

Chapter 1

Introduction to System Center Virtual Machine Manager 2008 R2

In IT environments today, virtualization is becoming the new hot technology. With the increased emphasis on power, cooling, and space savings due to cost, virtualization has made its entry into both the enterprise and the datacenter. It was initially used as a technology to consolidate legacy hardware, but administrators are now seeing the full range of benefits offered by virtualization. Products like Virtual Machine Manager (VMM) provide end-to-end management of the entire virtualized infrastructure, from the physical hosts to the guest operating systems. VMM is one of the first products on the market today to offer heterogeneous management; you can use it to manage Microsoft's Windows Hyper-V and Virtual Server as well as VMware's ESX infrastructure through VMware VirtualCenter. The ease of use of a central console for managing the entire infrastructure is one of the key benefits of VMM.

Planning for a virtualized environment is not easy, but with the proper knowledge of the key architecture pieces and how they interact with each other, it becomes an easier process. This book will provide you with what you need to know to plan, design, and manage your virtualized environment. Most IT administrators would argue that setting up a virtualized environment and calculating growth are some of the hardest steps to take for an IT department. Once the virtualized environment is configured and you have virtualization hosts with available capacity, however, deployment of a new server as a virtual machine becomes a 1-hour process. This is compared to the number of weeks it takes today to provision a new physical server, including purchasing the new hardware.

Before we get into the details of VMM, we need to ensure that you understand all the moving pieces and how they are used. Having a common language is also essential in understanding the material in this book. You need to have this knowledge early on to maximize the benefit of reading this book. Once you have read this chapter, you will have an overall high-level knowledge of VMM and how it can be tailored to your needs. Once we lay the foundation here, further chapters will go over different scenarios and what an administrator needs to know when implementing and managing a virtualized environment. By the time you finish this book, you'll have in-depth knowledge of Virtual Machine Manager and related virtualization technologies. Armed with this knowledge, you will be ready to plan, deploy, and manage a virtualized environment.

In this chapter, you will learn to how to:

- ◆ Identify and explain the components in the VMM architecture
- ◆ Determine the ports and protocols required for communication between the various VMM components
- ◆ Determine the various roles and privileges of VMM
- ◆ Explain the differences between the migration options offered in VMM
- ◆ Describe the authentication methods between VMM and hosts

A Quick Overview of Virtual Machine Manager

System Center Virtual Machine Manager (VMM) is a multivendor heterogeneous virtualization management solution tailored for enterprises and virtualized datacenters. It enables the centralized and unified administration of both physical and virtual servers, increases server utilization, and provides rapid provisioning. Through its integration with System Center Operations Manager (OpsMgr), VMM provides real-time health monitoring for the virtualized infrastructure and the ability to monitor and optimize application performance. The latter is achieved through a feature of VMM called Performance and Resource Optimization (PRO). PRO is covered extensively in Chapter 9 of this book.

The following list includes some of the key benefits of VMM:

- ◆ Support for managing heterogeneous virtualization platforms, including Microsoft Hyper-V, Microsoft Virtual Server, and VMware ESX. (VMware ESX is managed through the VirtualCenter web interface.)
- ◆ A powerful and easy-to-use console that enables the management of the virtualized infrastructure.
- ◆ A fully scriptable environment through Windows PowerShell.
- ◆ PRO, a feature of VMM and OpsMgr for the dynamic datacenter.
- ◆ Virtual machine conversions, either Physical to Virtual (P2V) or Virtual to Virtual (V2V) are reduced to a simple wizard with VMM.
- ◆ Quick template-based provisioning of virtual machines. Virtual machines can be deployed at a fraction of the time it would require to provision a new physical server.
- ◆ Intelligent Placement, which offers an administrator the ability to ensure that virtual machines are placed on the most appropriate physical host. Behind the scenes, VMM does all the work to produce the host ratings using data gathered through performance counters from the hosts and virtual machines and capacity planning algorithms from Microsoft Research.
- ◆ The VMM library, which offers a centrally managed way to keep all the building blocks needed to keep virtual machines organized.
- ◆ The Self-Service Portal, which offers the ability to delegate the provisioning and management of virtual machines to end users through a set of permissions and privileges.

- ◆ Some features of VMM and OpsMgr offer health monitoring and smart reports to get a high-level view of the virtualized environment. For example, one valuable report is the Virtualization Candidates report, which helps identify physical computers that are good candidates for conversion to virtual machines.

The availability of VMM 2008 R2 was announced in August 2009, and it introduces several enhancements over VMM 2008. The most important ones are as follows:

- ◆ Storage migration (also known as Quick Storage Migration) for running virtual machines with minimal downtime for Windows Server 2008 R2 Hyper-V hosts and support for VMware Storage VMotion
- ◆ Template-based rapid provisioning for new virtual machines
- ◆ Maintenance mode for hosts to facilitate rapid evacuation of hosts
- ◆ Support for Windows Server 2008 R2
- ◆ Support for Live Migration of virtual machines
- ◆ Support for Cluster Shared Volumes (CSV) that enables many virtual machines to reside on the same LUN
- ◆ Support for SAN migration in and out of failover clusters
- ◆ Support for hot add of virtual hard disks
- ◆ Support for virtual machine network optimizations like Virtual Machine Queue (VMQ) and TCP Chimney
- ◆ Support for third-party cluster file systems like the Melio FS from Sanbolic
- ◆ Support for VMware vSphere (VI4) features that existed in VMware Virtual Infrastructure 3
- ◆ Support for processor flexibility during virtual machine migrations

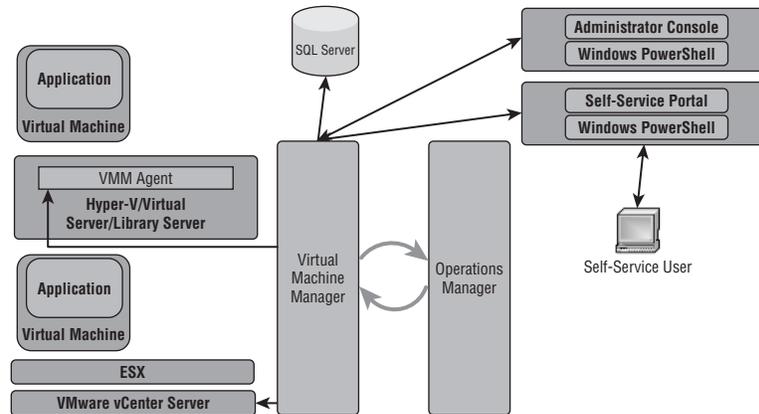
We will explain these features in more detail throughout this book. You can download the 180-day evaluation version of System Center Virtual Machine Manager 2008 R2 from the Microsoft Download Center at <http://www.microsoft.com/downloads/details.aspx?FamilyID=292de23c-845c-4d08-8d65-b4b8cbc8397b&displaylang=en>.

Exploring Virtual Machine Manager Components

VMM has a distributed-system architecture comprising several components. Figure 1.1 illustrates the high-level architecture of VMM and the various components that are part of VMM.

A VMM implementation is made of various core components that are required for every VMM installation. Various other components, like the Self-Service Portal, are not required but are very useful for specific scenarios like creating a development and test virtualization environment. PRO and the integration with OpsMgr is another optional feature of VMM, and together they offer a complete end-to-end service management solution for a dynamic virtualized environment.

FIGURE 1.1
Virtual Machine
Manager high-level
architecture



The following components are central to each VMM installation:

- ◆ VMM server
- ◆ VMM database
- ◆ VMM Windows PowerShell cmdlet interface
- ◆ VMM Administrator Console
- ◆ VMM library
- ◆ Managed virtualization hosts (VMM agents are installed on these virtualization hosts)
- ◆ VMM Self-Service Portal
- ◆ Managed virtualization managers (i.e., managed VMware VirtualCenter servers)
- ◆ OpsMgr management packs for monitoring, reporting, and PRO

Managed virtualization managers and the OpsMgr integration are optional components. Each VMM component fulfills a specific purpose and adds core virtualization management functionality. In the following sections, we will go through the various VMM components, introducing them to you and giving you a brief overview of their role and responsibilities. Installation and configuration of the various VMM components is covered in detail in Chapter 3. The integration of VMM with OpsMgr and the PRO functionality is covered in detail in both Chapter 3 and Chapter 9.

VMM Server and VMM Database

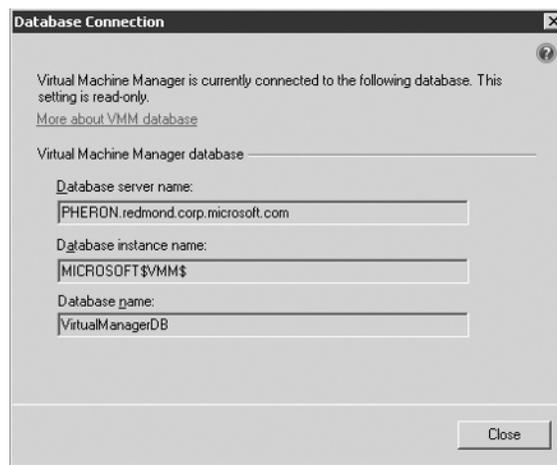
The VMM server component is the central component of any VMM deployment and the first VMM component that should be installed. The VMM server contains the core Windows service that includes the VMM engine. Through this service, VMM connects to the VMM database that stores all the configuration, management, and short-term performance information that VMM requires. At a high level, the VMM engine has three main purposes:

- ◆ It acts as the broker of information stored in the database. Any time a VMM client, such as the Administrator Console or a Windows PowerShell cmdlet, asks for information, that information is retrieved from the database by the VMM engine.

- ◆ It acts as the broker for communicating and executing commands with the VMM agents and for communicating and executing commands on the VMware VirtualCenter server.
- ◆ It coordinates the execution of VMM jobs. Every operation in VMM that has the potential to modify or modifies data either in the database or on any other VMM component (e.g., modifies a setting of a virtual machine on a virtualization host) becomes a VMM job. The engine coordinates the execution of jobs, monitors and reports on their progress, and lets clients know of any success or failures.

The VMM database can reside either locally on the VMM server or on a remote database server. Because of its importance to any VMM environment, it is recommended that you employ a highly available solution through failover clustering for the database server that hosts the VMM database. Figure 1.2 shows the connection information for the VMM database from the Administrator Console. Later in this chapter we will go through the network ports that are necessary for VMM to communicate with a remote SQL server.

FIGURE 1.2
Database connection
information



VMM clients like the Administrator Console, Self-Service Portal, and Windows PowerShell communicate with the VMM server component through a Windows Communication Foundation (WCF) private interface. The VMM server, which is the only component of VMM that communicates directly with VMM agents, uses the Windows Remote Management (WinRM) protocol to call into private interfaces on the VMM agent computer. The VMM server also uses WinRM to remotely invoke public Windows Management Instrumentation (WMI) interfaces on host and library server computers.

VMM Administrator Console

The VMM Administrator Console is the main user interface for managing a virtualized infrastructure using VMM. You can install the VMM Administrator Console either on the same computer as the VMM server component or on a separate computer and connect to the VMM server remotely. The VMM Administrator Console is built entirely on top of the VMM Windows PowerShell interface, utilizing the many cmdlets that VMM offers. This approach made VMM very extensible and partner friendly while also allowing customers to accomplish anything that VMM offers in the Administrator Console GUI via scripts and automation.

The Administrator Console has five main views and an optional view:

Hosts view facilitates the management of virtualized hosts.

Virtual machines view facilitates the management of virtual machines.

Jobs view lists the currently running jobs as well as a history of past jobs. By default, VMM will include a job history for 90 days and prune older jobs every 20 hours.

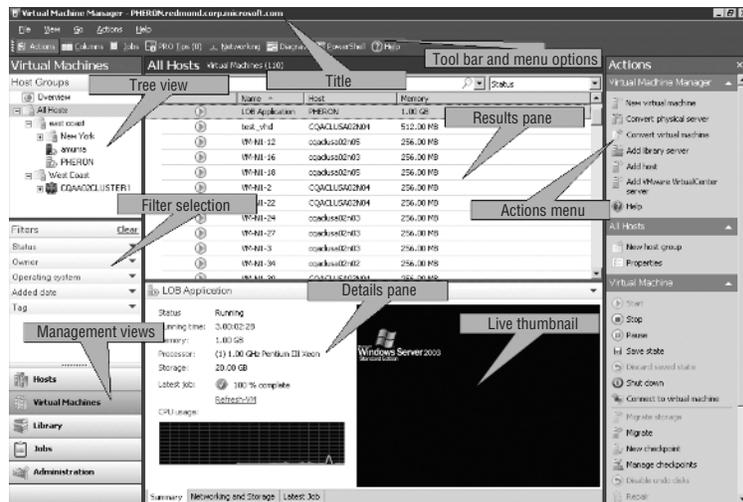
Library view lists all the building blocks for creating virtual machines.

Administration view includes the various administrative components for VMM.

Reporting view includes a list of reports and the ability to execute them against the OpsMgr reporting server. The reporting view is optional and can be enabled by integrating VMM with an OpsMgr reporting server after importing the VMM reports within the OpsMgr infrastructure.

Figure 1.3 shows the Administrator Console when the virtual machines view is selected. In this figure, you can see the various areas of the Administrator Console when virtual machines are being managed.

FIGURE 1.3
Virtual Machine
Manager Administrator
Console



The areas shown in Figure 1.3 are as follows (similar areas exist for the other views of the Administrator Console as well):

The tree view section includes host groups, Hyper-V failover clusters, and VMware ESX hosts organized hierarchically.

The filter selection section includes owner, status, operating system, date, and user-specified tag filters.

The main management view selection section includes the five main views of the Administrator Console.

The results pane with the list of virtual machines includes a search box, a group-by selection box, and the ability to add or remove columns from the view to make it easier for administrators to find the data they need.

The details pane for the selected virtual machine includes a live thumbnail of the virtual machine console, a CPU usage graph, and other details about the virtual machine. The details include networking and storage information, latest job status, and the current running time for a virtual machine that is in a running state.

The actions menu is divided into three areas:

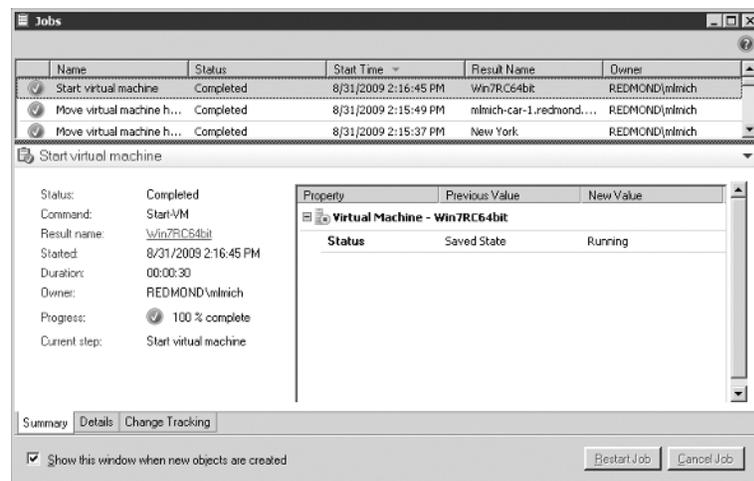
- ◆ The global actions for the Virtual Machine Manager Administrator Console
- ◆ The specific actions depending on the selection in the tree view (for example, host-group-specific actions)
- ◆ The context-sensitive actions that are specific to the virtual machine selected in the results pane

The title lists the name of the VMM server to which the Administrator Console is connected. If the VMM installation is an evaluation version, it will also list the number of days remaining in the evaluation period.

The toolbar and menu options make it easy to navigate to the different areas of the Administrator Console and to open separate windows. Separate windows are available for the following:

- ◆ The most recent jobs launched by the current user (Figure 1.4).

FIGURE 1.4
Jobs window



- ◆ The PRO tips that are currently active and waiting to be implemented (Figure 1.5).
- ◆ The networking view, scoped to a host group (Figure 1.6).
- ◆ The diagram view (Figure 1.7). When the diagram view is selected, it will launch the System Center Operations Manager Operations console and display the diagram view for this VMM server.
- ◆ The Windows PowerShell window with the VMM PowerShell cmdlets loaded.

FIGURE 1.5
PRO Tips window

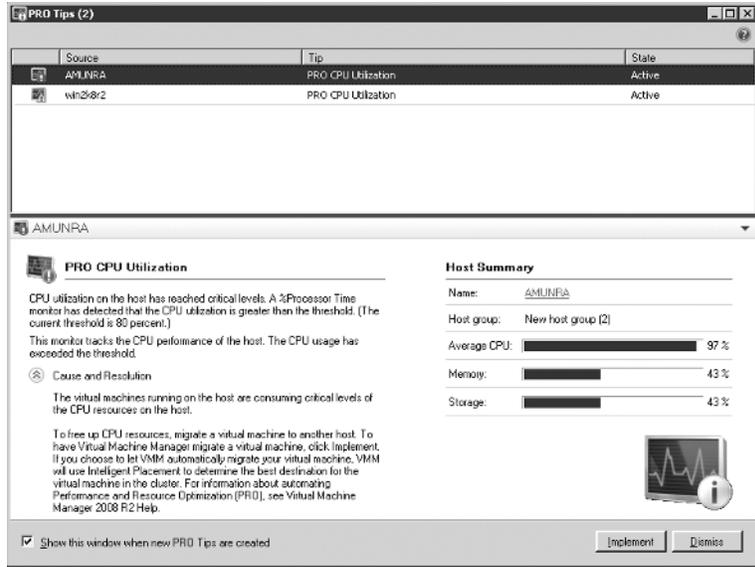


FIGURE 1.6
Networking window

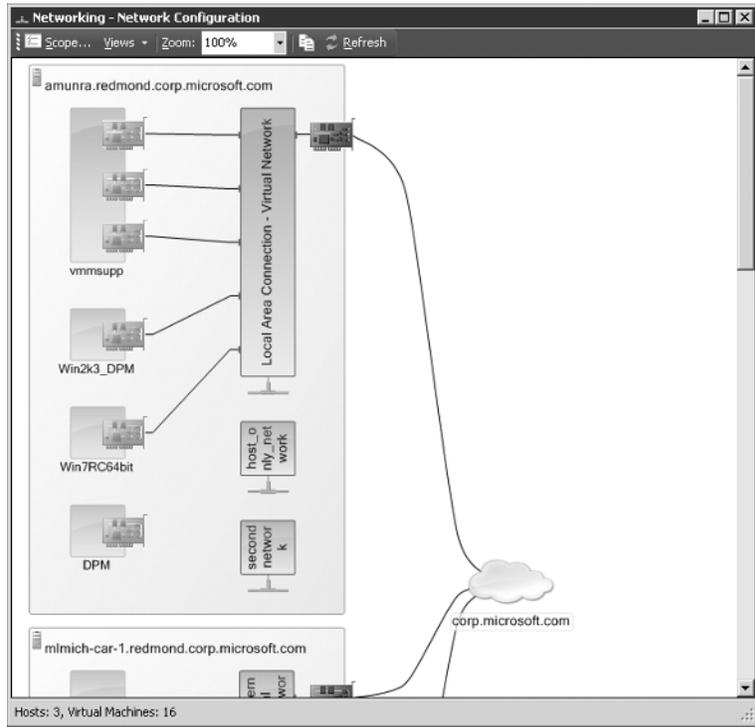
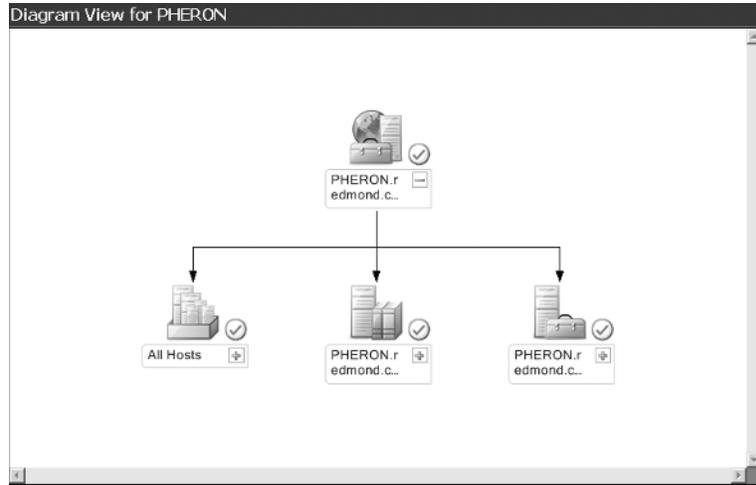


FIGURE 1.7
Diagram window



There are multiple other views of the Administrator Console, including the overview view. The views are listed here:

- ◆ Figure 1.8 shows the hosts view. In the details pane, all the VMs that reside on that host are listed in addition to the host details.

FIGURE 1.8
Hosts view

Name	Status	CPU Average	Total Memory	Available Memory	Virtualizat
PHERON.redmond...	OK	5 %	3.93 GB	401.00 MB	1.1.629.0
cqadusa02n05.re...	OK	53 %	8.00 GB	4.21 GB	6.1.7100.
CQACLUSA02N04...	OK	4 %	8.00 GB	2.88 GB	6.1.7100.
cqadusa02n02.re...	OK	2 %	8.00 GB	4.59 GB	6.1.7100.
stunra.redmond...	OK	2 %	8.00 GB	3.89 GB	6.1.7100.
cqadusa02n06.re...	OK	0 %	8.00 GB	6.61 GB	6.1.7100.
mimich-car-1.redm...	OK	2 %	3.25 GB	593.00 MB	1.1.629.0
cqadusa02n03.re...	OK	4 %	8.00 GB	4.01 GB	6.1.7100.

Status: OK	
Processor:	(4) 2.66 GHz Intel Xeon
Memory:	8.00 GB total, 512.00 MB reserve, 2.88 GB available
Storage:	719.13 GB capacity, 552.29 GB available
Operating system:	Microsoft Windows Server 2008 R2 Enterprise ,
Virtualization software:	Microsoft Hyper-V (Status: Up-to-date)
Virtual machines:	VM-N1-37 VM-N1-55 VM-N1-41 VM-N1-58 VM-N1-63 VM-N1-51 VM-N1-44 VM- VM-N1-74 VM-N1-77 VM-N1-22 VM-N1-17 VM-N1-2 VM-N1-50 VM-N1-11 VM-N1- VM-N1-5 VM-N1-52 VM-N1-21 VM-N1-28 VM-N1-36 VM-N1-47 VM-N1-9 test-3

- ◆ Figure 1.9 shows the library view. The details pane will list the details of the selected library item.
- ◆ Figure 1.10 shows the jobs view. The details pane will list the details of the selected job, including change tracking information.

FIGURE 1.9
Library view

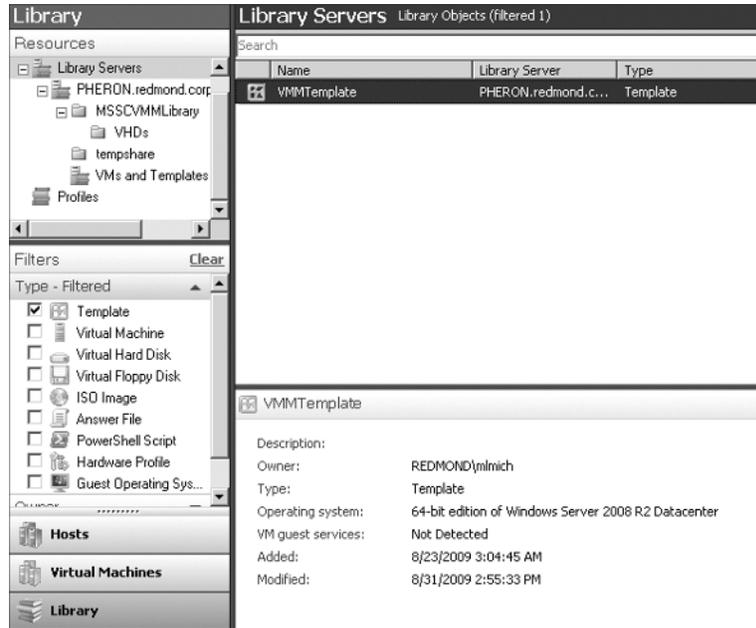
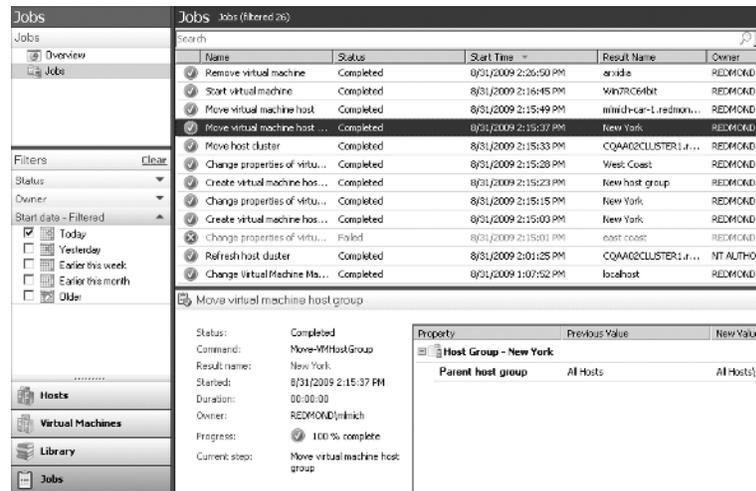


FIGURE 1.10
Jobs view



- ◆ Figure 1.11 shows the administration view. The results pane will list the different configuration options for each selection option in this view.
- ◆ Figure 1.12 shows the overview page. This page includes diagrams that provide an instant snapshot of the managed virtualized environment. This includes host information, recent job information, virtual machine status information, and a bar graph of library resources.

FIGURE 1.11
Administration view

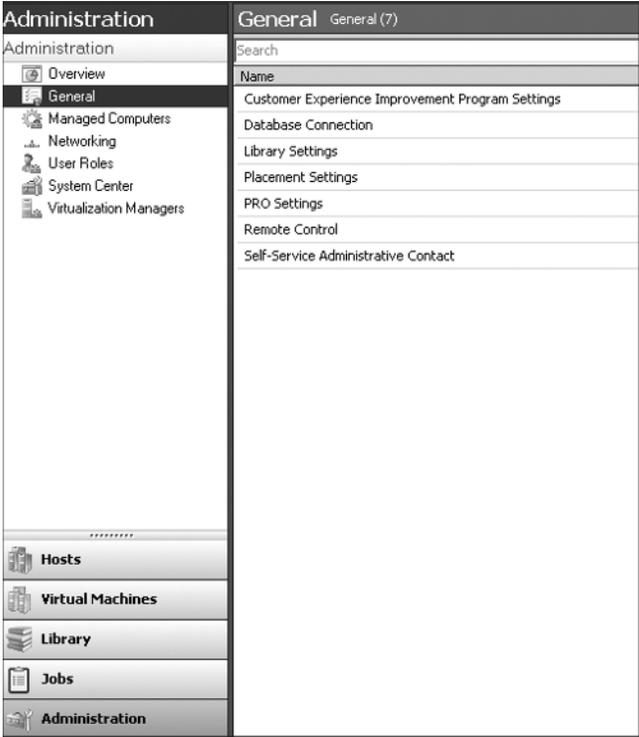
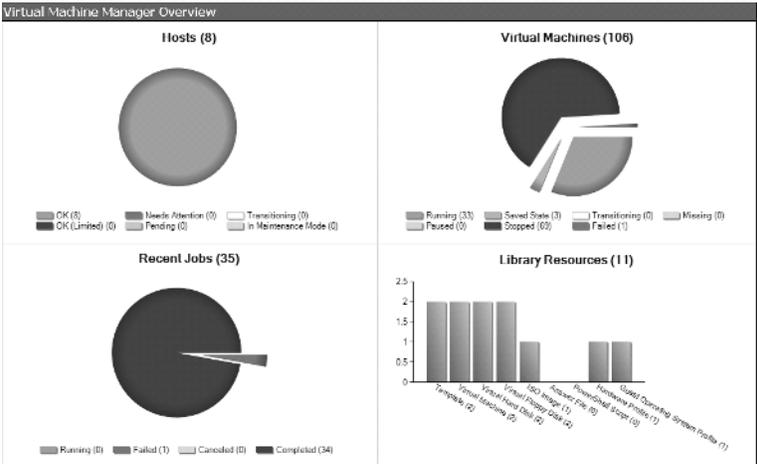


FIGURE 1.12
Virtual Machine
Manager Overview
window



The overview view link is present in the tree view pane for all Administrator Console views. In the overview view, an administrator gets a high-level snapshot of the VMM environment for hosts, virtual machines, jobs, and library resources. Hosts, virtual machines, and jobs are organized by status. Library resources are organized by quantity per resource.

In the VMM jobs view, jobs are audited with information on which user executed a job, when it was executed, and what information or properties were changed. The change information is displayed in the Change Tracking tab of the details pane for a selected job, as seen in Figure 1.13.

FIGURE 1.13
Change tracking for a VMM job

Property	Previous Value	New Value
Host - cqacusa02n06.redmond.corp.microsoft.com		
Status	Not Responding	Responding
Virtual Server status	Unknown	Running
Host Network Adapter - Broadcom NetXtreme 57xx Gigabit Controller		
IP address	10.177.21.226;10.177.20.93;fe80::8950:31f6:3...	10.177.20.93;fe80::8950:31f6:3e5d:cf2;2001:4...
Managed Computer - cqacusa02n06.redmond.corp.microsoft.com		
Status	Not Responding	Responding

The administration view of the Administrator Console further consists of six tree view options:

- ◆ General settings for Virtual Machine Manager
- ◆ Managed computers view
- ◆ Networking options
- ◆ User roles management
- ◆ System Center configuration options for Operations Manager
- ◆ Virtualization managers view

Windows PowerShell Interface

Virtual Machine Manager is one of the first Microsoft software products to fully adopt Windows PowerShell and give users a complete VMM management interface tailored for scripting. Windows PowerShell offers a rich scripting environment for administrators. Its full integration of cmdlets from various products and the native cmdlets of the operating system give an administrator the opportunity to write powerful PowerShell scripts and eliminate many manual daily operations.

Figure 1.14 shows the PowerShell button, which you can use to launch Windows PowerShell from the Administrator Console. Figure 1.15 shows Windows PowerShell in action, getting a list of running virtual machines and their current host.

Chapter 8 has a detailed description of the VMM Windows PowerShell interface and examples on how to automate VMM using Windows PowerShell.

FIGURE 1.14
Windows PowerShell button in the Administrator Console

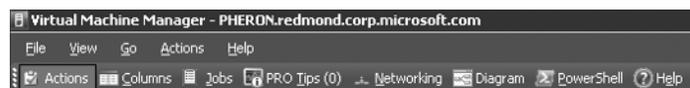
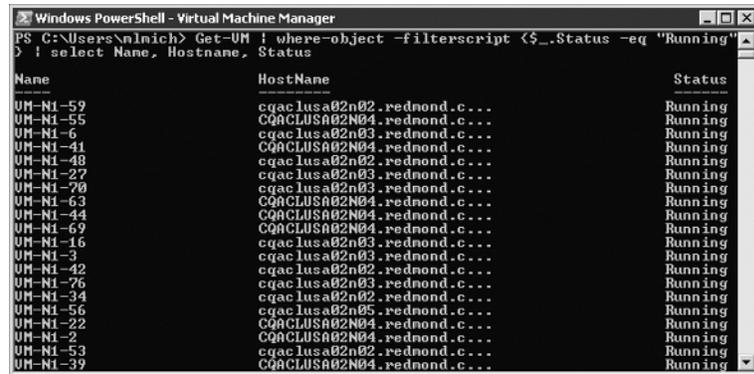


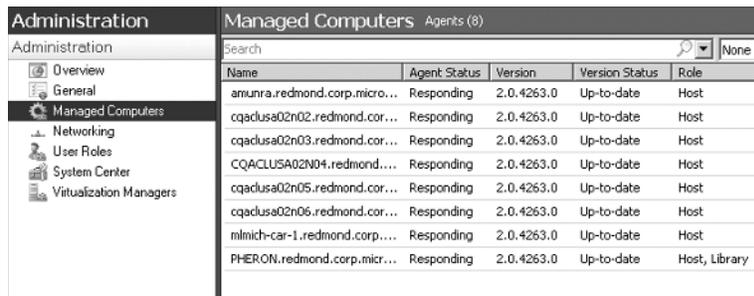
FIGURE 1.15
PowerShell window with list of running virtual machines



Virtual Machine Manager Agents

Virtual Machine Manager agents are installed on all Windows-based virtualization hosts and on all library servers. The Managed Computers page of the administration view in the Administrator Console lists all agents, their current version and status, and the VMM roles that the agent performs (i.e., host or library or both). Figure 1.16 shows an example view of the Managed Computers page.

FIGURE 1.16
VMM Managed Computers page



There are two ways that the VMM agent is installed:

- ◆ Automatically as part of adding a library server or adding a Windows-based virtualization host (e.g., Virtual Server or Hyper-V host). In this case, the VMM agent is pushed from the VMM server to the managed computer.
- ◆ Manually through the Virtual Machine Manager Setup. You can launch Setup and choose the Local Agent option to locally install the agent on a computer.

Local agent installation is necessary when deploying a perimeter network host. An administrator might also choose to install an agent locally on a host if the host is behind a firewall and cannot accept Distributed COM or WMI traffic across remote computers. Once the agent is installed, the VMM server will communicate with the agent through the WinRM and BITS protocols, which require only two ports to be opened on the firewall. WinRM provides the control channel and BITS provides the data channel of communication.

For Virtual Server hosts, the VMM agent also installs a set of private WMI interfaces that the VMM server invokes remotely through WinRM to get and set virtualization data. Hyper-V already has defined a public WMI interface that the VMM server invokes remotely using

WinRM. The VMM agent additionally installs and enables the BITS components that are necessary for transferring files to and from hosts and library servers. BITS file transfers are covered later in this chapter and in various other parts of this book.

Virtual Machine Manager Library

The VMM server can also act as the default library server after VMM is initially installed. The VMM library is the central repository for all the building blocks necessary for creating virtual machines. The library can be used to store all file-based resources, such as virtual hard disks and ISO images, templates, PowerShell scripts, sysprep answer files, operating system and hardware profiles, and offline (i.e., stored) virtual machines. After installation, you can use the Administrator Console to install additional library servers and add library shares to VMM. This is a recommended practice if you will be managing a large number of hosts or if your hosts are geographically dispersed. In the case of geographically dispersed hosts, file transfer times from the library to the host will be minimized if the library server is close in proximity and has high network bandwidth to the host.

The Virtual Machine Manager library provides an inventory of resources that are used to provision various types of virtual machines. The library server can be installed on any Windows Server computer acting as a file server that is capable of running the VMM agent. Physical file resources are managed through Windows shares on the library server. Each library server can have one or more shares. The library can store the following types of physical resources (listed here with their associated filename extensions):

- ◆ Virtual hard disk files (.vhd, .vmdk)
- ◆ PowerShell script files (.ps1)
- ◆ Sysprep answer files (.inf, .xml)
- ◆ ISO image files (.iso)
- ◆ Virtual floppy disk files (.vfd, .flp)

In addition, the library can store entire virtual machines in the form of templates or offline virtual machines:

- ◆ VMware templates can be imported in the VMM library through the Import Templates action when a VirtualCenter server is selected.
- ◆ Offline virtual machines stored in the VMM library need to be in an exported state for the Hyper-V virtualization platform.

The library also contains the following types of resources in the VMM database:

- ◆ Templates
- ◆ Hardware profiles
- ◆ Guest operating system profiles

These files do not have a physical representation in any library share. However, even though templates do not have a physical representation in a library share, they are linked to virtual hard disk files that do have a physical representation.

Figure 1.17 shows the VMM library with a variety of physical files and templates and their associated status organized by type. Figure 1.18 shows the details pane for a stored virtual machine. Figure 1.19 shows the profiles view of the VMM Library.

FIGURE 1.17
VMM library

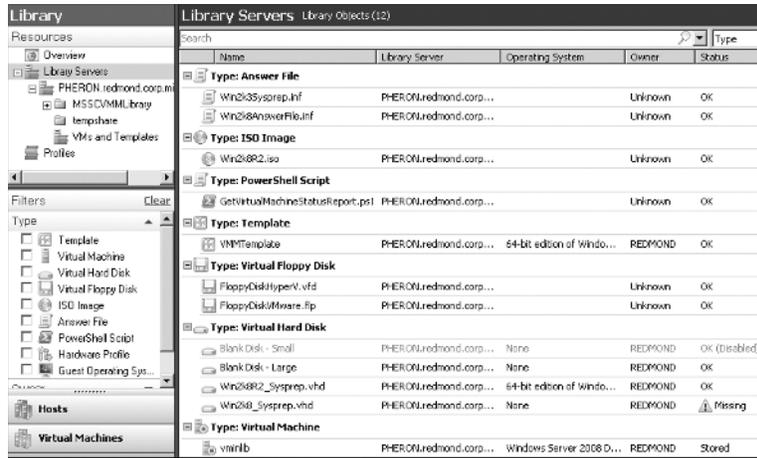
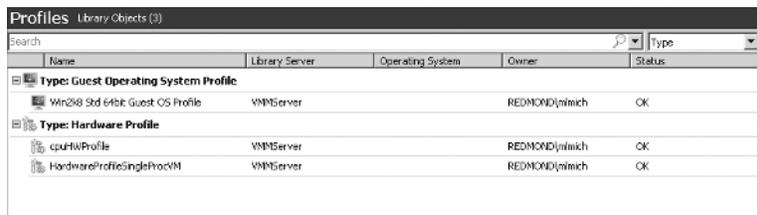


FIGURE 1.18
Details pane for a stored virtual machine in the VMM library



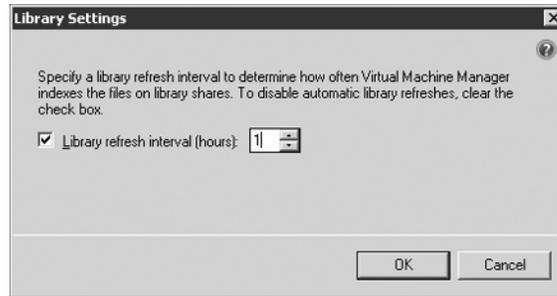
FIGURE 1.19
VMM library profiles



By default, the VMM library looks for new files or updates to existing files every hour. Physical files that can't be detected are flagged using the Missing status in the library view of the Administrator Console. This operation is performed as part of the library refresher that executes based on a user-customizable schedule. To configure the library refresh interval as seen in Figure 1.20, follow these steps:

1. Choose the administration view in the Administrator Console.
2. Click the General page.
3. Select the Library Settings option.
4. Change the library refresh interval to the desired value or disable the library refresher.

FIGURE 1.20
Configuring the library
refresh interval



For library servers that are in remote or branch offices, it might be desirable to either disable the library refresher or configure it to execute only once a day. A library server or an individual library share can be refreshed manually by clicking on the share or the server name in the library view and selecting the Refresh action.

Virtual Machine Manager Self-Service Portal

The VMM Self-Service Portal is an optional, web-based component that a VMM administrator can install and configure to allow users to create and manage their own virtual machines within a controlled environment on a limited group of virtual machine hosts. This avoids the need to install and grant access to the VMM Administrator Console for a set of users who need to accomplish a smaller set of targeted operations. The VMM administrator can create Self-Service User Roles using the Administrator Console. These user roles will determine the following:

- ◆ The domain users or domain groups that are members of the user role.
- ◆ The scope of the user role, defined at the host group level.
- ◆ The permissions of the Self-Service Users' actions for virtual machines, defined through a set of predefined privileges, as seen in Figure 1.21.
- ◆ The ability to enable the creation of new virtual machines through a set of templates chosen by the VMM administrator. A quota system can also be enforced to restrict the unlimited use of valuable resources by Self-Service Users. A VMM administrator can set quota points to the Self-Service User Role and assign quota points to virtual machine templates to limit the number of virtual machines that a user or group can deploy.
- ◆ The ability to store virtual machines in the VMM library and the library share location where the virtual machines will be put.

To create, operate, and manage virtual machines, Self-Service Users use the Virtual Machine Manager Self-Service Portal (SSP). The portal can be installed on the same computer as the VMM server or on a separate remote computer. The web portal utilizes the Web Server (Internet Information Services or IIS) Windows Server role and Windows PowerShell cmdlets to execute actions within the VMM infrastructure. In essence, the SSP is another client of the VMM server that utilizes WCF to communicate with the VMM server.

After the administrator determines which host groups Self-Service Users can create virtual machines on and what templates to use, a new virtual machine is automatically placed on the most suitable host in the host group based on host ratings and the Intelligent Placement feature of VMM. Figure 1.22 shows the New Virtual Machine Wizard for Self-Service Users.

FIGURE 1.21
Self-Service User Role
privileges

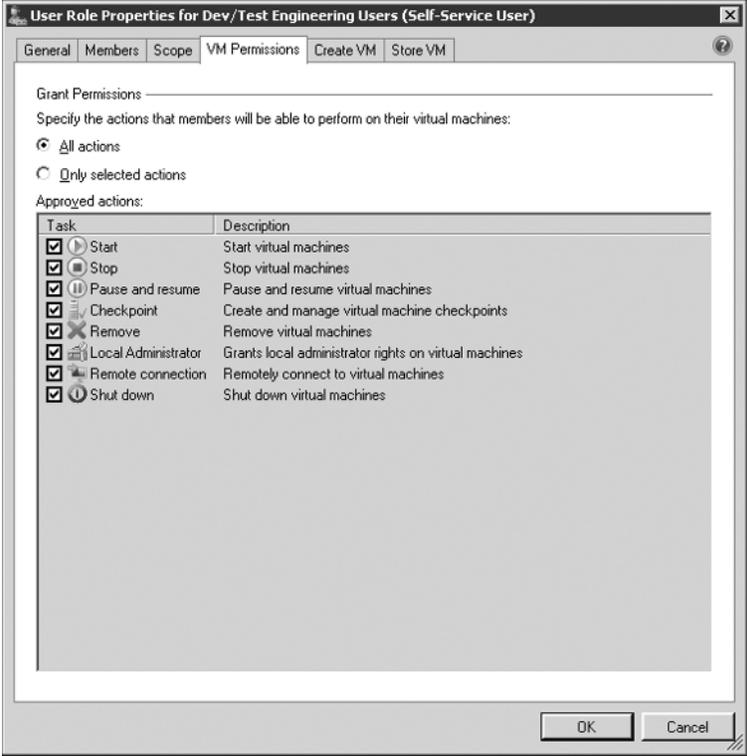
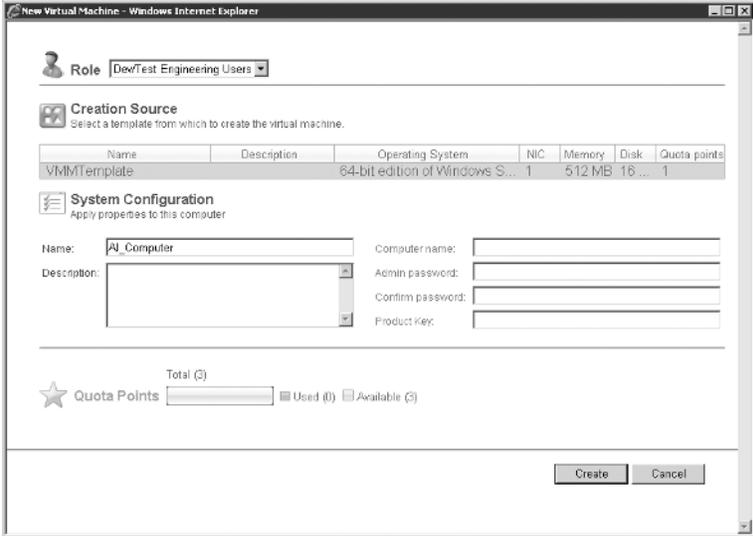


FIGURE 1.22
Self-Service Portal New
Virtual Machine Wizard



The Self-Service Portal is often leveraged in development and test scenarios and lab management scenarios as well as by help desk personnel that are responsible for fulfilling production virtual machine requests. In these scenarios, a set of common templates to provision virtual machines can be assigned ownership to a domain group in Active Directory that represents the Self-Service Users.

After a virtual machine is created, Self-Service Users can log in to the SSP and manage their virtual machines. The SSP supports two modes of authentication with the option to cache the user credentials:

- ◆ Anonymous forms-based authentication, where the SSP will ask users to log in first using a username and a password
- ◆ Windows integrated authentication

These are covered in more detail later on in this chapter.

INSTALLING THE SELF-SERVICE PORTAL ON A SEPARATE COMPUTER

If you have installed the VMM SSP on a computer other than the VMM server computer, there are two additional considerations:

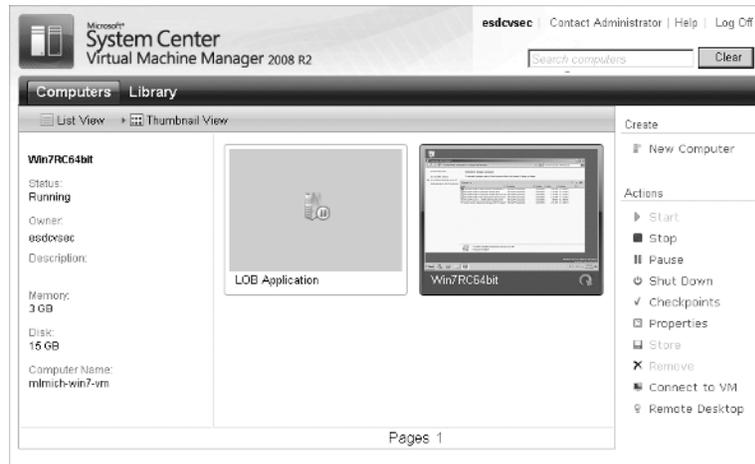
- ◆ You need to enable Kerberos Constrained Delegation in Active Directory for the SSP computer. This is necessary because of the double-hop of Self-Service User credentials from the client computer (e.g., a computer running Internet Explorer that is used to view the portal) to the web server (i.e., the Self-Service Portal server) to the VMM server. To configure constrained delegation, follow the instructions outlined in the How to Configure Integrated Windows Authentication for the VMM Self-Service Portal section of the System Center Virtual Machine Manager TechCenter at <http://technet.microsoft.com/en-us/library/cc956040.aspx>.
- ◆ If you need to connect to a different VMM server or if the VMM server has changed its computer name, you can edit the `VmmServerName` Registry key value of `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager Self-Service Portal\Settings` to modify the fully qualified domain name of the VMM server to the new computer name. After the computer name is changed, restart the IIS services for the VMM web components to establish connections to the new VMM server.

Virtual machines that were created through the SSP will automatically show up in the web interface. If they are created through other means and then assigned to Self-Service Users, three prerequisites have to be met before they can be managed through the SSP:

- ◆ The owner of the virtual machine has to be set to the user or group that is trying to manage this virtual machine through the SSP.
- ◆ The user or group that is trying to manage the virtual machine has to be a member of a Self-Service User Role that is scoped to include a host group that manages this virtual machine.
- ◆ The Self-Service User Role has to define enough privileges for its users to be able to manage this virtual machine.

Figure 1.23 shows you the main page of the SSP. Users can manage their virtual machines, view virtual machine properties, start or stop virtual machines, store virtual machines in the library, view live thumbnails of virtual machines, or view the console connection to a virtual machine.

FIGURE 1.23
VMM Self-Service Portal



Console connections to virtual machines are offered through three different mechanisms depending on the virtualization platform of the virtual machine:

- ◆ For virtual machines residing on a Hyper-V host, console connections are offered through the Virtual Machine Manager Self-Service Client. The Self-Service Client is an ActiveX control that utilizes the Remote Desktop Protocol (RDP) and the Hyper-V Single Port Listener feature to provide console connections to virtual machines through the Hyper-V host.
- ◆ For virtual machines residing on a Virtual Server host, console connections are offered through the Virtual Machine Remote Control (VMRC) ActiveX control that ships with Virtual Server and is redistributed by VMM.
- ◆ For virtual machines residing on a VMware ESX host, console connections are offered through the VMware MKS ActiveX control. This control is downloaded through a secure SSL channel when you try to view a live VMware virtual machine.

Figure 1.24 shows a live console connection to a virtual machine from the SSP. A user can send a Ctrl+Alt+Del or Reconnect to the virtual machine from this window.

There are situations in which a user connecting to the SSP is a member of more than one Self-Service User Role that is scoped over the same set of virtual machines and each user role provides a different set of privileges and permissions. To apply a certain user role to a virtual machine and manage it using that user role, follow these steps:

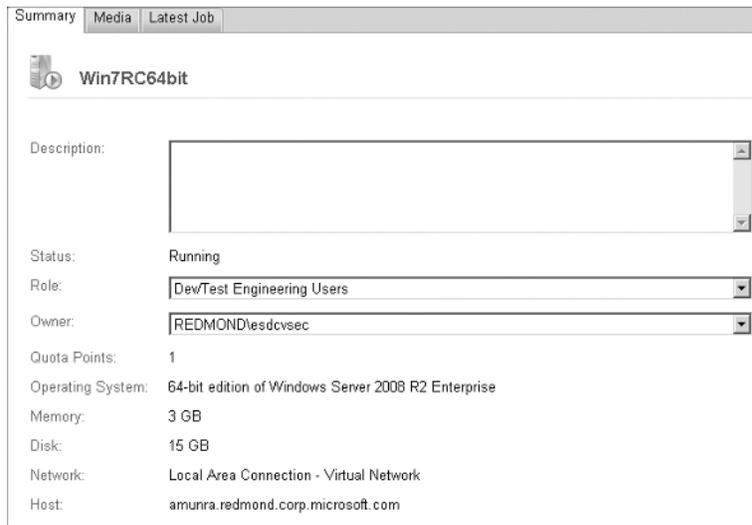
1. Select the virtual machine in the SSP.
2. Click the Properties action.
3. Ensure that you are in the Summary tab.
4. Change the Role selection box to the user role you want to use to manage this virtual machine, as seen in Figure 1.25.

Self-Service Users can also use the VMM Windows PowerShell interface directly and invoke cmdlets as a way to interact with the VMM infrastructure.

FIGURE 1.24
Console connection to a virtual machine



FIGURE 1.25
Changing the user role applied to a virtual machine



Microsoft Virtualization Management

Virtual Machine Manager manages both server virtualization technologies from Microsoft, Windows Hyper-V, and Microsoft Virtual Server. VMM 2007 supported only Microsoft Virtual Server, but with the release of VMM 2008, Hyper-V is supported as well.

MORE ABOUT HYPER-V

Hyper-V, formerly known as Viridian or Windows Server Virtualization, is a hypervisor-based virtualization system that is available both as a role of Windows Server 2008 and as a stand-alone product called Hyper-V Server. Hyper-V is Microsoft's first hypervisor, developed entirely out of a new code base, different than what Microsoft used for Virtual Server. Hyper-V is available on only 64-bit hardware and requires the hardware virtualization option, specifically Intel-VT and AMD-V.

VMM can manage the following:

- ◆ Stand-alone hosts
- ◆ Hosts that are part of a failover cluster (Hyper-V hosts only)
- ◆ Hosts that are in a perimeter network
- ◆ Hosts that are part of a domain that has no established trust with the domain of the VMM server

Virtual Server host clustering is managed by VMM in a cluster-agnostic way. Chapter 5 goes into more detail on managing Windows Hyper-V, and Chapter 6 is about managing Virtual Server with VMM.

HOST GROUPS

All hosts in VMM are organized into host groups, a logical grouping hierarchy that is visible in the VMM Administrator Console. Host groups are completely defined by the administrator based on the most convenient management grouping. Administrators can choose to organize hosts into host groups that represent physical geographical locations, or they can choose to organize hosts into host groups that represent product units or even staging areas in the production cycle (e.g., Testing, Staging, and Production) as seen in Figure 1.26.

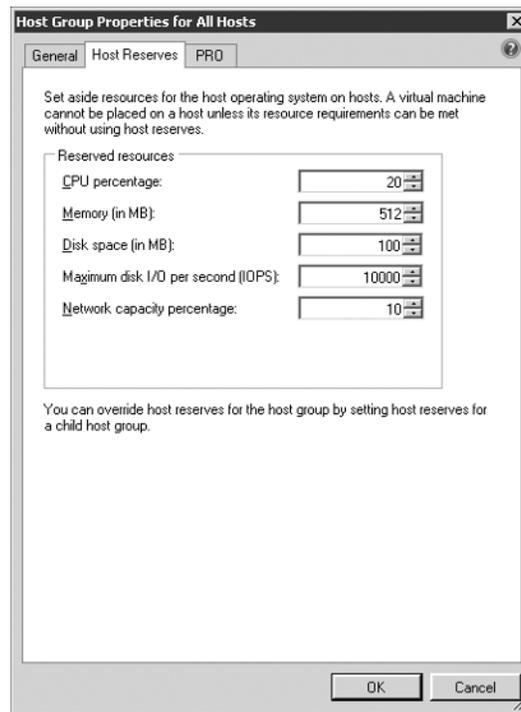
FIGURE 1.26
Host groups in VMM



Multiple sub host groups can also be created to combine different types of schemes. Hosts can be moved from one host group to another through drag-and-drop operations in the Administrator Console in the tree view pane. New host groups can also be created from the same pane. VMM ships with a built-in root host group called All Hosts that cannot be modified. In addition to organizing hosts into a logical hierarchy, host groups offer a few more pieces of functionality:

- ◆ Delegated Administrator and Self-Service User Roles are scoped to host groups.
- ◆ Host reserves that are used in Intelligent Placement can be assigned at the host group level, as seen in Figure 1.27.
- ◆ BITS transfers offer the option of unencrypted transfers, and this option can be enabled at the host group level.
- ◆ PRO settings can be modified per host group.

FIGURE 1.27
Host reserves in host groups



VMware VirtualCenter Management

With VMM 2008, VMM added heterogeneous virtualization support by managing VMware Virtual Infrastructure. VMM can manage stand-alone ESX hosts as well as clustered ESX nodes through the VMware VirtualCenter public web interfaces. VMM does not manage ESX nodes directly. By using this approach, any changes made to the VMware environment through VMM are automatically reflected in VirtualCenter and vice versa, so the two can coexist side by side. VirtualCenter, however, does not provide the ability to manage Hyper-V or Virtual

Server environments. Even though VMM uses VirtualCenter as a proxy to manage ESX, you can add a stand-alone ESX host to an already managed VirtualCenter server through the Add Host global action in VMM. To add a VirtualCenter server, use the Add VMware VirtualCenter Server global action. VMM does not require an agent on the VirtualCenter server in order to manage it.

Figure 1.28 shows the Administrator Console managing an ESX host using the same host group hierarchy seen in the VirtualCenter user interface. Figure 1.29 shows the Virtualization Managers page of the administration view of the VMM Administrator Console, where you can see all the VirtualCenter servers that VMM is managing and their current status.

FIGURE 1.28
Managing ESX hosts

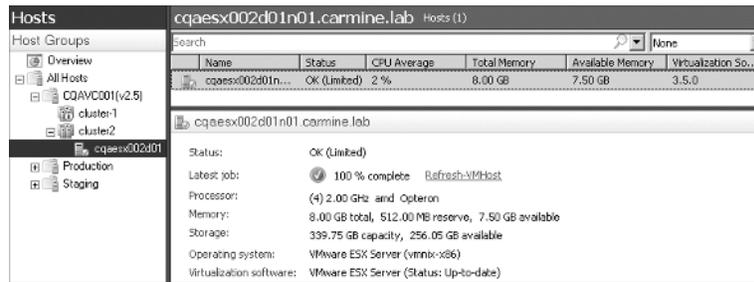
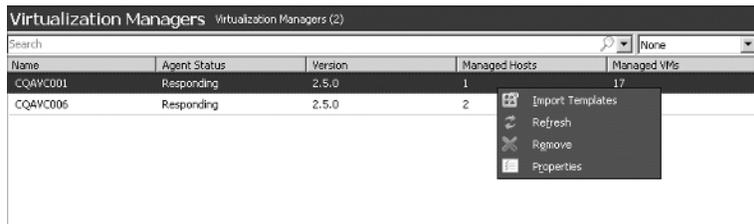


FIGURE 1.29
Virtualization managers
being managed by VMM



Chapter 4 goes into more detail about the support and management of VMware Virtual Infrastructure by VMM.

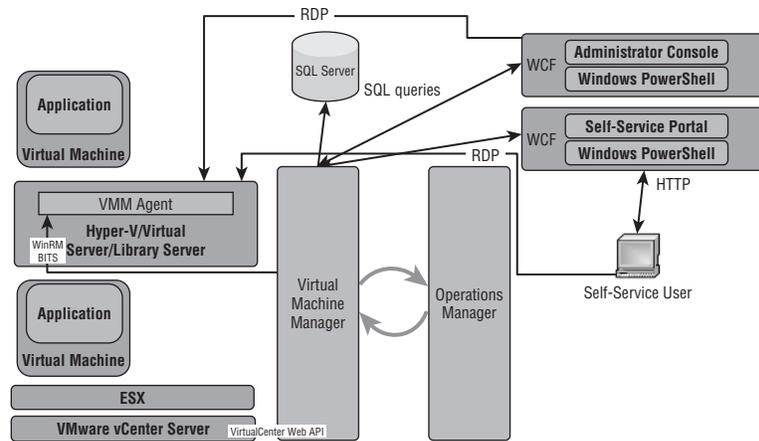
CASE STUDIES

The Virtual Machine Manager team has published a set of case studies on the VMM website at www.microsoft.com/systemcenter/virtualmachinemanager/en/us/case-studies.aspx. These case studies show how Virtual Machine Manager provides a comprehensive management solution for the virtualized datacenter. You can also use the Microsoft Case Study finder at www.microsoft.com/casestudies to find case studies related to Virtual Machine Manager or Hyper-V.

VMM Architecture

Figure 1.1 earlier in this chapter illustrated the high-level architecture of VMM and all its distributed components. Figure 1.30 shows the communication protocols used through the various system components.

FIGURE 1.30
The communication protocols used with the components of Virtual Machine Manager



In the following sections, we will dive into the technical details and architecture of VMM and its components. We will discuss the protocols and ports used for communication among the various VMM components, time-outs that can result from communication protocols, the communication method used for interacting with OpsMgr, the different transfer methods that VMM utilizes, and the way that VMM refreshes information in the environment. In addition, we will discuss the authentication and authorization model of the various VMM components. Role-based administration of VMM is also covered.

Protocols

VMM uses a variety of protocols for connecting to its components. The central hub of communication is the VMM server. The information in this section will aid the coordination with network administrators in opening all the required network ports and adding firewall exceptions for VMM to operate properly. During setup, VMM will properly configure Windows Firewall and create the necessary exceptions for the ports mentioned, which are detailed here:

- ◆ The VMM server communicates with the VMM agents on the Hyper-V host servers, the Virtual Server host servers, and the VMM library servers via Windows Remote Management (WinRM). WinRM is also often referred to as the control channel of communication since VMM does not transfer virtual machine images through WinRM. This communication is always initiated by the VMM server, which polls for data or initiates commands with the other server roles. A default VMM agent is always installed on the VMM server during setup so that the default VMM library role can be created.
- ◆ VMM uses the Background Intelligent Transfer Service (BITS) as the data channel for transferring data from one server role to another.
- ◆ Windows Communication Foundation (WCF) is used for communication between the VMM server and the Administrator Console or PowerShell cmdlets. WCF allows both the Administrator Console and the cmdlets to reside on a server other than the server on which the VMM server role is installed.
- ◆ The VMM server can connect to either a local or a remote SQL server. VMM also offers the option to install SQL Server Express on the same machine where the VMM server setup is being executed.

- ◆ VMM uses the Remote Desktop Protocol (RDP) in two ways to connect to virtual machines and provide a console session to the user:
 - ◆ If the client machine running the Administrator Console or the Self-Service Portal web session is not executing on top of Windows Server 2008 or on top of Windows Vista Service Pack 1 (SP1), then VMM will use standard RDP to connect to the guest operating system inside the virtual machine. In order for this to be feasible, the Virtual Guest Services need to be installed inside the virtual machine and the computer name of the guest operating system needs to be surfaced in VMM.
 - ◆ If the client machine uses either Windows Server 2008 or Windows Vista SP1 or later, then VMM will take advantage of the enhancements in RDP and the Credential Security Service Provider (CredSSP) to connect to the virtual machine via the host operating system. This feature is also known as the RDP Single Port Listener, and it allows VMM to connect to any virtual machine through a host connection without imposing any networking requirements on the VM.
- ◆ For Virtual Server hosts, VMM utilizes VMRC and the ActiveX control for VMRC to give users console access to a VM.
- ◆ When communicating with VMware VirtualCenter, VMM utilizes the public Web Services API for VMware Virtual Infrastructure. Transfer of files from an ESX server to a Windows-based host utilizes HTTPS or SFTP.

CONSOLE CONNECTIONS TO A HYPER-V VIRTUAL MACHINE

Hyper-V will allow only one connection at a time to a virtual machine. If a second connection is attempted, the first connection will be terminated. Virtual Server behaved a little bit differently, giving the administrator the option to enable or disable multiple concurrent VMRC connections to a virtual machine.

Hyper-V and Virtual Server will also create the necessary exceptions for the ports utilized for virtual machine console access. Table 1.1 shows the comprehensive list of ports needed by VMM to function properly.

TABLE 1.1: Default network ports utilized by VMM

VMM COMPONENT	NETWORK PORT	PROTOCOL
VMM server	80	HTTP, WinRM
VMM server	443	BITS
VMM server	8100	WCF
SQL Server	1433	Remote SQL instance
SQL Server	1434	SQL Server Browser service
Windows host or library server	80	HTTP, WinRM

TABLE 1.1: Default network ports utilized by VMM (*CONTINUED*)

VMM COMPONENT	NETWORK PORT	PROTOCOL
Windows host or library server	443	BITS
Windows host	3389	RDP
Hyper-V host	2179	RDP Single Port Listener for Hyper-V or Hyper-V remote connection port
Virtual Server host	5900	VMRC
VMware VirtualCenter Server	443	HTTPS for VI Web Services
VMware ESX host (all versions)	443	HTTPS for VI Web Services
VMware ESX 3.0, 3.5 host	22	SSH for SFTP
Self-Service Portal	80	HTTP (without SSL)
Self-Service Portal	443	HTTPS (with SSL)

It is a recommended practice that during VMM setup you change the default ports for WinRM, BITS, and WCF to something that is unique to your enterprise. Figure 1.31 and Figure 1.32 show the wizard pages you'll use to configure the ports for VMM server setup and for the local agent setup, respectively.

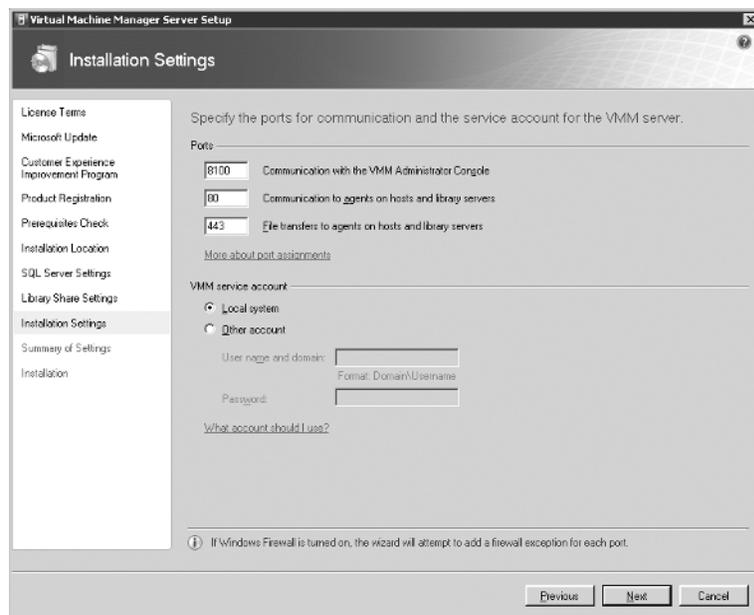
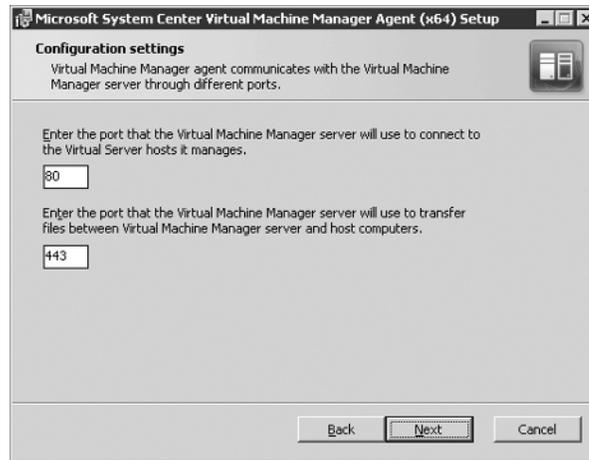
FIGURE 1.31
VMM server port assignment installation settings

FIGURE 1.32
Port settings for local
agent installation



Real World Scenario

CONNECTING TO VIRTUAL MACHINES IN A PRIVATE NETWORK

The administrator for SupServers, a fictional company, has set up a private Active Directory domain environment inside a virtual machine. This domain environment is connected via an internal virtual network to three other virtual machines on the same host server. All four virtual machines comprise a test workload that the company's security officer will use to validate new software that will be introduced to the company. It is important that this workload and the four virtual machines are isolated from the main network and that any potential issues are contained within the virtual environment. The security officer, Daphne, is a VMM Self-Service User and can connect to her virtual machines through the Self-Service Portal user interface.

In order for Daphne to connect to this isolated environment, she has to utilize the Self-Service Portal UI. However, because her virtual machines are not on the corporate network, standard RDP cannot be used for connections. For standard RDP to work, a network connection between the client machine and the virtual machine is necessary. Daphne needs to connect to the portal from a computer running Windows Vista SP1 to utilize the RDP Single Port Listener. This would enable her to connect to the Hyper-V host server, which is on the corporate network, and Hyper-V would redirect the connection to the virtual machine, which is in a private network.

The Self-Service Portal of VMM allows an end user to connect to the portal from a client computer using a browser like Internet Explorer. The end user can then choose to connect to a virtual machine and view the console session.

Now, there are some requirements and advantages of each type of console connection. Here are the requirements for using standard RDP to connect to a virtual machine:

- ◆ The virtual machine has to be connected to an accessible network.
- ◆ The client computer has to be able to resolve the virtual machine's computer name through DNS.
- ◆ The client should have a clear firewall path for the RDP port to each virtual machine.

However, if the Single Port Listener is used, these requirements are not applicable. This is because instead of the RDP connection being routed from the client computer to the virtual machine's guest operating system, the RDP connection is routed from the client computer to the host operating system. This means that only the host computer needs to be in the network and accessible from the client computer (this is already a requirement because VMM has to be able to manage the host computer). This approach includes the following added advantages:

- ◆ You can view the virtual machine boot process, boot into safe mode, or change BIOS settings.
- ◆ You can view the console session of non-Windows operating systems.
- ◆ You can view the console session of virtual machines that don't have the Virtual Guest Services installed.
- ◆ The virtual machine does not need to be connected to any network (this works well for fenced or network-isolated computers).
- ◆ The client needs a clear firewall path for only the Hyper-V remote connection port to each Hyper-V server.

The many advantages of using the Single Port Listener make for a compelling reason to upgrade client computers to the Vista SP1 or Windows Server 2008 or later operating systems.

One way to change the VMM ports is during VMM server setup as per Figure 1.31 (shown earlier). If you are installing the VMM agent locally, make sure the WinRM and BITS ports match with what you specified during the VMM server setup. If your environment requirements change after deployment, the only way to alter the ports used by VMM is by manually modifying a set of Windows Registry entries.

The process for changing the ports through the Windows Registry for WinRM, BITS, and WCF is as follows:

1. Stop the Virtual Machine Manager Windows Service.
2. Open Windows Registry.
3. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager Server\Settings.
4. Change the value of IndigoTcpPort (for WCF), WSMANtcpPort (for WinRM), or BITSTcpPort (for BITS).
5. Ensure that the proper firewall rules exist for communication on the changed ports. If both a hardware and a software firewall are in place in your environment, consult with the system administrator to enable these firewall rules on both types of firewall.
6. Start the Virtual Machine Manager Windows Service.

The preceding process will only change the ports on the VMM server. The Administrator Console and Windows PowerShell cmdlets will not be able to connect to the VMM server until you change the port number to the appropriate value in the connection settings.

For BITS and WinRM, you need to manually edit the same values under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager Agent\Setup on every single host and library server that is managed by VMM. The Windows service to restart for that procedure is Virtual Machine Manager Agent. VMM will stop communicating with the hosts and library servers if the ports are changed on only the VMM

server. To ensure that no interruption of management service occurs, it is recommended that all steps are followed at the same time across the entire environment before restarting all the VMM services.

Windows Remote Management

VMM utilizes WinRM to communicate with the VMM agent on the host and library servers. During the remote agent deployment, VMM will create a WinRM listener on the HTTP port specified during setup.

CHECKING THE STATUS OF THE WINRM LISTENER

From an administrator command prompt, run `winrm enumerate winrm/config/listener` to check the status of the listener created by VMM. To check the rest of the configuration settings for WinRM, run `winrm get winrm/config`.

WinRM was chosen as the communication protocol because of its ability to communicate via HTTP and limit firewall changes, its ability to run without the need for .NET, and for its native support for Windows Management Instrumentation (WMI). When VMM manages Virtual Server, which exposes only a COM interface for management, the local VMM agent implements a set of WMI providers that wrap the functionality of the COM interface. These WMI providers can be invoked remotely from the VMM server via WinRM. In supporting Hyper-V, since the native management interface is WMI, the functionality implemented by the local agent is greatly reduced since all Hyper-V-specific functions are invoked remotely from the VMM server using WMI over WinRM.

Because the P2V process in VMM does not utilize WinRM for the control channel, the appropriate ports need to be opened so that the VMM server can communicate with the source machine using WMI over DCOM. One of the reasons for not requiring WinRM in this scenario is so that the source computer does not have to be altered as a requirement for the P2V process.

Windows Communication Foundation

Windows Communication Foundation (WCF) is the protocol that VMM uses for communicating between all clients and the VMM server. The clients are the VMM Administrator Console, the Windows PowerShell cmdlets for VMM, and the Self-Service Portal web server. Communication is established over a single port via a duplex channel. The clients establish a connection to the VMM server and will keep this connection open for the duration of their session. If at any point in time the connection to the VMM server is lost, the affected client will be disconnected and a new connection will need to be made. In the case of the Administrator Console, it will prompt the user with an error and will have to be reopened.

After the initial connection to the VMM server is made, the clients query for data and execute commands via the private WCF interfaces that VMM exposes on the VMM server. However, VMM also leverages WCF callbacks to push data out to clients. Through WCF callbacks, VMM implements its own internal eventing mechanism that allows it to update all subscribed clients simultaneously with the current state of the system. For example, if a virtual machine changes its state outside VMM from running to stopped, the VMM server will detect that change on the host system using a refresher and through an event will update all clients with the new state of the virtual machine. The VMM eventing infrastructure ensures that if multiple VMM administrators have the Administrator Console open and are working on

VMM simultaneously, they are all viewing an always up-to-date view (i.e., live view) of the virtualized environment (i.e., no VMM administrator will be working with stale data because another administrator has made a change in VMM a few minutes earlier).

Background Intelligent Transfer Service

Background Intelligent Transfer Service (BITS) is the technology that VMM utilizes for transferring data from one server to another. To transfer a virtual machine or any other file from one server to another, VMM has to create a BITS job and initiate a BITS session. The VMM server is always the one to start the BITS job, and all BITS jobs created by VMM have the Foreground priority. VMM has its own implementation of a BITS server residing inside the VMM agent.

In most cases, the VMM server initiates a download of data through BITS (versus an upload). VMM initiates an upload in the following cases:

- ◆ When transferring data to a perimeter network host or a non-trusted domain host
- ◆ When transferring data from a source server during a P2V process

In the case of an upload transfer, the client of the job is the sender of the data and the server of the job is the destination host for the data. For download transfers, the roles are reversed.

In environments where IPsec is already deployed, it might be beneficial to disable the encryption that BITS offers to speed up transfers. VMM enables an administrator to allow unencrypted BITS network transfers in VMM. This property can be changed at the host group level and for each library server.

Operations Manager Connector

VMM 2008 and VMM 2008 R2 have a deeper connection with System Center Operations Manager (OpsMgr) through a connector. A connector is a standard communication method that allows OpsMgr to communicate with external software like VMM. Using this connector, VMM can share data with OpsMgr and provide the full layout of the virtualized environment managed by VMM. For scalability reasons, VMM opens 32 connectors to provide discovery information about the hosts and virtual machines under management.

For the entire environment to be fully managed in OpsMgr and take advantage of all the features and functionality, OpsMgr agents need to be installed on all the hosts and all the virtual machines.

When VMM gets configured to use a specific OpsMgr root management server, a snapshot discovery is initiated, and this will provide all the required information to OpsMgr so that it can start monitoring the environment. VMM will continue to keep the data in OpsMgr in sync and will communicate any changes that result with the addition or removal of hosts.

A snapshot discovery is issued when the Virtual Machine Manager service starts and every 6 hours thereafter. One way to trigger immediate discovery is to reconfigure the OpsMgr connection in VMM through the PowerShell interface.

VMM also uses the connector to retrieve the alerts necessary to generate and surface PRO tips in the VMM Administrator Console. These alerts are retrieved and updated every 60 seconds. When an administrator chooses to implement a PRO tip, VMM will ask OpsMgr to invoke the Recovery action of the PRO tip monitor through the connector.

Role-Based Administration

One of the main new features of VMM 2008 and VMM 2008 R2 over VMM 2007 is the introduction of role-based administration through the use of VMM roles. This feature is also called delegated administration. In VMM 2007, there were only two types of users for VMM,

the administrators and the end users. End users had access only to the Self-Service Portal of VMM, while administrators had access to the Administrator Console. Starting with VMM 2008, with the introduction of roles, VMM provides the capability to designate a user in one of three categories:

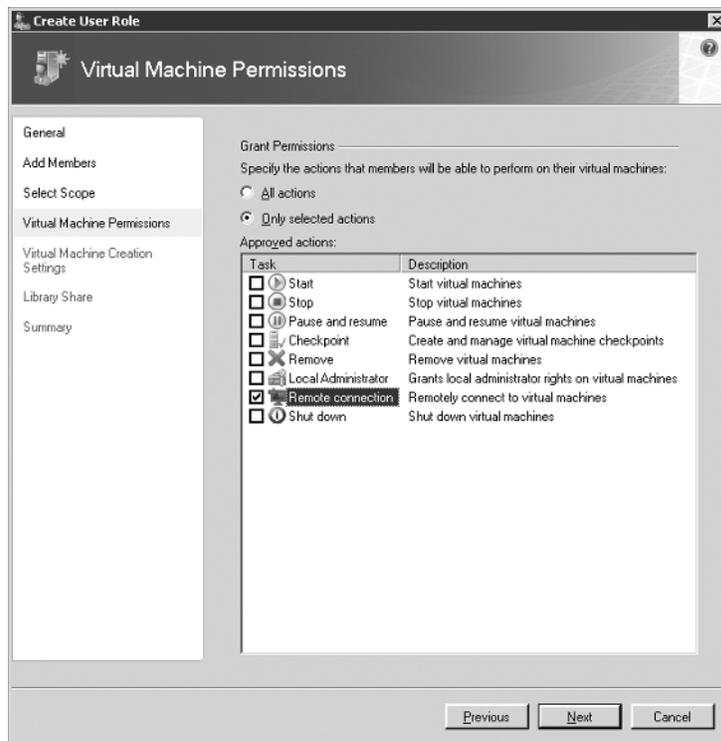
- ◆ Administrator
- ◆ Delegated Administrator
- ◆ Self-Service User

Administrator An administrator has full functionality privileges over the entire VMM environment and can access any virtual machine on any host server. More importantly, an administrator has direct console access to all virtual machines in the system.

Delegated Administrator A delegated administrator can perform all the functions of an administrator; however, access is scoped down to a set of host groups and library servers. Using this role, an administrator can enable a user to fully administer a subset of the VMM environment.

Self-Service User Through the use of the Self-Service User Role, an administrator can enable a set of users to create and manage their own virtual machines within a controlled environment. This controlled environment includes a scoped set of templates and library servers these users can use, a quota point system for creating virtual machines, a set of host groups that these users can use, and a configurable list of privileges for executing virtual machine actions. Figure 1.33 shows the list of privileges that an administrator can grant users.

FIGURE 1.33
End user role virtual machine permissions



In VMM 2008 and VMM 2008 R2, Self-Service Users have access not only to the Self-Service Portal, but also to the Windows PowerShell cmdlets for VMM. When using cmdlets, Self-Service Users will be able to see only the VMM objects they have access to, and they would be able to execute only the cmdlets that the administrator specifically allowed for them in the configuration of the user role.

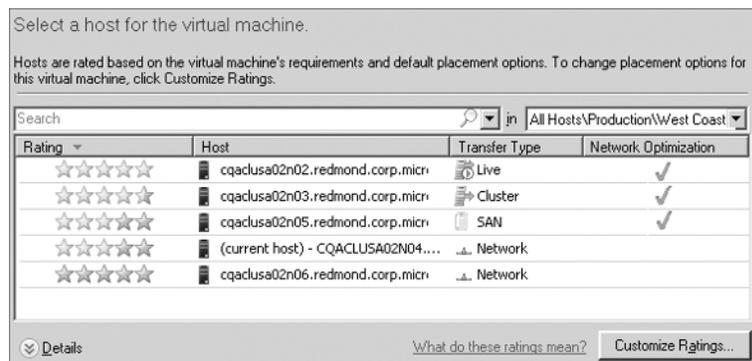
For Hyper-V, VMM will translate the user roles into data that can be consumed by Authorization Manager on the Hyper-V host. VMM will use a local XML file for representing the authorization store for each Hyper-V server. It is highly recommended that no application or user modifies this XML file directly. If any changes are needed to provide access to users, these users need to become a member of a user role in VMM so that the appropriate permissions can be set. A typical customer scenario is to give individual users access to connect to the console of a virtual machine. For this scenario, the recommendation is to create a user role for these virtual machines and enable only the remote connection permission. Access can then be controlled through the Owner property of a virtual machine.

Third-party applications that interface with Hyper-V directly and need access to the Hyper-V environment can create roles and tasks in the root scope of the Authorization Manager store. Properly configured roles and tasks should not interfere with VMM's operations, and VMM will be able to coexist with the third-party application while managing the same Hyper-V server.

Types of Virtual Machine Migration in VMM

Virtual Machine Manager at its core level supports four types of migrations of virtual machines from one server to another. The transfer type that will be used is displayed in the placement wizard page of VMM when you attempt to migrate a virtual machine, as shown in Figure 1.34. The Transfer Type column includes both an icon and text that describes the type of transfer method that VMM will use when migrating the virtual machine to this host. In addition, the Network Optimization column will indicate if this host has support for the new Windows Server 2008 R2 network optimization features (i.e., Virtual Machine Queue and TCP Chimney).

FIGURE 1.34
Placement star ratings and migration transfer types



The four types of virtual machine migration (or transfer types) that VMM supports are as follows:

Quick Migration (also known as cluster transfer) This is the type of migration that is available when you have a highly available virtual machine in a Windows Server failover cluster and you move or fail over the virtual machine from one node of the cluster to another. In the VMM Administrator Console, this is also called a Cluster Migration or Cluster transfer.

SAN migration This type of migration is available when both the source and the destination hosts have access to the same storage infrastructure (i.e., the LUN) and you can transfer the storage from one host to another. This is where NPIV, iSCSI, and VDS are introduced, and we will discuss them in depth in this section. Typically this does not require copying the actual files around, and the SAN infrastructure is used to mask/unmask LUNs, depending upon the direction of the transfer.

Live Migration and VMware VMotion VMotion is available only for VMware ESX hosts when they are properly configured for VMotion. The VMotion technology enables the migration of a virtual machine from one ESX host to another without any user-perceivable downtime. Live Migration is available only for Hyper-V servers that are part of a failover cluster of Windows Server 2008 R2 computers. Just like VMware VMotion, Live Migration enables the migration of a virtual machine from one Hyper-V cluster node to another without any user-perceivable downtime.

Network migration This is the slowest of the migration types since it involves a network copy of the data using BITS from one server to another. The amount of downtime introduced is directly proportional to the size of the data being transferred. With VMM 2008 R2, the Quick Storage Migration (QSM) significantly reduces the downtime for a network migration for Windows Server 2008 R2 host computers. QSM takes a snapshot of the virtual machine and begins the transfer of data to the destination host without requiring the virtual machine to be turned off during the initial and bulky transfer of data.

For SAN migration, the files associated with a virtual machine are not copied from one server to another, thus minimizing the downtime during the VM migration. VMM supports the following SAN infrastructures for SAN-based migration:

- ◆ Fibre Channel
- ◆ iSCSI SANs using the Microsoft Software Initiator
- ◆ N_Port ID Virtualization (NPIV)

SAN transfers are available for only the following scenarios: moving a virtual machine from one host to another, moving a virtual machine from the library to a host, and moving a virtual machine from a host to the library. In all three cases, the servers need to be properly configured and the VM has to reside on SAN storage for the SAN migration option to be available in the Administrator Console. VMM enforces the additional requirement that each SAN LUN only contains one virtual machine. In addition, the LUN has to be configured as a basic disk. Since the unit of migration is a LUN, having two virtual machines on the same LUN would introduce unexpected downtime to the second virtual machine once you start migrating the first one.

VMM requires that automount is disabled on all servers that will be hosts to virtual machines you wish to migrate via SAN. VMM does not provision or manage the SAN infrastructure. LUNs need to be created outside VMM and surfaced to the host servers before VMM can start using them.

To properly configure the environment for SAN transfers, you need to make sure the following components are installed on the various VMM servers:

- ◆ Fibre Channel SAN migrations require each host/library that is part of the SAN to have Virtual Disk Service (VDS) 1.1 or later installed. Windows Server 2008 comes with VDS 2.1 preinstalled and does not need any configuration. The VMM server needs to have the

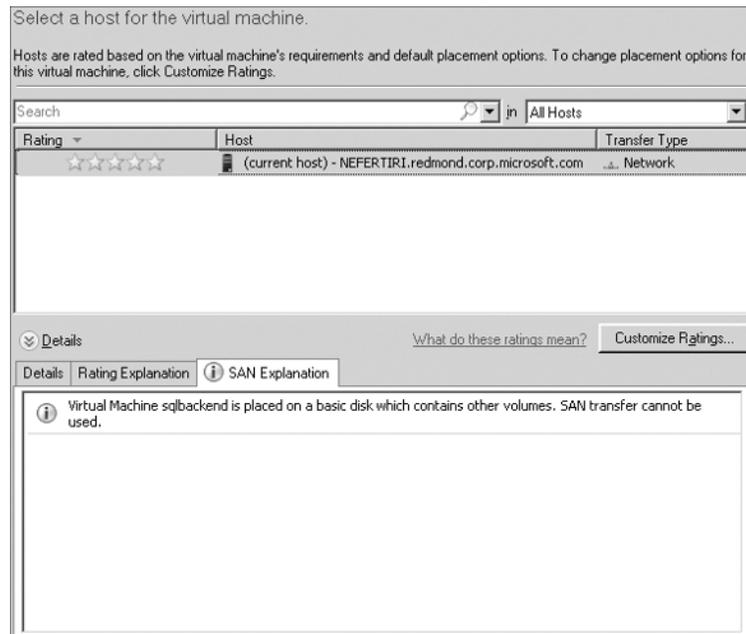
vendor-specific VDS hardware provider installed. Once the proper software is installed on all the nodes, you should be able to see all the providers and subsystems the VMM server has access to from either the Storage Management user interface or the diskraid utility.

- ◆ N_Port Identification Virtualization (NPIV) migrations require each host/library that is part of the SAN to have VDS 1.1 or later installed. Windows Server 2008 comes with VDS 2.1 preinstalled and does not need any configuration. The VMM server needs to have the vendor-specific VDS hardware provider installed.
- ◆ iSCSI SAN migrations require each host/library that is part of the SAN to have VDS 1.1 or later installed. Windows Server 2008 comes with VDS 2.1 preinstalled and does not need any configuration. Each host should also have the latest Microsoft iSCSI Initiator installed in it. The VMM server needs to have Microsoft VDS hardware provider installed.

If your environment utilizes Multipath I/O (MPIO), you must install the MPIO drivers provided by your storage vendor on all the host/library servers that are part of the SAN.

After the software requirements are installed, it is a best practice to create one or two test LUNs and try migrating them from one server to a different server to ensure that they are visible in the Disk Management user interface. Once you create a virtual machine on one of these test LUNs, open the Virtual Machine Manager migration wizard to ensure that the placement page of VMM correctly shows a SAN transfer as being available. If for some reason a SAN transfer is not available, VMM will have details in the SAN Explanation tab to explain the rationale behind the unavailability of SAN migration, as shown in Figure 1.35.

FIGURE 1.35
SAN transfer explanation



SAN migration plays a big role in a Desktop Virtualization (or VDI) environment because of its ability to do rapid migrations of virtual machines from one server to another. In a typical customer scenario, hundreds of users could be associated with a VDI solution. However, the

hosts might not have enough capacity to keep all the virtual machines running at all times for all users. To load balance resources dynamically based on load, SAN migration can play a big part in migrating the resources in the smallest amount of time possible, thus keeping the downtime introduced by the migration under customer SLA requirements. With Windows Server 2008 R2 and failover clustering, Live Migration makes this scenario even more potent, allowing you to dynamically load balance resources without impacting the services of your users.

When you're using VMM to provision or migrate virtual machines, it automatically detects which types of migration are available based on the capabilities and connectivity between the host and target servers. By default, VMM uses the most efficient form of transfer, but this can be overridden by the administrator.

Authentication and Authorization Model

When talking about authentication and authorization, the main questions that administrators have are related to how VMM authenticates and authorizes hosts and how users are authorized to use the VMM interfaces. Protecting the hosts and the VMs is tantamount to having a successful virtualization deployment. In addition to properly authorizing the control channel and the APIs, VMM ensures that the data channel is protected. The data channel is utilized during the migration of virtual machines from one computer to another.

In the following sections, we will cover the authentication and authorization that is used for the different types of hosts that can be managed in VMM. Self-Service Portal authentication and authorization is also covered.

HOST SERVER AUTHENTICATION AND AUTHORIZATION

VMM manages Windows-based hosts in three different ways based on the environment requirements. Authentication and authorization of VMware ESX hosts is covered in Chapter 4.

Trusted domain hosts If hosts are part of the same domain as the VMM server, or are part of a domain that has a full two-way trust with the domain of the VMM server, VMM manages them as trusted domain hosts. In the case of trusted domain hosts, VMM relies on WinRM and Kerberos to do both the authentication and the authorization when communicating with the hosts. The Virtual Machine Manager service account (either a domain user account or local system) is also an administrator on all host servers, ensuring that all WinRM commands are properly authorized at the host level. Transfers of files over BITS are encrypted by default because files are transferred via the HTTP protocol over SSL.

If you have deployed IPsec in your environment, there will be a double encryption of the data transferred over BITS, potentially slowing down the transfer operation because of the amount of CPU spent on encrypting and decrypting data. VMM 2008 R2 includes a new feature that gives the administrator the option to disable BITS encryption for host groups and for library servers.

Non-trusted domain hosts If hosts are part of a domain that is not trusted by the domain of the VMM server, VMM manages them as non-trusted domain hosts. In the case of non-trusted domain hosts, authorization and authentication is done using NTLM and the random username/password that VMM creates as part of deploying the agent to these types of hosts. You can find this local account that VMM creates on your host by looking for a username that is prefixed with *VMM*, followed by an alphanumeric random number. This account will have a secure strong password assigned to it that is not user visible and only VMM would know it. BITS transfers in this environment are secured through a certificate that VMM creates and adds in the trusted root of the VMM server and the managed host.

VMM does not currently support a public key infrastructure. VMM will create the certificates and add them to the trusted root of the host and to the trusted root of the VMM server. VMM also will not support managing a Windows failover cluster for a non-trusted domain host or for a perimeter network host.

Perimeter network hosts If hosts are in a workgroup mode or part of a perimeter network (e.g., DMZ), VMM manages them as perimeter network hosts. Authentication and authorization in this case is the same as for non-trusted domain hosts. VMM can manage such a host either by IP address or by the local computer name. Managing by the local computer name will require the name to be resolvable by DNS when the VMM server tries to access the host. VMM does not allow the management of a host that is not part of the domain unless that host is managed as a perimeter network host.

SELF-SERVICE PORTAL AUTHENTICATION AND AUTHORIZATION

The Self-Service Portal and its users have their own authentication and authorization model. End users can connect to the portal and get authenticated in two different ways.

Anonymous forms-based authentication In this case, the administrator has not set up any authentication in IIS and the VMM Self-Service Portal site will ask end users for their credentials before they log in. Users can select the option for VMM to store their credentials for the duration of the session. This functionality has a couple of benefits: In environments where the Self-Service Portal client is running on a machine with no domain connectivity, VMM is able to propagate the credentials stored to the RDP protocol for displaying the virtual machine console. Without stored credentials, the end user would be challenged for credentials every time a new connection to a VM is necessary. This form of authentication is particularly useful when the client machines are not members of the domain or when the currently logged-on user is not the same user that owns the virtual machines in VMM.

Windows Integrated Authentication An IIS administrator can set up Windows Integrated Authentication such that when a domain user visits the Self-Service Portal, IIS is able to utilize single sign-on and pass the credentials to your site. This is the recommended way of setting up the Self-Service Portal. RDP connections to virtual machines from the SSP will utilize the currently logged-on user's credentials. If these credentials are not authorized for the console connection to the virtual machine, the user will be challenged for authentication by RDP.

If the Self-Service Portal web server is not residing on the same computer as the VMM server, a domain administrator needs to ensure that constrained delegation is set up in Active Directory for this computer. This means that the IIS web server needs to be trusted for delegation via Kerberos only to the host service type on the VMM server. If the VMM server is not running as a local system, you would need to create an SPN for the domain user under which the Virtual Machine Manager service runs and then use that same domain user account when setting up the trust for delegation from the IIS server to the VMM server. The requirements around constrained delegation and the SSP was covered in more detail earlier in this chapter in the section "Virtual Machine Manager Self-Service Portal."

In both authentication cases, when the VMM cmdlets on the web server get to execute, they execute under the credentials of the user who logged into the portal. Once VMM authenticates this user as a valid user role user, VMM will create a connection to the VMM server for this user and properly authorize them for the objects and commands they have access to.

Refreshers

Virtual Machine Manager periodically collects information from the virtualization hosts and the library servers and compares them with knowledge that already exists in the VMM database. Any changes that are detected from the hosts or the library servers are updated in the VMM database. For every change that is updated in the VMM database through a refresh, VMM will create an audit log in the jobs view of the Administrator Console. These operations are executed through a set of system jobs called refreshers. The following sections describe all the refreshers in VMM, their intervals, and the data they refresh. In general, even though host-based refreshers say they execute every 30 minutes, not all the refreshers execute at once for all hosts. VMM uses a staggered approach of refreshing hosts to evenly spread the consumption of VMM Server resources.

Refresher times are customizable, but the VMM team has not made that information public as it can have deep performance and operational impact to the virtualized environment. Generally speaking, users should not notice the refreshers when navigating the user interface, and in all cases, users can manually refresh the status of an object if information seems to be reported inaccurately.

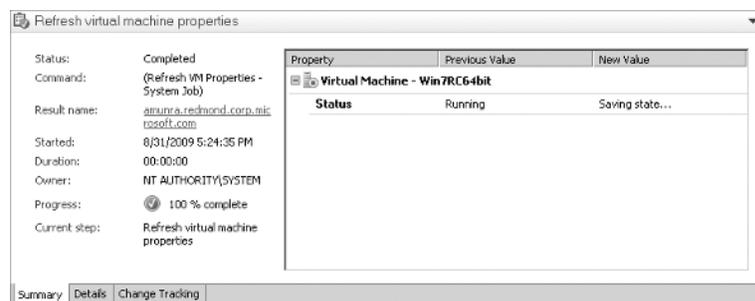
VIRTUAL MACHINE PROPERTIES REFRESHER

This is also called the Virtual Machine Light Refresher. It runs every 2 minutes on every host and it performs the following operations:

- ◆ Checks the host for successful connections through WinRM
- ◆ Checks the status of all the virtual machines residing on that host
- ◆ Marks a virtual machine as missing if it no longer exists on the host
- ◆ Imports newly discovered virtual machines from the host if they don't exist in VMM

Figure 1.36 shows an update to a virtual machine that was detected and audited through the Virtual Machine Properties Refresher.

FIGURE 1.36
Virtual Machine
Properties Refresher



VIRTUAL MACHINE REFRESHER

This is also called the Virtual Machine Heavy Refresher because it does a more extensive refresh than the previous refresher. It runs every 30 minutes on every host and it performs the following operations:

- ◆ Refreshes all the virtualization information for all virtual machines on the host. This includes but is not limited to virtual machine settings, virtual disk drives, storage

information, DVD information, floppy drives, networking information, and clustering information for highly available virtual machines.

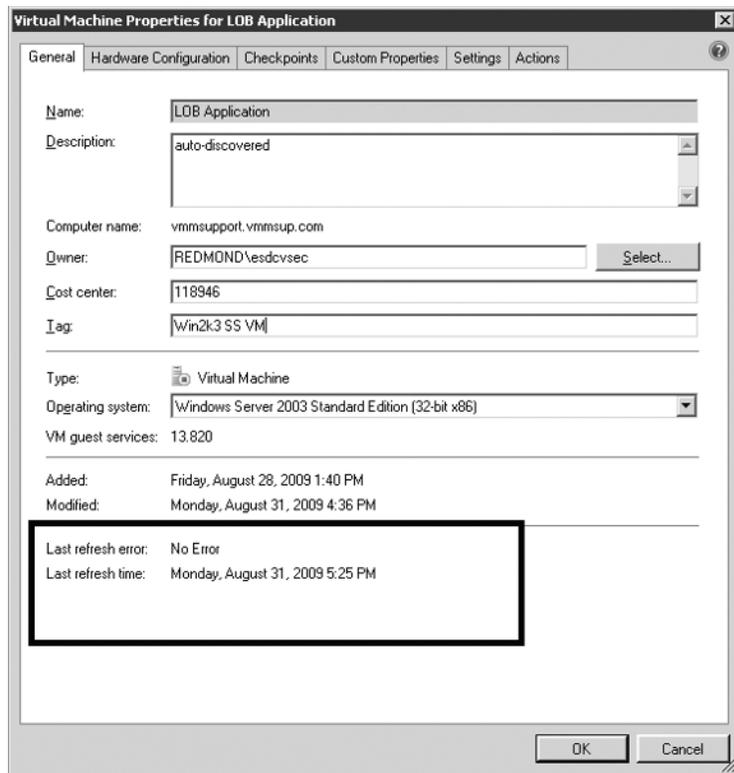
- ◆ Refreshes all the Fibre Channel, iSCSI, or NPIV storage information for each virtual machine.
- ◆ Refreshes all snapshot information and differencing disk information for each virtual machine.

The Virtual Machine Refresher can also be invoked for a specific virtual machine two more ways:

- ◆ Using the Refresh-VM Windows PowerShell cmdlet
- ◆ Selecting a virtual machine in the virtual machines view of the Administrator Console

The Virtual Machine Refresher status can be checked for a virtual machine through the virtual machine properties in the Administrator Console. As seen in Figure 1.37, you can check the last refresh time and the last refresh error.

FIGURE 1.37
Virtual Machine
Refresher properties



HOST REFRESHER

The Host Refresher runs every 30 minutes on every host and it performs the following operations:

- ◆ Updates virtualization host properties and status
- ◆ Updates physical disks and SAN information
- ◆ Updates networking information like physical NICs and virtual switches

The Host Refresher will not update any state information for hosts that are in maintenance mode in VMM. The Host Refresher can also be invoked for a specific host two more ways:

- ◆ Using the `Refresh-VMHost` Windows PowerShell cmdlet
- ◆ Selecting a host in the tree view pane and choosing the Refresh action in the Administrator Console

LIBRARY REFRESHER

The Library Refresher runs on a user-configurable schedule (the default is 1 hour and the maximum is 336 hours) that can be customized from the administration view of the Administrator Console. This refresher can be turned off completely. It performs the following operations for all library servers:

- ◆ It updates the library shares that are under management in VMM.
- ◆ For each library share, it finds new library objects, detects changes in existing objects, and marks objects as missing if they can no longer be found on a library share.
- ◆ It finds and imports any offline or stored virtual machines in the library that were not already under management.
- ◆ For each library object, it marks it with a VMM-specific globally unique identifier (GUID). This VMM GUID is specified in an alternate data stream of the physical file.

The Library Refresher can also be invoked for a specific library server two more ways:

- ◆ Using the `Refresh-LibraryShare` Windows PowerShell cmdlet to refresh a specific library share
- ◆ Selecting a library server or a library share in the tree view pane and choosing the Refresh action in the Administrator Console.

CLUSTER REFRESHER

The Cluster Refresher runs every 30 minutes and it performs the following operations for all clusters:

- ◆ Refreshes all cluster-related properties that are displayed in Virtual Machine Manager, including available storage for creating new highly available virtual machines
- ◆ Flags newly added cluster nodes that have not been associated with VMM
- ◆ Flags removed cluster nodes

The Cluster Refresher can also be invoked for a specific cluster two more ways:

- ◆ Using the Refresh-VMHostCluster Windows PowerShell cmdlet
- ◆ Selecting a cluster in the tree view pane and choosing the Refresh action in the Administrator Console

PERFORMANCE REFRESHER

The Performance Refresher runs every 9 minutes on every host or whenever there is any state changing operation on the VM (e.g., start/stop/save/etc.). It collects performance counter information for both the virtualized hosts and all the virtual machines that reside on them.

VIRTUALCENTER REFRESHER

The VirtualCenter Refresher runs every 30 minutes and it performs the following operations for all VirtualCenter servers:

- ◆ Refreshes VirtualCenter properties
- ◆ Refreshes the VMware ESX hosts that are managed by this VirtualCenter
- ◆ Refreshes resource pool information
- ◆ Refreshes the hierarchical structure of folders and datacenter objects from VirtualCenter

The VirtualCenter Refresher can also be invoked for a specific VirtualCenter server two more ways:

- ◆ Using the Refresh-VirtualizationManager Windows PowerShell cmdlet
- ◆ Selecting a VirtualCenter server in the Virtualization Managers page of the Administrator Console and choosing the Refresh action.

USER ROLE REFRESHER

The User Role Refresher runs every 30 minutes and updates user role properties for each host. If, for example, new domain users are added to a Self-Service User Role and the Remote Connection privilege is enabled, the User Role Refresher will ensure that these domain users have the appropriate access in the Authorization Manager store of Hyper-V to be able to remotely connect to the virtual machines through the RDP Single Port Listener.

PRO TIPS REFRESHER

The PRO Tips Refresher runs every minute and it looks for PRO-enabled alerts in OpsMgr that need to be surfaced in VMM as PRO tips. It also reconciles the PRO tips in the VMM database against the data that is brought back from OpsMgr.

TROUBLESHOOTING ISSUES WITH REFRESHERS

If any product issue is caused by the refreshers (information is not properly updated, refreshers are running for a long time, refreshers are consuming too many resources, etc.), contact Microsoft Customer Service and Support (CSS). CSS will collect additional data from your environment and will work with you to troubleshoot and fine-tune the refreshers and their intervals as needed. They will then closely monitor your environment to prevent any side effects from modifying the refreshers and to ensure that VMM is functioning as expected.

Time-Outs

Virtual Machine Manager has two main time-outs that could possibly surface in customer environments:

WinRM operation time-out When a WinRM time-out occurs, there is a generic error code that is associated with the failed VMM job that indicates that the operation took too long to complete on the server. The default time-out is 5.5 minutes for VMM 2008 R2 (the default time-out was 2 minutes for VMM 2008); when this time-out triggers, it is a good indication that the host machine is overloaded with operations and could not complete the request in time. The recommendation to the user is to retry the operation after the host machine is in a better condition in terms of resources (e.g., CPU).

WCF operation time-out When a WCF time-out occurs, the VMM Administrator Console or the PowerShell cmdlets will lose their connection to the VMM server. The only way to identify that this loss of connectivity was due to the WCF time-out being exceeded is to check the VMM trace logs and look for a time-out exception from WCF. WCF might exceed the default 5.5-minute time-out because of memory or CPU pressure either on the VMM server or on the machine running the Administrator Console or the VMM cmdlets. (The 5.5-minute time-out is a new VMM 2008 R2 feature. In VMM 2008, the time-out was set at 2 minutes.) Such errors could also occur if the environment scales beyond the published guidelines of 400 hosts and 8,000 virtual machines or if the hardware being used does not conform to the minimum hardware requirements for running VMM.

To change either of these two time-outs, follow these steps as necessary:

1. Go to the VMM server computer.
2. Open the Registry key HKLM\Software\Microsoft\Microsoft System Center Virtual Machine Manager Server\Settings.
3. Modify the value of IndigoSendTimeout to 500. This value is in seconds and the default in VMM 2008 R2 is 330 seconds. The default value for the time-out was lower in previous versions of VMM.
4. Restart the Virtual Machine Manager Windows Service on this computer.
5. Go to the client computer running the VMM Administrator Console that is exhibiting WCF time-out issues.
6. Open the Registry key HKLM\Software\Microsoft\Microsoft System Center Virtual Machine Manager Server\Settings and modify the value of IndigoSendTimeout to 500.
7. Close the Administrator Console and launch it again.
8. Go to the VMM agent computer(s) that is exhibiting WinRM time-out issues.
9. Open the Registry key HKLM\Software\Microsoft\Microsoft System Center Virtual Machine Manager Server\Settings and modify the value of IndigoSendTimeout to 500.
10. Restart the Virtual Machine Manager Agent Windows Service on this computer.

The Bottom Line

Identify and explain the components in the VMM architecture. Virtual Machine Manager has a distributed system architecture that administrators need to understand well before deploying VMM in their virtualized environment. Knowing the architecture of VMM gives you the opportunity to make educated choices during deployment of the various VMM components.

Master It Name the different components of Virtual Machine Manager.

Which VMM components can reside on a separate computer from the VMM server?

Name four new features of VMM 2008 R2.

Determine the ports and protocols required for communication between the various VMM components. Being able to identify the different ports and communication protocols used by VMM makes it easier to talk to the network administrator and plan for a secure network.

Master It Name the differences between regular RDP and the RDP Single Port Listener for Hyper-V.

What is the protocol that VMM uses for transferring virtual machine images from one server to another?

Describe the differences between the console access for Hyper-V and the console access for Virtual Server.

Determine the various roles and privileges of VMM. VMM allows an administrator to define a variety of roles and privileges for delegated administrators and end users. Choosing the correct user roles and delegating access to these users will ease the burden on the administrator and allow users to be self-sufficient.

Master It Name the different user roles that VMM allows you to create.

What are the differences between a delegated administrator and a regular VMM administrator?

Can end users get console access to a virtual machine?

What are the interfaces that end users can utilize to access VMM?

Explain the differences of the migration options offered in VMM. Understanding the different migration options offered in VMM allows an administrator to properly configure their environment (from a hardware and software perspective). Such a configuration will take advantage of faster migration methods and minimize downtime of a VM.

Master It What are the different transfer types that VMM utilizes?

Which is the fastest transfer type?

If you receive a zero-star rating for a host, how would you find out what is causing this result?

Describe the authentication methods between VMM and hosts. Virtual machines are running the same type of critical workloads as physical machines. The need to secure the data in these VMs is even more important because everything is contained in a collection of a couple of files. When virtual machines move from one host to another, it is important to understand the authentication methods used to secure your data.

Master It What encryption method does VMM use when transferring data across hosts in a trusted domain?

Are transfers of data from a trusted domain to a perimeter network host secure?

Under what circumstances is constrained delegation required for the Self-Service Portal?

