Microsoft

MCTS EXAM

70-652

Includes coverage of:

- MCTS Exam 70-403
- Hyper-V™ in Windows Server 2008 R2

Configuring Windows Server® Virtualization

Nelson Ruest,
Danielle Ruest,
and GrandMasters

SELF-PACED

Training Kit

How to access your CD files

The print edition of this book includes a CD. To access the CD files, go to http://aka.ms/626799/files, and look for the Downloads tab.

Note: Use a desktop web browser, as files may not be accessible from all ereader devices.

Questions? Please contact: mspinput@microsoft.com

Microsoft Press

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Control Number: 2009928206

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 QWE 4 3 2 1 0 9

Distributed in Canada by H.B. Fenn and Company Ltd.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at www.microsoft.com/mspress. Send comments to tkinput@microsoft.com.

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

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

Acquisitions Editor: Ken Jones
Developmental Editor: Laura Sackerman
Project Editor: Denise Bankaitis
Editorial Production: Christian Holdener, S4Carlisle Publishing Services
Technical Reviewer: Rodney Buike; Technical Review services provided by Content Masters, a member of CM Group, Ltd.
Cover: Tom Draper Design

Body Part No. X15-66454

Exam 70-652: Configuring Windows Server Virtualization

OBJECTIVE	LOCATION IN BOOK
INSTALLING HYPER-V	
Select and configure hardware to meet Hyper-V prerequisites.	Chapter 1, Lessons 1, 2, and 3
Configure Windows Server 2008 for Hyper-V.	Chapter 1, Lesson 2 Chapter 2, Lessons 1 and 2
Configure Hyper-V to be highly available.	Chapter 3, Lesson 1
CONFIGURING AND OPTIMIZING HYPER-V	
Manage and optimize the Hyper-V Server.	Chapter 3, Lesson 3 Chapter 4, Lesson 2 Chapter 7, Lesson 1 Chapter 8, Lessons 1 and 2
Configure virtual networking.	Chapter 2, Lesson 3
Configure remote administration.	Chapter 3, Lesson 2
DEPLOYING VIRTUAL MACHINES	
Migrate a computer to Hyper-V.	Chapter 6, Lesson 1
Create or clone a virtual machine.	Chapter 4, Lesson 1 Chapter 5, Lesson 2
Create a virtual disk.	Chapter 4, Lesson 2
Manage templates, profiles, and the image library by using SCVMM 2008.	Chapter 5, Lessons 1 and 2
MANAGING AND MONITORING VIRTUAL MACHINES	
Monitor and optimize virtual machines.	Chapter 7, Lesson 1 Chapter 10, Lesson 1
Manage virtual machine settings.	Chapter 4, Lessons 1 and 2
Manage snapshots and backups.	Chapter 9, Lesson 1
Configure a virtual machine for high availability.	Chapter 10, Lesson 1

Exam Objectives The exam objectives listed here are current as of this book's publication date. Exam objectives are subject to change at any time without prior notice and at Microsoft's sole discretion. Please visit the Microsoft Learning Web site for the most current listing of exam objectives: *http://www.microsoft.com/learning/en/us/exams/70-652.mspx*.

Exam 70-403: Configuring System Center Virtual Machine Manager 2008

OBJECTIVE	LOCATION IN BOOK
INSTALLING SCVMM	
Install SCVMM server components	Chapter 3, Lesson 2
Install administrator console	Chapter 3, Lesson 2
Install self-service portal	Chapter 5, Lesson 2
Install PRO tips	Chapter 6, Lesson 1
ADMINISTRATING SCVMM	
Configure user roles	Chapter 8, Lesson 2
Setup self service	Chapter 5, Lesson 2
Maintain VMM library	Chapter 5, Lesson 1
Configure hosts	Chapter 3, Lesson 2
Monitor jobs	Chapter 3, Lesson 2
MAINTAINING AND MONITORING VMs	
Configure VM hardware	Chapter 5, Lesson 1
Manage virtual machine checkpoints and patches	Chapter 5, Lesson 1
Monitoring and reporting VMs	Chapter 3, Lesson 2
DEPLOYING AND MIGRATING VMs	
Convert from physical or virtual platforms	Chapter 6, Lesson 1
Move VMs between hosts	Chapter 6, Lesson 1
Deploy VMs	Chapter 6, Lesson 1
Deploy a High Availability VM	Chapter 3, Lesson 2

This book is dedicated to the IT professionals who take the time to become virtualization professionals and resource pool administrators. We hope you will find this guide useful in your studies and in your efforts to improve virtual infrastructure deployments.

—Danielle and Nelson

Contents

Acknowledgments

We want to thank Ken Jones and Laura Sackerman at Microsoft Press for giving us the opportunity to write this great book. We’ve been working with Hyper-V for a long time and we are very pleased to share our knowledge in this way.

We would like to thank David Greschler and Edwin Yuen from the Microsoft Integrated Virtualization Strategy team for all their help and assistance. We would also like to thank Symon Perryman from the Microsoft Clustering and High Availability team for his help in testing failover clusters with Hyper-V. And a great thank you to Rodney Buike, IT Pro Advisor from Microsoft Canada for his help in the technical review.

Thanks must go to Lisa Kreissler and Richard Kobylka of GrandMasters for supporting us throughout this project. Finally, thanks to the Microsoft Press production team for their great work in helping us complete this book.

Introduction

This training kit is designed for IT professionals who plan to take the Microsoft Certified Technical Specialist (MCTS) Exam 70-652: Windows Server Virtualization, Configuring. The primary objective of this exam is to certify that architects know how to deploy and manage an efficient virtualization solution. We assume that before you begin using this kit, you have spent at least three years working with IT infrastructures. We also assume that you have worked on different phases of virtualization deployment projects, including design, deployment, and post-production/maintenance. The Preparation Guide for Exam 70-652 is available at *http://www.microsoft.com/learning/exams/70-652.mspx*.

The labs in this training kit will use Microsoft Windows Server 2008 Enterprise edition. If you do not have access to this software, you can download a 180-day trial of Microsoft Windows Server 2008 through *http://www.microsoft.com/windowsserver2008/en/us/trial-software.asp*.

By using this training kit, you will learn how to do the following:

- Select and configure hardware to meet Hyper-V prerequisites.
- Configure Windows Server 2008 for Hyper-V.
- Configure Hyper-V high availability.
- Configure and optimize Hyper-V.
- Deploy virtual machines.
- Manage and monitor virtual machines.
- Implement a virtual machine management environment.
- Protect and secure virtual machines.
- Automate virtual machine management.

MORE INFO **VIRTUALIZATION TEAM BLOG**

Note that the Virtualization team blog is also a great source of information in support of the exam. Find it at *http://blogs.technet.com/virtualization/default.aspx*.

UPDATE ALERT **UPDATE ALERTS AND COVERED EXAMS**

You'll also find special notes called "Update Alerts" within this guide. These updates provide information about new features and functionality that were added to Hyper-V and other tools after their initial release. This includes the R2 releases of the products covered in this guide. This information is mostly available in Update Alerts since it is not included in the original 70-652 exam.

In addition, since there are no Microsoft Press Training Kits for exams 70-693: Windows Server Virtualization Administrator or 70-403: System Center Virtual Machine Manager 2008, Configuring, this guide attempts to perform triple duty by adding content in support of these exams along with the content for exam number 70-652.

Hardware Requirements

Because of the nature of virtualization technologies, you will require access to hardware resources to complete the exercises in each lab. To complete the practice exercises, the system requirements include:

- Two computers including the following features:
  - x64 processor with hardware-assisted virtualization and a minimum of 4 GB of RAM.
  - Two network interface cards (NICs) on each computer.
  - One computer will run the Windows Server 2008 Full Installation.
  - One computer will run the Windows Server 2008 Server Core Installation.
  - Both computers will be joined to the Contoso.com domain.
- You need a preinstalled Domain Controller running Windows Server 2008 with the Active Directory Domain Services (AD DS) role on a separate virtual machine or physical machine. It should be a single domain forest named Contoso.com and the name of the server should be Server01.
- One workstation running Windows XP SP3 or Windows Vista SP1 must be joined to the Contoso domain.
- Three external USB disk drives with a minimum of 100 GB.
- Ideally, you will have access to an MSDN or TechNet subscription to obtain source ISO files, but once again, the instructions in this guide work around this issue by targeting evaluation versions of software products that are in either ISO or EXE format. Wherever possible, the guide directs you to download preconfigured virtual machines in VHD format.

Table 1 lists the computer names, roles, and IP addresses required for the completion of the practice exercises.

IMPORTANT **ACCESS RIGHTS FOR THE PRACTICES**

To facilitate the exercises in this guide, all activities are performed with domain administrator access rights. However, note that in production environments you should always use the least privilege approach. This approach is detailed in Chapter 6, "Securing Hosts and Virtual Machines."

TABLE 1 Computer Role and IP Address

COMPUTER NAME	ROLE	IP ADDRESS
Server01	Domain Controller	192.168.0.5
	Subnet mask	255.255.255.0
	Default gateway	192.168.0.1
ServerFull01	x64 Windows Server 2008 Enterprise edition	192.168.0.6
		192.168.0.7
ServerCore01	x64 Windows Server 2008 Enterprise edition	192.168.0.8
		192.168.0.9
Hyper-V Cluster	Temporary requirement	192.168.0.10
SSCVMM01	x64 Windows Server 2008 Enterprise edition	192.168.0.11
MAP Workstation	Windows Vista or Windows XP SP2	192.168.0.12

Because of the prohibitive cost of shared storage, the instructions in this guide work around this issue but still allow you to view and test all of the aspects of Hyper-V required for the exam. However, if you have access to some form of shared storage, your experience will be more complete.

Software Requirements

For all the exercises, you will need to download several software products and updates. The following list provides links for all the required major downloads. Required updates are indicated in each exercise.

1. VHD images of Windows Server 2008, Full installation and Server Core installation *http://www.microsoft.com/windowsserver2008/en/us/trial-software.aspx*.
2. Microsoft Assessment and Planning tool *http://www.microsoft.com/downloads/details.aspx?familyid=67240B76-3148-4E49-943D-4D9EA7F77730*.

3. Windows Server 2008 Evaluation Copy
http://www.microsoft.com/windowsserver2008/en/us/trial-software.aspx.
4. Remote Server Administration Tools (RSAT) (KB941314)
http://support.microsoft.com/default.aspx/kb/941314.
5. Hyper-V RTM version update (KB950050):
Update for Windows Server 2008, 32-bit editions
http://www.microsoft.com/downloads/details.aspx?FamilyId=6F69D661-5B91-4E5E-A6C0-210E629E1C42.
Update for Windows Server 2008, 64-bit editions
http://www.microsoft.com/downloads/details.aspx?FamilyId=F3AB3D4B-63C8-4424-A738-BADED34D24ED.
6. Hyper-V Manager on Windows Vista Service Pack 1 or later (KB952627)
http://support.microsoft.com/kb/952627.
7. Virtual Machine Manager Configuration Analyzer
http://www.microsoftpressstore.com/title/9780735626799.
Microsoft Baseline Configuration Analyzer (MBCASetup64.msi)
http://www.microsoftpressstore.com/title/9780735626799.
8. System Center Virtual Machine Manager VHD
http://www.microsoft.com/downloads/details.aspx?FamilyID=4a27e89c-2d73-4f57-a62c-83afb4c953f0&DisplayLang=en.
9. System Center Virtual Machine Manager 2008 Evaluation Copy
http://technet.microsoft.com/en-us/evalcenter/cc793138.aspx.
10. Windows Server 2008 Enterprise edition Evaluation ISO
http://www.microsoft.com/downloads/details.aspx?FamilyID=13C7300E-935C-415A-A79C-538E933D5424&displaylang=en.
11. OpsMgr 2007 Evaluation Copy
http://www.microsoft.com/downloads/details.aspx?familyid=C3B6A44C-A90F-4E7D-B646-957F2A5FFF5F&displaylang=en.
12. OpsMgr SP1
http://www.microsoft.com/Downloads/details.aspx?FamilyID=ede38d83-32d1-46fb-8b6d-78fa1dcb3e85&displaylang=en.
13. OpsMgr Management Packs
http://www.microsoftpressstore.com/title/9780735626799.
14. SCVMM 2008 Management Pack for OpsMgr
http://www.microsoft.com/downloads/details.aspx?FamilyID=d6d5cddd-4ec8-4e3c-8ab1-102ec99c257f&DisplayLang=en.

15. VMDK to VHD Converter
http://vmtoolkit.com/files/default.aspx.

16. Optional: Windows Server 2008 Failover Cluster Manager Console Update for x64 edition (KB951308)
http://support.microsoft.com/kb/951308.

17. Hyper-V with SCVMM updates for Windows Server 2008 x64 edition KB956589 and KB956774
http://www.microsoftpressstore.com/title/9780735626799.
http://www.microsoftpressstore.com/title/9780735626799.

18. Offline Virtual Machine Servicing Tool
http://technet.microsoft.com/en-us/library/cc501231.aspx.

19. System Center Data Protection Manager 2007 Evaluation Copy
http://technet.microsoft.com/en-us/evalcenter/bb727240.aspx.

20. System Center Data Protection Manager 2007 SP1 Update
http://www.microsoftpressstore.com/title/9780735626799.

21. iSCSI Initiator Software for Windows Server 2003
http://www.microsoft.com/downloads/details.aspx?familyid=12cb3c1a-15d6-4585-b385-befd1319f825&displaylang=en.

We suggest you download these components ahead of time because several of them require quite some time to complete. Store them in an easily accessible shared folder and label them appropriately. This will improve the quality of your experience during the practices.

Using the CD

A companion CD is included with this training kit. The companion CD contains the following:

- **Practice tests** You can practice for the 70-652 certification exam by using tests created from a pool of realistic exam questions. These questions give you enough different practice tests to ensure that you're prepared.
- **eBook** An electronic version (eBook) of this training kit is included for use at times when you don't want to carry the printed book with you. The eBook is in Portable Document Format (PDF), and you can view it by using Adobe Acrobat or Adobe Reader.
- **Sample chapters** Sample chapters from other Microsoft Press titles. These chapters are in PDF format.

How to Install the Practice Tests

To install the practice test software from the companion CD to your hard disk, perform the following steps:

1. Insert the companion CD into your CD-ROM drive and accept the license agreement that appears onscreen. A CD menu appears.

> ***NOTE***
>
> **If the CD menu or the license agreement doesn't appear, AutoRun might be disabled on your computer. Refer to the Readme.txt file on the companion CD for alternative installation instructions.**

2. Click Practice Tests and follow the instructions on the screen.

How to Use the Practice Tests

To start the practice test software, follow these steps:

1. Click Start and select All Programs, Microsoft Press Training Kit Exam Prep. A window appears that shows all the Microsoft Press training kit exam prep suites that are installed on your computer.
2. Double-click the practice test that you want to use.

Practice Test Options

When you start a practice test, you can choose whether to take the test in Certification Mode, Study Mode, or Custom Mode.

- **Certification Mode** Closely resembles the experience of taking a certification exam. The test has a set number of questions, it is timed, and you cannot pause and restart the timer.
- **Study Mode** Creates an untimed test in which you can review the correct answers and the explanations after you answer each question.
- **Custom Mode** Gives you full control over the test options so that you can customize them as you like.

In all modes, the user interface that you see when taking the test is basically the same, but different options are enabled or disabled, depending on the mode.

When you review your answer to an individual practice test question, a "References" section is provided. This section lists the location in the training kit where you can find the information that relates to that question, and it provides links to other sources of information. After you click Test Results to score your entire practice test, you can click the Learning Plan tab to see a list of references for every objective.

How to Uninstall the Practice Tests

To uninstall the practice test software for a training kit, use the Add Or Remove Programs option (Windows XP or Windows Server 2003) or the Program And Features option (Windows Vista or Windows Server 2008) in Control Panel.

Case Scenarios

In the case scenarios at the end of each chapter, you will apply what you've learned in that chapter. If you have difficulty completing this work, review the material in the chapter before beginning the next one. You can find answers to these questions in the "Answers" section on the companion CD which accompanies this book.

Case Scenarios and the 70-652 Exam

Of the approximately 200 practice test questions included on the companion CD, 180 are based on case scenarios. Case scenario–based practice test questions provide a way to assess whether the certification candidate understands the information that he or she has learned. Each case scenario describes a fictional company that is facing some dilemma. The case scenario will be exhaustive and will feature both technical and non-technical details. You need to be able to analyze and interpret not only the technical issues, but the business needs as well.

You will need to read each case scenario more than once. It is a good idea to read through the case scenario quickly the first time. Try to identify the major obstacle(s) facing the fictional company. Then read the questions associated with this case scenario. Approximately five questions accompany each scenario.

On the next pass, pick out details that will help you answer the questions. Note portions of the case scenario that relate to specific questions. It will be necessary to read the scenarios thoroughly and to absorb as much information as possible rather than reading only the sections that you think are relevant.

Case Scenario Structure

Each case scenario contains several sections that cover different aspects of the fictional company. The first part of the scenario provides background information, such as an overview of the company and any changes the company plans to make. It might also reveal any major problems the company is currently facing.

There will also be sections describing the company's business requirements, including general or technical requirements. The technical requirements section specifies technical details involving security, maintainability, availability, and recoverability.

Prepare for Your Microsoft Certification Exam

Use the following checklist to determine whether you're ready for your exam. This compilation stems from the experience we have gathered from the more than 40 exams we have taken ourselves.

- **Be ready** It is useless to take an exam if you don't think you're ready. Perform lots of practice and ensure that you are not only familiar with the technology itself, but also how it interacts with other Microsoft technologies.
- **Practice** New exams include software simulations. This simulates the activity you perform in the actual software program. If you don't have the opportunity to practice with this tool, you'll never be able to answer the questions.

When actually taking the exam, remember the following:

- **Mark your questions** Several questions are very detailed. If you see that a question is too time-consuming mark it and move on to the next one.
- **Mark your time** Make sure you have enough time for the exam. It would be sad not to pass because you didn't have enough time to at least read every question.
- **Read each question attentively** Questions often include a lot of clutter—information that is there to confuse you. Make sure you carefully read the beginning and the end of each question before you answer.
- **Return to previous questions** An exam often includes several questions on the same subject. One question can often provide the answer to another.
- **The first answer is most often right** If you don't know the answer, follow your intuition.
- **It's better to answer something than leave blanks** Blank answers are worth nothing.
- **Don't stress yourself** After all, it's just an exam and if you know your stuff, you won't sweat it.

Microsoft Certification Programs

The Microsoft certifications provide the best method to prove your command of current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop—or implement and support—solutions with Microsoft products and technologies. Computer professionals who become Microsoft-certified are recognized as experts and are sought after industry-wide. Certification brings a variety of benefits to the individual and to employers and organizations.

MORE INFO **ALL THE MICROSOFT CERTIFICATIONS**

For a full list of Microsoft certifications, go to *http://www.microsoft.com/learning/mcp/default.mspx*.

Every effort has been made to ensure the accuracy of this book and the contents of the companion CD. If you have comments, questions, or ideas regarding this book or the companion CD, please send them to Microsoft Press by using either of the following methods:

E-mail:

- *tkinput@microsoft.com*

Postal Mail:

- *Microsoft Press*

  Attn: Microsoft Certified Technical Specialist (MCTS) Exam 70-652: Configuring Windows Server Virtualization, *Editor*

  One Microsoft Way

  Redmond, WA 98052-6399

For additional support information regarding this book and the CD-ROM (including answers to commonly asked questions about installation and use), visit the Microsoft Press Technical Support Web site at *http://www.microsoft.com/learning/support/books*. To connect directly to the Microsoft Knowledge Base and enter a query, visit *http://support.microsoft.com/search*. For support information regarding Microsoft software, please visit *http://support.microsoft.com*.

CHAPTER 6

Migrating to Hyper-V

Now that your Hyper-V host server or resource pool infrastructure is ready, you can move on to populate it with production-oriented virtual machines. This means transforming your production machines into virtual machines running on Hyper-V. Chapter 1, "Implementing Microsoft Hyper-V," introduced the concept of starting points for Hyper-V migrations in Lesson 2. Three starting points are possible:

- **Organizations running a traditional physical infrastructure** These organizations need to implement a completely new server virtualization infrastructure and then convert their existing physical workloads to virtual machines.
- **Organizations already using software-based server virtualization** Organizations using tools such as Virtual Server or VMware Server need to implement new host servers running Hyper-V and then perform a virtual machine conversion to transform existing virtual machines into Hyper-V VMs.
- **Organizations already using hardware-based server virtualization** Organizations using tools such as VMware ESX or Citrix XenServer need to convert their host servers to Hyper-V and then convert their virtual machines into the Hyper-V format. In the case of Citrix XenServer, the virtual machine conversion process should be easier because it relies on the same virtual hard disk (VHD) format as Hyper-V.

This is the focus of this chapter: moving either physical or virtual machines from their current state to VMs hosted on Hyper-V infrastructures.

Exam objective in this chapter:

- Migrate a computer to Hyper-V.

Before You Begin

To complete this chapter, you must have:

- Access to a setup as described in the Introduction. In this case, it is also practical to have access to existing physical computers you can transfer into virtual machines, as well as virtual machines in other formats that can be transferred into Hyper-V format. This will give you more hands-on practice for the exam objective in this chapter.

Lesson 1: Working with Migration Scenarios

When you migrate existing machines—physical or virtual—to host them on the Microsoft Windows Server 2008 Hyper-V role, you need to understand and perform the following tasks, which are focused on the transformation process of a source machine into a target virtual machine (VM) running on Hyper-V. Specific tasks differ if the source machine is physical or virtual, but the basic process remains the same.

After this lesson, you will understand:

- The potential migration scenarios to Hyper-V.
- The impact of migration on the source machines.
- How each different migration functions.
- How to perform manual migrations.
- How to prepare specific prerequisites for certain types of migrations. This involves installing System Center Operations Manager (OpsMgr) to use the Performance and Resource Optimization (PRO) or integrating VMware to SCVMM.
- How to perform automated migrations with SCVMM.
- The potential post-migration operations that might be required on your new VMs.

Estimated lesson time: 50 minutes

Understanding Hyper-V Migration Scenarios

When you get to the stage where you begin to perform migrations from a variety of platforms to virtual machines—in this case virtual machines that will run on top of Hyper-V host servers—you arrive at the most exciting stage of any server virtualization project. That's because you're finally ready to begin to profit from the resource pool you have put in place. From this stage on, you'll be transforming the way you work with production systems because all of your production machines—at least all of the machines that provide end user–facing services—will now be virtual machines. Your datacenter will now have one exclusive role for physical servers: the host server role, and all of these host servers will be part of your resource pool.

But before you can begin to profit from the resource pool and look to change your systems administration practices to support the dynamic datacenter, you have to migrate your machines—VMs or physical—to run them on top of Hyper-V. As mentioned at the beginning of this chapter, this move has several different starting points. And although your organization may only find itself dealing with one of these starting points, you—as a resource pool administrator—should be aware of all of the potential migration paths and how you address each of them. Of course, each of these migration paths should be fully tested in the laboratory before you put it to work in production.

NOTE **MIGRATING VMs TO PRODUCTION**

Keep in mind that when you migrate machines—VMs or physical—to a new production environment running on top of Hyper-V, you are migrating more than the machines that run in your production environment. The machines you migrate include any machines that your organization actively relies on to perform work. This includes machines in testing, training, development, pre-production, and production environments. In this case, the term *production* refers to the fact that your Hyper-V hosts are now in production mode and can support the operation of any type of VM.

Organizations performing migrations of machines onto production Hyper-V resource pools need to be familiar with the following migration types:

- Migrations from physical machines onto virtual machines
- Migrations from machines running on Microsoft Virtual PC or Microsoft Virtual Server to Hyper-V
- Migrations of machines that have been captured in disk image format using third-party tools such as Acronis True Image Echo or Symantec Ghost
- Migrations of machines that are running as virtual machines within a VMware environment
- Migrations of machines that are running as virtual machines within a Citrix XenServer environment
- Migrations of machines that are already in Hyper-V format but are running on another host

Any of these migrations can occur when you are running a datacenter that relies on the Hyper-V hypervisor. Many of these migrations can be fully automated if you have the appropriate tool; however, many resource pool administrators will find themselves without the appropriate tool or without the funds to acquire the appropriate tool. Therefore, they must be aware of other means to perform the migration—means that often take more time. Performing a migration—manually or through automated processes—saves time and helps maintain the investment you already have in an existing machine.

Preparing for a Migration

Whichever source you use, the migration process includes some caveats. Basically, the migration process involves not only copying the contents of the hard disks—physical or virtual—that make up the source machine into the VHD format supported by Hyper-V, but also involves transforming the drivers—once again physical or virtual—that are currently installed on the source machine to run on Hyper-V. If the operating system of the source machine is a supported version, or a version for which Hyper-V includes a set of Integration Services or Components, the machine will run as an enlightened guest and perform very well. If the source operating system is not a supported version, it will run as a legacy guest operating system. In either case, you need to convert the drivers from the existing ones to drivers supported by Hyper-V. In some cases, custom drivers need to be removed before the transformation and in others, new drivers can automatically be installed either through the installation of the Integration Services or Components or through plug and play. In other cases, both removal and reinstallation of drivers have to be performed manually.

In addition, it is good practice to defragment hard disk drives, both system and data drives, before performing the migration. This optimizes the placement of data into the new virtual or pass-through disks you use. Also keep in mind that Hyper-V virtual machines must boot from an IDE drive; therefore, if your source systems run SCSI or iSCSI drives as a system drive, the system disk needs to be converted to an IDE disk to work with Hyper-V. As you will see, there are several ways to perform this conversion.

The entire point of transforming a machine—physical or virtual—into a new Hyper-V VM is to have the applications or services that the machine supported run from a Hyper-V VM. When you convert an entire machine—including operating system, applications, and data—from one format to another, you risk damaging the machine in some way. Driver conversions don’t work, systems do not boot up because of the disk transformation process, and so on. This is why you should always begin with the examination of the service or application you want to convert. If you have a way to simply install a new guest operating system into a Hyper-V VM, add a role or application, and then rely on the role or application’s own migration process to move it from the source machine to the target machine, you should opt for this method first because the results will always be better. This way, you won’t transfer the issues that can arise from the conversion process. Your target machine will be a pristine installation of a guest operating system into a Hyper-V VM and the service or application will run as it should because it also benefited from a clean installation.

It is also essential to perform a proper assessment of the source machines because you must be aware of peaks and lows in machine performance to properly size the virtual hardware in the target VM. You already relied on the Microsoft Assessment and Planning tool to perform an initial assessment in Lesson 2 of Chapter 1, “Implementing Microsoft Hyper-V”. In this chapter, you’ll be able to use Performance and Resource Optimization (PRO), a feature that is available when SCVMM is linked with System Center Operations Manager to perform an updated assessment on the machines you need to migrate.

The assessment is also a requirement to properly position the VM on a host with the appropriate resources to support its operation. This is where SCVMM’s Intelligent Placement feature becomes useful because it rates host servers and categorizes them according to available resources. PRO is also helpful in this case. When you have the assessment in hand, you’ll want to categorize the different workloads you run to determine in which order they will be migrated. The simplest categories include three different types of workloads:

- **Simple Workloads** This category includes single-purpose servers, servers with low input and output (I/O) rates, and servers that run only a single network interface card (NIC).
- **Advanced Workloads** More advanced workloads include applications that are configured for high availability through either server load balancing or failover clustering, servers with ongoing high I/O, and multi-homed computers using multiple NICs to route traffic.

- **Special Workloads** Special workloads include applications that use multiple tiers (N-tiered), applications that span multiple sites, applications that require custom hardware or dongles to work, and applications over which you have no ownership. The last type of workload often requires you to launch a negotiation with an application's "owners," which may include other business units, departments, groups in different locations, or even other groups within IT.

You'll want to begin a migration process with the most basic applications and then progress to more complex workloads once you gain experience with the process. You'll most likely keep the special workloads for the end. When ownership is in question for these workloads, you may need to deal with a lot of negotiation with other departments and their stakeholders. This sometimes lengthy administrative process should begin as soon as possible, even if the workloads themselves will only be migrated at the end.

MORE INFO **CATEGORIZING WORKLOADS**

For a more detailed categorization of source workloads, see "Scope Your Infrastructure" at *http://virtualizationreview.com/columns/article.aspx?editorialsid=2933*.

Understanding Virtual Machine Provisioning Approaches

The best machine is a clean machine—one that was cleanly installed and to which the workload has been newly applied. In IT, this caveat has proven itself time and time again. When organizations face an operating system migration, especially a server operating system migration, they rarely opt for an upgrade and most often choose to create a pristine installation of the new operating system and migrate the workload to that new operating system image. The same applies to your new virtual machines.

However, the bottom line is that moving to a virtual infrastructure is supposed to be a simple process that should remove—not add—overhead to administrative processes. Although this migration should be run as a project that will have a variable duration depending on the number of machines you need to convert, this move should not add a massive workload to your administrative staff and should be as simple as possible. That's why virtual infrastructure manufacturers such as Microsoft offer tools that can automate physical to virtual (P2V) or virtual to virtual (V2V) conversions.

These tools target a physical or virtual server and convert its disks into virtual disk drives. The key to this process, however, is driver injection. Because physical machines rely on custom drivers—drivers that are specific to the hardware platform—these drivers must be converted to the legacy or synthetic drivers that are used in Hyper-V (see Figure 6-1). The P2V/V2V engine must be able to properly replace hardware or other drivers with the virtualization drivers you need to use. If this process does not work or work completely, you'll be faced with broken systems and unstable servers.

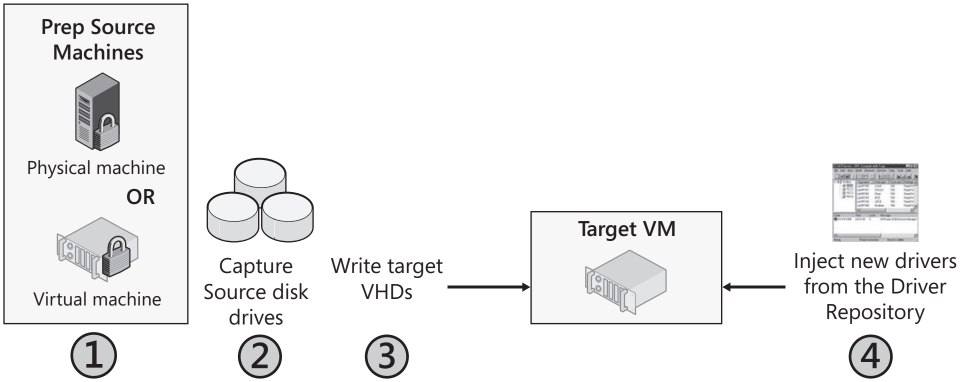


FIGURE 6-1 The key to P2V/V2V conversions is proper driver injection.

For Microsoft, the automated conversion tool is SCVMM. Even an evaluation version of this tool can support a complete conversion process from either physical or virtual machines. But even if you have access to a full version of SCVMM, you'll find that your conversions will focus on three possible approaches:

- **Manual conversion** The first approach involves the creation of a brand-new virtual machine running a stable operating system configuration. This VM serves as the seed machine or template for all workload migrations. If you have multiple operating systems in your data center, you may require more than one seed machine, but keep the number of templates to a minimum. Remember, you'll need to manage a reference VM for each template. You rely on the template to generate a new VM and then you use the workload's own migration process to move the service from the source to the new target machine. Although this process may be more time consuming, it provides excellent results and leaves you with very stable results.
- **Semi-automated (offline) conversion** The second approach consists of using an offline P2V conversion tool (some third-party tools are free) to move the workload as is and convert the operating system from one contained in a source machine to one contained in a target VM. This process is riskier than the first approach but is sometimes necessary, especially when a workload lacks a migration capability of its own. This is often the case for legacy or custom in-house code. Because the tools offer offline conversion—in which the source machine is taken offline during the conversion process—some manual operations may be required when the conversion is complete or even before the conversion begins to prepare the source computer properly.

  If the conversions are performed with SCVMM, then you can only use this process for products newer than Windows 2000 Server. Older operating systems such as Windows NT 4 require intermediary steps, converting the machine using another tool to a specific format and then converting the intermediary format to a Hyper-V VM.
- **Fully automated (online) conversion** Fully automated conversions transform the source machine while the system runs, copying disk drive contents to virtual disk drives and then booting a VM to replace a source machine's workload. For this method, you

use a tool that migrates a server over a network without user interaction. When you perform this process with SCVMM, the disk contents of the source machine are copied using the Volume Shadow Copy Service (VSS) and the VSS images are duplicated while the source server continues to process end-user requests. Online conversions with SCVMM are only supported for guest operating systems that are supported by Hyper-V and will be able to install Integration Services.

Although the manual conversion process is often the best choice for small numbers of workloads, you'll most likely find that you will perform both of the other conversion types if your organization runs hundreds or even thousands of workloads and you want to convert them all.

EXAM TIP **OFFLINE VS. ONLINE CONVERSIONS**

Keep in mind that to use an online conversion process for a machine that runs an unsupported operating system, you can upgrade the operating system to a newer, supported version first—if possible—and then perform the online conversion. Also note that while the source machine may be running a supported operating system for online conversion, its workload may not be suitable for this conversion type and you may have to use an offline conversion instead. This is the case with domain controllers, for example.

When you rely on SCVMM to perform the conversions, it differentiates between online and offline conversions:

- **Online conversions** SCVMM uses the Background Intelligent Transfer Service (BITS) to copy data while the source computer continues to run. BITS relies on VSS to ensure data consistency during the transfer. The source computer must have a minimum of 512 MB of RAM to support online conversions.
- **Offline conversions** SCVMM uses Windows PE to reboot the source computer and perform an offline conversion. Because the conversion is performed on the network, you must have appropriate drivers for Windows PE for both network and storage that fit the source hardware platform. If drivers are not generic, you must provide them to SCVMM.

Keep in mind that the P2V conversion process in SCVMM is the only process that supports online conversions; the V2V process only performs offline conversions from VMware VMs to Hyper-V. If you want to convert a VM from any source while it is running (online), use the P2V conversion process instead of the V2V conversion process. SCVMM does not really differentiate between the fact that the source machine is a VM and not a physical machine. After all, virtual machines are supposed to emulate physical machines as much as possible.

Understanding Conversion Caveats

Keep the following in mind when you finalize the preparations for your conversions:

- **Clean up your source environment** Before you begin the conversion process, you need to clean up your server environment. You don't want to find yourself amid a massive file server conversion only to discover that 90 percent of the files on the server haven't been accessed in months and are ready for archiving. Use your network assessment to determine which machines should be migrated first. To do so, rely on metrics such as hardware requirements, software dependencies, licensing requirements, and current resource utilization ratios.

- **Prepare for some downtime** Because a migration copies the contents of source disk drives to target drives, the process relies heavily on the network to move the data from one machine to another. As a result, the migration process can involve downtime. And although several technologies support live conversions, you'll generally perform these conversions offline and during maintenance windows. You'll most likely need to schedule downtime—and possibly even a special migration period—and negotiate with your stakeholders to pre-empt migration issues.
- **Aim to minimize downtime** When machines have redundant services, such as when they are running Failover Clustering or Network Load Balancing (NLB), downtime risks decrease considerably. For example, if you migrate a service running on an NLB or failover cluster, you shouldn't face downtime because the service continue to be provided by other nodes. Note, however, that this strategy does not work for organizations that use all-in-one servers such as Windows Small Business Server (SBS). In such cases, all server roles run on the same machine, so virtualizing technologies like SBS will most certainly involve downtime.
- **Prepare storage and network requirements** Make sure you are prepared for the migration. Do you have enough storage to virtualize all the machines you've targeted? Will you be using shared storage for the VMs? If so, you need spare space to hold machines while in transition. Are the source machines on a storage area network? If so, you can rely on high-speed SAN Transfers if you are using SCVMM. If not, your conversions will occur through the network. Can your network sustain the load? If you are at peak performance today, adding a conversion workload may overly stress your network. Perhaps you should consider performing the conversions on a dedicated network.
- **Determine the conversion type** The number of conversions you need to make is a factor in determining which tools to use. If you run a basic network with workloads that are classified as simple, you may be able to rely solely on a manual conversion. If you have several legacy workloads and can take them offline during a migration, you can rely on the semi-automated conversion process. If you have a high volume of workloads to migrate, you'll most likely want to use both the manual and the fully automated method. In this case, you'll also want the ability to convert machines in any direction: P2V, V2V, and possibly, V2P. These reverse conversions may be required to obtain support from certain application vendors. Although over time the need for these reverse conversions will decrease and possibly disappear, they are still necessary in early stages of your hypervisor implementation.
- **Determine the support policy** Determine whether your application providers support virtualizing their workloads. Over the past 10 years, vendors that do not support virtualization have become far rarer, but you always need to check on proper

application support. In some cases, you may have to return workloads to physical machines to obtain support from a given vendor. In others, you may be able to obtain best-effort support from your vendor—they will try their best to help solve issues, but if they can't come to a solution, you may have to revert the workload to a physical system. Microsoft server product groups have been working at developing official support policies for virtualizing their products. These policies form the basis of Chapter 10, "Ensuring Virtual Machine High Availability," as you learn to provide high availability for different server workloads. Because of these support considerations, you should also consider integrating the conversion process you select with the ability to convert machines from one state to another and back.

- **Rely on a safety-net strategy** Select appropriate migration candidates in order of importance. Your migration strategy should begin by tackling low-risk, non-business-critical workloads such as the test and development environments you run. This enables you to become expert at the conversion process without incurring the consequences of missteps. Web servers are also often good candidates for initial conversions. If your Web site is properly set up, you may already have redundant Web servers running in NLB clusters; beginning with redundant services reduces the risks of your first conversion experiments. Then move on to low-use systems that host less critical applications. Next, work on higher-use systems that are not critical; this can include application-specific servers or routing and virtual private networking servers. Migrate servers running critical workloads last. By this time, you should be familiar with the process and ready for any eventuality.

These caveats will help improve the results of your conversions.

Relying on a Conversion Checklist

When you're ready to move on to your conversions, you should rely on the following checklist:

1. Determine the validity of a candidate for conversion.
2. Clarify the vendor's support policy for the new virtual workload.
3. Consider potential licensing changes in regards to virtualization and, if necessary, make adjustments.
4. Identify the appropriate target host for the virtual machine.
5. Identify CPU and memory requirements for the VM.
6. Determine whether the VM will be using VHDs or pass-through disks and identify the storage location for the VM's disks.
7. Identify network requirements and ensure that the appropriate virtual NICs are available on the host.
8. Identify a failover strategy for this VM both during and after the conversion.
9. Use a standard naming strategy to differentiate the new virtual service offering from the source machine that used to run the workload. Alternatively, use the same name and keep track of the progress of your conversions.

10. Schedule downtime in support of the migration. You may not need it, but if you do, it is safer to have it ready.
11. Prepare your testing plan for the new VM. Run the virtual machine in a lab first to ensure that it is completely stable.
12. Prepare a go-live plan for the VM when it has passed all tests. This go-live plan should include the decommissioning of the source machine.

Source-to-target conversions are often one-time procedures, and when machines have been properly migrated, you rarely need to touch their workloads again. In some instances, of course, odd workloads need to move back and forth if support issues arise. Be ready, become familiar with your tools, and have a fallback strategy for each conversion.

Working with Clean Provisioning or Manual Conversions

Several types of workloads can rely on manual conversions. In a Windows environment, these workloads can include domain controllers, Internet Information Services (IIS) Web servers, Exchange servers, Microsoft SQL Server machines, and more. In Linux environments, workloads supporting migration include similar services. In both Windows and Linux environments, you can also migrate clustered servers as well as servers running either NLB or other server load-balancing technologies. Keep the following in mind when converting Windows workloads:

- **Domain controllers (DCs)** To migrate a DC from a source to a target machine, create a new VM running the appropriate virtualization drivers, configure this VM according to your internal best practices, and promote it to a domain controller within the same domain. The promotion process automatically copies the contents of the Active Directory database to the new VM. Repeat for as many DCs as you require. When you are ready, you can move the operations master roles to the new virtual DCs and decommission the source DCs. You can also add the Domain Naming System (DNS) to the new DCs and perform two conversions at once. Remember to update the Dynamic Host Configuration Protocol address pools with new DNS server addresses when the conversion is complete.
- **SQL Server servers** To migrate databases running on Microsoft SQL Server, create new virtual machines running the appropriate version of SQL Server—ideally version 2008—and then use the SQL Server data migration process to move the workload. Begin with the analysis of your databases with the SQL Server Upgrade Advisor and follow its recommendations if corrections are required for the existing databases. (Find the Advisor at *http://www.microsoft.com/downloads/details.aspx?FamilyId=F5A6C5E9-4CD9-4E42-A21C-7291E7F0F852&displaylang=en.*) Copy the databases—detaching and attaching the databases from one machine to the other—and perform any required manual modifications. Convert the database to the new format if possible and decommission the source servers. Even better, with SQL Server 2008, capture the entire process into a Windows PowerShell script to automate the process.

- **Exchange Servers** To migrate email services on a Microsoft Exchange Server, especially Exchange Server 2007 SP1, create new VMs and prepare them to host Exchange Server roles. For the Hub Transport server role, simply join the VM to Active Directory and install the Exchange role. After the role is installed, the new VM acquires its configuration from the Active Directory Exchange Configuration Container. For the Edge Transport role, create a new VM and install the Exchange role. Use the Edge Subscription feature in Exchange to assign the appropriate configuration to the VM. For the Mailbox server role, create highly available VMs and use the Exchange *move* cmdlet to move the mailboxes from the physical servers to the VMs. For the Client Access role, create a new VM, install IIS, and join the new VM to the domain; then install the Exchange role. Once again the configuration will be picked up from Active Directory. Finally, for the Unified Messaging role, create a VM, connect it to the appropriate hardware infrastructure—Voice over IP (VOIP) or PBX gateways—and install the role. Add the new VM to your round-robin DNS structure for the service and then decommission the source machines when ready. Once again, you can capture several of these processes in Windows PowerShell to automate them.
- **Failover clusters** To migrate failover clusters, add new VMs as nodes of the cluster using pass-through disks or iSCSI connectivity, fail over the services onto the new VMs, and decommission the source physical nodes of the cluster when ready. When this is complete, your virtual machines will still be tied to physical storage.
- **Network Load Balancing clusters** For NLB clusters, create new VMs, install the required service on the VM—these services can be anything such as Web servers, or Terminal Services, or other stateless workloads—and then perform a drain stop on the source physical machines before decommissioning them.
- **Backup and restore** When all else fails and the workload you are trying to migrate does not support migration on its own, you can create a clean VM, then use a backup of the application on the source server and then restore the workload into the virtual machine. Make sure you test this process fully before releasing the new VM into production because it is not as clean as the other processes in this list.

These examples provide manual migration methods that you can rely on without having to use conversion tools. In addition, each VM is a new and pristine installation of the guest operating system and service or application, often making it more stable and reliable than a converted machine.

Optimizing VMs

After your machines are converted to VMs, you should use the following best practices to make sure they run at their very best:

- **Set the VM display** You should set display parameters on your VMs for Best Performance. This ensures that hardware acceleration for the display is set to On and will provide the best experience in VMs.

- **Use fixed-sized or pass-through disks** Use fixed-sized disks as much as possible for improved performance. You can use dynamically expanding disks during conversions to save time and improve conversion speeds, but after a machine is converted, you should change the disk type to fixed-size. For special workloads that need absolutely the best performance, use pass-through disks instead of VHDs.
- **Assign resources to meet peak demands** Make sure you assign resources—processors and RAM—to VMs based on anticipated peaks on the VMs. Otherwise, you might choke the performance of the workload in the new VM. This is where your assessments greatly help.
- **Use SCSI virtual adapters** Although you must boot from an IDE disk, you should use SCSI virtual adapters for data disks because SCSI adapters support many more disks than IDE virtual adapters. Remember however that performance is nearly identical between IDE and SCSI virtual adapters in Hyper-V.
- **Protect VM configurations** If you use a shared folder to store all VM configuration files and therefore make sure they are available to any host, make sure the shared folder is highly available. This means running it on a failover cluster and storing the data on shared storage.
- **Manage time synchronization properly** If your entire end user–facing infrastructure is running in VMs, consider how you should set time synchronization. By default, time is synchronized with the host server through Integration Services. However, if you run domain controllers as VMs, you can set all of your VMs to synchronize time with the PDC Emulator Operations Master Role. When you do this, clear Time Synchronization in the VM's Integration Services section of its properties and make sure it synchs with the PDC Emulator. Also make sure you do not pause, save state, or otherwise take your DCs offline—this will adversely affect data replication with other DCs and may put the DC out of synch. Finally, don't use snapshots on DCs because they operate best when they do not use differencing disks.

These guidelines will ensure that your VMs run at their best after they are converted.

Installing Additional Components in Support of Migrations

A lot has been said to date on the potential integration of OpsMgr and SCVMM. Now it is time to perform this integration to provide additional support to the conversion or migration process.

One of SCVMM 2008's biggest strengths is its ability to manage VMware infrastructures and support the conversion of VMware machines to Hyper-V and vice versa. But to access these features, you must first learn to integrate VMware ESX host servers to the SCVMM environment. Both operations are described here.

Using Performance and Resource Optimization (PRO)

OpsMgr integrates with SCVMM to support SCVMM's Performance and Resource Optimization (PRO) feature. PRO relies on OpsMgr's monitoring capabilities to monitor both host servers and virtual machines and help maintain the health of your production environment. PRO uses the collected information to generate tips that help resource pool administrators place, move, and reconfigure VMs for optimal operation.

PRO integrates with SCVMM's Intelligent Placement feature to provide expert-level advice on how VMs should be operated. Although Intelligent Placement on its own can position VMs based on host performance, integrating it with PRO lets you gain more insight into the requirements of a particular workload and its affinity to other workloads placed on the same host. In this case, PRO generates guidelines and rules that help resource pool administrators rely on heterogeneous workload placement on specific hosts. For example, you would not want to place 10 domain controller VMs on the same host because all of these DCs would rely on the same resources at the same time. Instead, you would place a DC, an e-mail server, a database server, and perhaps a Web server on the same host to call upon different host system resources at different times during a workday. This uses a host's resources more efficiently and provides better performance for VMs.

PRO includes the following capabilities:

- Integration with Intelligent Placement
- Support for clustered hosts and clustered OpsMgr operation
- Decisions based on health monitoring of both hosts and VMs
- Internal guest operating system monitoring
- VM configuration correction suggestions for improved performance
- Host load balancing to improve host performance
- Automatic remediation of situations monitored by PRO

Administrators can therefore rely on PRO to automatically remediate problematic situations, or they can rely on it to alert them to provide a manual response to a situation. Perhaps the best approach is to manage responses manually at first to become familiar with the PRO feature set and then activate them automatically when you understand how PRO responds to given situations.

Installing System Center Operations Manager to Work with SCVMM

System Center Operations Manager is an agent-based monitoring technology that collects and centralizes service and application activity within a network. In addition, it monitors devices and operating systems. The base structure of OpsMgr is the management pack—a set of monitoring and alerting rules that is designed for a specific application, device, or operating system. These management packs must be added on to the OpsMgr infrastructure to provide complete monitoring services. For example, SCVMM has its own management pack that must be integrated with OpsMgr for the two products to work together.

Event messages are filtered when they arrive at the OpsMgr central database. OpsMgr uses these filters to determine which action type must be performed when the event information arrives. Actions can include doing nothing; sending an email alert, a notification, or an event; or taking a series of corrective actions to remediate the situation. Actions are based on workflows and can be customized to your environment. All event messages are stored in the database to maintain a historical record of events for the entire network infrastructure.

Event messages are transferred from originating systems to the central database through the Windows Communications Foundation over TCP/IP port 5723. The agents are responsible for this communication. Management packs include custom filtering rules for particular applications and because Microsoft publishes the management pack authoring outlines, several third-party organizations have produced custom management packs to extend OpsMgr's reach into non-Microsoft technologies. For example, nWorks produces a management pack for VMware Virtual Infrastructure, letting you integrate the management of VMware host servers into an OpsMgr infrastructure.

> ***MORE INFO*** **nWorks VMWare MANAGEMENT PACK**
>
> **Find out more about the nWorks VMware management pack at *http://www.nworks.com/vmware*.**

OpsMgr uses a similar installation process as SCVMM. Table 6-1 outlines the prerequisites for an OpsMgr installation. You should avoid installing OpsMgr on the same system as the SCVMM Server as much as possible because it will impact system performance. When you place the two products on different systems, as you would in larger environments, you must make sure that the SCVMM Server account is granted full access to the OpsMgr server. Place this account into the local administrator group on the OpsMgr server to ensure that the integration works properly.

TABLE 6-1 System Center Operations Manager 2007 Prerequisites

COMPONENT	SOFTWARE REQUIRED
Operations Manager Database	x86 or x64 edition of SQL Server 2005 Standard or Enterprise edition with SP1 or SQL Server 2008.
Management Server	The Microsoft .NET Framework 2.0 or higher. Microsoft Core XML Services (MSXML) 6.0. This is installed automatically during the OpsMgr installation.
Operations Console	.NET Framework 2.0 or higher. The following components are optional, but required to create or edit Management Pack knowledge data. ■ Microsoft Windows PowerShell for the OpsMgr Command Shell. ■ Microsoft Office Word 2003 with .NET Programmability feature and Microsoft Visual Studio 2005 Tools for the Microsoft Office System
Agent	MSXML 6.0, which will be installed automatically if the agent is deployed from the Operations Console. It must be installed manually otherwise.
Reporting Data Warehouse	SQL Server 2005 with SP1 or SQL Server 2008.

COMPONENT	SOFTWARE REQUIRED
Reporting Server	.NET Framework 2.0 or higher. SQL Server 2005 Reporting Services with SP1 or SQL Server 2008.
Gateway Server	.NET Framework 2.0 or higher. MSXML 6.0.
Web Console	.NET Framework 2.0 or higher. Internet Information Services. ASP.NET.
Audit Collection Database	SQL Server 2005 Standard or Enterprise edition with SP1 or SQL Server 2008.

When you install OpsMgr on the SCVMM Server, you need to obtain two files. The first includes the OpsMgr 2007 code itself. The second includes Server Pack 1 for OpsMgr. Both are required for the integration.

MORE INFO **OpsMgr 2007 INFORMATION AND EVALUATION**

For more information on OpsMgr 2007, go to *http://technet.microsoft.com/en-us/library/bb310604.aspx*. To obtain the OpsMgr evaluation files, go to *http://www.microsoft.com/downloads/details.aspx?familyid=C3B6A44C-A90F-4E7D-B646-957F2A5FFF5F&displaylang=en*. These files include both the OpsMgr installation and Service Pack 1. Note, however, that you cannot upgrade the evaluation version to SP1. SP1 only works with a full version of OpsMgr. To obtain OpsMgr SP1 on its own, go to *http://www.microsoft.com/Downloads/details.aspx?FamilyID=ede38d83-32d1-46fb-8b6d-78fa1dcb3e85&displaylang=en*.

MORE INFO **USING SQL SERVER 2005**

Your SQL Server 2005 installation will require Service Pack 1 or more to work with OpsMgr. Currently, Service Pack 3 is available for SQL Server 2005 at *http://www.microsoft.com/DOWNLOADS/details.aspx?familyid=AE7387C3-348C-4FAA-8AE5-949FDFBE59C4&displaylang=en*.

Use the following steps to install OpsMgr:

1. Install SQL Server 2005. Install the Database Service and Workstation components into a Default Instance. Apply Service Pack 3 or later when done.
2. Add Windows PowerShell and the .NET Framework 3.0 to your Windows Server 2008 machine.

3. Download the OpsMgr installation files with SP1. Place them in the Documents folder on the OpsMgr Server. Double-click SetupOM.EXE file to install OpsMgr. Click Run to start the installation.

4. The OpsMgr installation screen appears (see Figure 6-2). Click Check Prerequisites to make sure your system includes all of the required components. Click Check to verify the prerequisites. If all prerequisites pass, click Close (see Figure 6-3). If issues arise, click More beside the issue to see what needs to be done to correct the situation. Verify the prerequisites for the following:

   - Operational Database
   - Server
   - Console
   - Windows PowerShell

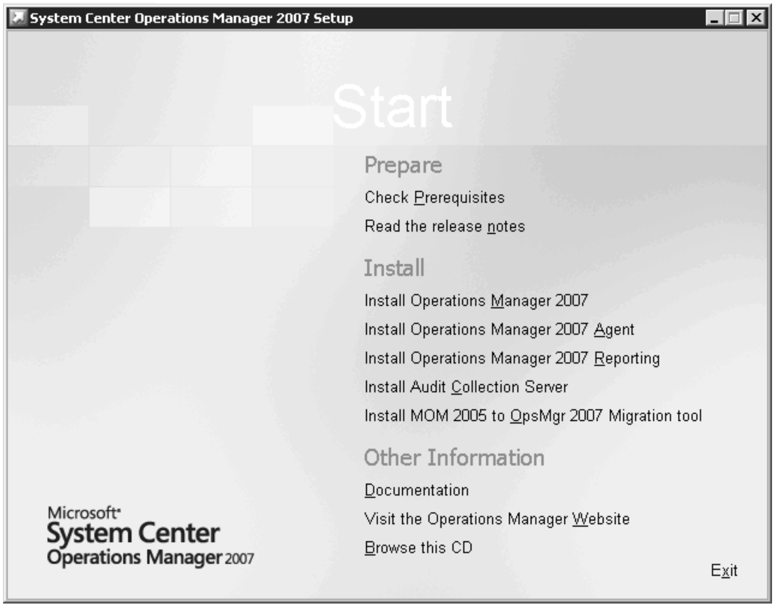
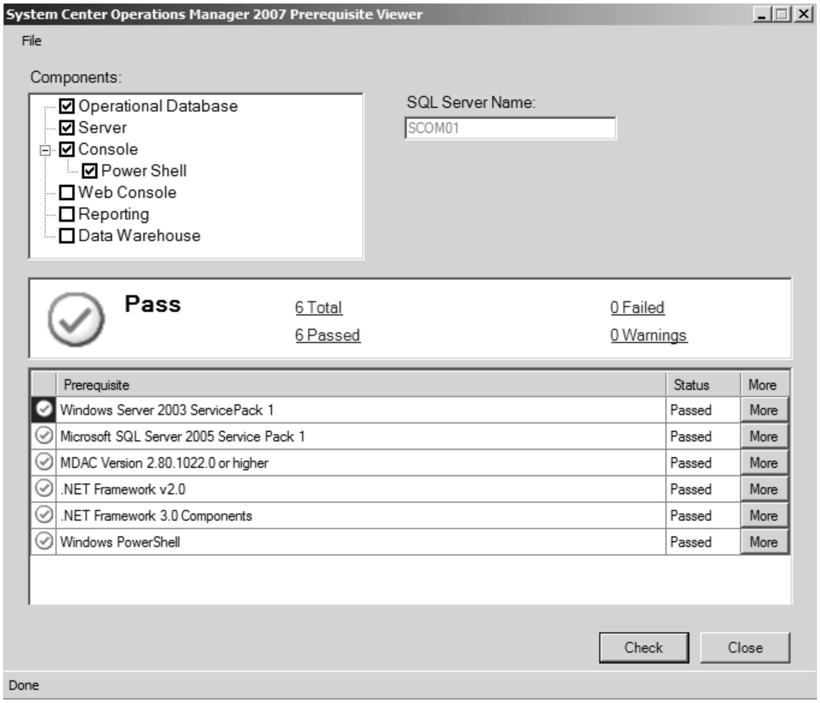

System Center Operations Manager 2007 Setup
Start
Prepare
Check Prerequisites
Read the release notes
Install
Install Operations Manager 2007
Install Operations Manager 2007 Agent
Install Operations Manager 2007 Reporting
Install Audit Collection Server
Install MOM 2005 to OpsMgr 2007 Migration tool
Other Information
Documentation
Visit the Operations Manager Website
Browse this CD
Exit
Microsoft System Center Operations Manager 2007

FIGURE 6-2 The OpsMgr 2007 SP1 installation screen

5. Install Operations Manager 2007. Windows Installer launches the setup. Click Next.
6. Accept the license terms and click Next.
7. Type in your name and organization details and your product key and click Next.
8. Select the components to install. Make sure all components are set to install on the hard disk, except for the Web Console. This component is not required for SCVMM integration, but if you are running OpsMgr in your network, you might require it for other purposes. Click Next.
9. Type in your management group name. Use your organization's name to keep it simple. Click Next.



Components:

- ☑ Operational Database
- ☑ Server
- ☑ Console
  - ☑ Power Shell
- □ Web Console
- □ Reporting
- □ Data Warehouse

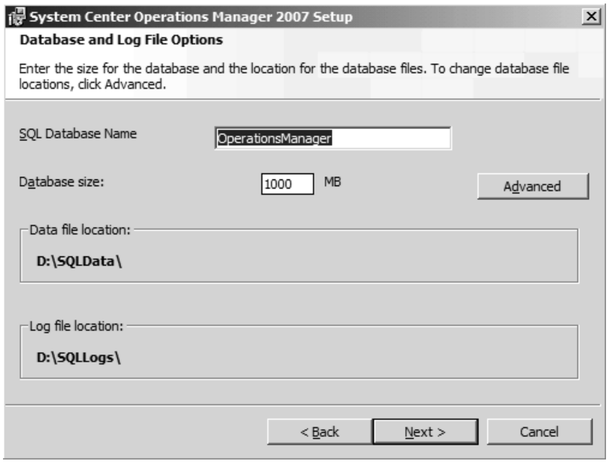
SQL Server Name: SCOM01

Pass 6 Total 6 Passed 0 Failed 0 Warnings

	Prerequisite	Status	More
✓	Windows Server 2003 ServicePack 1	Passed	More
✓	Microsoft SQL Server 2005 Service Pack 1	Passed	More
✓	MDAC Version 2.80.1022.0 or higher	Passed	More
✓	.NET Framework v2.0	Passed	More
✓	.NET Framework 3.0 Components	Passed	More
✓	Windows PowerShell	Passed	More

FIGURE 6-3 Verifying the OpsMgr 2007 SP1 prerequisites

10. You must also select the domain users that will be allowed to interact with OpsMgr on this screen. You can accept the default (Builtin\Administrators), which means that only local administrators will be allowed to use OpsMgr, but you should create an OpsMgr group in Active Directory Domain Services and assign it to this role. Remember that you will have to add the SCVMM service account to this role to support the integration. Use the Browse button to select your Active Directory group and then click Next.
11. Select the name of the database instance to use for the OpsMgr database. Choose the name of your server because you installed a default SQL instance. The communications port will be 1433. Keep this port number. Note that the SQL service will automatically be started if it is not already. Click Next.
12. If you set up your SQL Server defaults properly, the location of the database files and logs should be automatically provided (see Figure 6-4). The name of the database will be OperationsManager and the database size will be 1000 MB. You can change the location of the database files by clicking the Advanced button. Click Next.
13. Select the account to use to run the Management Server Actions. You should use a custom service account for this role. Make sure this account is not granted too many privileges—for example, using a domain administrator account—otherwise, you will be given a warning by OpsMgr Setup. Type in the account values and click Next.



System Center Operations Manager 2007 Setup

Database and Log File Options

Enter the size for the database and the location for the database files. To change database file locations, click Advanced.

SQL Database Name: OperationsManager

Database size: 1000 MB

Data file location: D:\SQLData\

Log file location: D:\SQLLogs\

FIGURE 6-4 Choosing database settings for OpsMgr

14. Select the account to use for the Software Development Kit (SDK) and Configuration Service. You can use the local system account in this case, but it is best to use a domain service account in this situation as well. Type in the account parameters and click Next.
15. Choose whether you want to send error reports to Microsoft and click Next.
16. Choose whether you want to send customer improvement data to Microsoft and click Next.
17. If your organization uses its own internal software update servers, leave the Update setting as is. If not, select Use Microsoft Update and click Next.
18. Click Install to begin the installation.
19. When the installation completes, you will be asked to back up the encryption key used in the OpsMgr setup and launch the OpsMgr console. Choose to back up the key, but do not open the console. Click Finish.
20. The Encryption Key Wizard appears. Click Next.
21. Make sure Back Up The Encryption Key is selected and click Next.
22. Click Browse to select the location to back up the key. Choose a secure location because this key is very valuable. Type in a filename—for example, **OpsMgr Key**—and do not assign an extension. Click Open to return to the wizard. Click Next.
23. Type in and confirm a password to protect the key. Choose a strong password and keep it secure. Click Next.
24. Click Finish to generate the backup.
25. Click Exit to close the OpsMgr Setup window.

Now apply Service Pack 1 to the installation by following these steps:

1. Double-click the SP1Upgrade.EXE file.
2. The OpsMgr SP1 Upgrade screen appears. Click Operations Manager 2007 under Apply Service Pack 1. Click Yes if an update warning appears.

3. Select Upgrade To Operations Manager SP1 and click Next. Accept the license agreement and click Install.
4. When the installation completes, you will be asked to back up the encryption key again and launch the OpsMgr console. Choose to back up the key and open the console. Click Finish. Save the encryption key again.
5. Click Exit to close the OpsMgr Setup window.

Your server is ready for the SCVMM integration.

Integrating OpsMgr with SCVMM

Now that the installation of OpsMgr is complete, you can begin its integration with SCVMM. Begin by importing OpsMgr Management Packs. Download the required management packs. Obtain the following:

- Windows Server Operating System
- Windows Server 2008 Application Server
- Windows Server Internet Information Services (IIS) 2000/2003
- SQL Server MP for OpsMgr 2007
- Virtual Machine Manager 2008

MORE INFO **OpsMgr MANAGEMENT PACKS**

Obtain the appropriate management packs by going to the following location: ***http://go.microsoft.com/fwlink/?LinkId=82105*****.**

MORE INFO **OpsMgr AND SCVMM INTEGRATION**

For step-by-step instructions for the integration of OpsMgr with SCVMM, go to ***http://blogs.microsoft.co.il/blogs/oshria/archive/2009/01/08/configuring-scvmm-2008-s-pro-feature-with-ops-manager.aspx*****. To download the SCVMM 2008 Management Pack for OpsMgr, go to** ***http://www.microsoft.com/downloads/details.aspx?FamilyID=d6d5cddd-4ec8-4e3c-8ab1-102ec99c257f&DisplayLang=en*****.**

Save all of these management packs into your Documents folder on the OpsMgr machine. Run each one of the installations. Double-click the management pack file, click Run, accept the license, and Next. Choose the default folder for installation, click Everyone, click Next, click Install, and then click Close. A Windows Explorer window opens to display the installed management packs. Close the window and repeat the operation for all other downloaded management packs. When all packs are installed, proceed as follows:

1. In the Operators Console of OpsMgr, change the view to Administration view, and click the Management Packs node in the navigation pane.
2. In the Actions pane on the right, click Import Management Packs.

3. Browse to the Program Files (x86) folder and then to System Center Management Packs and navigate through the subfolders to select the management pack files in the following list, and then click Open. The Import Management Packs dialog box opens. Click Add to select the other management packs until all of the packs listed here are selected. Make sure you select the packs in the order listed here; otherwise, the packs will not work properly (see Figure 6-5).

   Click Import to import each of the packs. You will be given a warning about a security risk. Click Yes to continue. The Import operation proceeds. Click Close when done.

   - Mirosoft.Windows.InternetInformationServices.CommonLibrary.MP
   - Microsoft.Windows.InternetInformationServices.2003.MP
   - Microsoft.Windows.Server.Library.mp
   - Microsoft.Windows.Server.2008.Discovery.mp
   - Microsoft.Windows.Server.2008.Monitoring.mp
   - Microsoft.Windows.AppServer.2008.mp
   - Microsoft.Windows.AppServer.Library.mp
   - Microsoft.SQLServer.Library.mp
   - Microsoft.SQLServer.2005.Monitoring.mp
   - Microsoft.SQLServer.2005.Discovery.mp
   - Microsoft.SystemCenter.VirtualMachineManager.2008.mp
   - Microsoft.SystemCenter.VirtualMachineManager.Pro.2008.Library.mp
   - Microsoft.SystemCenter.VirtualMachineManager.Pro.2008.HyperV.Host Performance.mp
   - Microsoft.SystemCenter.VirtualMachineManager.Pro.2008.VMRightSize.mp
   - Microsoft.SystemCenter.VirtualMachineManager.Pro.2008.VMWare.Host Performance.mp

4. Because OpsMgr and SCVMM are installed on two different machines, you have to grant access to the SCVMM Server on the Operations Manager Administrators user profile in the Ops Mgr machine. You do that by adding the SCVMM Server machine account to the Local Administrators group on the OpsMgr server and then restart the OpsMgr SDK Service. Use the following instructions:

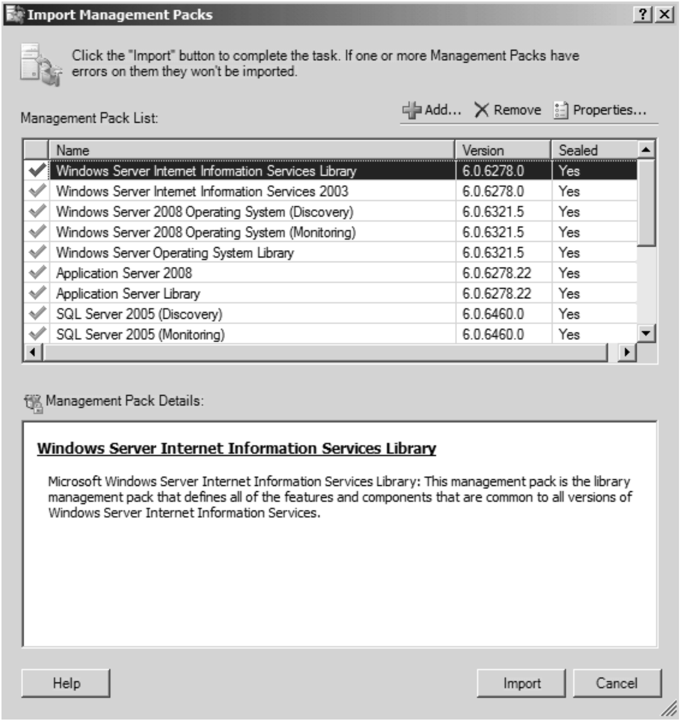
   a. Launch Server Manager on the OpsMgr server.

   b. Move to the Configuration, then Local Users and Groups, and then the Groups node in the Tree pane.

   c. Double-click Administrators and click Add.

   d. Click Object Types, select Computers, and click OK.

   e. Type in the name of your SCVMM Server—for example, **SCVMM01**—and click Check Name. Click OK twice.



Click the "Import" button to complete the task. If one or more Management Packs have errors on them they won't be imported.

Management Pack List:

	Name	Version	Sealed
✓	Windows Server Internet Information Services Library	6.0.6278.0	Yes
✓	Windows Server Internet Information Services 2003	6.0.6278.0	Yes
✓	Windows Server 2008 Operating System (Discovery)	6.0.6321.5	Yes
✓	Windows Server 2008 Operating System (Monitoring)	6.0.6321.5	Yes
✓	Windows Server Operating System Library	6.0.6321.5	Yes
✓	Application Server 2008	6.0.6278.22	Yes
✓	Application Server Library	6.0.6278.22	Yes
✓	SQL Server 2005 (Discovery)	6.0.6460.0	Yes
✓	SQL Server 2005 (Monitoring)	6.0.6460.0	Yes

Management Pack Details:

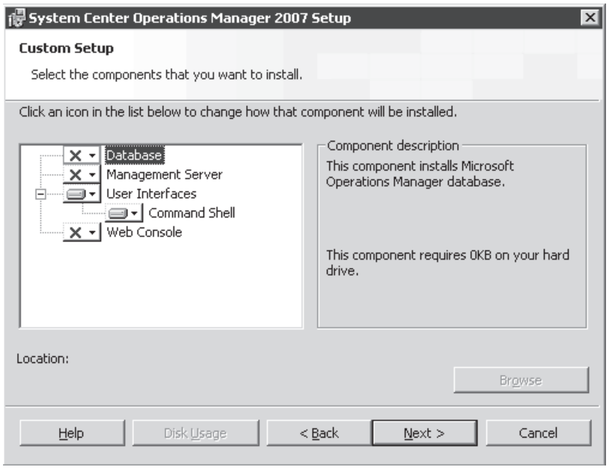
Windows Server Internet Information Services Library

Microsoft Windows Server Internet Information Services Library: This management pack is the library management pack that defines all of the features and components that are common to all versions of Windows Server Internet Information Services.

FIGURE 6-5 Importing management packs

f. Move to the Configuration, and then the Services node in the Tree pane and select the OpsMgr SDK Service in the list of services. Click Restart to recycle the service. Minimize Server Manager.

5. Log on to the SCVMM Server. Locate the installation files for OpsMgr and place them into the Documents folder on the SCVMM Server. Double-click SetupOM.exe file to install the OpsMgr console. Click Run to start the installation.
6. The OpsMgr installation screen appears. Click Install Operations Manager 2007 under Install. Click Next.
7. Accept the license and click Next.
8. Type your name, your organization's name, and your license key and click Next.
9. Do not install the Database, the Management Server, or the Web Console. Select only User Interfaces and Command Shell (see Figure 6-6). Click Next.
10. Choose whether you want to send customer improvement data to Microsoft and click Next.
11. Click Install to begin the installation.
12. Choose not to start the console and then click Finish. Click Exit to close the Setup Page.
13. Double-click SP1Ugrade.exe and then click Run to start the program.



System Center Operations Manager 2007 Setup

Custom Setup

Select the components that you want to install.

Click an icon in the list below to change how that component will be installed.

- ☒ Database
- ☒ Management Server
- User Interfaces
  - Command Shell
- ☒ Web Console

Component description

This component installs Microsoft Operations Manager database.

This component requires 0KB on your hard drive.

Location:

FIGURE 6-6 Installing the OpsMgr console

14. Click Operations Manager 2007 under Apply Service Pack 1. Click Yes if an update warning appears.
15. Select Upgrade To Operations Manager SP1 and click Next.
16. Accept the license agreement and click Install.
17. When the installation completes, click Finish. Click Exit to close the OpsMgr Setup window.

Your OpsMgr console is installed. Now add the systems to manage to OpsMgr:

1. Log on to the OpsMgr server with local administrative access rights. Launch the OpsMgr Administration Console. Make sure Administration is selected in the Tree pane and that you are in Administration view.
2. Click Configure Computers And Devices To Manage under Actions in the Details pane. Click Next.
3. Choose Automatic Computer Discovery and click Next. This will verify Active Directory Domain Services for computer names.
4. Choose Use Selected Management Server Action Account and click Discover.
5. Click Select All to choose all discovered computers. Make sure Agent is selected as the Management Mode and click Next.
6. Leave the target folder as is and use the Local System account to install and run the agent. Click Finish.
7. Click Close to close the Agent Installation window when all installations are complete.

IMPORTANT **OpsMgr MANAGEMENT AGENTS**

Perform the installation manually on each machine if the remote installation does not work properly. Use the OpsMgr setup files for the installation and make sure you upgrade the agent to SP1.

IMPORTANT **MANAGING VMs**

If you want to use this OpsMgr server to monitor VMs, you must add the agent inside the VM's guest operating system. In many cases, your VMs will belong to different AD DS forests and therefore you will need to use the manual agent installation process.

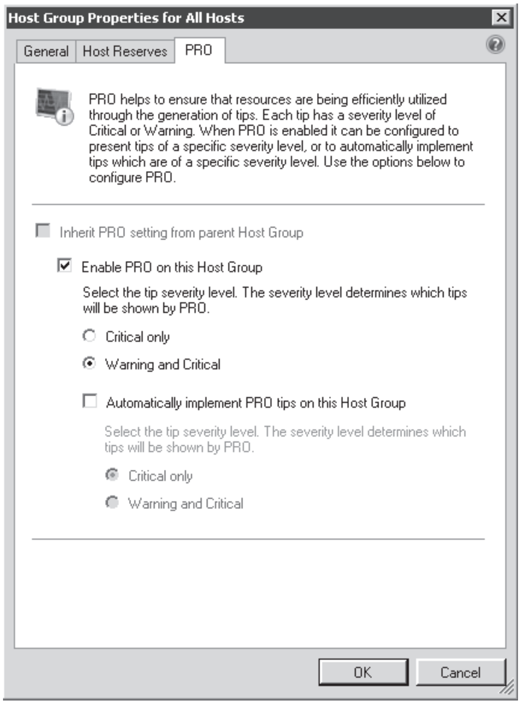
IMPORTANT **MANAGING VMware HOSTS**

If you are also managing VMware hosts, you don't need to install an agent. OpsMgr uses the VMware Web APIs to monitor host status.

Now prepare the OpsMgr server for SCVMM intregration. Perform this task on the OpsMgr server.

1. Open Windows Explorer, locate the SCVMM installation files, double-click Setup.exe, and then click Run to start the program.
2. Click Configure Operations Manager under Setup.
3. Accept the license terms and click Next.
4. This tool automatically links you to the Microsoft Customer Experience program. Click Next.
5. The wizard performs a prerequisite check. Click Next.
6. Choose the default installation location and click Next.
7. Enter the SCVMM Server name—for example, **Contoso\SCVMM01**—and leave the port (8100) as is. Click Next.
8. Click Install. This installs the SCVMM Administration console on your OpsMgr server and also verifies that all prerequisites are set properly.
9. Check for updates and create a shortcut on your Desktop if you want to. Do not choose to open the SCVMM Administrator Console. Click Close.
10. If no updates are available, close the Internet Explorer window. If updates are available, install them.
11. Click Exit to close the SCVMM Setup window.
12. Click Start, click All Programs, click Microsoft System Center, click Virtual Machine Manager, and then click Windows PowerShell – Virtual Machine Manager. If prompted, select Always to make sure this tool is trusted on this computer.
13. Return to the SCVMM Server and the Administrator Console to complete the configuration.
14. Choose the Administration View and click User Roles. Double-click Administrators in the Details pane. Click Add and type in your OpsMgr Action and Agent account names. If the Agent is using Local System, add the OpsMgr Computer account name. Click Check Names and then click OK twice. This grants access rights to your OpsMgr server to SCVMM.

15. Select the System Center node, right-click Operation Manager Server in the results pane, and then click Modify.
16. Enter the name of the Root Management Server of your Operations Manager installation—for example, **SCOM01**—and click OK. This action can take some time to complete.
17. Change to the Hosts view. Right-click the All Hosts group and choose Properties.
18. Click the PRO tab and select Enable PRO On This Host Group. Choose Warning and Critical as the implementation mode, but do not choose Automatically Implement PRO Tips On This Host Group. It is preferable to become familiar with PRO tips before assigning them automatically to host and client machines (see Figure 6-7). Click OK.



PRO helps to ensure that resources are being efficiently utilized through the generation of tips. Each tip has a severity level of Critical or Warning. When PRO is enabled it can be configured to present tips of a specific severity level, or to automatically implement tips which are of a specific severity level. Use the options below to configure PRO.

□ Inherit PRO setting from parent Host Group

☑ Enable PRO on this Host Group

Select the tip severity level. The severity level determines which tips will be shown by PRO.

○ Critical only

● Warning and Critical

□ Automatically implement PRO tips on this Host Group

Select the tip severity level. The severity level determines which tips will be shown by PRO.

● Critical only

○ Warning and Critical

FIGURE 6-7 Enabling PRO

Your configuration is complete. From now on, the PRO window will automatically open in the console when and if tips are generated by the information collected by OpsMgr.

NOTE **AUTOMATIC TIP IMPLEMENTATION**

After you get used to PRO, you can return to the Host Group's Properties window to set automatic PRO actions on the group.

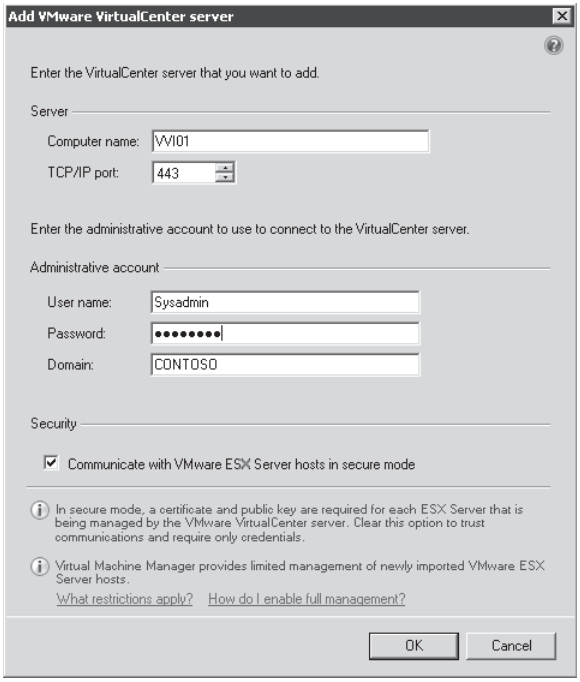
EXAM TIP **PRO INHERITANCE**

Note that all subgroups within each Host Group are set to automatically inherit the PRO settings from parent host groups. You can clear this option if you have a host group that you do not want to include in PRO. You can also clear this option on individual VMs through their settings.

Integrating SCVMM with VMware ESX

You can also manage VMware host servers with SCVMM. To do so, you must add the VMware server to the managed hosts in SCVMM. If your servers are part of a VMware Virtual Infrastructure, you can add the entire infrastructure at once. Proceed as follows:

1. Log on to the SCVMM Server and open the Administrator Console.
2. Add your VMware Virtual Infrastructure server to SCVMM. SCVMM relies on this tool to use the VMware Infrastructure APIs to manage ESX hosts. Make sure you are in the Hosts view and click Add VMware VirtualCenter Server in the Actions pane.
3. Enter the computer name, leave the port as is, and enter appropriate credentials. Make sure Communicate With VMware ESX Server Hosts In Secure Mode is selected and click OK (see Figure 6-8).



Add VMware VirtualCenter server

Enter the VirtualCenter server that you want to add.

Server

Computer name: VVI01

TCP/IP port: 443

Enter the administrative account to use to connect to the VirtualCenter server.

Administrative account

User name: Sysadmin

Password: ••••••••

Domain: CONTOSO

Security

☑ Communicate with VMware ESX Server hosts in secure mode

In secure mode, a certificate and public key are required for each ESX Server that is being managed by the VMware VirtualCenter server. Clear this option to trust communications and require only credentials.

Virtual Machine Manager provides limited management of newly imported VMware ESX Server hosts.

FIGURE 6-8 Adding a VMware VirtualCenter server

EXAM TIP **SECURE VMware COMMUNICATIONS**

When you use secure communications between VMware and SCVMM, you must have both a valid account and a valid server certificate on each host. This enables secure SSL communications on port 443. If your servers are using self-signed certificates, you must import the certificate into your SCVMM Server's operating system. View the certificate and choose Import to do so.

EXAM TIP **VMware VERSIONS**

SCVMM 2008 can integrate with VMware VirtualCenter 2.0.1 and 2.5 and ESX Server 3.0.2 and 3.5 as well as ESXi (formerly ESX 3i).

4. The hosts that are part of the VirtualCenter will be imported and placed into a special VMware host group. To finalize the configuration of each host—they are listed with a status of OK (Limited)—you must add a secure account to the properties of each host. Right-click the host name and choose Properties.
5. Click the Security tab and type the user name and password for the appropriate account in the Credentials For This Host section.
6. In the Certificate And Public Key section, click Retrieve to upload the certificate and its public key.
7. Select Accept Both The Certificate And Public Key For This Host and click OK. Repeat for each VMware host. The status should change to OK when this is complete.

Your SCVMM Server is now managing the VMware infrastructure. If you add new hosts to VirtualCenter, you will need to use the Add Host Wizard and choose a VMware ESX server to include this server in the SCVMM infrastructure. Now that your machines are integrated to SCVMM, you can perform V2V migrations between VMware and Hyper-V.

Table 6-2 outlines the different features that are available when managing ESX hosts in Secure or Non-secure mode. As you can see from the information in this table, it is always best to use Secure mode.

TABLE 6-2 VMware Host Modes in SCVMM

ACTION	SECURE (STATUS OK)	NON-SECURE (STATUS OK (LIMITED))
Start, Pause And Stop VM	Yes	Yes
Modify Settings	Yes	Yes
Create And Manage Checkpoints (similar to Hyper-V Snapshot)	Yes	Yes
Remove VM	Yes	Yes
Move With VMotion (move hosts while machine is running)	Yes	Yes

ACTION	SECURE (STATUS OK)	NON-SECURE (STATUS OK (LIMITED))
Migrate (move or convert with V2V) With SCVMM	Yes	No
Save Or Discard Machine State	Yes	No
Store In VMM Library	Yes	No
Clone Within VirtualCenter Group Or On Same Host	Yes	No
Create VM From Blank Disk Or From Template	Yes	No

Performing Source-to-Target Conversions

When you're ready to perform your conversions, you'll need to look to a series of tools to support the process. Manual conversions really only require a hypervisor engine that you can use to generate new VMs and then migrate the workload. But offline and online conversions need other tools to support the process. As you have seen, SCVMM is a great tool in support of conversions. Table 6-3 outlines the conversion types supported by SCVMM.

TABLE 6-3 SCVMM Source-to-Target Conversions

SOURCE PLATFORM	TARGET PLATFORM	METHOD TO USE
Physical machine	Hyper-V	P2V Conversion
Hyper-V	Hyper-V	Migration or Move
Virtual Server	Virtual Server	Migration or Move
Virtual Server	Hyper-V	Migration or Move
VMware ESX Server	VMware ESX Server	Migration or Move
VMware ESX Server	Hyper-V	V2V Conversion
VMware ESX Server	Virtual Server	V2V Conversion

You can also convert machines from Virtual PC to Hyper-V, but you must load them into a managed host running Virtual Server first to perform a move to Hyper-V.

SCVMM supports VM migrations in three ways:

- Drag the VM onto a new host server.
- Drag the VM onto a new host group. This uses automatic placement to choose the best host in the group for the VM.
- Use the Migrate command in the Actions pane. This launches the Migrate Virtual Machine Wizard. In some cases, you can use Convert Physical Machine or Convert Virtual Machine.

SCVMM is not the only tool available to support these migrations. Some other useful tools are covered in the next sections. These sections also cover conversions, migrations, and movements through SCVMM.

Migrating from Physical Machines

As you can see, you have several ways to convert source machines to Hyper-V VMs even without a conversion tool. Source machines can either be physical or virtual machines, but because the whole point of implementing a resource pool is to transform your end user–facing workloads into VMs, you will most likely be performing a number of P2V conversions. If the number of conversions you must perform is considerable, you should obtain SCVMM at the very least.

In addition, you should integrate SCVMM with OpsMgr to be able to rely on PRO, especially if you have a vast number of physical machines to convert. This helps during several aspects of the conversion:

- It supplements your original performance assessment.
- It relies on this additional assessment to suggest a more intelligent placement because it relies on both host server resource availability and workload performance requirements.
- It continues to provide performance optimization after the workload has been migrated.

If you rely on SCVMM to perform the conversion, you should aim for online conversions as much as possible. Although the conversion process may affect the source machine's performance during conversion, you can opt to perform the conversion during off hours to minimize the impact on end users. Remember that online conversions are only supported for workloads that are running on the Windows operating systems that are supported as enlightened guests in Windows Server 2008 Hyper-V. Also remember that even if the operating system is supported, the workload itself might not be supported for online conversions. This means that the online conversion process is only supported on the following Windows operating systems:

- Windows Server 2008
- Windows Server 2003 (32-bit) SP1 or later
- Windows Server 2003 (64-bit) SP1 or later
- Windows XP Professional (32-bit) SP2 or later
- Windows XP Professional (64-bit) SP2 or later
- Windows Vista Service Pack 1 (32-bit)
- Windows Vista SP1 or later (64-bit)

EXAM TIP **OFFLINE CONVERSIONS**

Remember that all of the operating systems that are supported for online conversion are also supported for offline conversions.

If your source computer does not include these operating system versions, you can upgrade the operating system to a newer version or simply apply the appropriate service pack before performing the conversion. If offline conversions are your only choice for a source machine, the physical server must include the following minimum requirements:

- 512 MB of RAM to support booting into Windows PE.
- Must be a trusted computer. This means it must be in a workgroup for which you have administrative credentials, it must be in the same domain as the SCVMM server, or it must include a full two-way trust if it is in a different domain or forest.
- Must include enough disk space to support the installation of the SCVMM P2V Agent. 1 MB of disk space is all that is required (the agent files are 888 KB in size and are installed in %ProgramFiles%\Microsoft System Center Virtual Machine Manager 2008 P2V Agent), but you should increase this to 10 MB as a minimum. Note that this installation is only temporary and is required for both offline and online conversions.
- If a firewall is enabled, an exception is required for the Remote Administration service. SCVMM can create this exception automatically. This exception can be removed once the conversion is complete.

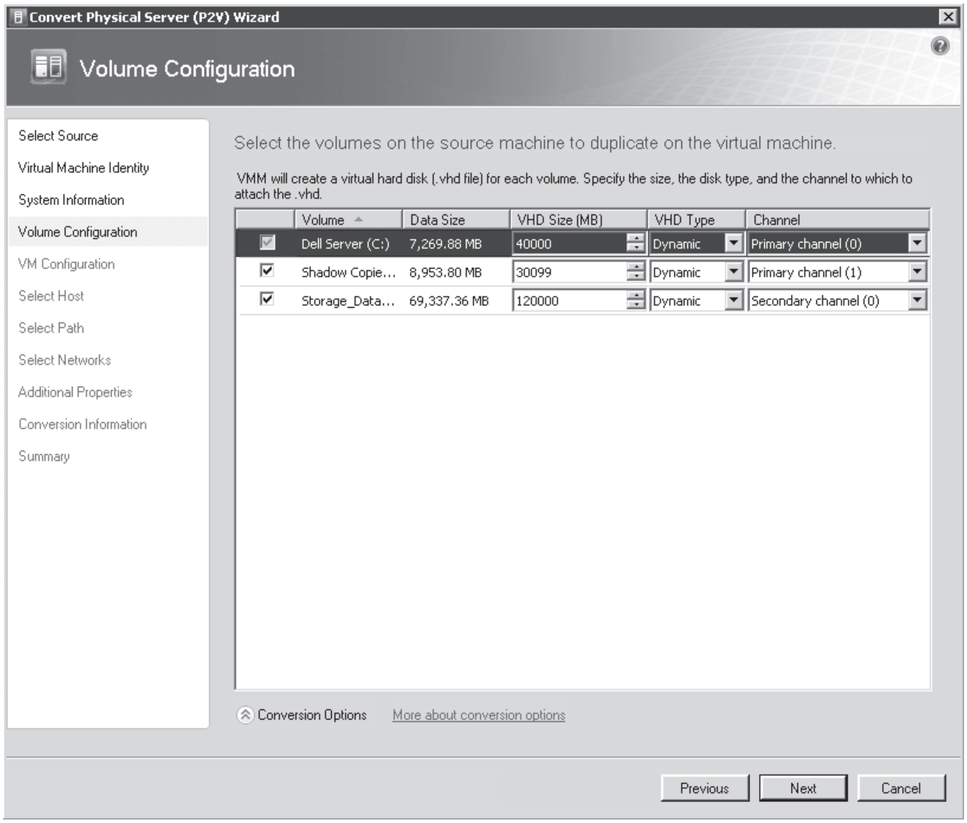
EXAM TIP **WINDOWS NT SERVER 4**

SCVMM does not support the conversion of physical machines running Windows NT Server 4 even with updated service packs. To migrate a physical machine from NT 4 to a Hyper-V VM, you must use an intervening migration step. For example, you can use the Microsoft Virtual Server 2005 Migration Toolkit (VSMT), which can be found at *http://technet.microsoft.com/en-us/virtualserver/bb676674.aspx*. Alternatively, you can also use a third-party method such as generating a disk image of the NT machine and then converting the disk image to a VHD.

Also note that in both online and offline conversions, SCVMM converts the physical machine's disks to VHDs only. Keep the following in mind during this process:

- If you intend to use pass-through disks, consider converting the VM's disks to VHDs first, then converting the VHDs to pass-through disks.
- To speed the conversion process, consider using dynamically expanding VHDs during the conversion, and then convert the dynamically expanding VHDs to fixed-size VHDs after the conversion is complete. Using dynamically expanding disks at first will only create files that are relatively the same size as the contents of the physical source disks.
- Consider resizing your VHDs before the conversion begins. Physical machines, especially older physical machines, often have disks that are smaller than what is required by more modern machines and operating systems. Take advantage of the Volume Configuration window to resize volumes, especially system volumes on older machines (see Figure 6-9).

When you perform the conversion, the process will carry out several tasks, which are outlined in Table 6-4. The various choices you are presented with in the SCVMM P2V Wizard are outlined in Table 6-5. You launch the P2V Wizard by using the Convert Physical Server command in the top portion of the Actions pane. This command is available in all views except the Administration view.



Select the volumes on the source machine to duplicate on the virtual machine.

VMM will create a virtual hard disk (.vhd file) for each volume. Specify the size, the disk type, and the channel to which to attach the .vhd.

	Volume	Data Size	VHD Size (MB)	VHD Type	Channel
☑	Dell Server (C:)	7,269.88 MB	40000	Dynamic	Primary channel (0)
☑	Shadow Copie...	8,953.80 MB	30099	Dynamic	Primary channel (1)
☑	Storage_Data...	69,337.36 MB	120000	Dynamic	Secondary channel (0)

FIGURE 6-9 Resizing target VHDs

TABLE 6-4 Offline vs. Online SCVMM P2V Conversion Tasks

ITEM NUMBER	OFFLINE CONVERSION	ONLINE CONVERSION
Task Group Name	Physical-to-virtual conversion	Physical-to-virtual conversion
Step 1	Collect machine configuration	Collect machine configuration
Step 1.1	Add source machine agent	Add source machine agent
Step 2	Create virtual machine	Create virtual machine
Step 3	Copy hard disk	Copy hard disk
Step 3a	Boot the physical machine into Windows PE	
Step 3.1	Deploy file (using LAN)	Deploy file (using LAN)
Step 3b	Boot the physical machine back into the original operating system	
Step 4	Make operating system virtualizable	Make operating system virtualizable

ITEM NUMBER	OFFLINE CONVERSION	ONLINE CONVERSION
Step 4.1	Install Virtual Machine components	Install Virtual Machine components
Step 4.2	Start virtual machine to install Virtual Machine components	Start virtual machine to install Virtual Machine components
Step 4.3	Stop virtual machine	Stop virtual machine
Step 5	Remove source machine agent	Remove source machine agent
Step 5.1	Remove Virtual Machine Manager agent	Remove Virtual Machine Manager agent

As you can see, there are only slight differences between the offline and the online conversion, but the impact on end users between the two is considerable.

TABLE 6-5 The SCVMM P2V Conversion Wizard

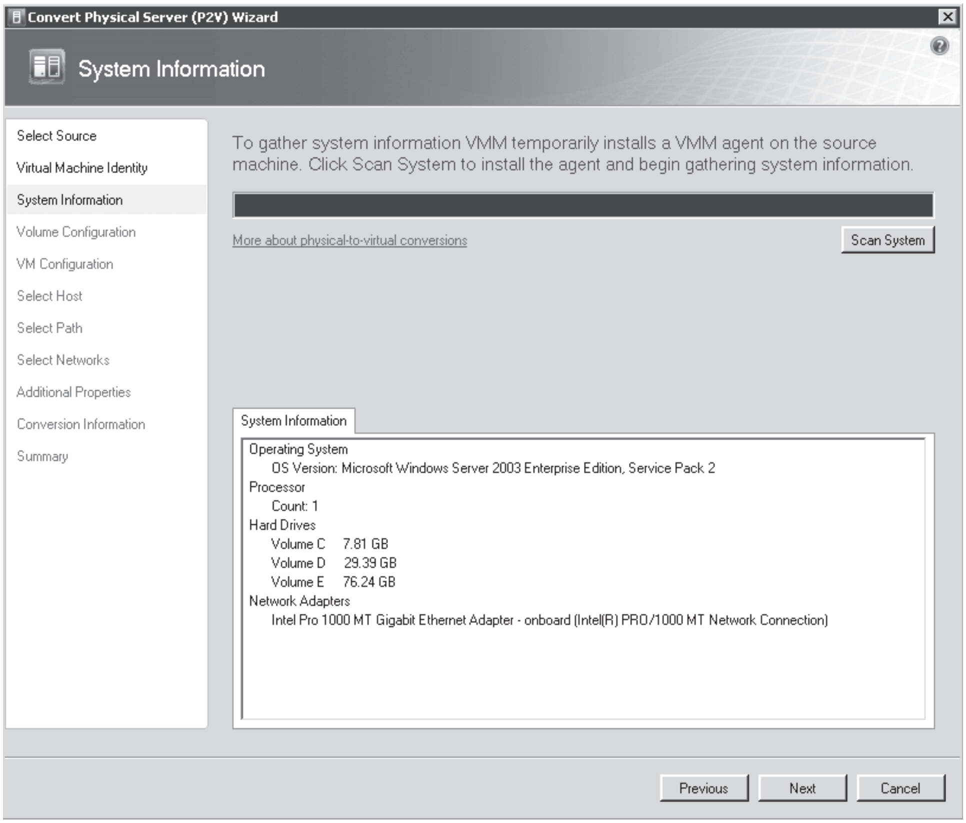
WIZARD PAGE	ACTION
Select Source	Select the source physical computer that you want to convert to a virtual machine: ■ Enter the computer name or IP address or use Browse to locate the computer name in Active Directory Domain Services Administrative account: ■ User name ■ Password ■ Domain (or if the source machine is not in a domain, specify the source machine name or IP address)
Virtual Machine Identity	This is where you name the new VM, assign the VM owner, and provide a description for the VM. Descriptions are very useful, especially when you run hundreds of VMs. It is good practice to name the VM with the machine's computer name. Using this approach provides consistent VM displays in both SCVMM and in OpsMgr.
System Information	SCVMM needs to gather summary system information before it can perform the P2V operation (see Figure 6-10). To do so, it installs a temporary agent on the source machine. Click Scan System to install the agent and scan the system. The following information is gathered: ■ Operating system ■ Processor ■ Hard drives ■ Network adapters

WIZARD PAGE	ACTION
Volume Configuration	This page displays the disk volume(s) discovered during the scan. SCVMM creates a virtual hard disk for each volume. You can specify: ■ VHD Size (MB) ■ VHD Disk type: dynamic or fixed; dynamic is the default ■ Channel to which to attach the VHD: IDE or SCSI; remember that you must use IDE for boot and system volumes Note that all volumes are selected by default. You can clear data volumes, but you cannot clear the system volume. By default, the Conversions Options are hidden. Click Conversion Options to display additional information about the conversion mode (see Figure 6-11). This lets you choose between an online and an offline conversion. Online is the default for supported operating systems. This is also where you can select to turn off the source computer after the conversion, moving users to the new VM.
Offline Conversion Options	If the source machine storage and network adapters are not supported in Windows PE by default, you can select Use Storage And Network Drivers From The Following Location and browse to locate the source drivers. These must be located on a network share. If the devices are supported, this option does not appear. Because the offline conversion process reboots the VM into Windows PE, it requires an IP address to work properly. This page lets you assign the IP address to use (see Figure 6-12). Three options are available: ■ Automatic IP address from DHCP ■ Specified IPv6 address ■ Specified IPv4 address You can also select which network adapter (listed by MAC address) to use. Use the source machine's own IP address as a best practice. Because the machine will be off, it will not be using its own IP address.
VM Configuration	On this page, you need to specify the number of virtual processors and the amount of memory to assign to the new VM.
Select Host	SCVMM uses Intelligent Placement to locate an appropriate host from your pool of hosts. Hosts are rated using five-star ratings. Choose the host to use.
Select Path	When you place the VM on a host, you can select the path to the folder that will store the files that make up the VM.
Select Networks	On this page, you choose which network to attach to the VM's adapter(s).
Additional Properties	On this page, configure which actions will be applied to the VM when the host starts or stops.

WIZARD PAGE	ACTION
Conversion Information	SCVMM verifies whether the conversion is possible and suggests a recommendation if the conversion is not possible. For example, SCVMM suggests that domain controllers are best converted while offline (see Figure 6-13). If the conversion mode is supported for the workload, no issues will be detected. If you use the wrong conversion process, use the back button to return to the Volume Configuration page to change the conversion mode.
Summary	On this page, you can view and copy the Windows PowerShell script to be used to generate the new VM. You can also launch the process.

Capturing the Windows PowerShell script lets you automate this process to repeat on any server in your network. More on this topic is covered in Chapter 7, "Automating VM Management with Windows PowerShell."

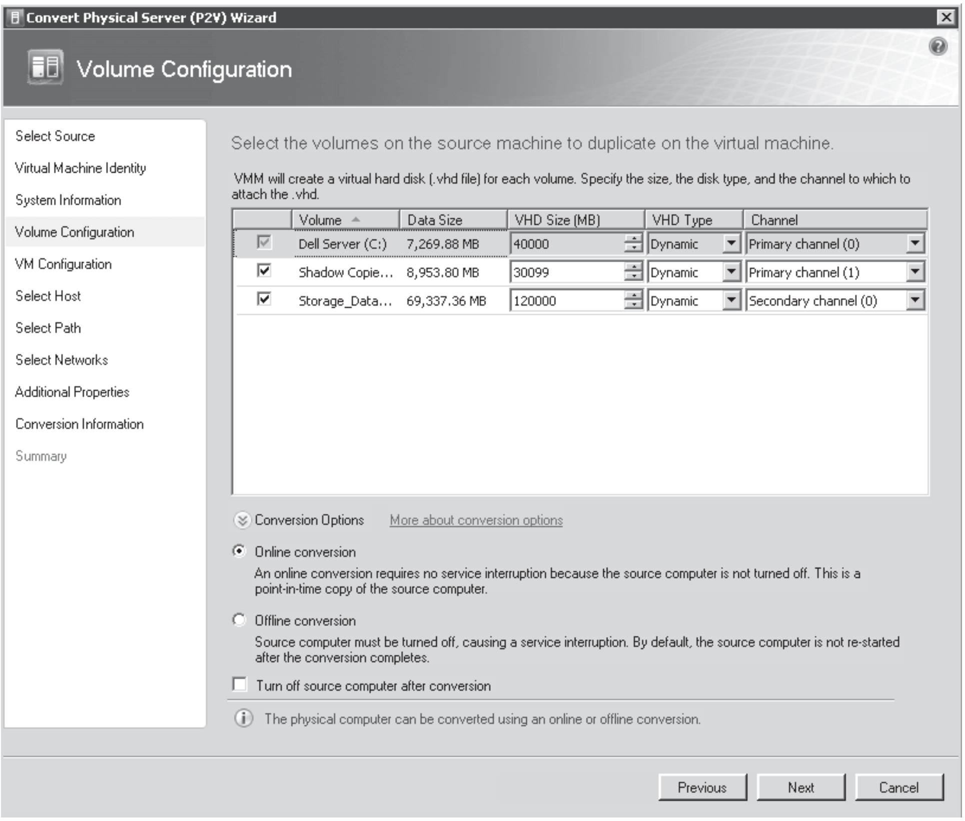
Launching the conversion process opens the Jobs window and displays job status and progress. Close the window when the job is complete.



To gather system information VMM temporarily installs a VMM agent on the source machine. Click Scan System to install the agent and begin gathering system information.

```
Operating System
    OS Version: Microsoft Windows Server 2003 Enterprise Edition, Service Pack 2
Processor
    Count: 1
Hard Drives
    Volume C    7.81 GB
    Volume D    29.39 GB
    Volume E    76.24 GB
Network Adapters
    Intel Pro 1000 MT Gigabit Ethernet Adapter - onboard (Intel(R) PRO/1000 MT Network Connection)
```

FIGURE 6-10 System information captured by the SCVMM P2V Agent



Select the volumes on the source machine to duplicate on the virtual machine.

VMM will create a virtual hard disk (.vhd file) for each volume. Specify the size, the disk type, and the channel to which to attach the .vhd.

	Volume	Data Size	VHD Size (MB)	VHD Type	Channel
☑	Dell Server (C:)	7,269.88 MB	40000	Dynamic	Primary channel (0)
☑	Shadow Copie...	8,953.80 MB	30099	Dynamic	Primary channel (1)
☑	Storage_Data...	69,337.36 MB	120000	Dynamic	Secondary channel (0)

Conversion Options More about conversion options

● Online conversion
An online conversion requires no service interruption because the source computer is not turned off. This is a point-in-time copy of the source computer.

○ Offline conversion
Source computer must be turned off, causing a service interruption. By default, the source computer is not re-started after the conversion completes.

□ Turn off source computer after conversion

The physical computer can be converted using an online or offline conversion.

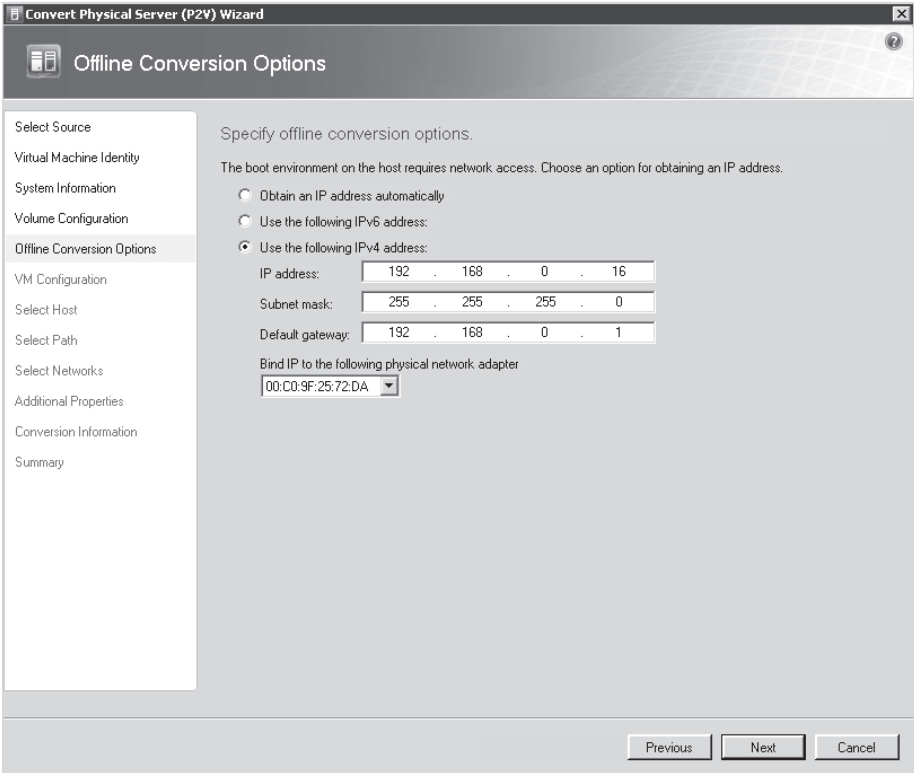
FIGURE 6-11 Choosing between online and offline conversions

Migrating from Virtual Server 2005 or Virtual PC

Migrating machines from Virtual Server 2005 or Virtual PC relies on a V2V conversion process. Conversions are usually relatively simple because all of the products—Virtual Server, Virtual PC, and Hyper-V—use the same virtual hard disk format. However, virtual machines running in Virtual Server or Virtual PC do not use Integration Services or Components. Instead, they use VM Additions that are not compatible with Hyper-V. In addition, the virtual machine configuration (VMC) files used in Virtual Server and Virtual PC are not compatible with the XML files Hyper-V relies on. This means that you must use the following process to convert machines between Virtual PC or Virtual Server and Hyper-V:

1. Begin by launching the machine and removing the VM Additions. Use the Control Panel, Add Or Remove Programs Or Programs, Uninstall A Program tools to do so.

2. Prepare the VHDs. Defragment the VHD using the guest operating system's internal tools. Then compact the VHD using either Virtual PC or Virtual Server tools. In Virtual Server, begin by inspecting the disk and then choosing Compact Virtual Hard Disk (see Figure 6-14). Click Compact to begin the compaction. You may have to run the Precompaction tool included in Virtual Server and Virtual PC on the disk beforehand. To do so, load the Precompact.iso file as the DVD drive in the guest operating system and then use AutoPlay to run the precompaction engine on the disk.



Specify offline conversion options.

The boot environment on the host requires network access. Choose an option for obtaining an IP address.

○ Obtain an IP address automatically

○ Use the following IPv6 address:

● Use the following IPv4 address:

IP address: 192 . 168 . 0 . 16

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

Bind IP to the following physical network adapter

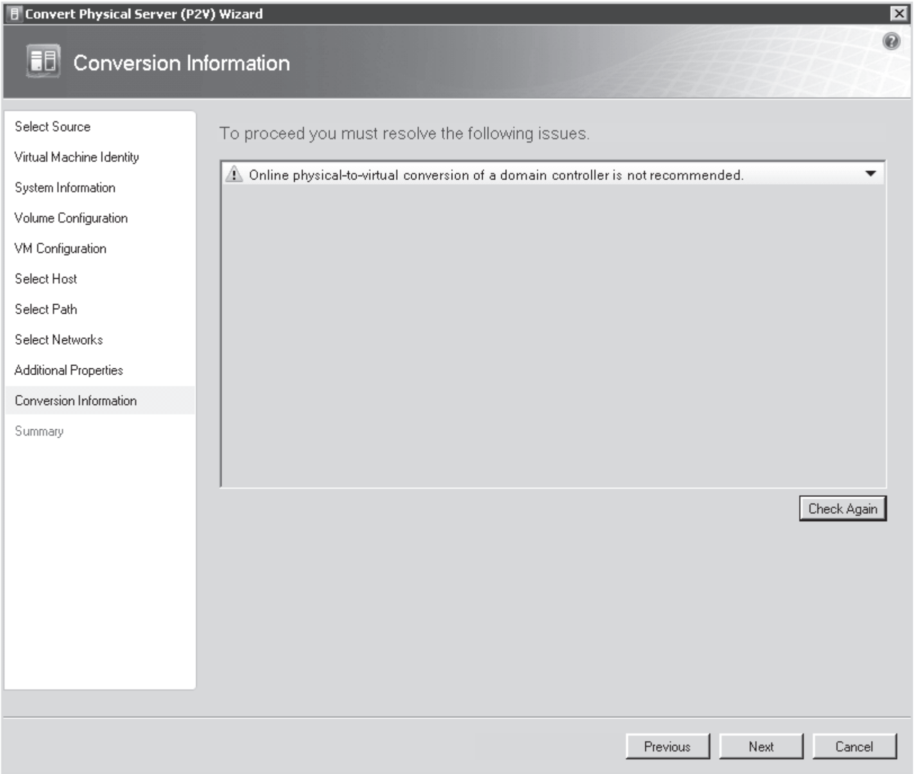
00:C0:9F:25:72:DA

FIGURE 6-12 Assigning an IP address and network adapter for Windows PE

3. Move the VM's VHDs if required.

4. Create a new VM in Hyper-V using the source machine's VHDs or convert the VM's configuration file (VMC) to a Hyper-V configuration file (XML).

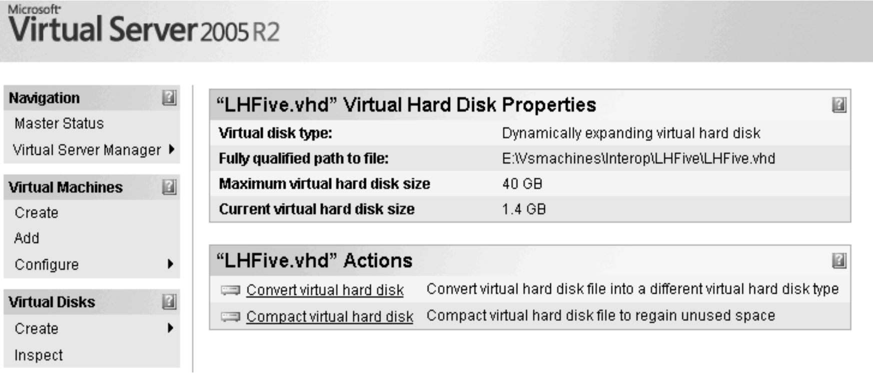
5. Install Hyper-V's Integration Services or Components into the new Hyper-V VM.



To proceed you must resolve the following issues.

⚠ Online physical-to-virtual conversion of a domain controller is not recommended.

FIGURE 6-13 SCVMM does not recommend an online conversion for domain controllers.



“LHFive.vhd” Virtual Hard Disk Properties

Virtual disk type:	Dynamically expanding virtual hard disk
Fully qualified path to file:	E:\Vsmachines\Interop\LHFive\LHFive.vhd
Maximum virtual hard disk size	40 GB
Current virtual hard disk size	1.4 GB

“LHFive.vhd” Actions

Convert virtual hard disk	Convert virtual hard disk file into a different virtual hard disk type
Compact virtual hard disk	Compact virtual hard disk file to regain unused space

FIGURE 6-14 Preparing a VHD drive in Virtual Server

Keep the items in Table 6-6 in mind when you perform the conversion.

TABLE 6-6 Virtual Server and Virtual PC Migration Caveats

SOURCE VMs	HYPER-V TARGETS
Virtual machines that are running on Virtual Server or Virtual PC include a configuration file (.VMC) and data files that include virtual hard disk files (.VHD), media files such as images files (.ISO), and virtual floppy disk files (.VFD).	The only files that can be used by Hyper-V are the .VHD, .ISO, and .VFD files. Configuration files are incompatible with Hyper-V.
Uninstall Virtual Machine Additions before the machine migration.	Only VM Additions version 13.813 and later can be uninstalled in Hyper-V. Hyper-V replaces Virtual Machine Additions with its Integration Services.
Verify the operating system of the virtual machine.	The VMs should run an operating system that takes advantage of Hyper-V Integration Services.
Document the existing configuration settings of the VM that runs in Virtual Server.	This will let you re-create them on the new VM in Hyper-V if you use manual re-creation.
Change the system disk from SCSI to IDE before the migration.	You cannot use a SCSI disk to boot virtual machines in Hyper-V. You will need to change the SCSI disk to an IDE disk. You can use a script to perform this operation. The script is available at: *http://go.microsoft.com/fwlink/?LinkId=135672*.
The source VM should be up to date with all required software updates and hotfixes.	Make sure the source machine's operating system is running the right service pack. For more information, see *http://go.microsoft.com/fwlink/?LinkId=135673*.
Saved State files are not supported for conversion.	You should launch the VM in Virtual Server or Virtual PC and then shut down the VM properly.
Virtual Server and Virtual PC use undoable disks (Undo Disks) whereas Hyper-V uses Snapshots.	Undoable disks are not compatible with Hyper-V. You should commit undoable disks to the VM before converting it.
Merge all differencing disks.	Make sure a single .VHD file is all that remains.

SOURCE VMs	HYPER-V TARGETS
The source VM uses a shared SCSI bus as part of a cluster.	You must break the cluster, migrate one node, and move the VM to an alternate form of shared storage such as iSCSI prior to migration. Virtual Server and Virtual PC supported parallel SCSI to create VM clusters, but Hyper-V does not.
Check hardware abstraction layer (HAL) compatibility.	By default, Hyper-V installs an APIC MP HAL at the installation of Integration Services. Because of this, you may need to reactivate the guest operating system.
If the source VM uses several virtual hard disks, don't start the VM at the end of the creation.	Open the settings for the new VM and add each VHD to the configuration. If you have more than four VHDs for the source VM, add a SCSI controller and attach the extra VHDs to it.
Convert VMs through SCVMM.	If you want to perform the conversion through SCVMM, you must add the Virtual Server or Virtual PC VMs to a managed Virtual Server host so that they are available within the SCVMM interface.

EXAM TIP **HOST SERVER CHIPSETS**

Even if saved states were compatible between different virtualization platforms, they might still not work between different hosts. A saved state includes in-memory instructions for a VM. These instructions differ between processor chipsets. For example, you cannot use a saved state from an Intel processor on an AMD processor and vice versa, you cannot use a saved state from a 32-bit processor on a 64-bit processor, and so on.

MORE INFO **MOVING VMs FROM VIRTUAL SERVER TO HYPER-V**

For more information on the Virtual Server to Hyper-V migration process, go to *http://technet.microsoft.com/en-us/library/dd296684.aspx*.

SCVMM can convert and manage a virtual machine that is running in Virtual Server 2005 R2 SP1. The only requirement is that the virtual machine must have the Virtual Machine Additions version 13.813 or later installed. If not, you must uninstall the VM Additions manually prior to the migration. During the migration, SCVMM uninstalls Virtual Machine Additions, upgrades the hardware abstraction layer (HAL), and installs the virtual guest services.

Using the VMC to Hyper-V Import Tool

If you simply want to convert your VMC files to Hyper-V format and open the VMs in Hyper-V directly, you can use the VMC To Hyper-V Import tool. This tool will convert VMC files to a format that Hyper-V understands. In addition, it does the following:

- Supports VMC files from both Virtual Server 2005 and Virtual PC 2007
- Creates the target VM on either local or remote Hyper-V hosts
- Validates VHD and ISO files attached to the source VM
- Supports virtual disk path editing
- Swaps a system disk from SCSI to IDE
- Supports the specification of a static MAC address for the target VM
- Lets you choose between a legacy and an enhanced virtual network adapter in the target VM
- Supports the modification of processors and other resources as well as management settings in the target VM
- Runs on x86 or x64 versions of Windows Vista or Windows Server 2008

You must still follow the caveats mentioned in Table 6-6 before using this tool to convert your VMCs.

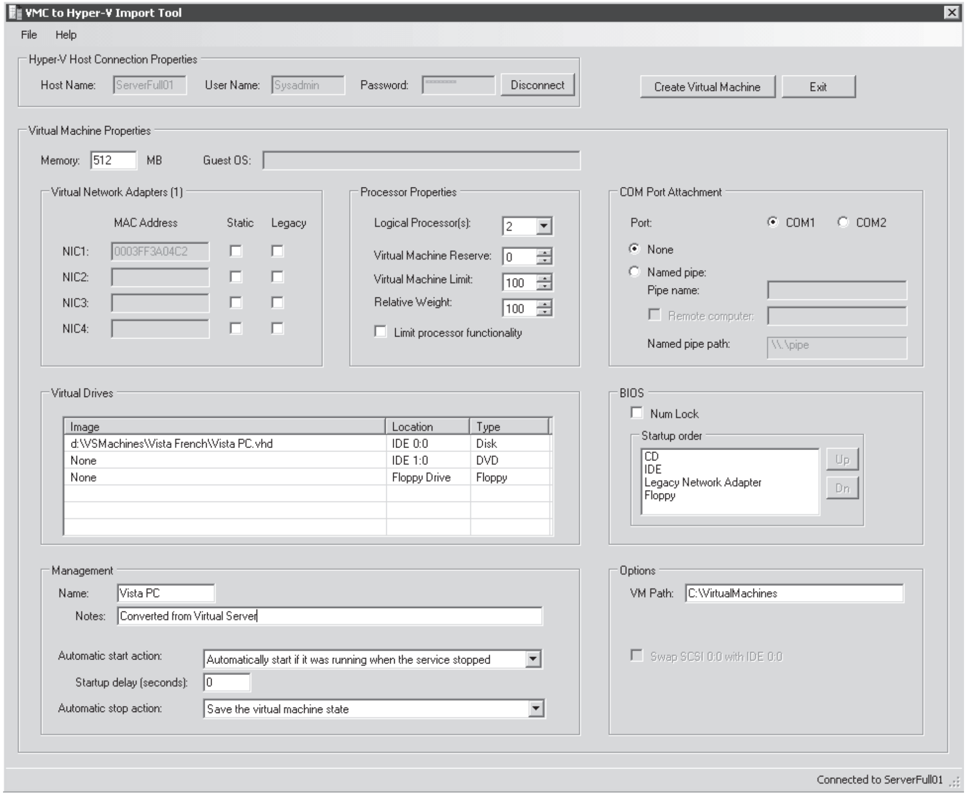
MORE INFO **THE VMC TO HYPER-V IMPORT TOOL**

Obtain the Import tool at *http://go.microsoft.com/fwlink/?LinkId=135683*.

To convert your VMs, download the appropriate version of the tool, save it to the Documents folder, and then proceed as follows:

1. Double-click the compressed file and then double-click the Windows Installer package. Click Run to start the installation.
2. Click Next. Accept the license terms and click Next.
3. Accept the default location and click Next, click Install, and then click Finish.
4. Click Start and then click VMC To Hyper-V at the top of the menu.
5. Type in the Hyper-V host server name, your account, and password. Click Connect.
6. On the File menu, click Open VMC File. You can use either local or remote VMC files. Browse to locate the VMC you want to convert. Select it and click Open.
7. This populates the VMC properties into the dialog box (see Figure 6-15). You can edit most of the settings on this VM. For example, you can change target VHD names, change the machine's name, and add a description. Click Create Virtual Machine when ready.

You'll find this tool quite handy if you have a lot of VMs—especially Virtual PC VMs—to convert from VMC to Hyper-V format.



Hyper-V Host Connection Properties
Host Name: ServerFull01
User Name: Sysadmin
Password: ********

Virtual Machine Properties
Memory: 512 MB
Guest OS:

Virtual Network Adapters (1)

	MAC Address	Static	Legacy
NIC1:	0003FF3A04C2	□	□
NIC2:		□	□
NIC3:		□	□
NIC4:		□	□

Processor Properties
Logical Processor(s): 2
Virtual Machine Reserve: 0
Virtual Machine Limit: 100
Relative Weight: 100
□ Limit processor functionality

COM Port Attachment
Port: ● COM1 ○ COM2
● None
○ Named pipe:
Pipe name:
□ Remote computer:
Named pipe path: \\.\pipe

Virtual Drives

Image	Location	Type
d:\VSMachines\Vista French\Vista PC.vhd	IDE 0:0	Disk
None	IDE 1:0	DVD
None	Floppy Drive	Floppy

BIOS
□ Num Lock
Startup order
CD
IDE
Legacy Network Adapter
Floppy

Management
Name: Vista PC
Notes: Converted from Virtual Server
Automatic start action: Automatically start if it was running when the service stopped
Startup delay (seconds): 0
Automatic stop action: Save the virtual machine state

Options
VM Path: C:\VirtualMachines
□ Swap SCSI 0:0 with IDE 0:0

Connected to ServerFull01

FIGURE 6-15 Converting a VMC to Hyper-V

Migrating from a Third-Party Disk Image

In some cases, you cannot migrate a machine using the various tools that are available for virtual machine management. In other cases, you have system images of the disks that make up a machine and you want to simply convert these images to virtual hard drives to generate a VM from the image. Two tools support this type of conversion: Acronis True Image and WinImage. Both tools offer conversion from a variety of sources to VHDs.

MORE INFO **ACRONIS TRUE IMAGE**

Find Acronis True Image at *http://www.acronis.com*.

Acronis True Image is a disk-imaging technology that captures complete disk backups in the TIB format. It also includes a conversion tool to convert TIB images into a variety of virtual disk formats. For example, it supports the conversion of TIB files to VMDK files, which are the virtual disk format for VMware. It also converts TIB files to VHD format for use with Virtual PC, Virtual Server, Hyper-V, and even Citrix XenServer.

After the TIB image is converted, you can link it to a virtual machine and use it either as a source disk drive for the VM—which would then be used to boot the VM—or simply link it to the VM as a data disk, mount it in the VM, and then recover data from within the new VHD file.

In addition, because driver injection is the most important aspect of a conversion from one state to another—for example, physical to virtual conversions—True Image uses Acronis Universal Restore to inject virtualization drivers into the image during the conversion to VHD format.

To perform a P2V or V2V conversion with True Image, use the following steps:

1. Create TIB images of all of the source machine disks, including the system disk.
2. Convert the images to virtual disks.
3. Create a new VM with the converted disks.
4. Add any additional converted disk to the vM.
5. Start the VM, log on, and complete any plug-and-play configurations presented by Windows.

This converts any version of Windows to a VM.

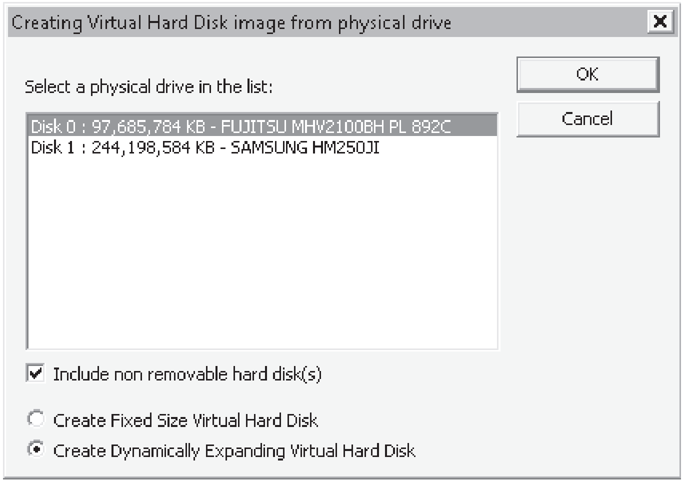
You can also take a True Image backup of a source machine, create a new VM, and perform a True Image restore to the new VM to perform the conversion. Acronis Universal Restore will automatically inject the appropriate drivers during the restore process as long as a driver repository has been created beforehand. Note that this process works in any direction: physical to virtual, virtual to virtual, or even virtual to physical. This makes Acronis True Image a valuable addition to any environment that requires the ability to perform P2V, V2V, or even V2P conversions.

WinImage is also a very useful third-party addition to any resource pool administrator's toolkit. This product has already been mentioned for its ability to convert ISO files to DVDs and vice versa. But in addition to its ability to convert to and from ISO formats, WinImage can do the following:

- Create a virtual hard disk image from a physical disk.
- Restore a virtual hard disk image to a physical disk.
- Convert a virtual hard disk image to another format. This includes the following formats:
  - VHD to VMware VMDK
  - VMDK to VHD
  - IMA (image file) to VHD or VMDK

Creating a VHD from a physical drive converts the file (see Figure 6-16), but it does not replace drivers. You must convert the drivers manually after the conversion.

Converting a virtual disk or a disk image to a virtual disk format (see Figure 6-17) also does not replace or inject drivers. You must perform a manual driver conversion after the source file has been converted. However, you can see that this software tool would be very useful, especially in shops that do not have access to another, more sophisticated conversion tool.



Creating Virtual Hard Disk image from physical drive

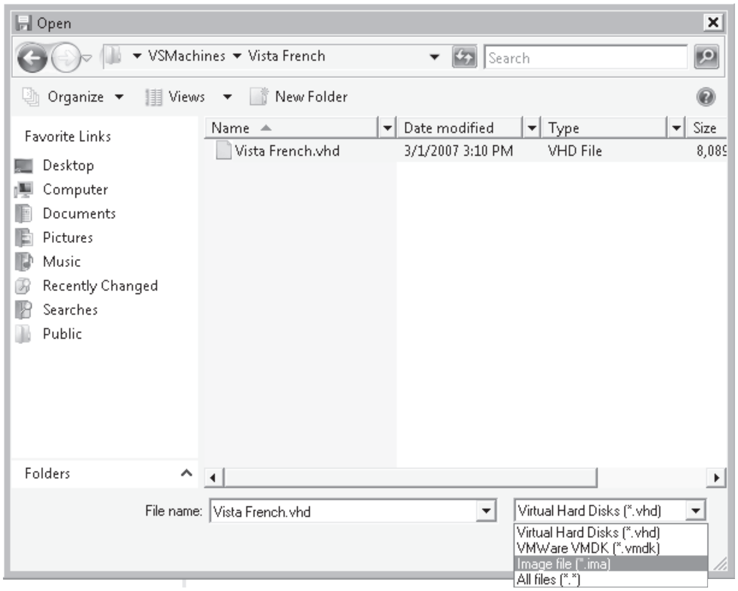
Select a physical drive in the list:

Disk 0 : 97,685,784 KB - FUJITSU MHV2100BH PL 892C
Disk 1 : 244,198,584 KB - SAMSUNG HM250JI

☑ Include non removable hard disk(s)

○ Create Fixed Size Virtual Hard Disk
● Create Dynamically Expanding Virtual Hard Disk

FIGURE 6-16 Using WinImage to convert a physical drive to a VHD



Open

VSMachines ▸ Vista French

Name	Date modified	Type	Size
Vista French.vhd	3/1/2007 3:10 PM	VHD File	8,089

File name: Vista French.vhd

Virtual Hard Disks (*.vhd)

FIGURE 6-17 Using WinImage to convert a disk image to a virtual disk format

MORE INFO **WINIMAGE**

Find WinImage at *http://www.winimage.com*.

Migrating from VMware ESX Server or Virtual Infrastructure

SCVMM will convert virtual machines from VMware ESX format to Hyper-V format. However, only the following guest operating systems are supported for conversion. Also note that the ESX server must be a managed host in your SCVMM environment for the conversion to work.

- Windows Server 2008 (32-bit or 64-bit)
- Windows 2000 Server SP4 and Windows 2000 Advanced Server SP4 or later
- Windows XP Professional (32-bit or 64-bit) SP2 or later
- Windows Vista Service Pack 1 (32-bit or 64-bit)
- Windows Server 2003 SP1 or later (32-bit or 64-bit)

The V2V process converts virtual disks from the VMDK format to VHD, uninstalls VMware Tools, and installs Integration Services. Machines can be dragged from an ESX host to a Hyper-V (or Virtual Server) host to begin the conversion process, or you can use the Convert Virtual Machine command in the Actions menu of the SCVMM Administrator Console. The process uses the following steps:

1. Launch the Conversion Wizard and click Browse to select the source VM to convert. Click OK and then click Next.
2. Change the VM name if you need to, use the default owner, and add a description if required. Click Next.
3. Assign the appropriate resources to the target VM and click Next.
4. Select an appropriate host as presented by Intelligent Placement and click Next.
5. Select the host path to store the target VM and click Next.
6. Attach the network adapters of the target VM and click Next.
7. Modify Additional Properties if required and click Next.
8. Review your settings and click Create to begin the conversion process. You can also click View Script to capture this script for later use.

The Jobs window opens and display the status and progress of the operation.

If you do not use SCVMM or if your VMware virtual machines are not running on ESX servers and are from VMware Workstation or VMware Server, you might want to rely on the VMDK to VHD conversion tool instead.

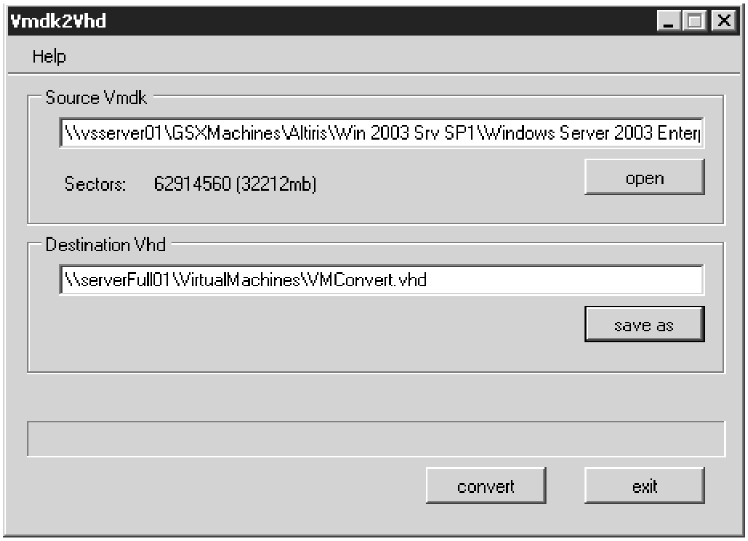
MORE INFO **VMDK TO VHD CONVERTER**

Obtain the VMDK to VHD Converter from the VMToolkit Web site at *http://vmtoolkit.com/files/default.aspx*. You must join the site before you can download the tool. Note that you can also obtain a VHD Resizing tool from this site.

Note that this tool does not perform any VM creation or any operations within the guest operating system. Therefore, you should use the following process to run this tool:

1. Clean up your source VM. Remove VMware Tools from the source machine.
2. Compact the VMDK before the move and remove any undoable disks.

3. Make sure the guest operating system is running a version of the operating system that supports Integration Services or Components. If not, update it if possible.
4. Unzip the tool and then launch VMDK2VHD.exe.
5. Select the source VMDK. Only one disk can be converted at once. Files can be either local or remote.
6. Name the target **VHD** and click Convert (see Figure 6-18). The conversion process will take some time depending on the size of the source disk.



Source Vmdk: \\vsserver01\GSXMachines\Altiris\Win 2003 Srv SP1\Windows Server 2003 Enter

Sectors: 62914560 (32212mb)

Destination Vhd: \\serverFull01\VirtualMachines\VMConvert.vhd

FIGURE 6-18 Converting a VMware disk to a virtual hard disk

7. Repeat for all required disks.
8. Create a new machine in Hyper-V and make sure you assign the system disk to an IDE connection.
9. Boot the VM in Hyper-V and install Integration Services or Components.
10. Move to Device Manager within the VM and make sure all of the devices work properly. If not, remove unnecessary devices and correct any issues that appear.

Your machine is ready to run in Hyper-V.

Migrating from Citrix XenServer

In many ways, migrations from XenServer are much easier than migrations from VMware because XenServer machines can use the VHD virtual disk format. However, some caveats still apply:

- XenServer VMs use paravirtualized drivers that are installed through the XS-Tools.iso image file. These drivers must be removed after you generate a Hyper-V VM. However, they must be kept within the VM during the conversion; otherwise, the VM will not boot in Hyper-V.
- The XenServer VM configuration file is not compatible with Hyper-V. Therefore, you will need to generate a new VM in Hyper-V.

Use the following instructions to convert XenServer VMs:

1. Determine the format of the source disk. If it is in RAW format, you may be able to use it as is in a pass-through disk. If it is in a storage repository, you may be able to convert it to VHD format. You can also use the XenConvert utility to convert the drive to VHD format. Use the Physical to VHD conversion process in this utility.
2. Make sure the guest operating system is running a version of the operating system that supports Integration Services or Components. If not, update it if possible.
3. Shut down the VM and copy the disk—VHD or RAW—to a storage location accessible to Hyper-V.
4. Create a new machine in Hyper-V using the copied disk and make sure you assign the system disk to an IDE connection. Use a virtual disk if the disk is in VHD format. Use a pass-through disk if it is in RAW format.
5. Boot the VM in Hyper-V. It will boot to a working state because of the compatibility of the XenServer Tools. Log on to the VM and install Integration Services or Components depending on the operating system used.
6. Reboot the VM. Remove the XenServer Paravirtualization Tools when the VM is rebooted. Reboot the VM again.
7. Log on and move to Device Manager within the VM to make sure all of the devices work properly. If not, remove unnecessary devices and correct any issues that appear.

Repeat for any VM you want to move from XenServer to Hyper-V.

You can also use the Citrix Project Kensho to convert virtual machines from Citrix to Hyper-V format. Project Kensho has actually been designed as a conversion tool for Open Virtualization Format (OVF) files to either Citrix XenServer or Microsoft Hyper-V formats and vice versa. The OVF format is an open standard format that captures all of the information about a virtual machine and converts it into a transportable format that can be imported into any hypervisor. OVF files include VM configuration files, virtual hard disks, and any other file that makes up the VM. OVF contents are compressed for easier transportability. Project Kensho examines the contents of the OVF and can then convert it to the appropriate file format for either XenServer or Hyper-V (see Figure 6-19). Note, however, that this conversion process does not include the installation of either the Integration Services for Hyper-V or the Paravirtualization Tools for XenServer.

MORE INFO **PROJECT KENSHO AND OVFs**

Obtain the Project Kensho tool from *http://community.citrix.com/display/xs/Kensho*.
For more information on the Open Virtualization Format, go to *http://www.vmware.com/appliances/learn/ovf.html*.

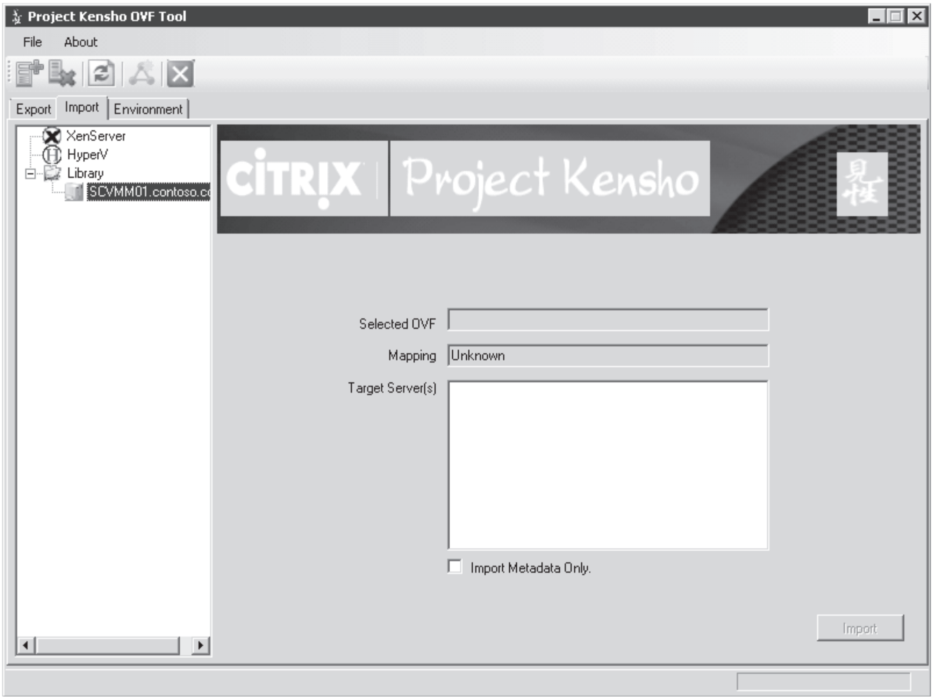


FIGURE 6-19 Running Project Kensho to convert OVF files

Migrating from Hyper-V to Hyper-V (Import/Export)

The last migration type is the migration or the movement of a VM from one Hyper-V host to another. If you run SCVMM, you simply move the VM by right-clicking it and choosing the Migrate command. But if you do not run SCVMM, you need to use the Hyper-V Export and Import feature.

You have already performed this operation in Lesson 2 of Chapter 3, “Completing Resource Pool Configurations.” Keep in mind that the machine must be packaged in Export format before it can be imported on another host. When you export a VM, Hyper-V prepares all of the VM’s files and moves them to a specific folder. When you import the VM, Hyper-V reads the VM configuration from the export folder and runs the VM from that location. If you do not want to run the VM from the export location, you must move it through Windows Explorer prior to the import operation.

EXAM TIP **CONVERSION TERMS**

Note that a lot of terms are used for source-to-target conversions: conversions, migrations, moves, and more. In addition, when you run VMs in a failover cluster, you can perform Quick Migrations. However, there is a major difference between a move and a machine conversion. Quick Migrations are only VM movements and do not involve a migration process at all. Migrations in SCVMM only involve a conversion process when the source and the target hosts run different virtualization software. Keep this in mind as you run through the exam and don’t get confused by different conversion terms.

PRACTICE Performing a Source-to-Target Conversion

In this practice, you will perform a physical to virtual source-to-target conversion. In addition, you will perform an Export/Import operation on a Hyper-V host from SCVMM to see the different approach it uses for this operation. This practice consists of four exercises. In the first exercise, you prepare a source machine for conversion. The source machine will be the workstation identified in the Introduction setup instructions. In the second exercise, you perform the conversion. In the third exercise, you will log on to the VM to examine its operation. In the last exercise, you use SCVMM to export and then import a Hyper-V VM.

EXERCISE 1 Prepare a P2V Migration

In this exercise you will prepare a physical machine for migration. Perform this operation on the workstation identified in the Introduction setup instructions. This machine should be part of the Contoso domain as per those instructions.

1. Log on to your workstation with administrative credentials.
2. View the Device Manager. In Windows XP or Windows Vista, right-click Computer in the Start Menu and choose Properties.
3. In Windows XP, click the Hardware tab and then click Device Manager. In Windows Vista, click Device Manager under Tasks.
4. Scan for any potential hardware issues. Disable any unknown devices (see Figure 6-20).

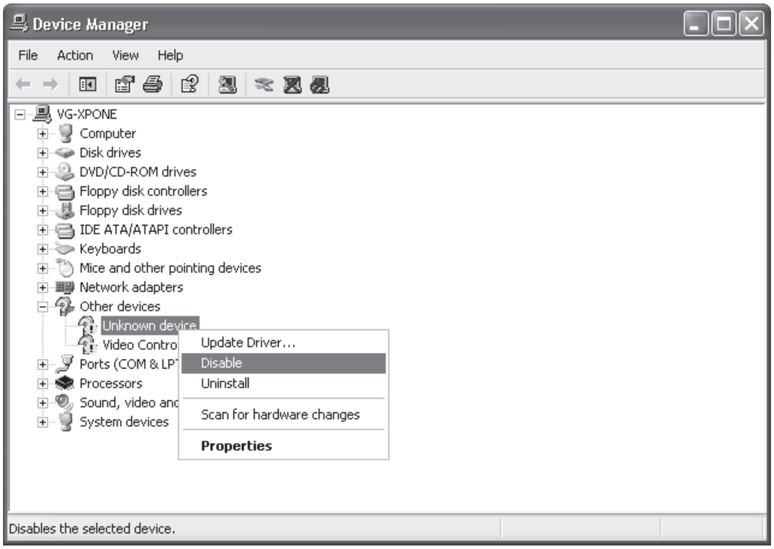


FIGURE 6-20 Disabling unknown devices in Windows XP

5. Close Device Manager when done.

6. Defragment the hard disk. Use the following command on Windows XP or Windows Vista. You need an elevated command prompt in Windows Vista.

```
defrag c:
```

7. Log out of the system after the defragmentation is complete, but leave it running.

Your source machine is ready for the conversion.

EXERCISE 2 Perform a P2V Migration

In this exercise you will migrate your physical workstation to a VM on Hyper-V. Perform this exercise on SCVMM01. Log on with domain administrator credentials.

1. Log on to SCVMM01 and open the Administrator Console. Move to the Virtual Machines view and click Convert Physical Server in the Actions pane.
2. Enter the computer name of your workstation and enter an account name and password that is a local administrator on the workstation. Click Next.
3. Name the VM **WorkstationVM**, assign yourself as owner, and click Next.
4. Click Scan System to collect information on the source machine. Click Next when the scan is complete.
5. Only one volume should be displayed. You can resize it to make it bigger or smaller as needed. Make sure a dynamic VHD is the target and that it is tied to an IDE connector. Click Conversion Options to make sure Online Conversion is selected and that Turn Off Source Computer After Conversion is selected. Click Next.
6. Assign 1 virtual processor to the VM and 1024 MB of memory.
7. Select ServerFull01 as the host for this VM and click Next.
8. Choose D:\VirtualMachines as the target path and click Next.
9. Leave the network attached to None and click Next.
10. Leave the automatic actions as is and click Next.
11. Make sure the Conversion Information lists No Issues and click Next.
12. Review the conversion options and click Convert.

The Jobs window will open and display the conversion task list. The conversion will take some time. Move on to Exercise 3 when the conversion is complete.

EXERCISE 3 Verify the Migrated System

In this exercise you will verify a converted VM. Perform this exercise on SCVMM01. Log on with domain administration privileges.

1. Log on to SCVMM01 and open the Administrator Console. Move to the Virtual Machines view and click WorkstationVM in the Details pane.
2. Right-click the VM and click Start.
3. After the VM is started, double-click its thumbnail image to open a connection to the VM.

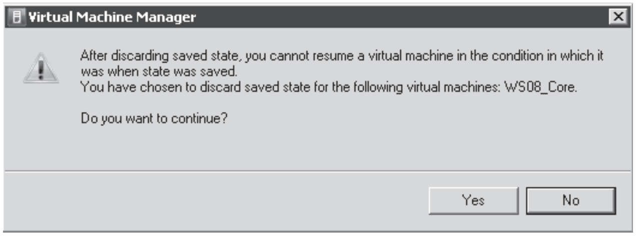
4. Press Ctrl+Alt+Delete and log on with a local administrator account.
5. Move to Device Manager to see whether there are any issues in the VM. Correct any driver issues, exit the remote connection window, right-click the VM, and choose Save.

Your new VM is running properly. It is now in a saved state and will run as a VM. If an activation window appears, you will need to connect the network adapter to an external link in the VM's settings and activate the VM before you can move on to correct potential device issues.

EXERCISE 4 Export and Import a Hyper-V VM with SCVMM

In this exercise you will use SCVMM to export and then import a VM in Hyper-V to see the differences in the process between Hyper-V and SCVMM. In Hyper-V Manager, you can export a VM from one host in a resource pool and then import it in another resource pool. In SCVMM, you migrate a VM from one Hyper-V host to another, but both hosts must be managed hosts and must be under the aegis of the same SCVMM Server. Perform this exercise on SCVMM01. Log on with domain administration privileges.

1. Log on to SCVMM01 and open the Administrator Console. Move to the Virtual Machines view and click VM01 in the Details pane.
2. If the machine is in a saved state, right-click the VM name and choose Discard Saved State. Click Yes when the warning message appears (see Figure 6-21). You can migrate a VM when it includes a saved state, but you must make sure both host servers—the source and the target—include the same chipset. In this case, you delete the saved state to reduce the time it takes to migrate the VM. If the machine does not include a saved state, move to step 3.


Virtual Machine Manager

After discarding saved state, you cannot resume a virtual machine in the condition in which it was when state was saved.
You have chosen to discard saved state for the following virtual machines: WS08_Core.

Do you want to continue?

FIGURE 6-21 Discarding a saved state

3. Right-click the VM name and choose Migrate.
4. Choose ServerCore01 as the destination host and click Next.
5. Choose D:\VirtualMachines as the path and click Next.
6. Leave the network adapter to Not Connected and click Next.
7. Click Move to migrate the VM.

The Jobs window will open and display the status of the job. Close the window when the job is complete. You chose VM01 because it is a small VM with no guest and therefore the migration should be relatively quick. As you can see, however, a move in SCVMM is not the same as an Export/Import operation in Hyper-V Manager—yet in many ways, it achieves the same results.

✓ Quick Check

1. From which disk drive types can Hyper-V virtual machines boot?
2. What are the three different types of workloads in terms of conversions?
3. What are the three possible approaches for conversion?
4. Name at least three capabilities of PRO.
5. What are the types of conversions that SCVMM can support?
6. What type of workloads can you convert when you use the online conversion?
7. What are the differences in steps between online and offline conversions?

Quick Check Answers

1. Hyper-V virtual machines can only boot from an IDE drive. If the source machine is running SCSI or iSCSI drives as a system drive, you need to convert these disks to IDE drives.
2. The three different types of source workloads are simple workloads, advanced workloads, and special workloads.
3. The three possible conversion approaches are manual conversion, semi-automated (offline) conversion, and fully automated (online) conversion.
4. PRO includes several capabilities:
   - Integration with Intelligent Placement
   - Support for clustered hosts and clustered OpsMgr operation
   - Decisions based on health monitoring of both hosts and VMs
   - Internal guest operating system monitoring
   - VM configuration correction suggestions for improved performance
   - Host load balancing to improve host performance
   - Automatic remediation of situations monitored by PRO
5. SCVMM supports P2V conversion for a physical machine to Hyper-V, migration or move for Hyper-V machines or Virtual Server machines, and V2V conversion for VMware EXS Server.
6. The online conversion only supports workloads that are running on the Windows operating systems that are supported as enlightened guests in Windows Server 2008 Hyper-V. But even then, SCVMM recommends offline conversions for certain workload types.
7. The online conversion does not include two steps: rebooting the physical machine into Windows PE and then booting the physical machine back into the original operating system. All other steps are identical.

Case Scenarios

In the following case scenario, you will apply what you've learned in this chapter. You can find answers to these questions in the "Answers" section on the companion CD which accompanies this book.

Case Scenario: Moving from Physical to Virtual Machines

You are the resource pool administrator for Lucerne Publishing, a medium-sized organization that has decided to take full advantage of server virtualization technologies. You have prepared your resource pool and deployed SCVMM 2008 to administer it. All host servers are running Hyper-V. Now you're ready to begin the conversion process and convert your physical machines to VMs running on your Hyper-V resource pool.

Your network consists of 12 servers running various roles (see Figure 6-22). You have categorized each server and outlined its role in a table (see Table 6-7).

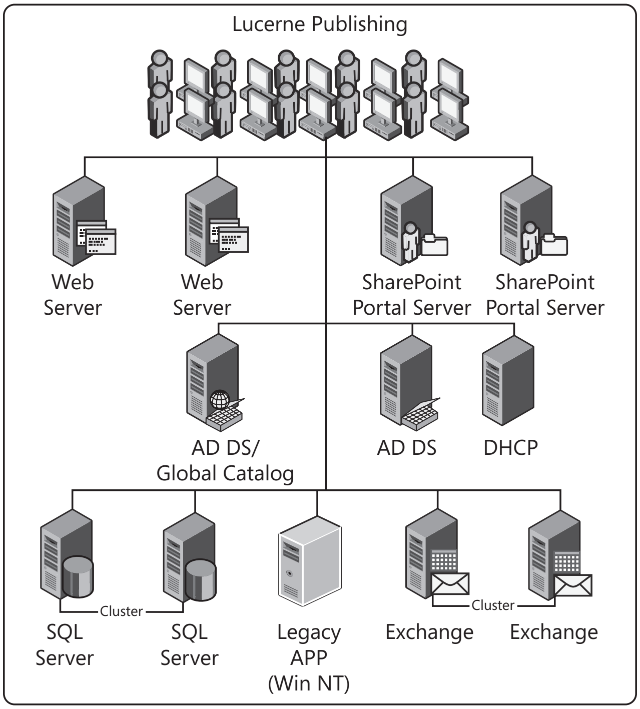


FIGURE 6-22 The Lucerne Publishing network

TABLE 6-7 Lucerne Publishing Server Roles

SERVER NAME	ROLE	CONVERSION TYPE
Server01	Web Server	
Server02	Web Server	

SERVER NAME	ROLE	CONVERSION TYPE
Server03	SharePoint Portal Server	
Server04	SharePoint Portal Server	
Server05	Active Directory Domain Services and Global Catalog	
Server06	Active Directory Domain Services	
Server07	SQL Server in Cluster	
Server08	SQL Server in Cluster	
Server09	Legacy App (Win NT)	
Server10	Exchange Server in Cluster	
Server11	Exchange Server in Cluster	
Server12	DHCP	

You are at the stage where you will determine how to convert each machine. Specifically, you must answer the following questions:

1. Which machines should be migrated manually?
2. Which machines should be migrated offline?
3. Which machines should be migrated online?
4. How should Table 6-7 be filled in?

Suggested Practices

To help you successfully master the exam objectives presented in this chapter, complete the following tasks.

Preparing for Migrations

- **Practice 1** Take the time to assess your own environment and identify which categories your machines fit into. Also determine which process—manual, offline, or online—should be used for which machine.
- **Practice 2** Perform some manual conversions. Examine the results and the process to use very carefully and generate documentation for your own projects.

Performing Migrations

- **Practice 1** Take the time to perform several physical migrations. Use third-party tools from Acronis and WinImage to place with the physical migration process. Use SCVMM (even an evaluation version) to perform migrations with the product. Compare the processes.
- **Practice 2** Perform some V2V conversions if you have access to the proper source VMs. Convert VMware machines to Hyper-V with third-party tools and with SCVMM. Convert Virtual Server or Virtual PC VMs with third-party tools and with SCVMM. Compare all of the processes. Prepare your own migration checklist.

Chapter Summary List

- There are several Hyper-V migration scenarios and it is important to understand and be familiar with each of them.
- The preparation for a migration involves copying the contents of hard disks, transforming the drivers in the machine, and creating a VM configuration file. If the source operating system is not a supported version, it will run as a legacy guest operating system.
- Before you perform conversions, you need to examine the service or application to convert, possibly perform an assessment with PRO, and properly position the target VM on a host with the appropriate resources.
- When working with clean provisioning or manual conversions, you need to understand which workloads can rely on manual conversion in the Windows and Linux environments.
- OpsMgr and SCVMM can work together to manage the virtual and physical machines—even VMware ESX server machines. In addition, you can rely on PRO to convert a vast number of physical machines. If you rely on SCVMM to perform the conversion, aim for online conversions as much as possible. During the process, SCVMM converts a physical machine's disks to VHDs only.
- Virtual Server 2005 or Virtual PC migration relies on a V2V conversion in Hyper-V. If you want to convert VMC files to Hyper-V format and open the VMs in Hyper-V, you can use the VMC To Hyper-V Import Tool.
- To convert system images of disks that make up a machine to virtual hard drives to generate a VM from the image you can use third-party tools such as Acronis True or WinImage.
- The migration from Citrix XenServer is simple because XenServer machines can use the VHD virtual disk format.
- To migrate from Hyper-V to Hyper-V, in SCVMM you need to right-click the name of the VM and choose Migrate; in Hyper-V you use the Hyper-V Export and Import feature.

CHAPTER 8

Securing Hosts and Virtual Machines

Microsoft, as the manufacturer of Microsoft Windows, provides you with tools and guidelines for securing your systems. One excellent example is the *Windows Server 2008 Security Guide*, as well as its sister publication, the *Windows Vista Security Guide*. Both offer a structured way for you to further protect your systems beyond the base protections enabled when you install Windows. In addition, Microsoft has published a specific security guide for Hyper-V, the *Hyper-V Security Guide*. This last guide offers advice on security for host servers and virtual machines along with a strategy for administrative role delegation.

EXAM TIP **HYPER-V SECURITY**

This chapter introduces you to securing Hyper-V host servers and the virtual machines they run. However, you are not expected to understand complex security parameters on the 70-652 exam. The exam has questions about the assignment of role-based access controls in Hyper-V, and this topic is also covered in this chapter. However, any organization deploying Hyper-V as a host environment should be aware of much more in terms of security than the basic topics covered on the exam.

MORE INFO **WINDOWS SERVER 2008, WINDOWS VISTA, AND HYPER-V SECURITY GUIDES**

Look up the *Windows Server 2008 Security Guide* at *http://www.microsoft.com/technet/security/prodtech/windowsserver2008/default.mspx*; look up the *Windows Vista Security Guide* at *http://www.microsoft.com/technet/windowsvista/security/guide.mspx*; and look up the *Hyper-V Security Guide* at *http://technet.microsoft.com/en-us/library/dd569113.aspx*.

UPDATE ALERT **HYPER-V SECURITY GUIDE**

Note that the information from the *Hyper-V Security Guide* is not part of the exam because it was released much later than the exam. However, you should be aware of this document because it is an important part of any Hyper-V deployment.

But security has a life cycle of its own. On the technical side, it begins with the planning and then the installation of a computer system and lasts throughout the duration of its usefulness to you until its retirement. Security is not only a technical operation; it must also involve everyone in your organization. Even if you provide the most stringent technical levels of security on your systems, all of it can come crashing down if your users are not aware of their own responsibilities in the security life cycle.

Protecting traditional networks is nothing new. Protecting virtual infrastructures, however, presents challenges that you may never have faced before. First, you need to understand which types of challenges will arise in the resource pool—the grouping of your host servers. Second, you need to learn whether unknown or unforeseen challenges will arise in the infrastructure you create to run your virtual workloads. This division of the infrastructure into physical and virtual machines demands new approaches and a serious reflection on security practices.

However, traditional security approaches still apply, even if you have two different infrastructures to protect. To protect each of these infrastructures, you must put in place a layered protection system that will provide the ability to perform the following activities:

- Identify people as they enter each infrastructure.
- Identify appropriate clearance levels for people who work within each environment and provide them with appropriate access rights once identified.
- Verify that the person modifying the data is the person who is authorized to modify the data (irrevocability or non-repudiation).
- Guarantee the confidentiality of information once it's stored within your infrastructures.
- Guarantee the availability of information in your infrastructures.
- Ensure the integrity of the data stored within your infrastructures.
- Monitor the activities within each infrastructure.
- Audit security events within the network and securely store historical auditing data.
- Put in place the appropriate administrative activities to ensure that the network is secure at all times and at all levels.

Each of these activities has various scopes of interaction:

- **Local** People interact with systems at the local level; these systems must be protected, whether or not they are attached to a network.
- **Intranet** People interact with remote systems on the internal network. These systems must also be protected at all times, whether they are located on the local area network (LAN) or the wide area network (WAN).
- **Internet** Systems that are deemed public must also be protected from attacks of all types. These are in a more vulnerable situation because they are exposed outside the boundaries of the internal network.
- **Extranet** These systems are often deemed internal, but are exposed to partners, suppliers, and clients. The major difference between extranet and Internet systems is authentication—although there may be identification on an Internet system, authentication is *always* required to access an extranet environment.

The challenge is to identify how security must differ when running virtual infrastructures. Virtual service offerings (VSOs) will run all of the networked services your end users interact with. Therefore, the traditional security measures you undertake when building and designing these services still apply. The fact that users interact with virtual machines instead of physical machines does not change the need for tight security at all levels in this infrastructure.

What does change is how you secure resource pools. By their very nature, resource pools are not designed to interact with users. They are nothing more than host servers that run a virtualization engine. Because of this, they are dealt with by administrators and technicians only. An end user running Microsoft Office Outlook will never have any interaction with the resource pool itself. Instead, the end user will interact with a number of different virtual machines running Active Directory Domain Services, Microsoft Exchange, and perhaps a collaboration engine such as Microsoft Office SharePoint Server. Because all of these machines are virtual, users and host or physical servers have no direct interaction (see Figure 8-1).

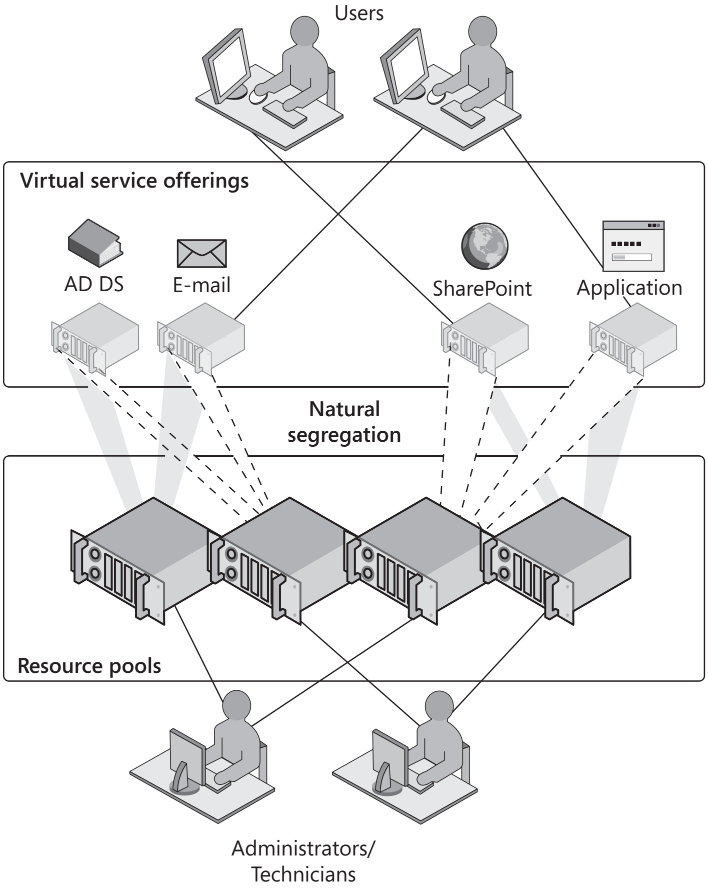


FIGURE 8-1 The natural segregation of resource pools and virtual service offerings

This segregation of the two environments is what forms the key to the protection of your resource pool and the VMs it runs. This is the focus of this chapter.

Exam objective in this chapter:

- Manage and optimize Hyper-V Server.

Before You Begin

To complete this chapter, you must have:

- Experience with Windows Server 2003 and or Windows Server 2008 security implementations.
- Access to a setup as described in the Introduction. In this case, you need to access host servers as well as virtual machines running domain controller services and SCVMM and an administrative workstation.

Lesson 1: Securing the Resource Pool

When you want to secure Hyper-V hosts and management virtual machines, you need to work at several different layers in your Hyper-V installation. Each of these layers adds significant protection to your systems. Understanding these layers will help you protect host systems and the virtual machines they run.

After this lesson, you will understand:

- The potential threats and risks for host computers.
- The security features you should set for hosts.
- How to secure a Hyper-V host.

Estimated lesson time: 50 minutes

Securing Hyper-V Resource Pools

Securing a virtual environment requires a different approach than securing a traditional physical network. A lot of opportunities for threats exist on a traditional physical network, but most of these potential security holes are becoming well known to most administrators. In a virtual environment, several new threats arise from the very fact that end user–facing machines are now virtual machines connected to virtual networks and running on virtual hard disks. This means you must take a different approach to the security of these systems, keeping the following guidelines in mind:

- **VMs are also assets** Virtual machines are important assets and must be treated as such. For example, you cannot apply an antivirus engine to host servers only—it must also be applied to VMs if you are to protect your entire environment.
- **Control resource pool access** If you take the time to segregate the resource pool environment from the virtual workloads it runs, make sure that only trusted individuals have access to the resource pool.
- **Control resource pool tool access** Also make sure that only trusted individuals have access to the remote administration tools for your resource pool. Too many organizations let users run with local administrative privileges and thereby allow users access to tools they should never have.
- **Control virtual engine access** If your users can install their own software on their systems through local administrative access rights, what is to stop them from installing their own software virtualization engine and creating and running their own virtual machines? Make sure that if your users need access to virtual machines, these virtual machines are built and secured through your administrative staff first.

- **Control access to VM files** One of the simplest attacks on virtual machines is the modification or even the replacement of a virtual hard disk drive. For example, if a malicious user has access to the files that make up VMs, it is easy for that user to replace a valid VHD with his or her own untrusted VHD. This could easily cause havoc in your virtual environment. Make sure that you secure VM file paths with NTFS access rights.
- **Reduce host attack surfaces** Run Server Core installations on your host servers to reduce the potential attack surface for that host.
- **Implement proper tools** Make sure your infrastructure includes all of the appropriate tools in support of a proper security policy—antivirus engine, anti-malware tools, update and hotfix package management tools, and so on. Apply this policy to both environments, and if you need to, segregate the tools for each environment. This lets you put stronger policies in the resource pool and more open policies for the VSOs.
- **Segregate network traffic** Make sure you protect network traffic from your resource pool. Use virtual local area networks (VLANs) to control the traffic that manages and maintains host servers, and separate it from any traffic that emerges from the virtual workloads.

These are only a few of the items you'll need to think about as you secure both host servers and the VMs they run.

MORE INFO **SECURITY IN A VIRTUAL WORLD**

For a great overview of the difference between physical and virtual network security, read "Security in a Virtual World," by Kai Axford from the Microsoft Trustworthy Computing Group at *http://technet.microsoft.com/en-us/library/cc974514.aspx*.

MORE INFO **VLAN TAGGING**

More information on VLAN tagging in Hyper-V is covered in Chapter 10, "Working with VM High Availability."

Understanding the Potential Hyper-V Attack Surface

Chapter 2, "Configuring Hyper-V Hosts," discussed the creation of a segregated security context for resource pools. If you were running hypervisors from Citrix or VMware, the security context of the resource pool would automatically be separate from the Windows security context you run in your virtual workloads because both of these hypervisors run on Linux code. But when you are running host servers that rely on the same operating system as the virtual machines you run, you must make a conscious decision to segregate the security context of the resource pool from the virtual environment.

This means creating a separate Active Directory Domain Services forest for resource pools and for virtual service offerings and making sure they are not linked together in any way, such as through multidirectional trusts. When you segregate contexts in this way, end users have no access to the resource pool because they do not have accounts within the resource pool. The resource pool then contains only administrative and technical accounts. This also means that resource pool administrators and technicians must log on to the resource pool with different credentials than those they use in the virtual workload environment.

Remember that so far, your environment can be in one of two configurations. If you run only Hyper-V host servers in your resource pool and you run SCVMM to control them and the VMs they operate, you will have a homogeneous resource pool (see Figure 8-2). If you run multiple hypervisors in your resource pool and you manage them through SCVMM, you will have a heterogeneous resource pool (see Figure 8-3). In either case, the resource pool should be contained within its own AD DS utility forest. This forest can consist of one single root domain and should contain only administrative and technical accounts.

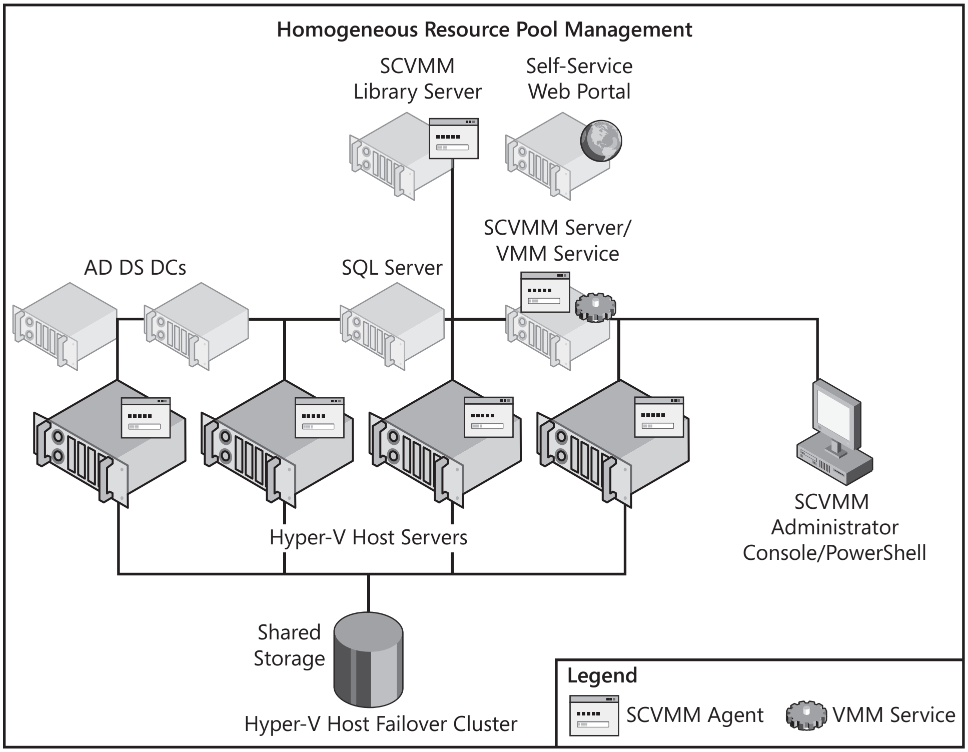

Homogeneous Resource Pool Management
SCVMM Library Server
Self-Service Web Portal
SCVMM Server/ VMM Service
AD DS DCs
SQL Server
Hyper-V Host Servers
SCVMM Administrator Console/PowerShell
Shared Storage
Hyper-V Host Failover Cluster
Legend
SCVMM Agent
VMM Service

FIGURE 8-2 A homogeneous resource pool configuration

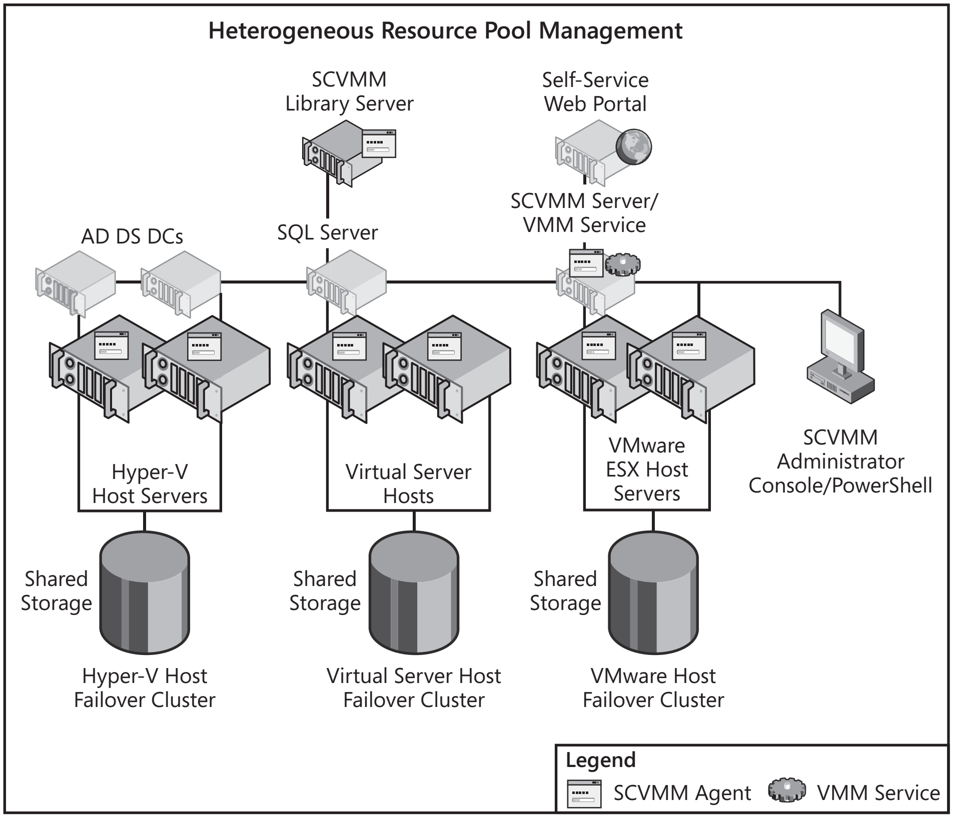


FIGURE 8-3 A heterogeneous resource pool configuration

Few organizations deliberately build out heterogeneous resource pools from scratch. Instead, most of the organizations that run heterogeneous resource pools do so because they already had some form of virtualization technology in place when they introduced Hyper-V into the mix. Therefore, it is reasonable to assume that these organizations already have some form of security in place for the other hypervisors (in this case, Virtual Server and VMware ESX Server).

The new factor in both the heterogeneous and the homogeneous resource pools is Hyper-V and the Windows Server 2008 operating system it relies on. When you add the Hyper-V role to a host server running either the full or the Server Core installation of Windows Server 2008, the role changes the potential attack surface of the computer. It does so by modifying three aspects of the default Windows Server 2008 installation:

- **Installed files** New files are installed in support of the Hyper-V role.
- **Installed services** Services are installed in support of the Hyper-V role.
- **Firewall rules** Rules are modified or enabled with the addition of the Hyper-V role.

Maintaining the integrity of these three aspects is one of the main goals of the security implementation you perform on Hyper-V host servers.

NOTE **USEFUL UTILITIES**

Microsoft's Sysinternals division provides two free utilities that may be useful in the protection of Hyper-V servers: RootkitRevealer and Sigcheck. The former can be used to determine whether root kits have been installed on a host system. The latter can verify the integrity of the files installed in support of Hyper-V. Find RootkitRevealer at *http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx* and Sigcheck at *http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx*.

Note that TripWire also offers tools in this space. TripWire for Servers is useful to monitor changes of any kind on a server configuration. Find it at *http://www.tripwire.com/products/*.

Finally, System Center Configuration Manager (SCCM) also offers support for Desired Configuration Management, which can be useful to monitor host server configurations. Find more information on SCCM's Desired Configuration Management features at *http://www.microsoft.com/systemcenter/configurationmanager/en/us/desired-configuration-management.aspx*.

MORE INFO **HYPER-V COMPONENT LIST**

To see a list of the files, services, and firewall rules installed with the Hyper-V role, go to *http://download.microsoft.com/download/8/2/9/829bee7b-821b-4c4c-8297-13762aa5c3e4/Windows%20Server%202008%20Hyper-V%20Attack%20Surface%20Reference.xlsx*.

Understanding Security Features for Host Computers

With Windows Server 2008, Microsoft has enhanced and improved the base security features of the operating system, as well as provided new security capabilities. The security features of Windows Server 2008 that apply to Hyper-V hosts include:

- **Software restriction policies** These policies can control which code is allowed to run within the network. This includes any type of code—corporate applications, commercial software, scripts, and batch files—and can even be defined at the dynamic-link library (DLL) level. This is a great tool to prevent malicious scripts from even being able to run in your network. In fact, in a Hyper-V resource pool, you can use this policy to disable all scripts except for PowerShell scripts which are more secure than other types such as Visual Basic scripts.
- **Network Access Protection (NAP)** Windows Server 2008 can now enforce client health levels before they are allowed to connect to your network. Given the right infrastructure, NAP can even update the clients before they are given full network access. In a Hyper-V utility domain, you can rely on NAP to make sure all of your administrative workstations are completely up to date in terms of security and other updates before they can connect to a host server or SCVMM management server.
- **Windows Server Firewall with Advanced Security** To facilitate the connections remote systems make with your servers, Windows Server 2008 now provides

an integrated interface for IP-level security (IPsec), with incoming and outgoing communications controls. In a Hyper-V resource pool, you can ensure that any remote connections made to host or management servers are completely secure.

- **Public Key Infrastructure** Windows Server 2008 includes improved PKI, Active Directory Certificate Services (AD CS), that supports auto-enrollment and automatic X.509 certificate renewal. It also supports the use of delta certificate revocation lists (CRLs), simplifying the CRL management process. In large Hyper-V environments, you can rely on AD CS to support encrypted communications between host servers, management servers, and administrative workstations. These communications should always be encrypted because they contain sensitive information such as administrative passwords and configuration file paths.

MORE INFO **ACTIVE DIRECTORY CERTIFICATE SERVICES**

For more information on Active Directory Certificate Services, refer to *MCTS Self-Paced Training Kit (Exam 70-640): Configuring Windows Server 2008 Active Directory* by Holme, Ruest, and Ruest. Find it at *http://www.microsoft.com/learning/en/us/books/11754.aspx*.

- **Digitally signed Windows Installer Packages** Windows Server 2008 supports the inclusion of digital signatures within Windows Installer packages so that administrators can ensure that only trusted packages are installed within the network, especially on host servers.
- **Multiple password policies** AD DS supports the application of multiple password policies, letting you require highly complex passwords for administrators and less complex passwords for end users. In environments that choose not to use a utility forest for the resource pool, you can rely on these password policies to ensure that resource pool administrators have highly complex passwords.
- **Role-based access control (RBAC)** Windows Server 2008 includes the Authorization Manager, which supports the use of role-based access controls for applications. RBAC stores can be in either Extensible Markup Language (XML) or within AD DS. In a resource pool, you rely on RBAC to assign least-privilege rights to administrators and technicians.
- **Permissions management and access-based enumeration** It is now possible to view effective permissions with Windows Server 2008 through the Properties dialog box for file and folder objects. Also, users will only be able to view items they actually have access to, as opposed to previous versions, where users could see all of the contents of a share, even if they could not open the documents. This is useful in resource pools where you can hide the files that make up VMs from unauthorized users.
- **Auditing** Auditing in Windows Server 2008 is now operations-based. This means that it is more descriptive and offers the choice of which operations to audit for which users or groups. You can also audit AD DS changes and use the audit reports to reverse those changes if they were performed in error. This is very useful in resource pools because it tracks all changes to privileged objects.

- **Reset security defaults** It is now much simpler to use the Security Configuration Wizard (SCW) to reapply computer security settings from base templates. In resource pools, you rely on the SCW to create the base security template for your host servers.
- **Small footprint servers** Through the use of Server Core, you can deploy servers that provide a limited set of services and a smaller attack surface. This is the preferred host operating system for any Hyper-V resource pool.
- **Constrained roles and features** Each role or feature only installs components that are absolutely required to make it run. This lets you control exactly what is installed on your servers. For example, when you enable the Hyper-V role, you can know exactly what has changed on your host system.
- **BitLocker drive encryption** You can now fully encrypt system and data drives on servers so that malicious users cannot access their contents even if they disappear with the server. This is an absolute must on any host server that is not properly protected through an access-controlled datacenter.
- **Device control** Through device control, you can ensure that malicious users cannot connect rogue Universal Serial Bus (USB) devices to your servers, or even to your workstations, to steal the contents of your shared folders or collaboration environments. In resource pools, this policy ensures that no one can take unauthorized copies of your VHDs.

This list includes a few items that can help secure your resource pool environment. Some are simpler to implement than others and in some cases, only larger installations will implement the full suite of features.

Securing Hyper-V Hosts

When you prepare to secure the resource pool, you need to look at different security aspects. This pool must include very strict protection strategies because it is so easy to walk away with an entire virtual machine. After all, a VM is nothing but a set of files in a folder. As such, the security plan for resource pools requires that particular attention be paid to the levels identified in Table 8-1.

TABLE 8-1 Applying the Security Plan to Resource Pools

CONTENT	COMMENTS
Data protection	Pay special attention to the storage containers that include the files that make up virtual machines.
Application Hardening	Secure the installations of Windows Server Hyper-V. Rely on the *Hyper-V Security Guide* and the contents of this chapter to do so.
Physical environment	Make sure datacenters have sufficient power and cooling resources to run host servers.
Physical access controls	Pay special attention to physical access to servers. All servers, especially remote servers, should be under lock and key.

CONTENT	COMMENTS
Communications	Make sure all resource pool administrators and technicians understand their responsibilities in terms of security practices. These are highly trusted roles.
Surveillance	If possible, have sign-in and sign-out sheets for administrators physically accessing the datacenter.
Security configuration	Pay special attention to the following: ■ Server Core configuration ■ Service hardening ■ Security Configuration Wizard settings for host servers ■ Limited role installations on each host; do not run any other role on the host parent partition ■ Configuration of virtual machine management systems ■ BitLocker Drive Encryption for host servers in remote offices ■ Device control to ensure that unauthorized USB disk drives cannot be connected to any physical server.
Anti-malware and antivirus	Implement Windows Defender along with proper antivirus technologies on the parent partitions of host servers. Configure antivirus software to bypass Hyper-V processes and directories for improved performance. This means you need to exclude the VMMS.exe and VMWP.exe processes (in %SystemRoot%\System32) as well as the directories that contain virtual machine configuration files and VHDs from active scanning. You have two ways to do this. You can exclude the actual directories, which contain the VHDs and the configuration and other files that make up the VMs; this is the recommended approach. Or you can exclude the VM file types such as .vhd, .avhd, .vfd, .vsv, .xml, and .bin. This latter approach entails more risk because it can include files that are not necessarily part of a VM. Also run antivirus engines from within the VMs to scan their own contents.
General AD DS security	Implement very tight permissions management on the utility forest. Implement software restriction policies to ensure that no malicious code is allowed to run in this domain.
File system	Secure the file system with NTFS permissions to protect VSOs. Rely on digitally signed Windows Installer packages for all third-party or custom product installations.

CONTENT	COMMENTS
Print system	Limit the print systems in this network. If printing is required, administrators can copy the contents to the production network.
.NET Framework security	Applicable to the full installations used in the System Center Virtual Machine Manager systems you create to administer the resource pool—they rely on Windows PowerShell to run cmdlets.
Internet Information Services (IIS)	Avoid the installation of IIS as much as possible. Deploy Microsoft Virtual Server through SCVMM to install it without IIS if you need to add life to 32-bit hardware. If you use a Self-Service SCVMM Portal, run the portal in controlled virtual machines.
System redundancy	Ensure business continuity and redundancy of your host servers. This was covered in Chapter 3, "Completing Resource Pool Configurations."
User identification	Rely on smart card or two-factor authentication for administrators in very secure environments.
Resource access	Only administrative accounts are required in this network.
Role-based access control	Assign least-privilege access rights to both administrators and technicians in this network.
Access auditing/ monitoring	Turn on auditing, as well as AD DS auditing, to track all changes. Consider running System Center Operations Manager in larger environments.
Perimeter networks	There should be no perimeter network in the resource pool, but you should still properly configure the Windows Server Firewall with Advanced Security to control access to host servers.
Virtual Private Networks (VPNs)	Rely on VPN connections for all remote administration.
Routing and Remote Access (RRAS)	Implement a remote access authentication service for administrators working remotely.
Secure Sockets Tunneling Protocol (SSTP)	Ensure that all remote communications, as well as internal intra-server communications, are encrypted.
Public key infrastructures (PKIs)	Implement Active Directory Certificate Services in support of smart card deployment and software restrictions.
Network Access Protection (NAP)	In larger environments, implement NAP to ensure that all machines that link to the resource pool have approved health status.

IMPORTANT ACTIVE DIRECTORY DOMAIN CONTROLLERS FOR THE UTILITY FOREST

You can run the domain controllers for the utility forest in VMs that are hosted on the resource pool. However, you must make sure these VMs are set to start automatically at all times to avoid being locked out from the host servers. Note, however, that if you log on to each host server with domain credentials at least once while the DCs are running, the credentials will automatically be cached into Windows Server 2008's secure Credential Manager store and will be available even if the DCs are turned off.

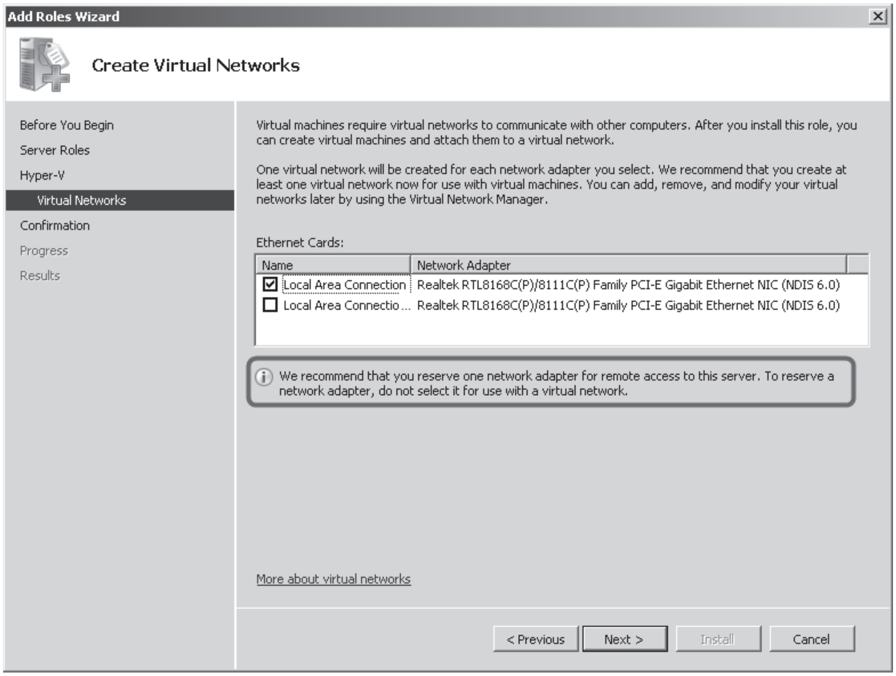
NOTE SECURITY FOR HYPER-V RESOURCE POOLS

Covering the entire range of different security technologies for resource pools is beyond the scope of this book. Many of these technologies require extensive coverage to be addressed properly. Some of the technologies that provide direct support for Hyper-V resource pool security are covered in more depth in this chapter. For the others, refer to the "References" section at the end of this book.

Resource pools are a new concept in IT and therefore need particular attention to detail when it comes to the implementation of their security settings. Make sure you fully understand the scope of protection you need to apply to this infrastructure.

In Hyper-V, your security plan must focus on several key aspects of the host server:

- Begin by properly configuring the server installation. As mentioned in Chapter 2, you should run Server Core installations. Only enable the settings that are absolutely required to remotely administer this installation as per the instructions in Chapter 2.
- Have multiple network interface adapters for each host server. You run multiple adapters to be able to dedicate an adapter to administration traffic. In fact, this is a basic recommendation of the Hyper-V Installation Wizard (see Figure 8-4). When an adapter is not assigned to virtual networks, it will only communicate with the physical host server. Make this a best practice for each host server configuration.
- Focus on the Hyper-V architecture during the application of your security measures. As documented in Chapter 1, "Implementing Microsoft Hyper-V" the Hyper-V architecture is based on partitions. The parent partition runs the core operating system for the host and manages all virtual machine communications with physical resources. Child partitions run guest operating systems as virtual machines. Ideally, they will be running enlightened guests and use proper communication channels through the VMBus. If not, the VMs will require device emulation, which is one more channel to manage.
- Make sure that applications only run in child partitions or VMs. You should not install any additional applications—except for utilities such as antivirus engine, SCVMM agent, and so on—in the parent partition to minimize the operational overhead of this partition as well as minimize the requirement for updates.



Virtual machines require virtual networks to communicate with other computers. After you install this role, you can create virtual machines and attach them to a virtual network.

One virtual network will be created for each network adapter you select. We recommend that you create at least one virtual network now for use with virtual machines. You can add, remove, and modify your virtual networks later by using the Virtual Network Manager.

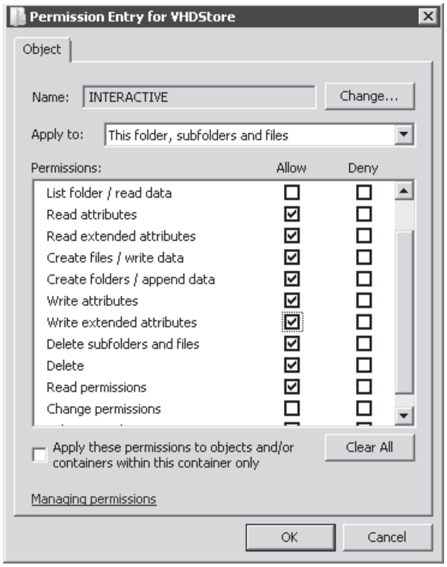
Ethernet Cards:

Name	Network Adapter
☑ Local Area Connection	Realtek RTL8168C(P)/8111C(P) Family PCI-E Gigabit Ethernet NIC (NDIS 6.0)
☐ Local Area Connectio...	Realtek RTL8168C(P)/8111C(P) Family PCI-E Gigabit Ethernet NIC (NDIS 6.0)

We recommend that you reserve one network adapter for remote access to this server. To reserve a network adapter, do not select it for use with a virtual network.

FIGURE 8-4 The Hyper-V Installation Wizard recommends reserving one adapter for management purposes.

- Secure the storage containers that will include the files that make up your VMs. Ideally, you will have redirected the default locations for both VHDs and virtual machine configuration files in Hyper-V as outlined in Chapter 4, "Creating Virtual Machines." In addition, you should store the files that make up VMs on separate spindles from the operating system for the parent partition. If possible, this storage should be separate from the host server itself. If you are running clustered host servers (as you should in most cases), you will be using separate shared storage to store VM files. VM files should also be kept together as much as possible to make them easier to manage and protect. If the VM configuration file is in one location, the VHD files are in another, and potential snapshots are in yet another, properly securing VM files becomes difficult if not impossible. When you move the default locations, you must ensure that NTFS access rights are configured properly. Most are configured by default—including Administrators, System, and Creator Owner permissions—but some must be configured manually. The settings that must be configured manually are for three special accounts found in the local system: Interactive, Batch, and Service accounts. Use the Advanced Settings in the Security dialog box of a folder's properties to assign the required settings for each of these three special accounts (see Figure 8-5).



Name: INTERACTIVE

Apply to: This folder, subfolders and files

Permissions:	Allow	Deny
List folder / read data	□	□
Read attributes	☑	□
Read extended attributes	☑	□
Create files / write data	☑	□
Create folders / append data	☑	□
Write attributes	☑	□
Write extended attributes	☑	□
Delete subfolders and files	☑	□
Delete	☑	□
Read permissions	☑	□
Change permissions	□	□

□ Apply these permissions to objects and/or containers within this container only

FIGURE 8-5 Assigning proper permissions to the three special accounts: Interactive, Batch, and Service

- Centralize all file resources—such as ISO files, update files, and virtual floppy drives—so that all host servers can access them from a single location. In larger sites, this location will be a clustered file server to make sure it is highly available.
- Consider encrypting all virtual machine files and resources to protect them from theft. Use BitLocker Full Drive Encryption to do so because you cannot use the Encrypting File System to store virtual machine files. Keep in mind that encryption adds some overhead to the operation of the VMs.

EXAM TIP **BITLOCKER AND VMs**

Remember that BitLocker is not supported in a VM because it cannot access either a USB port—not supported in this version of Hyper-V—or the Trusted Platform Module (TPM) chip that might be contained on the server's hardware. Therefore, you cannot run BitLocker in a child partition.

- Make sure that the administrators and technicians that have access to the parent partition are granted only appropriate rights. Anyone who can access the parent partition can make global modifications to the Hyper-V configuration and possibly break all of the child partitions that run on this host. This is why it is so important to assign role-based access rights. RBAC assignments are covered further in this lesson.
- Consider the security or sensitivity level of the VMs you run on a particular host. Do not run unsecured VMs on a highly secure host. Instead, try to match security levels between hosts and the VMs they run.

Child partitions are automatically segregated from the parent partition through Hyper-V's internal architecture. However, it is easy to blur this segregation when administrators are responsible for both the resource pool and the virtual workloads it runs. Ideally, you will be able to assign separate roles to your IT administration team and ensure that the operators that perform one duty are not responsible for the other. If you cannot have different administrators for each role, you should at least make sure your administrators use separate accounts for each operation as mentioned earlier in the introduction to this chapter.

These recommendations are summarized in Table 8-2, including important caveats.

TABLE 8-2 Parent Partition Summary Security Recommendations

RECOMMENDATION	BENEFIT	CAVEAT
Default Installation: Install Hyper-V on Windows Server 2008 Server Core.	The attack surface for the host server partition is minimized. The host attack surface is reduced. System uptime improves because there are fewer components to update.	Management is either from a remote console, the command line, or through WMI actions. Server Core does not include the .NET Framework and therefore, no Windows PowerShell. Initial installation and configuration must follow strict instructions (see Chapter 2).
Network Configuration: Install at least two NICs: one for host management and other one(s) for child partitions.	Using a separate adapter for host communications ensures that there is no possibility of compromising management traffic. If you share host management communications with child partition communications, someone on the child network can possibly "listen in" on host communications.	Ideally, you reserve two adapters for host management to avoid a single point of failure. When an adapter is not selected during the creation of virtual networks, it is automatically reserved for host management communications. This must be a conscious decision on the administrator's part.
Hyper-V Architecture: Segregate parent and child partitions.	The Hyper-V architecture provides natural segregation of parent and child partitions.	Run enlightened guest operating systems as much as possible to use proper communication channels through the VMBus and not device emulation.

RECOMMENDATION	BENEFIT	CAVEAT
Host Applications: Do not run applications in parent partitions.	The parent partition is designed to run the hypervisor only. Do not install any other application (core utilities are OK, of course) in the parent partition.	Install applications only in VMs. Installing an application or server role other than Hyper-V into the parent partition can impact performance and force you to update host systems more often.
Dedicated VM Storage: Configure separate logical partitions to store VM files.	Creating custom folders for VM file storage lets you bring all of a VM's files together into a single folder and makes them easier to manage.	If you specify a different location, ensure that you set the appropriate permissions on the new folder.
Resource Storage: Configure separate storage for VM resource files.	Regroup all VM resource files—VFDs, ISO files, executables, and updates—in a shared folder that is accessible by all host servers.	Ideally, this shared folder would be highly available and would run on a failover cluster.
Storage Encryption: Use BitLocker to protect VM files and other file-based resources.	In highly secure or unprotected environments, modify the default location of file-based resources on host servers and run BitLocker Full Drive Encryption on these storage containers to protect from data theft.	Run BitLocker on both the system and the data partitions. You must include the system partition to protect the data partition encryption keys because they are stored on the system partition by default. Also note that you cannot encrypt storage area network volumes because they do not run the Windows Server operating system.
Host Management: Maintain a clear separation between the resource pool administrators and VM administrators.	Segregating security contexts between the resource pool and the virtual workloads helps protect resource access.	By default, child partition administrators are not granted administrative access to the management partition. Maintain this as much as possible. Also, place your host servers into a utility forest. This will require at least two additional domain controllers, but they can be virtual machines.

RECOMMENDATION	BENEFIT	CAVEAT
VM Sensitivity Level: Run sensitive VMs on highly secure hosts.	Match the sensitivity level of a VM with the security level of the host to provide adequate protection for the VMs.	Do not run highly sensitive VMs such as domain controllers on unsecured host servers. Ideally, match host and VM security levels. For example, you can create multiple levels of security for host servers: ■ Low for test and development environments. ■ Medium for VMs running open services such as public Web sites or public file shares. ■ High for sensitive workloads such as DCs.

Use these best practices when working with Hyper-V hosts. This will secure the host but will not secure the remainder of the resource pool components. These must also be secured to ensure that the entire host environment is secure.

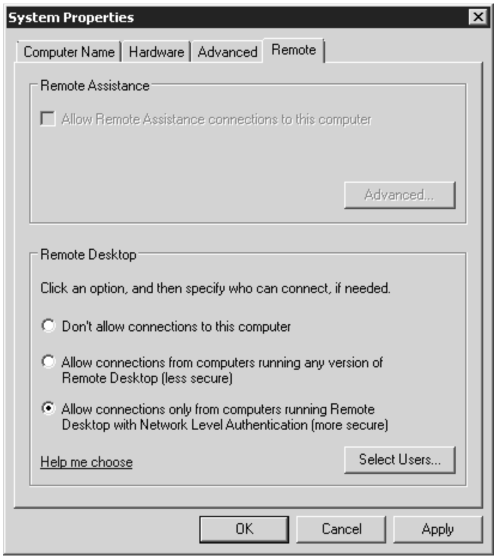
> ***MORE INFO*** **SECURING HYPER-V**
>
> **For more information on securing Hyper-V, go to *http://technet.microsoft.com/en-us/library/dd283088.aspx*.**

Securing the Resource Pool

The resource pool usually contains several components in addition to the host servers you run. These components can include both required and optional elements. Required elements must be part of the resource pool for it to function properly, whereas optional elements may not be necessary for small datacenters, but will be for medium to large datacenters. These components include:

- **Host Servers** Ideally, your host servers will be homogeneous and will rely on a single, secured configuration image.
- **Domain Controllers** Whether you use a utility forest or you run a mixed forest—where both host servers and production virtual machines operate—you need domain controllers, because Hyper-V hosts should belong to a domain to simplify access and centralize security settings. Even if you run a separate utility forest, these DCs can be virtual machines and can run on the same hosts as your production VMs. Make sure, however, that even if the DCs run on the same hosts, they are not connected to the same virtual networks as the production VMs you run.

- **Central File Share** This file share should store virtual machine resources such as ISO files, VFDs, executables, and updates. Again, this can be a VM, but it should use a segregated virtual network. Ideally, this file share will be highly available and will be running Failover Cluster services.
- **Administrator Workstations** Ideally, the workstations your administrators and technicians rely on will be running Windows Vista and will be using User Account Control (UAC) to ensure that they are aware of each time they perform an activity that requires elevated rights. These workstations can be virtual machines and can be accessed through Remote Desktop Connections. Using Windows Vista as the operating system for the workstation allows you to use network-level authentication for the connections, providing a higher level of security for the communication (see Figure 8-6). Again, if the workstations are VMs, they should not be connected to the same virtual networks as your production VMs.



Remote Assistance

□ Allow Remote Assistance connections to this computer

Remote Desktop

Click an option, and then specify who can connect, if needed.

○ Don't allow connections to this computer

○ Allow connections from computers running any version of Remote Desktop (less secure)

● Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

FIGURE 8-6 Using secure communications for the Remote Desktop

- **System Center Virtual Machine Management Server (Optional)** Larger environments will want to run SCVMM to simplify host and VM management. Again, this machine can be a VM that is on an isolated virtual network.
- **System Center Database Server (Optional)** Very large environments with more than 100 hosts should run Microsoft SQL Server on a separate system for the SCVMM database. Ideally, this machine will be clustered through Failover Cluster services to make it highly available. This database can run on VMs and could possibly be running on the same servers as the central file share. In addition, this server could provide the required database services for any number of additional System Center tools if you choose to run them.

- **SCVMM Library Server (Optional)** If you are running SCVMM, your central file share will be contained within an SCVMM Library. This can run on a separate VM and could share the role with the database servers.
- **System Center Essentials (Optional)** Small to medium environments—those with fewer than 500 PCs and 30 servers—may want to deploy System Center Essentials, a tool that regroups the functionality of other independent System Center products such as Operations Manager, Configuration Manager, and more. If you deploy System Center Essentials, it can share the database server with SCVMM. This machine should also be on a segregated virtual network. In terms of security, System Center Essentials supports controlled configuration management, updates to both hosts and VMs, and system monitoring.
- **System Center Operations Manager (Optional)** Organizations wanting to take advantage of Performance and Resource Optimization (PRO) in SCVMM will want to deploy OpsMgr along with SCVMM. This can also be within virtual machines and can also take advantage of the database server. This machine should be on a segregated virtual network.

MORE INFO **OpsMgr AND SECURITY**

Operations Manager can also be used to control security because it includes the ability to centrally collect and filter audit records from source computers. If you run a number of Hyper-V hosts and you want to audit all access as well as privileged activity on these servers, you can use Windows Server 2008 to audit these events and then rely on OpsMgr to collate them centrally and alert you in the event of violations.

- **System Center Data Protection Manager (Optional)** Environments wanting to centralize all backup and recovery operations for both hosts and VMs may want to deploy DPM. DPM provides the ability to centrally control all backups, collate all Volume Shadow Copy Services (VSS) snapshots into a central location, and restore to any point in the enterprise. More on DPM is covered in Chapter 9, "Protecting Hyper-V Resource Pools." However, note for now that DPM can also run in a VM that is on a segregated virtual network and can also rely on the shared database server.
- **System Center Configuration Manager (Optional)** Larger environments wanting to centralize system configuration and application deployment can deploy SCCM within the resource pool. In terms of security, SCCM can offer configuration controls through its Desired Configuration Management feature and can control updates to both hosts and VMs. It should run within a VM on the segregated virtual network and share the database server.
- **Windows Server Update Services (Optional)** Environments that do not run either SCCM or System Center Essentials will want to deploy WSUS in support of a special update service within the resource pool and ensure that it is not linked to the production network in any way. This can also be a VM on a segregated virtual network and can also rely on the shared database.

- **Network Access Protection Server (Optional)** Larger environments will want to run a separate NAP environment to ensure that all machines comply with security standards before they can connect to the network. The NAP server can be in a VM on the segregated virtual network.

IMPORTANT **NAP AND HOST SERVERS**

Be very careful if you run NAP in a host environment. Do not apply NAP rules to host servers because you may find that your host can no longer connect to any network, which would cause all of the VMs it runs to fail. Apply NAP rules only to workstations and other non-critical components. You do not want to find yourself in a situation in which your console cannot connect to a host in an emergency because you are not running the appropriate updates.

- **Certificate Servers (Optional)** Run Active Directory Certificate Services if you want to secure all communications with server-side certificates. AD CS lets you generate your own certificates and assign them to each server in your resource pool infrastructure—hosts, SCVMM, and more. Using certificates ensures that all hosts are properly identified when you connect to them and can support remote connection encryption through the Secure Sockets Layer. Certificate servers can also be useful to support virtual private network connections using the new Secure Sockets Tunneling Protocol (SSTP) built into Windows Server 2008. The certificate server is an ideal candidate for virtualization because the root server should be taken offline to protect it. Again, connect these servers to the segregated virtual network.

MORE INFO **USING SELF-SIGNED CERTIFICATES**

In smaller organizations, you can also use self-signed certificates instead of the certificates you would obtain through AD CS. This avoids having to run an AD CS infrastructure. To use self-signed certificates, download the SelfSSL.exe, which is a utility in the IIS 6 Resource Kit that can be found at *http://www.microsoft.com/downloads/details.aspx?familyid=56FC92EE-A71A-4C73-B628-ADE629C89499&displaylang=en*. You can then use it to generate a certificate for each server and install this certificate within the Trusted Root Authorities container of each machine that will interact with the servers.

- **Routing and Remote Access Server (Optional)** You might require RRAS servers to support remote connections from outside your network. Rely on SSTP to support virtual private network connections and ensure all remote connections are completely secure. These can also be VMs and should be on the segregated virtual network.

As you can see, a complete resource pool can include several components (see Figure 8-7). It can become even more complicated if your host systems run different hypervisors. If so, you will need to rely on the vendor's recommended security practices to tighten security on these hosts.

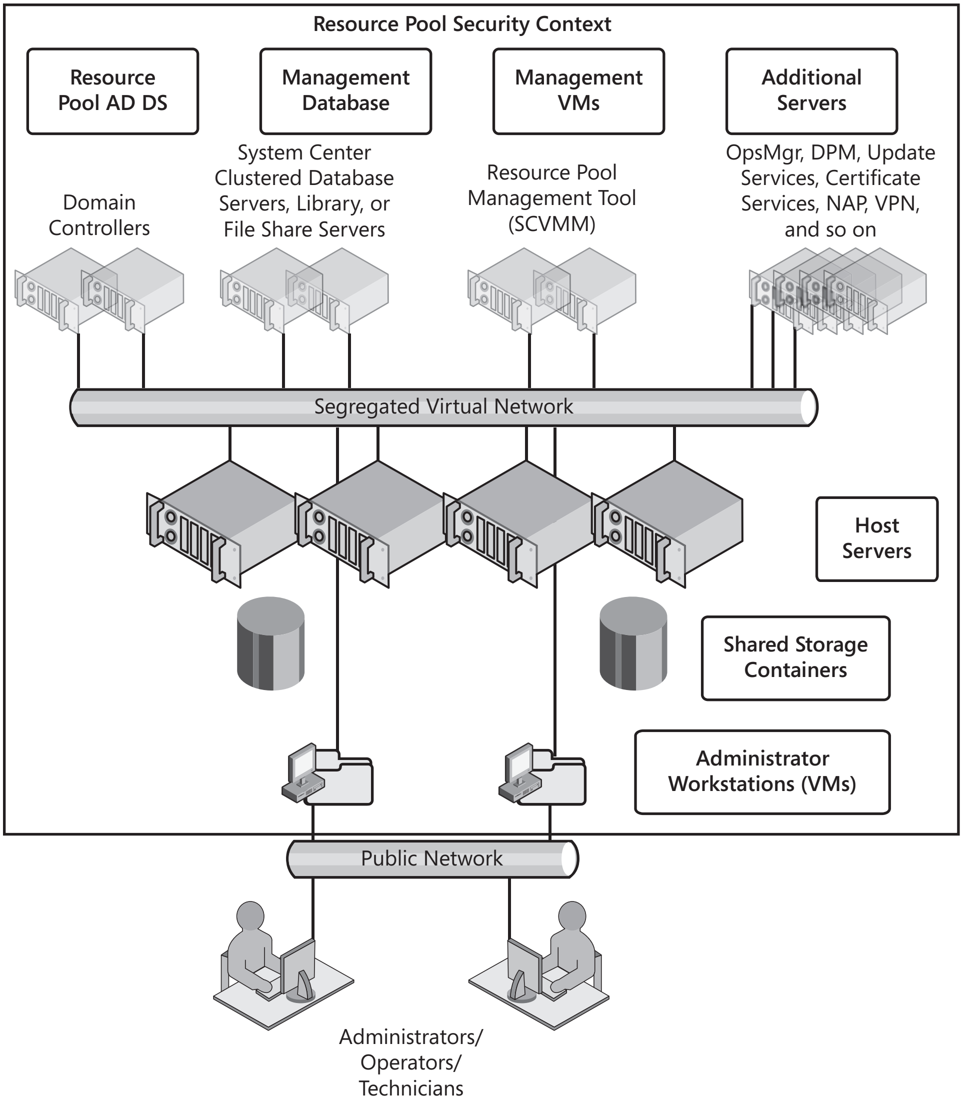

Resource Pool Security Context
Resource Pool AD DS
Management Database
Management VMs
Additional Servers
Domain Controllers
System Center Clustered Database Servers, Library, or File Share Servers
Resource Pool Management Tool (SCVMM)
OpsMgr, DPM, Update Services, Certificate Services, NAP, VPN, and so on
Segregated Virtual Network
Host Servers
Shared Storage Containers
Administrator Workstations (VMs)
Public Network
Administrators/ Operators/ Technicians

FIGURE 8-7 A resource pool including required and optional components

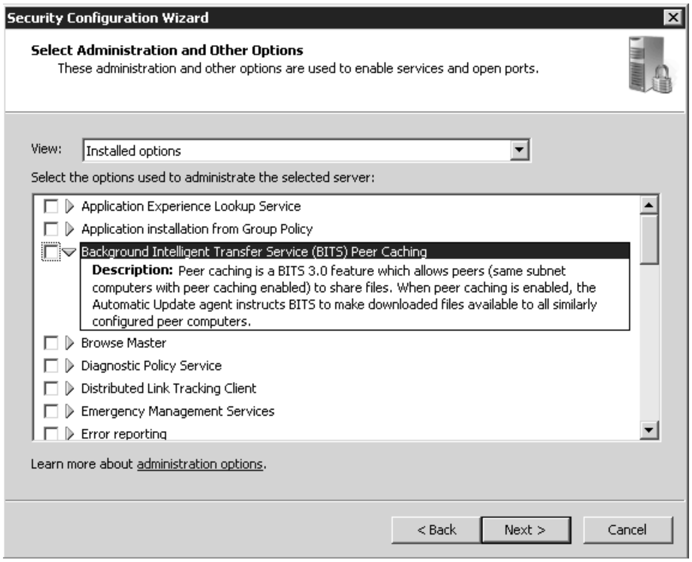
Using the Security Configuration Wizard

One of the best tools contained within Windows Server 2008's full installation for the application of security parameters and the lockdown of servers is the Security Configuration Wizard (SCW). This tool is designed to generate security profiles based on the role of a server within your network. SCW lets you configure four key components of a system:

- Tighter service configurations through pre-defined role-based configurations.
- Tighter network security.
- Tighter registry settings.
- Implement an audit policy.

These are the default controls you'll find in SCW. They are quite sophisticated.

Perhaps the best part of SCW is that it provides complete explanations for each of the settings it will modify. You now have a single place to determine what a particular security setting will modify and why. Just click the arrow located before the item name to see explanations for the item (see Figure 8-8).



Security Configuration Wizard

Select Administration and Other Options

These administration and other options are used to enable services and open ports.

View: Installed options

Select the options used to administrate the selected server:

- □ Application Experience Lookup Service
- □ Application installation from Group Policy
- □ Background Intelligent Transfer Service (BITS) Peer Caching

  Description: Peer caching is a BITS 3.0 feature which allows peers (same subnet computers with peer caching enabled) to share files. When peer caching is enabled, the Automatic Update agent instructs BITS to make downloaded files available to all similarly configured peer computers.
- □ Browse Master
- □ Diagnostic Policy Service
- □ Distributed Link Tracking Client
- □ Emergency Management Services
- □ Error reporting

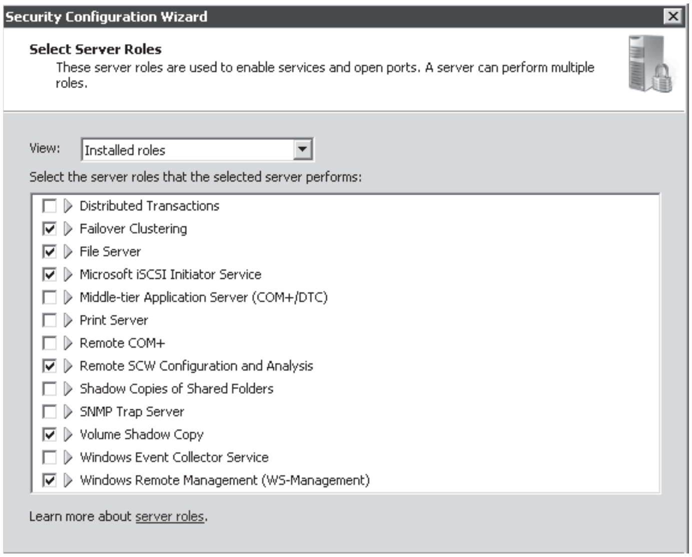
Learn more about administration options.

FIGURE 8-8 Obtaining additional information from the Security Configuration Wizard

You can use SCW to create new policies, edit existing policies, apply policies, and—perhaps its best feature—roll back the assignment of a security policy. Security policies are generated from a base server configuration. Unfortunately, SCW does not include specific information on the Hyper-V role, which is odd because it covers every other role contained within Windows Server 2008 (see Figure 8-9). It does, however, understand the Hyper-V services and can support the generation of a security configuration that supports Hyper-V (see Figure 8-10).

You launch the Security Configuration Wizard through the Administrative Tools on any Windows Server 2008 running the full installation. You can use a full installation of Windows Server 2008 with Hyper-V to generate the SCW configuration file and then apply it remotely to host servers running the Server Core installation.

SCW includes a corresponding command-line tool, SCWCMD.exe, which lets you mass-produce the application of security policies generated through the SCW graphical interface. However, this tool only works on the local machine and cannot apply security policies to remote machines. However, SCW produces output in XML format, which—although incompatible by default with Group Policy Objects (GPOs)—can be converted into a GPO. You can then use a GPO to assign the security settings to your Server Core machines.



Security Configuration Wizard

Select Server Roles

These server roles are used to enable services and open ports. A server can perform multiple roles.

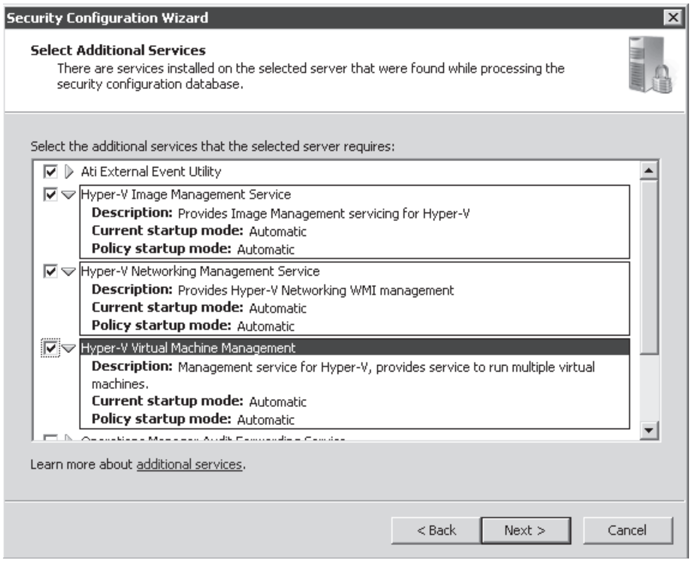
View: Installed roles

Select the server roles that the selected server performs:

- □ Distributed Transactions
- ☑ Failover Clustering
- ☑ File Server
- ☑ Microsoft iSCSI Initiator Service
- □ Middle-tier Application Server (COM+/DTC)
- □ Print Server
- □ Remote COM+
- ☑ Remote SCW Configuration and Analysis
- □ Shadow Copies of Shared Folders
- □ SNMP Trap Server
- ☑ Volume Shadow Copy
- □ Windows Event Collector Service
- ☑ Windows Remote Management (WS-Management)

Learn more about server roles.

FIGURE 8-9 The Security Configuration Wizard does not include specific information on the Hyper-V role even if it is installed.



Security Configuration Wizard

Select Additional Services

There are services installed on the selected server that were found while processing the security configuration database.

Select the additional services that the selected server requires:

- ☑ Ati External Event Utility
- ☑ Hyper-V Image Management Service
  Description: Provides Image Management servicing for Hyper-V
  Current startup mode: Automatic
  Policy startup mode: Automatic
- ☑ Hyper-V Networking Management Service
  Description: Provides Hyper-V Networking WMI management
  Current startup mode: Automatic
  Policy startup mode: Automatic
- ☑ Hyper-V Virtual Machine Management
  Description: Management service for Hyper-V, provides service to run multiple virtual machines.
  Current startup mode: Automatic
  Policy startup mode: Automatic

Learn more about additional services.

FIGURE 8-10 The Security Configuration Wizard understands Hyper-V services.

IMPORTANT **GPO SETTINGS FOR HYPER-V**

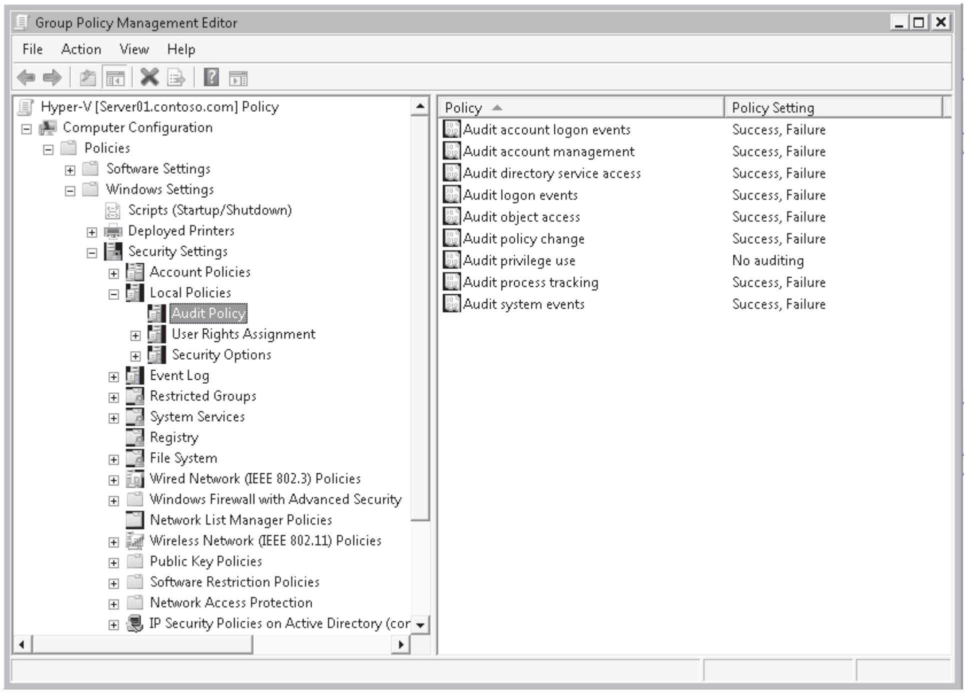
There are no specific Group Policy settings for Hyper-V in Active Directory Domain Services, but if you capture a security policy generated with SCW and convert it into a GPO, you can then use this GPO to remotely configure any Hyper-V host running either the full installation or Server Core.

To convert SCW output into a readable format for inclusion in a GPO, you must use the following command line:

```
scwcmd transform /p:PolicyFile.xml /g:GPOName
```

This transforms the XML file into a new GPO and stores it in AD DS. The GPO must then be applied using domain administrator privileges. Policies are saved by default under the %SystemRoot%\Security\MSSCW\Policies folder. The resulting GPO will include the contents of the SCW XML file and assign them to various sections of the GPO. These settings will include content for security settings, IP Security policies, and Windows Firewall (see Figure 8-11). This new GPO is stored in the Group Policy Objects container in AD DS and must be linked to appropriate organizational units (OUs) to be applied. Ideally, you create an OU for the host servers, move all of the host server accounts to this OU, and assign the GPO to this OU. It will then be processed by each of your host servers. Use the Group Policy Management Console to perform these tasks.

SCW policies are much more powerful than any other single component for the application of security settings to Windows servers.


Group Policy Management Editor
File
Action
View
Help
Hyper-V [Server01.contoso.com] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Network Access Protection
IP Security Policies on Active Directory (cor

Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	No auditing
Audit process tracking	Success, Failure
Audit system events	Success, Failure

FIGURE 8-11 The Audit section of a security policy generated through SCW and then converted to a GPO

MORE INFO **THE SECURITY CONFIGURATION WIZARD**

More information on the Security Configuration Wizard can be found at *http://technet2.microsoft.com/windowsserver/en/library/38f0693d-59eb-45ca-980d-31fe03eb54df1033.mspx?mfr=true*. For more information on converting a SCW policy into a GPO, go to *http://technet.microsoft.com/en-us/library/cc779290.aspx*.

IMPORTANT **APPLYING GPOs TO HOST SERVERS**

Make sure you test the GPO in a laboratory before you apply it to production host servers. You don't want it to lock down inappropriate ports and have all your VMs fail.

Protecting Hosts from Removable Devices

Windows Vista introduced a new capability for the Windows operating system—the ability to configure removable device controls through the use of Group Policy. This is done through the control of device installations, letting you manage which devices can be installed on any given system. For example, you can use this policy to prevent a malicious user from plugging in a removable disk drive and walking away with your intellectual property. When you remember that a VM is nothing but a set of files in a folder, you soon realize that protection of these files is an important part of any host or resource pool security policy.

The application of this policy is simple. Basically, you create a list of approved devices on your network and include it in your GPO. For example, you might let users install USB mice and keyboards, but prevent them from installing either Flash memory devices or external disk drives. Apple iPods and iPhones, Windows Mobile Devices, and digital music players, for example, are also disk drives that can be used to transport very large amounts of information—most of these devices can store multiple GB of information. Because you can't prohibit the use of these types of devices on your network, you must control their use through a properly designed GPO.

Ideally, you will assign this policy to both host servers and administrative workstations. This means that you should implement removable device controls in the resource pool so that no one can connect a USB drive to a server and use it to remove copies of your virtual machines. In addition, you should apply it to PCs linked to the virtual service offerings you run in production to ensure that no one can use a PC from your production domain to connect a device and somehow traverse the VSO domain to the resource pool utility domain and steal virtual machines. The best protection is complete protection.

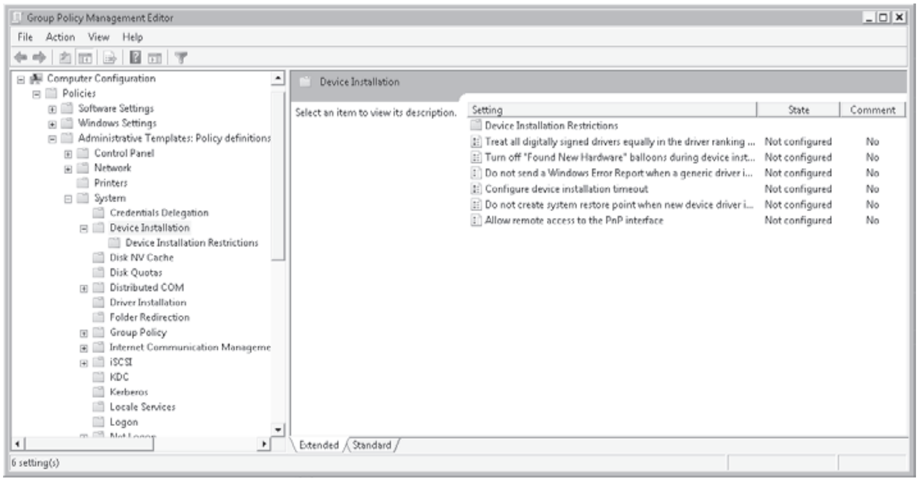
In the resource pool, you will probably add these settings to a new GPO because they are required for both host servers and administrative workstations. And although you can use these controls to prevent installation of all devices, it is best to allow the installation of authorized devices. To do this, you need to be able to identify devices. You have two ways to do this:

- You can use *device identification strings*—which are contained both within the device and within the .inf file that comes with the driver—to block or authorize devices. The two different types of device ID strings are hardware IDs and compatible IDs. Hardware IDs provide the most direct match between a device and its driver. Compatible IDs provide a list of compatible drivers that can give you at least basic functionality for the device. If you use these IDs to allow or deny devices, you must include all of the possible IDs for the device. If not, multifunction devices especially might be blocked at one level but not at another.

- You can use *device setup classes* to control devices. Classes divide devices into groups that use the same installation process. Classes are identified by globally unique identifiers (GUIDs), which are complex numbers that uniquely represent a class of devices. For example, if you want to block USB disk drives, block the GUID for these devices and no USB disk drive can be installed on your systems.

Device authorizations are set up through Group Policy. Use a computer that has the Group Policy Management Console installed and follow these steps:

1. Launch the GPMC. To do so, click Start, click Administrative Tools, and then click Policy Management Console.
2. Because this policy affects every physical computer in the resource pool, apply it to the OU that contains both host servers and physical workstations. This can be applied through any GPO that would affect all physical systems. If the GPO exists, right-click and select Edit. If it doesn't, create it, name it, link it to the appropriate OU, and then edit it.
3. Go to the Device Installation settings by navigating through Computer Configuration, then Policies, then Administrative Templates, then System, and then click Device Installation (see Figure 8-12). Also set up the policies for Removable Storage at Computer Configuration, then Policies, then Administrative Templates, then System.



Select an item to view its description.

Setting	State	Comment
Device Installation Restrictions		
Treat all digitally signed drivers equally in the driver ranking ...	Not configured	No
Turn off "Found New Hardware" balloons during device inst...	Not configured	No
Do not send a Windows Error Report when a generic driver i...	Not configured	No
Configure device installation timeout	Not configured	No
Do not create system restore point when new device driver i...	Not configured	No
Allow remote access to the PnP interface	Not configured	No

FIGURE 8-12 Setting device restrictions in a GPO

4. Set up the policies according to the recommendations in Table 8-3. Examine the explanation for each setting to learn more about its intent and configuration possibilities. Each setting that is not configured relies on the default behavior for that setting. Close the GPO when done.
5. Test the settings with various devices of each type you authorized and de-authorized.

Your host environment is protected as soon as you apply the GPO and the GPO is updated on each host and workstation.

TABLE 8-3 Secure Virtual Service Offerings

LOCATION	SETTING	RECOMMENDATION
Device Installation	Treat All Digitally Signed Drivers Equally In The Driver Ranking And Selection Process	Not Configured
	Turn Off Found New Hardware Balloons During Device Installation	Not Configured
	Do Not Send A Windows Error Report When A Generic Driver Is Installed On A Device	Not Configured
	Configure Device Installation Timeout	Not Configured
	Do Not Create System Restore Point When New Device Driver Installed	Not Configured
	Allow Remote Access To The PnP Interface	Not Configured
Device Installation Restrictions	Allow Administrators To Override Device Installation Restriction Policies	Configure only if you fully trust your administrators or anyone with administrative access rights.
	Allow Installation Of Devices Using Drivers That Match These Device Setup Classes	Enable and add the appropriate GUID entries.
	Prevent Installation Of Devices Using Drivers That Match These Device Setup Classes	Enable and add the appropriate GUID entries.
	Display A Custom Message When Installation Is Prevented By Policy (Balloon Text)	Enable and type in an appropriate violation of policy message.
	Display A Custom Message When Installation Is Prevented By Policy (Balloon Title)	Enable and type in an appropriate message title.
	Allow Installation Of Devices That Match Any Of These Device IDs	Not Configured.
	Prevent Installation Of Devices That Match Any Of These Device IDs	Not Configured.
	Prevent Installation Of Removable Devices	Not Configured.
	Prevent Installation Of Devices Not Described By Other Policy Settings	Enable.

LOCATION	SETTING	RECOMMENDATION
Removable Storage Access	Time (In Seconds) To Force Reboot	Not Configured.
	CD And DVD: Deny Read Access	Not Configured.
	CD And DVD: Deny Write Access	Enable only in very secure environments. Users often rely on this for backups.
	Custom Classes: Deny Read Access	Enable only if you have appropriate GUIDs.
	Custom Classes: Deny Write Access	Enable only if you have appropriate GUIDs.
	Floppy Drives: Deny Read Access	Not Configured.
	Floppy Drives: Deny Write Access	Not Configured.
	Removable Disks: Deny Read Access	Not Configured.
	Removable Disks: Deny Write Access	Enable.
	All Removable Storage Classes: Deny All Access	Enable in very secure environments.
	All Removable Storage: Allow Direct Access In Remote Sessions	Enable in very secure environments.
	Tape Drives: Deny Read Access	Enable.
	Tape Drives: Deny Write Access	Enable.
	WPD Devices: Deny Read Access	Enable only if your users do not use smart phones or Pocket PCs.
	WPD Devices: Deny Write Access	Enable only if your users do not use smart phones or Pocket PCs.

MORE INFO **SETTING DEVICE CONTROL POLICIES**

For more information on how to implement removable device controls for both the resource pool and VSO networks, go to http:*//www.microsoft.com/technet/windowsvista/library/9fe5bf05-a4a9-44e2-a0c3-b4b4eaaa37f3.mspx*.

MORE INFO **DEVICE ID STRINGS AND SETUP CLASSES**

Rely on classes instead of IDs because they are more comprehensive. To obtain the classes for a specific device group, look up the listings available on the Microsoft Web site at *http://msdn2.microsoft.com/en-us/library/ms791134.aspx*. Use these classes to set up your device restrictions. Find out more about device identification strings at *http://go.microsoft.com/fwlink/?linkid=52665*.

MORE INFO **LOCKING USB STORAGE DEVICES**

Microsoft Knowledge Base Article 823732 documents an alternative and perhaps easier method for locking down USB storage: *http://support.microsoft.com/default.aspx/kb/823732*.

Securing VM Files with BitLocker

With the release of Windows Vista, Microsoft introduced BitLocker Full Drive Encryption. BitLocker lets you encrypt the contents of your operating system volume so that malicious attackers cannot access them. BitLocker is most often used for mobile systems or systems that contain sensitive data and leave your office premises.

You can also use BitLocker to protect server drives because it is also included in Windows Server 2008. You might apply BitLocker to the storage container of your virtual machines so that even if malicious attackers steal the hardware or hard drives that make them up, they can't access any data that may reside inside them. This, however, is an extreme measure that would only be applied in very secure environments, because partition encryption adds a certain amount of overhead to the operation of a server. A more likely scenario is the encryption of host server drives that are in remote offices. This way, if someone walks off with a physical server in a remote office, not only does she not have access to any of the virtual machines that may be located on the host, but the host server itself is also protected.

To be able to use BitLocker, your system must:

- Include a minimum of two NTFS partitions: a system volume and an operating system volume. The system volume is the boot partition and only requires about 1.5 GB of space.
- Include a USB flash drive and a BIOS that supports reading and writing to a USB flash drive at startup.
- Ideally, include a Trusted Platform Module (TPM) version 1.2 or later microchip.
- Ideally, include a Trusted Computing Group (TCG)–compliant BIOS.

BitLocker can either be run through the use of an external USB flash drive or through the TPM module. A flash drive can store the encryption key used to lock and unlock the operating system partition. However, using a USB drive is risky—it can be lost or stolen. This is why it is ideal to use a server that has the full TPM components. In this case, the encryption key is stored securely within the TPM chip and cannot be stolen.

If the host servers you use for remote offices include these capabilities and you intend to encrypt their contents, use the following procedure:

1. Begin by creating two partitions during installation. Both partitions must be primary partitions. In addition, the smaller partition should be set as active. Both partitions must be formatted with NTFS. You can use the installation media to create these partitions.
2. Install Server Core into the operating system partition.

> ***NOTE*** **THE BITLOCKER DRIVE PREPARATION TOOL**
>
> **If your drive partitions are already created and the operating system is installed, you can use the BitLocker Drive Preparation Tool to restructure the partitions as needed. Find the tool at *http://support.microsoft.com/kb/933246*.**

3. When Server Core is installed, perform the post-installation configurations found in Lesson 1 of Chapter 2.
4. Install the BitLocker feature:

   ```
   start /w ocsetup BitLocker
   ```

5. Restart the system as soon as BitLocker is installed. When the system restarts, you'll be ready to configure BitLocker. Begin by getting BitLocker to list compatible drives. Make sure you go to the appropriate folder to do this:

   ```
   cd\windows\system32
   cscript manage-bde.wsf -status
   ```

6. Encrypt the system drive:

   ```
   cscript manage-bde.wsf –on C: -RecoveryPassword NumericalKey –RecoveryKey
   BitLockerDrive –StartupKey BitLockerDrive
   ```

   BitLockerDrive is the drive letter you gave to the system partition. *NumericalKey* is a 48-digit number, divided into 8 groups of 6 digits, using hyphens to separate groups. Each group of 6 digits must be divisible by 11 but not greater than 720,896.

You can repeat the last command to encrypt any other drive on the host server. From this point on, all data on the drives is encrypted and must be decrypted with the proper key to be read.

Use BitLocker with caution on your host servers. Apply it only where it is deemed absolutely necessary.

> ***MORE INFO*** **USING BITLOCKER**
>
> **For more information on using BitLocker to encrypt drives, go to *http://technet.microsoft.com/en-us/library/cc732774.aspx*.**

Auditing Object Access in the Resource Pool

Highly secure environments will need to audit all object access within their resource pool to track who is performing which operation within the environment. Auditing lets you track resource usage and monitor log files to determine that users have appropriate access rights and that no user is trying to abuse his or her rights.

Auditing is a two-step process. First, you must enable the auditing policy for an event. This is done within a Group Policy Object. Then you must turn on the auditing for the object you want to track and identify who you want to track. Windows Server 2008 lets you audit several different types of events:

- Account logon events
- Account management
- Directory service access
- Logon events
- Object access
- Policy change
- Privilege use
- Process tracking
- System events

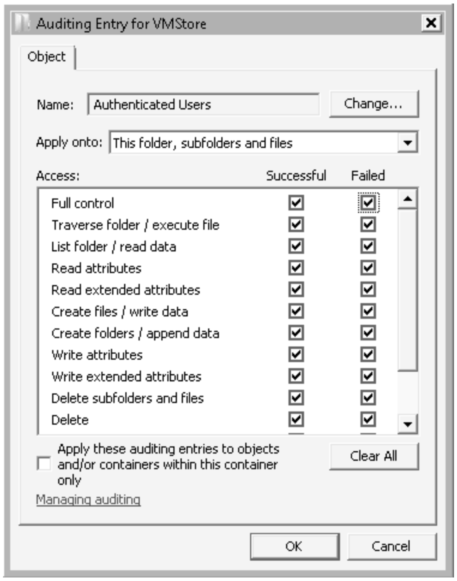
Use the following procedure to define the audit policy for the resource pool. Perform this procedure on a computer that has the Group Policy Management Console installed and use domain administrator credentials.

> ***NOTE*** **AUDITING AND THE SECURITY CONFIGURATION WIZARD**
>
> **Remember that auditing is one of the four key components that the Security Configuration Wizard can control. If you have already created a security policy with SCW and turned on auditing, you can use the following procedure to refine or modify the settings SCW applied.**

1. Launch the GPMC by clicking Start, clicking Administrative Tools, and then clicking the console shortcut. Expand the local forest when the tool is open.
2. Create a new GPO. Right-click the Group Policy Objects container and choose New. Name the Policy **Audit Policy** and click OK.
3. Right-click the new policy and choose Edit to launch the Group Policy Editor.
4. Expand Computer Configuration, then Policies, then Windows Settings, then Security Settings, and then Local Policies. Click Audit Policy.
5. Double-click each setting you want to change to modify it. For example, if you double-click Audit Logon Events, the Audit Logon Events Properties dialog box opens, letting you configure it to identify successes and failures as needed.
6. Repeat step 5 for any setting you want to turn on and then close the Group Policy Editor. Policies are automatically saved as soon as you make the change in the Editor.

The audit policy is turned on. Now you need to tell the system which objects you want to audit. For example, if you want to audit all changes to the folders where you store VM files, use the following procedure on a host server:

1. Launch Windows Explorer and move to the drive containing the VM files.
2. Right-click the folder containing the VMs—for example, VMStore—and choose Properties.
3. Click the Security tab and then click Advanced.
4. Click the Auditing tab. Click Edit and then click Add.
5. Type **Authenticated Users**, click Check Names, and then click OK.
6. In the Auditing Entry For VMStore dialog box, select This Folder, Subfolders And Files from the drop-down list (this is the default), select Full Control under Successful and possibly under Failed (see Figure 8-13), and click OK to close the dialog box.



Name: Authenticated Users

Apply onto: This folder, subfolders and files

Access:	Successful	Failed
Full control	☑	☑
Traverse folder / execute file	☑	☑
List folder / read data	☑	☑
Read attributes	☑	☑
Read extended attributes	☑	☑
Create files / write data	☑	☑
Create folders / append data	☑	☑
Write attributes	☑	☑
Write extended attributes	☑	☑
Delete subfolders and files	☑	☑
Delete	☑	☑

□ Apply these auditing entries to objects and/or containers within this container only

FIGURE 8-13 Auditing changes in a VM storage folder

7. Close all other dialog boxes and repeat these steps for any other folder you want to audit.

From this point on, object modifications in this folder will be tracked for all users. Audited entries will be listed in the Security Event Log and can be viewed in Server Manager under the Diagnostics node in the Tree pane.

IMPORTANT **AUDITING HOST SERVERS**

Enabling the audit policy on a host server can have significant impact. Audited objects and events slow down the system, so it is important to audit only those events or objects you deem critical on each system. In addition, if the Security Event Log fills up entirely, it will stop a server from running and shut it down. Modify the settings for the Security Event Log to make sure this does not happen and monitor its growth closely. The last thing you want is a host server that no longer runs because its Security Event Log is full.

MORE INFO **COLLECTING EVENTS CENTRALLY**

Windows Server 2008, like Windows Vista, can now forward events to a central collection system. You might find this useful in an environment that relies mostly on Server Core machines. For instructions on how to forward events to a central collection system, look up "Collect Vista Events" at *http://www.prismmicrosys.com/newsletters_june2007.php*. For more information on Event Log operation in Windows Vista and Windows Server 2008, search for *Ruest* on the Prism Microsystem Web site.

Updating Host Servers

Host servers, like all other servers, must be updated on a regular basis. Applying updates during the installation of a server was discussed in Chapter 2 as you built your host systems. But after the server is running and hosting VMs, the process becomes slightly more complex.

As you know, many updates require a server reboot. Rebooting a host server can impact several production VMs and therefore must be done only when absolutely required. This is one reason why you should be running host servers in failover clusters. When you have highly available host servers, you use the following process to update each cluster node (see Figure 8-14):

1. Use Quick Migration to move the VMs running on one host node off to another node in the cluster (see Figure 8-15).
2. When the node is empty of VMs, apply the updates to the node.
3. Reboot the empty node if required.
4. Move the VMs back to the original node when the process is complete.

   You can repeat this process on other nodes until your entire resource pool is updated. Remember that the first version of Hyper-V only supports Quick Migration and therefore will cause a temporary stoppage of the services provided by a VM. For this reason, you should perform this operation during maintenance windows when you will not impact users by pausing the VMs they rely on.

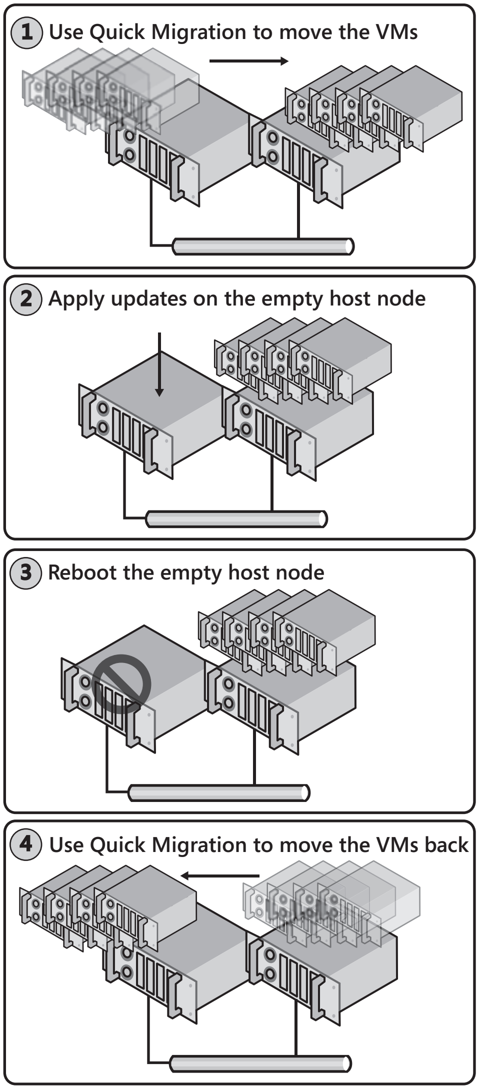

1 Use Quick Migration to move the VMs
2 Apply updates on the empty host node
3 Reboot the empty host node
4 Use Quick Migration to move the VMs back

FIGURE 8-14 Updating clustered hosts

The operation becomes much more complex when your host servers are not clustered. If you are running standalone hosts that support upward of 10 VMs each, you must wait until the appropriate maintenance window to update the hosts because all of the VMs can be shut down during the update process. Because you also have to update the VMs, this maintenance window must be considerable in length. This is one more reason why clustered host servers are the best host servers.

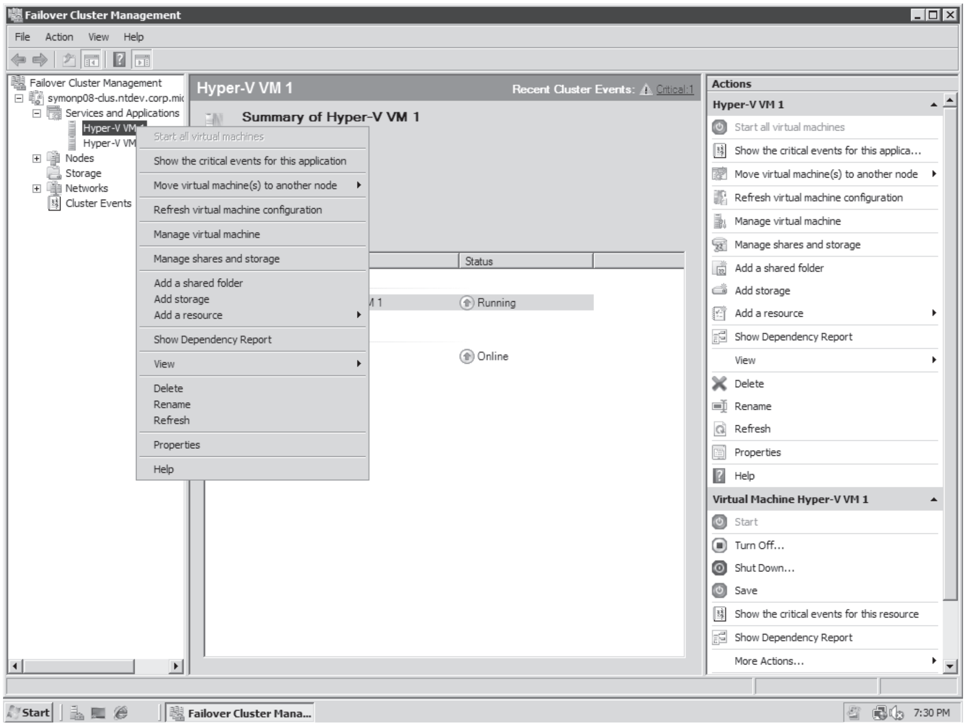

Failover Cluster Management
File Action View Help
Failover Cluster Management
symonp08-clus.ntdev.corp.mic
Services and Applications
Hyper-V VM
Hyper-V VM
Nodes
Storage
Networks
Cluster Events
Hyper-V VM 1
Recent Cluster Events: Critical: 1
Summary of Hyper-V VM 1
Start all virtual machines
Show the critical events for this application
Move virtual machine(s) to another node
Refresh virtual machine configuration
Manage virtual machine
Manage shares and storage
Add a shared folder
Add storage
Add a resource
Show Dependency Report
View
Delete
Rename
Refresh
Properties
Help
Status
Running
Online
Actions
Hyper-V VM 1
Start all virtual machines
Show the critical events for this applica...
Move virtual machine(s) to another node
Refresh virtual machine configuration
Manage virtual machine
Manage shares and storage
Add a shared folder
Add storage
Add a resource
Show Dependency Report
View
Delete
Rename
Refresh
Properties
Help
Virtual Machine Hyper-V VM 1
Start
Turn Off...
Shut Down...
Save
Show the critical events for this resource
Show Dependency Report
More Actions...
Start
Failover Cluster Mana...
7:30 PM

FIGURE 8-15 Moving VMs to another cluster node

PRACTICE Creating the Management Virtual Network

One of the most important tasks you will perform as a resource pool administrator is the configuration of security settings on your host servers. This is the subject of this practice. In this case, you will prepare a management virtual network to link the resource pool VMs to this network and therefore segregate the traffic from this utility domain from production systems. Because of its nature, this practice is very similar to that of Lesson 3 in Chapter 2. Ideally, this practice is performed using a third network adapter in each host server, but it can also be performed with only two. In production environments, make sure you set this up with a minimum of three adapters. This practice consists of three exercises. In the first exercise, you begin to prepare ServerFull01 by creating a new public virtual network connection. This connection will be linked to the management network adapter if only two adapters are present. If three adapters are present, you link it to the third adapter. In the second exercise, you perform the same activity on ServerCore01. In the third exercise, you connect the VMs belonging to the utility network to the new management virtual network adapter. This will serve to segregate all management traffic from other VM traffic.

EXERCISE 1 Create a Management Virtual Network Interface on a Full Installation

In this exercise you will configure an additional virtual network adapter on the full installation of Windows Server 2008. This exercise is performed on ServerFull01. Log on with domain administrator credentials.

1. This operation is performed either with Hyper-V Manager or with the Hyper-V Manager section of Server Manager. Click ServerFull01 in the Tree pane under Hyper-V Manager.
2. Click Virtual Network Manager in the Actions pane of the console. This opens the Hyper-V Virtual Network Manager dialog box. Note the existing networks.
3. Create a new virtual adapter. Click New Virtual Network in the left part of the dialog box, choose External, and then click Add.
4. Name the adapter **Hyper-V Management** and make sure External is selected as the connection type. Choose the appropriate physical adapter from the drop-down list. If you have only two adapters, choose the one that is not bound to the Hyper-V External virtual network adapter. If you have three, choose one of the other two that are not bound to the Hyper-V External network. Click OK. Do not apply a VLAN to the parent partition at this time. Click OK. The Apply Networking Changes warning will appear. Click Yes. This creates the new virtual adapter.
5. Move to the Network Connections window to rename the connections. Renaming the connections makes it much easier to link the network with the network type when working in the Windows interface of the parent partition. Click Start and then click Control Panel. In the Control Panel view, click Network And Internet, then click Network And Sharing Center, and then click Manage Network Connections in the Tasks section of the window. This opens the Network Connections window.
6. Rename the physical connection to which you bound the new management network. You can check each connection's properties to make sure you are renaming the appropriate network. This physical network adapter should only be bound to the Microsoft Virtual Network Switch Protocol. Right-click it and choose Rename. Type **Management NIC** and press Enter.

The new management virtual network is ready on ServerFull01.

EXERCISE 2 Create a Management Virtual Switch on a Server Core Installation

In this exercise you will create a new virtual network switch on Server Core. Perform this operation from ServerFull01. Log on with domain administrator credentials.

1. This operation is performed either with Hyper-V Manager or with the Hyper-V Manager section of Server Manager. Click ServerCore01 in the Tree pane under Hyper-V Manager.
2. Click Virtual Network Manager in the Actions pane of the console. This opens the Hyper-V Virtual Network Manager dialog box.
3. New Virtual Network and the External network type should already be selected. Click Add.

4. Name this adapter **Hyper-V Management**, make sure the External connection type is selected, and make sure the appropriate adapter is selected from the drop-down list. Use the same selection process as in step 4 of the previous exercise. Do not apply a VLAN to the parent partition at this time. Click OK. The Apply Networking Changes warning will appear. Click Yes.
5. To rename the network adapter in Server Core, you need to log on to the Server Core machine and use the *netsh* command to rename it. Log on with domain administrator credentials.
6. List the adapters, making note of the adapter ID number and then rename the appropriate adapter. Use the following commands. Your connection names may differ from the following example. Make sure you rename the appropriate adapter. This is why you run the *show interface* command first:

```
netsh interface ipv4 show interface
netsh interface set interface name=”Local Area Connection 5” newname=”Hyper-V
Management”
```

If you run the *show interface* command again (hint: use the Up arrow to call the command back), you will see that the interface has been renamed. The new management virtual network is ready on this server.

EXERCISE 3 Assign Management VMs to the New Management Virtual Network

In this exercise you will change the properties of any VM that belongs to the utility management domain for your resource pool. Connecting these machines to this network automatically segregates management traffic from any other traffic linked to other production virtual machines. Perform this exercise on ServerFull01. Log on with domain administrator credentials. You perform this exercise with Hyper-V Manager instead of SCVMM because the SCVMM server is a VM and will be one of the VMs you modify.

1. Log on to ServerFull01. This operation is performed either with Hyper-V Manager or with the Hyper-V Manager section of Server Manager. Click ServerFull01 in the Tree pane under Hyper-V Manager.
2. Right-click SCOM01 and choose Settings; then click Network Adapter.
3. Click the drop-down list of adapters and choose Hyper-V Management. Click OK. This changes the network this VM is attached to but does not change any other parameters.
4. Repeat steps 2 and 3 for any resource pool VM that is on ServerFull01.
5. Click ServerCore01 in the Tree pane and repeat the operation for any resource pool VM that is on this host server. This includes SCVMM01 at the very least.

When the operation is complete, all of the resource pool VMs will be on a segregated network.

IMPORTANT **SEGREGATING NETWORK TRAFFIC**

When you segregate network traffic and link it to a particular physical network adapter, it is no longer visible by other virtual networks and other adapters. However, be careful not to create two networks of different sensitivity on the same physical adapter. Traffic from one network will be visible to the other because they both share the same physical adapter.

✓ Quick Check

1. What are the three aspects of the default Windows Server 2008 installation that are modified when you add the Hyper-V role on either a full or a Server Core installation?
2. What are software restriction policies?
3. From where do you launch the Security Configuration Wizard?
4. How can you determine which authorized devices can be installed on servers and PCs?
5. Name at least two requirements for the use of BitLocker Full Drive Encryption.

Quick Check Answers

1. The three aspects of the default Windows Server 2008 installation that are modified are:
   - Installed Files New files installed in support of the Hyper-V role.
   - Installed Services The services installed in support of the Hyper-V role.
   - Firewall Rules The rules that are modified or enabled with the addition of the Hyper-V role.
2. Software restriction policies are policies that control which code is allowed to run with your network.
3. The Security Configuration Wizard is launched through the Administrative Tools.
4. You can use device control policies in Active Directory Domain Services to determine which devices are allowed on your network.
5. To be able to use BitLocker Full Drive Encryption you need:
   - A minimum of two NTFS partitions.
   - A USB flash drive and a BIOS that supports reading and writing to a USB flash drive at startup.
   - A Trusted Platform Module version 1.2 or later.
   - A Trusted Computing Group-compliant BIOS.

Lesson 2: Securing the Virtual Environment

In addition to the security settings you assign to host servers and resource pool components, you should also look to the security of your production virtual machines. Another element that is essential in any virtual infrastructure security policy is the assignment of appropriate roles to administrators and technicians. Both help complete your virtual infrastructure security strategy.

After this lesson, you will understand:

- The various Hyper-V management roles.
- The potential threats and risks for virtual machines.
- The security features you should set for virtual machines.
- How to secure a Hyper-V virtual machine.

Estimated lesson time: 30 minutes

Preparing Hyper-V Management Roles

You can prepare management and administration roles with Hyper-V in two ways. The first is designed for smaller resource pools and the second is designed for resource pools that rely on a central host server management tool.

- **Distributed Management Resource Pools** In small resource pools, you must rely on the Authorization Manager to assign least-privilege access to administrators and technicians with various roles. These are called *distributed management* resource pools because they do not contain a central management tool and all Hyper-V hosts are managed individually. Only organizations running very small resource pools would use this approach.
- **Centrally Managed Resource Pools** Resource pools that rely on a host server and virtual machine management tool will also rely on this tool's delegation capabilities to assign least-privilege access rights to administrators and technicians. For example, organizations that rely on SCVMM would use SCVMM's internal controls to assign delegation rights.

EXAM TIP **USING SCVMM VS. USING AUTHORIZATION MANAGER**

You cannot use Authorization Manager to assign delegation rights on a Hyper-V host that is already being managed by SCVMM because permissions will conflict and you may lose access to the host server. Keep this in mind as you run through the delegation of rights portion of the exam.

The method you will rely on is determined by the type of environment you work in, the trust you have in your fellow administrators, and the number of host servers and virtual machines you have to manage.

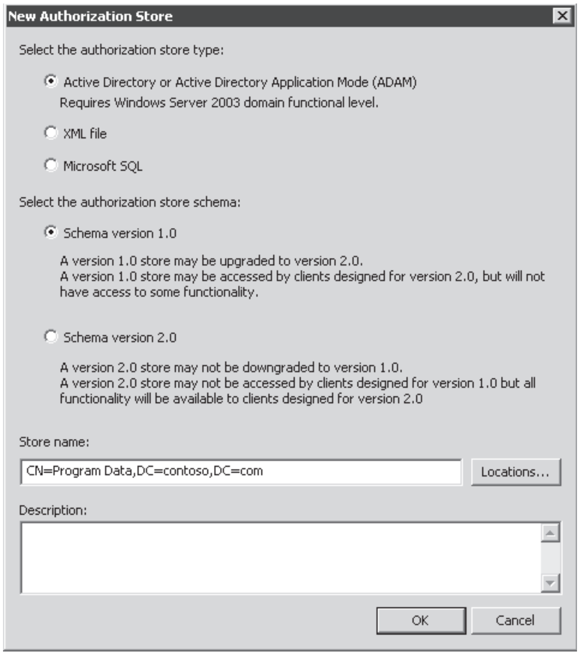
EXAM TIP **USING SCVMM AND AUTHORIZATION MANAGER**

The exam topics cover the assignment of role-based access control settings in both Authorization Manager and in SCVMM, so be sure to read and practice with both.

Introducing Authorization Manager

Authorization Manager (AzMan) is a tool that allows you to manipulate special, application-specific credential stores in Windows servers called *authorization stores*. Note that Authorization Manager is only available on full installations of Windows Server 2008. Server Core has no equivalent tool. The benefit of these stores is that they can be tied to specific applications and they can be used to assign role-based access controls to either users or groups. As always, groups are preferred because they guarantee that each user is given a specific set of access rights.

Authorization stores can be stored in a variety of locations (see Figure 8-16). Each has its own characteristics, which are outlined in Table 8-4.



New Authorization Store

Select the authorization store type:

● Active Directory or Active Directory Application Mode (ADAM)
Requires Windows Server 2003 domain functional level.

○ XML file

○ Microsoft SQL

Select the authorization store schema:

● Schema version 1.0

A version 1.0 store may be upgraded to version 2.0.
A version 1.0 store may be accessed by clients designed for version 2.0, but will not have access to some functionality.

○ Schema version 2.0

A version 2.0 store may not be downgraded to version 1.0.
A version 2.0 store may not be accessed by clients designed for version 1.0 but all functionality will be available to clients designed for version 2.0

Store name: CN=Program Data,DC=contoso,DC=com

Description:

FIGURE 8-16 Choosing the store type during the creation of a new store

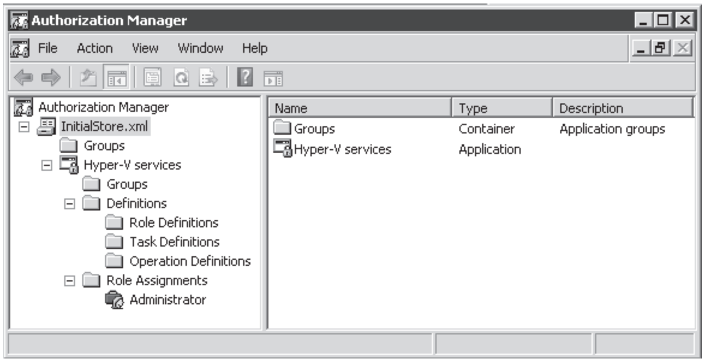
TABLE 8-4 Secure Virtual Service Offerings

LOCATION	DESCRIPTION
Locally in an XML file	For Hyper-V host servers, the XML store is located in %ProgramData%\Microsoft\Windows\Hyper-V\InitialStore.XML. This file must be secured and guarded carefully if you choose to work with local stores. Note that this file is located on both full and Server Core installations. However, because it is only an XML text file, it can easily be replicated to any number of independent Hyper-V servers and then reloaded locally to ensure that all hosts run the same access rights configuration. This store can only be protected through NTFS access rights or through Full Drive Encryption with BitLocker.
Active Directory Lightweight Directory Services	The authorization store can also be located within an AD LDS directory store. AD LDS does not offer the network operating system capabilities of AD DS, but it does support the ability to create a replication scope for its application-specific directory stores. Therefore, you could use it to ensure that multiple Hyper-V host servers rely on the same authorization settings. This store is slightly more secure than the XML store because it is also located within a file on the local file system. However, you need to use directory interfaces to manipulate it.
SQL Server	The authorization store can also be stored within a SQL Server database. Because many Hyper-V resource pools include a database server to support management tools and utilities, this is unlikely to be a viable option for Hyper-V. Remember that if you use a management tool, you should not rely on Authorization Manager stores. However, this option would be more secure than the first two because it is centralized and is contained within a database.
Active Directory Domain Services	Configuring the authorization store to be saved within the directory service automatically makes it available to any number of domain-joined Hyper-V member servers. Authorization stores are not only used with Hyper-V, but because they are application-specific, you can also save several of them in the directory without impacting the others. This option is the most secure and should be the default in any environment where authorization stores for Hyper-V are required, there is no other management tool, and the host servers are joined to a domain.

EXAM TIP **AUTHORIZATION STORES AND AD DS**

Authorization stores were introduced with Windows Server 2003. Therefore, when you store them in Active Directory, the directory must at least be at the Windows Server 2003 functional level. Keep that in mind when AzMan questions come up.

Authorization stores provide a simplified data structure for the integration of groups and business rules as well as authorization policies. They can be manipulated through the Authorization Manager Snap-in or its application programming interface (API). In Windows Server 2008, this snap-in is already included in a console that can be called by typing **AzMan.msc** at the prompt in the Start menu. By default, no store is opened when you first launch Authorization Manager. To open the Hyper-V initial store, right-click Authorization Manager in the Tree pane, choose Open Authorization Store, and then navigate to %ProgramData%\Microsoft\Windows\Hyper-V to open InitialStore.xml. This will populate AzMan with the default Hyper-V store (see Figure 8-17).



Name	Type	Description
Groups	Container	Application groups
Hyper-V services	Application	

FIGURE 8-17 The structure of the Hyper-V initial store

Authorization Manager was first introduced in Windows Server 2003. Stores that use the AzMan Schema version 1.0 are compatible with Windows Server 2003. Stores that use Schema version 2.0 are only compatible with Windows Server 2008. Version 1.0 stores can be upgraded to version 2.0, but the upgrade process is one-way and irreversible. Because all servers running Hyper-V are also running Windows Server 2008, you can create version 2.0 stores to manage RBAC in Hyper-V. Remember, however, that your domain controllers will also need to be running Windows Server 2008 and be running the Windows Server 2008 directory functional level.

MORE INFO **AUTHORIZATION MANAGER**

One of the best places to obtain information on AzMan and authorization stores is with the Windows Server 2008 Help System. Use the Help button in the AzMan console when on a local system. You can also access it online at *http://technet.microsoft.com/en-us/library/cc726036.aspx*.

XML stores provide limited role-based access control functionality because they do not support delegation of applications, stores, or scopes. This is because its sole protection is the NTFS access control entries (ACEs) and this level of protection can only control access to the entire contents of the store within the file. In addition, NTFS cannot support sequential writes to a file as a single operation. Therefore, the XML file could become corrupted if two administrators modified it at the same time from two different interfaces. This does not happen with the other locations for authorization stores.

Hyper-V authorization stores are made up of four different components:

- **Store scope** The scope of a store determines its breadth in your organization. Scopes can span geographical locations; organizational structures; operational functions such as development, staging, testing, training, or production; or can simply be assigned to a directory in AD DS. When assigned to AD DS directories, the scope will span the entire directory it is stored in. This is because AD DS authorization stores use Lightweight Directory Application Protocol (LDAP) naming structures and these naming structures provide a directory-level scope.
- **Store tasks** Tasks are based on operations. Even though you cannot create any new Hyper-V operations in AzMan, you can regroup any number of tasks to create specific roles within your organization. Table 8-5 outlines examples of the various tasks you can assign in AzMan with regard to Hyper-V as well as the operations they allow access to. These tasks are not predefined in AzMan and must be defined interactively before you can assign them.
- **Store roles** Roles regroup different tasks to support specific operational functions within your resource pool. Roles can include administrators who have access to everything; Host Monitors; VM Monitors, who monitor either the hosts or the VMs they run; VM Creators, who manage the state of VMs; Host Administrators, who control host-only operations; or any other required role according to your organizational standards.
- **Assigned users or groups** Users or groups—preferably groups—are assigned to the various roles you generate in the authorization store.

Similarly, the process of creating or modifying a store follows a four-step procedure that focuses on each one of the four aspects of a store.

TABLE 8-5 Tasks and Operations

TASKS	OPERATIONS
Add external network to server	■ Bind External Ethernet Port ■ Connect Virtual Switch Port ■ Create Internal Ethernet Port ■ Create Virtual Switch ■ Create Virtual Switch Port ■ View External Ethernet Ports ■ View Internal Ethernet Ports ■ View LAN Endpoints

TASKS	OPERATIONS
	■ View Switch Ports ■ View Switches ■ View Virtual Switch Management Service ■ View VLAN Settings
Add internal network to server	■ Connect Virtual Switch Port ■ Create Internal Ethernet Port ■ Create Virtual Switch ■ Create Virtual Switch Port ■ View Internal Ethernet Ports ■ View LAN Endpoints ■ View Switch Ports ■ View Switches ■ View Virtual Switch Management Service ■ View VLAN Settings
Add private network	■ Connect Virtual Switch Port ■ Create Virtual Switch ■ View Switch Ports ■ View Switches ■ View Virtual Switch Management Service
Apply a snapshot	■ Allow Output From Virtual Machine ■ Pause And Restart Virtual Machine ■ Read Service Configuration ■ Reconfigure Virtual Machine ■ Start Virtual Machine ■ Stop Virtual Machine ■ View Virtual Machine Configuration
Attach internal network adapter to virtual machine	■ Allow Output From Virtual Machine ■ Change VLAN Configuration On Port ■ Connect Virtual Switch Port ■ Create Virtual Switch Port ■ Read Service Configuration ■ Reconfigure Virtual Machine

TASKS	OPERATIONS
	View Internal Ethernet Ports View LAN Endpoints View Switch Ports View Switches View Virtual Machine Configuration View Virtual Switch Management Service View VLAN Settings
Connect to a virtual machine	Allow Input To Virtual Machine Allow Output From Virtual Machine Read Service Configuration
Create a virtual floppy disk or virtual hard disk	Read Service Configuration
Create a virtual machine	Allow Output From Virtual Machine Change Virtual Machine Authorization Scope Create Virtual Machine Read Service Configuration Optional: Connect Virtual Switch Port
Delete a private network	Delete Virtual Switch View Switch Ports View Switches View Virtual Switch Management Service
Delete a snapshot	Delete Virtual Machine Read Service Configuration
Delete a virtual machine	Allow Output From Virtual Machine Delete Virtual Machine Read Service Configuration
Export virtual machine	Allow Output From Virtual Machine Read Service Configuration
Import virtual machine	Allow Output From Virtual Machine Change Virtual Machine Authorization Scope Create Virtual Machine View Virtual Machine Configuration

TASKS	OPERATIONS
Modify virtual machine settings (reconfigure a virtual machine)	■ Allow Output From Virtual Machine ■ Read Service Configuration ■ Reconfigure Virtual Machine ■ View Virtual Machine Configuration
Pass Ctrl+Alt+Delete (send control signals to a VM)	■ Allow Input To Virtual Machine ■ Allow Output From Virtual Machine ■ Read Service Configuration
Pause a virtual machine	■ Allow Output From Virtual Machine ■ Pause And Restart Virtual Machine ■ Read Service Configuration
Remove external network adapter from a virtual machine	■ Allow Output From Virtual Machine ■ Change VLAN Configuration On Port ■ Create Virtual Switch Port ■ Disconnect Virtual Switch Port ■ Read Service Configuration ■ Reconfigure Service ■ Reconfigure Virtual Machine ■ View External Ethernet Ports ■ View LAN Endpoints ■ View Switch Ports ■ View Switches ■ View Virtual Machine Configuration ■ View Virtual Switch Management Service ■ View VLAN Settings
Remove external network adapter from server	■ Delete Internal Ethernet Port ■ Delete Virtual Switch ■ Delete Virtual Switch Port ■ Disconnect Virtual Switch Port ■ Unbind External Ethernet Port ■ View External Ethernet Ports ■ View Internal Ethernet Ports ■ View LAN Endpoints

TASKS	OPERATIONS
	■ View Switch Ports ■ View Switches ■ View Virtual Switch Management Service ■ View VLAN Settings
Remove internal network adapter from a virtual machine	■ Allow Output From Virtual Machine ■ Change VLAN Configuration On Port ■ Create Virtual Switch Port ■ Disconnect Virtual Switch Port ■ Read Service Configuration ■ Reconfigure Service ■ Reconfigure Virtual Machine ■ View Internal Ethernet Ports ■ View LAN Endpoints ■ View Switch Ports ■ View Switches ■ View Virtual Machine Configuration ■ View Virtual Switch Management Service ■ View VLAN settings
Remove internal network adapter from server	■ Delete Internal Ethernet Port ■ Delete Virtual Switch ■ Delete Virtual Switch Port ■ Disconnect Virtual Switch Port ■ View Internal Ethernet Ports ■ View LAN Endpoints ■ View Switch Ports ■ View Switches ■ View VLAN Settings ■ View Virtual Switch Management Service
Remove private network adapter from a virtual machine	■ Allow Output From Virtual Machine ■ Create Virtual Switch Port ■ Disconnect Virtual Switch Port ■ Read Service Configuration

TASKS	OPERATIONS
	Reconfigure Service Reconfigure Virtual Machine View LAN Endpoints View Switch Ports View Switches View Virtual Machine Configuration View Virtual Switch Management Service
Remove private network adapter from server	Delete Virtual Switch View Switch Ports View Switches View Virtual Switch Management Service
Rename snapshot	Allow Output From Virtual Machine Read Service Configuration Reconfigure Virtual Machine View Virtual Machine Configuration
Rename a virtual machine	Allow Output From Virtual Machine Read Service Configuration Reconfigure Virtual Machine View Virtual Machine Configuration
Resume a virtual machine	Allow Output From Virtual Machine Pause and Restart a Virtual Machine Read Service Configuration
Save a virtual machine and stop a virtual machine	Allow Output From Virtual Machine Read Service Configuration Stop Virtual Machine
Start a virtual machine	Allow Output From Virtual Machine Read Service Configuration Start Virtual Machine
Turn off a virtual machine	Allow Output From Virtual Machine Read Service Configuration Stop Virtual Machine

TASKS	OPERATIONS
View Hyper-V Server settings	■ Allow Output From Virtual Machine ■ Read Service Configuration ■ Reconfigure Service ■ View Virtual Machine Configuration
View network adapter management	■ View Switch Ports ■ View Virtual Switch Management Service
View virtual machine	■ Allow Output From Virtual Machine ■ Read Service Configuration ■ View Virtual Machine Configuration

Using the Authorization Manager to Assign Management Roles

By default, only the local administrator of a host system has any role within the default InitialStore.xml policy. Also, the policy is an XML policy by default and is individual to each host server.

AzMan operates in two different modes. Administrator mode lets you modify an existing policy. Developer mode lets you create new policies and modify the structure of an existing policy. AzMan launches in Administrator mode by default.

Ideally, your policies will be stored within the utility directory you use to centralize host server access. This means that you need to create a new policy. When you do so, you'll need to perform several activities:

- Change to developer mode.
- Create the store and place it in AD DS. This also defines the scope of the policy.
- Identify the application for which you want to create a store.
- Define the roles you want to assign.
- Identify the groups to which you want to assign the roles.

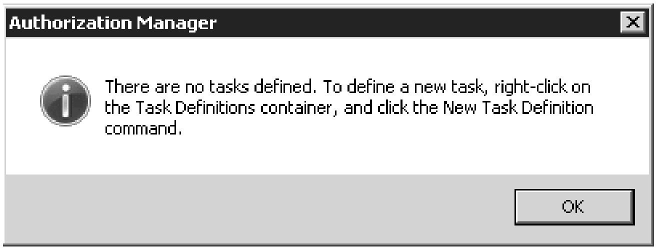
IMPORTANT **SCVMM AND AUTHORIZATION MANAGER**

Do not use Authorization Manager if you are using SCVMM because the two authorization systems will conflict and you may lose access to your host servers.

Ideally, you will begin with the last task because these groups will be required to assign roles to them. Proceed as follows:

1. Log on with domain administrator credentials on a computer that includes the Active Directory Users And Computers (ADUC) console. Launch the console through the Start menu and Administrative Tools. Alternatively, you can use the ADUC portion of the Server Manager console if you are logged on to a server or are using the console remotely through Terminal Services RemoteApps.

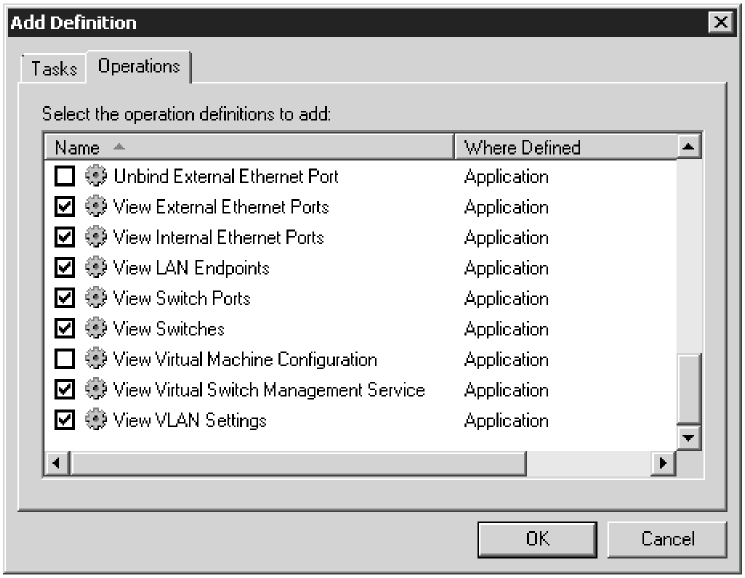
2. Create the required security groups. These groups should be placed within their own OU if possible. If you have an existing OU structure, identify an appropriate location for the OU in your hierarchy. If you don't have an existing structure, you can create a new top-level OU called RBAC Assignments. Right-click the domain name, select New, select Organizational Unit, type **RBAC Assignments**, and click OK. This creates the OU and moves you into it.
3. Right-click the OU, select New, and then select Group. Name the group, make sure it is a Global Security group, and click OK. You should create as many groups as you intend to have roles. Keep the structure as simple as your organizational policies allow.
   For example:
   - **Resource Pool Administrators** Includes the domain administrators for the utility forest. You should limit the number of users in this role.
   - **VM Users** Includes anyone who can use a VM but can only use VMs.
   - **VM Administrators** Includes anyone who can modify VM settings.
4. Add the appropriate accounts to each group. Right-click the group, select Properties, move to the Members tab, and then click Add to locate the accounts to add. Click OK twice when done and repeat for each group. Remember the group names you used and close ADUC.
5. You can now move to AzMan. Use a computer that has AzMan installed. A full installation of a computer running Hyper-V will work. Log on with domain administrator credentials and launch AzMan by typing **AzMan.msc** in the Search box in the Start menu. Press Enter to launch the tool.
6. Note that the existing policy is not displayed. Remember that it is stored within the ProgramData folder, which is a hidden folder by default. You can either type the path to InitialStore.xml or change your settings to view hidden files and folders and simply navigate to locate the file through the Browse button. Open the XML store to view its contents. The path to the store is c:\ProgramData\Microsoft\Windows\Hyper-V. If you are performing this operation remotely, the path is \\servername\C$\ProgramData\Microsoft\Windows\Hyper-V, where *servername* is the name of the Hyper-V host server whose store you want to modify. Right-click Authorization Manager in the Tree pane and choose Open Authorization Store. Note the structure of this store. Expand each section of the store.
7. Create new tasks. Rely on the information in Table 8-5 listed earlier. Create each of the tasks in this table. Proceed as follows.
   a. Right-click Task Definitions under Definitions in the Tree pane and choose New Task Definition. Name the task as displayed in Table 8-5. You do not need to add a description because the task name is already descriptive.
   b. Click Add to add operations to this task. You will receive a warning that there are no tasks defined (see Figure 8-18); this message appears only the first time you create a task. Click OK. This opens the Add Definition dialog box.



There are no tasks defined. To define a new task, right-click on the Task Definitions container, and click the New Task Definition command.

FIGURE 8-18 The No Tasks Defined warning

c. Move to the Operations tab and select each of the operations listed in Table 8-5 for this task (see Figure 8-19).



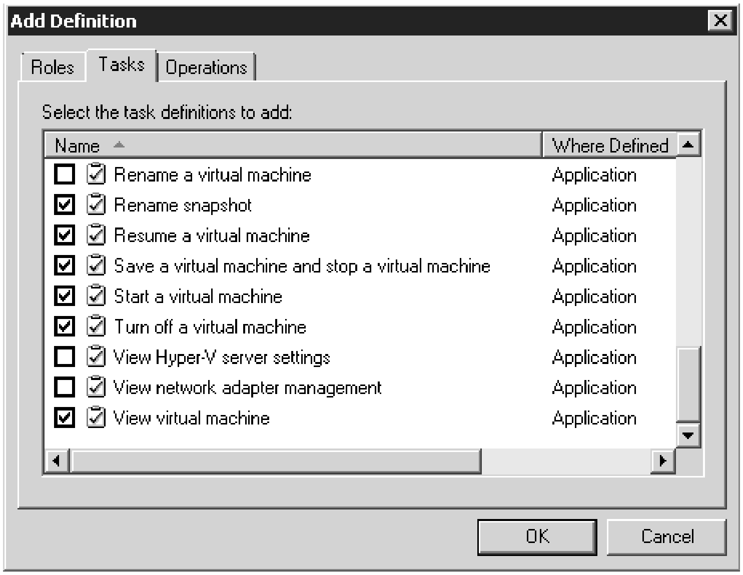
Select the operation definitions to add:

	Name	Where Defined
□	Unbind External Ethernet Port	Application
☑	View External Ethernet Ports	Application
☑	View Internal Ethernet Ports	Application
☑	View LAN Endpoints	Application
☑	View Switch Ports	Application
☑	View Switches	Application
□	View Virtual Machine Configuration	Application
☑	View Virtual Switch Management Service	Application
☑	View VLAN Settings	Application

FIGURE 8-19 Assigning operations to tasks

d. Click OK twice when done and repeat for each of the task definitions in the table.

8. When you have defined the tasks, you can move on to create new roles. Right-click Role Definitions under Definitions in the Tree pane and choose New Role Definition. Type **VM Users**, add a short description such as **Members can work with virtual machines**, and click Add to assign tasks to this role. Click the Tasks tab, select the appropriate tasks (see Figure 8-20), and click OK twice to complete the role definition process. Repeat for the VM Administrators role with a description of **Members can create and manage virtual machines**. Use the values in Table 8-6 to assign tasks to each role.



Select the task definitions to add:

	Name	Where Defined
☐	Rename a virtual machine	Application
☑	Rename snapshot	Application
☑	Resume a virtual machine	Application
☑	Save a virtual machine and stop a virtual machine	Application
☑	Start a virtual machine	Application
☑	Turn off a virtual machine	Application
☐	View Hyper-V server settings	Application
☐	View network adapter management	Application
☑	View virtual machine	Application

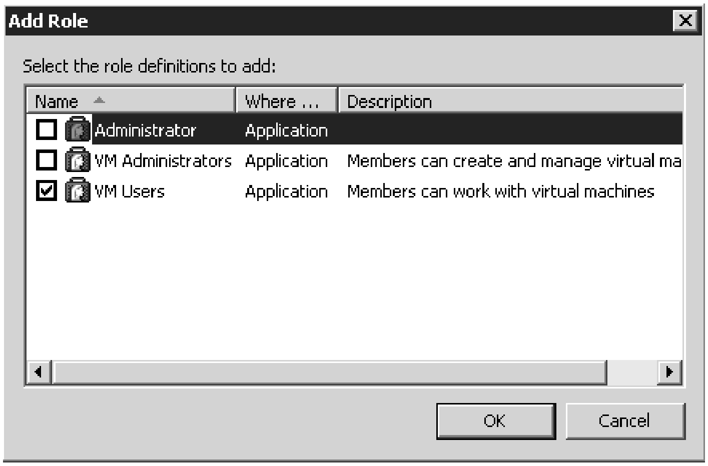
FIGURE 8-20 Assigning tasks to role definitions

TABLE 8-6 Assigning Tasks to Roles

ROLE	TASKS
VM User	■ Apply A Snapshot ■ Connect To A Virtual Machine ■ Pass Ctrl+Alt+Delete (Send control signals to a VM) ■ Pause A Virtual Machine ■ Rename Snapshot ■ Resume A Virtual Machine ■ Save A Virtual Machine And Stop A Virtual Machine ■ Start A Virtual Machine ■ Turn Off A Virtual Machine ■ View Virtual Machine
VM Administrator	■ Apply A Snapshot ■ Attach Internal Network Adapter To Virtual Machine ■ Connect To A Virtual Machine ■ Create A Virtual Floppy Disk Or Virtual Hard Disk ■ Create A Virtual Machine ■ Delete A Snapshot ■ Delete A Virtual Machine ■ Export Virtual Machine

ROLE	TASKS
	■ Import Virtual Machine ■ Modify Virtual Machine Settings (reconfigure a virtual machine) ■ Pass CTRL+ALT+DELETE (send control signals to a VM) ■ Pause A Virtual Machine ■ Remove External Network Adapter From A Virtual Machine ■ Remove Internal Network Adapter From A Virtual Machine ■ Remove Private Network Adapter From A Virtual Machine ■ Rename Snapshot ■ Rename A Virtual Machine ■ Resume A Virtual Machine ■ Save A Virtual Machine And Start A Virtual Machine ■ Start A Virtual Machine ■ Turn Off A Virtual Machine ■ View Virtual Machine

9. Now assign the role definitions to role assignments. Right-click Role Assignments and choose New Role Assignment. Select the VM Users role (see Figure 8-21) and click OK. Repeat for the VM Administrators role. This adds the two role definitions to your authentication store.



Add Role

Select the role definitions to add:

Name	Where ...	Description
□ Administrator	Application	
□ VM Administrators	Application	Members can create and manage virtual ma
☑ VM Users	Application	Members can work with virtual machines

FIGURE 8-21 Assigning role definitions to role assignments

10. You can now assign users to the two new roles. Right-click VM Users under Role Assignments in the Tree pane, click Assign Users And Groups, then choose from Windows and Active Directory, type **VM Users** and click Check Names, then click OK. Repeat for the VM Administrators role.

Your role assignments are complete for the first server you were working with. Now copy this updated XML file to each of your host servers:

1. Use Windows Explorer to copy the file to each of the hosts on your network. Make sure you copy the InitialStore.xml to the %ProgramData%\Microsoft\Windows\Hyper-V folder and replace the existing file.
2. Return to Authorization Manager, right-click Authorization Manager in the Tree pane, and choose Open Authorization Store. Open the remote store on the other host servers. Use \\servername\c$\ProgramData\Microsoft\Windows\Hyper-V to open a remote store. Click OK.
3. Right-click the new store and choose Reload. This reloads the information in the store. Note that it is identical to the one you just created.
4. Repeat steps 1 through 3 on each host server to ensure that they all use the same authorization store.

Make sure you repeat this copy and reload process each time you modify the store. This is one more reason why you should use AD DS groups to assign roles: If you need to add or remove a user, you only have to do it in a single location—Active Directory Domain Services—and it will be modified on each of your host servers.

IMPORTANT **HYPER-V ADMINISTRATOR ROLE**

Keep in mind that any user you add to the Hyper-V Administrator role in Authorization Manager in the InitialStore.xml will automatically gain all administrative rights for a Hyper-V even if that user is not a local administrator on the server. Use these rights with care.

MORE INFO **HYPER-V REMOTE MANAGEMENT CONFIGURATION UTILITY**

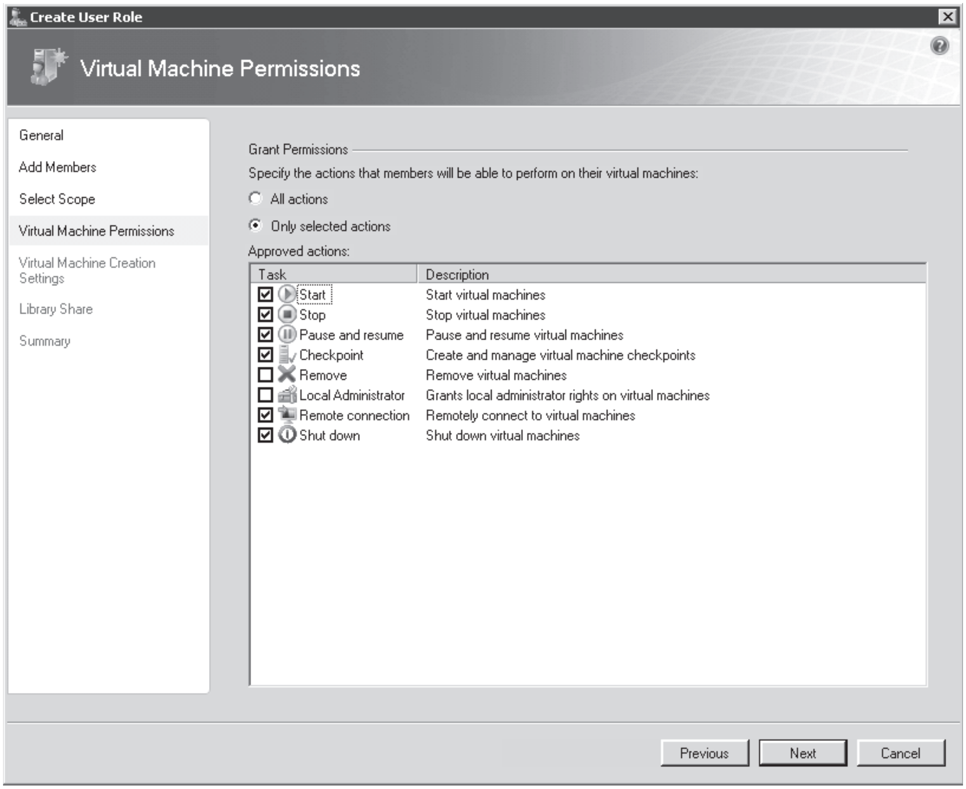
John Howard, a member of the Hyper-V development team, has created a useful utility for configuring Hyper-V authorization stores remotely. Find it at *http://code.msdn.microsoft.com/HVRemote*.

Using SCVMM to Assign Management Roles

As you learned in Chapter 3, SCVMM relies on a SQL Server database to store configuration information about the environment it controls. In addition, it is a sophisticated virtualization management tool that can support homogeneous or heterogeneous resource pools. Because of this, it already includes defined roles, tasks, and operations for the delegation of administrative tasks in resource pools. For example, you have already seen and used the Self-Service Portal, which relies on role delegation to allow users to work with their own VMs. This portal defines roles for users. The Delegated Administrator section of SCVMM defines roles for administrative delegation. Three main roles can be defined with SCVMM:

- **Full Resource Pool Administrator** This is the default administrator role in SCVMM. This role grants access to every SCVMM feature on every host server.

- **Delegated Administrator** This role supports the delegation of administration to portions of SCVMM. These portions include:
  - **Host Groups** Delegated administrators can access host server properties and the VMs they run through the host groups you assign them.
  - **Libraries** Delegated administrators can access VMs, templates, guest operating system and hardware profiles, ISOs, and more through the libraries you assign them.
- **Virtual Machine User** This role is defined by the Self-Service Portal. Any user that has access to this portal can work with the VMs you assign and the VM rights you grant to the role (see Figure 8-22).


Create User Role
Virtual Machine Permissions
General
Add Members
Select Scope
Virtual Machine Permissions
Virtual Machine Creation Settings
Library Share
Summary
Previous
Next
Cancel

Grant Permissions

Specify the actions that members will be able to perform on their virtual machines:

○ All actions

● Only selected actions

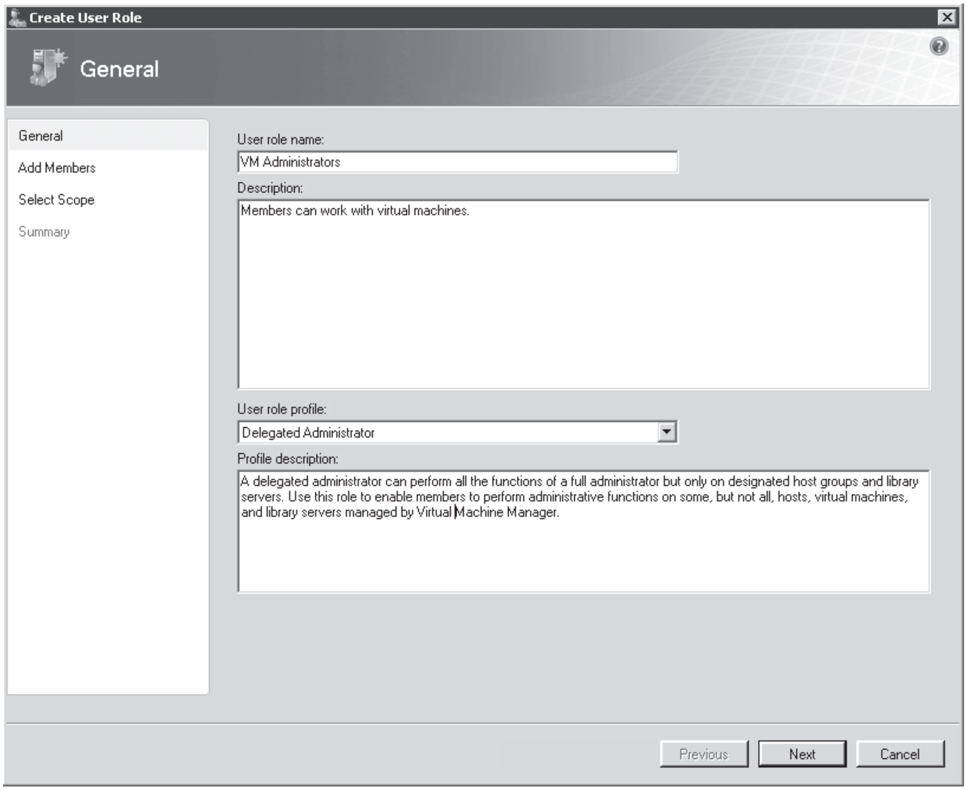
Approved actions:

Task	Description
☑ Start	Start virtual machines
☑ Stop	Stop virtual machines
☑ Pause and resume	Pause and resume virtual machines
☑ Checkpoint	Create and manage virtual machine checkpoints
□ Remove	Remove virtual machines
□ Local Administrator	Grants local administrator rights on virtual machines
☑ Remote connection	Remotely connect to virtual machines
☑ Shut down	Shut down virtual machines

FIGURE 8-22 Controlling self-service user rights in SCVMM

Working with a variety of the various assignments you create in SCVMM allows you to control exactly which access rights users will be granted.

Delegation in SCVMM is performed through the Administrators view under User Roles. To create a new user role, click New User Role in the Actions pane and then follow the steps in the wizard. The New User Role Wizard in SCVMM lets you assign two different types of delegations: for delegated administrators or for self-service users (see Figure 8-23). By default, the wizard starts in Self-Service User mode.



User role name: VM Administrators

Description: Members can work with virtual machines.

User role profile: Delegated Administrator

Profile description: A delegated administrator can perform all the functions of a full administrator but only on designated host groups and library servers. Use this role to enable members to perform administrative functions on some, but not all, hosts, virtual machines, and library servers managed by Virtual Machine Manager.

FIGURE 8-23 Delegating administrative tasks in SCVMM

Securing Hyper-V VMs

When it comes to protecting virtual machines, you should already be in familiar territory because the VMs you run are mostly production machines and as such should benefit from the standard security features you assign to production systems.

You should still be aware of a few caveats with regard to the VMs you run and who has access to the files that make them up:

- Consider how you will structure your storage system for VMs. You should keep all of the files that make up a VM in the same folder for ease of use. However, keep in mind that doing this also makes it easy to steal a VM. Make sure you set tight access control lists on the storage folders you use for VMs and their components.
- Parked VMs might be more at risk. Resource pool administrators often have a number of different virtual machines that are not necessarily in a running state. In addition, resource pool administrators often have a tendency to place these resting VMs in a saved state. This generates a file with the memory contents of the VM. In certain situations, this file can be a risk because it can contain in-memory passwords. Malicious

users who gain access to this file could use it to discover these passwords and gain access to information they should not have. Keep this in mind each time you save the state of a sensitive VM.

- Audit all VM access, as mentioned in Lesson 1. This ensures that you know who has and who wants access to the files that make up your VMs.
- Verify that all virtual machines are up to date before you deploy them in a production environment. This process was discussed in Chapter 4.
- Keep all VMs—parked or running—up to date in terms of updates and hotfix packages. It is very easy to fall into the "update trap" with VMs and forget to update VMs that have been parked for long periods of time. Then, when the VM is finally restarted, it is at risk and could cause a serious security breach in your network.
- Keep the number of resource pool administrators to a minimum while still being able to maintain and operate the environment properly. Resource pool administrators are highly trusted individuals. Screen these individuals thoroughly before giving them this level of authority in your network. If more administrators are required, use the delegation practices mentioned at the beginning of this lesson to assign appropriate rights.

As a rule, you should consider running Windows Server 2008 on your virtual machine servers because this is the most secure version of Windows Server and you should update it whenever new versions come out. In addition, you should be relying on the security technologies outlined in Table 8-7 within your production virtual workloads.

TABLE 8-7 Secure Virtual Service Offerings

CONTENTS	COMMENTS
Communications	Make sure all users, including administrators, understand their responsibilities in terms of security practices.
Security configuration	Pay special attention to the following: ■ Service hardening ■ Security Configuration Wizard settings for virtual servers ■ Limited role installations on each virtual machine with only required components for the service it delivers ■ User Account Control (UAC) for all administrators and all users ■ Device control, to ensure that unauthorized USB disk drives cannot be connected to any access point, including any PC or thin client on the network ■ BitLocker Drive Encryption for highly secure notebooks ■ Wireless networking security
Anti-malware	Implement Windows Defender along with proper antivirus technologies.

CONTENTS	COMMENTS
General AD DS security	Implement very tight permissions management. Implement multiple password policies to require highly complex passwords for administrators. Tighten delegation-of-authority settings on your servers. Implement read-only domain controllers in remote offices. Implement software restriction policies to ensure that no malicious code is allowed to run in the production domain.
File system	Secure the file system to protect VSOs. Implement access-based enumeration to further protect information. Rely on digitally signed Windows Installer packages for all third-party or custom product installations.
Print system	Implement a full security strategy for all printers.
.NET Framework security	Applicable to any machine that has an application role or any machine that includes Windows PowerShell. (In many cases, this will be every server in the VSO network.)
Internet Information Services (IIS)	Implement tight Web server security on all Web servers.
User identification	Rely on smart card or two-factor authentication for administrators in very secure environments. Highly secure environments will use two-factor authentication for all users.
Security policies	Assign proper policies for the VSO network.
Resource access	Tightly control all resource access. Implement EFS for mobile users. Rely on AD LDS for custom application resource access.
Role-based access control	Implement in every application as much as possible.
Access auditing/ monitoring	Turn on auditing, as well as AD DS auditing, to track all changes.
Digital Rights Management (DRM)	Rely on Active Directory Rights Management Services to apply DRM to all documentation that is copyrighted or sensitive in any way.

CONTENTS	COMMENTS
Perimeter networks	Configure the Windows Server Firewall with Advanced Security to control access to all servers, especially those in the perimeter network. Apply the same tool to Windows Vista PCs and mobile workstations.
Virtual private networks (VPNs)	Rely on VPN connections for all remote access.
Routing and Remote Access (RRAS)	Implement a remote access authentication service for users working remotely.
Secure Sockets Tunneling Protocol (SSTP)	Ensure that all remote communications, as well as internal intra-server communications, are encrypted.
Public key infrastructures (PKIs)	Implement Active Directory Certificate Services (AD CS) in support of smart card deployment and software restrictions.
Identity federation	Rely on Active Directory Federation Services for extranet access, if it is required.
Security Configuration Wizard	Ideally, create base servers for each role you intend to deploy, create a baseline policy from each of these servers, and apply the policy each time you work with a new server for any given role.

Virtual service offerings require more in terms of security settings because they are designed to interact with end users and therefore have more services built into the infrastructure. The scope of protection for VSOs depends on the size of the organization. Certain security technologies are reserved for resource pools, just the way that some are reserved for virtual service offerings. For example, you should not need to run Server Core in your VSOs because they are virtual machines. It is more important to make sure that you apply the appropriate level of security on a full installation of Windows Server 2008 than to deploy Server Core on virtual machines. In the long run, you will appreciate the access to the graphical interface when it comes to long-term management practices of your VSOs.

Populating Virtual Machines on Host Servers

You should consider relying on the various virtual networks supported by Hyper-V to segregate traffic between machines. Remember that Hyper-V supports four different virtual network types: public, internal, dedicated, and private. By linking your virtual machines to each different network type, you can further protect them from attack (see Figure 8-24).

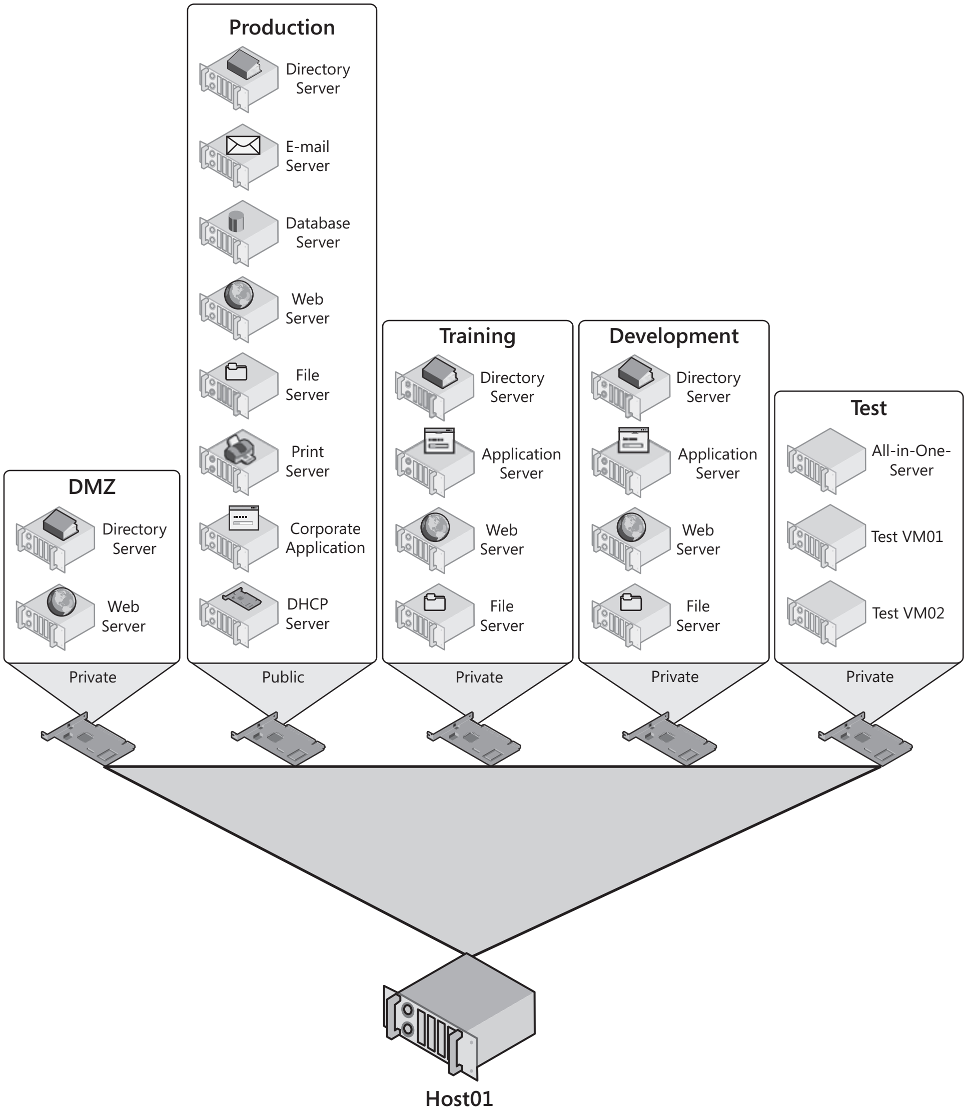


FIGURE 8-24 Controlling VM connectivity through Hyper-V virtual networks

You can also use *multi-homing*—the inclusion of multiple virtual adapters in a VM, with each adapter linked to a separate network—to further reduce VM access to public networks (see Figure 8-25). For example, you might prepare a perimeter network and link each machine—authentication server, Web Server, management systems, and so on—to a private network. Then you multi-home the Web server or any server that needs to interact directly with the public to a public, external network. This lets Internet users access the Web server, but all other perimeter communications are handled over the private network and are more secure because they are not exposed to other networks.

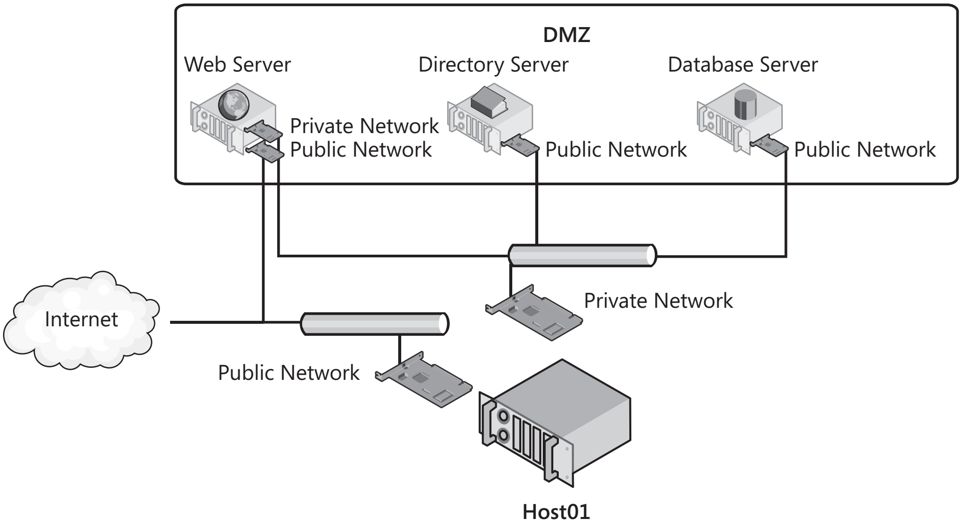


FIGURE 8-25 Creating a perimeter network in a virtual environment

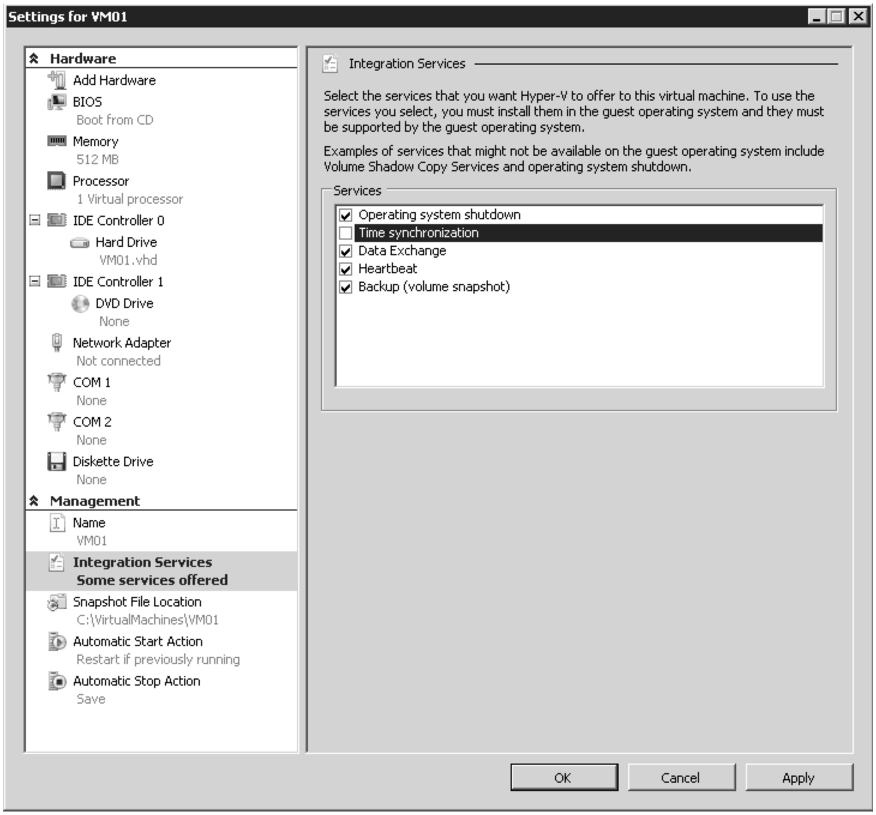
Be creative when you position virtual machines on your servers. After all, you want to maximize virtual machine density on your host servers to minimize the number of hosts you require. However, always make sure that VMs that are of a different level of sensitivity are isolated from each other. This can only be done by managing and assigning Hyper-V's virtual networks.

Managing Time Synchronization in VMs

When you run enlightened guest operating systems in your virtual machines, you run virtual machines that can take full advantage of Hyper-V's Integration Services. One of these services is time synchronization. As you know, time synchronization is an essential part of any modern network and is crucial when working with Active Directory forests and domains. By default, machines that are members of Active Directory domains will connect to the PDC Emulator master of operations—a special domain controller role designed to manage time in AD DS networks—to synchronize their clocks. This ensures that all machines in the domain use the same time source. Proper time synchronization is essential if you want Kerberos authentication to work properly. Any machine that is out of time synch with a domain controller cannot log on, nor can users on that machine log on.

However, when you work with directories in a virtualized environment, your machines can obtain time synchronization from two sources: the host server in Hyper-V and the PDC Emulator in the network. If someone compromises the time on a host server, all of the VMs on the server will be unable to log on. Therefore, you should carefully consider where you want your VMs to obtain their time. The best policy is as follows:

- Turn off host time synchronization on each virtual machine in a production domain. This is done in the VM's settings under Integration Services. Simply clear the Time Synchronization check box (see Figure 8-26).



Hardware

- Add Hardware
- BIOS
  Boot from CD
- Memory
  512 MB
- Processor
  1 Virtual processor
- IDE Controller 0
  - Hard Drive
    VM01.vhd
- IDE Controller 1
  - DVD Drive
    None
- Network Adapter
  Not connected
- COM 1
  None
- COM 2
  None
- Diskette Drive
  None

Management

- Name
  VM01
- **Integration Services**
  Some services offered
- Snapshot File Location
  C:\VirtualMachines\VM01
- Automatic Start Action
  Restart if previously running
- Automatic Stop Action
  Save

Integration Services

Select the services that you want Hyper-V to offer to this virtual machine. To use the services you select, you must install them in the guest operating system and they must be supported by the guest operating system.

Examples of services that might not be available on the guest operating system include Volume Shadow Copy Services and operating system shutdown.

Services

☑ Operating system shutdown
☐ Time synchronization
☑ Data Exchange
☑ Heartbeat
☑ Backup (volume snapshot)

FIGURE 8-26 Setting time synchronization settings for a VM

- Use appropriate policies to have all member machines synchronize with the PDC Emulator for the domain. This is automatic when a machine joins a domain. If the domain is at the bottom of a forest hierarchy, its PDC Emulator will automatically connect with the PDC Emulator of its parent domain, the PDC Emulator for the parent domain will connect to its parent domain, and so on until you get to the root domain.
- Root domain PDC Emulators should use the network time protocol to connect to a proper external time source. If you prefer to avoid this, change the properties for the VM that runs the PDC Emulator role in the root domain and have it synchronize time with its host server.

Now you will have a single VM that synchronizes with the host server and all VMs will synchronize with this VM. Make sure you protect the host server that runs this very important virtual machine.

Note that time synchronization is less important on other virtual machine networks such as training, testing, and development environments. Use your discretion to configure it for these networks.

Updating Offline VMs

As mentioned earlier, it is very easy for administrators of hundreds of virtual machines—especially virtual machines that are at rest—to let them fall out of synch with software updates. Few organizations take the time to manually start each VM once a month, update it, reboot it as required, and then store it again. This is why Microsoft has developed the Offline Virtual Machine Servicing Tool (OVMST). This tool is designed to automatically update all VMs whether they are on or off. The OVMST is a solution accelerator and, like all solution accelerators, it includes both guidance and some utilities. To be able to use this tool, you must have the proper infrastructure in place:

- The downloaded OVMST, which can be found at *http://technet.microsoft.com/en-us/library/cc501231.aspx*.
- System Center Virtual Machine Manager. Either version 2007 or 2008 will work.
- Windows Server Update Services version 3.0 or 3.0 SP1 or System Center Configuration Manager 2007 SP1 or 2007 R2.

The last requirement is for an internal update delivery mechanism, which can either be WSUS or SCCM. At least one of the two is required. The process for applying updates is relatively straightforward. All operations are based on resources being stored within SCVMM Libraries.

Because the update process can require extensive resources, you should use a maintenance host dedicated to the OVMST updating process for stored resources and for staging VMs before you deploy them in the production environment. Note that this host—or at least the machine running the OVMST—must use a full installation of Windows Server 2008 because the OVMST relies on the .NET Framework and Windows PowerShell to operate.

Basically, the OVMST performs the following operations (see Figure 8-27):

1. A servicing job is created within the Windows Task Scheduler. This job can be set to start once per month—for example, after the second Tuesday of each month.
2. The servicing job relies on logic from the Windows Workflow Foundation—part of the .NET Framework—to launch Windows PowerShell operations on each stored virtual machine.
3. For each machine, the servicing job performs the following tasks:
   a. Deploys the “at rest” VM from the SCVMM Library to a servicing host.
   b. Wakes the virtual machine by turning it on or restoring it from a saved state. This VM is woken on an isolated network to ensure that it does not conflict with existing VMs that have the same name. Note that the isolated network must be prepared beforehand on your servicing host.
   c. Launches the update cycle using the technology you have in place (either WSUS or SCCM).
   d. Reboots the VM as required to complete the update process.
   e. Returns the VM to its original state—off or saved.
   f. Returns the VM to the Library.
   g. Proceeds to the next at -rest VM.

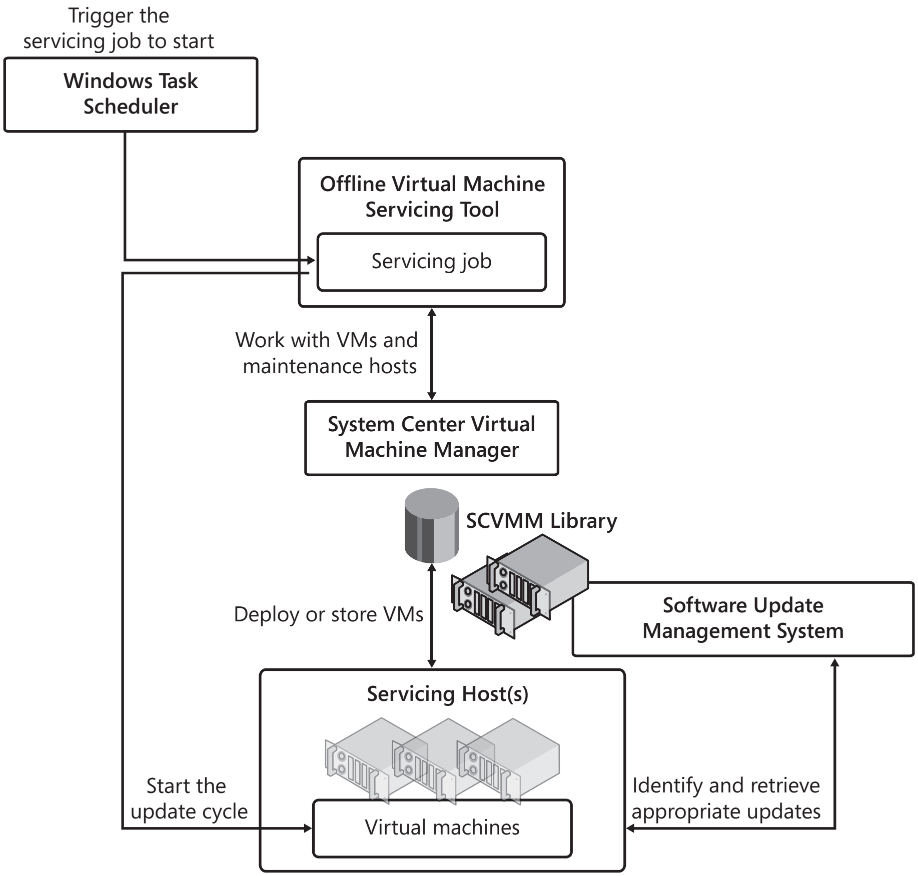

Trigger the servicing job to start
Windows Task Scheduler
Offline Virtual Machine Servicing Tool
Servicing job
Work with VMs and maintenance hosts
System Center Virtual Machine Manager
SCVMM Library
Deploy or store VMs
Software Update Management System
Servicing Host(s)
Start the update cycle
Virtual machines
Identify and retrieve appropriate updates

FIGURE 8-27 The OVMST update process

If you have a large VM environment and have several VMs that are continuously at rest, you should look into the OVMST and deploy it in your network. Organizations with such a need should find it relatively easy to have one or more hosts dedicated to the servicing role because updating VMs is such an important task.

PRACTICE Delegating Administrative Roles in SCVMM

In this practice, you will work with SCVMM to create delegated administration roles and then view the results. This practice consists of three exercises. In the first exercise, you will create a new account that will be a delegated administrator. This is performed in Active Directory Users And Computers. In the second exercise, you will create the delegation role. In the third exercise, you will log on as the delegated user to view the results of a role delegation in SCVMM. Perform these exercises first on Server01 and then in SCVMM01. Log on with domain administrator credentials to begin the exercise.

EXERCISE 1 Create a Delegated User

In this exercise you will use Server01 to create a new user in the Contoso directory. Perform this exercise with domain administrator credentials.

1. Log on to Server01 with domain administrator credentials. Launch the Active Directory Users And Computers (ADUC) console through the Start menu and Administrative Tools. Alternatively, you can use the ADUC portion of the Server Manager console.
2. Create the new user account. You should normally place the user in a proper OU, but for the purpose of this exercise, you will place it in the Users container. Right-click Users, select New, and then select User. Name the user **Terry Adams** with a logon name of **Terry.Adams** and click Next. Assign a complex password to the account, clear the User Must Change Password At Next Logon check box, and select Password Never Expires. The last selection ensures that you do not need to worry about password changes while studying for the exam. Click Next and then click Finish. The account is created.
3. Create a new top-level OU called RBAC Assignments. Right-click the Contoso.com domain name, select New, select Organizational Unit, type **RBAC Assignments**, and click OK. This creates the OU and moves you into it.
4. Create the required security group. You create a group to simplify long-term delegation management. If you ever need to assign these rights to another user, all you need to do is add them to the group. Right-click the RBAC Assignments OU to select New, and then Group. Name the group **Library Administrators**, make sure it is a Global Security group, and click OK. You would normally create as many groups as you intend to have roles. Remember, however, to keep the structure as simple as your organizational policies allow.
5. Add the Terry Adams account to the Library Administrators group. Right-click the new group, select Properties, click the Members tab, click Add, type **Terry Adams**, and click Check Names. Click OK twice when done. Close ADUC.

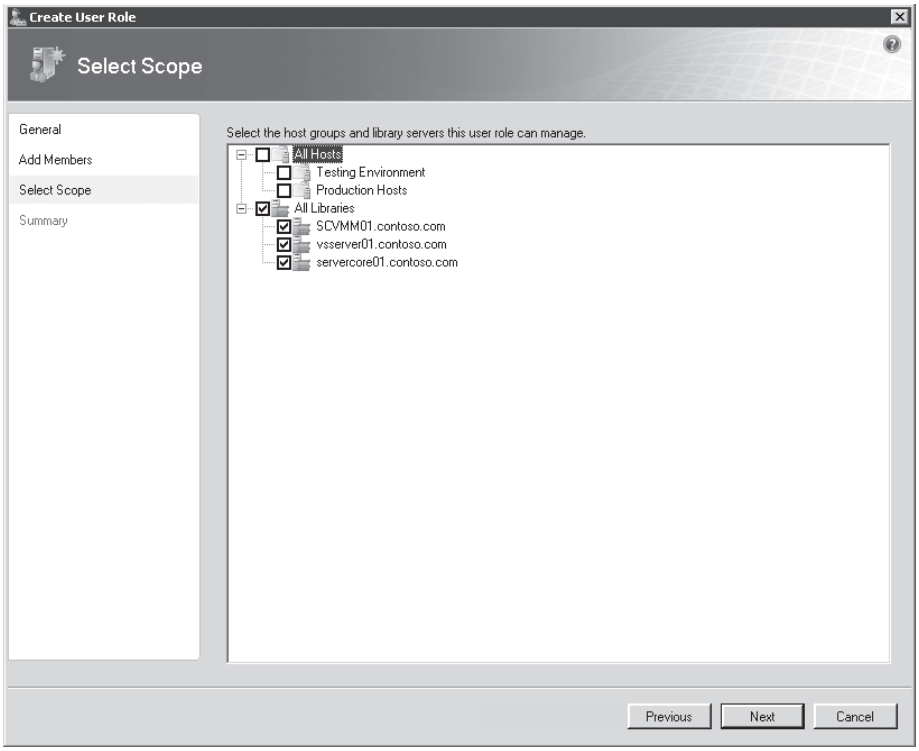
Your directory is ready to support role delegation in SCVMM.

EXERCISE 2 Create a Role Delegation in SCVMM

In this exercise you will create a role delegation in SCVMM. Perform this exercise on SCVMM01 and log on with domain administrator credentials.

1. Log on to SCVMM. Launch the SCVMM Administrator Console. You can double-click the shortcut on the desktop or use Start, then All Programs, then Microsoft System Center, and then Virtual Machine Manager 2008 to click the Virtual Machine Manager Administrator Console shortcut.
2. Move to the Administration View and click User Roles. Two roles should appear: Administrator under the Administrator profile type and Testers under the Self-Service User profile type.

3. Click New User Role in the Actions pane. This launches the Create User Role Wizard. Type **Library Administrators**, type a short description, and select Delegated Administrator from the drop-down list under User Role Profile. Click Next.
4. Click Add, type **Library**, and click Check Names and then OK. Click Next.
5. On the Select Scope page, select All Libraries and click Next (see Figure 8-28). As you can see, this page lets you determine the scope of delegation. By selecting All Libraries, you grant access to Library Stores only. Click Create to generate the new role.



Select the host groups and library servers this user role can manage.

- □ All Hosts
  - □ Testing Environment
  - □ Production Hosts
- ☑ All Libraries
  - ☑ SCVMM01.contoso.com
  - ☑ vsserver01.contoso.com
  - ☑ servercore01.contoso.com

FIGURE 8-28 Selecting the scope of delegation

Your new role has been created and is now available in SCVMM. Now make sure the Library Administrators can log on to the remote server.

1. Return to Server Manager, which should be open in the Task Bar.
2. Click Server Manager (SCVMM01) to view the Server Manager Home Page.
3. Click Configure Remote Desktop and then click Select Users.
4. Click Add, type **Library**, click Check Names, and then click OK three times.

Your computer is ready for delegation.

EXERCISE 3 View the Results of a Role Delegation

In this exercise you will log on as a delegated administrator and view the access this grants you. Perform this exercise on SCVMM01 and log on with the Terry Adams account.

1. Log on to SCVMM01 with the Terry Adams account. Launch the SCVMM Administrator Console. You can double-click the shortcut on the desktop or click Start, click All Programs, click Microsoft System Center, click Virtual Machine Manager 2008, and then click the Virtual Machine Manager Administrator Console shortcut. This opens the Connect To Server window.
2. Localhost:8100 is already listed and Make This Server My Default is selected. Click Connect.
3. The console opens in the Overview and is focused on the Hosts view. Note that you do not see any hosts, but you have full access to the Libraries (see Figure 8-29).

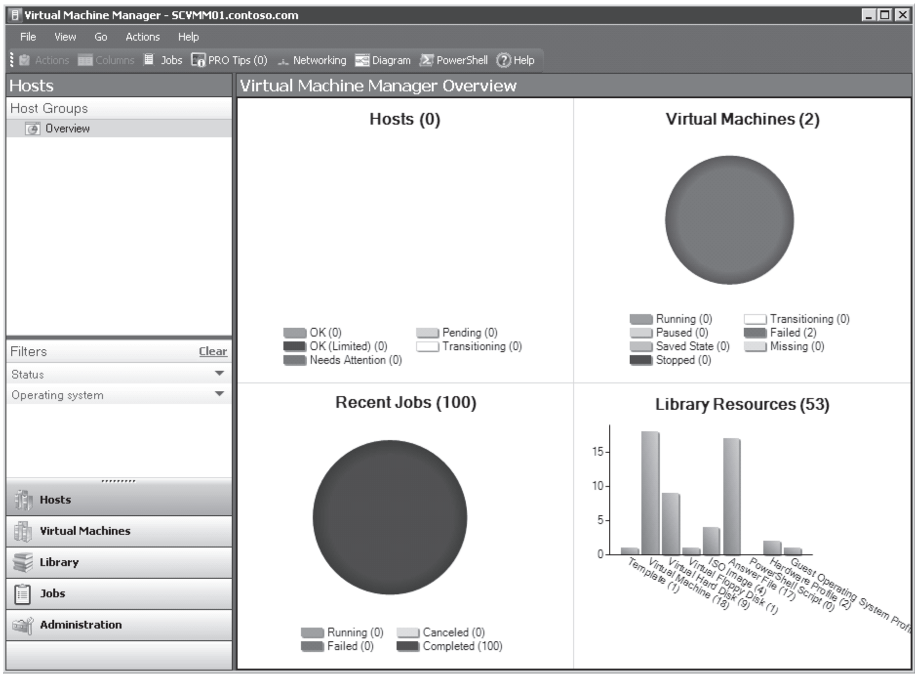
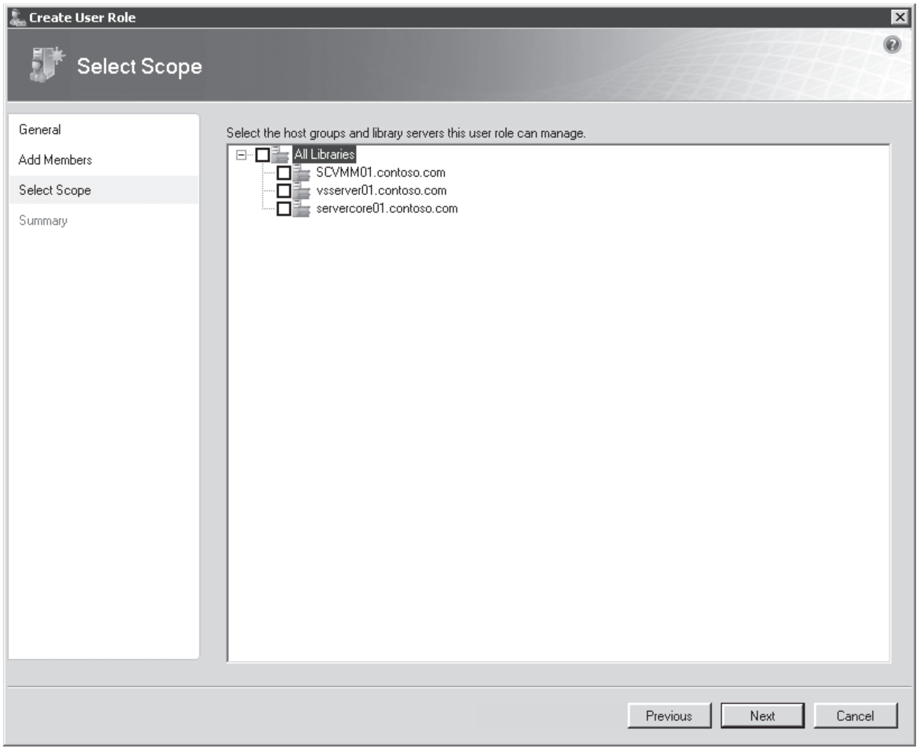


FIGURE 8-29 Viewing a delegated console

4. Change to Virtual Machines view. Notice that you do not have access to this view, either. However, when you change to Library View, you'll notice that you have full access to all Library resources. You can manage resources, deploy VMs, and perform any task that is tied to an SCVMM Library.

5. Change to Administration view. Notice that you have access to some items in Administration view—even the ability to create new user roles. However, if you create a new delegated administration user role, you will find that the only thing you can delegate is Libraries (see Figure 8-30). Explore the console thoroughly to view what can be done as a Library—only administrator.



Select the host groups and library servers this user role can manage.

- □ All Libraries
  - □ SCVMM01.contoso.com
  - □ vsserver01.contoso.com
  - □ servercore01.contoso.com

FIGURE 8-30 Delegated administrators only have control over their own delegation scope.

Log off when your tour is complete.

✓ Quick Check

1. When can you use Authorization Manager (AzMan)?
2. What are the three main roles that can be defined within SCVMM?
3. What is the required infrastructure to put OVMST in place?

Quick Check Answers

1. AzMan is only available on full installations of Windows Server 2008 and is launched by typing **AzMan.msc** at the prompt in the Start menu.
2. The three main roles in SCVMM are:
   - Full resource pool administrator The default administrator role in SCVMM.
   - Delegated administrator Supports the delegation of host groups and/or libraries.
   - Virtual machine user A role defined by the Self-Service Portal.
3. The requirements for the OVMST are:
   - The tool itself, which must be downloaded
   - SCVMM 2007 or 2008
   - Windows Server Update Services version 3.0 or 3.0 SP1 or System Center Configuration Manager
   - Optionally, a dedicated servicing host

Case Scenario: Planning a Resource Pool Security Strategy

In the following case scenarios, you will apply what you've learned about securing hosts and virtual machines. You can find answers to these questions in the "Answers" section on the companion CD which accompanies this book.

You are the resource pool administrator for Lucerne Publishing. The Lucerne resource pool contains 12 main VMs in production running on 3 hosts. All hosts are managed with SCVMM and all hosts are running Hyper-V only. One new host has been brought in to support better levels of high availability in your machines. Lucerne also runs test and development environments on machines in other host groups.

Recently, one of your IT managers assisted a presentation on virtualization. The speaker talked a lot about security and the potential threats organizations face when working with virtual machines in production. Now the manager is all fired up and wants some answers to some tough questions. He has downloaded the *Hyper-V Security Guide* and is asking what kind of security has been implemented in your resource pool. He insists that it is necessary to document the security practices you put in place in the resource pool. Specifically, the manager wants answers to the following questions:

1. How is the resource pool configured and which components are running in it?
2. How do the resource pool components interact with each other?
3. How are the virtual machines running on the resource pool secured?

Suggested Practices

To help you successfully master the exam objectives presented in this chapter, complete the following tasks.

Hyper-V Security

- **Practice 1** Take the time to work with the various virtual network adapters available in Hyper-V. Connect different virtual machines to each adapter type in an effort to isolate their network traffic. This will be useful practice for the exam.
- **Practice 2** Take the time to create new folders for the storage of virtual machine files. Take a close look at the access control lists that must be enabled to support moving these storage locations from their defaults. One good way to do this is to examine the security properties of the default locations.

Hyper-V Role Delegation

- **Practice 1** Play with the various roles you can generate for Hyper-V role delegation with Authorization Manager. Rely on the InitialStore.xml file to begin this practice and save your changes. Copy the updated stores to other servers to load them and then log on with different accounts to test the access you have granted.
- **Practice 2** Play with the various roles you can generate for SCVMM role delegation with the Administrator Console. Then log on with different accounts to test the access you have granted.

Chapter Summary

- Virtual environments need a different security approach. When you are running host servers and virtual machines that rely on the same operating system, you need to segregate the security context of the resource pool from the virtual environment.
- It is important to maintain the integrity of the installed files, installed services, and firewall rules of the Windows Server 2008 installation when adding the Hyper-V role for the security implementation.
- The Security Configuration Wizard in Windows Server 2008 generates security profiles based on the role of a server within the network and allows you to configure service configurations through predefined, role-based configurations; network security; and registry settings; as well as implement an audit policy.
- Windows Vista added a new capability for the Windows operating system—being able to configure removable device controls through the use of Group Policy. This is done through the control of device installations. To increase the security context in the resource pool, this GPO should be applied on both servers and PCs so that no unauthorized user can connect a USB drive.
- BitLocker Full Drive Encryption allows you to encrypt the contents of the operating system volume and is often used for mobile systems, but can be also used to protect server drives.
- To be able to audit an object you need to enable the auditing policy within a Group Policy object, and you must turn on auditing for the object itself.
- In a distributed management resource pool, you rely on Authorization Manager to manage Hyper-V hosts. In a centrally managed resource pool, you rely on a host server and virtual machine management tool—for example SCVMM—to assign least-privilege access rights.

- The Hyper-V authorization stores are made up of four components: store scope, store tasks, store roles, and assigned users or groups. AzMan can operate in Administrator mode to modify an existing policy and in Developer mode to create new policies and to modify the structure of an existing policy.
- Virtual Service Offering's scope of protection depends on the size of the organization. You should rely on the various virtual networks supported by Hyper-V to segregate traffic between virtual machines of different sensitivity.
- Time synchronization in virtual machines is very important when working in Active Directory forests and domains, and is also essential if you want Kerberos authentication to work properly.
- The Offline Virtual Machine Servicing Tool (OVMST) is designed to automatically update all virtual machines whether they are on or off.

Index

About the Authors

DANIELLE RUEST is an IT professional focused on technology futures. She is passionate about virtualization technologies and has been working in this field for over 10 of her more than 20 years of IT experience. Her customers include governments and private enterprises of all sizes. She has been instrumental in supporting virtualization deployments in environments that range from test and development to production systems with a wide range of clients.

NELSON RUEST is an IT professional focused on the technology futures. He is passionate about continuous service delivery and has been supporting clients in this field for more than 20 years. His customers also include organizations of all sizes. He has been instrumental in supporting deployments of virtualization and continuous service infrastructures in a wide variety of different client environments.

In 2007 and 2008, Danielle and Nelson toured the United States to talk about all levels of virtualization with thousands of people. Discussions with session attendees led Danielle and Nelson to understand that no matter what level of sophistication people think they have in terms of virtualization, there is always a topic with which people in general are not familiar.

Together they have coauthored a wide variety of books, including *Virtualization, a Beginner's Guide* and *Windows Server 2008, The Complete Reference* for McGraw-Hill Osborne as well as *MCTS Self-Paced Training Kit (Exam 70-238): Deploying Messaging Solutions with Microsoft Exchange Server 2007* and *MCTS Self-Paced Training Kit (Exam 70-640): Configuring Windows Server 2008 Active Directory* for Microsoft Press. Danielle and Nelson are also freelance writers for several IT publications, produce white papers for various vendors (*http://www.reso-net.com/articles.asp?m=8*), and deliver Webcasts and conferences (*http://www.reso-net.com/presentation.asp?m=7*).

Danielle and Nelson work for Resolutions Enterprises Ltd., a consulting firm focused on IT infrastructure design and optimization. Resolutions can be found at *http://www.Reso-Net.com.*