
   You can delete members from the **Members** page by selecting an entry and then clicking **Remove**.
5. Click **OK** to save your changes.

How to Create a Delegated Administrator User Role in VMM

Use this procedure to create a Delegated Administrator user role in System Center 2012 – Virtual Machine Manager (VMM).

Account requirements Administrators and delegated administrators can create a Delegated Administrator user role. Delegated administrators can create Delegated Administrator user roles that include a subset of their scope, library servers, and Run As accounts.

To create a Delegated Administrator user role

1. In the **Settings** workspace, on the **Home** tab in the **Create** group, click **Create User Role**.
2. In the **Create User Role Wizard**, enter a name and optional description for this Delegated Administrator user role. Click **Next** to continue.
3. On the **Profile** page, select **Delegated Administrator**, and then click **Next**.
4. On the **Members** page, click **Add** to add user accounts and Active Directory groups to the user role with the **Select Users, Computers, or Groups** dialog box. After you have added the members, click **Next**.
5. On the **Scope** page, select private clouds or host groups for this Delegated Administrator, and then click **Next**. A delegated administrator differs from an administrator by having a defined scope in which the delegated administrator can make changes.
6. On the **Library servers** page, click **Add** to select one or more library servers with the **Select a Library server** dialog box. Click **OK** to select a server, and then click **Next**.
7. On the **Run As accounts** page, click **Add** to open the **Select a Run As account** dialog box. Select one or more accounts and click **OK** to add the account to the **Run As accounts** page.
   - Use the Ctrl key to select multiple accounts.
   - Click the **Create Run As Account** button to access the **Create Run As Account** dialog box.

   After selecting accounts, click **Next** to continue.
8. Review the settings you have entered and then click **Finish** to create the Delegated Administrator user role.

After you create a delegated administrator, you can change **Members**, **Scope**, **Library servers**, and **Run As accounts** in the **Properties** dialog box for the Delegated Administrator user role.

See Also

Creating User Roles in VMM

How to Create a Self-Service User Role in VMM

How to Create a Read-Only Administrator User Role in VMM

Use this procedure to create a Read-Only Administrator user role in System Center 2012 – Virtual Machine Manager (VMM).

Account requirements Administrators and delegated administrators can create a Read-Only Administrator role. Delegated administrators can create Read-Only Administrator user roles that include a subset of the Delegated Administrator user role's scope, library servers, and Run As accounts.

To create a Read-Only Administrator user role

1. In the **Settings** workspace, on the **Home** tab in the **Create** group, click **Create User Role**.
2. In the **Create User Role Wizard**, enter a name and optional description for this **Read-Only Administrator**. Click **Next** to continue.
3. On the **Profile** page, select **Read-Only Administrator** and then click **Next**.
4. On the **Members** page, click **Add** to add user accounts and Active Directory groups to the user role with the **Select Users, Computers, or Groups** dialog box. After you have added the members, click **Next**.
5. On the **Scope** page, select private clouds or host groups for this read-only administrator, and then click **Next**. A read-only administrator can only view items within this defined scope.
6. On the **Library servers** page, click **Add** to select one or more library server with the **Select a Library server** dialog box. Click **OK** to select a server, and then click **Next**.
7. On the **Run As accounts** page, click **Add** to open the **Select a Run As account** dialog box. Select one or more accounts and click **OK** to add the account to the **Run As accounts** page.
   - Use the Ctrl key to select multiple accounts.
   - Click the **Create Run As Account** button to access the **Create Run As Account** dialog box.

   After selecting accounts, click **Next** to continue.
8. Review the settings you have entered and then click **Finish** to create the Read-Only Administrator user role.

After you create a read-only administrator, you can change its **Members**, **Scope**, **Library servers**, and **Run As accounts** in the **Properties** dialog box for the Read-Only Administrator user role.

See Also

Creating User Roles in VMM

How to Create a Self-Service User Role in VMM

How to Create a Tenant Administrator User Role in VMM

As of Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1), you can create a Tenant Administrator user role. Tenant administrators can create and manage self-service users and VM networks. Tenant administrators can create, deploy, and manage their own virtual machines and services by using the VMM console or a web portal. A tenant administrator can specify which tasks the self-service users can perform on their virtual machines and services, and can place quotas on computing resources and virtual machines.

Account requirements Administrators and delegated administrators can create a Tenant Administrator user role.

To create a Tenant Administrator user role

1. In the **Settings** workspace, on the **Home** tab in the **Create** group, click **Create User Role**.
2. In the **Create User Role Wizard**, enter a name and optional description for this Tenant Administrator user role, and then click **Next**.
3. On the **Profile** page, select **Tenant Administrator**, and then click **Next**.
4. On the **Members** page, click **Add** to add user accounts and Active Directory groups to the user role. Add the members by using the **Select Users, Computers, or Groups** dialog box, and then click **Next**.
5. On the **Scope** page, select the private clouds that the members of this Tenant Administrator role can use. If you want to allow members of this role to receive and implement Performance and Resource Optimization (PRO) tips, select **Show PRO tips**. Then click **Next**.
6. If one or more **Quotas** pages appear (based on whether you selected private clouds on the previous wizard page), review and specify quotas as needed for each private cloud. Otherwise, skip to the next step.

   To set quotas for the combined use of all members of this user role, use the upper list. To set quotas for each individual member of this user role, use the lower list. By default, quotas are unlimited. To create a limit, clear the appropriate check box under **Use Maximum** and then, under **Assigned Quota**, select a limit. When you have completed all settings, click **Next**.
7. On the **Networking** page, to add the VM networks that the members of this Tenant Administrator role can use, click the **Add** button, select one or more VM networks, and

then click **OK**. Then click **Next**.

8. On the **Resources** page, do the following:
   a. Under **Resources**, click **Add** to select resources by using the **Add Resources** dialog box, and then click **OK**.
   b. Under **Specify user role data path**, click **Browse** to specify a library path that members of this user role can use to upload data.
   c. Click **Next**.
9. Select one or more actions that the members of this role can perform, as follows:
   - As of System Center 2012 R2, on the **Permissions** page, select global actions, and any cloud-specific actions.
   - Otherwise, select global actions.

   Click **Next**.
10. If the **Run As accounts** page appears (based on whether you selected the **Author** action on the **Actions** page), add Run As accounts that you want the members of this user role to be able to use. Otherwise, skip to the next step.
11. If the **Quotas for VM networks** page appears (based on whether you selected the **Author VMNetwork** action on the **Actions** page), review and specify quotas to limit the number of VM networks that members of this user role can create. Otherwise, skip to the next step.

    To limit the combined number of VM networks that can be created by all members of this user role, use the upper setting. To limit the number of VM networks that can be created by each individual member of this user role, use the lower setting.
12. On the **Summary** page, review the settings you have entered. Click **Finish** to create the Tenant Administrator user role, or click **Previous** to change any settings.
13. In the **Settings** pane, expand **Security** and then click **User Roles**. Verify that the Tenant Administrator user role that you created appears in the User Roles pane.

After you create a Tenant Administrator user role, you can change **Members**, **Scope**, **Networking**, **Resources**, and **Actions** in the **Properties** dialog box for the Tenant Administrator user role.

See Also

Creating User Roles in VMM

How to Create a Self-Service User Role in VMM

Disable Support for SSL 2.0

SSL 2.0 was originally released in 1995. Since that time a number of security flaws have been discovered and therefore, SSL 2.0 no longer meets our security standards. VMM defaults to using SSL 3.1 however it is possible that during the SSL handshake process, the operating system

might fall back to using SSL 2.0. To prevent this from occurring, you should explicitly disable the use of SSL 2.0 in the operating system. For more information see the Microsoft Knowledge Base article How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services.

Ports and Protocols for VMM

When you install the VMM management server in System Center 2012 – Virtual Machine Manager (VMM), you can assign some of the ports that it will use for communications and file transfers between various VMM components and other devices. While it is a best security practice to change the default ports, not all of the ports can be changed through VMM. The default settings for the ports are listed in the following tables.

Note
P2V functionality has been removed in the System Center 2012 R2 release, and the VMM Self-Service Portal was removed in the System Center 2012 SP1 release. As such, these applicable ports are not listed.

VMM Management Server - Source

The VMM Management Server communicates with various components and devices over these ports:

Component/device connection target	Default ports(s)	Protocol(s)	Where to change port settings
Hyper-V Host (VMM agent)	80/135/139/445	WinRM/RPC/NetBIOS/SMB (over TCP)	VMM Setup Wizard
Hyper-V Host (file transfer)	443	HTTPS (using BITS)	
Hyper-V Host (control channel)	5985/5986	WS-Management	VMM Setup Wizard
VM Guest Agent (file transfer)	443	HTTPS (using BITS)	Windows Registry
VM Guest Agent (control channel)	5985	WS-Management	
VMWare ESX 3.0/3.5 Host (file transfer)	22	SFTP	Windows Registry
VMWare ESXi Host	443	SSH/HTTPS (using BITS)	

Component/device connection target	Default ports(s)	Protocol(s)	Where to change port settings
(file transfer)			
XenServer Host (control channel)	5989	HTTPS	
XenServer Host (data channel)	3260	iSCSI	
WSUS Server (data channel)	80/443	HTTP	Windows Registry
WSUS Server (control channel)	8530/8531	HTTPS	Windows Registry
SQL Server database (remote)	1433	TDS	
Load Balancer	80/443	Load balancer config provider	
Storage Management Service	n/a	WMI	

VMM Management Server - Target

The following components and devices communicate with the VMM Management Server over these ports:

Component/device connection source	Default ports(s)	Protocol(s)	Where to change port settings
VMM Administrator Console	8100, 8101 (HTTPS), 8102 (NET.TCP), 8103 (HTTP)	WCF	VMM Setup Wizard
Windows PE Agent	8101 (control), 8103 (time sync)	WCF	VMM Setup Wizard
WDS PXE Provider	8102	WCF	VMM Setup Wizard

VMM Library Server

The VMM Library Server communicates with various components and devices over these ports:

Component/device connection target	Default ports(s)	Protocol(s)	Where to change port settings
Hyper-V Host (file transfer)	443	BITS	VMM Setup Wizard

VMM Administrator Console

The VMM Administrator Console communicates with various components and devices over these ports:

Component/device connection target	Default ports(s)	Protocol(s)	Where to change port settings
VMM Management Server	8100, 8101 (HTTPS), 8102 (NET.TCP), 8103 (HTTP)	WCF	VMM Setup Wizard
Hyper-V Host	2179	RDP (using VMConnect)	VMM Administrator Console
VMWare Web Services	443	WCF	VMM Administrator Console

Other

The following miscellaneous ports are also used:

Component/device connection target	Default ports(s)	Protocol(s)	Where to change port settings
Baseboard Management Controller	443	HTTPS (SMASH over WS-Management)	On BMC device
Baseboard Management Controller	623	IPMI	On BMC device

Clear Text Passwords in Unattend.xml

There is a possibility that if the installation of a VMM host fails to complete successfully, the installation process might not delete some temporary files. In this situation, a file named

unattend.xml might remain on your computer. It is possible that unencrypted passwords might be visible in this file. To improve security, we recommend the following:

- Manually delete the file named unattend.xml.
- During installation, use an account with only domain join privileges, not necessary a full administrator's account.

Troubleshooting System Center 2012 - Virtual Machine Manager

The following troubleshooting resources for System Center 2012 – Virtual Machine Manager (VMM) are available on the TechNet Wiki:

Resource	Description
System Center 2012 – Virtual Machine Manager (VMM) General Troubleshooting Guide	General information about troubleshooting VMM, such as collecting traces and logging information.
Troubleshooting System Center 2012 - Virtual Machine Manager (VMM)	List of known issues with VMM, and possible resolutions or workarounds for those known issues.
System Center 2012 – Virtual Machine Manager (VMM) Error Codes	List of VMM error messages, grouped by error code number.

The following are other troubleshooting resources that are available for VMM:

Resource	Description	Location
Virtual Machine Manager Configuration Analyzer (VMMCA) for System Center 2012	A diagnostic tool that you can use to evaluate important post-installation configuration settings for computers that either might serve or are serving VMM roles or other VMM functions.	Microsoft Download Center
VMM forums	Ask questions about or discuss VMM	System Center Virtual Machine Manager Forums

For an overview of VMM, see Overview of System Center 2012 - Virtual Machine Manager.

Microsoft Server Application Virtualization

You can use Microsoft Server Application Virtualization (Server App-V) to create virtual application packages that can be deployed to computers running Windows Server and the Server App-V Agent. Click any of the following links for more information about how to use Server App-V.

- **Server Application Virtualization Overview**

  Learn about Server App-V (Server App-V) and what it can do for your organization.
- **Installing Server Application Virtualization**

  Learn how to install Server App-V
- **Packaging Applications With Server Application Virtualization**

  Learn how to package applications for Server App-V.
- **Server Application Virtualization Sequencer Technical Reference**

  Technical reference for the Server App-V Sequencer.
- **Troubleshooting Server Application Virtualization**

  Learn about troubleshooting resources for Server App-V.

Other resources for Server Application Virtualization

- **Supporthttp://support.microsoft.com/**

  Find Solutions to your technical problems in our Support Centers.

Server Application Virtualization Overview

You can use Microsoft Server Application Virtualization (Server App-V) to create virtual application packages. Virtual application packages are images of applications that can be copied to a computer running the Server App-V Agent and started without requiring a local installation. The application then runs as if it is a locally installed application. Running virtual applications can help reduce hardware and operational costs and help streamline enterprise application management. Server App-V builds on the technology used with Application Virtualization (App-V) by separating the application configuration and state from the underlying operating system running on computers in a data center environment. Server App-V allows for dynamic composition of application and hardware images which can help significantly reduce the number of images that need to be managed. Server App-V also enables automation of deployment and management scenarios which can improve reliability, availability and serviceability of datacenter applications.

Not all applications are supported for use with Server App-V. Applications such as antivirus software that require device or kernel driver support are not supported. Server App-V is primarily designed for use with business applications or the business tiers of multi-tiered applications.

Consequently some large server applications such as Microsoft Exchange Server, Microsoft SQL Server, and Microsoft SharePoint are not supported. While there is no list of supported applications for use with Server App-V, Server App-V has been optimized to create virtual application packages for applications with the following attributes:

- State persisted to local disk
- Microsoft Windows Services
- Internet Information Services (IIS)
- Registry
- COM+ / DCOM
- Text-based Configuration Files
- WMI Providers
- Microsoft SQL Server Reporting Services
- Local Users and Groups
- Scheduled Tasks
- Microsoft SQL Server Databases

For more information about configuring Server App-V see Server Application Virtualization Software Requirements.

You should also familiarize yourself with the following terminology:

Virtual Application Package

An application packaged by the Sequencer to run in a self-contained, virtual environment. The virtual environment contains the information necessary to run the application on the client without installing the application locally.

Deployment Configuration File

An .xml file that contains customized settings that are applied to a specific virtual application package when the package is run on a target computer.

Virtual Environment

A runtime container that defines the resources available to application processes that are launched from a sequenced application package.

Steps to take to implement Server App-V

There are two major steps that you must take to implement Server App-V in your environment:

- Create a virtual application package by sequencing an application

  Using the application installation media, create a virtual application package that includes all required resources and configuration settings. You should also identify any items that will

require configuration when the package is run. For more information about sequencing applications, see How to Sequence a New Server Application.

- Deploy the virtual application package

  Specify any configuration settings that must be set for a particular instance of the application, then deploy it using the appropriate tools. For more information about configuring an application, see How to Perform Post-Sequencing Configuration. For test deployments, you can use the Server App-V PowerShell cmdlets to deploy and manage your package. For more information about using cmdlets to deploy a package, see How to Deploy a Virtual Application Package for Testing.

Differences between Server App-V and App-V

The following table shows some of the differences in Server App-V and App-V.

Server App-V	App-V
If an application creates data or modifies configuration in a user-specific location in the registry when the application is sequenced, the data or configuration remains associated with the same user at deployment time and run time.	If an application creates data or modifies configuration in a registry location specific to the current user when the application is sequenced, the data or configuration is mapped so that it is accessible to any user running the application.
Application files that are part of a virtual application package, such as the .exe files and libraries that are required to run the application, are available to all processes that are running on the computer where the application is copied.	Application files that are part of a virtual application package are only available to that virtual application and any other processes started in that application's virtual environment.
COM objects, DCOM objects, COM+ objects, WMI Providers, and NT Services that are part of a virtual application package are exposed on the local system to let the operating system, tools, and other applications interact with them. For example, the native Service Control Manager (SCM) can be used to start a service that is part of a virtual application package.	COM, DCOM, COM+, WMI, and service information that is associated with a virtual application package is kept within that package, unavailable to any processes running outside that package. For example, the native SCM will not see any NT services that are running inside a virtual environment.
The Server App-V Agent uses heuristics to automatically detect which processes on a computer must be run within virtual environments. Typically, no launcher shim is needed. To explicitly add a process to a virtual environment, you can add `"/RunInVE:<package`	For a process to be virtualized, that process must be opened by an App-V program such as **sfttray.exe**, or it has to be the child of another virtual process. To explicitly add a process to a virtual environment, you can run the command `"sfttray.exe /exe <executable to launch>`

Server App-V	App-V
GUID>" to the end of the process's command line.	/app <name of application>".

See Also

Microsoft Server Application Virtualization

Installing Server Application Virtualization

Packaging Applications With Server Application Virtualization

Server Application Virtualization Sequencer Technical Reference

Troubleshooting Server Application Virtualization

Server Application Virtualization Release Notes

To search these Release Notes, press CTRL+F.

Important

Read these Release Notes thoroughly before you install the Microsoft Server Application Virtualization (Server App-V). These Release Notes contain information that you must have to successfully install Server App-V. This document contains information that is not available in the product documentation. If there is a difference between these Release Notes and other Server App-V documentation, the latest change should be considered authoritative. These Release Notes supersede the content included with this product.

Protect Against Security Vulnerabilities and Viruses

To help protect against security vulnerabilities and viruses, it is important to install the latest available security updates for any new software being installed. For more information, see the Microsoft Security website at http://go.microsoft.com/fwlink/?LinkId=3482.

Providing Feedback

You can provide feedback, make a suggestion, or report an issue with the Microsoft Application Virtualization (App-V) Management System in a community forum on the Microsoft Application Virtualization TechCenter (http://go.microsoft.com/fwlink/?LinkId=122917).

You can also provide your feedback about the documentation directly to the App-V documentation team. Send your documentation feedback to appvdocs@microsoft.com.

Known Issues with Server Application Virtualization

This section provides the most up-to-date information about issues with Server App-V. These issues do not appear in the product documentation and in some cases might contradict existing product documentation. When it is possible, these issues will be addressed in later releases.

When sequencing Team Foundation Server 2010, you receive the following error: - db backup error - file not found

When you sequence Team Foundation Server 2010 and you specify Microsoft SharePoint integration by providing a location of the Windows SharePoint Services installer, a db backup error occurs when you stop monitoring. This occurs because Team Foundation Server 2010 creates the Windows SharePoint Services databases on the remote SQL server. This is an unsupported scenario.

WORKAROUND During the monitoring phase of sequencing, follow these steps:

1. Install the Windows SharePoint Services and configure for your environment.
2. Install Team Foundation Server 2010 and configure it to reference the Windows SharePoint Services installation during the Team Foundation Server 2010 configuration phase.

When you remove a package that contains COM+ components the associated native registration overrides are also removed

After you remove a virtual application package that contains COM+ components, any overrides that were applied by using the native registration after you deployed the virtual application are also removed.

WORKAROUND After you remove the virtual application package, you must reapply the overrides that were applied by using the native registration.

Changing credentials of an interactive service renders the credentials noninteractive

Interactive windows services (services that can interact with the desktop) can only run as Local System. If your package has an interactive Windows Service, and if you change its credentials from Local System to another user during deployment, the service can no longer interact with the desktop. Therefore, the package might lose some of its functionality.

WORKAROUND To preserve this functionality, you should not change the credentials of interactive services.

Deleting a deployment configuration item causes the sequencer to quit unexpectedly

Server App-V automatically captures configuration items associated with a virtual application package that can be used during deployment to configure an instance of the deployed application package. After sequencing an application, these configuration items are displayed in the deployment configuration section of the sequencer console. If any of the configuration items are deleted using the sequencer console, the sequencer can crash, causing a loss of the virtual application package that was created.

WORKAROUND To delete a configuration item, you should first save your package and then manually edit the **deploymentconfig.xml** document. To remove an item from the file, you should delete the applicable **.xml** node for the required deployment configuration item.

Release Notes Copyright Information

Installing Server Application Virtualization

Use the following information to implement Microsoft Server Application Virtualization (Server App-V).

The Server App-V Sequencer

To create a Server App-V virtual application package, you must first install the Sequencer on a computer in your environment. The Sequencer creates a virtual application package by monitoring and recording the entire installation and setup process for an application. The computer that you install the Sequencer on must meet the Server Application Virtualization Software Requirements. For information about how to install the Sequencer, see How to Install the Server Application Virtualization Sequencer.

Important
The computer that you install the Sequencer on must not be running any version of the Server App-V Agent.

The Server App-V Agent

Before you can deploy a virtual application package that you have sequenced, you must install the Server App-V Agent on all computers to which you intend to deploy a package. The Server App-V Agent accepts a virtual application package, including a deployment configuration file that contains settings specific to an instance of the application, and sets the package up on the target computer. For information about how to install the Agent, see How to Install the Server Application Virtualization Agent. For information about how to remove the Agent, see How to Remove the Server Application Virtualization Agent.

Planning for testing virtual application packages

The Server App-V PowerShell Agent Cmdlets let you manage your virtual application packages for testing packages in a lab environment. The Cmdlets can be installed on the computer running the Server App-V Agent for local management or on a remote computer that will be used to manage the Windows Servers that run virtual application packages. The Server App-V Cmdlets can be used to perform various management tasks such as deploying, configuring, retiring, upgrading or backing up a virtual application package. The Server App-V Agent functions require PowerShell 2.0.

The Server App-V PowerShell Sequencer Cmdlets let you perform sequencing tasks on the computer running the Sequencer. You can create a new package, or update an existing package.

To install the Cmdlets, see How to install the Server Application Virtualization PowerShell Cmdlets

Important
You should only use the Cmdlets to manage packages in a test environment to ensure functionality.

See Also

Microsoft Server Application Virtualization

Server Application Virtualization Overview
Packaging Applications With Server Application Virtualization
Server Application Virtualization Sequencer Technical Reference
Troubleshooting Server Application Virtualization

Server Application Virtualization Software Requirements

The following tables show the supported operating systems and subsystems that are required to run the Microsoft Server Application Virtualization (Server App-V) Agent and Sequencer.

Warning
Installing the Server App-V Agent or Server App-V Sequencer is not supported on computers that are running client operating system versions or Application Virtualization (App-V).

Software Requirements

The following table displays the supported operating systems for running the Server App-V Agent and Sequencer.

Operating System	Edition	Service Pack	System Architecture
Windows Server 2003	R2	SP2	x86, x64
Windows Server 2008		SP2	x86, x64
Windows Server 2008	R2		x64
Windows Server 2012			x64

See Also

Server Application Virtualization Overview
How to Install the Server Application Virtualization Sequencer
How to Install the Server Application Virtualization Agent
How to Remove the Server Application Virtualization Agent
How to install the Server Application Virtualization PowerShell Cmdlets

How to Install the Server Application Virtualization Sequencer

Important

The computer that you install the sequencer on cannot be running any version of the Microsoft Server Application Virtualization (Server App-V) Agent. Running the sequencer in safe mode is not supported and you must have administrative rights on the computer that you are using to sequence an application.

To install the Server App-V Sequencer

1. Copy the Server App-V Sequencer installation files (**SeqSetup.exe**) to the computer that is running Windows Server that you want to install it on. You must also locate the correct version of the installation file that matches the architecture of the computer that you are installing on, **x86** or **x64**. The Server App-V installation files are located in the following directory: **Program Files\ Microsoft System Center 2012 \ Virtual Machine Manager \ SAV**.
2. To start the Server App-V Sequencer installation wizard, double-click **SeqSetup.exe**. If the **Microsoft Visual C++ SP1 Redistributable Package (x86)** is not detected before installation, click **Install** to install the prerequisite. If the **Microsoft Visual C++ SP1 Redistributable Package (x86)** has already been installed, skip to step 3 of this procedure.
3. On the **Welcome** page, to join the **Customer Experience Improvement Program**, select **Join the Customer Improvement Program**, and click **Next**. To start the Sequencer installation without joining the **Customer Experience Improvement Program**, click **Next**.
4. On the **License** page, to accept the terms of the license agreement, select **I accept the license terms**, and then click **Next**.
5. On the **Destination Folder** page, to accept the default directory where the Sequencer will be installed, click **Next**. To change the location, click **Change**, and in the **Browse for Folder** dialog box, specify the new location and then click **OK**. Click **Next**.
6. On the **Ready to Install** page, to start the installation with the specified settings, click **Install**. To change the settings, click **Back** and update the preferred settings. Click **Next**.
7. After you have installed the Server App-V Sequencer, to close the Server App-V Sequencer installation wizard, click **Finish**. To open the Sequencer, click **Start** / **All Programs** / **Microsoft Application Virtualization** / **Microsoft Application Virtualization Sequencer**.

How to uninstall the Server App-V Sequencer

1. Click **Start**, and then click **Control Panel**, and then click **Programs and Features**.
2. In **Control Panel**, select **Uninstall a Program**. Select **Microsoft Server Application Virtualization Sequencer** and then click **Uninstall/Change**. Click **Continue**.

Important
After you uninstall the Sequencer, you must restart the computer to complete the installation.

See Also

Server Application Virtualization Overview

Server Application Virtualization Software Requirements

How to Install the Server Application Virtualization Agent

How to Remove the Server Application Virtualization Agent

How to install the Server Application Virtualization PowerShell Cmdlets

How to Install the Server Application Virtualization Agent

Important
You must have administrative rights on the computer that the Microsoft Server Application Virtualization (Server App-V) Agent will be installed on.

Use one of the following ways to install the Server App-V Agent. After you install the Agent, you can review the **SAVSetupChainerLog.txt** file for information about the installation process.

The Server App-V installation files are located in the following directory: **Program Files\ Microsoft System Center 2012 \ Virtual Machine Manager \ SAV**.

To install the Server App-V Agent

1. Copy the Server App-V Agent installation files (**Agentsetup.exe**) to the computer that is running Windows Server where you want to install the Server App-V Agent. You must also use the correct version of the installation file that matches the architecture of the computer that you are installing on, **x86** or **x64**.
2. To start the Microsoft Server Application Virtualization Agent setup wizard, double-click **AgentSetup.exe**.
3. On the **Welcome** page, click **Next**.
4. On the **License** page, to accept the terms of the license agreement, select **I accept the license terms**, and then click **Next**.
5. On the **Microsoft Update Opt-In** page, to let Microsoft Update to run while you install the Agent, select **Use Microsoft Update when I check for updates (recommended)**. To disallow Microsoft Update from running while you install the Agent, select **I don't want to use Microsoft Update**. Click **Next**.

6. On the **Destination Folder** page, to accept the default directory where the Agent will be installed, click **Next**. To change the location, click **Change**. Then, in the **Browse For Folder** dialog box, specify the new location and click **OK**. Click **Next**.
7. On the **Ready to Install** page, confirm the Agent installation settings. To start the installation by using the specified settings, click **Next**. To change the settings, click **Back** and update the preferred settings. Click **Next**.
8. To complete the Agent installation, click **Finish**.

To install the Server App-V Agent (silently)

1. You can also install the Server App-V Agent silently by using the following as an example:

   ```
   AgentSetup.exe /q INSTALLDIR=c:\serverappv SWIGLOBALDATA=c:\SWIGlobalData
   SWIUSERDATA=c:\SWIUserData SWIFSDRIVE=q /ACCEPTEULA
   ```

   The following list displays more information about each parameter:

   - **INSTALLDIR** specifies the installation location.
   - **SWIGLOBALDATA** specifies the global data directory. This is the primary location where the Server App-V Agent stores associated cached data, including deployed packages.
   - **SWIUSERDATA** specifies the user data directory. This is the location where the Server App-V Agent stores settings and some package state.
   - **SWIFSDRIVE** specifies the file system drive letter.
   - **OPTIN** opts in to Microsoft Update. If this parameter is set to FALSE or if it is omitted, the installer does not perform MU opt in. Otherwise, the installer performs MU opt-in.
   - **LOG_LEVEL** specifies the log level that will be used during the installation.
   - **ACCEPTEULA** accepts the associated EULA agreement. This is mandatory for silent installations and the agreement must also be accepted or the installation will fail.

   The following switches are also available:

   - **/q** specifies a silent setup.
   - **/u** specifies an uninstallation of the Agent.
   - **/?** displays help associated with the installer. The installation log is saved in the **%temp%** directory.

See Also

Server Application Virtualization Overview

Server Application Virtualization Software Requirements

How to Install the Server Application Virtualization Sequencer

How to Remove the Server Application Virtualization Agent

How to install the Server Application Virtualization PowerShell Cmdlets

How to Remove the Server Application Virtualization Agent

You can uninstall the Microsoft Server Application Virtualization (Server App-V) Agent by using either **AgentSetup.exe /u** or **Control Panel**. To remove all Server App-V components from your computer you must delete all of the virtual applications saved on the computer before you perform the following procedures.

Use one of the following procedures to remove the Server App-V Agent.

Important
When you uninstall the Agent, you must restart the computer to complete the installation.

To uninstall the Server App-V Agent by using AgentSetup.exe

1. On the computer that is running the Server App-V Agent, to open a command prompt, click **Start** and type **cmd**. To browse to the directory that contains **AgentSetup.exe**, type **cd** and specify the path to the directory that contains **AgentSetup.exe** .

   Type **AgentSetup.exe /u** and press Enter.
2. On the **Welcome** page, to start uninstalling the Agent, click **Next**.

   Important
   You must restart the computer for the configuration changes to take effect.
3. To complete the removal of the Agent and to exit the wizard, click **Finish**. To restart the computer immediately, click **Yes**; to restart the computer later, click **No**. You must restart the computer to uninstall the Server App-V Agent.

To uninstall the Server App-V Agent by using control panel

1. On the computer that is running the Server App-V Agent, select **Start** / **Control Panel** / **Programs and Features**.
2. To uninstall the Server App-V Agent, right-click Microsoft Server Application Virtualization Agent and select **Uninstall/Change**.
3. On the **Welcome** page, to remove the Agent, click **Next**.
4. To complete the removal of the Agent and to exit the wizard, click **Finish**. To restart the computer immediately, click **Yes**; to restart the computer later, click **No**. You must restart the computer to uninstall the Server App-V Agent.

See Also

Server Application Virtualization Overview

Server Application Virtualization Software Requirements
How to Install the Server Application Virtualization Sequencer
How to Install the Server Application Virtualization Agent
How to install the Server Application Virtualization PowerShell Cmdlets

How to install the Server Application Virtualization PowerShell Cmdlets

Note
After you install PowerShell, you can also use the **Get-Help** command in a PowerShell console for more information about these functions.

To install the Server App-V PowerShell Cmdlets

1. Copy the Server App-V PowerShell Cmdlet installation file (**AgentCmdletsSetup.exe** for the Server App-V Agent functions or **SequencerCmdletsSetup.exe** for the Server App-V Sequencer functions.) to the computer that is running Windows Server that you want to install it on. Use the correct version of the installer based on your computer's architecture, **x86** or **x64**.
2. To start the Server App-V PowerShell Cmdlet installation wizard, double-click **sav_cmdlets.exe** or **SequencerCmdletsSetup.exe**.
3. On the **License** page, to accept the terms of the license agreement, select **I accept the license terms**. To start the installation, click Next.
4. To complete the installation and close the setup wizard, click **Finish**.
5. To use the Server App-V PowerShell Cmdlets open an elevated PowerShell cmd prompt and import the modules by running the following commands:
   a. `PS C:\> Set-ExecutionPolicy Remotesigned`
   b. `PS C:\> Import-Module ServerAppVAgent`

   Note
   You must run the **Import-Module ServerAppVAgent** command every time that you open a new PowerShell command prompt.

See Also

Server Application Virtualization Overview
Server Application Virtualization Software Requirements
How to Install the Server Application Virtualization Sequencer
How to Install the Server Application Virtualization Agent

How to Remove the Server Application Virtualization Agent

Packaging Applications With Server Application Virtualization

Sequencing is the process of creating a virtual application package. The following information provides an overview of creating and configuring virtual application package using Microsoft Server Application Virtualization (Server App-V). You can copy virtual application packages to computers that are running the Server App-V Agent. Virtual application packages are images of applications that can be copied to a computer and started without requiring a local installation but will run similarly to a locally installed application.

Sequencing

After you have successfully installed the Sequencer, you must create a virtual application package. The Sequencer creates applications that run in a virtual environment. The Server App-V Sequencer monitors the installation and setup process for an application, and records the information that is necessary for the application to run in a virtual environment. A sequenced application is separated from the operating system and is run in a virtual environment. This separation makes it easier than a standard application to deploy, manage, move, and remove a virtual application package.

Caution
We highly recommended that the operating system image that you use to sequence an application matches the operating system image to which you plan to deploy the virtual application package.

For computers running Windows Server 2008 or later, before you sequence an application, you should understand the Windows Server Roles and Features that are required for the application to run. All the required Roles and Features should be enabled before you sequence the application. Additionally, the required Roles and Features must also be enabled on all computers that will run the virtual application package.

For information about how to sequence an application, see How to Sequence a New Server Application.

You can also use the command line to sequence an application. For more information about using PowerShell to automate sequencing an application, see How to install the Server Application Virtualization PowerShell Cmdlets, or review the associated help using the PowerShell console.

After you have created a virtual application package, for information about the sequencing process you can review **Reports.xml** file which is located in the directory specified on the **Create Package** page of the **Create New Package** wizard.

If you plan to sequence an application that creates a database on a Microsoft SQL Server, the following the following prerequisites must be installed. The following components are part of the Microsoft® SQL Server® 2012 Feature Pack.

1. Microsoft® SQL Server® 2012 Data-Tier Application Framework
2. Microsoft® SQL Server® 2012 Transact-SQL Language Service
3. Microsoft® SQL Server® 2012 Shared Management Objects
4. Microsoft® SQL Server® 2012 Transact-SQL ScriptDom
5. Microsoft® System CLR Types for Microsoft® SQL Server® 2012

Post-sequencing tasks

After you have sequenced an application, you can customize how the virtual application package will run by configuring the associated deployment configuration items. These settings are applied to the virtual application package at run time and the information is saved in the associated deployment configuration file. The deployment configuration file is an .xml file, and you can assign a unique deployment configuration file to multiple instances of the same package running on different computers. The deployment configuration items are displayed on the **Deployment Configuration Items** tab in the Server App-V Sequencer.

Note
Modifying local group memberships using the deployment configuration file is not supported. To change local group memberships, you should use a script after you deploy the virtual application package, or update the membership requirements manually.

For more information about configuring virtual application packages, see How to Perform Post-Sequencing Configuration.

After you configure the package you must save the package. For more information about saving a package, see How to Save a Server Virtual Application Package.

Important
You should never let untrusted users to connect to computers in a datacenter environment to run or configure a virtual application package.

Virtual Application Package deployment example

Use the following information to deploy a server virtual application package to a computer that is running the Server App-V Agent. The deployment is done by using the Server App-V PowerShell Cmdlets. These prerequisites must be available before you perform the procedure to deploy the application package:

- A computer that is running the Server App-V Agent.
- An installed server virtual application package.
- A computer that is running PowerShell 2.0 and the Server App-V Cmdlets.

The computer that is running the Server App-V Agent can be the same as the computer that has the Server App-V Cmdlets installed, although it is not required. If you use different computers, they must be able to contact one another over the network. The user account performing the deployment must be a member of the Local Administrators local security group on both computers. The virtual application package must be copied locally to the computer that is running the Server App-V Agent. The deployment process will occur completely on the computer that is running the Server App-V Cmdlets.

Important
You should only use the Cmdlets to manage packages in a test environment to ensure and test package functionality.

For information about deploying a package for testing, see How to Deploy a Virtual Application Package for Testing. For a list of the cmdlets that are available with Server App-V, see Server Application Virtualization Cmdlets.

Updating an existing virtual application package

If you have a previously created virtual application package, you can use update or edit a package. For information about either procedure see How to Update an Existing Virtual Application Package and How to Edit an Existing Virtual Application Package.

See Also

Microsoft Server Application Virtualization

Server Application Virtualization Overview

Installing Server Application Virtualization

Server Application Virtualization Sequencer Technical Reference

Troubleshooting Server Application Virtualization

How to Sequence a New Server Application

To sequence a new application

1. To start the Server App-V Sequencer, on the computer that is running Sequencer select, **Start** / **All Programs** / **Microsoft Application Virtualization** / **Microsoft Application Virtualization Sequencer**.
2. Select **Create a New Virtual Application Package**.
3. On the **Prepare Computer** page, review the issues that could cause the package update to fail, or for the package update to contain unnecessary data. It is strongly recommend that you resolve all potential problems before you continue. After you have fixed the conflicts, to update the information displayed, click **Refresh**. After you have resolved all

potential issues, click **Next**.

Important
If you have to disable virus-scanning software, you should scan the computer that is running the Sequencer to make ensure there are no unwanted or malicious files that might be added to the package.

4. On the **Select Installer** page, click **Browse** and specify the installation file for the application that you are sequencing. If the application does not have an associated installer file and you plan to run all installation steps manually, select **Select this option to perform a custom installation**. Click **Next**.
5. On the **Package Name** page, specify a name that will be associated with the package. The name that you specified should help identify the purpose and version of the application that will be added to the package.

   Important
   The name you specify must be unique across the enterprise.

   The **Installation Location** displays the Application Virtualization path where the application will be installed to. To edit this location select **Edit (Advanced)**.

   Important
   Editing the Application Virtualization path is an advanced configuration task. You should fully understand the implications of changing the path. For most applications, the default path is recommended.

   Click **Next**.

6. On the **Installation** page, when the Sequencer and application installer are ready, install the application to the package root you selected (typically **Q:**) so that the Sequencer can monitor the installation process. Perform the installation by using the application's installation process.

   Important
   If the application you are sequencing requires **Dcomcnfg.exe** as part of the installation, you should run it during the configuration phase (Step 8 of this procedure), not during the monitoring phase.

   If there are additional installation files that must be run as part of the installation, click **Run** and locate and run the additional installation files. When you are finished with the installation, select **I am finished installing**. Click **Next**.

   Tip
   Instead of clicking the **Run** button, you can minimize the Sequencer and perform any additional required installation steps directly on the computer running the Sequencer. This is because the Sequencer is monitoring all system activity, whether or not it originates from within the Sequencer user interface (UI).
7. On the **Installation** page, wait while the Sequencer configures the virtual application

package.

8. On the **Configure Software** page, optionally run the programs that are contained in the package. This step is helpful for completing any associated license or configuration tasks that are required to run the application before you deploy and run the package. To run all the programs at the same time click **Run All**. To run specific programs select the program or programs that you want to run, and click **Run Selected**. Complete the required configuration tasks and then close the applications. It can take several minutes for all programs to run. Click **Next**.
9. On the **Installation Report** page, you can review information about the virtual application package that you just sequenced. For a more detailed explanation about the information displayed in **Additional Information**, double-click the event. After you have reviewed the information, click **Next**.
10. On the **Create Package** page, optionally add **Comments** that will be associated with the package. Comments are useful for identifying version and other information about the package. The default **Save Location** is also displayed. To change the default location, click **Browse** and specify the new location. Click **Create**.
11. On the **Completion** page, after you have reviewed the information displayed in the **Virtual Application Package Report** pane, click **Close**.

    The package is now available in the Sequencer console.
12. In the Sequencer console, to save the package select **Package** / **Save**. Assign a name to the package and also specify where the package should be saved.

    Important

    Virtual application packages can contain sensitive information, for example usernames and passwords. You should always save virtual application packages in a secure location.

    After you have created a virtual application package, for information about the sequencing process you can review **Reports.xml** file which is located in the directory specified in **Step 10** page of the **Create New Package** wizard.

See Also

How to Update an Existing Virtual Application Package

How to Edit an Existing Virtual Application Package

How to Perform Post-Sequencing Configuration

How to Save a Server Virtual Application Package

How to Deploy a Virtual Application Package for Testing

How to Update an Existing Virtual Application Package

You must have the Server App-V Sequencer installed to change a server virtual application package. For more information about how to install the App-V Sequencer see How to Install the Server Application Virtualization Sequencer.

To update an application in an existing server virtual application package

1. To start the Server App-V Sequencer, on the computer that is running the Server App-V Sequencer, select **Start** / **All Programs** / **Microsoft Application Virtualization** / **Microsoft Application Virtualization Sequencer**.
2. In the App-V Sequencer, click **Modify an Existing Virtual Application Package** and then click **Next**.
3. On the **Select Task** page, click **Update Existing Package**. Click **Next**.
4. On the **Select Package** page, click **Browse** and locate the virtual application package (**.sprj** file) that contains the virtual package that you want to update. Click **Next**.
5. On the **Prepare Computer** page, review the issues that could cause the package update to fail, or for the package update to contain unnecessary data. It is strongly recommend that you resolve all potential problems before you continue. After you have fixed the conflicts, to update the information displayed, click **Refresh**. After you have resolved all potential issues, click **Next**.

   Important
   If you have to disable virus-scanning software, you should scan the computer that is running the Sequencer to make ensure there are no unwanted or malicious files that might be added to the package.
6. On the **Upgrade Configuration** page confirm whether any further configuration is required. Click **Next**.
7. On the **Select Installer** page, click **Browse** and specify the update installation file for the package. If the update does not have an associated installer file and you plan to run all installation steps manually, select **Perform a custom installation**. Click **Next**.
8. On the **Installation** page, when the Sequencer and application installer are ready, install the application to the package root you selected (typically **Q:**) so that the Sequencer can monitor the installation process. Perform the installation by using the application's installation process.

   If there are additional installation files that must be run as part of the installation, click **Run** and locate and run the additional installation files. When you are finished with the installation, select **I am finished installing**. Click **Next**.

   Tip
   Instead of clicking the **Run** button, you can minimize the Sequencer and perform any additional required installation steps directly on the computer running the

Sequencer. This is because the Sequencer is monitoring all system activity, whether or not it originates from within the Sequencer user interface (UI).

9. On the **Installation Report** page, you can review information about the virtual application that you just sequenced. For a more detailed explanation about the information displayed in **Additional Information**, double-click the event. After you have reviewed the information, click **Next**.
10. On the **Create Package** page, add **Comments** that will be associated with the package. Comments are useful for identifying version and other information about the package. The default **Save Location** is also displayed. To change the default location, click **Browse** and specify the new location. Click **Create**.
11. On the **Completion** page, to exit the wizard, click **Close**. The package is now available in the Sequencer.

    In the Sequencer console, to save the package select **Package** / **Save**. Assign a name to the package and also specify where the package should be saved.

    Important
    Virtual application packages can contain sensitive information, for example usernames and passwords. You should always save virtual application packages in a secure location.

See Also

How to Sequence a New Server Application

How to Edit an Existing Virtual Application Package

How to Perform Post-Sequencing Configuration

How to Save a Server Virtual Application Package

How to Deploy a Virtual Application Package for Testing

How to Edit an Existing Virtual Application Package

You must have the Server App-V Sequencer installed to modify a server virtual application package.

You can perform these tasks when you edit a virtual application package:

- View package properties
- View package change history
- View associated package files
- Edit registry settings

- Review additional package settings (except operating system file properties)
- Modify OSD file
- Set virtualized registry key state (override or merge)
- Set virtualized folder state
- Edit virtual file system mappings

For more information about installing the App-V Sequencer, see How to Install the Server Application Virtualization Sequencer.

To edit an existing Server App-V package

1. To start the App-V Sequencer, on the computer that is running the App-V Sequencer, select **Start** / **All Programs** / **Microsoft Application Virtualization** / **Microsoft Application Virtualization Sequencer**.
2. In the App-V Sequencer, click **Modify an Existing Virtual Application Package**.
3. On the **Select Task** page, click **Edit Package**. Click **Next**.
4. On the **Select Package** page, click **Browse** and locate the server virtual application package (**.sprj**) that contains the application properties you want to modify. Click **Edit**.
5. When you have finished changing the package properties, to save the package, select **File**, and then click **Save**. For more information about the Sequencer Console and the associated controls see, Sequencer Console.

See Also

How to Sequence a New Server Application

How to Update an Existing Virtual Application Package

How to Perform Post-Sequencing Configuration

How to Save a Server Virtual Application Package

How to Deploy a Virtual Application Package for Testing

How to Perform Post-Sequencing Configuration

When you sequence a new application, the associated settings are saved in a file called the deployment configuration file. The deployment configuration file is an .xml file that contains customized settings that are applied to a specific virtual application package when the package is run on a target computer. Some deployment configuration settings are detected automatically by the Sequencer however; you can also add additional configuration items. Additionally, you can assign a unique deployment configuration file to multiple instances of the same package running on different computers.

To configure a virtual application package

1. After you have sequenced an application, select the **Deployment Configuration** tab in the Server App-V Sequencer.

   Or, if this is an existing virtual application package, click **Start** and then point to **All Programs**. Point to **Microsoft Application Virtualization** and then click **Microsoft Application Virtualization sequencer**. Select **Modify an Existing Virtual Application Package**. On the **Select Task** page, click **Edit Package** and then click **Next**. On the **Select Package** page, click **Browse** and locate the virtual application package that you want to configure and then click **Edit**.
2. You can review the existing configuration items associated with the package in the **Deployment Configuration Items** pane.
3. You can follow these steps on the **Deployment Configuration** tab:

Task	Description
Make Item Mandatory	A value for a mandatory configuration item must be provided when the package is deployed. To make the selected item mandatory, click **Make Item Mandatory** in the **Deployment Configuration Item** pane. To remove the mandatory setting, select the item and then click **Make Item Mandatory** again.
Delete Item	To delete a configuration item, select the item that should be deleted and then click **Delete Item** in the **Deployment Configuration Item** pane.
Properties	To view the properties associated with the configuration item, click **Properties** in the **Deployment Configuration Item** pane. In the Deployment Configuration Item Properties dialog box, you can you can do the following: • Change the default value. • Change the **Name**. • Change the **Description**. • Make the configuration item mandatory. Mandatory items must be run when the package is deployed.

Add Deployment Configuration Items	To add a new deployment configuration item click **Add Deployment Configuration Item** in the **Deployment Configuration Item** pane. Deployment configuration items are settings, for example a database connection string that will impact how the virtual application package runs on target computers.
Manage Scripts	To specify scripts that should run either inside or outside the virtual environment when the package is deployed to a computer, click **Manage Scripts** in the **Deployment Configuration Item** pane.

4. After you have made all required updates, to save the package to save the package select **File** and then select **Save**.

See Also

How to Sequence a New Server Application

How to Update an Existing Virtual Application Package

How to Edit an Existing Virtual Application Package

How to Save a Server Virtual Application Package

How to Deploy a Virtual Application Package for Testing

How to Save a Server Virtual Application Package

Use the following procedures to save a server virtual application package.

Important
Virtual application packages can contain sensitive information, for example usernames and passwords. You should always save virtual application packages in a secure location.

You must have the Server App-V Sequencer installed to open and save a server virtual application package. For more information about how to install the App-V Sequencer, see How to Install the Server Application Virtualization Sequencer.

To save a virtual application package

1. To start the Server App-V Sequencer, on the computer that is running Sequencer select, **Start** / **All Programs** / **Microsoft Application Virtualization** / **Microsoft Application Virtualization Sequencer**.
2. If you are saving a new virtual application package, go to step 3 of this procedure. To save an existing virtual application package, after you have made any required updates or modifications, select **File** / **Save**. To create a new version of an existing package, after you have made the necessary modifications select **File**, then click **Save As** and specify the directory where the virtual application package should be saved. If you do not want to overwrite the original version of the package, you must select **Save As** and specify a unique directory and file name for the updated version of the virtual application package.
3. If this is a new virtual application package, select **File** / **Save** and specify the directory where the virtual application package should be saved.

   Note
   If the application connects to a Microsoft SQL database and creates databases, a SQL components folder will also be created in the package directory.
4. To close the Server App-V Sequencer, click **File**, and then click **Exit**.

See Also

How to Sequence a New Server Application

How to Update an Existing Virtual Application Package

How to Edit an Existing Virtual Application Package

How to Perform Post-Sequencing Configuration

How to Deploy a Virtual Application Package for Testing

How to Deploy a Virtual Application Package for Testing

Important
You should only use the Server App-V Cmdlets to manage packages in a test environment to ensure and test package functionality.

Deploying a virtual application package

1. Open an elevated PowerShell console window and run the following command:

   ```
   Set-ExecutionPolicy Remotesigned –Scope Process -Force
   ```

   The Set-ExecutionPolicy cmdlet changes the user preference for the Windows PowerShell execution policy. The execution policy is part of the security strategy of Windows PowerShell. It determines whether you can load configuration files (including

your Windows PowerShell profile) and run scripts, and it determines which scripts, if any, must be digitally signed before they will run.

2. Import the Server App-V Cmdlets.

```
PS C:\> Import-Module ServerAppVAgent
```

3. Use the following information to customize the deployment configuration document associated with the virtual application package:

   Note
   If the package has associated Microsoft SQL Server components, those components should be deployed to the server running Microsoft SQL so the application runs successfully.

   - Open the **deploymentconfig.xml** by using an XML editor for example XML Notepad 2007 (http://go.microsoft.com/fwlink/?LinkId=208297). The **deploymentconfig.xml** is located in the root of the package folder on the computer that is running the Server App-V Agent.
   - Review the **ENTRY** nodes under **/CONFIGURATION/VIRTUALENVIRONMENT** and **/CONFIGURATION/LOCAL**.
   - Under each **ENTRY**, review the **VALUE** node data that requires customization. Typically, this is the name of a server or a missing or incorrect password. This data may stand-alone, or it may be part of a larger structure like a database connection string. You can use other information in the **ENTRY** node to understand where it came from and what it controls.
   - Update the **VALUE** node data with the appropriate customization. Do not change attributes on the **VALUE** node. Also, do not change anything else in the **ENTRY** node.
   - Save deploymentconfig.xml and close the XML editor.

     Note
     If the deployment configuration file contains sensitive information, such as passwords, you should save the file in a secure location.

4. Add the package. Replace the **bold** sample parameters with data that is specific to your deployment.

   PS C:\> Add-ServerAppvPackage –Name **MyApp** –Manifest **C:\MyApp\MyApp_manifest.xml**

   –SFT **C:\MyApp\MyApp.sft** –Configuration **C:\MApp\deploymentconfig.xml**

5. Start the package. Replace the **bold** sample parameters with data that is specific to your deployment.

   PS C:\> Start-ServerAppVPackage –Name **MyApp**

See Also

How to Sequence a New Server Application

How to Update an Existing Virtual Application Package

How to Edit an Existing Virtual Application Package

How to Perform Post-Sequencing Configuration

How to Save a Server Virtual Application Package

Server Application Virtualization Sequencer Technical Reference

Click any of the following links for technical reference information about Microsoft Server Application Virtualization (Server App-V).

In This Section

Server Application Virtualization Cmdlets

Provides information about the cmdlets that are available with Server App-V.

Sequencer Console

Provides information about the Server App-V Sequencer console.

Dialog Pages

Provides information about the Server App-V dialog pages.

Wizard Pages

Provides information about the Server App-V wizard console.

See Also

Microsoft Server Application Virtualization

Server Application Virtualization Overview

Installing Server Application Virtualization

Packaging Applications With Server Application Virtualization

Troubleshooting Server Application Virtualization

Server Application Virtualization Cmdlets

Server Application Virtualization Agent Cmdlets

You can install these cmdlets on any computer and manage the Server App-V Agent remotely. You do not need to install the cmdlets on the computer running the Server App-V Agent because Server App-V uses Windows Management Instrumentation (WMI) remoting.

Managing applications remotely using the Server App-V PowerShell cmdlets is suggested for the following scenarios:

- The remote server is running the Server App-V agent and is connected to the domain.
- When you are using an account that is a member of the domain.
- The domain account is a member of the local administrators group on the server you are deploying the application to. However, in a standalone environment, it's not possible to provision a Server App-V application using a cmdlet to a remote server.

For Workgroup scenarios, customers should run the cmdlet locally on the server to which you are deploying the application. Domain joined computers will not be impacted by this issue.

Note

You may need to open the firewall on the computer running the Server App-V Agent to allow WMI remoting.

The following list displays the function names and a brief description of the functions that are currently available for use with Server App-V Agent:

- **Add-ServerAppvPackage**

  Adds a new virtual application package to a computer running the Server App-V Agent, or upgrades an existing virtual application package on a computer running the Server App-V Agent.
- **Backup-ServerAppvPackageState**

  Backs up the runtime state associated with an existing virtual application package to a specified location.
- **Get-ServerAppvAgent**

  Returns information about the Server App-V Agent.
- **Get-ServerAppvPackage**

  Queries for and retrieves information about a virtual application package that has been deployed to a specified computer running the Server App-V Agent.
- **Remove-ServerAppvPackage**

  Deletes a deployed virtual application package from a specified computer running the Server App-V Agent.
- **Remove-ServerAppvPackageState**

Removes all runtime state associated with a virtual application package and returns the virtual application package to the initial state.

- **Restore-ServerAppvPackageState**

  Restores the runtime state associated with a virtual application package using a backup.

- **Set-ServerAppvPackageConfiguration**

  Configures an existing virtual application package using the deployment configuration document provided.

- **Start-ServerAppvPackage**

  Starts a virtual application package and all associated subsystems.

- **Stop-ServerAppvPackage**

  Stops a virtual application package and all associated subsystems.

Server Application Virtualization Sequencer Cmdlets

To use the Sequencer cmdlets to create packages, you must install the cmdlets and PowerShell 2.0 on the computer running the Sequencer. PowerShell 2.0 remote functionality is supported, so you can use these cmdlets from any computer running PowerShell 2.0.

The following list displays the function names and a brief description of the functions that are currently available for use with Server App-V Sequencer:

- **New-ServerAppVSequencerPackage**

  Creates a new virtual application package.

- **Protect-UpdateConfiguration**

  Encrypts the private values in the deployment configuration document.

- **Unprotect-UpdateConfiguration**

  Decrypts the encrypted sections of a deployment configuration document.

- **Update-ServerAppVSequencerPackage**

  Updates an existing virtual application package.

See Also

Sequencer Console

Dialog Pages

Wizard Pages

Sequencer Console

Click any of the following links for information about the Server App-V Sequencer console.

In This Section

Deployment Configuration Tab

Properties Tab

Change History Tab

Files Tab

Virtual Registry Tab

Virtual File System Tab

OSD Tab

See Also

Server Application Virtualization Cmdlets

Dialog Pages

Wizard Pages

Deployment Configuration Tab

Use the **Deployment Configuration** tab to add, modify, and remove application-specific configuration settings the application will use when it is deployed. For example, if your application needs to connect to a different database depending on whether it is deployed in a staging or production environment, you can include the database name as a deployment configuration item and set it appropriately before deploying to each environment.

Deployment Configuration Items

Name

Displays the name of the configuration item.

Default Value

Displays the value specified for the configuration item when the application was sequenced. If you do not specify a different value at deployment time, this is the value that will be used when the virtual application package is run.

Source

Displays the source of the deployment configuration item. If the item was automatically suggested by a virtualization subsystem, the name of the subsystem is displayed. If it is an item you added manually by searching for it, the source is **Manual**.

Type

Displays the type of configuration item. For example:

- Registry
- INI
- XML
- Credentials

Mandatory

Indicates if the configuration item must be specified when you deploy the virtual application package.

See Also

Sequencer Console

Properties Tab

Use the **Properties** tab to view basic statistical information about a virtual application package. The information is automatically generated unless otherwise noted. This tab contains the following elements.

Package Information

Package Name

Displays a friendly name that describes the virtual application package. This name should be unique across your enterprise.

Comments

Displays a short description of the contents of the virtual application package. This can be used to keep track of helpful information such as version or update levels of the applications contained in the virtual application package.

Package Version

Displays the virtual application package version.

Package GUID

Displays a globally unique identifier automatically assigned to the virtual application package.

Package Version GUID

Displays the virtual application package version GUID. If you upgrade a package to a new version using the Sequencer, both versions of the package will have the same Package GUID but each will have a unique Package Version GUID.

Root Directory

Displays the directory on the computer running the Sequencer to which files for the sequenced virtual application package are installed. This directory is also created on the computer to which a sequenced virtual application package will be streamed. This name must be unique across your enterprise.

Created

Displays the date and time the virtual application package was created.

Modified

Displays the date and time the virtual application package was last modified.

Package Size

Displays the size of the package in megabytes.

Virtualization Subsystems

Displays the different subsystems that were detected when the application was sequenced for example, **IIS** and **COM**.

See Also

Sequencer Console

Change History Tab

After you sequence an application and before you save it, you can use the **Change History** tab to view the historical information about a sequenced application package. This tab is read only and cannot be modified. It contains the following elements.

Modification Date

Modification Date

The date a sequenced application package was modified.

Package Information

Package Version GUID

The GUID for the version of the sequenced virtual application package that is loaded.

Sequencer Information

This section of the **Change History** tab displays specific information about the Server App-V Sequencer (the Sequencer) that was used to create the sequenced application package. It contains the following elements.

Sequencer Version

The version of the Sequencer used to create the package.

Sequenced By

The name of the sequencing engineer.

Sequencing Station

The sequencing computer used to create the sequenced application package.

Package Upgrade

Indicates whether the sequenced application package was upgraded and saved.

Save Mode

Indicates the method used to save the application package.

Windows Information

Windows Version

The version of Windows used to create a sequenced application package.

System Folder

The path on the Sequencing computer of its System folder.

Windows Folder

The location on the sequencing computer of its Windows folder.

User Folder

The location on the sequencing computer of its User folder.

System Type

The type of operating system on the computer running the sequencer.

System Information

Processor

The processor of the sequencing computer system.

Last Boot Normal

Indicates the last time the computer running the sequencer started without any errors.

Terminal Services

Indicates whether Terminal Services is enabled on the computer running the sequencer.

Remote Desktop

Indicates whether Remote Desktop is enabled on the computer running the sequencer.

.NET Framework Version

Indicates the availability of any version of the .NET Framework on the computer running the sequencer.

Internet Explorer Version

Indicates the availability of any version of Internet Explorer on the computer running the sequencer.

Windows Media Player Version

Indicates the availability of any version of Windows Media Player on the computer running the sequencer.

See Also

Sequencer Console

Files Tab

The **Files** tab displays the complete list of files that are included in a sequenced application package. The left pane displays in a standard file browse format the complete list of files in the package that was created during the application sequencing. These files include the package root directory (the directory you specified during the application installation phase), the Virtual File System (VFS) folder, and the virtual environment files. The right pane displays the file name, file attributes, and the Sequencer attributes.

File Name and Short Name

File Name

The name of the file is in the left pane. The files displayed in the left pane are created during sequencing.

Short Name

This is the name of a file selected in the left pane, written in the 8.3 format naming convention.

File Attributes

File Size

The size of the file in bytes.

File Version

The version of the selected file.

Date Created

The date and time the selected file was created.

Date Modified

The date and time the selected file was last modified.

File ID

The file GUID.

Sequencer Attributes

The settings under Sequencer Attributes control how files are treated during upgrade operations on the computer where the application will be deployed.

In general, application binaries (for example, .dll and .exe files) are marked as Application Data by the Sequencer, and all other files are considered User Data. The Sequencer does not set the Override flag on any application files by default. Using the Sequencer controls described here, you can modify these default settings.

To understand how the Server App-V Agent uses these settings during package upgrades, consider the case where an application modifies a file at runtime, and the same file is modified during a package upgrade. When that upgraded package is deployed, the Server App-V Agent has to determine which version of the file to keep, the upgraded one or the one modified at runtime.

User Data

If selected, this file is marked as User Data. If it is changed at runtime, it will not be updated during upgrades unless the Override flag is also set.

Application Data

If selected, this file is marked as Application Data and will be replaced during upgrade regardless of whether it was modified at runtime.

Override

If selected, the Server App-V Agent will ignore the User/Application Data distinction and always replace this file with the upgraded version, even if it was modified at runtime.

If a file is not modified at runtime, it does not matter whether the file was marked as User or Application data. The Server App-V Agent will always choose the upgraded version.

See Also

Sequencer Console

Virtual Registry Tab

A virtual registry is created during sequencing. The **Virtual Registry** tab displays all the registry keys and values that are required for a sequenced application package to run. Use this tab to add, edit, and delete registry keys and registry values.

You can also choose to ignore the hosting system's keys by selecting **Override Local Key**, or you can create a merged view of the key from within the virtual environment by selecting **Merge with Local Key**.

The changes to the virtual registry **Settings** tab affect applications that are part of the specific sequenced application package, but they do not affect the operation of other applications that are streamed to or locally installed on the Application Virtualization Desktop Client.

Note

Exercise caution when changing virtual registry keys and values. Changing these keys and values might render your sequenced application package inoperable.

The left pane of the **Virtual Registry** tab displays the full list of virtual registries created during the sequencing of an application.

Columns

Name

The name for the entry in the virtual registry.

Type

How the entry stores its data.

Data

The value stored by the entry.

Attributes

Displays the file attributes.

See Also

Sequencer Console

Virtual File System Tab

Although an application may install a file to a location such as **C:\Program Files\MyApp\MyApp.exe**, with Server App-V the file is only saved on the file system drive in a location such as **Q:\VFS\CSIDL_PROGRAM_FILES\MyApp\MyApp.exe**. The file does not actually exist in **C:\Program Files\MyApp** at runtime. The Server App-V Agent ensures that

when an application attempts to interact with a file at runtime, the request for the file is redirected to the file's actual location on the file system drive.

The Virtual File System is the set of mappings between files and folders created by the application installer, and their redirected locations on the file system drive. These mappings are created automatically during sequencing. You can use the controls on this tab to add new mappings, edit existing mappings, and delete mappings.

Columns

From

Displays the path where the application will locate the file at runtime, for example **C:\Program Files\MyApp\MyApp.exe**.

To

Displays the path where the file will actually be deployed at runtime, for example **Q:\VFS\CSIDL_PROGRAM_FILES\MyApp\MyApp.exe**.

See Also

Sequencer Console

OSD Tab

An Open Software Descriptor (.osd) file is produced after sequencing for each application detected in the virtual application package. It provides information that enables the Server App-V Agent to configure and open the application it describes. Use the **OSD** tab to display and modify the .osd files in the sequenced virtual application package.

Drop-Down List

Drop down

Displays a list of sequenced applications. Select a sequenced application package to modify the elements of its OSD file.

Navigation Pane

Navigation Pane

Displays a list of elements in the OSD file.

Results Pane

Attribute

Displays one or more attributes of an element.

Value

Displays the value that corresponds to an attribute.

Element Text

Displays an editable comment that corresponds to an element.

See Also

Sequencer Console

Dialog Pages

Click any of the following links for information about the Server App-V dialog pages.

In This Section

Application Selection Page

Best Practices for Server Application Virtualization

Options

See Also

Server Application Virtualization Cmdlets

Sequencer Console

Wizard Pages

Application Selection Page

Use this page to specify if you would like to create a new virtual application package, or modify an existing virtual application package.

This page contains the following elements:

Task List

UIElement List

Create a New Virtual Application Package

Select this option to create a new server virtual application package by installing an application on the computer running the Server App-V Sequencer while the Sequencer monitors the installation. You should also copy all the required installation files to a local directory on the computer running the Sequencer.

Modify an Existing Virtual Application Package

Select this option to modify an existing virtual application package. You can also add a new application to an existing package.

Best Practices for Server Application Virtualization

This topic provides best practices for running Server App-V. You should review and consider the following recommendations when planning and using Server App-V in your environment.

Server App-V Best Practices

- **Deploy virtual application packages to the same drive letter on target computers that was specified when the virtual application package was sequenced.**

  You should always deploy virtual application packages using the same drive letter on target computers running the Server App-V Agent that you specified when you sequenced the package. For example, if you sequenced the application to **Q:\MyApp**, you should deploy the virtual application package to **Q:\MyApp** on the target computer.

- **Never allow untrusted users to create login sessions on datacenter computers.**

  You should never allow untrusted users to connect, for example, by using Remote Desktop Protocol (RDP), to computers running virtual application packages in a data center environment. Additionally, running virtual application packages on computers that have Windows Terminal Services enabled is not supported.

- **Configure the temp directory with enough free disk space.**

  The Sequencer uses the **%TMP%** or **%TEMP%** directory and the **Scratch** directory to store temporary files during sequencing. You should configure these directories on the computer running the Sequencer with free disk space equivalent to the estimated application installation requirements.

- **Sequence on a computer that has a similar configuration and that is running the same version of the operating system as the target computers.**

  Ensure that the computer that is running the Sequencer is running the same version of the operating system as the target computers. This includes the service pack and update versions.

- **Sequence applications using a computer running in a virtual environment.**

  You will sequence most applications more than once. To help facilitate this, you should consider sequencing on a computer running in a virtual environment. This will allow you to sequence an application and revert to a clean state, with minimal reconfiguration, on the computer that is running the Sequencer.

  If you are running Microsoft Hyper-V in your environment the Server App-V Sequencer will run when the computer running Hyper-V virtual is:

  - paused and resumed.
  - has its state saved and restored.
  - saved as a snapshot and is restored.
  - migrated to different hardware as part of a live migration.

- **Before you sequence a new application, shut down other running programs.**

  Processes and scheduled tasks that normally run on the sequencing computer can slow down the sequencing process and cause irrelevant data to be gathered during sequencing. All unnecessary applications and programs should be shut down before you begin sequencing.

- **Sequence on a computer that is running Terminal Services**

You should not configure the install mode on a computer that is running Terminal Services before you install the Sequencer.

See Also

Server Application Virtualization Sequencer Technical Reference

Options

Use the **General** tab to configure options for Server Application Virtualization Sequencer.

UIElement List

Scratch Directory

Specifies the path to the location where the Sequencer will temporarily save files generated during sequencing. The default path is C:\Program Files\Microsoft Application Virtualization Sequencer\Scratch. To specify a new path, click **Browse**.

Log Directory

Specifies the path to the directory where the Sequencer will save log files. The default path is C:\Program Files\Microsoft Application Virtualization Sequencer\Logs. To specify a new path, click **Browse**

Allow Use of MSI Installer

Select this option to allow interaction between the Sequencer and the application installer. This setting is used to determine if the Windows Installer (.msi) file service is allowed to run during monitoring. Without this service running, Windows Installer (.msi) based installations will fail. This option is selected by default.

Allow Microsoft Update to run during monitoring

If you are sequencing an application that receives updates through Microsoft Update, select this option to allow the latest application-specific updates to be retrieved and applied during sequencing.

Note

Be sure to check for updates prior to sequencing so that the operating system and anything installed natively are up to date. Otherwise, running Microsoft Update during sequencing could result in a package containing extra files that could enlarge or corrupt it.

Append Package Version to Filename

When you are upgrading a package, the Sequencer will automatically append the version number of the package to the SFT file name if this option is selected for example, **my_app_3.sft** for the third version of **my_app**. This option is selected by default and is recommended.

OK

Saves changes and closes the dialog box.

Cancel

Exits the dialog box without saving any changes.

Apply

Saves the changes and remains in the dialog box.

Parse Items

The **Parse Items** tab displays the mapping rules that the Sequencer uses to accommodate differences that exist between configurations on the sequencing computer and the App-V Desktop Client. This tab contains the following elements.

Parse From

Displays read-only variable names evaluated by the Application Virtualization Sequencer to determine important operating system locations on the sequencing computer.

Parse To

Displays read-only variable names that the Application Virtualization Sequencer substitutes when encountering variable names in the associated **Parse From** column, while parsing items in the virtual file system or virtual registry.

Map Type

Displays read-only mapping rules that the Application Virtualization Sequencer applies to parse items in the virtual file system or virtual registry.

OK

Saves the changes and exits the dialog box.

Cancel

Exits the dialog box without saving any changes.

Apply

Saves the changes and remains in the dialog box.

Exclusion Items Tab

The **Exclusion Items** tab displays the expressions that the Server App-V Sequencer excludes from the virtual file system or virtual registry. These expressions are excluded to ensure that the sequenced application package can run on computers running the Server App-V Agent. You can also exclude non-standard installation directories that might be unwanted in the sequencing.

UIElement List

Exclude Path

Displays variable names that the Sequencer excludes if encountered while parsing virtual file system items or virtual registry items.

Resolves To

Displays the actual paths that correspond to the Sequencer variables.

Map Type

Displays mapping rules that the Sequencer applies to parse items in the virtual file system or virtual registry.

New

Click to enter a new exclusion item.

Edit

Click to edit a selected exclusion.

Delete

Click to remove a selected exclusion.

OK

Click to accept the displayed exceptions.

Cancel

Click to cancel any changes you have made.

Wizard Pages

Click any of the following links for information about the Microsoft Server Application Virtualization (Server App-V) wizard pages.

In This Section

Create New Package Wizard

See Also

Server Application Virtualization Cmdlets

Sequencer Console

Dialog Pages

Create New Package Wizard

Click any of the following links for information about the Server App-V Create New Package Wizard.

In This Section

Prepare Computer Page

Upgrade Configuration Wizard

Select Installer Page

Package Name Page

Installation Page

Configure Software Page

See Also

Server Application Virtualization Online Help

Prepare Computer Page

Use the **Prepare Computer** to review the issues that might cause the virtual application package creation to fail, or for the package to contain unnecessary data. We strongly recommend that you resolve all potential issues before you continue. After you have fixed the conflicts, to update the information displayed, click **Refresh**. After you have resolved all potential issues, you can proceed to the next step.

This page contains the following elements.

Note
For more detailed information, double-click an item in the list.

UIElement List

Description

Displays the potential conflicting applications or programs that are currently running on the computer running the Server App-V Sequencer.

Resolution

Displays the recommended action to ensure that the computer running the Sequencer has been optimized to create the virtual application package.

Refresh

Refreshes the information displayed in the **Description** pane. After you performed the suggested steps, click **Refresh**.

See Also

Create New Package Wizard

Upgrade Configuration Wizard

Use the **Upgrade Configuration** screen to provide application configuration values to be used during the upgrade process.

This page contains the following elements.

UIElement List

Name

Displays the name of the configuration item.

Description

Displays the description of the configuration item.

Default Value

Displays the current value associated with the configuration item.

Value

You can use this field to specify the updated value that will be assigned to the virtual application package. This field is available after selecting a non-credential configuration item to edit.

Username

You can use this field to modify the username portion of a credential item. This field is available after selecting a credential configuration item to edit.

Password

You can use this field to modify the password portion of a credential item. This field is available after selecting a credential configuration item to edit.

See Also

Create New Package Wizard

Select Installer Page

Use the **Select Installer** page to specify the installation (**.msi**, **.exe**) files or programs for the application that you are sequencing. The files specified on this page must be the actual files that will be used to install the application you are sequencing.

This page contains the following elements:

UIElement List

Select the installer for the application.

Specifies the installation file or files that the sequencer runs and records while creating the virtual application package. You must specify a valid Windows Installer or an executable (**.exe**) program.

Select this option to perform a custom installation.

If you need to do more than just open a single executable or Windows Installer (.msi) file to install your application, select this option. At the appropriate time, the Sequencer will monitor all activity on the computer, allowing you to run programs, move files, use configuration tools, or do anything else you need to do to get your application installed correctly.

See Also

Create New Package Wizard

Package Name Page

Use the **Package Name** page to specify a name for the virtual application package. You can also configure where the package will reside on the target computers.

Note

Editing the primary virtual application directory is not recommended.

This page contains the following elements:

UIElement List

Virtual Application Package Name

Specifies the name that will be associated with virtual application package. The name specified should help identify the purpose and version of the application.

Edit (Advanced)

Select this option to change the root directory in which the virtual application will be installed during sequencing. This root directory will also be used at deployment time and should be unique across your enterprise to avoid conflicts with other packages. Editing the Application Virtualization path is an advanced configuration task. You should fully understand the implications of changing the path. For most applications, we recommend the default path. Only select this option, if you prefer to generate your own file name.

See Also

Create New Package Wizard

Installation Page

If you provided the path to an installer on the **Select Installer** page, the Sequencer will run it for you now. You can use the controls on this page if you need to run additional commands to complete the application's installation.

At this point during sequencing, the Sequencer is monitoring all system activity. You can minimize the Sequencer and perform any installation activities necessary to get your application into a working state.

This page contains the following elements:

UIElement List

Run

Opens the **Select installation file** dialog box. Choose an installation or Windows Installer (.msi) file and click **Open** to have the Sequencer open it. You can use this technique to run multiple installers during a single monitoring session.

I am finished installing

After you have completely finished installing your application (using the **Run** button or interacting directly with the system), select this box to enable **Next**.

See Also

Create New Package Wizard

Configure Software Page

Use the **Configure Software** page to run each program to complete any configuration tasks after the installation. For example, this step helps configure any associated application license agreements.

This page contains the following elements:

UIElement List

Run Selected

Opens only the selected programs associated with the application.

Run All

Opens all programs associated with the application.

See Also

Create New Package Wizard

Troubleshooting Server Application Virtualization

Troubleshooting content is not included in the help content for Microsoft Server Application Virtualization (Server App-V). Instead, troubleshooting information for Server App-V can be found on the TechNet Wiki (http://go.microsoft.com/fwlink/?LinkId=224905).

How to find troubleshooting information

Use the guidance that follows to find troubleshooting and additional information for Server App-V.

Search the documentation

To find help for Server App-V, first perform a scoped search in the Online Help product documentation. If your issue is not addressed in the Online Help documentation, search for Server App-V troubleshooting information in the TechNet Wiki. The TechNet Wiki portal offers guidance contributed by Microsoft teams and community-generated troubleshooting information.

You can also use the Microsoft Server Application Virtualization Team Blog for additional troubleshooting information.

To search the TechNet Wiki

1. In a web browser, locate the TechNet Wiki home page (http://go.microsoft.com/fwlink/?LinkId=224905).
2. In the **Search TechNet Wiki** search box located on the TechNet Wiki home page, enter the search terms or briefly describe your issue. Be sure to include the word “Server App-V” to help scope your search.
3. Review the search results for your issue.

How to create a troubleshooting article

If you have a troubleshooting tip or best practice to share that is not already included in the TechNet Wiki, you can also create your own TechNet Wiki articles.

To create a TechNet Wiki troubleshooting or best practices article

1. In a web browser, locate the TechNet Wiki home page (http://go.microsoft.com/fwlink/?LinkId=224905).
2. Log on with your Windows Live ID.
3. Review the Wiki: Getting Started (http://go.microsoft.com/fwlink/?LinkId=224937) information to learn about the TechNet Wiki and its articles.
4. Select **Post an article >>** at the end of the **Getting Started** section.
5. On the Wiki article **Add Page** page on the tool bar, click **Insert Template**, select the troubleshooting article template (**Troubleshooting.html**), and then click **Insert**.
6. Give the article a descriptive title and then overwrite the template information to create your troubleshooting article.
7. After you review your article, create the following tags to help others find your article:
   - **Troubleshooting**
   - **Server App-V**
8. Click **Save** to publish the article to the TechNet Wiki.

See Also

Server Application Virtualization Overview

Installing Server Application Virtualization

Packaging Applications With Server Application Virtualization

Server Application Virtualization Sequencer Technical Reference

Server Application Virtualization Privacy Statement

Microsoft is committed to protecting your privacy, while delivering software that brings you the performance, power and convenience you desire in your personal computing. This privacy statement explains many of the data collection and use practices of Microsoft Server Application Virtualization (Server App-V). This is a disclosure that focuses on features that communicate with the Internet and is not intended to be an exhaustive list. It does not apply to other online or offline Microsoft sites, products or services.

Collection and Use of Your Personal Information

When we need information that personally identifies you or allows us to contact you, we will explicitly ask you for it. The personal information we collect from you will be used by Microsoft and its controlled subsidiaries and affiliates to provide the service(s) or carry out the

transaction(s) you have requested or authorized, and may also be used to request additional information on feedback that you provide about the product or service that you are using; to provide important notifications regarding the software; to improve the product or service, for example bug and survey form inquiries; to provide you with advance notice of events; or to tell you about new product releases.

Except as described in this statement, personal information you provide will not be transferred to third parties without your consent. We occasionally hire other companies to provide limited services on our behalf, such as packaging, sending and delivering purchases and other mailings, answering customer questions about products or services, processing event registration, or performing statistical analysis of our services. We will only provide those companies the personal information they need to deliver the service, and they are prohibited from using that information for any other purpose.

Information that is collected by or sent to Microsoft may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries or agents maintain facilities, and by using a Microsoft site or service, you consent to any such transfer of information outside of your country. Microsoft abides by the safe harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of data from the European Union. Microsoft may disclose personal information about you if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on Microsoft; (b) protect and defend the rights of Microsoft (including enforcement of our agreements); or (c) act in urgent circumstances to protect the personal safety of Microsoft employees, users of Microsoft products or services, or members of the public.

Collection and Use of Information about Your Computer

Server App-V contains Internet enabled features that can collect information from your computer ("standard computer information") and send it to Microsoft. This information is generally not personally identifiable. Standard computer information typically includes information such as your IP address, operating system version, browser version, your hardware ID which indicates the device manufacturer, device name, and version and your regional and language settings. If a particular feature or service sends information to Microsoft, standard computer information will be sent as well.

The privacy details for each Server App-V feature, software or service listed here will disclose what additional information is collected and how it is used.

Security of your information

Microsoft is committed to protecting the security of your information. We use a variety of security technologies and procedures to help protect your information from unauthorized access, use, or disclosure. For example, we store the information you provide on computer systems with limited access, which are located in controlled facilities.

Changes to this privacy statement

We will occasionally update this privacy statement to reflect changes in our products and services and customer feedback. When we post changes to this Statement, we will revise the "last updated" date at the top of this statement. If there are material changes to this statement or in how Microsoft will use your personal information, we will notify you either by prominently posting a notice of such changes prior to implementing the change or by directly sending you a notification. We encourage you to periodically review this statement to be informed of how Microsoft is protecting your information.

For More Information

Microsoft welcomes your comments regarding this privacy statement. If you believe that Microsoft has not adhered to this statement, please contact us via email (appvdocs@microsoft.com) or using the address provided here and we will use commercially reasonably efforts to promptly determine and remedy the problem.

Microsoft Privacy

Microsoft Corporation

One Microsoft Way

Redmond, WA 98052

Microsoft Update

What This Feature Does:

Microsoft Update is a service that provides Windows updates as well as updates for other Microsoft software.

Information Collected, Processed, or Transmitted:

For details about what information is collected and how it is used, see the Update Services Privacy Statement at http://go.microsoft.com/fwlink/?LinkID=115475.

Use of Information:

For details about what information is collected and how it is used, see the Update Services Privacy Statement at http://go.microsoft.com/fwlink/?LinkID=115475.

Customer Experience Improvement Program

What This Feature Does:

The anonymous information CEIP collects includes the type and number of errors console users encounter, software and hardware performance, and the speed of services. We do not collect names, addresses or other contact information.

This feature generates a Globally Unique Identifier (GUID) that is stored on your computer to uniquely identify it. The GUID is a randomly generated number; it does not contain any personal information and will not be used to identify console users. CEIP uses the GUID to distinguish how widespread the feedback we receive is and how to prioritize it. For example, this number allows Microsoft to distinguish between one customer having an error 100 times and 100 customers having the same error once. The GUID is persistent.

Use of Information:

We use this information to improve the quality, reliability, and performance of Microsoft software and services.

Error Reporting

What This Feature Does:

The Error Reporting feature provides a service which allows you to report problems you may be having with Server App-V to Microsoft and to receive information that may help you get around or solve such problems.

Information Collected, Processed, or Transmitted:

The Error Reporting feature collects Internet Protocol (IP) addresses, which are not used to identify users. It does not intentionally collect anyone's name, address, email address, computer name, or any information that will be used to identify you or contact you. It is possible that such information may be captured in memory or in the data collected from open files, but Microsoft does not use it to identify or contact you.

In rare cases, such as problems that are especially difficult to solve, Microsoft may request additional data, including sections of memory (which may include memory shared by any or all applications running at the time the problem occurred), some registry settings, and one or more files from your computer. Your current documents may also be included. For more details on what information is collected and how it is used, see the Error Reporting privacy information at http://go.microsoft.com/fwlink/?linkid=31490.

Use of Information:

We use the error reporting data to solve customer problems and improve our software and services.

Choice/Control:

On Windows Server 2008 family operating systems, error reporting is enabled by default but you can configure or disable error reporting any time through **Enable automatic updating and feedback** in the **Initial Configuration Tasks** window, or through **Windows Error Reporting** in the **Resources and Support** area of Server Manager.

Enterprise customers can use Group Policy to configure how Error Reporting behaves on their computers. Configuration options include the ability to completely turn off Error Reporting. If you are an administrator and wish to configure Group Policy for Error Reporting, technical details are available at http://go.microsoft.com/fwlink/?LinkId=120553 for Windows Server 2008.