

# Technical Documentation for System Center 2012 – Virtual Machine Manager

VMM Information Experience Team

## Guide

# Technical Documentation for System Center 2012 – Virtual Machine Manager

VMM Information Experience Team

**Summary:** 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.

**Category:** Guide

**Applies to:** System Center 2012 – Virtual Machine Manager (VMM) and Virtual Machine Manager in System Center 2012 Service Pack 1

**Source:** TechNet Library(<http://go.microsoft.com/fwlink/p/?LinkID=263937>)

**E-book publication date:** April 2013

Copyright © 2013 by Microsoft Corporation

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Microsoft and the trademarks listed at <http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx> are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

# Contents

---

Getting Started with System Center 2012 - Virtual Machine Manager .....	2
System Requirements for System Center 2012 - Virtual Machine Manager .....	26
Deploying System Center 2012 - Virtual Machine Manager .....	47
Upgrading to System Center 2012 - Virtual Machine Manager .....	89
Upgrading to VMM in System Center 2012 SP1.....	115
Administering System Center 2012 - Virtual Machine Manager.....	135
Configuring Security in System Center 2012 - Virtual Machine Manager.....	464
Troubleshooting System Center 2012 - Virtual Machine Manager.....	479
Glossary for System Center 2012 - Virtual Machine Manager.....	480
Microsoft Server Application Virtualization .....	484

# 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 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.

## Deploying VMM

A deployment of VMM consists of the following:

Name	Description
VMM management server	The computer on which the Virtual Machine Manager service runs and which 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.
VMM console	The program that allows you to connect to a VMM management server 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

Name	Description
	<p>hard disks, templates, and profiles) that are used to deploy virtual machines and services.</p> <p>A library server hosts shared folders that are used to store file-based resources in the VMM library.</p>
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)   <b>Note</b> In System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed.	A web site that users who are assigned to a self-service user role can use to deploy and manage their own virtual machines to 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
Create user roles	Create self-service users, delegated administrators, and read-only administrators to ensure users can perform the appropriate actions on the appropriate resources in VMM.	<a href="#">Creating User Roles in VMM</a>
Configure Run As accounts	Create Run As accounts to provide the necessary credentials for performing operations in VMM.	<a href="#">Configuring Run As Accounts in VMM</a>

## Configuring Fabric Resources in VMM

VMM enables you to configure and manage the following resources. These resources need to be configured before you can deploy virtual machines and services to a private cloud or to virtual machine hosts.

Resource	Description	For more information
Virtual machine hosts	<p>Microsoft Hyper-V, Citrix XenServer, and VMware ESX hosts and host clusters on which you will deploy virtual machines and services.</p> <p>You can create host groups to organize your hosts based on physical site location, resource allocation, or some other criteria.</p>	<p><a href="#">Adding and Managing Hyper-V Hosts and Host Clusters in VMM</a></p> <p><a href="#">Managing Citrix XenServer Overview</a></p> <p><a href="#">Managing VMware ESX Hosts Overview</a></p> <p><a href="#">Creating Host Groups Overview</a></p>
Networking	Networking resources, such as logical networks, IP address pools, and load balancers that are used to deploy virtual machines and services.	<p><a href="#">Configuring Networking Overview</a></p>
Storage	Storage resources, such as storage classifications, logical units, and storage pools that are made available to Hyper-V hosts and host clusters.	<p><a href="#">Configuring Storage Overview</a></p>
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.	<p><a href="#">Configuring the Library Overview</a></p>

## Deploying Virtual Machines and Services in a Private Cloud in VMM

After you have configured 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. For example, a deployment of a multi-tier line of business application.

Task	Description	For more information
Create private clouds	Combine hosts and networking, storage, and library resources together to create a private cloud.	<a href="#">Creating a Private Cloud in VMM Overview</a>
Create sequenced applications	Use Microsoft Server Application Virtualization (Server App-V) to sequence applications to be deployed by VMM.	<a href="#">Microsoft Server Application Virtualization</a>
Create profiles	<p>Create profiles (hardware profiles, guest operating system profiles, application profiles, and SQL Server profiles) that will be used in a virtual machine template to deploy virtual machines.</p> <p>For example, an application profile provides instructions for installing Microsoft 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.</p>	<a href="#">Creating Profiles in VMM</a>
Create virtual machine	Create virtual machine templates	<a href="#">How to Create a Virtual Machine</a>

Task	Description	For more information
templates	that can be used to create new virtual machines and to configure tiers in services.	<a href="#">Template</a>
Create service templates	Use the Service Template Designer to create service templates that can be used to deploy services.	<a href="#">Creating Service Templates in VMM</a>
Deploy virtual machines	Deploy virtual machines to private clouds or hosts by using virtual machine templates.	<a href="#">Creating and Deploying Virtual Machines in VMM</a>
Deploy services	Deploy services to private clouds or hosts by using a service template.	<a href="#">Creating and Deploying Services in VMM</a>
Scale out a service	Add additional virtual machines to a deployed service.	<a href="#">Scaling Out a Service in VMM</a>
Update a service	Make changes to a deployed service.	<a href="#">Updating a Service in VMM</a>

## 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 servers (for example, Hyper-V hosts and library servers)	Scan servers (for example, Hyper-V hosts and library servers) for update compliance, view update compliance status, and perform update remediation by using a Windows Server Update Services	<a href="#">Managing Fabric Updates in VMM</a>

Task	Description	For more information
	(WSUS) server.	
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).	<a href="#">Configuring Operations Manager Integration with VMM</a>

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

This topic provides categorized lists of several tasks that you can perform in System Center 2012 – Virtual Machine Manager (VMM). These are followed by a section that describes what was added specifically in System Center 2012 Service Pack 1 (SP1), [What's New in System Center 2012 SP1](#).

For an overview of VMM, see [Overview of System Center 2012 - Virtual Machine Manager](#).

### Deploying VMM

Task	For more information
Install a highly available VMM management server.	<a href="#">Installing a Highly Available VMM Management Server</a>

### Configuring Security in VMM

Task	For more information
Create Run As accounts to provide the necessary credentials for performing operations in VMM.	<a href="#">Configuring Run As Accounts in VMM</a>
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.	<a href="#">Creating User Roles in VMM</a>
Create a Read-Only Administrator user role	<a href="#">Configuring Run As Accounts in VMM</a>

## 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.	<a href="#">Adding Physical Computers as Hyper-V Hosts in VMM Overview</a>
Use the VMM console to create a Hyper-V cluster from two or more standalone Hyper-V hosts that are managed by VMM.	<a href="#">Creating and Modifying Hyper-V Host Clusters in VMM</a>
Use Citrix XenServer as a virtual machine host.	<a href="#">Managing Citrix XenServer Overview</a>
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.	<a href="#">Configuring Networking in VMM Overview</a>
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.	<a href="#">Configuring Storage in VMM Overview</a>
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.	<a href="#">Managing Fabric Updates in VMM</a>
Perform resource balancing by migrating virtual machines within host clusters that support live migration (Dynamic Optimization).	<a href="#">Configuring Dynamic Optimization and Power Optimization in VMM</a>

Task	For more information
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).	<a href="#">Configuring Dynamic Optimization and Power Optimization in VMM</a>

## 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.	<a href="#">Creating a Private Cloud in VMM Overview</a>
Use Server Application Virtualization (Server App-V) to sequence applications to be deployed by VMM.	<a href="#">Microsoft Server Application Virtualization</a>
Create a custom capability profile to limit the resources that are used by virtual machines that are created in a private cloud.	<a href="#">How to Create a Private Cloud from Host Groups</a>
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.	<b>How to Create an Application Profile [VMM 2012]</b>
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.	<b>How to Create a SQL Server Profile [VMM 2012]</b>
Deploy virtual machines to private clouds by	<a href="#">Creating and Deploying Virtual Machines</a>

Task	For more information
using virtual machine templates.	
Use the Service Template Designer to create service templates that can be used to deploy services.	<b>Creating Service Templates in VMM</b>
Deploy services to private clouds or hosts by using a service template.	<a href="#">Creating and Deploying Services in VMM</a>
Scale out a service: Add additional virtual machines to a deployed service.	<b>Scaling Out a Service in VMM</b>
Update a service: Make changes to a deployed service.	<b>Updating a Service in VMM</b>
Export and import service templates and virtual machine templates.	<b>Exporting and Importing Service Templates in VMM</b>

### What's New 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 (synthetic) fiber channels that are configured for virtual machines in Hyper-V.

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	For a complete list of supported and required


Deploying VMM	For more information
versions of operating systems and other required software.	configurations, see <a href="#">System Requirements for System Center 2012 - Virtual Machine Manager</a> .
Integration with Windows Server 2012 which delivers numerous enhancements to the Microsoft Hyper-V features, as follows: <ul style="list-style-type: none"> <li>• Large virtual machines</li> <li>• Clusters that can support a larger numbers of nodes</li> <li>• Storage management through SMI-S (Storage Management Initiative – Specification)</li> </ul>	See the Supported Storage Arrays section in <a href="#">Configuring Storage Overview</a> .
Ability to manage vSphere 5.1 and Citrix XenServer 6.0 .	For more information about Citrix, see <a href="#">Managing Citrix XenServer Overview</a> . For more information about vSphere see <a href="#">How to Add VMware ESX Hosts to VMM</a> and <a href="#">How to Configure Network Settings on a VMware ESX Host</a> .

Configuring Fabric Resources in VMM - Networks	For more information
New model for virtual machine networking, including network virtualization and virtual local area networks (VLANs) for network isolation.	<a href="#">Network Virtualization</a>  <a href="#">How to Create a VM Network in System Center 2012 SP1</a>
Management of the Hyper-V extensible switch, including deployment and configuration of virtual switch extensions using a new logical switch concept.	<a href="#">How to Add a Virtual Switch Extension Manager in System Center 2012 SP1</a>

Configuring Fabric Resources in VMM - Networks	For more information
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.	<a href="#">Network Virtualization</a>
Software-defined networking with support for Hyper-V network virtualization and switch extension management. This allows a constant network configuration in the datacenter.	<a href="#">Configuring VM Networks and Gateways in System Center 2012 SP1</a> <a href="#">Configuring Ports and Switches for VM Networks in System Center 2012 SP1</a> <a href="#">How to Add a Virtual Switch Extension Manager in System Center 2012 SP1</a>
Introduction of a logical switch that allows you to manage individual switch instances across multiple Hyper-V hosts as a single entity.	<a href="#">How to Create a Logical Switch in System Center 2012 SP1</a>
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.	<a href="#">How to Create a Logical Switch in System Center 2012 SP1</a>

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	<p>For more information about SMB 3.0 in Windows Server 2012, see <a href="#">Server Message Block Overview</a>.</p> <p>For more information about how to create a highly available SMB 3.0 file share, see <a href="#">Scale-Out File Server for Application Data Overview</a>,</p>

Configuring Fabric Resources in VMM - Storage	For more information
<p>for virtual machine files, such as configuration, virtual hard disk (.vhd/.vhdx) files and checkpoints.</p> <p>SMB 3.0 file shares provide the following benefits when they are used with VMM in this release:</p> <ul style="list-style-type: none"> <li>• Hyper-V over SMB supports file servers and storage with improved efficiency compared to traditional storage area networks (SANs).</li> <li>• 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.</li> </ul> <p>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.</p>	<p>and steps 1 and 2 of the Deploy Scale-Out File Server scenario that is linked to from that topic.</p>
<p>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</p>	<p><a href="#">Configuring Storage Overview</a></p>

Configuring Fabric Resources in VMM - Storage	For more information
<p>WMI-based programming interface that is included in Windows Server 2012. This new API enables you to discover storage by using multiple provider types.</p> <p> <b>Important</b> The Windows Storage Management API supersedes the Virtual Disk Service (VDS) interface. Therefore, if you are using a storage array that uses 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.</p> <p>In this release, VMM supports the following types of storage providers and arrays:</p> <ul style="list-style-type: none"> <li>• 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 <a href="#">Configuring Storage Overview</a>.</li> <li>• Symmetric multiprocessing (SMP)</li> </ul> <p>Supported array: Dell EqualLogic PS Series using iSCSI.</p>	

Configuring Fabric Resources in VMM - Storage	For more information
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.	<a href="#">How to Discover Physical Computers and Deploy as Hyper-V Hosts in VMM</a>
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 <i>deep discovery</i> 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	<a href="#">How to Discover Physical Computers and Deploy as Hyper-V Hosts in VMM</a>  <a href="#">How to Create a Host Profile in VMM</a>

<b>Configuring Fabric Resources in VMM - Hyper-V</b>	<b>For more information</b>
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.	
Support for physical network adapter configuration as follows: <ul style="list-style-type: none"> <li>• IP configuration</li> <li>• Logical switch creation</li> <li>• NIC Teaming</li> </ul>	
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.	

<b>Virtual Machines and Services</b>	<b>For more information</b>
Support for deployment of services to virtual machines in a domain or workgroup that does not have a trust relationship with the domain of the VMM management server.	<b>Preparing to Create Services in VMM</b>
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,	<b>Preparing to Create Services in VMM</b>

Virtual Machines and Services	For more information
or to both.	
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.	<b>How to Create a SQL Server Profile</b>
<p>Application profiles:</p> <ul style="list-style-type: none"> <li>• For the deployment of application packages, added support for updated versions of the following applications: <ul style="list-style-type: none"> <li>• Web Deploy 3.0</li> <li>• Data-tier Application Framework (DAC Fx) 3.0</li> <li>• Server App-V SP1</li> </ul> </li> <li>• 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.</li> <li>• 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).</li> </ul>	<b>How to Create an Application Profile</b>
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.	<b>How to Apply Updates to a Deployed Service in VMM</b>
Support for the new version of the virtual hard	For more information about the benefits of the

Virtual Machines and Services	For more information
<p>disk format that is introduced in Windows Server 2012. This new format is referred to as 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.</p> <p>Support for VHDX includes the following:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• You can use VMM to "rapidly provision" any virtual machines that use VHDX-based virtual hard disks from SAN-copy capable templates.</li> <li>• A VMM library server that runs Windows Server 2012 automatically indexes .vhdx files.</li> <li>• In addition to the small and large blank</li> </ul>	<p>VHDX format in Windows Server 2012, see <a href="#">Hyper-V Virtual Hard Disk Format Overview</a>.</p> <p><a href="#">Rapid Provisioning of Virtual Machines Using SAN Copy Overview</a></p>


Virtual Machines and Services	For more information
<p>.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.</p>	
<p>Support for provisioning a physical computer as a Hyper-V host. When you provision a physical 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.</p>	<p>For background information about adding a physical computer as a Hyper-V host, see <a href="#">Adding Physical Computers as Hyper-V Hosts Overview</a>.</p>
<p>Linux-based virtual machines are now fully supported with the following:</p> <ul style="list-style-type: none"> <li>Added settings for Linux-specific operating system specialization when you are creating a Linux-based virtual machine template.</li> </ul> <p> <b>Important</b> These settings are supported only when the Linux virtual machine is deployed on Hyper-V.</p> <ul style="list-style-type: none"> <li>Ability to include a Linux virtual machine template in a service template that deploys a multi-tier application or service.</li> <li>Updated Windows PowerShell cmdlets to support this new functionality.</li> </ul>	<p><b>How to Create a Virtual Machine Template</b></p> <p><b>Requirements for Linux-Based Virtual Machines</b></p>
<p>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.</p>	<p><b>Configuring Availability Options for Virtual Machines</b></p>

Live Migration	For more information
<p>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.</p>	<p>For more information about live migration in Windows Server 2012, see the following topics:</p> <ul style="list-style-type: none"> <li>• <a href="#">Virtual Machine Live Migration Overview</a></li> <li>• <a href="#">Virtual Machine Storage Migration Overview</a></li> <li>• <a href="#">Migrating virtual machines and storage in System Center SP1 - Virtual Machine Manager</a></li> </ul>
<p>Live migration between nodes in two different clusters. You can migrate between nodes within a cluster, or between nodes in different clusters.</p>	<p><b>Migrating virtual machines and storage in System Center SP1 - Virtual Machine Manager</b></p> <p><b>How to configure live virtual machine and storage migration in System Center SP1 - Virtual Machine Manager</b></p>
<p>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.</p>	<p><b>Migrating virtual machines and storage in System Center SP1 - Virtual Machine Manager</b></p> <p><b>How to configure live virtual machine and storage migration in System Center SP1 - Virtual Machine Manager</b></p>
<p>Live VSM. By using live virtual system migration (VSM) you can migrate both virtual machines and storage in a single action.</p>	<p><b>Migrating virtual machines and storage in System Center SP1 - Virtual Machine Manager</b></p> <p><b>How to configure live virtual machine and storage migration in System Center SP1 - Virtual Machine Manager</b></p>
<p>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</p>	<p><b>Migrating virtual machines and storage in System Center SP1 - Virtual Machine Manager</b></p> <p><b>How to configure live virtual machine and</b></p>

Live Migration	For more information
manually. Attempted concurrent live migrations in excess of the limit will be queued.	<b>storage migration in System Center SP1 - Virtual Machine Manager</b>

VMM Console	For more information
<p>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:</p> <ul style="list-style-type: none"> <li>• Add ribbon entries in the VMM console to launch web browsers and Windows applications directly from the ribbon.</li> <li>• Enable new actions or additional configuration for VMM objects by writing an application that uses context that is passed regarding the selected VMM objects.</li> <li>• 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.</li> </ul>	<p><a href="#">Virtual Machine Manager Add-in SDK</a> in the TechNet Wiki.</p>
<p>Several significant performance enhancements 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.</p>	
<p>Overview pages in the VMM console now display various reports about usage and capacity metrics for services, tenants and</p>	

VMM Console	For more information
clouds.	

Additional Improvements	For more information
<p>Performance and scalability:</p> <ul style="list-style-type: none"> <li>Increased the scale of a VMM management server to be able to manage 1000 hosts and 25,000 virtual machines.</li> </ul> <p> <b>Note</b> Scale limits remain consistent no matter which supported hypervisors are used. VMM can manage 25,000 virtual machines, wherever they are located.</p> <ul style="list-style-type: none"> <li>Support for a 64 node cluster.</li> <li>Performance enhancement to the VMM console.</li> </ul>	
<p>Integration with Operation Manager as follows:</p> <ul style="list-style-type: none"> <li>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.</li> <li>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 reallocated to meet the demand.</li> <li>Generate reports that track the resource usage of each configured service or service</li> </ul>	<p><b>Configuring Operations Manager Integration with VMM</b></p>

Additional Improvements	For more information
user, to aid in capacity planning.	
Support for updateable Help for VMM cmdlets.	<p>Type the following command in a command shell:</p> <pre>Get-Help about_VMM_2012_Updating_Help</pre>

## 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](#).

## 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.	<a href="#">Microsoft Download Center</a>

### Documentation for VMM

The following documentation is available for VMM:

Name	Description	Location
VMM technical documentation	Provides content about VMM for the following areas:	<a href="#">Virtual Machine Manager</a> in the TechNet Library

Name	Description	Location
	<ul style="list-style-type: none"> <li>• Getting Started</li> <li>• Deploying</li> <li>• Administering</li> <li>• Configuring Security</li> <li>• Scripting</li> </ul>	
VMM troubleshooting content	<p>Provides information about troubleshooting VMM.</p> <p>For example, a list of known issues with VMM, and possible resolutions or workarounds for those known issues.</p>	<a href="#">Troubleshooting System Center 2012 - Virtual Machine Manager</a> 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.	<a href="#">Microsoft Download Center</a>
VMM cmdlet reference (download)	Provides the VMM cmdlet help topics.	<a href="#">Microsoft Download Center</a>
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.	<a href="#">Microsoft Server Application Virtualization</a> in the TechNet Library
Release Notes for VMM in System Center 2012 Service Pack 1 (SP1)	Provides information about issues and workarounds for VMM in System Center 2012 Service Pack 1 (SP1)	<a href="#">Release Notes for System Center 2012 Service Pack 1 – Virtual Machine Manager</a>

## 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](#).

## System Requirements for System Center 2012 - Virtual Machine Manager

---

This section provides information about system requirements and supported operating systems to install and run Virtual Machine Manager (VMM).

The following topics are covered:

- [System Requirements: VMM Management Server](#)
- [System Requirements: VMM Console](#)
- [System Requirements: VMM Self-Service Portal](#)
- [System Requirements: VMM Database](#)
- [System Requirements: VMM Library Server](#)
- [System Requirements: Virtual Machine Hosts](#)
- [System Requirements: Hyper-V Host Deployment to a Bare-Metal Computer](#)
- [System Requirements: Update Management](#)
- [System Requirements: Monitoring and Reporting](#)

For more information about system requirements for System Center 2012 Service Pack 1 (SP1), see **System Requirements for System Center 2012 SP1**.

### System Requirements: VMM Management Server

#### Hardware requirements

The following tables list the minimum and recommended hardware requirements for the VMM management server, based on the number of hosts that you manage.

#### Managing up to 150 hosts

Hardware component	Minimum	Recommended
Processor	Pentium 4, 2 GHz (x64)	Dual-Processor, Dual-Core, 2.8 GHz (x64) or greater
RAM	2 GB	4 GB
Hard disk space - without a local VMM database	2 GB	40 GB
Hard disk space - with a local, full version of Microsoft SQL Server	80 GB	150 GB



#### Note

If you use the VMM management server as a library server, you must provide additional hard disk space to store objects. For more information about the requirements for a VMM library server, see [System Requirements: VMM Library Server](#).

### Managing more than 150 hosts

Hardware component	Minimum	Recommended
Processor	Pentium 4, 2.8 GHz (x64)	Dual-Processor, Dual-Core, 3.6 GHz or greater (x64)
RAM	4 GB	8 GB
Hard disk space	10 GB	50 GB




#### Note

For better performance when you manage more than 150 hosts, it is recommended that you use a dedicated computer for the VMM management server and do the following:

- Add one or more remote computers as library servers and do not use the default library share on the VMM management server.
- Use a version of SQL Server that is installed on a different computer for the VMM database.

### Software requirements

Before you install the VMM management server, you must install the following software.

Software	Notes
A supported operating system	For more information, see <a href="#">Supported operating systems</a> in this topic.
Windows Remote Management (WinRM) service	<p>WinRM 2.0 is included in Windows Server 2008 R2, and by default, the Windows Remote Management (WS-Management) service is set to start automatically (delayed start).</p> <p> <b>Note</b> If the Windows Remote Management (WS-Management) service is not started, the setup process will display an error during the prerequisites check. The service must be started before setup can continue.</p> <p>WinRM is included in Windows Server 2012, and by default, the Windows Remote Management (WS-Management) service is set to start automatically.</p>
<p>Microsoft .NET Framework:</p> <ul style="list-style-type: none"> <li>For System Center 2012 – Virtual Machine Manager: At least Microsoft .NET Framework 3.5 Service Pack 1 (SP1)</li> <li>For VMM in System Center 2012 SP1: Microsoft .NET Framework 4, or Microsoft .NET Framework 4.5</li> </ul>	<p>To obtain Microsoft .NET Framework:</p> <ul style="list-style-type: none"> <li>On a computer that runs Windows Server 2008 R2, if the Microsoft .NET Framework 3.5.1 feature is not installed (it is not installed by default), the VMM setup wizard will install the feature.</li> <li>Microsoft .NET Framework 4 is included in Windows Server 2012.</li> <li>Microsoft .NET Framework 4.5 is available at the <a href="#">Visual Studio 2012 Download</a> page.</li> </ul>
Windows deployment and installation kit:	To obtain a Windows deployment and

Software	Notes
<ul style="list-style-type: none"> <li>For System Center 2012 – Virtual Machine Manager: Windows Automated Installation Kit (AIK) for Windows 7</li> <li>For VMM in System Center 2012 SP1: Windows Assessment and Deployment Kit (ADK) for Windows 8</li> </ul>	<p>installation kit:</p> <ul style="list-style-type: none"> <li>Windows AIK is available on the <a href="#">Microsoft Download Center</a>. To install the Windows AIK, you can download the ISO file, write the ISO file to a DVD by using a third party tool, and then install the Windows AIK from the DVD.</li> <li>Windows ADK is available at the <a href="#">Microsoft Download Center</a>. When you install Windows ADK, select the <b>Deployment Tools</b> and the <b>Windows Preinstallation Environment</b> features.</li> </ul>
A supported version of SQL Server	For more information about the supported versions of SQL Server, see <a href="#">System Requirements: VMM Database</a> .

### Supported operating systems

For System Center 2012 – Virtual Machine Manager	Edition	Service pack	System architecture
Windows Server 2008 R2 (full installation)	Standard, Enterprise, and Datacenter	Service Pack 1 or earlier	x64

For VMM in System Center 2012 SP1	Edition	Service pack	System architecture
Windows Server 2012 (full installation or Server Core installation)	Standard and Datacenter	N/A	x64

### Additional information

- The computer on which you install the VMM management server must be a member of an Active Directory domain.
- The name of the computer on which you install the VMM management server cannot exceed 15 characters.



#### Note

The computer name cannot contain the character string of **–SCVMM–**, but you can use the character string of **SCVMM** in the computer name. For example, the computer name can be SEASCVMMLAB, but the computer name cannot be SEA-SCVMM-LAB.

- If you install the VMM management server in a virtual machine and you use the Dynamic Memory feature of Hyper-V, you must set the startup RAM for the virtual machine to be at least 2048 MB.
- VMM allows you to install a highly available VMM management server on a failover cluster that runs any supported operating system.

For information about how to install a VMM management server, see [Installing a VMM Management Server](#) and [Installing a Highly Available VMM Management Server](#).

## System Requirements: VMM Console

### Hardware requirements

The following requirements are the minimum and recommended hardware requirements for the VMM console, based on the number of hosts that you manage.

#### Managing up to 150 hosts

Hardware component	Minimum
Processor	Pentium 4, 1 GHz or greater
RAM	2 GB
Hard disk space	2 GB

#### Managing more than 150 hosts

Hardware component	Minimum
Processor	Pentium 4, dual processor, 2 GHz or greater
RAM	4 GB
Hard disk space	4 GB

## Software Requirements

The following software must be installed before you install the VMM console.

Software	Notes
A supported operating system for the VMM console	For more information, see <a href="#">Supported operating systems</a> in this topic.
<p>Windows PowerShell:</p> <ul style="list-style-type: none"> <li>For System Center 2012 – Virtual Machine Manager: Windows PowerShell 2.0</li> <li>For VMM in System Center 2012 SP1: Windows PowerShell 3.0</li> </ul>	<ul style="list-style-type: none"> <li>Windows PowerShell 2.0 is included in Windows Server 2008 R2 and Windows 7.</li> <li>Windows PowerShell 3.0 is included in Windows Server 2012. Otherwise, you can install Windows PowerShell 3.0 from <a href="http://go.microsoft.com/fwlink/p/?LinkId=262217">http://go.microsoft.com/fwlink/p/?LinkId=262217</a>.</li> </ul>
<p>Microsoft .NET Framework:</p> <ul style="list-style-type: none"> <li>For System Center 2012 – Virtual Machine Manager: At least Microsoft .NET Framework 3.5 Service Pack 1 (SP1)</li> <li>For VMM in System Center 2012 SP1: Microsoft .NET Framework 4, or Microsoft .NET Framework 4.5</li> <li>For the VMM Console in System Center 2012 SP1: Microsoft .NET Framework 4.5 is required for computers running Windows</li> </ul>	<ul style="list-style-type: none"> <li>On a computer that runs Windows 7, Microsoft .NET Framework 3.5.1 is installed by default.</li> <li>On a computer that runs Windows Server 2008 R2, if the Microsoft .NET Framework 3.5.1 feature is not installed (it is not installed by default), the VMM setup wizard will install the feature.</li> <li>On a computer that runs Windows 8 or/and Windows Server 2012, Microsoft .NET Framework 4 is included.</li> <li>Microsoft .NET Framework 4.5 is available at</li> </ul>

Software	Notes
Server 2008 R2 and Windows 7	the <a href="#">Visual Studio 2012 Download</a> page.

### Supported operating systems

Operating system for System Center 2012 – Virtual Machine Manager	Edition	System architecture
Windows Server 2008 R2 Service Pack 1 or earlier (full installation)	Standard, Enterprise, and Datacenter	x64
Windows 7 Service Pack 1 or earlier	Professional, Enterprise, and Ultimate	x86 and x64

Operating system for VMM in System Center 2012 SP1	Edition	System architecture
Windows Server 2008 R2 Service Pack 1 (full installation)	Standard, Enterprise, and Datacenter	x64
Windows 7 with or without Service Pack 1	Professional, Enterprise, and Ultimate	x86 and x64
Windows Server 2012	Standard and Datacenter	64bit
Windows 8 Client	Professional and Enterprise	32bit and 64bit

### Additional information

- The computer on which you install the VMM console must be a member of an Active Directory domain.
- For information about how to install the VMM console, see [Installing and Opening the VMM Console](#).

## System Requirements: VMM Self-Service Portal



### Note

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

## Hardware Requirements

The following tables provide the minimum and recommended hardware requirements for the VMM Self-Service Portal based on the number of concurrent connections that are maintained on the Web server.

### Maintaining up to 10 concurrent connections

Hardware component	Minimum	Recommended
Processor	Pentium 4, 2.8 GHz	Pentium 4, 2.8 GHz
RAM	2 GB	2 GB
Hard disk space	512 MB	20 GB

### Maintaining more than 10 concurrent connections

Hardware component	Minimum	Recommended
Processor	Pentium 4, 2.8 GHz	Dual-Core 64-bit, 3.2 GHz or greater
RAM	2 GB	8 GB
Hard disk space	10 GB	40 GB

## Software Requirements

The following software must be installed prior to installing the VMM Self-Service Portal.

Software Requirement	Notes
A supported operating system	For more information, see <a href="#">Supported Operating Systems</a> later in this topic.
Web Server (IIS)	<p>You must install the Web Server (IIS) role and the following Web Server (IIS) features:</p> <ul style="list-style-type: none"> <li>• .NET Extensibility</li> <li>• ASP.NET</li> <li>• Default Document</li> <li>• Directory Browsing</li> <li>• HTTP Errors</li> <li>• IIS 6 Metabase Compatibility</li> <li>• IIS 6 WMI Compatibility</li> <li>• ISAPI Extensions</li> <li>• ISAPI Filters</li> <li>• Request Filtering</li> <li>• Static Content</li> </ul>
Windows PowerShell 2.0	Windows PowerShell 2.0 is included in Windows Server 2008 R2.
At least Microsoft .NET Framework 3.5 Service Pack 1 (SP1)	On a computer running Windows Server 2008 R2, if the .NET Framework 3.5.1 feature is not installed (it is not installed by default), the VMM setup wizard will install the feature.

## Supported Operating Systems

Operating System	Edition	Service Pack	System Architecture
Windows Server 2008 R2 (full installation)	Standard, Enterprise, and Datacenter	Service Pack 1 or earlier	x64



### Important

Installing the VMM Self-Service Portal on a computer that is running Windows Server® 2012 is not supported.

### Additional information

- Installing the VMM Self-Service Portal on a domain controller is not supported.
- To use the VMM Self-Service Portal, client computers must be running Internet Explorer 8 or Internet Explorer 9.
- For better performance, it is recommended that you install the VMM Self-Service Portal on a separate computer from the VMM management server.

For information about installing the VMM Self-Service Portal, see [Installing and Opening the VMM Self-Service Portal](#).

## System Requirements: VMM Database

### Hardware requirements

The following tables provide the minimum and recommended hardware requirements for the VMM database. These requirements are based on the number of hosts that you manage.

#### Managing up to 150 hosts

Hardware component	Minimum	Recommended
Processor	Pentium 4, 2.8 GHz	Dual-Core 64-bit, 2 GHz
RAM	2 GB	4 GB
Hard disk space	80 GB	150 GB

#### Managing more than 150 hosts

Hardware component	Minimum	Recommended
Processor	Dual-Core 64-bit, 2 GHz	Dual-Core 64-bit, 2.8 GHz
RAM	4 GB	8 GB
Hard disk space	150 GB	200 GB

### Supported versions of Microsoft SQL Server

To host the VMM database, VMM supports the following versions of SQL Server.

SQL Server for System Center 2012 – Virtual Machine Manager	Service Pack	Editions
SQL Server 2008 R2 (64-bit)	Service Pack 1 or earlier	Standard, Enterprise, and Datacenter
SQL Server 2008 (64-bit)	Service Pack 2 or Service Pack 3	Standard and Enterprise

SQL Server for VMM in System Center 2012 SP1	Service Pack	Editions
SQL Server 2008 R2 (64-bit)	Service Pack 1 or Service Pack 2	Standard, Enterprise, and Datacenter
SQL Server 2012	With or without Service Pack 1	Enterprise, Standard (64-bit)

### Additional information

- You must use a case-insensitive instance of SQL Server.
- When you install SQL Server, select the **Database Engine Services** and the **Management Tools - Complete** features.
- If the VMM management server and the computer on which SQL Server runs are not members of the same Active Directory domain, there must be a two-way trust between the two domains.

- The name of the computer on which SQL Server is installed cannot exceed 15 characters.
- For information about AlwaysOn support and additional information related to SQL Server support, see **SQL Server**.

## System Requirements: VMM Library Server

### Hardware requirements

The minimum and recommended hardware requirements for a VMM library server vary depending on a number of factors. These factors include, but are not limited to the quantity and size of the following files, which will be stored on the library server:

- Virtual machine templates
- Virtual hard disks
- Virtual floppy disks
- ISO images
- Scripts
- Hardware profiles
- Guest operating system profiles
- Stored virtual machines

Hardware component	Minimum	Recommended
Processor	Pentium 4, 2.8 GHz	Dual-Core 64-bit, 3.2 GHz or greater
RAM	2 GB	2 GB
Hard disk space	Varies based on the number and size of the stored files.	Varies based on the number and size of the stored files.

### Software requirements

Before you add a VMM library server, you must install the following software.

Software	Notes
A supported operating system for the VMM library server	For more information, see <a href="#">Supported operating systems</a> in this topic.
Windows Remote Management (WinRM)	<p>WinRM 1.1 is included in Windows Server 2008, and by default, the Windows Remote Management (WS-Management) service is set to start automatically.</p> <p>WinRM 2.0 is included in Windows Server 2008 R2, and by default, the Windows Remote Management (WS-Management) service is set to start automatically (delayed start).</p> <p>WinRM is included in Windows Server 2012, and by default, the Windows Remote Management (WS-Management) service is set to start automatically.</p>

### Supported operating systems

Operating system for System Center 2012 – Virtual Machine Manager	Edition	System architecture
Windows Server 2008 R2 Service Pack 1 or earlier  (full installation or Server Core installation)	Standard, Enterprise, and Datacenter	x64
Windows Server 2008 Service Pack 2  (full installation or Server Core installation)	Standard, Enterprise, and Datacenter	x86 and x64
Windows Server 2008 Service Pack 2	Standard, Enterprise, and	x86 and x64

Operating system for System Center 2012 – Virtual Machine Manager	Edition	System architecture
without Hyper-V  (full installation or Server Core installation)	Datacenter	

Operating system for VMM in System Center 2012 SP1	Edition	System architecture
Windows Server 2008 R2 Service Pack 1	Standard, Enterprise, and Datacenter	x64
Windows Server 2012  (full installation or Server Core installation)	Standard and Datacenter	X64

### Additional information

- For more information about library servers in VMM, see [Configuring the Library Overview](#).
- System Center 2012 – Virtual Machine Manager allows you to add highly available library shares on a failover cluster that is created in the following operating systems:
  - Windows Server 2008 R2, Datacenter Edition
  - Windows Server 2008 R2, Enterprise Edition
  - Windows Server 2008, Datacenter Edition
  - Windows Server 2008, Enterprise Edition

VMM in System Center 2012 SP1 allows you to add highly available library shares on a failover cluster that is created in Windows Server 2012, Standard and Datacenter editions.

- VMM does not provide a method for replicating physical files in the VMM library or metadata for objects that are stored in the VMM database. Physical files must be replicated outside of VMM, and metadata must be transferred by using scripts or other means.

- VMM does not support file servers that are configured with the case-insensitive option for Windows Services for UNIX, because the Network File System case control is set to Ignore. For more information about Network File System case control, see [Windows Services for UNIX 2.0 NFS Case Control](#).

## System Requirements: Virtual Machine Hosts

Virtual Machine Manager (VMM) supports the following software as virtual machine hosts:

- Microsoft Hyper-V
- VMware ESX
- Citrix XenServer

VMM does not support Microsoft Virtual Server 2005 R2 as a virtual machine host.

For more information, see the following topics:

- [System Requirements: Hyper-V Hosts](#)
- [System Requirements: VMware ESX Hosts](#)
- [System Requirements: Citrix XenServer Hosts](#)

## System Requirements: Hyper-V Hosts

To manage hosts, Virtual Machine Manager (VMM) supports the following versions of Hyper-V.

Operating system for System Center 2012 – Virtual Machine Manager (VMM)	Edition	Service pack	System architecture
Windows Server 2008 R2 (full installation or Server Core-MiniShell installation)	Standard, Enterprise, and Datacenter	Service Pack 1 or earlier	x64
Hyper-V Windows Server 2008 R2	N/A	N/A	x64
Windows Server 2008 (full installation or Server Core-MiniShell installation)	Enterprise and Datacenter	Service Pack 2	x64

Operating system for VMM in System Center 2012 SP1	Edition	Service pack	System architecture
Windows Server 2008 R2 (full installation or Server Core-MiniShell installation)	Standard, Enterprise, and Datacenter	Service Pack 1	x64
Hyper-V Windows Server 2008 R2	N/A	N/A	x64
Windows Server 2012 (full installation or Server Core installation)	Standard and Datacenter	N/A	X64
Hyper-V Windows Server 2012	N/A	N/A	X64

For information about which guest operating systems are supported by Hyper-V, see [About Virtual Machines and Guest Operating Systems](#).

For more information about how to manage Hyper-V hosts in VMM, see [Adding and Managing Hyper-V Hosts and Host Clusters in VMM](#).

### System Requirements: VMware ESX Hosts

To manage hosts, System Center 2012 – Virtual Machine Manager (VMM) supports the following VMware virtualization software.

Software	Notes
vCenter Server:  For System Center 2012 – Virtual Machine Manager:  <ul style="list-style-type: none"> <li>VMware vCenter Server 4.1</li> </ul>	For more information about the requirements for vCenter Server, refer to the VMware product documentation.

Software	Notes
<p>For VMM in System Center 2012 SP1:</p> <ul style="list-style-type: none"> <li>• VMware vCenter Server 4.1</li> <li>• VMware vCenter Server 5.0</li> <li>• VMware vCenter Server 5.1</li> </ul>	
<p>Virtual machine hosts and host clusters that run any of the following versions of VMware:</p> <p>For System Center 2012 – Virtual Machine Manager:</p> <ul style="list-style-type: none"> <li>• ESXi 4.1</li> <li>• ESX 4.1</li> <li>• ESXi 3.5</li> <li>• ESX 3.5</li> </ul> <p>For VMM in System Center 2012 SP1:</p> <ul style="list-style-type: none"> <li>• ESXi 5.1</li> <li>• ESXi 4.1</li> <li>• ESX 4.1</li> </ul>	<p>The host or host clusters must be managed by a vCenter Server, which is managed by VMM.</p>

For more information, see [Managing VMware ESX Hosts Overview](#).

### System Requirements: Citrix XenServer Hosts

The following software is required for a host that runs Citrix virtualization software.

Software	Notes
<ul style="list-style-type: none"> <li>• Citrix XenServer 6.0</li> <li>• Citrix XenServer – Microsoft System Center Integration Pack</li> </ul>	<p>For more information about the requirements for XenServer, refer to the Citrix product documentation.</p> <p>For more information about the Citrix</p>

Software	Notes
	XenServer – Microsoft System Center Integration Pack, see <a href="#">Citrix XenServer – Microsoft System Center Integration Pack</a> .

For more information, see [Managing Citrix XenServer Overview](#).



#### Note

All information and content at <http://www.citrix.com> is provided by the owner or the users of the website. Microsoft makes no warranties, express, implied, or statutory, as to the information at this website.


### System Requirements: Hyper-V Host Deployment to a Bare-Metal Computer

Virtual Machine Manager (VMM) provides the capability to discover physical computers on the network and then automatically install the Windows operating system on these computers and convert them into managed Hyper-V hosts. The targeted physical computer can be a computer that does not have an operating system installed, often referred to as a “bare-metal” computer, or it can be a computer on which you want to overwrite an existing operating system.

For more information, see [Adding Physical Computers as Hyper-V Hosts in VMM Overview](#).

#### Software requirements

System role	System requirement
Physical computer to be discovered	<p>Must have a baseboard management controller (BMC) with a supported out-of-band management protocol. VMM supports the following out-of-band management protocols:</p> <ul style="list-style-type: none"> <li>• Intelligent Platform Management Interface (IPMI) versions 1.5 or 2.0</li> <li>• Data Center Management Interface (DCMI) version 1.0</li> <li>• System Management Architecture for Server Hardware (SMASH) version 1.0 over WS-Management (WS-Man)</li> </ul>

System role	System requirement
	 <b>Note</b> If you use SMASH, make sure that you use the latest version of firmware for the baseboard management controller (BMC) model.
PXE Server that is used to initiate the operating system installation on the physical computer.	Requirements for System Center 2012 – Virtual Machine Manager: <ul style="list-style-type: none"> <li>• A computer that runs Windows Server 2008 R2 with the Windows Deployment Services role installed.</li> </ul> Requirements for VMM in System Center 2012 SP1: <ul style="list-style-type: none"> <li>• A computer that runs Windows Server 2008 R2 with the Windows Deployment Services role installed.</li> <li>• A computer that runs Windows Server 2012 with the Windows Deployment Services role installed.</li> </ul> Other types of PXE servers are not supported.
Image operating system	For System Center 2012 – Virtual Machine Manager: <ul style="list-style-type: none"> <li>• A Windows Server 2008 R2 operating system image.</li> </ul> For VMM in System Center 2012 SP1: <ul style="list-style-type: none"> <li>• A Windows Server 2008 R2 operating system image.</li> <li>• A Windows Server 2012 operating system image.</li> </ul> The operating system image must support the option to boot from virtual hard disk.

System role	System requirement
	You can create the virtual hard disk by running the System Preparation Tool (Sysprep.exe) on a virtual machine that runs the operating system that will be on the image.

## System Requirements: Update Management


Virtual Machine Manager (VMM) provides the capability to use a Windows Server Update Services (WSUS) server to manage updates for the following computers in your VMM environment:

- Virtual machine hosts
- Library servers
- VMM management server
- PXE servers
- The WSUS server

You can configure the update baselines, scan computers for compliance, and perform update remediation.

### Software requirements

Software	Notes
<p>For System Center 2012 – Virtual Machine Manager:</p> <ul style="list-style-type: none"> <li>• A 64-bit edition of Windows Server Update Services (WSUS) 3.0 Service Pack 2 (SP2)</li> </ul> <p>For VMM in System Center 2012 SP1:</p> <ul style="list-style-type: none"> <li>• A 64-bit edition of Windows Server Update Services (WSUS) 3.0 Service Pack 2 (SP2)</li> <li>• A 64-bit edition of Windows Server Update Services (WSUS) 4.0</li> </ul>	<ul style="list-style-type: none"> <li>• For information about WSUS system requirements and to download WSUS 3.0 SP2, see <a href="#">Windows Server Update Services 3.0 SP2</a> on the Microsoft Download Center.</li> <li>• WSUS 4.0 is a server role that is integrated with Windows Server 2012.</li> <li>• VMM can use either a WSUS root server or a downstream WSUS server. VMM does not support using a WSUS replica server.</li> <li>• The WSUS server can either be dedicated to VMM or can be a WSUS server that is already in use in your environment.</li> </ul>

Software	Notes
	<ul style="list-style-type: none"> <li>• VMM supports using a WSUS server that is part of a Configuration Manager 2007 R2 or System Center 2012 Configuration Manager environment, but additional configuration steps are required. For more information, see <a href="#">How to Integrate Fabric Updates with Configuration Manager</a>.</li> <li>• If VMM will process a very large volume of updates, consider installing the WSUS server on a separate computer from the VMM management server.</li> <li>• If you do not install WSUS server on the same computer as the VMM management server, you must install a WSUS Administrator Console on the VMM management server. If you use a highly available VMM management server, you must install a WSUS Administrator Console on each node.</li> </ul> <p> <b>Important</b>  If you use WSUS 3.0 SP2 to enable updates for Windows Server 2012 hosts, then you must apply <a href="#">KB2734608</a>. Make sure that you carefully read the Known Issues for this update as they apply to VMM.</p>

### Additional information

- For more information about update management in VMM, see [Managing Fabric Updates in VMM](#).
- VMM can also work with System Center Updates Publisher, but only full content updates are supported. Metadata-only updates cannot be added to an update baseline.

### System Requirements: Monitoring and Reporting

Virtual Machine Manager (VMM) provides the capability to monitor the health and performance of virtual machines and their hosts. To do so, VMM integrates with Operations Manager and enables Performance and Resource Optimization (PRO).

VMM supports the following versions of Operations Manager:

- Operations Manager 2007 R2
- System Center 2012 – Operations Manager



**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.

VMM also provides the capability to use the reporting functionality of Operations Manager. To use the forecasting reports, SQL Server Analysis Services must be installed on the Operations Manager Reporting server. The version of Analysis Services must be at least SQL Server 2008 with Service Pack 2 (SP2).

For more information, see [Configuring Operations Manager Integration with VMM](#).

## 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](#)
- [Installing System Center 2012 - Virtual Machine Manager](#)
- [Installing a Highly Available VMM Management Server](#)
- **How to Configure Windows SQL Server with AlwaysOn**

Before you start the deployment of VMM in System Center 2012 Service Pack 1 (SP1), ensure that you read the release notes at [Release Notes for System Center 2012 Service Pack 1 – Virtual Machine Manager](#), and review system requirements at [System Requirements for System Center 2012 - Virtual Machine Manager](#).

For an overview of VMM, see [Overview of System Center 2012 - Virtual Machine Manager](#).

## 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 VMM management server, you will need to 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.



### Important

By default, VMM encrypts some data in the VMM database (for example Run As account credentials and passwords in guest operating system profiles) by using the Windows Data Protection API (DPAPI). The encryption of this data is tied to the specific computer on which

VMM is installed and the service account used by VMM. Therefore, if you need to move your VMM installation to another computer, the encrypted data will not be retained.

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

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

The following are some considerations about using distributed key management in VMM:

- 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 is only possible if the encryption keys are stored in a central location like AD DS.

- You must create a container in AD DS before installing VMM. You can create the container by using ADSI Edit.
- 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 to be used by the System Center Virtual Machine Manager service, 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 named **VMMDKM**, you would specify the container location as **CN=VMMDKM,DC=corp,DC=contoso,DC=com**.

- After the Active Directory administrator has created the container, the account with which you are installing VMM must be given **Full Control** permissions to the container in AD DS. Also, the permissions must apply to **This object and all descendant objects** of the container.
- 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**.

## 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 to System Center 2012 - Virtual Machine Manager](#).



**Note**

In 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
<a href="#">How to Install a VMM Management Server</a>	Describes how to install a VMM management server.

## How to Install a VMM Management Server

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

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. Unlike VMM 2008 R2, System Center 2012 – Virtual Machine Manager will not automatically install an Express edition of SQL Server.

In System Center 2012 Service Pack 1 (SP1) you can take advantage of the AlwaysOn feature in Microsoft SQL Server 2012 to ensure high availability of the VMM database. To configure SQL Server with the AlwaysOn feature, complete both procedures below.

For more information about the AlwaysOn feature, and AlwaysOn availability groups see the followings:

- [Overview of AlwaysOn Availability Groups \(SQL Server\)](#)
- [AlwaysOn Availability Groups \(SQL Server\)](#)

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 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 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**.

If you have not installed Microsoft .NET Framework, VMM will prompt you to install 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, 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**.
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. 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 installing the 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. 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 **Database configuration** page appears.

9. On the **Database configuration** page, perform the following steps:
  - If you are installing System Center 2012 SP1, determine whether you want to configure your SQL Server-based computer with the AlwaysOn option.
  - If you are installing System Center 2012 SP1 and configuring your SQL Server-based computer with the AlwaysOn option, complete the following steps:
    - i. On the **Database configuration** page, in the **Server name** box, type the name of the availability group listener.
    - ii. Leave **Instance name** empty.
    - iii. Create a new database.
  - If you are not configuring your SQL Server-based computer with the AlwaysOn option, complete the following steps:
    - i. 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**.
    - ii. Ensure that the SQL 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.

- iii. Select or type the name of the instance of SQL Server that you want to use.
- iv. 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 will be used by the Virtual Machine Manager service. Realize that it is not supported to change the identity of the Virtual Machine Manager 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. For more information about key management, see [Configuring Distributed Key Management in VMM](#).

After you have selected an account and, if necessary, entered Active Directory information, click **Next**.

12. On the **Port configuration** page, use the default port numbers or 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 installation of a VMM management server cannot be changed without uninstalling and reinstalling the VMM management server.

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 created by VMM is named **MSSCVMMLibrary** and the folder is located at **%SYSTEMDRIVE%\ProgramData\Virtual Machine Manager Library Files**. **ProgramData** is a hidden folder.

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

After you have specified 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 installation 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 for VMM in System Center 2012 SP1, you can click the **Virtual Machine Manager Console** icon on the desktop.



#### **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.

### **► For System Center 2012 SP1 only: To configure Microsoft SQL Server with AlwaysOn**

1. Complete the VMM Setup wizard to install the VMM management server, as described in the previous procedure.
2. Add the VMM database to the availability group.
3. On the secondary SQL Server node, create a new login with the following characteristics:
  - The login name is identical to the VMM service account name.
  - The login has the user mapping to the VMM database.
  - The login is configured with the database owner credentials.
4. Initiate a failover to the secondary SQL Server node, and verify that you can restart the VMM service (scvmmsservice).
5. Repeat the last two steps for every secondary SQL Server node in the cluster.
6. If this is a high availability VMM setup, continue to install other high availability VMM nodes.

### **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: <a href="#">How to Install the VMM Console</a>	Describes how to install the VMM console.
Step 2: <a href="#">How to Connect to a VMM Management Server by Using the VMM Console</a>	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.

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 the VMM console

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**.
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** to continue.
6. 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.

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 computer on which you are installing the VMM console 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 **Port configuration** page will appear.

8. On the **Port configuration** page, type the port 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.

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 installation progress is displayed.

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 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 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, 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

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

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: <a href="#">How to Install the VMM Self-Service Portal</a>	Describes how to install the VMM Self-Service Portal.
Step 2: <a href="#">How to Open the VMM Self-Service Portal</a>	Describes how to open the VMM Self-Service Portal.

## How to Install 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.

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

In 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 in System Center 2012 – Virtual Machine Manager (VMM). 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

In 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**.

#### ▶ 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**.

## 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.

To upgrade from an evaluation version of VMM to a licensed 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 have the option of installing Virtual Machine Manager (VMM) using a Command Prompt. Installing VMM features involves saving installation settings in an .ini file and using **setup.exe** with that file.



### Important

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

## The installation files

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

- **VMServer.ini**

Settings for VMM management server

- **VMClient.ini**

Settings for VMM console

- **VMEUP.ini**

Settings for VMM Self-Service Portal



**Note**

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

- **VMServerUninstall.ini**

Uninstall settings for VMM management server

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

### Installing a VMM management server using the Command Prompt

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





**Note**


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



### Configuring options for 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
UserName	An optional display name for the user	Administrator

Option	Values	Default
	installing the features.   <b>Note</b> This is not the user account for the installation.	
CompanyName	An optional display name for organization installing the features.	Microsoft Corporation
ProgramFiles	The location for VMM files.	C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager
CreateNewSqlDatabase	0 : Use an existing SQL Server database.  1 : Create a new SQL Server database.	1
SqlInstanceName	Name for the new or existing instance of SQL Server.	MICROSOFT\$VMM\$
SqlDatabaseName	Name of the new or existing SQL Server database.	VirtualManagerDB
RemoteDatabaseImpersonation	0 : Use a local SQL Server installation.  1 : Use a remote SQL Server installation.   <b>Important</b> When you run <b>setup.exe</b> , provide value for the <i>SqlDBAdminName</i> , <i>SqlDBAdminPassword</i> , and <i>SqlDBAdminDomain</i> unless the user running Setup is an administrator for the SQL	0

Option	Values	Default
	Server.	
SqlMachineName	Name of the server hosting the SQL server. Do not specify 'localhost', specify the actual name of the computer.	<sqlmachinename>
(various ports)	For information about ports, see <a href="#">Ports and Protocols for VMM</a> .	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 file share to be used or created.	MSSCVMMLibrary
LibrarySharePath	Location of file share or for new file share to be created.	C:\ProgramData\Virtual Machine Manager Library Files
LibraryShareDescription	Description of 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	0

Option	Values	Default
	<a href="#">Microsoft Customer Experience Improvement Program</a>  For CEIP privacy information, see <a href="#">Privacy Statement for the Microsoft Customer Experience Improvement Program</a>	
MUOptIn	0 : Do not opt into Microsoft Update.  1 : Opt into Microsoft Update.  For more information about Microsoft Update, see <a href="#">Frequently Asked Questions</a> .  For Microsoft Update privacy information, see <a href="#">Update Services Privacy Statement</a> .	0
VmmServiceLocalAccount	0 : Use a domain account for the VMM service (scvmm-service).  1 : Use the Local System account for the VMM service.   <b>Note</b> To use a domain account, when you run <b>setup.exe</b> , provide values for the <i>VMMServiceDomain</i> , <i>VMMServiceUserName</i> , and <i>VMMServiceUserPassword</i> .  For more information about service accounts, see <a href="#">Specifying a Service Account for VMM</a> .	0

Option	Values	Default
TopContainerName	<p>The container for Distributed Key Management (DKM), for instance "CN=DKM,DC=contoso,DC=com".</p> <p>For more information about DKM, see <a href="#">Configuring Distributed Key Management in VMM</a>.</p>	VMMServer
HighlyAvailable	<p>0 : Do not install as highly available.</p> <p>1 : Install as highly available.</p> <p>For information about highly available installations, see <a href="#">Installing a Highly Available VMM Management Server</a>.</p>	0
VmmServerName	<p>Clustered service name for a highly available VMM management server.</p> <p> <b>Important</b> 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. For more information, see <a href="#">How to Install a Highly Available VMM Management Server</a>.</p>	<VMMServerName>
VMMStaticIPAddress	<p>Provide IP address for the clustered service name for a highly available VMM management server, if not using DHCP.</p> <p> <b>Note</b> Both IPv4 and IPv6 are</p>	<comma-separated-ip-for-HAVMM>

Option	Values	Default
	supported.	
Upgrade	0 : Do not upgrade from a previous version of VMM to System Center 2012 – Virtual Machine Manager.  1 : Upgrade from previous version.	1

### Installing a VMM management server using the Command Prompt

After you edit VMServer.ini, open an elevated Command Prompt, and then run **setup.exe** using the following parameters.

- */server*  
Specifies installation of the VMM management server.
- */i* or */x*  
Whether to install (*/i*) or uninstall (*/x*) the server.
- */f <filename>*  
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 using its own default values.

- */VmmServiceDomain <domainName>*  
Specifies the domain name for the account running the VMM service (scvmmsservice). Use this parameter only if you set *VmmServiceLocalAccount* to 0 in **VMServer.ini**.
- */VmmServiceUserName <userName>*  
Specifies the user name for the account running the VMM service (scvmmsservice). Use this parameter only if you set *VmmServiceLocalAccount* to 0 in **VMServer.ini**.
- */VmmServiceUserPassword <password>*

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

- */SqlDBAdminDomain <domainName>*  
  
Domain name the SQL Server database administrator account. Use this parameter if the current user does not have administrative privileges on the SQL server.
- */SqlDBAdminName <userName>*  
  
User name for the SQL Database administrator account. Use this parameter if the current user does not have administrative privileges to SQL Server.
- */SqlDBAdminPassword <password>*  
  
Password for the SQL Server database administrator account. Use this parameter if the current user does not have administrative privileges to SQL Server.

For instance, to use a **VMServer.ini** file that is stored in **C:\Temp** with an SQL Server administrator account **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 using the 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 : A local SQL Server installation  1 : A remote SQL Server installation.  When you run <b>setup.exe</b> , provide a value for the <i>SqlDBAdminName</i> , <i>SqlDBAdminPassword</i> , and <i>SqlDBAdminDomain</i> unless the user running setup.exe is an administrator	0

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

### Uninstalling a VMM management server using the Command Prompt

To uninstall a VMM management server with a **VMServerUninstall.ini** file that is stored in **C:\Temp**, with an 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 using the Command Prompt

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

To uninstall the 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 with the VMM management server.

Instead, first uninstall the VMM management server.

### Configuring options for a VMM console

Option	Values	Default
ProgramFiles	The location for VMM files.	C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager
IndigoTcpPort	The port used for communication between VMM management server and VMM console.	8100
MUOptIn	0 : Do not opt into Microsoft Update.  1 : Opt into Microsoft Update.  For more information about Microsoft Update, see <a href="#">Frequently Asked Questions</a> .  For Microsoft Update privacy information, see <a href="#">Update</a>	0

Option	Values	Default
	<a href="#">Services Privacy Statement</a> .	
VmmServerForOpsMgrConfig	This setting is not used. For more information, see <b>Configuring Operations Manager Integration with VMM</b> .	<VMMServerName>

## Installing a VMM console using the Command Prompt

After you edit **VMClient.ini**, use an elevated Command Prompt to run **setup.exe** using the following parameters.

- */client*  
Specifies installation of the VMM console.
- */i* or */x*  
Whether to install (*/i*) or uninstall (*/x*) the console.
- */f <filename>*  
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 using its own default values.

- */opsmgr*  
Whether to configure a pre-installed instance of Operations Manager 2007.



### Caution

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

For instance, 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 using the Command Prompt



### Note

In System Center 2012 Service Pack 1 (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	Specify the location in which to store program files.	C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager
VmmServerName	The name of the VMM management server that this VMM Self-Service Portal connects to.	<machineName>
IndigoTcpPort	The port used for communication between VMM management server and VMM Self-Service Portal.	8100
SelfServicePortalTcpPort	The port used for users to connect to the VMM Self-Service Portal.	80
SelfServicePortalHeader	If the same port is being used by other web sites on this server, specify a header for VMM Self-Service Portal.  For more information about headers, see <a href="#">How to Install the</a>	<headerName>

Option	Values	Default
	<a href="#">VMM Self-Service Portal.</a>	
MUOptIn	<p>0 : Do not opt into Microsoft Update.</p> <p>1 : Opt into Microsoft Update.</p> <p>For more information about Microsoft Update, see <a href="#">Frequently Asked Questions.</a></p> <p>For Microsoft Update privacy information, see <a href="#">Update Services Privacy Statement.</a></p>	0

### Installing or uninstalling the VMM Self-Service Portal using the Command Prompt

After you edit **VMEUP.ini**, use an elevated Command Prompt to run **setup.exe** using the following parameters.

- */eup*  
Specifies installation of the VMM Self-Service Portal.
- */i* or */x*  
Whether to install (/i) or uninstall (/x) the VMM Self-Service Portal.
- */f <filename>*  
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 using its own default values.

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

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

To uninstall a 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

In 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**.

If you have not installed Microsoft .NET Framework 3.5 SP1, VMM will prompt you to install now.

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

In 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**.
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**

In 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**.
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 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 for System Center 2012 - Virtual Machine Manager](#).

Software	Supported version	Additional information
Virtual Machine Manager	VMM 2008 R2 SP1	<ul style="list-style-type: none"><li>• The following are not supported: Upgrading from</li></ul>

Software	Supported version	Additional information
		<p>System Center 2012 – Virtual Machine Manager Release Candidate, System Center 2012 – Virtual Machine Manager Beta, VMM 2008 R2, VMM 2008, or VMM 2007.</p> <ul style="list-style-type: none"> <li>For information about upgrading to VMM 2008 R2 SP1, see <a href="#">Upgrading to VMM 2008 R2 Service Pack 1 from VMM 2008 R2</a>.</li> </ul>
Microsoft Windows Server	Windows Server 2008 R2	<ul style="list-style-type: none"> <li>The VMM management server is only supported on a computer that is running Windows Server 2008 R2.</li> <li>For information about specific editions and service packs of Windows Server 2008 R2 that are supported, see <a href="#">System Requirements: VMM Management Server</a>.</li> <li>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.</li> <li>For information about upgrading to Windows Server 2008 R2, see <a href="#">Guide for Upgrading to Windows Server 2008 R2</a>.</li> </ul>
Microsoft SQL Server	SQL Server 2008 R2 or SQL Server 2008	<ul style="list-style-type: none"> <li>For information about specific editions and service packs of SQL Server that are supported, see <a href="#">System Requirements: VMM Database</a>.</li> </ul>

Software	Supported version	Additional information
		<ul style="list-style-type: none"> <li>• System Center 2012 – Virtual Machine Manager does not support Express editions of SQL Server for the VMM database.</li> <li>• For information about moving a VMM database to a supported version of SQL Server, see <a href="#">How to Move a VMM Database to Another Computer</a>.</li> </ul>
SQL Server 2008 R2 Command Line Utilities	Microsoft SQL Server 2008 R2 Feature Pack	<ul style="list-style-type: none"> <li>• The SQL Server 2008 R2 Command Line Utilities are not a mandatory requirement for upgrade, but they are highly recommended.</li> <li>• 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 to perform certain management tasks.</li> <li>• To download the SQL Server 2008 R2 Command Line Utilities, see <a href="#">Microsoft SQL Server 2008 R2 Feature Pack</a>.</li> </ul>
Windows Automated Installation Kit (AIK)	Windows Automated Installation Kit (AIK) for Windows 7	<ul style="list-style-type: none"> <li>• Previous versions of Windows AIK must be uninstalled before you can install Windows AIK for Windows 7.</li> <li>• To download Windows AIK for Windows 7, see <a href="#">The Windows Automated Installation Kit (AIK) for Windows 7</a>.</li> </ul>

Software	Supported version	Additional information
Microsoft .NET Framework	.NET 3.5.1	<ul style="list-style-type: none"> <li>• Microsoft .NET 3.5.1 is included in all versions of Windows Server 2008 R2.</li> <li>• System Center 2012 – Virtual Machine Manager automatically enables .NET 3.5.1 if it is not already enabled.</li> </ul>
Windows Remote Management (WinRM)	WinRM 2.0	<ul style="list-style-type: none"> <li>• 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).</li> <li>• 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.</li> </ul>

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	<ul style="list-style-type: none"> <li>• Virtual machine hosts running Microsoft Virtual Server 2005 R2 are no longer supported in VMM.</li> <li>• If you upgrade a VMM environment that has Virtual Server hosts, the hosts are</li> </ul>


Item	Planning consideration
	<p>removed from the VMM database.</p> <ul style="list-style-type: none"> <li>• If you do not want these hosts to be removed automatically, you must remove the hosts manually before you upgrade.</li> </ul>
VMware ESX and certain versions of VMware vCenter Server	<ul style="list-style-type: none"> <li>• Virtual machine hosts running certain versions of VMware ESX and certain versions of VMware vCenter Server are no longer supported.</li> <li>• For more information about which versions of VMware are supported, see <a href="#">System Requirements: VMware ESX Hosts</a>.</li> <li>• If you upgrade with these hosts and their managed objects, they are removed from the VMM database.</li> <li>• If you do not want these hosts to be removed automatically, you must remove the hosts manually before you upgrade.</li> </ul>
Performance and Resource Optimization (PRO)	<ul style="list-style-type: none"> <li>• Performance and Resource Optimization (PRO) configurations are not maintained during an upgrade to System Center 2012 – Virtual Machine Manager.</li> <li>• Any existing connection to Operations Manager is removed during the upgrade process.</li> <li>• If you do not want the Operations Manager connection to be automatically removed, you can remove the connection manually before the upgrade.</li> <li>• After the upgrade process completes, you can reconfigure your connection to Operations Manager.</li> <li>• For information about using Operations Manager with System Center 2012 – Virtual Machine Manager, see <a href="#">Configuring Operations Manager Integration with</a></li> </ul>

Item	Planning consideration
	<a href="#">VMM</a> .
Library server	<ul style="list-style-type: none"> <li>• System Center 2012 – Virtual Machine Manager does not support a library server on a computer that is running Windows Server 2003.</li> <li>• 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.</li> <li>• If you want to use the library server in System Center 2012 – Virtual Machine Manager, click <b>Cancel</b> to exit the upgrade and then move the library server to a computer that is running a supported operating system.</li> <li>• For information about VMM library server requirements, see <a href="#">System Requirements: VMM Library Server</a>.</li> </ul>
Service account	For more information, see <a href="#">Choosing Service Account and Distributed Key Management Settings During an Upgrade</a> .
Distributed key management	For more information, see <a href="#">Choosing Service Account and Distributed Key Management Settings During an Upgrade</a> .

### 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	<ul style="list-style-type: none"> <li>• You must create and configure a failover cluster prior to upgrading.</li> <li>• For information about installing and configuring a failover cluster, see <a href="#">Overview of Failover Clusters</a>.</li> </ul>
VMM database	<ul style="list-style-type: none"> <li>• The VMM database cannot be installed on the same computer as the highly available VMM management server.</li> <li>• 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.</li> <li>• 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.</li> <li>• For information about moving a VMM database to another computer, see <a href="#">How to Move a VMM Database to Another Computer</a>.</li> </ul>
Library server	<ul style="list-style-type: none"> <li>• We recommend that the library server is installed on a highly available file server.</li> <li>• 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.</li> <li>• For more information about relocating your VMM library after the upgrade, see <a href="#">Relocating the VMM Library</a>.</li> </ul>
VMM Self-Service Portal	<ul style="list-style-type: none"> <li>• The VMM Self-Service Portal should not be installed on the same computer as the</li> </ul>

Item	Planning consideration
 <b>Note</b> In System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed.	<p>highly available VMM management server.</p> <ul style="list-style-type: none"> <li>• 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 R2 SP1 before you upgrade to System Center 2012 – Virtual Machine Manager.</li> <li>• We recommend that you install the VMM Self-Service Portal on a highly available web server.</li> </ul>
Service account	<ul style="list-style-type: none"> <li>• You must configure the System Center Virtual Machine Manager service to use a domain account for a highly available VMM management server.</li> <li>• For more information, see <a href="#">Choosing Service Account and Distributed Key Management Settings During an Upgrade</a>.</li> </ul>
Distributed key management	<ul style="list-style-type: none"> <li>• You must use distributed key management to store encryption keys in Active Directory Domain Services (AD DS) for a highly available VMM management server.</li> <li>• For more information, see <a href="#">Choosing Service Account and Distributed Key Management Settings During an Upgrade</a>.</li> </ul>

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	<ul style="list-style-type: none"> <li>Virtual Machine Manager</li> <li>Virtual Machine Manager Agent</li> </ul>	<ul style="list-style-type: none"> <li>vmmservice</li> <li>vmmagent</li> </ul>
System Center 2012 – Virtual Machine Manager	<ul style="list-style-type: none"> <li>System Center Virtual Machine Manager</li> <li>System Center Virtual Machine Manager Agent</li> </ul>	<ul style="list-style-type: none"> <li>scvmmservice</li> <li>scvmmagent</li> </ul>

### 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 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	<i>(This configuration is not supported.)</i>	<i>(This configuration is not supported.)</i>
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	Domain account	Domain account	Encrypted data is not preserved	Encrypted data is not preserved

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
service account				



#### 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](#).

### ► 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](#).

## 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

In 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 for System Center 2012 - Virtual Machine Manager](#).

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 [Planning Considerations for highly available VMM](#) in the [Planning Considerations for Upgrading to 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 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 for System Center 2012 - Virtual Machine Manager](#).

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 Overview](#).

### 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 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 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

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**.
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**.

## 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.

## 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	<ul style="list-style-type: none"><li>• If you upgrade with these hosts and their managed objects, they are removed from the VMM database.</li><li>• If you do not want these hosts to be removed automatically, remove the hosts</li></ul>

Item	Planning considerations
	<p>manually before upgrading.</p> <ul style="list-style-type: none"> <li>For more information about which versions of VMware are supported, see <a href="#">System Requirements: VMware ESX Hosts</a>.</li> </ul>
Performance and Resource Optimization (PRO)	<ul style="list-style-type: none"> <li>PRO configurations are not maintained during this upgrade.</li> <li>If you have an existing connection to Operations Manager, the connection is removed during the upgrade process.</li> <li>If you do not want the connection to be removed automatically, remove the connection manually before upgrading.</li> <li>After the upgrade process completes, you can reconfigure your connection to Operations Manager.</li> <li>For information about using Operations Manager with VMM, see <b>Configuring Operations Manager Integration with VMM</b>.</li> </ul>
Library server	<ul style="list-style-type: none"> <li>If you want to use the library server in VMM for System Center 2012 SP1, click <b>Cancel</b> to exit the upgrade, and then move the library server to a computer that is running a supported operating system.</li> <li>For information about VMM library server requirements, see <a href="#">System Requirements: VMM Library Server</a>.</li> </ul>
Service account	<p>For more information, see <a href="#">Choosing Service Account and Distributed Key Management Settings During an Upgrade</a>.</p>
Distributed key management	<p>For more information, see <a href="#">Choosing Service Account and Distributed Key Management</a></p>

Item	Planning considerations
	<a href="#">Settings During an Upgrade.</a>

## 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	<ul style="list-style-type: none"> <li>You must create and configure a failover cluster before upgrading.</li> </ul>
VMM database	<ul style="list-style-type: none"> <li>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.</li> <li>For information about moving a VMM database to another computer, see <b>How to Move a VMM Database to Another Computer</b>.</li> </ul>
Library server	<ul style="list-style-type: none"> <li>We recommend that the library server be installed on a highly available file server.</li> <li>After you upgrade to a highly available VMM management server, we recommended that you relocate your VMM library to a highly available file server.</li> <li>For more information about relocating your VMM library after the upgrade, see <b>Relocating the VMM Library</b>.</li> </ul>
Service account	<ul style="list-style-type: none"> <li>You must configure the System Center Virtual Machine Manager service to use a domain account for a highly available VMM</li> </ul>

Item	Planning considerations
	<p>management server.</p> <ul style="list-style-type: none"> <li>For more information, see <a href="#">Choosing Service Account and Distributed Key Management Settings During an Upgrade</a>.</li> </ul>
Distributed key management	<ul style="list-style-type: none"> <li>You must use distributed key management to store encryption keys in Active Directory Domain Services (AD DS) for a highly available VMM management server.</li> <li>For more information, see <a href="#">Choosing Service Account and Distributed Key Management Settings During an Upgrade</a>.</li> </ul>

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
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	Domain account	Domain account	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
account in System Center 2012				
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.

#### **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 **How to Backup and Restore the VMM Database**. 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**.
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 “[Planning Considerations for highly available VMM](#)” in the [Planning Considerations for Upgrading to 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**.
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 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.

# Administering System Center 2012 - Virtual Machine Manager

---

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

- [Configuring Fabric Resources in VMM](#)
- [Creating and Deploying Virtual Machines and Services in VMM](#)
- [Monitoring and Reporting in VMM](#)
- [Performing Maintenance Tasks in VMM](#)

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 VMM in System Center 2012 and System Center 2012 Service Pack 1 (SP1).

- [Preparing the Fabric in VMM](#)
- [Adding and Managing Hyper-V Hosts and Host Clusters 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 System Center 2012 – Virtual Machine Manager, see [Overview of System Center 2012 - Virtual Machine Manager](#).

## Preparing the Fabric in VMM

This section explains how to prepare the fabric in VMM. The fabric consists of the infrastructure that you need to manage and deploy hosts, and to create and deploy virtual machines and services to a private cloud. This section covers the following areas:

- Configuring host groups

- Configuring the library
- Configuring networking
- Configuring storage

**Note**

Other fabric components, 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 Host Clusters in VMM](#), [Managing VMware ESX and Citrix XenServer in VMM](#), and the [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, contoso.com.

**In This Section****[Preparing the Fabric Scenario in VMM Overview](#)**

Provides an overview of the example fabric resources that are used in the fabric configuration scenarios.

**[Creating Host Groups in VMM Overview](#)**

Provides an overview of host groups in VMM.

**[Configuring the VMM Library Overview](#)**

Provides an overview of the library in VMM, including a description of the new library features.

**[Configuring Networking in VMM Overview](#)**

Provides an overview of the new networking features in VMM.

**[Configuring Storage in VMM Overview](#)**

Provides an overview of the new storage discovery, storage classification, and storage allocation features in VMM.


Preparing the Fabric Scenario in VMM Overview

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 the 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 examples that are used in this section.

Resource	Name	
Host groups	Seattle	
	Tier0_SEA	
	Tier1_SEA	
	Tier2_SEA	
	New York	
	Tier0_NY	
	Tier1_NY	
	Tier2_NY	
Library shares	VMMServer01\SEALibrary (in Seattle)	
	NYLibrary01\NYLibrary (in New York)	
Networking	Logical networks:	
	Name	Description

Resource	Name						
	FRONTEND	Public network. Use for Internet-facing Web servers.					
	BACKEND	<p>Corporate network. Use for internal servers such as application and database servers.</p> <p> <b>Note</b> 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.</p>					
	LAB	Lab network. Use for test and development labs.					
	<p>Network sites for the BACKEND logical network:</p> <table border="1"> <thead> <tr> <th>Name</th><th>Subnet</th><th>VLAN</th></tr> </thead> <tbody> <tr> <td>BACKEND - Seattle</td><td>10.0.0.0/24</td><td>7</td></tr> </tbody> </table>		Name	Subnet	VLAN	BACKEND - Seattle	10.0.0.0/24
Name	Subnet	VLAN					
BACKEND - Seattle	10.0.0.0/24	7					

Resource	Name		
	BACKEND – New York	172.16.0.0/24	12
	IP address pool:		
	Name	BACKEND - Seattle IP pool	
	Description	IP addresses for internal application and database servers - Seattle	
	Begin IP address	10.0.0.10	
	End IP address	10.0.0.99	
	Reserved range for virtual IP addresses associated with load balancers:	10.0.0.25 – 10.0.0.35	
	Default gateway	10.0.0.1	
	DNS server	10.0.0.2	
	WINS server	10.0.0.3	
	MAC address pool:		
	Name	MAC pool - Seattle	
	Starting address	00:1D:D8:B7:1C:00	

Resource	Name	
	Ending address	00:1D:D8:B7:1F:E8
	Load balancer:	
	Name	LoadBalancer01.contoso.com
	VIP template	Web tier (HTTPS traffic)
Storage	Storage classifications:	
	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

[Creating Host Groups in VMM Overview](#)

[Configuring the VMM Library Overview](#)

## Creating Host Groups in VMM Overview

The procedures in this section describe how to create a host group structure in System Center 2012 – Virtual Machine Manager (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
<a href="#">How to Create a Host Group Structure in VMM</a>	Describes how to create a host group hierarchy, and how to move a host group to another location.
<a href="#">How to Configure Host Group Properties in VMM</a>	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 System Center 2012 – Virtual Machine Manager (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 Overview](#)

[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 System Center 2012 – Virtual Machine Manager (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
<b>General</b>	Configure the host group name, the location in the host group hierarchy, the description, and whether to allow unencrypted file transfers.
<b>Placement Rules</b>	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.
<b>Host Reserves</b>	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.

	<p>You can configure reserve values for the following resources:</p> <ul style="list-style-type: none"> <li>• CPU</li> <li>• Memory</li> <li>• Disk I/O</li> <li>• Disk space</li> <li>• Network I/O</li> </ul>
<b>Dynamic Optimization</b>	<p>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 <a href="#">Configuring Dynamic Optimization and Power Optimization in VMM</a>.</p>
<b>Network</b>	<p>View inheritance settings, and configure whether to inherit network logical resources from parent host groups. The network logical resources include the following:</p> <ul style="list-style-type: none"> <li>• IP address pools</li> <li>• Load balancers</li> <li>• Logical networks</li> <li>• MAC address pools</li> </ul>
<b>Storage</b>	<p>View and allocate storage to a host group. For more information, see the following topics:</p> <ul style="list-style-type: none"> <li>• <a href="#">How to Allocate Storage Logical Units to a Host Group in VMM</a></li> <li>• <a href="#">How to Allocate Storage Pools to a</a></li> </ul>

	<a href="#">Host Group in VMM</a>
<b>Custom Properties</b>	<p>Manage custom properties for the following object types:</p> <ul style="list-style-type: none"> <li>• Virtual machine</li> <li>• Virtual machine template</li> <li>• Host</li> <li>• Host cluster</li> <li>• Host group</li> <li>• Service template</li> <li>• Service instance</li> <li>• Computer tier</li> <li>• Cloud</li> </ul>

**See Also**

[Creating Host Groups in VMM Overview](#)

[How to Create a Host Group Structure in VMM](#)

## Configuring the VMM Library Overview

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	.zip
 <b>Note</b> These appear in the library as the “Web Application Package” type.	
SQL Server data-tier applications (DACs)	.dacpac
Server App-V packages	.osd
 <b>Note</b> These appear in the library as the “Virtual Application Package” type.	
Driver files	.inf   <b>Important</b> 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

Library Resource	File Name Extension
	you delete an .inf driver package from the library, VMM deletes the entire folder where the driver .inf file resides. For more information, see <a href="#">How to Add Driver Files to the VMM Library</a> .
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, 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 [System Requirements: VMM Library Server](#).

## 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 [System Requirements: VMM Library Server](#). 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	<b>VMMServer01.contoso.com</b>
Library share in Seattle (added during VMM management server installation)	<b>VMMServer01\SEALibrary</b>
Library server and share in New York	<b>NYLibrary01\NYLibrary</b>

### In This Section

Use the following procedures to perform basic configuration of the VMM library.

Procedure	Description
<a href="#">How to Add a VMM Library Server or VMM Library Share</a>	Describes how to add a new library server or library share.
<a href="#">How to Associate a VMM Library Server with a Host Group</a>	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.
<a href="#">How to Add File-Based Resources to the VMM Library</a>	Describes how to add file-based resources to the library.
<a href="#">How to Create or Modify Equivalent Objects in the VMM Library</a>	Describes how to mark file-based objects as equivalent.
<a href="#">How to View and Remove Orphaned Resources in VMM</a>	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 in [System Requirements: VMM Library Server](#).
- 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 Overview](#)

[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 Overview](#)

### **How to Add File-Based Resources to the VMM Library**

You can use the following procedure to add file-based resources (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 Overview](#).

**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.

#### See Also

[Configuring the VMM Library Overview](#)

[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 Overview](#)

### 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 Overview](#)

## Configuring Networking in VMM Overview

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):** Networking in VMM in System Center 2012 Service Pack 1 (SP1) 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 Virtual Machine Manager](#)
  - **Configuring Logical Networking in VMM Illustrated Overview**
  - **Configuring VM Networks in VMM in System Center 2012 SP1 Illustrated Overview**
  - **Configuring Ports and Switches in VMM in System Center 2012 SP1 Illustrated Overview**
- For information about configuring networking options that are available in both System Center 2012 and System Center 2012 SP1, 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, see the following:
  - [Configuring Ports and Switches for VM Networks in System Center 2012 SP1](#)
  - [Configuring VM Networks and Gateways in System Center 2012 SP1](#)

## Next steps after configuring networking

For information about the next steps to take after configuring networking, see the following topics:

Topic	Step
<a href="#">Preparing the Fabric in VMM</a>	Configure additional fabric resources such as storage and library resources.
<a href="#">Adding and Managing Hyper-V Hosts and Host Clusters in VMM</a>	Configure hosts.

Topic	Step
<a href="#">Managing VMware ESX and Citrix XenServer in VMM</a>	
<a href="#">Creating and Deploying Virtual Machines and Services in VMM</a>	Deploy virtual machines, individually or as part of a service.

## Common Scenarios for Networking in Virtual Machine Manager

This topic presents various networking options in Virtual Machine Manager (VMM) that can help to enhance and extend the ways that you work with IP addressing, virtual local area networks (VLANs), routers, switches, and other elements of networking.

### Scenarios supported in both System Center 2012 and System Center 2012 SP1

The following table describes how you can use networking options in VMM to configure the fabric that host systems and virtual machines use.



#### Important

The scenarios in the following table can be configured in either System Center 2012 or System Center 2012 Service Pack 1 (SP1).

Scenario	Key information	For more information, see ...
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 ("logical networks") that virtual machines can use.	<ul style="list-style-type: none"> <li>• <b>In System Center 2012:</b> You can design logical networks to suit your environment.</li> <li>• <b>In System Center 2012 SP1:</b> Logical networks provide a foundation for virtual machine networks (VM networks), which expand your options. See the table in <a href="#">Scenarios for networking for virtual machines in System Center 2012 SP1</a> in this topic.</li> </ul>	<a href="#">Configuring Logical Networking in VMM Overview</a>  <a href="#">How to Create a Logical Network in VMM</a>
Simplify IP address management	<ul style="list-style-type: none"> <li>• <b>In System Center 2012:</b> After</li> </ul>	<a href="#">Configuring Logical Networking</a>

Scenario	Key information	For more information, see ...
in VMM on networks where you do not use Dynamic Host Configuration Protocol (DHCP).	<p>you create logical networks, you can create IP address pools and, if needed, media access control (MAC) address pools for the logical networks.</p> <ul style="list-style-type: none"> <li>• <b>In System Center 2012 SP1:</b> After you create logical networks, VM networks, or both, you can create IP address pools and, if needed, MAC address pools for those networks. (Also see the VM network scenarios in <a href="#">Scenarios for networking for virtual machines in System Center 2012 SP1</a> in this topic.)</li> </ul>	<p><a href="#">in VMM Overview</a></p> <p><a href="#">How to Create IP Address Pools for Logical Networks in VMM</a></p>
Automatically provision load balancers in your virtualized environment.	<ul style="list-style-type: none"> <li>• Either use Microsoft Network Load Balancing (NLB) or add supported hardware load balancers to VMM.</li> <li>• NLB is included as an available load balancer with VMM.</li> </ul>	<p><a href="#">Configuring Load Balancing in VMM Overview</a></p>

### Additional scenarios supported in System Center 2012 SP1

This section lists scenarios that are supported in VMM in System Center 2012 SP1, in addition to the scenarios in the previous section. The scenarios are presented in the following two categories:

- [Scenarios for creating the networking environment for hosts in System Center 2012 SP1](#)
- [Scenarios for networking for virtual machines in System Center 2012 SP1](#)



#### Important

The scenarios in the following tables can be configured only in System Center 2012 SP1.

### Scenarios for creating the networking environment for hosts in System Center 2012 SP1

The following table describes ways that you can use networking capabilities in VMM in System Center 2012 SP1 as you configure the networking environment for hosts. For additional scenarios, see [Scenarios for networking for virtual machines in System Center 2012 SP1](#) in this topic.

Scenario	Key information	For more information, see ...
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.	<ul style="list-style-type: none"> <li>Configure a native port profile for virtual network adapters that will limit the amount of bandwidth. Also configure a logical switch that includes that port profile.</li> <li>Assign the logical switch to the management adapter, either in the host's properties, or in a host profile that you use for deploying Hyper-V hosts.</li> </ul>	<a href="#">Configuring Ports and Switches for VM Networks in System Center 2012 SP1</a>  <a href="#">How to Configure Network Settings on a Host by Applying a Logical Switch in System Center 2012 SP1</a>  <a href="#">How to Create a Host Profile in VMM</a>
On a host, configure teaming of multiple physical network adapters for increased availability.	<ul style="list-style-type: none"> <li>Configure a logical switch and associate it with multiple physical adapters on the host.</li> <li>The logical switch that you create for this purpose must use <b>Team</b> for the uplink mode.</li> </ul>	<a href="#">Configuring Ports and Switches for VM Networks in System Center 2012 SP1</a>  <a href="#">How to Configure Network Settings on a Host by Applying a Logical Switch in System Center 2012 SP1</a>  <a href="#">How to Create a Host Profile in VMM</a>

### Scenarios for networking for virtual machines in System Center 2012 SP1

The following table describes ways that you can use networking capabilities in VMM to configure networks that virtual machines use. For additional scenarios, see [Scenarios for creating the networking environment for hosts in System Center 2012 SP1](#) in this topic.

#### Important

- The scenarios in the following table can be configured only in System Center 2012 SP1.

- In System Center 2012 SP1, VM networks and other VMM networking enhancements are based on Hyper-V Network Virtualization 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
<p>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 ("logical networks") that virtual machines can use.</p>	<ul style="list-style-type: none"> <li>• Logical networks, which were introduced in System Center 2012, can still be used in System Center 2012 SP1 by creating a logical network, then creating a VM network that specifies that logical network and specifies <b>No isolation</b>. The VM network will function as a logical network with no isolated networks within it. (For more options with VM networks, see the last seven rows in this table.)</li> <li>• Only one VM network that is configured with <b>No isolation</b> can be assigned to each logical network.</li> </ul>	<p><a href="#">Configuring Logical Networking in VMM Overview</a></p> <p><a href="#">How to Create a Logical Network in VMM</a></p> <p><a href="#">How to Create a VM Network in System Center 2012 SP1</a></p>
<p>In a virtualized network environment, monitor network traffic, use quality of service (QoS) to control network bandwidth usage, or enhance the level of security.</p>	<ul style="list-style-type: none"> <li>• 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).</li> <li>• 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</li> </ul>	<p><a href="#">Configuring Ports and Switches for VM Networks in System Center 2012 SP1</a></p>

Scenario	Key information	For more information
	to 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 VM networks.	<ul style="list-style-type: none"> <li>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.</li> <li>Then create logical switches, which bring together multiple network settings and capabilities that you want to make available on particular hosts.</li> </ul>	<a href="#">Configuring Ports and Switches for VM Networks in System Center 2012 SP1</a>  <a href="#">How to Add a Virtual Switch Extension Manager in System Center 2012 SP1</a>
Move virtual machines and their associated networks in a single operation.	<ul style="list-style-type: none"> <li>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 uses network virtualization if the logical network on which it is configured allows network virtualization.)</li> </ul>	<a href="#">Configuring VM Networks and Gateways in System Center 2012 SP1</a>  <a href="#">How to Create a VM Network in System Center 2012 SP1</a>  <b>How to Create a Virtual Machine Template</b>
Connect virtual machines on VM networks to computers on connected physical networks. (For a similar scenario for a hoster, see the last line in this table.)	<ul style="list-style-type: none"> <li>Create a VM network that uses network virtualization, and configure it with a gateway to <b>Local networks</b>. A VM network uses network virtualization if the logical network on which it is configured allows network virtualization.</li> <li>Before you configure the VM network to use the gateway, you must obtain provider software for the gateway and</li> </ul>	<a href="#">Configuring VM Networks and Gateways in System Center 2012 SP1</a>  <a href="#">How to Add a Gateway in System Center 2012 SP1</a>

Scenario	Key information	For more information
	<p>install it on the VMM management server.</p> <ul style="list-style-type: none"> <li>• The gateway will act as a router to the physical network.</li> </ul>	
<p>Manage networks that use familiar VLAN technology for network isolation, but use VMM to simplify the management process.</p>	<ul style="list-style-type: none"> <li>• Obtain information about the isolated VLANs that have been created within the physical network. Then, in VMM, create a logical network and specify <b>Network sites within this logical network are not connected</b>. Follow additional steps in <a href="#">Configuring VM Networks and Gateways in System Center 2012 SP1</a>.</li> <li>• The completed configuration has one VM network for each isolated VLAN in your physical network.</li> </ul>	<p><a href="#">Configuring VM Networks and Gateways in System Center 2012 SP1</a></p> <p><a href="#">How to Create a Logical Network in VMM</a></p> <p><a href="#">How to Create a VM Network in System Center 2012 SP1</a></p>
<p>In the hosted environment that you provide, allow each tenant, client, or customer to have their own networks that are isolated from the networks of other tenants, clients, or customers.</p>	<ul style="list-style-type: none"> <li>• Use network virtualization. To do this, create a logical network (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.</li> </ul>	<p><a href="#">Configuring VM Networks and Gateways in System Center 2012 SP1</a></p> <p><a href="#">How to Create a Logical Network in VMM</a></p> <p><a href="#">How to Create a VM Network in System Center 2012 SP1</a></p>
<p>In the hosted environment that you provide, allow your tenants, clients, or customers to “Bring your own IP”—in other words, you offer them an environment</p>	<ul style="list-style-type: none"> <li>• Use network virtualization. To do this, create a logical network (the foundation), specify that the logical network allows for VM networks that use network</li> </ul>	<p><a href="#">Configuring VM Networks and Gateways in System Center 2012 SP1</a></p> <p><a href="#">How to Create a Logical Network</a></p>

Scenario	Key information	For more information
in which they can use whatever IP addresses they want for their virtual machines.	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.	<a href="#">in VMM</a>  <a href="#">How to Create a VM Network in System Center 2012 SP1</a>
In the hosted environment that you provide, allow your tenants, clients, or customers to configure some aspects of their own networks, based on limits that you specify.	<ul style="list-style-type: none"> <li>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.)</li> </ul>	<a href="#">Configuring VM Networks and Gateways in System Center 2012 SP1</a>  <a href="#">How to Create a VM Network in System Center 2012 SP1</a>  <a href="#">How to Create a Tenant Administrator User Role in VMM in System Center 2012 SP1</a>
In the hosted environment that you provide, allow your tenants to connect their virtual machines to systems on their own premises. (From the tenant perspective, the connection is between “the cloud” and their local network.)	<ul style="list-style-type: none"> <li>Create the tenant’s VM network so that it uses network virtualization, and configure it with a gateway to <b>Remote networks</b>. A VM network uses network virtualization if the logical network on which it is configured allows network virtualization.</li> <li>Before you configure the gateway, you must first obtain the provider software that works with the tenant’s gateway and install that provider on the VMM management server.</li> <li>This configuration provides a site-to-site, virtual-private-network (VPN) connection from the tenant’s VM network (in the hosted environment that you</li> </ul>	<a href="#">Configuring VM Networks and Gateways in System Center 2012 SP1</a>  <a href="#">How to Add a Gateway in System Center 2012 SP1</a>

Scenario	Key information	For more information
	provide) to a VPN gateway on the tenant's premises.	

## See Also

**Configuring Logical Networking in VMM Illustrated Overview**

**Configuring Ports and Switches in VMM in System Center 2012 SP1 Illustrated Overview**

**Configuring VM Networks in VMM in System Center 2012 SP1 Illustrated Overview**

## Configuring Logical Networking in VMM Overview

With Virtual Machine Manager (VMM) in System Center 2012 or in System Center 2012 Service Pack 1 (SP1), 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.

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.



### 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 Overview](#). 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 Virtual Machine Manager](#)
- [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 System Center 2012 SP1](#) (for System Center 2012 SP1 only): 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 System Center 2012 SP1](#) (for System Center 2012 SP1 only): 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 in System Center 2012 SP1 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	<p><b>BACKEND – Seattle</b></p> <ul style="list-style-type: none"> <li>• Scoped to the Seattle host group</li> <li>• Associated subnet and VLAN: 10.0.0.0/24 VLAN 7</li> </ul> <p><b>BACKEND – New York</b></p>

Logical network	Network sites
	<ul style="list-style-type: none"> <li>• Scoped to the New York host group</li> <li>• Associated subnet and VLAN: 172.16.0.0/24 VLAN 12</li> </ul>

Before you create network sites, review the following guidelines.

- If you are running System Center 2012 SP1, 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 both System Center 2012 and System Center 2012 SP1.

- 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, 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.

For information about how to create static IP address pools for logical networks in both System Center 2012 and System Center 2012 SP1, 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 System Center 2012 SP1](#).

### **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**

With VMM in System Center 2012 SP1, 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 System Center 2012 SP1](#).

- **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.)

## Creating an IP address pool to support multicasting or broadcasting

With VMM in System Center 2012 SP1, 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 System Center 2012 SP1](#).) 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:** 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 Service Pack 1 (SP1), 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 System Center 2012 SP1](#).

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 System Center 2012 SP1](#)
- [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](#).

**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 Virtual Machine Manager](#)
- **Configuring Logical Networking in VMM Illustrated Overview**

To configure logical networking, complete the procedures in the following table.

Procedure	Description
<a href="#">How to Configure Global Network Settings in</a>	Describes how to configure default VMM settings for automatic logical network and

Procedure	Description
<a href="#">VMM</a>	virtual network creation.
<a href="#">How to Create a Logical Network in VMM</a>	Describes how to create a logical network, including how to create network sites and assign IP subnets and VLANs.
<a href="#">How to Modify or Delete a Logical Network in VMM</a>	Describes how to modify or delete a logical network, including associated network sites and IP address pools.
<a href="#">How to Create IP Address Pools for Logical Networks in VMM</a>	Describes how to create static IP address pools for logical networks. These IP address pools are made available to hosts, virtual machines, and services.
<a href="#">How to Create Custom MAC Address Pools in VMM</a>	Describes how to create custom MAC address pools so that they are available for assignment to virtual machines.
<a href="#">How to Release Inactive IP or MAC Addresses in VMM</a>	Describes how to return inactive addresses to the IP address or MAC address pools to make them available for reassignment.

### 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
<a href="#">Configuring Load Balancing in VMM Overview</a>	If necessary, configure load balancers in your virtualized environment.
<a href="#">Configuring Ports and Switches for VM Networks in System Center 2012 SP1</a> (for System Center 2012 SP1 only)	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

Topic	Step
	adapters. After you configure port settings, configure logical switches and, as necessary, switch extensions (for Quality of Service (QoS), monitoring, or security).
<a href="#">Configuring VM Networks and Gateways in System Center 2012 SP1</a> (for System Center 2012 SP1 only)	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
<a href="#">Preparing the Fabric in VMM</a>	Configure additional fabric resources, such as storage and library resources.
<a href="#">Adding and Managing Hyper-V Hosts and Host Clusters in VMM</a> <a href="#">Managing VMware ESX and Citrix XenServer in VMM</a>	Configure hosts.
<a href="#">Creating and Deploying Virtual Machines and Services in VMM</a>	Deploy virtual machines, either individually or as part of a service.

### See Also


[Configuring Networking in VMM Overview](#)

**Configuring Logical Networking in VMM Illustrated Overview**

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 between System Center 2012 and System Center 2012 Service Pack 1 (SP1). 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	<p>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.</p> <div> <b>Note</b> This setting is only applied when you add a host to VMM</div>

	<p>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 <b>First DNS Suffix Label</b> and <b>DNS Suffix</b> are not supported. Therefore, by default, ESX and XenServer hosts use the <b>Virtual Network Switch Name</b> option.</p> <ul style="list-style-type: none"> <li> <b>First DNS Suffix Label</b> (the default) <p>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”.</p> </li> <li> <b>DNS Suffix</b> <p>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”.</p> </li> <li> <b>Network Connection Name</b> <p>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”.</p> </li> <li> <b>Virtual Network Switch Name</b> <p>The name of the virtual network switch to which the physical network</p> </li> </ul>
--	---

	<p>adapter of the host is bound.</p> <ul style="list-style-type: none"> <li>• <b>Disabled</b></li> </ul> <p>You can also specify the option to use if the first logical network matching selection fails. You can select one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Virtual Network Switch Name</b> (default)</li> <li>• <b>Network Connection Name</b></li> <li>• <b>Disabled</b></li> </ul>
<b>Automatic creation of logical networks</b>	<p>By default, the <b>Create logical networks automatically</b> 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, on the logical network, VMM also creates a VM network configured with “no isolation.”</p> <p> <b>Note</b> 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.</p>
In System Center 2012: <b>Automatic creation of virtual networks</b>	<p>In System Center 2012, by default, the <b>Create virtual networks automatically</b> setting is enabled. If the host has a physical network adapter with an associated logical network, but no virtual networks attached, VMM</p>

	<p>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.</p> <p> <b>Note</b> This setting only applies to Hyper-V hosts.</p>
In System Center 2012 SP1: <b>Automatic creation of virtual switches</b>	In System Center 2012 SP1, there is a setting labeled <b>Create virtual switches automatically</b> . 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 Overview](#)

[Configuring Logical Networking in VMM Overview](#)

[Configuring Ports and Switches for VM Networks in System Center 2012 SP1](#)

[Configuring VM Networks and Gateways in System Center 2012 SP1](#)

## How to Create a Logical Network in VMM

With Virtual Machine Manager (VMM) in System Center 2012 or in System Center 2012 Service Pack 1 (SP1), 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 they continue as part of networking in System Center 2012 SP1.

For more information about logical networks and how they work with other network configuration options in VMM, see [Common Scenarios for Networking in Virtual Machine Manager](#) and [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, 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 Virtual Machine Manager](#) and [Configuring VM Networks and Gateways in System Center 2012 SP1](#).

Use of the VM network or networks that will be created on top of this logical network	Action
<b>Hyper-V network virtualization:</b> multiple VM networks with isolation	Select <b>Allow new VM networks created on this logical network to use network virtualization.</b>
<b>VLAN-based configuration:</b> manage VLANs that have been created for network isolation within the physical network	<p>Select <b>Network sites within this logical network are not connected.</b></p> <p>If you are using private VLAN technology, also select <b>Network sites within this logical network contain private VLANs.</b> (Otherwise, do not select it.)</p> <p>For information about additional steps for this configuration, see “VLAN-based configuration” in the list in <a href="#">Configuring VM Networks and Gateways in System Center 2012 SP1</a>.</p>
<b>One VM network that gives direct access to the logical network:</b> 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 allow network virtualization. If this logical network will not use network virtualization at all, leave all check boxes cleared.
<b>External networks:</b> use VMM in coordination with a vendor network-management console	Do not create the logical network manually from within VMM. Instead, follow the steps in <a href="#">How to Add a Virtual Switch Extension Manager in System Center 2012 SP1</a> . 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).

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 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

**Create Logical Network Wizard**

## Network Site

**Name**

Network Site

Summary

### Network sites

Network sites can be added to a logical network to associate VLANs and subnets to host groups.  
Enter IP subnets using CIDR notation, for example: 192.168.1.0/24, FD4A:29CD:184F:3A2C::/64.

**BACKEND-Seattle**

Host groups that can use this network site:

- ☐ All Hosts
- ☒ Seattle

Associated VLANs and IP subnets:

VLAN	IP subnet
7	10.0.0.0/24

Insert row

Delete row

Network site name: BACKEND-Seattle

Previous Next Cancel

- Optionally, create additional network sites by clicking **Insert row** 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 System Center 2012 SP1](#)

[Common Scenarios for Networking in Virtual Machine Manager](#)

**Configuring Logical Networking in VMM Illustrated Overview**

[Configuring Networking in VMM Overview](#)

**Configuring VM Networks in VMM in System Center 2012 SP1 Illustrated Overview**

#### How to Modify or Delete a Logical Network in VMM

You can use the following procedures to modify or delete a logical network in System Center 2012 – 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, 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, 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 Overview](#)

[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), 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:	<b>BACKEND – Seattle IP pool</b>
Description:	<b>IP addresses for internal application and database servers - Seattle</b>

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 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 and want to use multicasting or broadcasting, follow this step. Otherwise, skip to the next numbered step.

With System Center 2012 SP1, 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:	<b>10.0.0.10</b>
Ending IP address:	<b>10.0.0.99</b>

**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](#).

#### See Also

[How to Release Inactive IP or MAC Addresses in VMM](#)

[Configuring Logical Networking in VMM Overview](#)

[Configuring Networking in VMM Overview](#)

[How to Create a Logical Network in VMM](#)

[How to Create IP Address Pools for VM Networks in System Center 2012 SP1](#)

[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 X1, X3, X5, X7, X9, XB, XD, or XF, 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 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	<b>MAC pool - Seattle</b>
Description	<b>MAC pool for Seattle and its child host groups (Hyper-V and XenServer)</b>

- 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	<b>00:1D:D8:B7:1C:00</b>
Ending MAC address	<b>00:1D:D8:B7:1F:E8</b>

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](#)

## 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 Overview](#)

### 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, UDP, 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 Overview](#).

**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 learn about ways to use load balancing and other networking features in VMM, see the following list of scenarios:

- [Common Scenarios for Networking in Virtual Machine Manager](#)

To configure load balancing in your virtualized environment, follow these procedures:

Procedure	Description
<a href="#">How to Add Hardware Load Balancers in VMM</a>	<p>Describes how to add supported hardware load balancers to the VMM environment so that you can load balance service requests.</p> <p> <b>Note</b></p> <p>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.</p>
<a href="#">How to Create VIP Templates for Hardware Load Balancers in VMM</a>	<p>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.</p>
<a href="#">How to Create VIP Templates for Network Load Balancing (NLB) in VMM</a>	<p>Describes how to create NLB virtual IP templates that you can use during service creation to configure NLB for a service tier.</p>

**Next steps after configuring load balancing in System Center 2012 SP1**

For information about the next steps to take after configuring load balancing in System Center 2012 SP1, see the following networking overviews:

Topic	Step
<a href="#">Configuring Ports and Switches for VM Networks in System Center 2012 SP1</a> (for System Center 2012 SP1 only)	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).
<a href="#">Configuring VM Networks and Gateways in System Center 2012 SP1</a> (for System Center 2012 SP1 only)	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
<a href="#">Preparing the Fabric in VMM</a>	Configure additional fabric resources such as storage and library resources.
<a href="#">Adding and Managing Hyper-V Hosts and Host Clusters in VMM</a>  <a href="#">Managing VMware ESX and Citrix XenServer in VMM</a>	Configure hosts.
<a href="#">Creating and Deploying Virtual Machines and</a>	Deploy virtual machines, individually or as part

Topic	Step
<a href="#">Services in VMM</a>	of a service.

## See Also

[Common Scenarios for Networking in Virtual Machine Manager](#)

[Configuring Logical Networking in VMM Overview](#)

[Configuring Ports and Switches for VM Networks in System Center 2012 SP1](#)

[Configuring VM Networks and Gateways in System Center 2012 SP1](#)

[Configuring Networking in VMM Overview](#)

## 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 scvmm** service, press ENTER, type **net start scvmm** service, 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 Overview](#)

[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**
  - **HTTPS terminate**

If you click this option, encryption carries all the way through to the virtual machine, and it is not decrypted at the load balancer.

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 Overview](#)

[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 Overview](#)

[How to Configure NLB for a Service Tier](#)

#### Configuring Ports and Switches for VM Networks in System Center 2012 SP1

In Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1), 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 Virtual Machine Manager](#).
- For illustrations showing how logical switches relate to port profiles and port classifications, see **Configuring Ports and Switches in VMM in System Center 2012 SP1 Illustrated Overview**.
- In System Center 2012 SP1, some of the VMM networking enhancements are based on the Hyper-V Virtual Switch 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	A native port profile for uplinks (also called an uplink port profile) specifies which logical networks can connect through a particular

Networking item in VMM	Uses and settings
	<p>physical network adapter.</p> <p>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 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.</p> <p>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 <b>Uplink mode</b>, select <b>Team</b> to enable teaming. In the uplink port profile, select appropriate <b>Load-balancing algorithm</b> and <b>Teaming mode</b> settings (or use the default settings). For background information about load-balancing algorithms and teaming modes, see <a href="#">NIC Teaming Overview</a>.</p>
<b>Native port profile for virtual network adapters</b>	<p>A native 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 provides details about these capabilities:</p> <ul style="list-style-type: none"> <li>• <b>Enable virtual machine queue</b> (offload</li> </ul>

Networking item in VMM	Uses and settings
	<p>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.</p> <p>VMQ requires support from the physical network adapter.</p> <ul style="list-style-type: none"> <li> <b>Enable IPsec task offloading</b> (offload setting): With this type of offloading, some 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 <a href="#">What's New in Hyper-V Virtual Switch</a>.         </li> </ul> <p>IPsec task offloading requires support from the physical network adapter and the guest operating system.</p> <ul style="list-style-type: none"> <li> <b>Enable Single-root I/O virtualization</b> (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.         </li> </ul> <p>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.</p> <p>To use SR-IOV with VMM, SR-IOV must be enabled or configured in multiple places. It must be enabled in the native port profile</p>

Networking item in VMM	Uses and settings
	<p>and 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 <b>Offload Settings</b>, and in the logical switch configuration, it is in the <b>General</b> settings. In the virtual switch, 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 you can create your own port classification.</p> <ul style="list-style-type: none"> <li>• <b>Allow MAC spoofing</b> (security setting): 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 may require this setting to be enabled.</li> <li>• <b>Enable DHCP guard</b> (security setting): With DHCP guard, you can protect against a malicious virtual machine representing itself as a Dynamic Host Configuration Protocol (DHCP) server for man-in-the-middle attacks.</li> <li>• <b>Allow router guard</b> (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.</li> <li>• <b>Allow guest teaming</b> (security setting): With guest teaming, you can team the virtual network adapter with other network adapters that are connected to</li> </ul>

Networking item in VMM	Uses and settings
	<p>the same switch.</p> <ul style="list-style-type: none"> <li>• <b>Allow IEEE priority tagging</b> (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.</li> <li>• <b>Bandwidth settings:</b> 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.</li> </ul>
<b>Port classification</b>	<p>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 named FAST to identify ports that are configured to have more bandwidth, and one port classification 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.</p>
<b>Logical switch</b>	<p>A logical switch brings port profiles, port classifications, and switch extensions together</p>

Networking item in VMM	Uses and settings
	<p>so that you can apply them to multiple network adapters.</p> <p>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 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.</p> <p>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 <b>Uplink mode</b>, select <b>Team</b> to enable teaming. In the uplink port profile, select appropriate <b>Load-balancing algorithm</b> and <b>Teaming mode</b> settings (or use the default settings). For background information about load-balancing algorithms and teaming modes, see <a href="#">NIC Teaming Overview</a>.</p> <p><b>Switch extensions</b> (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. Four types of switch</p>

Networking item in VMM	Uses and settings
	<p>extensions are supported in VMM:</p> <ul style="list-style-type: none"> <li>• <b>Monitoring</b> extensions can be used to monitor and report on network traffic, but they cannot modify packets.</li> <li>• <b>Capturing</b> extensions can be used to inspect and sample traffic, but they cannot modify packets.</li> <li>• <b>Filtering</b> extensions can be used to block, modify, or defragment packets. They can also block ports.</li> <li>• <b>Forwarding</b> 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 be active on a logical switch.</li> </ul>
Virtual switch extension manager	<p>A virtual switch extension 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 first install provider software (which is provided by the vendor) on the VMM management server. Then you must add the virtual switch extension manager to VMM, which tells 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.</p>

## Prerequisites

Before you configure ports, switches, and switch extensions for virtual machine networks (VM networks) in System Center 2012 SP1, 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. For example, for vendor-provided switch extension managers, review the table regarding the provider software that you must install on the VMM management server.

Configurable item	Prerequisite
<b>Native port profile for uplinks</b>	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.
<b>Native port profile for virtual network adapters</b>	<p>Before you create a native port profile for virtual network adapters, review the following guidelines:</p> <ul style="list-style-type: none"><li>• If you want to enable VMQ, IPsec task offloading, or SR-IOV, review the requirements for these capabilities, as described in the <a href="#">Settings</a> section, earlier in this topic.</li><li>• Determine which security or bandwidth settings, if any, you want to use. For more information, see the <a href="#">Settings</a> section, earlier in this topic.</li></ul>

Configurable item	Prerequisite
<b>Port classification</b>	Decide how you want to classify ports in your networking environment. For more information, see the <a href="#">Settings</a> section, earlier in this topic.
<b>Logical switch</b> , regardless of whether you use switch extensions	Decide how you want to combine port profiles and port classifications together 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.
<b>Logical switch</b> 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 complete, in the <b>Extensions</b> property of a logical switch, the virtual switch extension will appear in the list of extensions that you can select.
<b>Virtual switch extension manager</b>	Before you can add a virtual switch extension manager to VMM, 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. Then you will be able to add

Configurable item	Prerequisite
	the virtual switch extension 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 in System Center 2012 SP1 Illustrated Overview**

The following procedures can help you to use VMM to configure uplink port profiles, virtual network adapter port profiles, logical switches, and switch extensions in System Center 2012 SP1.

Procedure	Description
<a href="#">How to Create a Native Port Profile for Uplinks in System Center 2012 SP1</a>	Describes how to create a native port profile for uplinks. Create native port profiles before you create logical switches.
<a href="#">How to Create a Native Port Profile for Virtual Network Adapters in System Center 2012 SP1</a>	Describes how to create a native port profile for virtual network adapters. Create native port profiles before you create logical switches.
<a href="#">How to Create a Port Classification in System Center 2012 SP1</a>	Describes how to create a port classification. You can create port classifications either before or during the process of creating a logical switch.
<a href="#">How to Add a Virtual Switch Extension Manager in System Center 2012 SP1</a>	Describes how to add a virtual switch extension manager (optional). If you want to add a virtual switch extension manager, we recommend that you add it before you create your logical switch.
<a href="#">How to Create a Logical Switch in System Center 2012 SP1</a>	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

Procedure	Description
	consistently configure the capabilities for network adapters across multiple hosts.
<a href="#">How to Configure Network Settings on a Host by Applying a Logical Switch in System Center 2012 SP1</a>	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 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 is the same concept as the Hyper-V Virtual Switch, which is described in <a href="#">Hyper-V Virtual Switch Overview</a> .

#### Next steps after configuring 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 System Center 2012 SP1](#).

#### Next steps after configuring networking

For information about the next steps to take after you configure networking, see the topics in the following table.

Topic	Step
<a href="#">Preparing the Fabric in VMM</a>	Configure additional fabric resources, such as storage and library resources.
<a href="#">Adding and Managing Hyper-V Hosts and Host Clusters in VMM</a>  <a href="#">Managing VMware ESX and Citrix XenServer in VMM</a>	Configure hosts.
<a href="#">Creating and Deploying Virtual Machines and</a>	Deploy virtual machines, individually or as part

Topic	Step
<a href="#">Services in VMM</a>	of a service.

## See Also

[Configuring Networking in VMM Overview](#)

## Configuring Ports and Switches in VMM in System Center 2012 SP1 Illustrated Overview

### How to Create a Native Port Profile for Uplinks in System Center 2012 SP1

In Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1), 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 System Center 2012 SP1](#).

The recommended sequence 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.

Use the following procedure to create a native port profile for uplinks.

#### To create a native 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 **Native Port Profiles**.
4. On the **Home** tab, in the **Create** group, click **Create**, and then click **Native Port Profile**.

The **Create Native Port Profile Wizard** 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:

- **HyperVPort:** Distributes network traffic based on the Hyper-V switch port identifier of the source virtual machine. This is the default algorithm.
- **TransportPorts:** 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.
- **IPAddresses:** 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.
- **MacAddresses:** 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.

**Teaming mode:** the mode of the NIC teaming. The following options are available:

- **SwitchIndependent:** 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:** 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 **Enable Windows Network Virtualization** check box.

**Note**

The **Enable Windows Network Virtualization** setting 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 System Center 2012 SP1](#)

[How to Create a Logical Network in VMM](#)

[How to Create a Logical Switch in System Center 2012 SP1](#)

[Configuring Networking in VMM Overview](#)

**How to Create a Native Port Profile for Virtual Network Adapters in System Center 2012 SP1**

In Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1), 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 System Center 2012 SP1](#). 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 native 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 native port profile for virtual network adapters.

► **To create a native 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 **Native Port Profiles**.
4. On the **Home** tab, in the **Create** group, click **Create**, and then click **Native Port Profile**.

The **Create Native Port Profile Wizard** 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 System Center 2012 SP1](#), 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**
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 System Center 2012 SP1](#)

[Configuring Networking in VMM Overview](#)

### How to Create a Port Classification in System Center 2012 SP1

In Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1), 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 System Center 2012 SP1](#).

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 System Center 2012 SP1](#)

[Configuring Networking in VMM Overview](#)

[How to Create a Logical Switch in System Center 2012 SP1](#)

### 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.

Use the following procedure to add a virtual switch extension manager to VMM.

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 System Center 2012 SP1](#).

### 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**

## How to Create a Logical Switch in System Center 2012 SP1

In Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1), 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 System Center 2012 SP1](#). It is especially important to review the prerequisites if you plan to enable single-root I/O virtualization (SR-IOV) in your logical switch.

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**

## **Configuring Ports and Switches in VMM in System Center 2012 SP1 Illustrated Overview**

## **How to Configure Network Settings on a Host by Applying a Logical Switch in System Center 2012 SP1**

You can use the procedures in this topic to configure a network adapter on a Hyper-V host in System Center 2012 Service Pack 1 (SP1) by associating logical networks with the adapter and applying a logical switch and port profiles to the adapter. This topic also includes a procedure for viewing compliance information for network adapters on the host.

In Virtual Machine Manager (VMM) in System Center 2012 SP1, you can bring together the network settings that you configured in port profiles and logical switches by applying them to network adapters on a host. The network 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 is the same concept as the Hyper-V Virtual Switch, described in [Hyper-V Virtual Switch Overview](#).



### **Note**

Use these procedures if you are running System Center 2012 SP1 and you prefer to apply port profiles and logical switches (that you have already configured) to network adapters. If you prefer to specify each network adapter setting individually, or you are running System Center 2012, do not use these procedures. Instead, use the procedures in [How to Configure Network Settings on a Hyper-V Host in VMM](#).

Perform the procedures in this topic in the following 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](#)
3. [View compliance information for a network adapter](#) (Repeat this procedure as needed.)

### **Prerequisites**

Before you can perform this procedure, you must first configure multiple networking elements, including logical networks, port profiles, and logical switches. For more information, see [Configuring Ports and Switches for VM Networks in System Center 2012 SP1](#). It is especially important to review

prerequisites if you want to configure single-root I/O virtualization (SR-IOV) for network adapters on the host.

Also, before you can perform this procedure, you must add the host or hosts to VMM. For more information, see [Adding Hyper-V Hosts and Host Clusters to VMM](#) and [Managing VMware ESX and Citrix XenServer 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 on them. If a virtual network is not associated with the network adapter, when VMM connects a virtual machine to the physical network adapter, VMM automatically creates an external virtual network and associates it with the logical network. For more information about the default behavior, see [How to Configure Global Network 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.



#### 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 the **Available for placement** check box is selected. If you want to use this network adapter for communication between the host and the VMM management server, ensure that the **Used by management** check box is selected.



#### Important

- Make sure that you have at least one network adapter that is available for communication between the host and the VMM management server, and that **Used by management** is

selected 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

In Virtual Machine Manager (VMM) in System Center 2012 SP1, you can bring together network settings that you configured in port profiles and logical switches, by applying them to network adapters on a host.



#### Note

Use this procedure if you are running System Center 2012 SP1 and you prefer to apply port profiles and logical switches (that you have already configured) to network adapters. If you prefer to specify each network adapter setting individually, or you are running System Center 2012, do not use this procedure. Instead, use the procedures in [How to Configure Network Settings on a Hyper-V Host in VMM](#).

### ► 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 creating 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.

If certain network optimization capabilities are available on a host that is running Windows Server 2008 R2 or Windows Server 2012, VMM automatically detects the capabilities and displays a message. These capabilities are Virtual Machine Queue (VMQ) and TCP Chimney Offload. After VMM has detected that either or both of these capabilities are available, in the **Host Properties** dialog box, the **Virtual switches** tab will display the message **Network optimization is available on this virtual switch**. For information about these network optimization capabilities, see [Using TCP Chimney Offload](#) and [Using Virtual Machine Queue](#). For information about these network optimization capabilities in the context of VMM, see the “Network Optimization Support” section in [Configuring Virtual Networks in VMM](#) (which describes the capabilities in an earlier version of VMM).

### **View compliance information for a network adapter**

Compliance information indicates whether the settings on the host are consistent with the configuration in VMM. For example, compliance information indicates whether all IP subnets and VLANs that are included in a network site in a logical network are assigned to a network adapter.

#### **To view compliance information for a 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 network adapter.
5. In the **Network Compliance** column, view the compliance status.
  - A value of **Fully compliant** indicates that the settings on the 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 details 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.



#### Tip

In addition to the compliance information, you can also view detailed information about the network adapter, such as the assigned IP address and MAC address, and the associated virtual networks.

#### See Also

[Configuring Ports and Switches for VM Networks in System Center 2012 SP1](#)

**Configuring Ports and Switches in VMM in System Center 2012 SP1 Illustrated Overview**

[Configuring Networking in VMM Overview](#)

[Adding Hyper-V Hosts and Host Clusters to VMM](#)

[How to Configure Network Settings on a Hyper-V Host in VMM](#)

#### Configuring VM Networks and Gateways in System Center 2012 SP1

Networking in Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1) 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 Virtual Machine Manager](#).
- For illustrations of VM networks, see **Configuring VM Networks in VMM in System Center 2012 SP1 Illustrated Overview**.
- In System Center 2012 Service Pack 1 (SP1), many of the VMM networking enhancements are based on Hyper-V network virtualization 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 offer the ability to use network virtualization, which extends the concept of server virtualization to make it possible for you 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 do this, create a logical network, and on top of that logical network create multiple VM networks, each of which uses the option to **Isolate using Hyper-V 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 allow your tenants to configure some aspects of their own networks, based on limits that you specify.
- **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, using VMM to simplify the management process.



#### Note

Network virtualization is supported only on hosts that are running Windows Server 2012. Hosts that are running Windows Server 2008 R2 do not support network virtualization.



#### 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 **Network sites within this logical network are not connected**. (Do not select the option for private VLANs unless you are using private VLAN technology.) Within the logical network, configure a separate network site for each existing VLAN. Give each network site a name that will be 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 native 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 Native Port Profile for Uplinks in System Center 2012 SP1](#).
- 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 a setting of **No isolation**. 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 vendor network-management console:** With this configuration option, you can use 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 easy to view those settings in the context of your other network configuration settings. For a detailed description of this option, see [How to Add a Virtual Switch Extension Manager in System Center 2012 SP1](#).
- **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.) 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 hoster and you want 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, 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.

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 System Center 2012 SP1](#)

## Prerequisites for gateways

If you want to add a gateway to your configuration in VMM, you must first 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. For more information about setting up a specific gateway device, refer to the manufacturer's documentation.

If you want to connect a VM network through a VPN tunnel to another site, when you configure the **Gateway** wizard page or the **Gateway** tab for that VM network, you will select the **Remote networks** setting. Before you configure this setting, 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).
- Identify the authentication method to use with the remote VPN server. If the remote VPN server is configured to use a preshared key, you can authenticate by using a **Run As** account in which you

specify the preshared 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 you gather will help 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, complete the procedures in the following table.

Procedure	Description
<a href="#">How to Configure Global Network Settings in VMM</a>	Describes how to configure default VMM settings for automatic logical network and virtual network creation.
<a href="#">How to Add a Gateway in System Center 2012 SP1</a>	Describes how to add a gateway that can connect your virtualized networks to other networks. If you want to add a 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.
<a href="#">How to Create a VM Network in System Center 2012 SP1</a>	Describes how to create a VM network, with information about deploying multiple VM networks with “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.
<a href="#">How to Create IP Address Pools for VM Networks in System Center 2012 SP1</a>	Describes how to create static IP address pools for VM networks. These IP address pools are made available to virtual machines and

Procedure	Description
	services that use the VM networks.
<a href="#">How to Release Inactive IP Addresses for VM Networks in System Center 2012 SP1</a>	Describes how to return inactive addresses to an IP address pool to make them available for reassignment.
<a href="#">How to View VMM Network Configuration Diagrams in System Center 2012 SP1</a>	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
<a href="#">Preparing the Fabric in VMM</a>	Configure additional fabric resources, such as storage and library resources.
<a href="#">Adding and Managing Hyper-V Hosts and Host Clusters in VMM</a> <a href="#">Managing VMware ESX and Citrix XenServer in VMM</a>	Add and configure hosts.
<a href="#">Creating and Deploying Virtual Machines and Services in VMM</a>	Deploy virtual machines, individually or as part of a service.

### See Also

[Configuring Networking in VMM Overview](#)

**Configuring VM Networks in VMM in System Center 2012 SP1 Illustrated Overview**

**How to Add a Gateway in System Center 2012 SP1**

In Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1), you can connect a VM network to other networks by using a gateway. This topic describes how you can add a gateway to the list of resources in VMM.

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 System Center 2012 SP1](#)

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

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 System Center 2012 SP1](#) and see the first procedure in [How to Create a VM Network in System Center 2012 SP1](#).

## See Also

[Configuring VM Networks and Gateways in System Center 2012 SP1](#)

[Configuring Networking in VMM Overview](#)

[How to Create a VM Network in System Center 2012 SP1](#)

## How to Create a VM Network in System Center 2012 SP1

With VMM in System Center 2012 Service Pack 1 (SP1), you can configure VM networks on top of your logical networks, to 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 System Center 2012 SP1](#).

### 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 Virtual Machine Manager](#).
- For illustrations of VM network configurations, see **Configuring VM Networks in VMM in System Center 2012 SP1 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.

In the following table, identify the VM network option that you want, based on the descriptions in [Configuring VM Networks and Gateways in System Center 2012 SP1](#). 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	Select the check box to enable	<a href="#">Create a VM network on a logical</a>

Intended VM network option	Correct setting for the logical network on which you will add the VM network	Procedure within this topic
(in other words, using isolation)	network virtualization.	<a href="#">network where network virtualization is enabled</a>
VLAN-based configuration	<p>Select <b>Network sites within this logical network are not connected</b>.</p> <p>If you are using private VLAN technology, also select the check box for private VLANs. Otherwise, do not select it.</p>	<a href="#">Create a VM network on a logical network that uses VLANs for isolation</a>
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.	<a href="#">Create a VM network that gives direct access to a logical network (no isolation)</a>
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 <a href="#">How to Add a Virtual Switch Extension Manager in System Center 2012 SP1</a> .

## 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 System Center 2012 SP1](#).
- 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. For more details, see [How to Add a Gateway in System Center 2012 SP1](#). You can also create your VM network without a gateway, then add a gateway to your VMM configuration, and later open the property sheet of the VM network and configure it to use the gateway.

► **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**, and then click **Next**. (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.)
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 System Center 2012 SP1](#). 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 System Center 2012 SP1](#).



#### 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 System Center 2012 SP1](#).



#### 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

## Configuring VM Networks in VMM in System Center 2012 SP1 Illustrated Overview

### [Configuring VM Networks and Gateways in System Center 2012 SP1](#)

### [Configuring Networking in VMM Overview](#)

## How to Create IP Address Pools for VM Networks in System Center 2012 SP1

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). 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 System Center 2012 SP1](#).

### To create static IP address pools for VM networks in System Center 2012 SP1

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 System Center 2012](#)

[SP1.](#)

## See Also

[How to Release Inactive IP Addresses for VM Networks in System Center 2012 SP1](#)

[Configuring VM Networks and Gateways in System Center 2012 SP1](#)

[How to Create a VM Network in System Center 2012 SP1](#)

[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 System Center 2012 SP1

With Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1), 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, Virtual Machine Manager (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 Overview](#)

[How to Release Inactive IP or MAC Addresses in VMM](#)

[How to Create a VM Network in System Center 2012 SP1](#)

### How to View VMM Network Configuration Diagrams in System Center 2012 SP1

With Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1), 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 Overview](#)

## Configuring VM Networks in VMM in System Center 2012 SP1 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 in System Center 2012 SP1 Illustrated Overview

## Configuring Storage in VMM Overview

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 available on a server (or directly attached to a server), and is typically used for low-cost virtualization solutions. Remote storage offloads work from the server to an external storage device, with scaling and capacity provided by the storage hardware.

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, using fiber channel, iSCSI, and SAS connection mechanisms.

- **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 Server 2012 file server or on a network-attached storage (NAS) device from storage vendors such as EMC and NetApp.

VMM in System Center 2012 Service Pack 1 (SP1) introduces a number of new changes for storage provider and automation support, including:

- 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 combines 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 using SMP, or uses SMAPI together with the Microsoft Standards-based Storage Management Service to communicate with SMI-S compliant storage. The Microsoft Standards-based Storage Management Service is an optional server feature that enables communication with SMI-S storage providers. It is enabled during installation of System Center 2012 SP1.
- SAN migration using the legacy Virtual Disk Service (VDS) hardware provider interface is not supported from System Center 2012 SP1 onwards. When upgrading from System Center 2012 to System Center 2012 SP1, you must remove the VDS hardware provider software from the VMM server and enable the SMI-S or native WMI SMP provider using instructions from the storage vendors.
- In addition to discovery and management of iSCSI arrays with static targets, System Center 2012 SP1 adds support for the discovery and management of iSCSI target arrays that support dynamic and manual targets (for example Starwind, HP P2000, HP Lefthand, Dell EqualLogic, and Microsoft iSCSI Software Target).
- VMM 2012 supports creation of a thin provisioning logical unit. System Center 2012 SP1 adds support for 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 thin provisioning must be enabled for a storage pool by the storage administrator.
- System Center 2012 SP1 provides support for the Microsoft iSCSI Software Target 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 System Center 2012 SP1 installation, in the path  
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 2012. Using System Center 2012 SP1 you can assign SMB file shares to Hyper-V stand-alone hosts and clusters. For more information, see [How to Assign SMB 3.0 File Shares to Hyper-V Hosts and Clusters in VMM](#)

## Deploying and managing storage resources

VMM allows you to model, deploy, and manage storage resources as follows:

- **Storage discovery**—Administrators often have little visibility into underlying storage infrastructures. Using System Center 2012 – VMM, you can automatically discover local and remote storage, including storage arrays, pools, logical units (storage volumes or logical unit numbers (LUNs), disks, volumes, and virtual disks).
- **Storage classification**—You can classify discovered storage using friendly descriptive names to create and expose a simplified storage model.
- **Storage provisioning**—System Center 2012 – VMM can create new logical units from available capacity, for provisioning to a Hyper-V host or cluster. New logical units can be provisioned using any of the following methods. The method you use depends on the type of storage array and the virtualization workload you need to deploy.
  - a. From available capacity—Creating a new logical unit from available capacity is useful when you have a pool of storage available, allowing control over how many logical units you create, and the size of each logical unit.
  - b. By creating a writeable snapshot of an existing logical unit—Creating a writeable snapshot of an existing logical unit allows you to rapidly create many copies of an existing virtual disk. You can provision multiple virtual machines in a small amount of time, with minimal load on the hosts. Depending on the array, snapshots can be created almost instantaneously, and are very space efficient.
  - c. By creating a clone of a logical unit—Creating 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 are typically not space efficient, and can take some time to create.
- **Storage allocation**—You can allocate available storage pools and LUNs to defined host groups that can represent business groups, locations and so on. Resources typically need to 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 storage area network (SAN) snapshots or cloning.
- **Storage decommission**—VMM can decommission the storage it manages. This 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 allocated it, and assigns it to Hyper-V hosts or clusters as required. VMM automates this process by exposing the storage to the hosts, initializing the disks, and formatting new volumes. For cluster deployments, VMM creates the required cluster 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 2012 SP1 can create a cluster with up to 64 Hyper-V nodes, and automate the assignment of cluster shared storage as part of the same workflow. Simplifying 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](#).
- **Rapid Provisioning**—Storage arrays can create copies of virtual disks very efficiently with minimal load on the host. VMM can leverage this capability to rapidly create virtual machines. VMM understands 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, using a snapshot or cloning. VMM then exposes the storage to the host, mounting the file system, and associating the virtual disk with the virtual machine. In the administrator 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 using PowerShell. For more information, see [Rapid Provisioning a Virtual Machine by Using SAN Copy Overview](#).

## Configuring storage automation

### Before you begin

Before you begin configuring storage settings, note the following:

- Storage automation with VMM is only supported for Hyper-V hosts.
- 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.
- 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 as 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 needs to 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 FQDN.

- Notify your storage administrator that by default, when VMM manages the assignment of logical units, 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, with all the initiators from that 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 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 used to discover, classify, and assign storage using VMM:

1. **Discover storage**—From the VMM console, start the Add Storage Devices Wizard, and select the required provider type (Windows File Server, SMI-S, or WMI SMP). Windows 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. For instructions, see [How to Add and Classify SMI-S and SMP Storage Devices in VMM](#).
2. **Classify storage**—Classifying storage assigns a meaningful classification to storage pools. For example, you may 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 will be created during virtual machine rapid provisioning. Note that by default new logical units are created from available capacity. You only need 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 using your array vendor's management tools. If you use this method it will take 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 from 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 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 configuring storage and assigning to host groups, you can assign the storage to Hyper-V hosts and clusters as shared (Cluster Shared Volume) or available storage. Note that all nodes in the cluster should have access to the storage array 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 from 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 from 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 are using a Fibre Channel SAN, each host must have a host bus adapter (HBA), and the hosts must be zoned correctly.

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.

**Configuring an SMI-S Provider for iSCSI Target Server**

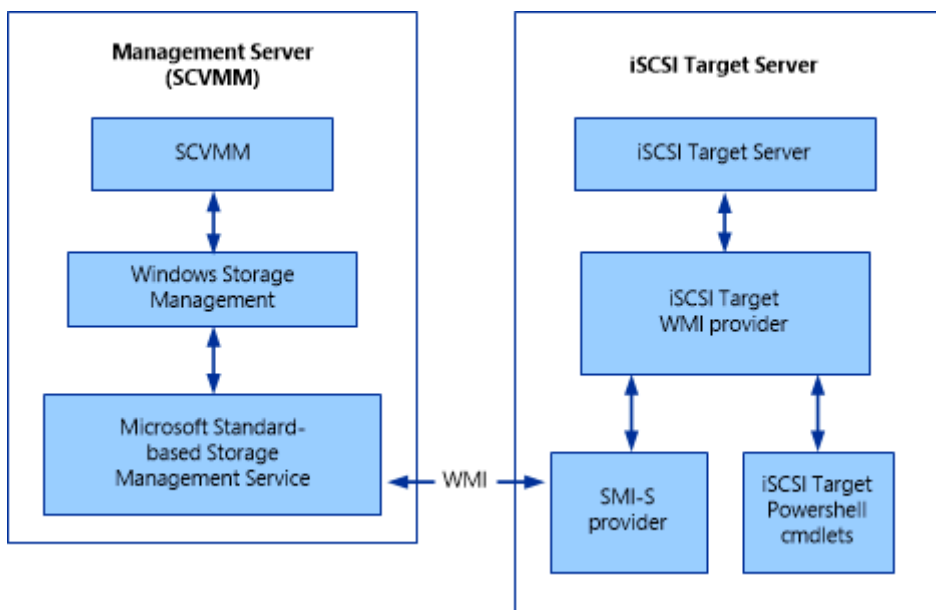
This topic provides information about the SMI-S provider required in order for the Microsoft iSCSI Target Server to be managed using Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1).

Microsoft iSCSI Target Server is a feature that enables a Windows Server 2012 server to function as a storage device. VMM 2012 supports the use of block storage devices implemented using the Storage

Management Initiative Specification (SMI-S), or using a native WMI storage management provider (SMP). VMM in System Center 2012 SP1 introduces support for the iSCSI Target Server using an SMI-S provider. Note that only VMM in System Center 2012 SP1 can be used to manage the SMI-S provider for iSCSI Target Server described in this topic. For more information, see [Introduction of iSCSI Target in Windows 2012](#).

## Architecture design

The SMI-S provider follows an “embedded” provider model, where the provider is installed on the iSCSI Target Server computer. The diagram below shows how the SMI-S provider interacts with other components. The SMI-S provider is WMI-based, and manages the iSCSI Target Server using the iSCSI Target WMI provider.



## Known issues

In this release of the SMI-S provider, there are a few known issues, as follows:

- iSCSI Target Server supports failover-clustering to provide high availability (HA). In order to be managed by the SMI-S provider, only one iSCSI Target Server resource group (VCO) can be supported per cluster. This is due to a limitation in the SMI-S provider, which currently can only handle one computer object. If there are multiple iSCSI Target resource groups (VCOs) present on the same cluster node, the SMI-S provider will not be able to obtain an accurate view of the objects on the computer.
- Only one WMI based SMI-S provider can be loaded on to one machine. Currently there are two WMI-based providers, and both of these will be affected by this issue:

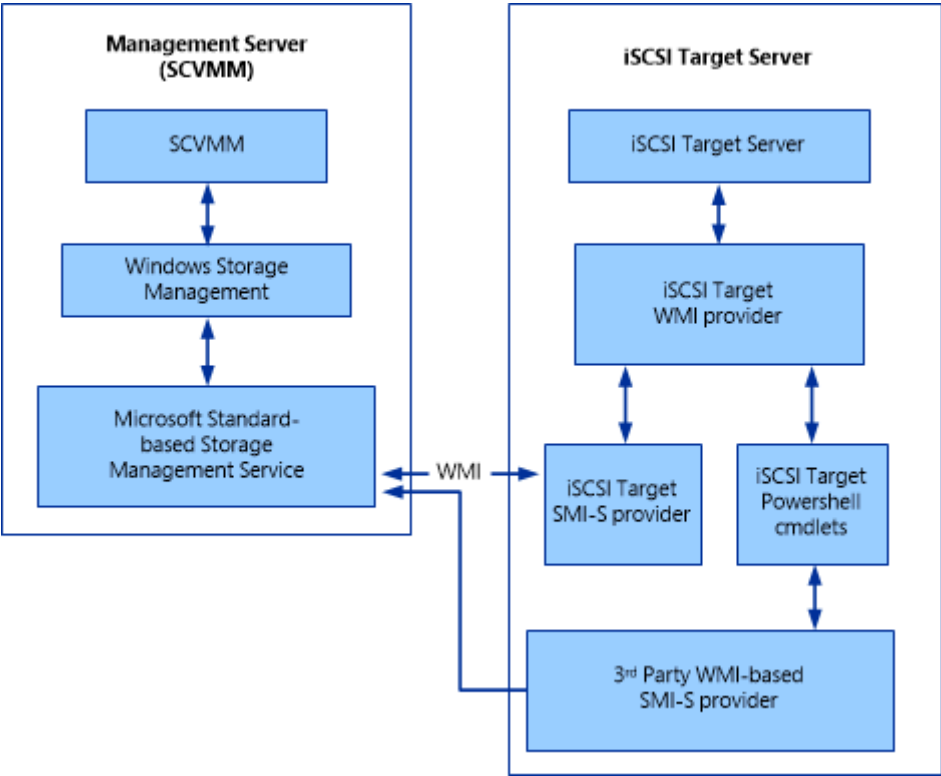
- iSCSI Target Server SMI-S provider
- LSI MegaRAID SMI-S provider

To avoid this issue, you will need to use a separate computer to host each SMI-S provider.

This issue will affect the two scenarios described in the following sections. The first scenario is where two SMI-S providers are installed on the same computer and both of them are intended for VMM management. The second is where two SMI-S providers are installed on the same computer and only one of them is intended for VMM management. In both of these scenarios, when two WMI-based SMI-S providers are installed on an iSCSI Target Server computer, only one of the providers will be discovered by the Storage Management Service.

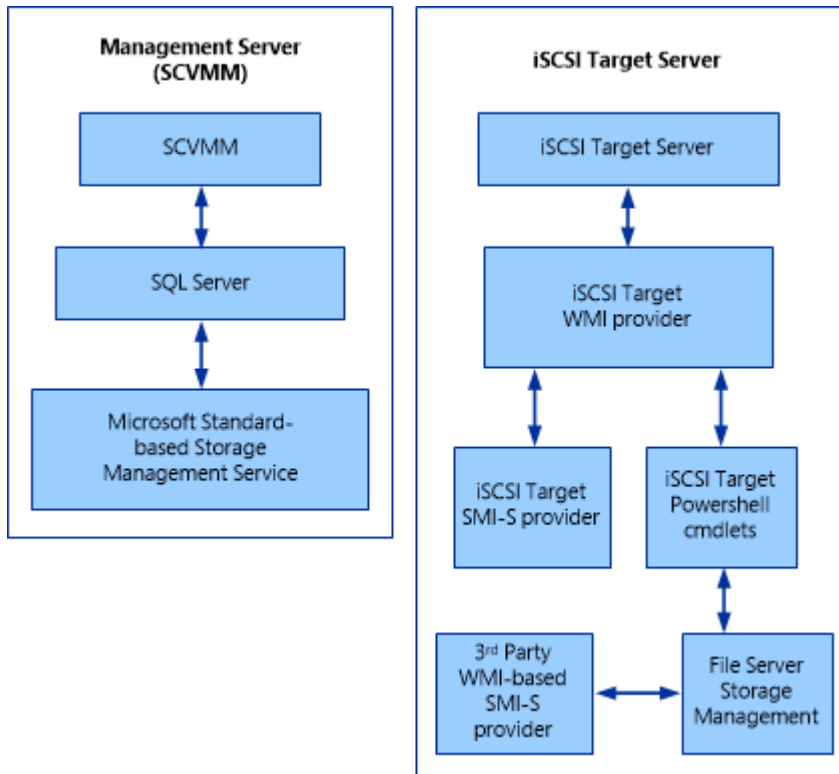
### Two providers intended for VMM management

As shown below, two SMI-S providers are installed on the same computer, and each is registered with the Storage Management service for VMM. Due to a known issue with the Storage Management service, only one of the providers will be discovered.



### Two providers intended for different storage management

Two WMI-based SMI-S providers are installed on the same computer. One SMI-S provider is intended for VMM management, and the other third-party SMI-S provider is intended for File Server Storage Management. Due to a known issue in the Storage Management service, both VMM and File Service Storage Management will only discover one provider, and it might not be the intended provider for the application.



## Provider details

As shown in the previous architecture diagrams, the SMI-S provider is WMI-based and passes information from the iSCSI Target service to the Storage Management service on the VMM server. After being registered with VMM, a full discovery request is sent to retrieve all the objects and their mappings from the SMI-S provider.

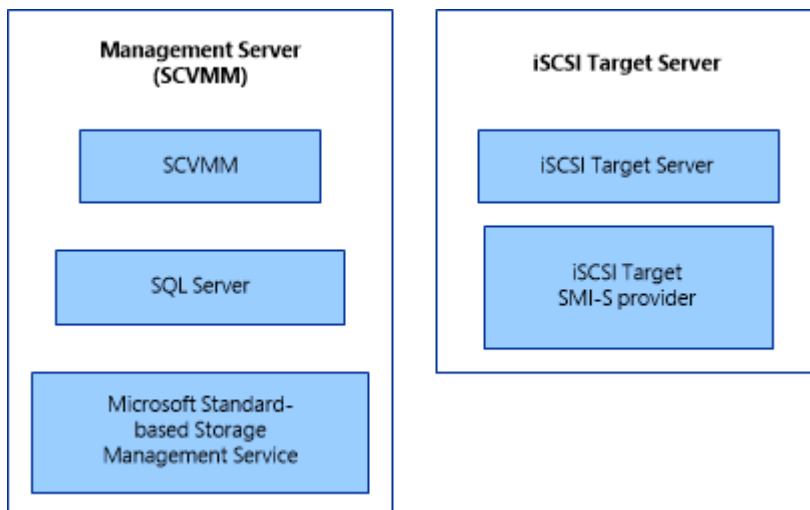
In a failover cluster for iSCSI Target Server, you will need to register the storage device using the network name or IP address for the iSCSI Target resource group (also referred as the client access point). In this way, the network name or IP address will be kept the same no matter which node is failed-over to, and VMM will be able to connect to the SMI-S provider that is running on the failed-over resource group node. After a failover event, you will need to perform a full discovery using VMM.

## Object mappings

1. MaskingSet maps to the iSCSI Target object—The friendly name of a MaskingSet by default uses the prefix string “SPC:” + 16-bit random. It is recommended to use a friendly name when creating the MaskingSet. VMM uses either the hostname or cluster name as the friendly name. The SMI-S provider will use the friendly name and this also becomes the “Description” property of the WT\_Host object for iSCSI Target Server.
2. StorageVolume maps to WT\_Disk (fixed Virtual Disk)—When a user creates an iSCSI disk using VMM, the SMI-S provider uses the friendly name as the VHD name. If the Virtual Disk already exists during SMI-S discovery, the provider uses its description as the friendly name. If the Virtual Disk already exists but does not have a description string (is empty or NULL), then the Virtual Disk friendly name uses the prefix string “VirtualDiskIndex:” + WTD (integer of the index).
3. ConcretePool maps to WT\_Volume—The friendly name displayed for the SMI-S provider is: “iSCSITarget: SubsystemName” + first mount point string. For example, if the mount point string is “C:”, then its name is “iSCSITarget: SubsystemName: C:”. There is a single PrimordialPool and its name is fixed as “MS iSCSITarget Primordial”

## SMI-S installation

The following example shows how to install the SMI-S provider:



The diagram above shows two computers; one for the management server running VMM, and one running iSCSI Target Server. The VMM server needs to be in a domain. The iSCSI Target server can be in a domain or a workgroup.

## Install VMM

VMM in System Center 2012 SP1 requires Microsoft SQL Server and Microsoft .NET Framework 3.5 - if you do not have these installed, VMM setup will prompt you to install them. For more information, see

[Upgrading to VMM in System Center 2012 SP1](#). The Microsoft Standard-based Storage Management service is enabled during VMM installation.

## Enable iSCSI target server and install updates

Enable and install iSCSI Target Server using the following steps:

1. Use the Windows PowerShell cmdlet `Add-WindowsFeature FS-IScsiTargetServer` to enable iSCSI Target Server. iSCSI Target Server is included in Windows Server 2012.
2. Install the update described in Microsoft KB article 27558246: [Update for Windows 8 \(KB2758246\)](#). Alternatively, this update is included in the rollup described in Microsoft KB article 2770917: [Windows 8 and Windows Server 2012 cumulative update: November 2012](#) installed. This update contains WMI-related changes to iSCSI Target Server that improve VMM discovery performance.
3. Install the SMI-S provider, using the iSCSI Target SMI-S Provider Setup wizard.

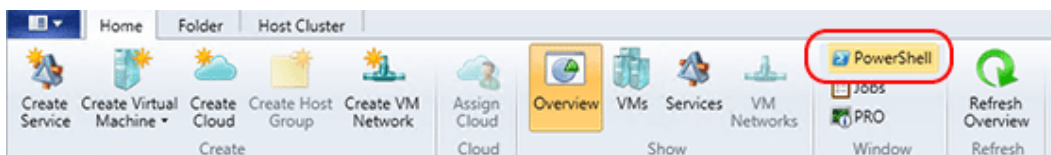


### Note

The SMI-S provider is included with System Center 2012 SP1 installation. You can find the setup file on the installation CD under the path: `\amd64\Setup\msi\iSCSITargetSMISProvider.msi`, or alternatively on the VMM server under `\Program Files\Microsoft System Center 2012\Virtual Machine Manager\setup\msi\iSCSITargetProv\iSCSITargetSMISProvider.msi`. Complete the wizard to install the SMI-S provider on the iSCSI Target Server computer.

## Configuration tasks

The goal is to use VMM to manage iSCSI Target Server. The SMI-S provider supports all management tasks through VMM. This section presents examples of using Windows PowerShell cmdlets for VMM. The following examples demonstrate how to use the Windows PowerShell cmdlets. To start, open the VMM PowerShell interface using the Windows PowerShell menu.



## Add a storage provider

Obtain the iSCSI Target Server local administrator credentials as follows:

```
$Cred = Get-Credential
```

Note that any account that is part of the Local Administrators group is sufficient.

Create a RunAs account in VMM as follows:

```
$Runas = New-SCRunAsAccount -Name "iSCSIRunas" -Credential $Cred
```

Add the storage provider as follows:

```
Add-SCStorageProvider -Name "Microsoft iSCSI Target Provider" -RunAsAccount  
$Runas -ComputerName "<computername>" -AddSmisWmiProvider
```

### **View storage properties**

Review the storage array attributes as follows:

```
$array = Get-SCStorageArray -Name "<computername>"
```

View available storage pools as follows:

```
$array.StoragePools
```

### **Add pools from iSCSI Target Server for VMM Management**

Get the specific storage pool to add as follows:

```
$pool = Get-SCStoragePool -Name "MS iSCSITarget Concrete: D:"
```

Create a storage classification (if none existed) as follows:

```
$class = New-SCStorageClassification -Name "gold"
```

Add the storage pool to VMM as follows:

```
Set-SCStorageArray -AddStoragePoolToManagement $pool -StorageArray  
$pool.StorageArray -StorageClassification $class
```

Allocate the storage pool to a host group as follows:

```
Set-SCStoragePool -StoragePool $pool -AddVMHostGroup (Get-SCVMHostGroup -Name  
"All Hosts")
```

### **Create a LUN**

Create an iSCSI logical unit number (LUN) as follows:

```
$LUN = New-SCStorageLogicalUnit -Name "iSCSI1" -StoragePool $pool -DiskSizeMB  
1000
```

Allocate the LUN to host group as follows:

```
Set-SCStorageLogicalUnit -StorageLogicalUnit $LUN -VMHostGroup (Get-  
SCVMHostGroup -Name "All Hosts")
```

Assign the LUN to the host group as follows:

```
$host = Get-SCVMHost -ComputerName <host name>
```

Add the host machine to the host group as follows:

```
Register-SCStorageLogicalUnit -StorageLogicalUnit $LUN -VMHost $host
```

## Clean-up tasks

Delete a LUN as follows:

```
Remove-SCStorageLogicalUnit -StorageLogicalUnit $LUN
```

Remove a storage provider as follows:

```
Remove-SCStorageProvider -StorageProvider (Get-SCStorageProvider -Name  
"Microsoft iSCSI Target Provider")
```

## Conclusion

This article demonstrated only a few of the tasks you can perform with VMM using the SMI-S provider. For information about additional Windows PowerShell cmdlets you can use to manage storage using the SMI-S provider, see [Cmdlet Reference for System Center 2012 - Virtual Machine Manager](#).

## 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 managed by Storage Management Initiative – Specification (SMI-S) or Store Management Provider (SMP) providers. You can assign 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 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 Overview](#).
- To add an SMI-S storage device, ensure 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 FQDN. For information about how to obtain SMI-S providers, see [Configuring Storage in VMM Overview](#).

**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 running the Add Storage Devices Wizard to discover storage, 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](#).

**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 **Add a storage device that is managed by an SMI-S provider** to specify and discover a storage device or array 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 array 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 **Use Secure Sockets Layer (SSL) connection** 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. If you are adding 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 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.
  - 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 tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure 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 (included in the system state), see [Windows Server Backup Step-by-Step Guide for Windows Server 2008 R2](#).

- 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 completes, 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 on creating 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. Make sure 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 Overview](#)

## 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 running the Add Storage Devices Wizard to discover storage, or during the wizard. The Run As account must have administrator permissions on the file server. VMM uses this account to perform administrative operations such as creating shares and modifying 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 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 Management console.
5. On the **Specify Discovery Scope** page, do the following:
  - a. In **Provider IP address or FQDN**, 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 that will use the file server storage are located, select **This computer is in an untrusted Active Directory domain**.
  - 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 will be displayed. When the process completes, click **Next**.
7. On the **Select Storage Devices** page, select the check box next to a file share you want VMM to manage.
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 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 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, so that Hyper-V can store virtual machine files, (including configuration, virtual hard disk (.vhd and .vhdx) files, and snapshots) on SMB file shares. Using Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1) you can assign SMB file shares to Hyper-V stand-alone hosts and host clusters. This topic describes the procedures required to deploy this configuration:

1. **Add a storage device**—As a first step add a storage device or Windows file server to the VMM console. As part of the Add operation, VMM discovers all the storage of shares 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 file server. For example, create a file share named `\\fileserver1\smbfileshare`. When you create the share, you do not need 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 host or cluster. VMM automatically modifies the share to assign the necessary permissions for the Hyper-V host or cluster to access the storage. For instructions, see [Assigning a file share](#). Note the following prerequisites for creating and assigning the share:
  - We recommend that you use a dedicated file server.

- The Windows file server should be in the same Active Directory domain as the virtual machine hosts.
- Files shares that will be 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 Hyper-V host. This also applies to a highly available file server. Do not add the file server (stand-alone or cluster) as a managed host in VMM.
- The VMM service account must have local administrative permissions 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 using the VMM Management console.

### To create a file share 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 will create 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 creating a host you must assign it to any host or cluster on which you want to create virtual machines that will 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 will access 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 checkmark 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 then 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 host cluster that you want to access the SMB 3.0 file share.

**See Also**

[Configuring Storage in VMM Overview](#)

[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** after you create each one.

For example, 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 Overview](#)

**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 SAN copy

technology. You can either create new logical units by using snapshot capability or by using cloning capability.



#### Note

The storage array must support the selected allocation method, and have that functionality enabled on the array. Also, realize that this may 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 either of the following options, and then click **OK**:
  - **Use snapshots** (the default)
  - **Clone logical units**

#### See Also

[Configuring Storage in VMM Overview](#)

#### 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 Hyper-V hosts 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, make sure that one or more storage pools are defined in VMM management. For more information, see [Configuring Storage in VMM Overview](#) 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 desired storage pool.
  - 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 Overview](#)

**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 System Center 2012 – Virtual Machine Manager (VMM) console. After you make the logical units

available to a host group, if Hyper-V hosts are configured to access the storage, you can assign the logical units to Hyper-V hosts 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 the topic [How to Add and Classify SMI-S and SMP Storage Devices in VMM](#).
- Unassigned logical units must exist in the storage pools that you want to allocate storage capacity from. For information on creating logical units using VMM, see [How to Provision Storage Logical Units in VMM](#). Alternately you can create logical units using your storage array vendor's management tools, or from a management Hyper-V host (if the host can access the storage array, and a storage pool has been allocated to the host group where the host 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 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 **Display as available only storage arrays that are visible to any host in the host group**.
7. For each logical unit 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 Hyper-V hosts 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 Overview](#)

## 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 Hyper-V hosts in the host group that can access the storage array where the storage pool resides.



### Note

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](#).

- Use the storage pool for the rapid provisioning of virtual machines. During rapid provisioning by using 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](#).



### Warning

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. This 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 **Display as available only storage arrays that are visible to any host in the host group**.
7. For each storage pool 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 Overview](#)

**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 you want to delete is not currently assigned to a Hyper-V host or assigned as storage to a virtual machine. For information about how to remove an assigned logical unit from a Hyper-V host or 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** To complete this procedure, you must be a member of the Administrator user role or a member of the Delegated Administrator user role.

### 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 will be 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 Overview](#)

### **Adding and Managing Hyper-V Hosts and Host Clusters in VMM**

This section shows how to do the following in System Center 2012 – Virtual Machine Manager (VMM):

- 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.



#### **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 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.

## Adding Hyper-V Hosts and Host Clusters to VMM

This section shows how to add Hyper-V hosts and Hyper-V host clusters to System Center 2012 – Virtual Machine Manager (VMM). This section also includes information about how to configure Hyper-V host properties, such as networking and storage settings.



### Note

The procedures in this section show how to add existing Hyper-V host clusters to VMM management. For information about how to create a Hyper-V host cluster from the VMM console, see [Creating and Modifying Hyper-V Host Clusters in VMM](#).

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 and Hyper-V host 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**

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.

**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 or host clusters.

Topic	Description
<a href="#">Adding Windows Servers as Hyper-V Hosts in VMM Overview</a>	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.
<a href="#">Adding Physical Computers as Hyper-V Hosts in VMM Overview</a>	Provides an overview, describes the Baseboard Management Controller (BMC) requirements, and links to the procedures for how to discover a physical computer and convert it to a

Topic	Description
	managed Hyper-V host.
<a href="#">Configuring Hyper-V Host Properties in VMM</a>	Describes the different host properties that you can configure in VMM. Includes detailed information about how to configure storage, networking and baseboard management 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 System Center 2012 – Virtual Machine Manager (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 [System Requirements: Hyper-V Hosts](#).




### 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	<b>HyperVHost01.contoso.com</b>
Windows Server in an untrusted Active Directory domain	<b>HyperVHost02.fabrikam.com</b>
Windows Server in a disjointed namespace	<b>HyperVHost03.contosocorp.com</b>
Windows Server in a perimeter network	<b>HyperVHost04</b>
Host groups	<ul style="list-style-type: none"><li>• <b>HyperVHost01.contoso.com</b> is added to the host group <b>Seattle\SEA_Tier0</b></li><li>• <b>HyperVHost02.fabrikam.com</b> is added to the host group <b>New York\NY_Tier2</b></li><li>• <b>HyperVHost03</b> is added to the host group <b>New York\NY_Tier1</b></li><li>• <b>HyperVHost04</b> is added to the host group <b>Seattle\SEA_Tier2</b></li></ul>
Run As accounts	<ul style="list-style-type: none"><li>• <b>Trusted Hyper-V Hosts</b></li></ul> <div> <b>Note</b> This Run As account is optional, as</div>

Resource	Resource Name
	<p>you can also specify a user name and password.</p> <ul style="list-style-type: none"> <li>• <b>Untrusted Hyper-V Hosts</b></li> </ul>

## In This Section

Follow these procedures to add Windows Server computers as managed Hyper-V hosts.

Procedure	Description
<a href="#">How to Add Trusted Hyper-V Hosts and Host Clusters in VMM</a>	Describes how to add Hyper-V hosts and host clusters that are in a trusted Active Directory domain.
<a href="#">How to Add Hyper-V Hosts in a Disjointed Namespace in VMM</a>	Describes how to add Hyper-V hosts and host clusters that are in a disjointed namespace.
<a href="#">How to Add Untrusted Hyper-V Hosts and Host Clusters in VMM</a>	Describes how to add Hyper-V hosts and host clusters that are in an untrusted Active Directory domain.
<a href="#">How to Add Hyper-V Hosts in a Perimeter Network in VMM</a>	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 computer or Windows Server failover cluster as one or more managed Hyper-V hosts in System Center 2012 – Virtual Machine Manager (VMM).

### Prerequisites

Before you begin this 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 Hyper-V host operating system requirements, see [System Requirements: Hyper-V Hosts](#).
- 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).

- 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 create it during the procedure.



### Important

If you configured the System Center Virtual Machine Manager 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 System Center Virtual Machine Manager 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 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**. On the next page of the wizard, all computers with names that begin with “HyperVHost” will be listed.

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 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, 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, 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 System Center 2012 – Virtual Machine Manager (VMM).

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 System Center 2012 – Virtual Machine Manager (VMM). 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 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 System Center 2012 – Virtual Machine Manager (VMM). 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 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 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 convert the computers into managed Hyper-V hosts. The physical computer can either be a computer that does not have an operating system installed (often referred to as a “bare-metal computer”), or a computer on which you want to overwrite an existing operating system installation.

**Operating system requirements**

The operating system image must use 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

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 converting physical computers to managed Hyper-V hosts.

**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 for the computer names that will be assigned to the hosts when they are deployed, 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. Create one or more host profiles in the library. A host profile includes configuration settings, such as the location of the operating system image, and hardware and operating system configuration settings.

6. Run the Add Resources Wizard to discover the physical computers, to configure settings such as the host group and the host profile to use, to configure custom deployment settings, and to start the operating system and Hyper-V 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 file) together with any specified driver files from the library, applies the drivers to the operating system image, enables the Hyper-V role, and then restarts the computer.

### 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 Profile 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	<b>HyperVHost05.contoso.com</b>  <b>HyperVHost06.contoso.com</b> (if you want to deploy two hosts that you will then cluster)
Target host group	<b>New York\Tier0_NY</b>   <b>Note</b> This host group structure is based on the example that is used in the <a href="#">Preparing the Fabric in VMM</a> section.
PXE server (provided through Windows Deployment Services)	<b>PXEServer01.constoso.com</b>
Run As accounts	<ul style="list-style-type: none"> <li>• <b>PXE Administrator</b></li> <li>• <b>Add Physical Host</b></li> <li>• <b>BMC Administrator</b></li> </ul>
Logical network	<b>BACKEND</b> (for use with a network site that defines a static IP pool)   <b>Note</b> You can also use DHCP.
Host profiles	<ul style="list-style-type: none"> <li>• <b>WS08R2Ent Hyper-V Hosts - Static</b></li> <li>• <b>WS08R2Ent Hyper-V Hosts - DHCP</b></li> </ul>

## In This Section

Follow the procedures listed here to discover physical computers and convert them to managed Hyper-V hosts.

Procedure	Description
<a href="#">Prepare the Physical Computers in VMM</a>	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.
<a href="#">How to Add a PXE Server to VMM</a>	Describes the PXE server requirements and how to add a PXE server to VMM management.
<a href="#">How to Add Driver Files to the VMM Library (optional)</a>	Describes how to add driver files to the library and how to add driver tags.
<a href="#">How to Create a Host Profile in VMM</a>	Describes how to create a host profile that contains hardware and operating system configuration settings.
<a href="#">How to Discover Physical Computers and Deploy as Hyper-V Hosts in VMM</a>	Describes how to use the Add Resources Wizard to discover the physical computers and deploy them as managed Hyper-V hosts.

## Prepare the Physical Computers in VMM

Before you can begin the host deployment process through Virtual Machine Manager (VMM), you must prepare the physical computers for discovery.

### Hyper-V Support

To support Hyper-V, 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 with a known IP address range.
- 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 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 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 Windows

Server 2008 R2 for either System Center 2012 or System Center 2012 SP1, or Windows Server 2012 for System Center 2012 SP1 only. 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 convert to managed Hyper-V hosts.
- 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:
  - 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 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 System Center 2012 – Virtual Machine Manager (VMM), and to assign tags to the drivers. By adding driver files to the library and configuring the host profile to add the driver files to the operating system during host deployment, VMM can install the drivers during the installation of the operating system on a physical host.

In the host 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 host 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 host 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 in VMM Overview](#)

[How to Create a Host Profile in VMM](#)

[How to Associate a VMM Library Server with a Host Group](#)

#### How to Create a Host Profile in VMM

You can use the following procedure to create a host profile in the library in Virtual Machine Manager (VMM). The host profile includes configuration settings such as the location of the operating system image to use during host deployment, together with hardware and operating system configuration settings.



#### Important

Make sure to determine whether the computers that you want to add uses Extensible Firmware Interface (EFI) or basic input/output system (BIOS). If you have computers of each type, you must create a separate host profile for each type.

#### Prerequisites

Before you begin this procedure, make sure that the following prerequisites are met:

- A generalized virtual hard disk with an appropriate operating system must exist in a library share.

With VMM in System Center 2012 Service Pack 1 (SP1), the format of the virtual hard disk file can be .vhd or .vhdx. With 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 (with System Center 2012 SP1)
Windows Server 2012	Windows Server 2012
Windows Server 2008 R2 with Service Pack 1	
Windows Server 2008 R2	

You must use an operating system edition that supports Hyper-V, and is supported by VMM. For more information, see [System Requirements: Hyper-V Hosts](#).

**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 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 to generalize the associated virtual hard disk. 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 Windows Server 2008 R2) or [Walkthrough: Deploy a Virtual Hard Disk for Native Boot](#) (for Windows Server 2012).

For more information about virtual hard disks with native boot, see [Understanding Virtual Hard Disks with Native Boot](#) (for Windows Server 2008 R2) or [Understanding Virtual Hard Disks with Native Boot](#) (for Windows Server 2012).

**Important**

We recommend that for production servers, you use a fixed disk .vhd or .vhdx to increase performance and to help protect user data. When you create the host profile, by default, VMM converts a dynamic disk to a fixed disk. If desired, you can change this setting when you create the host profile.

- If you plan to assign custom drivers, the driver files must exist in the library. If you want to select to filter the drivers by tags, the driver files must be appropriately tagged. For more information, see [How to Add Driver Files to the VMM Library](#).
- If you are running VMM in System Center 2012 SP1, and you plan to use a physical network adapter with a logical switch, or you plan to use a virtual network adapter, prepare your networking configuration as follows:

For a physical network adapter	For a virtual network adapter
<p>If you want to use a physical network adapter with a logical switch, before you create the new host 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 in VMM, create the uplink port profile and the logical switch.</p> <p>For more information, see <a href="#">How to Create a Native Port Profile for Uplinks in System Center 2012 SP1</a> and <a href="#">How to Create a Logical Switch in System Center 2012 SP1</a>.</p>	<p>If you want to create a virtual network adapter, before you create the new host 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, on the VMM management server, install all necessary virtual switch extensions and extension providers, create a logical switch, and create at least one VM network. If you will use a port classification with the virtual network adapter, create the port classification before you create the new host profile.</p> <p>For more information, see <a href="#">Configuring Ports and Switches for VM Networks in System Center 2012 SP1</a> and <a href="#">How to Create a VM Network in System Center 2012 SP1</a>.</p>

- 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 is managed by VMM. The network site must be available to the host group or to a parent host group of where you want to assign the hosts. For more information, see [Configuring Logical Networking in VMM Overview](#).

In this example scenario, the **BACKEND** logical network is used.

- If you want to use an answer file to specify additional host settings that are common to all hosts that will use this host profile, create an Unattend.xml file with 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 host 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 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.)

- A Run As account must exist that can be used 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 privileges. The account should be used 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

1. Open the **Library** workspace.
2. On the **Home** tab, in the **Create** group, click **Create**, and then click **Host Profile**.

The New Host Profile Wizard opens.

3. On the **Profile Description** page, enter a name and description for the host profile.

For example, if you want to assign an IP address through DHCP, enter 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 is needed.

- 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**:

<b>Management NIC</b>  (under <b>Network Adapters</b> )	<ul style="list-style-type: none"><li>• <b>For VMM in System Center 2012:</b> For the network adapter that will be used 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 for the <b>WS08R2Ent Hyper-V Hosts – DHCP</b> profile, click <b>Obtain an IP address through the DHCP service</b>.</li><li>• <b>For VMM in System Center 2012 SP1:</b> For the network adapter that will be used to communicate with the VMM management server, choose between configuring a physical network adapter and creating a virtual network adapter (which has certain requirements—see 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</li></ul>
---	---

	<p><b>Physical Properties.</b> For more information about switches and ports, see <a href="#">Configuring Ports and Switches for VM Networks in System Center 2012 SP1</a>.</p> <p>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 <b>IP Configuration</b>. (If this is a physical network adapter that you have connected to a logical switch, the <b>IP Configuration</b> options will be disabled.)</p> <p>For example, if you are configuring a host profile for the <b>WS08R2Ent Hyper-V Hosts – DHCP</b> profile that is intended for use with physical adapters that use a CDN of “Blue,” first select the physical adapter option and then click <b>Physical Properties</b> to specify the CDN. Next, click <b>IP Configuration</b> and then click <b>Obtain an IP address through the DHCP service</b>.</p> <p>You can also click the <b>Add</b> button and add a physical network adapter or virtual network adapter, or remove an adapter by selecting it and clicking the <b>Remove</b> button.</p>
<p><b>Disk</b>  (under <b>Disk and Partitions</b>)</p>	<p>Specify the partitioning scheme for the first disk. You can select either of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Master Boot Record (MBR)</b></li> </ul>

	<ul style="list-style-type: none"> <li>• <b>GUID Partition Table (GPT)</b></li> </ul> <p> <b>Note</b> If the host profile is for computers that use Extensible Firmware Interface (EFI), select <b>GUID Partition Table (GPT)</b> as the partitioning scheme.</p> <p>Under <b>Disk</b>, click the default partition name <b>OS</b>. In the <b>Partition information</b> pane, configure the following options:</p> <ul style="list-style-type: none"> <li>• The volume label.</li> <li>• Select whether to use all remaining free disk space, or to use a specific size (in gigabytes).</li> <li>• Select whether to designate the partition as the boot partition. By default, the <b>Make this the boot partition</b> check box is selected for the operating system partition.</li> </ul> <p> <b>Note</b> 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.</p> <p>To add a new disk or partition, with System Center 2012, click either <b>Add Disk</b> or <b>Add Partition</b> on the toolbar; with System Center 2012 SP1, click <b>Add</b> and then select <b>Disk</b> or <b>Partition</b>. The new disk or partition appears under the <b>Disk and Partitions</b> section. Configure the settings for the new disk or partition.</p>
<p><b>Driver filter</b> (under <b>Driver Options</b>)</p>	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>Filter drivers with matching PnP IDs.</b> By default, drivers that match the</li> </ul>

## See Also

[Adding Physical Computers as Hyper-V Hosts in VMM Overview](#)

[Configuring Networking in VMM Overview](#)

## 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
3. Bring the computer under VMM management as a managed Hyper-V host

### 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 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 Profile 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), 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, 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 host profile that contains these predefined network settings. Only the host 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** host 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** host profile, and then click **Next**.

10. If you are running VMM in System Center 2012 SP1, 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), 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 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, 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 host profile that uses DHCP or a host profile that uses static IP addresses.

If in step 9b you selected a host profile that uses DHCP, do the following:



#### **Note**

Until you type a computer name for each computer, a **Missing settings** warning appears.

- a. Click a BMC IP address in the list.
- b. 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**.

- c. 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, and you skip Active Directory verification, the deployment process will fail to join the computer to the domain.

- d. 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**.

- e. When you complete this step, and there are no more **Missing settings** warnings, click **Next**.
- f. Review the warning message, and then click **OK** to continue.

If in step 9b you selected a host profile that uses static IP addresses, do the following for each BMC IP address in the list:

 **Note**

Until you complete all required settings for a computer, a **Missing settings** warning or **Invalid MAC address** error appears.

- a. 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**.

- b. 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, and you skip Active Directory verification, the deployment process will fail to join the computer to the domain.

- c. 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.

- d. 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. The list of available logical networks matches what is available to the host group that you selected in step 9.
- e. 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.

- f. 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.

- g. When you complete this step, and there are no more warnings or error messages, click **Next**.
- h. 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:
- Open the **Fabric** workspace.
  - In the **Fabric** pane, expand **Servers**, expand **All Hosts**, and then expand the host group that you specified in step 9a.
  - 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 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 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
<b>General</b>	<ul style="list-style-type: none"><li>• 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.</li><li>• Enter a host description.</li><li>• Configure whether the host is available for placement.</li><li>• Configure the remote connection port. By default, the port is set to 2179.</li></ul>
<b>Hardware</b>	<p>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.</p> <ul style="list-style-type: none"><li>• For more information about how to configure network settings, see <a href="#">How to Configure Network Settings on a Hyper-V Host in VMM</a>.</li><li>• For more information about how to</li></ul>

Tab	Settings
	<p>configure BMC settings, see <a href="#">How to Configure Host BMC Settings in VMM</a>.</p>
<b>Status</b>	<p>Lists health status information for the host. Includes areas such as overall health, Hyper-V role health and VMM agent health. In the <b>Status</b> pane, you can also do the following:</p> <ul style="list-style-type: none"> <li>• View error details.</li> <li>• Refresh the health status.</li> <li>• Click <b>Repair all</b>. VMM will try to automatically fix any errors.</li> </ul>
<b>Virtual Machines</b>	<p>Shows the virtual machines that reside on the host, together with status information. Also enables you to register virtual machines on the host.</p>
<b>Reserves</b>	<p>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.</p>
<b>Storage</b>	<p>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 <a href="#">How to Configure Storage on a Hyper-V Host in VMM</a>.</p> <p> <b>Note</b> For information about how to configure storage for a Hyper-V host cluster, see <a href="#">How to Configure Storage on a Hyper-V Host Cluster in VMM</a>.</p>
<b>Virtual Networks</b>	<p>Enables you to configure virtual networks. For</p>

Tab	Settings
	more information about how to configure network settings, see <a href="#">How to Configure Network Settings on a Hyper-V Host in VMM</a> .
<b>Placement</b>	Enables you to configure the default virtual machine paths that will be used during virtual machine placement on the host.
<b>Servicing Windows</b>	Enables you to select servicing windows.
<b>Custom Properties</b>	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
<a href="#">How to Configure Storage on a Hyper-V Host in VMM</a>	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.
<a href="#">How to Configure Network Settings on a Hyper-V Host in VMM</a>	Describes how to configure network settings on a Hyper-V host, and how to view compliance information for physical network adapters on the host.
<a href="#">How to Configure Host BMC Settings in VMM</a>	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 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 Overview](#) 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 Overview](#)

## How to Configure Network Settings on a Hyper-V Host in VMM

You can use the procedures in this topic to configure network settings on a Hyper-V host in Virtual Machine Manager (VMM), and to view compliance information for physical network adapters on the host.



### Note

Use these procedures if you are running System Center 2012, or if you are running System Center 2012 Service Pack 1 (SP1) and you prefer to specify each network adapter setting individually. If you are running System Center 2012 SP1 and you prefer to apply port profiles and logical switches (that you have already configured) to network adapters, do not use these procedures. Instead, use the procedures in [How to Configure Network Settings on a Host by Applying a Logical Switch in System Center 2012 SP1](#).

Perform the procedures in this topic in the following order:

1. [Associate logical networks with a physical network adapter on a Hyper-V host](#)
2. [Configure settings for external, internal, and private virtual networks](#)
3. [View compliance information for a physical network adapter](#) (Repeat this procedure as needed.)

## Prerequisites

Before you associate logical networks with a physical adapter on a host, make sure that the following prerequisites are met:

- 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 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 on them. If a virtual network is not associated with the network adapter, when VMM connects a virtual machine to the physical network adapter, VMM automatically creates an external virtual network and associates it with the logical network. For more information about the default behavior, see [How to Configure Global Network Settings in VMM](#).

### Associate logical networks with a physical network adapter on a Hyper-V host

To make a logical network available to a Hyper-V host in VMM, you must associate the logical network with a physical network adapter on the host. You perform this association on a per network adapter basis.

#### ▶ To associate logical networks with a physical network adapter on a Hyper-V host

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 **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 the **Available for placement** check box is selected. If you want to use this network adapter for communication between the host and the VMM management server, ensure that the **Used by management** check box is selected.



#### Important

Make sure that you have at least one network adapter that is available for communication between the host and the VMM management server, and that **Used**

**by management** is selected for this network adapter.

7. If you are running System Center 2012, in the pane on the right, view **Logical network connectivity**, and if you are running System Center 2012 SP1, under the physical network adapter, click **Logical network connectivity**. Select the check box next to each logical network that you want to associate with the physical adapter. With System Center 2012 SP1, you can also view and modify the IP subnets and VLANs that are available for a given logical network on the network adapter. (For IP subnet and VLAN configuration with System Center 2012, see the next step.)



#### 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. If you are running System Center 2012 Service Pack 1 (SP1), ignore this step. If you are running System Center 2012, to configure advanced settings, click **Advanced**. In the **Advanced Network Adapter Properties** dialog box, you can configure the following:

- The mode of the physical switch port that the network adapter is connected to. You can select either **Trunk mode** or **Access mode**.

**Trunk mode.** Trunk mode enables multiple VLAN IDs to share the connection between the physical network adapter and the physical network. To give virtual machines external access through the same virtual network in multiple VLANs, you must configure both the port on the physical switch that the physical network adapter on the host is connected to, and the port of the virtual switch to use trunk mode. You must also provide the specific VLANs that will be used, and all of the VLAN IDs that are used by the virtual machines that the virtual network supports.

**Access mode.** In access mode, the external port of the virtual network is restricted to a single VLAN ID. Use access mode when the physical network adapter is connected to a port on the physical network switch that is also in access mode. To give a virtual machine external access on the virtual network that is in access mode, you must configure the virtual machine to use the same VLAN ID that is configured in the access mode of the virtual network.

- 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.

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. When you are finished, click **OK**.



#### 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 [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 define 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 is called a virtual switch.

Before applying the **External** setting, you must associate logical networks that you have configured in VMM with a physical network adapter, as described in the previous procedure.

#### ▶ To configure settings for external, internal, and private virtual networks

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, perform the following steps:
  - **For 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.

- **For System Center 2012 SP1:** 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 System Center 2012 SP1](#).

6. In the **Name** box, enter a name, or accept the default.
7. In the **Network binding** list, click the network type. You can configure the following types:
  - **External**

Use this type when you want to allow virtual machines to communicate with each other and with externally located servers, and optionally with the host operating system. The **External** type is bound to a physical network adapter. This type can be used to allow virtual machines to access a perimeter network and not expose the host operating system.
  - **Internal**

Use this type when you want to allow communication between virtual machines on the same host and between the virtual machines and the host. The **Internal** type is not bound to a physical network adapter. It is typically used to build a test environment where you want to connect to the virtual machines from the host operating system, but do not want to allow virtual machines on the host to communicate with external networks.
  - **Private**

Use this type when you want to allow communication between virtual machines on the same host but not with the host or with external networks. The **Private** type does not have a virtual network adapter in the host operating system, nor is it bound to a physical network adapter. The **Private** type is typically used when you want to isolate virtual machines from network traffic in the host operating system and in the external networks.
8. 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 network (which in System Center 2012 SP1 is called an external virtual switch).
  - b. Review the **Logical network** field, which indicates the logical networks that are associated with the network adapter. To associate logical networks with the physical network adapter, see [Associate logical networks with a physical network adapter on a Hyper-V](#)

[host](#), earlier in this topic.

- c. If you are running System Center 2012 SP1, skip this step. Otherwise, to enable the host to use the virtual network to communicate with virtual machines and also with the external network, select the **Host access** check box.



**Warning**

If you clear this 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, select the **Access host through a VLAN** check box (if available), and then select a VLAN number. The list of available VLANs is scoped to the VLANs that are configured as part of 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 the physical computer for 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.

If certain network optimization capabilities are available on a host that is running Windows Server 2008 R2 or Windows Server 2012, VMM automatically detects the capabilities and displays a message. These capabilities are Virtual Machine Queue (VMQ) and TCP Chimney Offload. After VMM has detected that either of these capabilities are available, in the **Host Properties** dialog box, the **Virtual Networks** tab (in System Center 2012) or the **Virtual Switches** tab (in System Center 2012 SP1) will display a message saying **Network optimization is available** on the virtual network or virtual switch. For information about these network optimization capabilities, see [Using TCP Chimney Offload](#) and [Using Virtual Machine Queue](#). For information about these network optimization capabilities in the context of VMM, see the “Network Optimization Support” section in [Configuring Virtual Networks in VMM](#) (which describes the capabilities in an earlier version of VMM).

### **View compliance information for a physical network adapter**

Compliance information indicates whether the settings on the host are consistent with the configuration in VMM. For example, compliance information indicates whether all IP subnets and VLANs that are included in a network site in a logical network are assigned to a network adapter.

## ► 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 **Network Compliance** column, view the compliance status.
  - A value of **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 IP subnets and VLANs that are included in the network site and those that are 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 in the **Compliance errors** section.

- A value of **Non compliant** indicates that none of the IP subnets and VLANs that are defined for the logical network are assigned to the physical 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 Networking in VMM Overview](#)

[Configuring Hyper-V Host Properties in VMM](#)

[How to Configure Network Settings on a Host by Applying a Logical Switch in System Center 2012 SP1](#)

## 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.



#### Note

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**.

## How to Configure Network Settings on a Host by Applying a Logical Switch in System Center 2012 SP1

You can use the procedures in this topic to configure a network adapter on a Hyper-V host in System Center 2012 Service Pack 1 (SP1) by associating logical networks with the adapter and applying a logical

switch and port profiles to the adapter. This topic also includes a procedure for viewing compliance information for network adapters on the host.

In Virtual Machine Manager (VMM) in System Center 2012 SP1, you can bring together the network settings that you configured in port profiles and logical switches by applying them to network adapters on a host. The network 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 is the same concept as the Hyper-V Virtual Switch, described in [Hyper-V Virtual Switch Overview](#).

**Note**

Use these procedures if you are running System Center 2012 SP1 and you prefer to apply port profiles and logical switches (that you have already configured) to network adapters. If you prefer to specify each network adapter setting individually, or you are running System Center 2012, do not use these procedures. Instead, use the procedures in [How to Configure Network Settings on a Hyper-V Host in VMM](#).

Perform the procedures in this topic in the following 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](#)
3. [View compliance information for a network adapter](#) (Repeat this procedure as needed.)

**Prerequisites**

Before you can perform this procedure, you must first configure multiple networking elements, including logical networks, port profiles, and logical switches. For more information, see [Configuring Ports and Switches for VM Networks in System Center 2012 SP1](#). It is especially important to review prerequisites if you want to configure single-root I/O virtualization (SR-IOV) for network adapters on the host.

Also, before you can perform this procedure, you must add the host or hosts to VMM. For more information, see [Adding Hyper-V Hosts and Host Clusters to VMM](#) and [Managing VMware ESX and Citrix XenServer 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 on them. If a virtual network is not associated with the network adapter, when VMM connects a virtual machine to the physical network adapter, VMM automatically creates an external virtual

network and associates it with the logical network. For more information about the default behavior, see [How to Configure Global Network 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.

#### **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 the **Available for placement** check box is selected. If you want to use this network adapter for communication between the host and the VMM management server, ensure that the **Used by management** check box is selected.



#### **Important**

- Make sure that you have at least one network adapter that is available for communication between the host and the VMM management server, and that **Used by management** is selected 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**

In Virtual Machine Manager (VMM) in System Center 2012 SP1, you can bring together network settings that you configured in port profiles and logical switches, by applying them to network adapters on a host.



### Note

Use this procedure if you are running System Center 2012 SP1 and you prefer to apply port profiles and logical switches (that you have already configured) to network adapters. If you prefer to specify each network adapter setting individually, or you are running System Center 2012, do not use this procedure. Instead, use the procedures in [How to Configure Network Settings on a Hyper-V Host in VMM](#).

### ► 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 creating 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.

If certain network optimization capabilities are available on a host that is running Windows Server 2008 R2 or Windows Server 2012, VMM automatically detects the capabilities and displays a message. These capabilities are Virtual Machine Queue (VMQ) and TCP Chimney Offload. After VMM has detected that either or both of these capabilities are available, in the **Host Properties** dialog box, the **Virtual switches** tab will display the message **Network optimization is available on this virtual switch**. For information about these network optimization capabilities, see [Using TCP Chimney Offload](#) and [Using Virtual Machine Queue](#). For information about these network optimization capabilities in the context of VMM, see the “Network Optimization Support” section in [Configuring Virtual Networks in VMM](#) (which describes the capabilities in an earlier version of VMM).

## **View compliance information for a network adapter**

Compliance information indicates whether the settings on the host are consistent with the configuration in VMM. For example, compliance information indicates whether all IP subnets and VLANs that are included in a network site in a logical network are assigned to a network adapter.

### **To view compliance information for a 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 network adapter.
5. In the **Network Compliance** column, view the compliance status.
  - A value of **Fully compliant** indicates that the settings on the 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 details 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.



#### Tip

In addition to the compliance information, you can also view detailed information about the network adapter, such as the assigned IP address and MAC address, and the associated virtual networks.

#### See Also

[Configuring Ports and Switches for VM Networks in System Center 2012 SP1](#)

**Configuring Ports and Switches in VMM in System Center 2012 SP1 Illustrated Overview**

[Configuring Networking in VMM Overview](#)

[Adding Hyper-V Hosts and Host Clusters to VMM](#)

[How to Configure Network Settings on a Hyper-V Host in VMM](#)

#### Creating and Modifying Hyper-V Host Clusters in VMM

This section explains how to create, add or remove nodes, and uncluster Hyper-V host clusters in Virtual Machine Manager (VMM). Managing clustered Hyper-V hosts through VMM enables you to support highly available virtual machines, and features such as Dynamic Optimization and Power Optimization.

In System Center 2012 and System Center 2012 SP1, 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 enables you 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 of VMM, and then bring it under VMM management. Be aware that this 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.

### In This Section

Use the information in the following topics to create or modify a Hyper-V host cluster through VMM.

Topic	Description
<a href="#">Creating a Hyper-V Host Cluster in VMM Overview</a>	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.
<a href="#">Modifying a Hyper-V Host Cluster in VMM</a>	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.
<a href="#">Configuring Hyper-V Host Cluster Properties in VMM</a>	Describes Hyper-V host cluster properties and 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 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	<b>HyperVHost05 and HyperVHost06</b>
Domain	<b>contoso.com</b>
Cluster name	<b>HyperVClus01.contoso.com</b>
Host group where added	<b>New York\Tier0_NY</b>
Logical network	<b>BACKEND</b>

### 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
<a href="#">Creating a Hyper-V Host Cluster in VMM Prerequisites</a>	Describes the host and fabric prerequisites that are required to complete the procedure.
<a href="#">How to Create a Hyper-V Host Cluster in VMM</a>	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 an appropriate operating system:
  - **For System Center 2012:** Windows Server 2008 R2 Enterprise Edition, Service Pack 1 or earlier, or Windows Server 2008 R2 Datacenter Edition, Service Pack 1 or earlier
  - **For System Center 2012 Service Pack 1 (SP1):** Windows Server 2008 R2 Enterprise Edition, Windows Server 2008 R2 Datacenter Edition, or Windows Server 2012 (any edition)

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 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 Overview](#) 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.

<b>Classification</b>	The storage classification value is pre-assigned in the VMM console, and is non-
-----------------------	--

	editable in the wizard.
<b>Partition Style</b>	Click <b>MBR</b> or <b>GPT</b> .   <b>Note</b> This setting is ignored if the disk is already initialized.
<b>File System</b>	Click <b>NTFS</b> or <b>Do not format</b> . By default, the file system is NTFS.
<b>Volume Label</b>	Enter a volume label.
<b>Quick Format</b>	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.
<b>CSV</b>	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
<a href="#">How to Add a Node to a Hyper-V Host Cluster in VMM</a>	Describes how to add a node to an existing Hyper-V host cluster through the VMM console.
<a href="#">How to Remove a Node from a Hyper-V Host Cluster in VMM</a>	Describes how to remove a node from an existing Hyper-V host cluster through the VMM console.
<a href="#">How to Uncluster a Hyper-V Host Cluster in VMM</a>	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 an appropriate operating system:
  - **For System Center 2012:** Windows Server 2008 R2 Enterprise Edition, Service Pack 1 or earlier, or Windows Server 2008 R2 Datacenter Edition, Service Pack 1 or earlier.
  - **For System Center 2012 Service Pack 1 (SP1):** Windows Server 2008 R2 Enterprise Edition, Windows Server 2008 R2 Datacenter Edition, or Windows Server 2012 (any edition).

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	<p>View the name, host group and description for the cluster. You can also configure the <b>Cluster reserve (nodes)</b> setting, and view the cluster reserve state and any cluster reserve details.</p> <p>The <b>Cluster reserve (nodes)</b> 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.</p>
Status	<p>View detailed status information for the host cluster. You can view the following information:</p> <ul style="list-style-type: none"><li>• 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.</li></ul> <div> <b>Note</b> To access the report, you must have administrative permissions on the cluster node where the report is located.</div> <div> <b>Tip</b></div>

Tab	Settings
	<p>You can perform an on-demand cluster validation through VMM. To do this, in the <b>Fabric</b> workspace, locate and click the host cluster. Then, on the <b>Host Cluster</b> tab, click <b>Validate Cluster</b>. Cluster validation begins immediately.</p> <ul style="list-style-type: none"> <li>• Whether cluster core resources are online.</li> <li>• Whether the disk witness in quorum is online.</li> <li>• Whether the cluster service on each node is online.</li> </ul>
<b>Available Storage</b>	<p>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).</p> <p>You can also do the following:</p> <ul style="list-style-type: none"> <li>• Add and remove storage logical units that are managed by VMM.</li> <li>• Convert available storage to shared storage (CSV).</li> </ul> <p>For information about how to configure storage for a Hyper-V host cluster, see <a href="#">How to Configure Storage on a Hyper-V Host Cluster in VMM</a>.</p>
<b>Shared Volumes</b>	<p>Shows the shared volumes (CSVs) that are allocated to the host cluster. You can also do the following:</p> <ul style="list-style-type: none"> <li>• Add and remove CSVs that are managed by VMM.</li> </ul>

Tab	Settings
	<ul style="list-style-type: none"> <li>• Convert CSVs to available (non-CSV) storage.</li> </ul> <p>For information about how to configure storage for a Hyper-V host cluster, see <a href="#">How to Configure Storage on a Hyper-V Host Cluster in VMM</a>.</p>
Virtual Networks	<p>Shows the external virtual networks that are common across all cluster nodes.</p> <p>From the Virtual Networks tab, you can also create and edit external virtual networks that are common across all nodes.</p> <p>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 <b>Create</b>, select a logical network, enter a name for the virtual network, configure whether to enable host access, and then click <b>Create</b>. Click <b>OK</b> to commit the changes.</p> <p> <b>Note</b> 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 <a href="#">How to Configure Network Settings on a Hyper-V Host in VMM</a>.</p>

Tab	Settings
<b>Custom Properties</b>	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
<a href="#">How to Configure Storage on a Hyper-V Host Cluster in VMM</a>	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 Overview](#) 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 Overview](#)

[How to Configure Storage on a Hyper-V Host in VMM](#)

## 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
<a href="#">How to Configure Dynamic Optimization and Power Optimization</a>	Describes how to configure Dynamic Optimization and Power Optimization for a host group.
<a href="#">How to Run Dynamic Optimization on a Host Cluster</a>	Describes how to initiate Dynamic Optimization on demand within a host cluster by using the <b>Optimize Hosts</b> action in the <b>Fabric</b> 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. However, you still need root credentials to enable file transfers between ESX hosts and VMM. Also, know that 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 [System Requirements: VMware ESX Hosts](#).



## 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	<p>You can deploy VMM services to ESX hosts.</p> <p> <b>Note</b> VMM services use a different model than VMware vApp. Therefore, the two methods can coexist. However, you cannot use VMM to deploy vApps.</p>
Private clouds	<p>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.</p> <p> <b>Note</b> VMM does not integrate with VMware vCloud.</p>
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

Feature	Notes
	<p>management.</p> <p> <b>Note</b> For power optimization, you can use the Dynamic Optimization feature in VMM or the VMware Dynamic Resource Scheduler.</p>
Migration	<p>Supported VMware transfer types include the following:</p> <ul style="list-style-type: none"> <li>• Live Migration between hosts within cluster (uses vMotion)</li> <li>• Live Storage Migration (uses Storage vMotion)</li> </ul> <p>Supported VMM transfer types include the following:</p> <ul style="list-style-type: none"> <li>• Network migration to and from the library</li> </ul> <p> <b>Note</b> VMware thin provision disks become thick when a disk is migrated to the VMM library.</p> <ul style="list-style-type: none"> <li>• Network migration between hosts</li> </ul>
Maintenance mode	<p>You can place an ESX host that is managed by VMM in and out of maintenance mode by using the VMM console.</p>
Library	<p>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.</p>

Feature	Notes
	<p> <b>Important</b></p> <p>If you want to use VMDK files that were 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:</p> <ul style="list-style-type: none"> <li>• Regular VMDK files: VMFS and monolithicFlat</li> <li>• VMDK files that are used to access physical disks: vmfsPassthroughRawDeviceMap</li> <li>• Snapshots: vmfssparse</li> </ul> <p>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.</p>
Templates	<p>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.</p> <p>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.</p>
Networking	<p>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</p>

Feature	Notes
	<p>recognizes and uses existing configured vSwitches and port groups for virtual machine deployment.</p> <p>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.</p> <p> <b>Important</b> 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.</p>
Storage	<p>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.”</p> <p> <b>Note</b> VMM does not support VMware virtual machines with virtual hard disks that are connected to an integrated drive electronics (IDE) bus.</p> <p>VMM supports VMware thin provision virtual hard disks through the dynamic disk type. Note the following behavior:</p> <ul style="list-style-type: none"> <li>• If you create and deploy a virtual machine</li> </ul>

Feature	Notes
	<p>to an ESX host that is configured to use a dynamic disk, the disk is created as a thin provisioned disk.</p> <ul style="list-style-type: none"> <li>• If a virtual machine uses a thin provisioned disk that was created out of band, VMM displays the disk as a dynamic disk.</li> <li>• 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.</li> </ul> <p>VMM supports the hot add and hot removal of virtual hard disks on VMware virtual machines.</p> <p> <b>Note</b> The new VMM storage automation features are not supported for ESX hosts. All storage must be added to ESX hosts outside VMM.</p>
Conversion	<p>Converting a VMware-based virtual machine to a Hyper-V based virtual machine is supported by using the virtual to virtual (V2V) process.</p> <p> <b>Note</b> 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.</p>
Performance and Resource Optimization (PRO)	Monitoring and alerting for ESX hosts is possible through VMM with the integration of

Feature	Notes
	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
<a href="#">How to Add a VMware vCenter Server to VMM</a>	Describes how to add a VMware vCenter server to VMM management.
<a href="#">How to Add VMware ESX Hosts to VMM</a>	Describes how to add ESX and ESXi hosts to VMM management.
<a href="#">How to Configure Network Settings on a VMware ESX Host</a>	Describes how to configure ESX host network settings to support the new logical network feature in VMM.
<a href="#">How to Configure Host BMC Settings in VMM</a>	Describes how to configure Baseboard Management Controller (BMC) settings on a host to support power management through

Procedure	Description
	VMM.
<a href="#">How to Import VMware Templates</a>	Describes how to import a VMware template to the VMM library.
<a href="#">How to Convert VMware Virtual Machines to Hyper-V</a>	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 [System Requirements: VMware ESX Hosts](#).
- 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 [System Requirements: VMware ESX Hosts](#).
- 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 must have root credentials on the ESX hosts that you want to add.

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 that has root 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 the Run As account that you specified does not have root credentials, or 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. In the **Credential** box, verify that the listed Run As account has root credentials on the host.
- d. To retrieve the certificate and public key for the host, click **Retrieve**.
- e. To view the thumbprint details, click **View Details**.
- f. To accept the certificate and public key, select the **Accept the certificate for this host** check box.
- g. When you are finished, click **OK**.
- h. 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.
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 Overview](#)

## 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.

**Note**

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**.

## How to Import VMware Templates

You can use the following procedure to import a VMware template into the System Center 2012 – Virtual Machine Manager (VMM) library.

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. Therefore, there is now a dependency on the VMware template on the 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](#).

Before you begin this procedure, make sure that the VMware vCenter Server where the template resides 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.



### 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.

VMM 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



### Note

In System Center 2012 SP1: Only the last two items are supported versions of VMware ESX in this scenario



### Important

Before you convert a VMware virtual machine to a Hyper-V virtual machine, you must uninstall VMware Tools on the guest operating system of the virtual machine.

## ▶ To convert a VMware virtual machine to a Hyper-V 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 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 the amount of memory to assign (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. If desired, 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 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 desired settings, 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 that 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

System Center 2012 – 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 in [System Requirements: Citrix XenServer Hosts](#).



### 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

Feature	Notes
	on host ratings during the creation, deployment, and migration of XenServer virtual machines. This includes concurrent virtual machine deployment during service deployment.
Services	You can deploy VMM services to XenServer hosts.
Private clouds	<p>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.</p> <p>For more information, see <a href="#">Creating a Private Cloud in VMM Overview</a>.</p>
Dynamic Optimization and Power Optimization	<p>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.</p>
Migration	<p>Supported migration types include the following:</p> <ul style="list-style-type: none"> <li>• Live Migration between hosts in a managed pool (through Citrix XenMotion)</li> <li>• LAN migration between a host and the library through BITS</li> </ul> <p> <b>Note</b> TransferVM is used for each virtual</p>

Feature	Notes
	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	<p>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.</p> <p> <b>Tip</b> If you store virtual hard disks for XenServer in the VMM library, we recommend that you open the properties of the .vhd or .vhdx file, and then on the <b>General</b> tab, in the <b>Virtualization platform</b> list, click <b>Citrix XENServer Server</b>. This will help you distinguish which files are for XenServer.</p>
XenServer Templates	<p>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.</p> <p> <b>Note</b> 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.</p>
VMM Templates	VMM virtual machine templates are supported with XenServer, with the following restrictions:

Feature	Notes
	<ul style="list-style-type: none"> <li>• The generalization and customization of virtual machines is supported for Windows-based virtual machines only.</li> <li>• You must manually install XenServer Tools (Citrix Tools for Virtual Machines).</li> <li>• 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.</li> </ul>
Networking	<p>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.</p> <p>Be aware that you must create external virtual networks through XenCenter. VMM recognizes and uses the existing external networks for virtual machine deployment.</p> <p> <b>Note</b> VMM uses a single virtual switch to represent all XenServer switches with different VLAN IDs that are bound to a single physical network adapter.</p>
Storage	<p>VMM supports all virtual disk storage repositories that XenServer does. These include the following:</p> <ul style="list-style-type: none"> <li>• Software iSCSI, Network File System (NFS) virtual hard disk, Hardware host bus adapters (HBAs), and Advanced</li> </ul>

Feature	Notes
	<p>StorageLink technology</p> <ul style="list-style-type: none"> <li>• Shared and local storage</li> </ul> <p>In addition, VMM supports ISO repositories on an NFS or a Windows File Sharing (Common Internet File System (CIFS)) share. Note the following:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul> <p> <b>Note</b> The new VMM storage automation features are not supported for XenServer hosts. All storage must be added to XenServer hosts outside VMM.</p>
Virtual machine management	<p>VMM supports paravirtual (PV) and hardware-assisted virtualization (HVM) virtual machines, with the following restrictions:</p> <ul style="list-style-type: none"> <li>• Windows-based operating systems will only run on HVM virtual machines.</li> <li>• If you create a new virtual machine through the VMM console, you can only create HVM virtual machines.</li> <li>• 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</li> </ul>

Feature	Notes
	<p>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.</p> <p>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.</p>
Conversion	<p>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.</p> <p> <b>Note</b> To start the P2V process, in the <b>VMs and Services</b> workspace, on the <b>Home</b> tab, in the <b>Create</b> group, click the <b>Create Virtual Machine</b> drop-down arrow, and then click <b>Convert Physical Machine</b>.</p>
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
<a href="#">How to Add XenServer Hosts to VMM</a>	Describes how to add a XenServer host or pool to VMM management.
<a href="#">Configuring XenServer Host Properties</a>	<p>Describes the settings that are available in the XenServer host properties. Includes the following subtopics:</p> <ul style="list-style-type: none"> <li>• <a href="#">How to Configure Network Settings on a Citrix XenServer Host</a> Describes how to configure XenServer host network settings, including how to configure logical network settings.</li> <li>• <a href="#">How to Configure Host BMC Settings in VMM</a> Describes how to configure Baseboard Management Controller (BMC) settings on a host to support power management through VMM.</li> </ul>

## 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 in [System Requirements: Citrix XenServer Hosts](#).
- 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> -skipcachecheck -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
<b>General</b>	<ul style="list-style-type: none"><li>• 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.</li><li>• Enter a host description.</li><li>• Configure whether the host is available for placement.</li><li>• View or change the remote connection port.</li></ul>
<b>Status</b>	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 <b>Status</b> pane, you can also do the following:

Tab	Settings
	<ul style="list-style-type: none"> <li>• View error details.</li> <li>• Refresh the health status.</li> </ul> <p> <b>Note</b> The <b>Repair all</b> option does not apply to XenServer hosts.</p>
<b>Management</b>	<p>Enables you to change the credentials that VMM uses to connect to the XenServer host, and to retrieve or view the host certificate.</p> <p> <b>Note</b> The account that you specify must have root credentials on the XenServer host.</p>
<b>Hardware</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• For more information about how to configure network settings, see <a href="#">How to Configure Network Settings on a Citrix XenServer Host</a>.</li> <li>• For more information about how to configure BMC settings, see <a href="#">How to Configure Host BMC Settings in VMM</a>.</li> </ul>
<b>Virtual Machine Paths</b>	<p>Shows the virtual machines that reside on the host, together with status information.</p> <p> <b>Note</b> The <b>Add</b> option to register virtual machines is not supported on a</p>

Tab	Settings
	XenServer host.
<b>Reserves</b>	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.
<b>Storage</b>	Shows storage that is allocated to the host.
<b>Virtual Networks</b>	Enables you to configure virtual networks. For more information about how to configure network settings, see <a href="#">How to Configure Network Settings on a Citrix XenServer Host</a> .
<b>Placement</b>	Enables you to view the virtual machine paths that will be used during virtual machine placement on the host.
<b>Servicing Windows</b>	Enables you to select servicing windows.
<b>Custom Properties</b>	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
<a href="#">How to Configure Network Settings on a Citrix XenServer Host</a>	Describes how to configure network settings on a XenServer host, and how to view compliance information for physical network adapters on the host.

Topic	Description
<a href="#">How to Configure Host BMC Settings in VMM</a>	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 Overview](#)

#### 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.



#### Note

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**.

## 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 [System Requirements: Update Management](#).

### 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
<a href="#">How to Install a WSUS Server for VMM</a>	Describes requirements for installing a dedicated WSUS server to use with VMM.
<a href="#">How to Add an Update Server to VMM</a>	Describes how to enable update management in VMM by adding a WSUS server to VMM.
<a href="#">How to Configure Update Baselines in VMM</a>	Describes how to edit a built-in update baseline and how to create new updates baselines for your VMM environment.
<a href="#">How to Scan for Update Compliance in VMM</a>	Describes how to scan managed computers for update compliance in <b>Compliance</b> view of the VMM console.
<a href="#">Performing Update Remediation in VMM</a>	Describes how to perform update remediations on stand-alone Hyper-V hosts that are managed by VMM and how to orchestrate updates on a Hyper-V host cluster in VMM.
<a href="#">How to Create and Remove Update Exemptions for Resources in VMM</a>	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.
<a href="#">How to Perform On-Demand WSUS Synchronizations in VMM</a>	Describes how to use the <b>Synchronize</b> action in the <b>Fabric</b> workspace to synchronize updates in VMM.
<a href="#">How to Update WSUS Settings in VMM</a>	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.
<a href="#">How to Integrate Fabric Updates with Configuration Manager</a>	Describes how to configure VMM to use a WSUS server that is part of a Microsoft System

Procedure	Description
	Center Configuration Manager environment.

## How to Install a WSUS Server for VMM

To manage updates in Virtual Machine Manager (VMM), you must either install 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](#).

VMM uses the WSUS Windows Update/Microsoft Update catalog, Windows Update Agent (WUA) integration in Windows Server, and WSUS for binary distribution to managed computers. VMM uses WSUS in a different manner than does Configuration Manager.

You can install the WSUS server on the VMM management server. However, we recommend installing the WSUS server on separate system, especially if the VMM management server is managing a large number of computers. If you install 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 WSUS 3.0 Class Library Reference.

This topic covers either a local or remote WSUS server without Secure Sockets Layer (SSL).

## Prerequisites for Installing WSUS

Before you install the WSUS server, ensure that the server meets all WSUS 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 server 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
<b>Microsoft Report View 2008</b>	This option is not needed if you install the WSUS server on your VMM management server.
<b>Choose Upstream Server</b>	<b>Synchronize with Microsoft Update</b>
<b>Choose Languages</b> <b>Choose Products</b> <b>Choose Classifications</b>	<p>To limit WSUS synchronization time, you can limit languages, products, and classifications.</p> <p><b>Products:</b> Limit products to the supported range for Hyper-V hosts, library servers, and the VMM management server in VMM.</p> <p><b>Classifications:</b> You can limit classifications</p>

	as desired, but consider keeping at least <b>Critical Updates</b> and <b>Security Updates</b> .
<b>Configure Sync Schedule</b>	<b>Synchronize manually</b>

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 System Center 2012 – Virtual Machine Manager (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. In **Computer name**, enter the fully qualified domain name (FQDN) of the WSUS server (for example, VMMServer01.contoso.com).
4. Specify which TCP/IP port that the WSUS website listens on for connections (for example, port 8530).
5. Enter credentials for connecting to the WSUS server. The account must have administrator rights on the WSUS server.
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 installed 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 should manage the WSUS server only through VMM, unless you are using a WSUS server in a Configuration Manager environment.

To verify that the WSUS server was added to VMM successfully:

1. In the **Fabric** workspace, on the **Fabric** pane, expand **Servers**, and click **Update Server**. The results pane should display the WSUS server.
2. In the **Library** workspace, on the **Library** pane, expand **Update Catalog and Baselines**, and then click **Update Catalog**. The results pane should display the updates that were downloaded during WSUS synchronization.

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, or a VMM management server. 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.

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.

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. To apply a baseline to all hosts, select the **All Hosts** root host group.

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 assign it to host groups, host clusters, or individual managed computers. 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 baselines.
6. Click **Assignment Scope** to open the **Assignment Scope** page and then, select host groups, host clusters, and computers to add to the baseline.

Computers are represented by the roles they perform in VMM. When you select a role, such as **VMM server**, all the 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, select the host groups or individual computers 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

- The WSUS server
- The 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.

## **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, each update has a compliance status of **Compliant**, **Non Compliant**, **Error**, or **Unknown**.

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
<a href="#">How to Remediate Updates on a Stand-Alone Hyper-V Host in VMM</a>	Describes how to install updates on noncompliant Hyper-V hosts.
<a href="#">How to Perform Rolling Updates on a Hyper-V Host Cluster in VMM</a>	Describes how to perform rolling orchestrate update remediation on a Hyper-V host cluster.

**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 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 and then return the resource to update compliance.

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 reinstalled 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**.

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 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**
- [Creating and Deploying Virtual Machines](#)
- [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](#)

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-premise by an organization. The private cloud is deployed using an organization's own hardware to leverage the advantages of the private cloud model. Through VMM, an organization can manage the private cloud definition, 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:

1. [How to Create a Private Cloud from Host Groups](#)
2. [How to Create a Private Cloud from a VMware Resource Pool](#)
3. [How to Increase the Capacity of a Private Cloud](#)
4. [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-premise by an organization. The private cloud is deployed using an organization's own hardware to leverage the advantages of the private cloud model. Through VMM, an organization can manage the private cloud definition, 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 retaining the opaque usage model. Self-service users do not need to ask the private cloud provider for administrative changes beyond increasing capacity and quotas as their needs 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
<b>Finance</b>  (Private cloud created from host groups)	Host groups: <b>Seattle\Tier0_SEA, Seattle\Tier1_SEA, New York\Tier0_NY, New York\Tier1_NY</b>  Logical network: <b>BACKEND</b>  Load balancer: <b>LoadBalancer01.contoso.com</b>  VIP profile: <b>Web tier (HTTPS traffic)</b>

Private Cloud	Resource
	Storage classification: <b>GOLD</b> and <b>SILVER</b>  Read-only library shares: <b>SEALibrary</b> and <b>NYLibrary</b>  Stored virtual machine path: <b>VMMServer01\Finance\StoredVMs</b>  Capability profile: <b>Hyper-V</b>
<b>Marketing</b>  (Private cloud created from a VMware resource pool)	VMware resource pool: <b>Resource pool 1</b>  Logical network: <b>BACKEND</b>  Load balancer: <b>LoadBalancer01.contoso.com</b>  VIP profile: <b>Web tier (HTTPS traffic)</b>  Read-only library shares: <b>SEALibrary</b> and <b>NYLibrary</b>  Stored virtual machine path: <b>VMMServer01\Marketing\StoredVMs</b>  Capability profile: <b>ESX Server</b>

### 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**.

## ▶ 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
------------	-------------

<b>Virtual CPUs</b>	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.
<b>Memory</b>	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.
<b>Storage</b>	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.
<b>Custom quota (points)</b>	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.
<b>Virtual machines</b>	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**.

## 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**.

### **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
<b>Virtual CPUs</b>	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.
<b>Memory</b>	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.
<b>Storage</b>	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.
<b>Custom quota (points)</b>	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.
<b>Virtual machines</b>	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**.

## 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. On the **Folder** tab, click **Delete**.
4. 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

In System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed. If you need a self-service portal solution in System Center 2012 SP1, we recommend that you use App Controller. For more information, see [App Controller](#).

Procedure	Description
<b>Configuring Self-Service in VMM Overview</b>	Provides an overview of self-service features in VMM.
<b>How to Create a Self-Service User Role in VMM 2012</b>	Describes how to create a self-service user role that can create and deploy virtual machines and services on a private cloud.
<b>How to Open a New Session While You Are Logged On to the VMM Console</b>	Describes how to open a new connection to the VMM console under a different user role.
<b>How to Enable Self-Service Users to Share Resources in VMM</b>	Describes how to enable resource sharing between self-service user roles.
<b>How to Share Resources as a Self-Service User in VMM</b>	Describes how to share resources as a self-service user in VMM.
<b>Configuring the Library to Support Self-Service Users</b>	Describes new methods that are available in VMM for sharing resources with self-service users
<b>How to Configure the Library to Support Self-Service Users</b>	Describes how to create read-only library shares and user role data paths
<b>How to Import and Export Physical Resources To and From the Library</b>	Describes how to import and export file-based resources between library servers and library shares.

**See Also**

[Creating User Roles in VMM](#)

**Creating and Deploying Virtual Machines**

The following topics provide information about creating and deploying virtual machines in Virtual Machine Manager (VMM):

- **Creating Virtual Machines Overview**
- **Understanding Virtual Machine Placement 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 Convert Physical Computers in VMM (P2V)**
- **How to Convert Virtual Machines in VMM (V2V)**
- **How to Deploy a Virtual Machine Stored in the VMM Library**

### **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 creating 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. Host profiles are not used for virtual machine creation. They are used during the conversion of a bare-metal computer to a Hyper-V host.

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**

### **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**

### **Rapid Provisioning of Virtual Machines Using SAN Copy Overview**

Rapid provisioning provides a method for deploying new virtual machines to storage arrays without the need for copying virtual machines over the network. System Center 2012 –

Virtual Machine Manager (VMM) allows you to take advantage of your Storage Area Network (SAN) infrastructure for cloning virtual machines, combined with a VMM template for customizing 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 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.

### **Rapid Provisioning by Using SAN Copy Methods**

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 the prerequisites are met. Links to more detailed procedures for each method are provided. The prerequisites are described in the “Rapid Provisioning by Using SAN Copy Prerequisites” section of 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 desired applications. Generalize the image by using Sysprep.exe.
4. Use the New 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, using disk that is allocated from the managed storage pool. VMM automatically unmarks 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 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, automatically creating a new logical unit from the storage pool. VMM automatically unmarks the new logical unit to the host.

For detailed steps, see **How to Create a SAN Copy-Capable Template from an Existing Virtual Machine**.

**Rapid Provisioning by Using SAN Copy Prerequisites**

Before you begin, make sure 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 have the feature enabled.

**Note**

Realize that this may require additional licensing from your storage vendor.

- The storage pool that you want to use for rapid provisioning must be under VMM management. This involves adding the SMI-S provider for the array, discovering storage pools, classifying the storage, and setting 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 rapid provision virtual machines.
- The Hyper-V hosts that you want to use as placement destinations must be members of the host group. Additionally:

- 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.)
- 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 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 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](#).

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

Follow these steps to deploy a virtual machine by using rapid provisioning.

Task	Description
<p>Step 1: Do either of the following:</p> <ul style="list-style-type: none"><li>• <b>How to Create a SAN-Copy Capable Template from a New Virtual Machine</b></li><li>• <b>How to Create a SAN Copy-Capable Template from an Existing Virtual Machine</b></li></ul>	Describes how to create a SAN copy-capable template from either a new or existing virtual machine. Includes scenario-specific prerequisites.
<p>Step 2: <b>How to Deploy a New Virtual Machine from the SAN Copy-Capable Template</b></p>	Describes how to create and deploy the new virtual machine by using the SAN copy-capable template.

## Configuring Virtual Machine Settings in VMM

The following topics provide information to help you create and deploy virtual machines in System Center 2012 – Virtual Machine Manager (VMM):

- **How to Create a Virtual Machine from a Blank VHD**
- **How to Create a Virtual Machine from an Existing Virtual Hard Disk**
- **How to Create a Virtual Machine from an Existing Virtual Machine**
- **How to Create a Virtual Machine Template**
- **How to Create a Virtual Machine from a Template**
- **Configuring Availability Options for Virtual Machines** (System Center 2012 SP1 only)
- **Converting Physical Computers to Virtual Machines (P2V)**
- **How to Convert Citrix XenServer Virtual Machines to Hyper-V**
- [How to Convert VMware Virtual Machines to Hyper-V](#)
- [Rapid Provisioning of Virtual Machines Using SAN Copy Overview](#)
- **Using the OVF Import/Export Tool**

## **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 using the Migrate VM Wizard or drag and drop, perform a quick storage migration, and run a live migration.

- **Migrating Virtual Machines and Storage Overview**
- **How to Migrate a Virtual Machine**
- **How to Run a Quick Storage Migration**
- **How to Run a Live Migration in VMM in System Center 2012 SP1**

## **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.

## **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.

- **How to Backup and Restore the VMM Database**

Describes how to backup and restore the SQL Server database that is used by VMM.

## 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](#)
- [Ports and Protocols for VMM](#)

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
<a href="#">How to Create a Run As Account in VMM</a>	Describes how to create Run As accounts
<a href="#">How to Disable and Enable Run As Accounts in VMM</a>	Describes how to disable and enable a Run As account to temporarily prevent its use.
<a href="#">How to Delete a Run As Account in VMM</a>	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	<p>Members of the Administrators user role can perform all administrative actions on all objects that VMM manages.</p> <p>Administrators have sole responsibility for these features of VMM:</p> <ul style="list-style-type: none"><li>• Only administrators can add stand-alone XenServer hosts and XenServer clusters (known as pools) to VMM management.</li><li>• Only administrators can add a Windows Server Update Services (WSUS) server to VMM to enable updates of the VMM fabric through VMM.</li></ul> <p>To change the members of the Administrator user role, see <a href="#">How to Add Users to the</a></p>

VMM User Role	Capabilities
	<a href="#">Administrator User Role.</a>
Fabric Administrator (Delegated Administrator)	<p>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.</p> <p>To create a delegated administrator, see <a href="#">How to Create a Delegated Administrator User Role.</a></p>
Read-Only Administrator	<p>Read-only administrators can view properties, 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.</p> <p>To create a read-only administrator, see <a href="#">How to Create a Read-Only Administrator User Role.</a></p>
Tenant Administrator	<p>In VMM in System Center 2012 Service Pack 1 (SP1), you can create Tenant Administrator user roles.</p> <p>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.</p>

VMM User Role	Capabilities
	<p>Tenant administrators can place quotas on computing resources and virtual machines.</p> <p>To create a tenant administrator, see <a href="#">How to Create a Tenant Administrator User Role in VMM in System Center 2012 SP1</a>.</p>
Application Administrator (Self-Service User)	<p>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.</p> <p>To create a self-service user, see <a href="#">How to Create a Self-Service User Role in VMM</a>.</p>

## See Also

[Configuring Self-Service in VMM](#)

## How to Add Users to the Administrator User Role

The Administrator user role is created when you install System Center 2012 – 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

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

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 in System Center 2012 SP1

With 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. On the **Actions** page, select one or more actions that the members of this role can perform, and then 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


### 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 the VMM components. 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 table.

Connection type	Protocol	Default port	Where to change port setting
SFTP file transfer from VMware ESX Server 3.0 and VMware ESX Server 3.5 hosts	SFTP	22	
VMM management server to P2V source agent (control channel)	DCOM	135	
VMM management server to Load Balancer	HTTP/HTTPS	80/443	Load balancer configuration provider
VMM management server to WSUS server (data channel)	HTTP/HTTPS	80/8530 (non-SSL), 443/8531 (with SSL)	These ports are the IIS port binding with WSUS. They cannot be changed from VMM.
VMM management server to WSUS server (control channel)	HTTP/HTTPS	80/8530 (non-SSL), 443/8531 (with SSL)	These ports are the IIS port binding with WSUS. They cannot be changed from VMM.
BITS port for VMM transfers (data channel)	BITS	443	During VMM setup

Connection type	Protocol	Default port	Where to change port setting
VMM library server to hosts file transfer	BITS	443 (Maximum value: 32768)	During VMM setup
VMM host-to-host file transfer	BITS	443 (Maximum value: 32768)	
VMM Self-Service Portal to VMM Self-Service Portal web server	HTTPS	443	During VMM setup
 <b>Note</b> In System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed.			
VMware Web Services communication	HTTPS	443	VMM console
SFTP file transfer from VMM management server to VMware ESX Server 3i hosts	HTTPS	443	
OOB Connection - SMASH over WS-Man	HTTPS	443	On BMC
VMM management server to in-guest agent (VMM to virtual	HTTPS (using BITS)	443	

Connection type	Protocol	Default port	Where to change port setting
machine data channel)			
VMM management server to VMM agent on Windows Server–based host (data channel for file transfers)	HTTPS (using BITS)	443 (Maximum value: 32768)	
OOB Connection IPMI	IPMI	623	On BMC
VMM management server to remote Microsoft SQL Server database	TDS	1433	
Console connections (RDP) to virtual machines through Hyper-V hosts (VMConnect)	RDP	2179	VMM console
VMM management server to Citrix XenServer host (customization data channel)	iSCSI	3260	On XenServer in transfer VM
Remote Desktop to virtual machines	RDP	3389	On the virtual machine
VMM management server to VMM agent on Windows Server–based host (control channel)	WS-Management	5985	During VMM setup

Connection type	Protocol	Default port	Where to change port setting
VMM management server to in-guest agent (VMM to virtual machine control channel)	WS-Management	5985	
VMM management server to VMM agent on Windows Server-based host (control channel - SSL)	WS-Management	5986	
VMM management server to XenServer host (control channel)	HTTPS	5989	On XenServer host in: /opt/cimserver/cimserver_planned.conf
VMM console to VMM management server	WCF	8100	During VMM setup
VMM Self-Service Portal web server to VMM management server   <b>Note</b> In System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed.	WCF	8100	During VMM setup
VMM console to VMM management	WCF	8101	During VMM setup

Connection type	Protocol	Default port	Where to change port setting
server (HTTPS)			
Windows PE agent to VMM management server (control channel)	WCF	8101	During VMM setup
VMM console to VMM management server (NET.TCP)	WCF	8102	During VMM setup
WDS provider to VMM management server	WCF	8102	During VMM setup
VMM console to VMM management server (HTTP)	WCF	8103	During VMM setup
Windows PE agent to VMM management server (time sync)	WCF	8103	During VMM setup
VMM management server to Storage Management Service	WMI	Local call	
VMM management server to Cluster PowerShell interface	PowerShell	n/a	
Storage Management Service to SMI-S Provider	CIM-XML	Provider-specific port	
VMM management server to P2V source	BITS	User-Defined	P2V cmdlet option

Connection type	Protocol	Default port	Where to change port setting
agent (data channel)			

## 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
<a href="#">System Center 2012 – Virtual Machine Manager (VMM) General Troubleshooting Guide</a>	General information about troubleshooting VMM, such as collecting traces and logging information.
<a href="#">Troubleshooting System Center 2012 - Virtual Machine Manager (VMM)</a>	List of known issues with VMM, and possible resolutions or workarounds for those known issues.
<a href="#">System Center 2012 – Virtual Machine Manager (VMM) Error Codes</a>	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.	<a href="#">Microsoft Download Center</a>

Resource	Description	Location
VMM forums	Ask questions about or discuss VMM	<a href="#">System Center Virtual Machine Manager Forums</a>

For an overview of VMM, see [Overview of System Center 2012 - Virtual Machine Manager](#).

## Glossary for System Center 2012 - Virtual Machine Manager

---

Term	Definition
Application Frameworks resources	A set of programs, Windows PowerShell cmdlets, and scripts that enable users to install virtual applications and Web applications during the deployment of a service.
application profile	A Virtual Machine Manager library resource that contains instructions for installing Microsoft Server App-V, the Web Deploy tool, and Microsoft SQL Server data-tier applications and for running scripts when you deploy a virtual machine as part of a service.
capability profile	A Virtual Machine Manager library resource that defines which resources (for example, number of processors or maximum memory) are available to a virtual machine that is created in a private cloud.
cloud library	A grouping of read-only library shares that are assigned to a private cloud and a location where self-service users of a private cloud can store virtual machines or services.

Term	Definition
dynamic optimization	The capability to perform resource balancing by automatically migrating virtual machines within host clusters that support live migration.
equivalent objects	Different files (for example, .vhd files) on which a user has set the same family and release properties to indicate that the different files are related.
fabric	In VMM, the infrastructure resources (for example, virtual machine hosts, networking, and storage) that are used to create and deploy virtual machines and services to a private cloud.
host profile	A Virtual Machine Manager library resource that contains hardware and operating system configuration settings to convert a bare-metal computer to a managed Hyper-V host.
instance count	The number of virtual machines to deploy for a given tier of a service.
logical network	A user-defined named grouping of IP subnets and virtual local area networks (VLANs) that is used to organize and simplify network assignments.
orphaned resource	A Virtual Machine Manager library resource on a library server that has been removed from VMM, but the resource is still used in a virtual machine template or a service template.
physical resource	A file (for example, .vhd files or script) that can be imported into or exported from the Virtual Machine Manager library.

Term	Definition
power optimization	The capability to automatically turn off a virtual host machine that is not needed to meet resource requirements within a host cluster and then turn the virtual host machine back on when it is needed again.
private cloud	A grouping of virtual machine hosts and networking, storage, and library resources that is assigned to users to deploy services.
Read-Only Administrator user role	A role that is used to limit users to only viewing status, job status, and properties of objects within their assigned host groups, private clouds, and library servers. A Read-Only Administrator cannot create new objects.
read-only library share	A library share that is assigned to a private cloud and that is used to share resources to self-service users that deploy services to that private cloud.
scale out (a service)	To add additional virtual machines to a tier of a deployed service.
Self-Service User Content	A node in the Library workspace that displays the resources (for example, .vhd files and scripts) that self-service users have uploaded for authoring templates and for sharing with other self-service users.
service	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.
Service Deployment Configurations	A node in the Library workspace where you can view instances of services that have been

Term	Definition
	saved (during the process of configuring specific deployment settings for the service instance) but have not been deployed.
service template	A Virtual Machine Manager library resource that contains the configuration settings used to deploy each tier of a service.
Service Template Designer	A graphical tool in the VMM console that is used to create and modify service templates.
servicing window	A user-defined time period that can be assigned to a virtual machine, host, or service to indicate when that object is available to be taken offline (for example, to perform maintenance).
SQL Server profile	A Virtual Machine Manager library resource that contains instructions for customizing an instance of Microsoft SQL Server for a SQL Server data-tier application (DAC) when you deploy a virtual machine as part of a service.
storage classification	A user-defined name assigned to a storage pool that is used to describe the particular capabilities of the storage pool.
tier	An element of a service template that contains the configuration settings necessary to deploy a particular portion of a service.
upgrade domain	A group in which Virtual Machine Manager automatically places instances of a tier of a service so that when the service is updated, those instances will be updated at the same time.

Term	Definition
virtual IP template	A template that contains configuration settings for how a load balancer should handle a specific type of network traffic.

## 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

- **Support**<http://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 <code>"/RunInVE:&lt;package GUID&gt;"</code> to the end of the process's command line.	For a process to be virtualized, that process must be opened by an App-V program such as <b>sfttray.exe</b> , 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 <code>"sfttray.exe /exe &lt;executable to launch&gt; /app &lt;name of application&gt;"</code> .

## See Also

[Microsoft Server Application Virtualization](#)

[Installing 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](mailto: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

Information in this document, including URL and other Internet website references, is subject to change without notice, and is provided for informational purposes only. The entire risk of the use or results of the use of this document remains with the user, and Microsoft Corporation makes no warranties, either express or implied. The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2011 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows Server, Windows Vista, Active Directory, and ActiveSync are either registered trademarks or trademarks of Microsoft Corporation in the USA. and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

## Server Application Virtualization Service Pack 1 Release Notes

To search these Release Notes, press CTRL+F.



### Important

Read these Release Notes thoroughly before you install Microsoft Server Application Virtualization (Server App-V) Service Pack 1. These Release Notes contain information that you must have to successfully install or use Server App-V Service Pack 1. 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 that is included with this product.

## Protect Against Security Vulnerabilities and Viruses

To help protect against security vulnerabilities and viruses, we recommend that you install the latest available security updates for any new software. 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=275110>).

You can also provide your feedback about the documentation directly to the App-V documentation team. Send your documentation feedback to [appvdocs@microsoft.com](mailto:appvdocs@microsoft.com).

## Known Issues with Server Application Virtualization Service Pack 1

This section provides the most up-to-date information about issues with Server App-V Service Pack 1. 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.

### Microsoft SQL Server databases are not captured during sequencing if the installer file uses a DSN-based ODBC connection

The Tier feature in Server App-V Server cannot detect connections that are made to databases that are made with DSN-based ODBC connections. If the installer file associated with the application you are trying to sequence requires this type of connection, the sequencer will not detect it during sequencing. An example of an application that exhibits this functionality is Microsoft Dynamics GP running on Microsoft Windows Server 2008 R2.

**WORKAROUND** During the monitoring phase of sequencing, use the following steps:

Because the sequencer does not automatically retrieve Microsoft SQL Server DACPAC's and T-SQL scripts from databases during sequencing, you must manually export these artifacts from the Microsoft SQL Server used during installation. After you have these artifacts, you can use them as if they were automatically generated by the sequencer. Use the following link for more information about how to manually extract DACPACs and T-SQL scripts:

[To extract a DAC from a Microsoft SQL Server Database](http://go.microsoft.com/fwlink/?LinkId=275108)  
(<http://go.microsoft.com/fwlink/?LinkId=275108>).

To generate T-SQL scripts, use the following procedure:

1. In Microsoft SQL Server Management Studio, right-click the database you wish to export and select **Tasks**, and then click **Generate Scripts**.

2. In **Choose Objects**, select **all Tables**.
3. In **Set Scripting Options**, select **Advanced**.
4. In the **General** section, change the value for Type of data to script to **Data Only**.
5. Proceed with the remainder of the steps of the wizard.

### **Error occurs when you sequence Microsoft Dynamics AX 2009**

After you sequence Microsoft Dynamics AX 2009 on a computer that is running Windows Server 2008 R2 x64, you may see an error **Side-by-side assembly privatization failed** message in the **Package Completed** section of the Server App-V sequencer.

**WORKAROUND** Despite the error, the package is actually created without issues. You can ignore this error. No workaround is required.

### **You cannot add an Server App-V package to a computer running Windows Server 2003 that uses IIS**

If an application is sequenced that requires an **IWAM\_ account** for IIS 6 on a computer running Windows Server 2003, the package is not added.

**WORKAROUND** This is a known issue. There is no workaround.

### **Database artifacts that are generated by the Server App-V sequencer do not support machine name accounts as database logins**

Applications such as Microsoft SQL Server Reporting Services that create machine name accounts as database logins (for example, **domain\machinename\$**) donot function as expected because they are tied to a specific machine name.

**WORKAROUND** After you deploy the DACPAC and T-SQL scripts to your database, manually add the appropriate machine name accounts by using the Microsoft SQL Server Management Studio or another database administrative tool.

### **Database logins are not automatically enabled**

Certain applications that create Microsoft SQL Server databases also create database logins. The DACPAC that is generated for these databases contains the definition for any new logins, but not the associated passwords. At deployment time, a password must be specified for the new logins.

**WORKAROUND** The T-SQL scripts that are generated by the Server App-V sequencer will have a line item for setting the password for each new login that is created during sequencing. Open the T-SQL

script and look for lines like this, where **LOGINNAME** is the new Microsoft SQL Server login. Replace **\$(LOGINNAME\_PASSWORD)** with the password that you want to use for the new login:

```
ALTER LOGIN [LOGINNAME] WITH PASSWORD = '$(LOGINNAME_PASSWORD)'
```

## 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

Operating System	Edition	Service Pack	System Architecture
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. To uninstall the Sequencer, 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  
/ACCEPTTEULA
```

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 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
<b>Make Item Mandatory</b>	A value for a mandatory configuration item must be provided when the package is deployed. To make the selected item mandatory, click <b>Make Item Mandatory</b> in the <b>Deployment Configuration Item</b> pane. To remove the mandatory setting, select the item and then click <b>Make Item Mandatory</b> again.
<b>Delete Item</b>	To delete a configuration item, select the item that should be deleted and then click <b>Delete Item</b> in the <b>Deployment Configuration Item</b> pane.
<b>Properties</b>	To view the properties associated with the configuration item, click <b>Properties</b> in the <b>Deployment Configuration Item</b> pane. In the Deployment Configuration Item Properties dialog box, you can do the following: <ul style="list-style-type: none"><li>• Change the default value.</li><li>• Change the <b>Name</b>.</li><li>• Change the <b>Description</b>.</li><li>• Make the configuration item mandatory. Mandatory items must be run when the package is deployed.</li></ul>
<b>Add Deployment Configuration Items</b>	To add a new deployment configuration item click <b>Add Deployment Configuration Item</b> in the <b>Deployment Configuration Item</b> pane. Deployment configuration items are settings, for example a database connection string that will impact how the virtual application

	package runs on target computers.
<b>Manage Scripts</b>	To specify scripts that should run either inside or outside the virtual environment when the package is deployed to a computer, click <b>Manage Scripts</b> in the <b>Deployment Configuration Item</b> 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) (<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](#)

## 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) (<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](http://go.microsoft.com/fwlink/?LinkId=224905) 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](http://go.microsoft.com/fwlink/?LinkId=224905) 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) (<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](mailto:appvdocs@microsoft.com)) or using the address provided here and we will use commercially reasonable 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.