

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

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

Copyright © 2009 by Nelson Ruest, Danielle Ruest, and GrandMasters

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

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.

Microsoft, Microsoft Press, Active Directory, ActiveX, Authenticode, BitLocker, BizTalk, Excel, Expression, Forefront, Groove, Hyper-V, Internet Explorer, MS, MSDN, MS-DOS, Natural, Outlook, PerformancePoint, SharePoint, SQL Server, Visio, Visual Basic, Visual C++, Visual Studio, Windows, Windows Live, Windows Media, Windows Mobile, Windows NT, Windows PowerShell, Windows Server, Windows Server System and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

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 Buik; 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.aspx>.

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

Introduction	xiii
Chapter 1 Implementing Microsoft Hyper-V	1
Before You Begin	2
Lesson 1: Planning for Microsoft Windows Server 2008 Hyper-V	3
Virtualization Technologies in the Datacenter	3
Software vs. Hardware Virtualization	7
Exploring Windows Server 2008 Hyper-V	10
Exploring Microsoft Hyper-V Server 2008	12
Understanding Hyper-V Features	13
Understanding the Hyper-V Architecture	16
Lesson 2: Evaluating Your Environment	25
Preparing to Deploy Hyper-V	25
Inventorying Your Existing Environment	27
Using the Microsoft Assessment and Planning Tool	29
Lesson 3: Implementing Windows Server 2008 for Hyper-V	40
Selecting the Right Hardware for Hyper-V	40
Installing Windows Server 2008	47
Case Scenario: Preparing for Server Virtualization	55
Suggested Practices	56
Windows Server 2008 Installation	56
Microsoft Assessment and Planning Tool	56
Server Hardware Configurations	56
Chapter Summary	57

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/

Chapter 2	Configuring Hyper-V Hosts	59
Before You Begin.		60
Lesson 1: Installing the Hyper-V Role		61
Performing the Initial Server Configuration		61
Performing the Hyper-V Role Installation		72
Installing Hyper-V Updates		79
Hyper-V and Active Directory Domain Services		80
Installing Windows Hyper-V Server		81
Lesson 2: Configuring Windows Server Hyper-V.		91
Working with the Hyper-V Management Tools		91
Understanding Hyper-V Settings		93
Lesson 3: Configuring Virtual Networking		104
Working with Virtual Network Types in Hyper-V		104
Configuring Hyper-V on Full vs. Server Core Installations		107
Using the Virtual Network Manager Tool		111
Case Scenario: Networking Virtual Machines		117
Suggested Practices		117
Windows Server 2008 Configuration		117
Hyper-V Role Installation		118
Virtual Network Configuration		118
Chapter Summary.		118
 Chapter 3	 Completing Resource Pool Configurations	 121
Before You Begin.		122
Lesson 1: Configuring Hyper-V High Availability		123
Understanding Failover Clustering		123
Creating a Hyper-V Two-Node Cluster		132
Lesson 2: Working with Hyper-V Host Remote Administration		148
Deploying Hyper-V Manager		148
Deploying the Failover Cluster Management Console		152
Understanding System Center Virtual Machine Manager		154
Preparing for SCVMM Implementation		168

Chapter 5 Automating Virtual Machine Creation	267
Before You Begin.	268
Lesson 1: Exploring System Center Virtual Machine Manager	269
Working with Hyper-V Through SCVMM	269
Managing the SCVMM Library	284
Working with SCVMM Add-Ons	289
Installing WDS	291
Working with WDS	292
Lesson 2: Automating Virtual Machine Creation.	304
Manually Creating a Duplicate Virtual Machine	304
Creating and Managing VMs with SCVMM	310
Managing the VMM Self-Service Portal	315
Case Scenario: Provisioning Virtual Machines	325
Suggested Practices	325
Working with SCVMM	325
Working with VMs with SCVMM	325
Working with the SCVMM Self-Service Portal	326
Chapter Summary.	326
 Chapter 6 Migrating to Hyper-V	 329
Before You Begin.	329
Lesson 1: Working with Migration Scenarios	330
Understanding Hyper-V Migration Scenarios	330
Installing Additional Components in Support of Migrations	340
Performing Source-to-Target Conversions	355
Case Scenarios.	379
Case Scenario: Moving from Physical to Virtual Machines	379
Suggested Practices	380
Preparing for Migrations	380
Performing Migrations	381
Chapter Summary List	381

Chapter 7 Automating VM Management with Windows PowerShell	383
Before You Begin.	384
Lesson 1: Automating Hyper-V Operations with Windows PowerShell.	385
Understanding Windows PowerShell	385
Managing Hyper-V Operations with Windows PowerShell	402
Using Windows PowerShell with SCVMM	409
Case Scenario: Automating Hyper-V Operations	429
Suggested Practices	429
Automating Hyper-V Tasks	429
Chapter Summary.	430
 Chapter 8 Securing Hosts and Virtual Machines	 431
Before You Begin.	434
Lesson 1: Securing the Resource Pool.	435
Securing Hyper-V Resource Pools	435
Lesson 2: Securing the Virtual Environment.	471
Preparing Hyper-V Management Roles	471
Securing Hyper-V VMs	488
Populating Virtual Machines on Host Servers	491
Case Scenario: Planning a Resource Pool Security Strategy	502
Suggested Practices	502
Hyper-V Security	502
Hyper-V Role Delegation	503
Chapter Summary.	503
 Chapter 9 Protecting Hyper-V Resource Pools	 505
Before You Begin.	507
Lesson 1: Protecting Your Resource Pools	508
Understanding Hyper-V Host Protection Strategies	508

Understanding Virtual Machine Protection Strategies	510
Working with Windows Server Backup	516
Working with System Center Data Protection Manager	529
Case Scenario: Dealing with a Host Server Failure	547
Suggested Practices	547
Windows Server Backup	548
System Center Data Protection Manager	548
Chapter Summary	548
Chapter 10 Configuring Virtual Machine High Availability	549
Before You Begin.	552
Lesson 1: Working with VM High Availability	553
Understanding Virtual Machine High Availability	553
Creating Supported VM Configurations	575
Case Scenario: Protecting Exchange 2007 VMs.	585
Suggested Practices	585
Guest Failover Clusters	586
Guest NLB Clusters	586
Supported VM Configurations	586
Chapter Summary	586
 <i>Glossary</i>	 589
<i>Index</i>	593

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://go.microsoft.com/fwlink/?LinkID=132136>.
Microsoft Baseline Configuration Analyzer (MBCASetup64.msi)
<http://go.microsoft.com/fwlink/?LinkID=97952>.
- 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://go.microsoft.com/fwlink/?LinkId=82105>.
- 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://go.microsoft.com/fwlink/?LinkID=113199>
<http://go.microsoft.com/fwlink/?LinkId=128540>.
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://go.microsoft.com/fwlink/?LinkID=120135>.
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.msp>.

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>.

Implementing Microsoft Hyper-V

With the release of Microsoft Windows Server 2008 Hyper-V, Microsoft joins the select group of manufacturers that provide a hardware-based *hypervisor*, or an engine that is designed to expose hardware resources to virtualized guest operating systems (OS). Hypervisors are transforming the way IT professionals interact with server workloads. When you use a hypervisor to support the operation of virtual workloads in production datacenters, physical servers are converted to resource pools that fulfill a single function: provide resources such as CPU cores, random access memory (RAM), network interface cards (NICs), and storage in support of the operation of the virtual workloads. This means that a new breed of IT professional is required: the resource pool administrator.

Resource pool administrators manage all of the hardware that is required to maintain and support virtual workloads or virtual service offerings—the networked services that were traditionally run on hardware but are now virtualized. Virtualizing workloads allows organizations to make more effective use of hardware. After organizations the world over discovered that they were running workloads on physical servers with less than 15 percent utilization, they began turning to virtualization to increase the utilization levels of their physical servers to 80 percent or more. A physical server running multiple virtual workloads—usually 10 or more virtual workloads per physical server—provides a more efficient utilization model and therefore provides support for the concept of a greener datacenter.

Hypervisor servers run workloads inside virtual machines—operating system instances that share hardware resources. These operating systems are x86-based and can run Windows or Linux in both 32-bit and 64-bit versions. Hypervisors do not support the operation of non-x86-based operating systems such as operating systems designed for Itanium processors. These virtual machines are used to run the traditional networked services organizations rely on to run their businesses. IT professionals continue to manage these workloads in the same way they always have—a virtual machine can behave and interact with the outside world in exactly the same way as a physical machine. However, physical server management has changed.

This new operational model relegates server hardware to the same level as other hardware devices such as routers, switches, and storage containers. Servers are resources that are pooled together into highly available clusters that ensure that the virtual machines running end user-facing workloads are always available. The resource pool administrator

is responsible for the creation, configuration, deployment, and management of physical servers in the datacenter and, possibly, in remote sites. Servers must be sized appropriately to manage multiple virtual machines. They must also rely on shared storage to create the failover clusters that render the Hyper-V service highly available. The resource pool administrator is also responsible for the transformation process used to convert physical workloads to virtual machines. After the virtual machines are created, the resource pool administrator will be responsible for their administration and management.

With this in mind, this chapter begins the exploration of the responsibilities of resource pool administrators. It delves into the Hyper-V feature set, its requirements, and its constraints. It also looks at how organizations will move to the virtualized datacenter. It examines the process that determines how physical or host servers should be sized and it covers the various approaches organizations will use to implement Hyper-V in their own networks.

Exam objectives in this chapter:

- Select and configure hardware to meet Hyper-V prerequisites.
- Configure Windows Server 2008 for Hyper-V.

Before You Begin

To complete this chapter, you must have:

- Experience with Windows Server 2003 and or Windows Server 2008.
- Experience with some form of guest operating system virtualization.
- Ideally, you will have access to a setup as described in the Introduction. If not, your experience with Hyper-V will be limited.
- Access to an existing legacy network of traditional physical services.

Lesson 1: Planning for Microsoft Windows Server 2008 Hyper-V

When you prepare to work with Microsoft Windows Server 2008 Hyper-V, you need to begin by gaining an understanding of several key concepts.

After this lesson, you will understand:

- The different layers of virtualization that can be addressed in the datacenter.
- The difference between hardware and software virtualization.
- The difference Windows Server 2008 Hyper-V and Windows Hyper-V Server.
- The Hyper-V feature set.
- The Hyper-V architecture.

Estimated lesson time: 20 minutes

Virtualization Technologies in the Datacenter

Virtualization is the means by which you can isolate one computing resource from another. In a traditional software stack, each resource is linked with the other. For example, a traditional application usually runs on specific hardware, physically tying the application to the resources that make it operate. Network resources are tied to specific locations; storage is tied to specific containers; operating systems are assigned to specific hardware; network interfaces are bound to specific processes; and applications are installed on specific hardware and run on a specific operating system.

When you virtualize various components in the datacenter, you release them from these traditional bindings (see Figure 1-1). Because of this, virtualized components often result in more efficient resource utilization, provide greater flexibility of operation, and simplify change management:

- You can virtualize networks to localize dispersed resources.
- You can virtualize storage to bring together various distributed containers into one single view.
- You can virtualize machines to run any operating system.
- You can virtualize presentation services to provide access to them from any connected location.
- You can virtualize applications to support computing on demand models.
- You can virtualize user profiles to give them access to their data from any location.

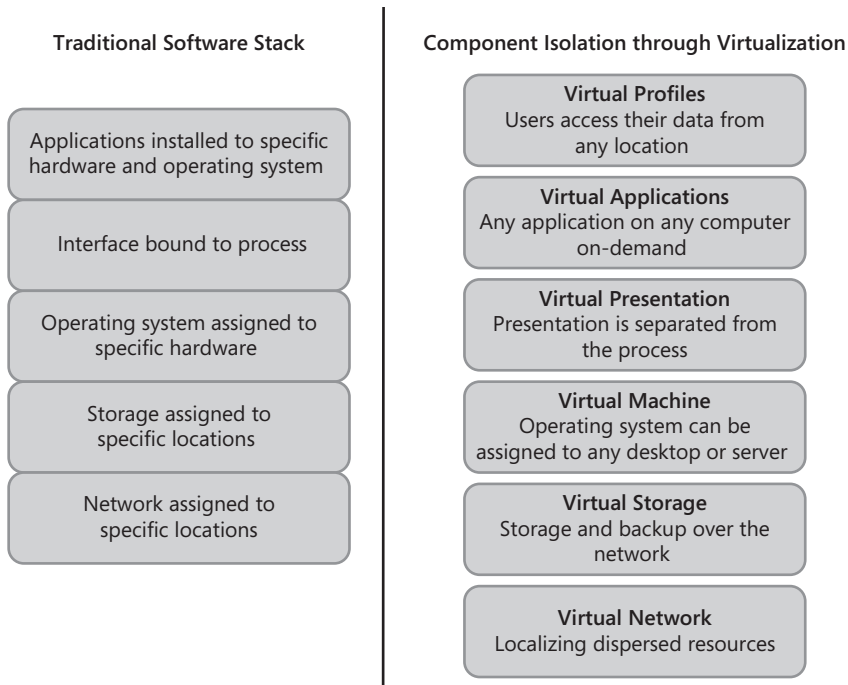


FIGURE 1-1 Virtualization transforms the traditional software stack by releasing it from its boundaries.

These various layers of virtualization can work together to create a completely dynamic datacenter—one where IT can respond rapidly and efficiently to the changing needs of the organization it supports.

NOTE LEARN MORE ABOUT THE DIFFERENT LAYERS OF VIRTUALIZATION

To learn more about the different layers of virtualization and how they should be implemented in datacenters of all sizes, look up the Microsoft Operations Framework (MOF) Virtualization Process Companion Guide at <https://connect.microsoft.com/InvitationUse.aspx?ProgramID=1880&InvitationID=MOFP-4JBP-P6C9&SiteID=14>. To learn more about virtualization in general and how the different layers of virtualization interact with each other, see *Virtualization, A Beginner's Guide* by Ruest and Ruest at <http://www.mhprofessional.com/product.php?isbn=007161401X>.

Microsoft products are designed to work together to provide support for each layer of the virtualization stack (see Figure 1-2). In fact, Microsoft provides a complete stack of products in support of virtualization in datacenters of all sizes. Table 1-1 outlines each product and its target virtualization layer.

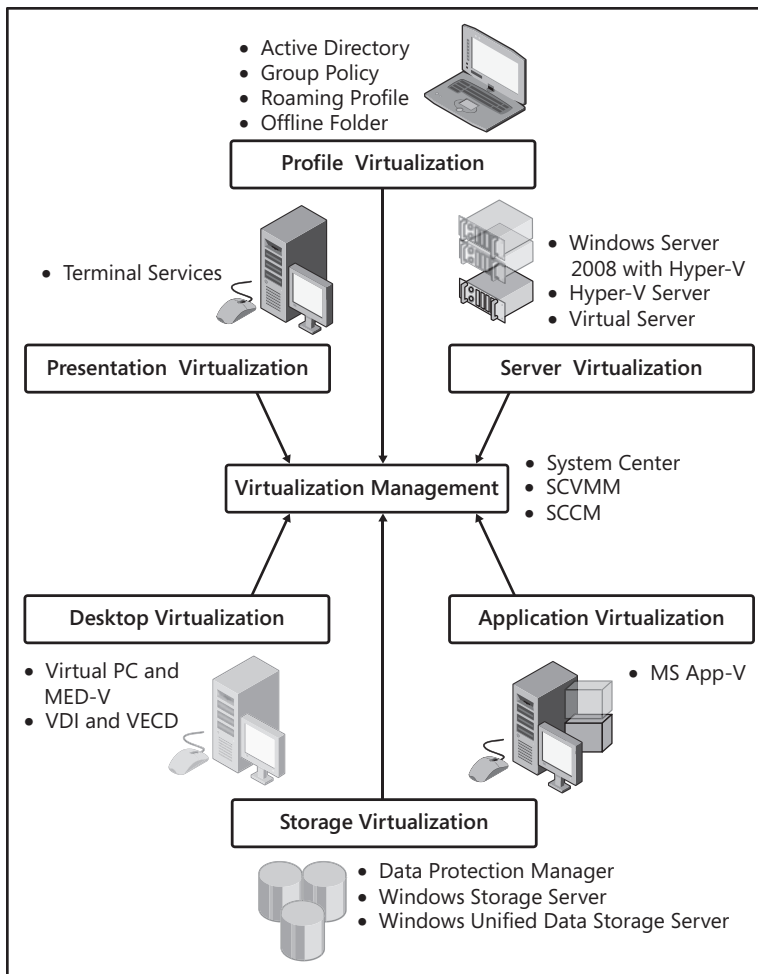


FIGURE 1-2 Microsoft's virtualization software stack

TABLE 1-1 Microsoft's Virtualization Software Stack

PRODUCT	PURPOSE
Windows Server 2008	Supports the Hyper-V role. Supports traditional network workloads in virtual machines. Supports virtual networking.
Windows Storage Server	Supports network-attached storage (NAS).
Windows Unified Data Storage Server	Supports NAS. Acts as a front end for storage area networks. Supports virtual hard disks (VHDs) as iSCSI targets.

PRODUCT	PURPOSE
System Center Data Protection Manager	Provides disk-to-disk backups. Provides remote-site backups. Backs up physical and virtual machines.
Windows Hyper-V Server	A free download that supports the Hyper-V role in a stand-alone configuration only.
Microsoft Virtual Server	Supports server-based virtual machine operation but requires an existing operating system.
Virtual PC	Supports desktop-based virtual machine operation but requires an existing operating system.
Microsoft Enterprise Desktop Virtualization (MED-V)	Supports centralized virtual machine image management. Supports virtual machine life-cycle management. Supports the application of usage policies for desktop virtual machines as well as data control policies. Publishes applications inside virtual machines seamlessly to the user's desktop. Requires Virtual PC to run.
Virtual Desktop Infrastructure (VDI) and Vista Enterprise Centralized Desktop (VECD)	Runs end-user desktops in centralized virtual machines using the Hyper-V server-based virtual machine engine. Relies on VECD for Windows Vista or downgraded operating system licensing of centralized desktop virtual machines.
Windows Server 2008 Terminal Services	Provides next-generation presentation virtualization services through server-based computing.
Microsoft Application Virtualization (App-V)	Supports application virtualization, transforming applications into centrally managed virtual services that are never installed and don't conflict with other applications. Supports application streaming and local application caching as a delivery mechanism.
Windows Server 2008 with Active Directory	Supports profile virtualization through a combination of Group Policy Objects (GPOs) running Folder Redirection and the Roaming Profile.
System Center Virtual Machine Manager	Supports centralized management of server-based virtual machine engines such as Hyper-V and Virtual Server. Supports virtual machine libraries. Provides self-service virtual machine provisioning. Provides physical-to-virtual and virtual-to-virtual machine conversion.

PRODUCT	PURPOSE
System Center Operations Manager	Supports monitoring and proactive rehabilitation of both physical and virtual machines.
System Center Configuration Manager	Supports inventorying and configuration management for both physical and virtual machines. Supports virtualized application deployment.

The products listed in Table 1-1 list the entire software stack Microsoft provides in support of virtualization. However, the virtualization industry moves at such a pace that it is very likely that new products will be made available by the time you read this. In fact, IDC, an international research firm, estimates that only 17 percent of the worldwide server market will be virtualized by 2010, compared to 5 percent in 2005 (*Information Week*, October 2007). This leaves a lot of room for the market to grow over the next few years.

Software vs. Hardware Virtualization

Hyper-V provides the engine, or hypervisor, required to support the operation of multiple virtual machines on top of standard server hardware. Hyper-V is Microsoft's first foray into hardware-accelerated hypervisors. Hyper-V extends the reach of Microsoft's initial guest operating system virtualization technologies—Virtual Server 2005 R2 and Virtual PC 2007—by providing a virtualization platform that is integrated into Windows Server 2008 as one of the 17 default server roles. As such, Hyper-V is available in the Standard, Enterprise, and Datacenter editions of Windows Server 2008. Hyper-V is also available through the stand-alone Windows Hyper-V Server.

NOTE WINDOWS SERVER 2008 WITHOUT HYPER-V

Microsoft also publishes a version of Windows Server 2008 without Hyper-V for those who need to work with Windows Server 2008 but do not want to implement the Hyper-V role. This version is also available in Standard, Enterprise, and Datacenter editions.

Hyper-V is a Type 1 hypervisor—that is, a hypervisor that is considered a bare-metal hypervisor and runs directly on top of hardware. Type 1 hypervisors are often referred to as *hardware virtualization engines*. Microsoft's previous hypervisor offerings were Type 2—hypervisors that operated as applications on top of existing operating systems. Microsoft Virtual Server and Microsoft Virtual PC are both Type 2 hypervisors. They provide software virtualization. Type 1 hypervisors provide better performance and greater flexibility because they operate as thin layers designed to expose hardware resources to virtual machines, reducing the overhead required to run the hypervisor itself (see Figure 1-3).

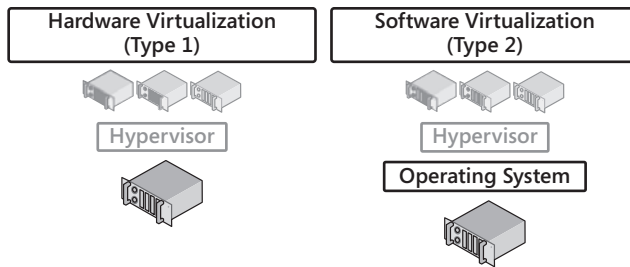


FIGURE 1-3 Type 1 versus Type 2 Hypervisors

Hypervisors are virtual machine monitors that are designed to keep track of all of the events that occur within a virtual machine and, when required, provide (or deny) access to appropriate resources to meet virtual machine operating requirements. Ideally, the virtual machine monitor will perform its operations through the use of policies that contain all of the settings assigned to a particular VM.

Hypervisors in general provide several benefits:

- **System Consolidation** Hypervisors support the operation of multiple systems on the same physical hardware, reducing costs and physical server footprint yet delivering similar and often improved services.
- **System Testing** Hypervisors support the isolation of systems, letting you test new software and applications without affecting production. They also provide a very low-cost testing alternative to physical systems.
- **Heterogeneous System Operation** Hypervisors support the simultaneous execution of multiple operating systems on the same physical hardware, letting organizations run heterogeneous systems on reduced hardware footprints.
- **Hardware Optimization** Hypervisors increase hardware usage through the operation of multiple workloads on each physical host server. Server usage can increase from 5 to 10 percent to upward of 60 or 70 percent.
- **Application High Availability** By sharing workloads through technologies such as failover clustering, servers running hypervisors can support application high availability, ensuring that services are always available when running inside virtual machines.
- **Resource Optimization** By running different applications in different virtual machines, hypervisors can increase resource utilization because each application requires different resources at different times.
- **Service Flexibility** Because hypervisors support the operation of systems through virtual machines, organizations gain flexibility because virtual machines are easier to clone and reproduce than physical machines.
- **Dynamic Resource Management** Hypervisors support manual or automated resource allocation to virtual machine workloads as peak usage occurs. Because of this, hypervisors provide better support for dynamic resource allocation in datacenters.

As mentioned earlier, Type 2 hypervisors run on top of existing operating systems and are nothing more than applications in their own right. There are several examples of Type 2 hypervisors, or virtual machine monitors, and the ones that IT professionals are most commonly familiar with are the Java virtual machine and the .NET environment, both of which are engines that can be used to spawn virtual environments at a higher level in the application stack. These two products are classic Type 2 virtual machine monitors because they control all access to the core resources of the operating system they rely on.

Microsoft Virtual Server and Microsoft Virtual PC are considered hybrid Type 2 virtual machine monitors because of the way they operate. Although they are used to spawn virtual environments higher in the application stack, they are also used to grant access to the operating system kernel or ring 0 to the virtual machines they support. This is done by putting the Windows operating system in stasis while the core CPU resources are assigned to the virtual machine. However, Virtual Server and Virtual PC are still considered Type 2 hypervisors because all VM requests are still routed through the underlying Windows operating system. However, these two products are often referred to as *hosted virtualization platforms* because they rely on an existing operating system to operate.

The advantage of Type 2 hypervisors is that they make it very easy to access virtual machines under normal circumstances. For example, you could easily run Virtual PC on your production desktop and gain access to all sorts of different operating systems and applications running inside virtual machines while continuing to have access to all of your productivity applications—given, of course, that your desktop has sufficient resources such as CPU, RAM, and disk space. Because of this, Type 2 hypervisors have become part of the standard toolkit for most IT professionals.

MORE INFO OTHER TYPE 2 HYPERVERSORS

Microsoft is not the only publisher of Type 2 hypervisors. VMware also offers several Type 2 hypervisors through VMware Server and VMware Workstation. Like Microsoft, VMware also offers a Type 2 hypervisor for Macintosh operating systems: VMware Fusion. More information on VMware hypervisors can be found at <http://www.vmware.com/products/>. Sun Microsystems also offers a Type 2 hypervisor through xVM VirtualBox. VirtualBox runs on the Windows, Macintosh, Linux, and Solaris operating systems. More information on xVM VirtualBox can be found at <http://www.sun.com/software/products/virtualbox/index.jsp>. You can find information on Microsoft Virtual Server at <http://www.microsoft.com/windowsserversystem/virtualserver/>; information on Microsoft Virtual PC is located at <http://www.microsoft.com/windows/products/winfamily/virtualpc/default.mspx>.

Type 1 hypervisors run directly on the hardware with no underlying operating system. Because of this, they are a function in and of themselves. Servers that run Type 1 hypervisors are often single-purpose servers that offer no other function. They become part of the resource pool and are designed specifically to support the operation of multiple applications within various virtual machines. Type 1 hypervisors are typically more efficient than Type 2 hypervisors, yet in many ways they both provide the same type of functionality. In the case of

Hyper-V, this hypervisor offers several improvements over Microsoft's Type 2 hypervisors—notably, support for x64 as well as x86 virtual machines, support for symmetric multiprocessing (SMP) within virtual machines, and significant performance improvements.

MORE INFO OTHER TYPE 1 HYPERVERSORS

Microsoft is not the only publisher of Type 1 hypervisors. VMware, Sun, Citrix, and others—notably most Linux distribution vendors—offer their own Type 1 hypervisors. Information on VMware hypervisors can be found at <http://www.vmware.com/products/>. Information on Sun hypervisors can be found at <http://www.sun.com/software/products/xvmserver/index.xml>. Information on Citrix XenServer hypervisors can be found at http://www.citrix.com/English/ps2/products/product.asp?contentID=683148&ntref=hp_nav_US. Information on Microsoft Hyper-V can be found at <http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx>.

Many IT professionals will become familiar with virtual machine technology through Type 2 hypervisors and then move on to Type 1 hypervisors when ready. Most organizations run Type 2 hypervisors in testing, development, and training environments because of the flexibility they provide. They run Type 1 hypervisors in production because of the stability, robustness, and high availability they can provide.

Exploring Windows Server 2008 Hyper-V

As mentioned earlier, there are several versions of Hyper-V, Microsoft's Type 1 hypervisor. The most complete version is found in Windows Server 2008. Note, however, that Hyper-V is an x64-only function of Windows Server 2008. This means that it is only available as a role within the x64 editions of Windows Server 2008. Although Hyper-V components are also available in x86 or 32-bit editions of Windows Server 2008, only the administration function of Hyper-V can be run on these platforms; the hypervisor itself cannot run on a 32-bit platform. Also note that the Web edition of Windows Server 2008 does not include any version of the Hyper-V function, nor do the versions that specifically state "without Hyper-V." In fact, the fully functional Hyper-V role can only be found in the following editions:

- **Windows Server 2008 Standard x64 edition** Provides support for the Hyper-V role. License includes support for one physical server installation plus one guest operating system or virtual machine.
- **Windows Server 2008 Enterprise x64 edition** Provides support for the Hyper-V role as well as Hyper-V failover clustering for high availability. License includes support for one physical server installation plus four guest operating systems or virtual machines.
- **Windows Server 2008 Datacenter x64 edition** Provides support for the Hyper-V role as well as Hyper-V failover clustering for high availability. License includes support for one physical server installation plus unlimited guest operating systems or virtual machines. Note that the Datacenter edition is licensed on a per-processor basis.

In addition to obtaining the appropriate edition of Windows Server 2008 to run the Hyper-V role, you must ensure that you have the right hardware platform. Hyper-V, because

it is a hardware-based hypervisor, must run on a 64-bit system with both hardware-assisted virtualization and data execution prevention (DEP) enabled. Systems that meet these requirements are x64 systems—not Itanium systems. x64 processors are simply a 64-bit extension of x86 or traditional 32-bit technology. Itanium processors are custom 64-bit processors produced by Intel to support special resource-intensive workloads.

x64 processors are available from both Intel and AMD. Intel x64 processors rely on Intel Virtualization Technology (Intel VT). AMD processors rely on AMD Virtualization (AMD-V). Both processors require specific Basic Input/Output System (BIOS) settings to control or enable the hardware-assisted virtualization function. This function supports hypervisors by providing direct interaction between the hypervisor and all system hardware. The hardware-assisted virtualization feature must be enabled within the system's BIOS for the hypervisor to operate.

As with many Windows Server 2008 roles, Hyper-V can be run in either the full installation or the Server Core installation. Keep in mind that running Hyper-V in a full installation of Windows Server 2008 (see Figure 1-4) will reduce the resources available to virtual machines because the full installation requires more resources to operate than the Server Core installation. In addition, the full installation will have an impact on virtual machine availability because it includes more components—Windows Media Player, Windows Photo Gallery, Internet Explorer, and so on—that require software updates. Each time you must update the base operating system and reboot the host server, you must shut down all of the virtual machines it may run—even if only temporarily. This significantly reduces the availability of virtual machines.

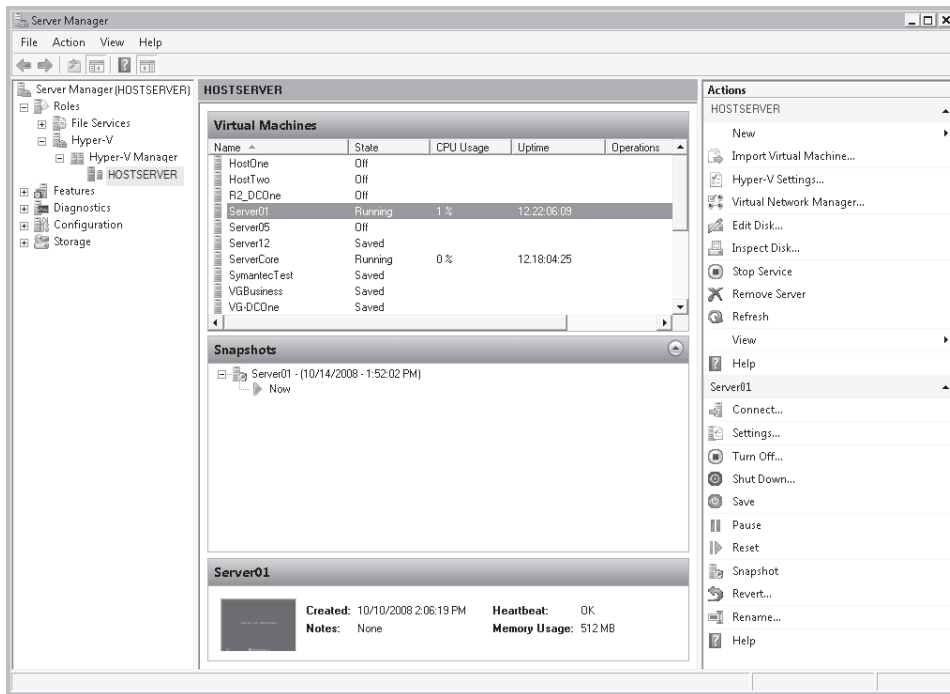


FIGURE 1-4 Hyper-V running in the full installation of Windows Server 2008

On the other hand, Server Core has been designed to run without a graphical interface (see Figure 1-5). It provides both a reduced attack surface and an improved platform for virtualization because it runs fewer processes and applications than the full installation. Yet it supports all of the functionality required to support the operation of a production hypervisor, including failover clustering, when based on the appropriate editions of Windows Server 2008. For these reasons, Server Core is the ideal platform for Hyper-V in production.



FIGURE 1-5 The Server Core interface

Note, however, that because of its lack of a graphical interface, most organizations choose to manage Server Core installations remotely through the use of the Windows Server 2008 Remote Server Administration Tools (RSAT). RSAT can be installed on either Windows Vista or the full installation of Windows Server 2008.

This does not mean that you cannot run Hyper-V on the full installation of Windows Server 2008. Just keep in mind that because of the higher overhead involved with this installation, you should keep instances of Hyper-V on full installations out of the production datacenter and reserve them for testing or development environments. This will reduce the impact the full installation has on the virtual machines you run.

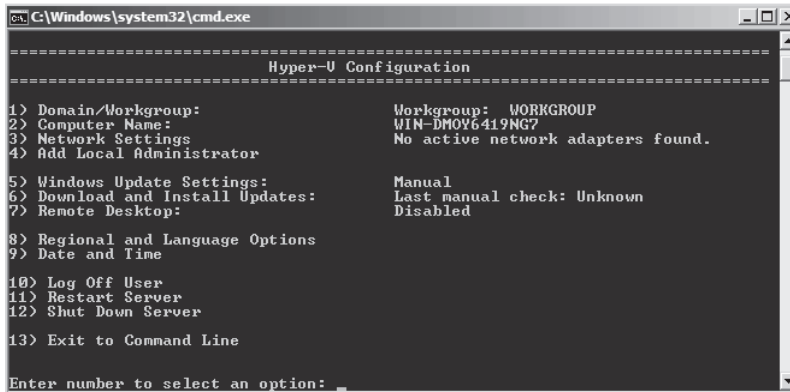
Exploring Microsoft Hyper-V Server 2008

Hyper-V is also available as a freely downloadable version through the Microsoft Hyper-V Server 2008. This version is a self-contained, single-purpose version of Windows Server 2008 that has been customized to support the Hyper-V role. It is based on the Standard edition of Windows Server 2008 and therefore lacks support for high availability and is limited to 32 gigabytes (GB) of RAM. Each machine you deploy with Hyper-V Server will be a stand-alone host server and will not be able to provide service redundancy for the virtual machines you deploy on them.

Hyper-V Server also relies on the Server Core interface and does not provide a graphical environment. Everything is run through a command line. Yet because Hyper-V Server is based on the core Windows Server code, it provides support for remote administration much the same way that Windows Server 2008 Hyper-V does when run in a Server Core installation.

Because of the Hyper-V Server's feature set, Microsoft recommends that you use it in test and development environments, for basic server consolidation where host server high availability is not a requirement, or in branch office consolidation scenarios. Keep this in mind as you choose which edition of Hyper-V to deploy in your environments. Note that as a free product, Hyper-V Server does not include any virtualization rights for Windows Server operating systems. To obtain additional virtualization rights, you must purchase a version of Windows Server 2008 that includes Hyper-V.

To simplify the installation and deployment of Hyper-V Server, Microsoft has included a custom configuration menu (see Figure 1-6)—something that is not available in Server Core installations of Windows Server 2008.



```
C:\Windows\system32\cmd.exe

=====
Hyper-V Configuration
=====

1) Domain/Workgroup:          Workgroup: WORKGROUP
2) Computer Name:             WIN-DMOY6419NG7
3) Network Settings           No active network adapters found.
4) Add Local Administrator

5) Windows Update Settings:    Manual
6) Download and Install Updates: Last manual check: Unknown
7) Remote Desktop:             Disabled

8) Regional and Language Options
9) Date and Time

10) Log Off User
11) Restart Server
12) Shut Down Server

13) Exit to Command Line

Enter number to select an option: _
```

FIGURE 1-6 The Hyper-V Server Configuration menu



EXAM TIP HYPER-V SERVER

Microsoft released Hyper-V Server after the release of the 70-652 exam. Because of this, no questions on this topic were on the exam when it was originally released. The exam might include Hyper-V questions at the time you take it. Hyper-V Server is an important part of any Hyper-V deployment, and information on this topic is included in this guide.

UPDATE ALERT HYPER-V SERVER R2

Hyper-V Server R2 is now based on the Enterprise edition of Windows Server 2008 R2 and because of this, can support up to 1 terabyte of RAM and up to eight processor sockets as well as the creation of failover clusters. Therefore, the scenarios in which you can rely on Hyper-V Server R2 change to include any server virtualization goal.

Understanding Hyper-V Features

Because it is integrated into the Windows Server operating system, Hyper-V benefits from the existing Windows Server feature set. In addition, Hyper-V relies on the Designed for Windows hardware specification, which gives it access to thousands of validated platform configurations. Table 1-2 outlines the specific features of Hyper-V.

TABLE 1-2 The Hyper-V Feature Set

FEATURE	BENEFIT
Access Control through Authorization Manager (AzMan)	Hyper-V includes support for role-based access control (RBAC) through the use of Authorization Manager. This allows organizations to create custom security roles to delegate specific activities within Hyper-V.
Extensibility	Hyper-V is integrated into the Windows Management Instrumentation (WMI) and includes several application programming interfaces (APIs) in support of third-party tool and utility development.
Fault Tolerance	Hyper-V can rely on the Failover Clustering feature of Windows Server 2008 to ensure that host servers are highly available. You must use either the Enterprise or the Datacenter editions of Windows Server 2008 to gain access to this feature. Virtual machines running in Hyper-V can take advantage of both the Failover Clustering feature and Network Load Balancing at the virtualization layer for fault tolerance.
Guest OS Support	Hyper-V supports the operation of both 32-bit and 64-bit virtual machines running a wide variety of operating systems.
Hardware Sharing Architecture	Hyper-V relies on a hardware sharing architecture that provides access and monitors utilization of core resources—disk, networking, video—through a virtual service provider (VSP)/virtual service client (VSC) architecture.
Improved Windows Server 2008 VM Performance	Because Windows Server 2008 includes the Hyper-V role, all virtual machines built on Windows Server 2008 automatically include integration components to improve VM performance.
Integration to Windows Server 2008	Hyper-V can rely on a multitude of certified devices and physical machine configurations because it is built on the x64 version of the Windows Server code.
Linux Integration Components	Hyper-V includes SUSE Linux Enterprise Server 10 SP1 x86 and x64 integration components. This provides improved performance for guest Xen-enabled Linux operating systems when running as virtual machines on Hyper-V.
Quick Migration	When running in a failover cluster, Hyper-V hosts can move a running virtual machine from one host to another with minimal service interruption. The virtual machine is paused on one host server and restored on another.
Remote Administration	Hyper-V includes a stand-alone Hyper-V Microsoft Management Console (MMC) that can be installed separately to provide remote administration of all Hyper-V hosts running either Server Core, the full installation, or running on Hyper-V Server.

FEATURE	BENEFIT
Server Core Integration	Hyper-V is available as a role in a Server Core installation, reducing the attack surface and the downtime associated with operating system updates on host servers.
Server Manager Support	Hyper-V is a role that is integrated into the Server Manager interface of Windows Server 2008. This facilitates the use of Hyper-V on full installations of Windows Server 2008. Note that Server Manager cannot manage remote instances of servers and therefore cannot be used to manage a Server Core installation of Hyper-V.
Settings Quick Reset	Administrators can quickly reset all check boxes and remove saved credentials from within the Hyper-V administration console.
Symmetric Multiprocessing Support	Virtual machines running in Hyper-V can rely on up to four virtual processors. However, the number of supported processors varies with the operating system installed in the guest VM.
Virtual Hard Disk (VHD) Tools	Hyper-V includes a set of tools that support the compaction, expansion, and inspection of virtual hard disk drives created with Hyper-V.
Virtual Machine Snapshots	Hyper-V supports the creation of point-in-time snapshots for virtual machines—images of a given state for the VM at a given time—and can create up to 50 snapshots per VM. Note that these VM snapshots are not to be confused with the snapshots taken by the Volume Shadow Copy (VSS) Service during backup operations.
Virtual Networking	Hyper-V includes a new virtual network switch that provides access to multiple network interface card types for each VM. The virtual network switch provides full support for features such as Network Load Balancing.
Virtual SCSI Support	Hyper-V supports up to four virtual SCSI controllers per virtual machine, giving your VMs access to a multitude of disks.
VM Manageability	Hyper-V provides support for importing and exporting virtual machine settings, letting you move VMs from host to host with little or no impact.
VM Memory Support	VMs running on Hyper-V can each access up to 64 GB of RAM.
Volume Shadow Copy Services (VSS) Support	Hyper-V includes support for VSS to allow the backup of running virtual machines through the use of VSS snapshots. This reduces the downtime that can be associated with VM backups.

Each of these features makes this first version of Hyper-V a powerful platform for machine virtualization.



EXAM TIP HYPER-V FEATURES

Microsoft released the release to manufacturing (RTM) version of Hyper-V several months after the release of Windows Server 2008. Therefore, several features were released even later than this. For example, the Linux Integration Components (LIC) were still in beta at time of the writing of this guide. Although the beta version of the Linux components are included in the exam topics, the full functionality of the Linux Integration Components may differ from the beta functionality included in the exam. Note that the LIC will no longer be in beta when you read this.

Understanding the Hyper-V Architecture

As mentioned earlier, Hyper-V uses a virtual service provider/virtual service consumer architecture to provide hypervisor services to the virtual machines it supports. The full Hyper-V architecture includes several core components:

- The hypervisor interacts directly with a hardware-enabled virtualization processor to provide resources to virtual machines. It is a thin layer of software (less than 1 KB) that provides and maintains separation between the various partitions that run on top of it. In Hyper-V, partitions are logical units of isolation in which operating systems execute. The hypervisor also serves to map real and virtual components such as processor, memory, storage, and network cards. In fact, the hypervisor acts as a redirector to control all access to processor resources.
- The hypervisor resides on Designed for Windows server hardware because of its integration into Windows Server 2008.
- A parent partition is a special system partition that is used to host the virtualization stack in support of virtual machine operation. Each instance of Hyper-V must have at least one parent partition—often called the *root partition*—running Windows Server 2008 64-bit edition. This partition has direct access to hardware devices through the use of the Virtual Machine Bus (VMBus). Because this parent partition is based on Windows Server 2008, it includes all of the features of the operating system installation. These features vary based on the type of installation: full or Server Core. Applications and services installed in the parent partition can run in kernel mode (ring 0) or user mode (ring 3). The parent partition is used to generate and manage child partitions. Child partitions are generated through the hypercall API included in Hyper-V.
- Child partitions are partitions that rely on separate memory spaces to host virtual machines. Virtual machines can include guest operating systems that are either hypervisor-aware or not hypervisor-aware. Hypervisor-aware guest operating systems provide better performance when running on Hyper-V because they can rely on the Hyper-V integration components to interact with virtual devices through the VMBus. Non-hypervisor-aware VMs provide poorer performance because they must rely on the hypervisor to access virtual hardware through a special emulation mode. Every application or service that operates within a child partition runs in user mode only and cannot access the kernel mode of Windows Server 2008.

The Hyper-V architecture is illustrated in Figure 1-7. As you can see, it includes several additional components that rely on the four key components of the architecture to provide additional services and features.

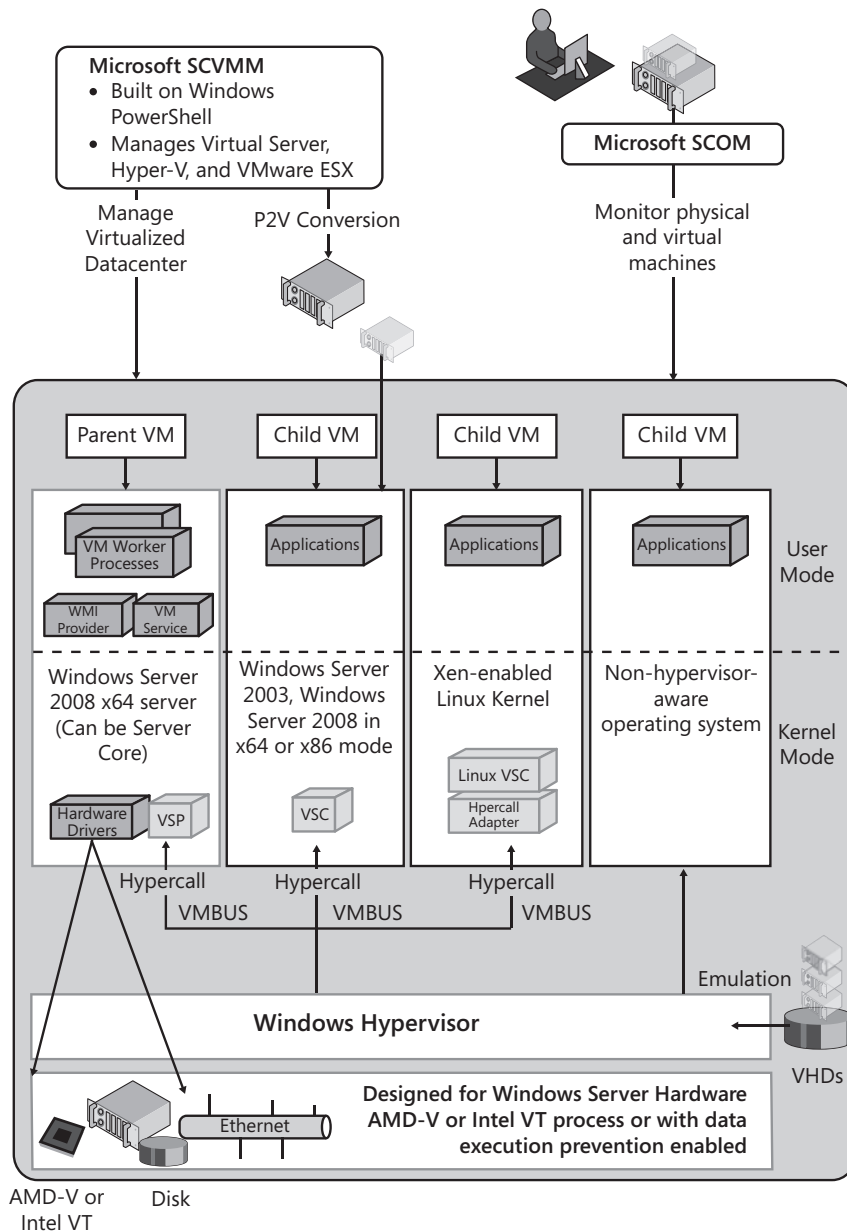


FIGURE 1-7 The Hyper-V architecture

Because Hyper-V operates as part of Windows Server 2008, it can interact with Microsoft System Center tools such as System Center Virtual Machine Manager (SCVMM) and Operations Manager (OpsMgr). SCVMM is a virtual machine management engine that is built on top of the

Windows PowerShell scripting language and therefore requires the Microsoft .NET Framework to operate. Although many organizations can manage multiple Hyper-V hosts adequately with the built-in Hyper-V management tools, datacenters that want to manage multiple resource pools will want to take advantage of the more complete feature set found in SCVMM.

In addition, Operations Manager can interface with both Hyper-V hosts and the virtual machines it supports to provide performance and operational monitoring for each machine. Once again, organizations that manage multiple VMs and several hosts will want to look to Operations Manager to ensure the proper operations of both virtual and physical machines.

Parent vs. Child Partitions

In Hyper-V, no partition has direct access to physical processors and they do not handle any processor interrupts. Instead, they gain a virtual view of processor and memory resources. The hypervisor handles all processor interrupts and redirects them to the appropriate parent or child partition. Although the parent partition has some access to physical hardware resources, child partitions only see virtual resources that are presented as virtual devices. Requests to these virtual devices are redirected through either the VMBus or the hypervisor to the actual devices in the parent partition designed to handle these requests. The VMBus is a logical inter-partition communication channel designed specifically to manage these requests and their results.

The VSP/VSC architecture comes into play because the parent partition includes Virtualization Service Providers that rely on the inter-partition communication process provided by the VMBus to listen to device requests from child partitions. Each child partition includes the Virtualization Service Clients, or clients which act as interface points for virtual device requests and results from the VSP. This entire process is transparent to the guest operating system. The VMBus provides high-speed communication between VSCs and VSPs, including system calls to video, I/O, storage, and networking.

Because they can access hardware directly, VSPs operate in the kernel mode of the parent partition to provide the emulation of hardware such as network interface cards (NICs) or hard disk storage. All device drivers—third-party, native, or otherwise—also operate in kernel mode. Operating in kernel mode grants the drivers direct access to the hardware and provides faster response to I/O requests. This is one more reason why the Designed for Windows Server hardware program is so important: it certifies that all drivers operate correctly and do not bring a system down.

The parent partition also runs several processes in user mode. User mode processes are isolated and cannot affect the core operating system. The processes run in user mode include the Virtual Machine Service (VM Service), which manages the virtualization service, provides virtual machine management for each child partition, and supports administrative interaction with each VM; several instances of the Virtual Machine Worker (VM Worker) process, which help run VMs—one worker process is required for each running child partition—by storing all of the settings for the child partition such as processor count, number of disks, number of NICs and so on; and the Windows Management Instrumentation (WMI) which provides an

interface to Hyper-V management. Table 1-3 outlines all of the processes found in the parent partition (see Figure 1-8) as well as the names of the executables running the processes. The processes running in this partition are called the Hyper-V virtualization stack. Note that some of the virtualization stack components in Table 1-3 do not have executable or system names, although they are important parts of the entire stack.

TABLE 1-3 Parent Partition Processes

PROCESS	OPERATING MODE	EXECUTABLE	DESCRIPTION
Virtual Machine Management Service	User Mode (Ring 3)	VMMS.exe	The service responsible for managing virtual machine states in child partitions
Virtual Machine Worker Process	User Mode (Ring 3)	VMWP.exe	Provides VM management services from the Windows Server 2008 instance in the parent partition to the guest operating system in child partitions
WMI Provider	User Mode (Ring 3)	Svchost.exe	Exposes a set of WMI-based application programming interfaces for managing and controlling VMs
Virtualization Infrastructure Driver	Kernel Mode (Ring 0)	VID.sys	Provides partition management, virtual processor management, and memory management services for all child partitions
Virtual Service Provider	Kernel Mode (Ring 0)		Provides a way to publish device services to child partitions through I/O-related resources to virtual service clients or consumers
Virtual Machine Bus	Kernel Mode (Ring 0)		An inter-partition communication mechanism between parent and child partitions
Windows Hypervisor Interface Library	Kernel Mode (Ring 0)	WinHV.sys	A dynamic-link library (DLL) that loads within the Windows Server 2008 instance in the parent partition and in Hyper-V aware child partitions to interface between them

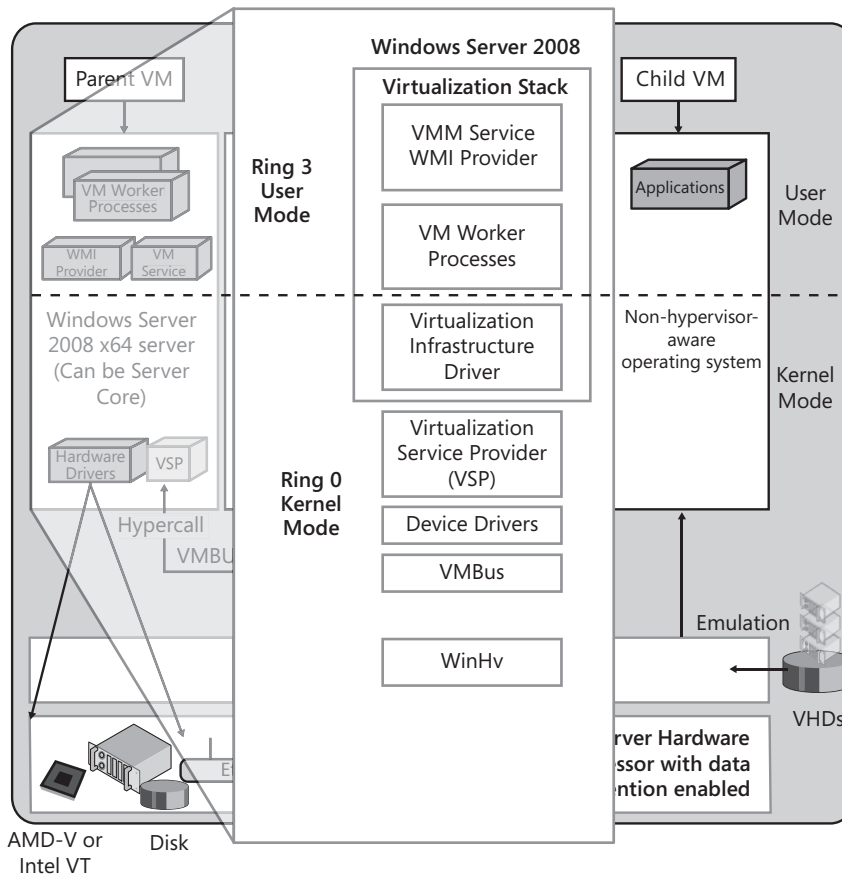


FIGURE 1-8 The Hyper-V parent partition and the virtualization stack

Enlightened vs. Legacy Guests

Several operating systems have been updated to provide better performance when running in a virtual machine. By default, operating systems are designed to require exclusive access to hardware resources, but when they run alongside several other operating systems in virtual machines, they cannot gain this exclusive access. An *enlightened* guest operating system is an operating system that has been designed to share resources when running in a virtual machine and is Hyper-V-aware.

In Hyper-V, a special feature named Enlightened I/O is designed to provide increased performance for guest operating systems running in VMs when they need to access virtual devices such as storage, networking, graphics, or input subsystems. Enlightened I/O is a virtualization-aware implementation of communication protocols that interact directly with the VMBus to provide high-speed access to resources. Protocols such as SCSI, iSCSI, and others can take advantage of this improved communication level because they bypass any emulation layer. Protocols that are not enlightened face reduced performance because they must first interact

with this emulation layer and translate all requests during all communications processes. Virtual machines running non-enlightened protocols or drivers are deemed *legacy* VMs.

Hyper-V provides direct interaction with the VMBus through the installation of Integration Components—special components that enable both Enlightened I/O and provide a hypervisor-aware kernel to the guest operating system. The Hyper-V Integration Components also include the virtual service client drivers required to support direct interaction with the VMBus. As mentioned earlier, Windows Server 2008 already includes the Integration Components, but Hyper-V can inject the Integration Components into other Windows operating systems such as Windows Server 2003, Windows HPC Server, Windows 2000 Server, Windows Vista, and Windows XP. Hyper-V also includes Integration Components for Xen-enabled distributions of SUSE Linux Enterprise Server. The full list of supported guest operating systems is provided in Table 1-4, which also lists the number of supported virtual processors per guest operating system.

TABLE 1-4 Supported Guest Operating Systems in Hyper-V

OPERATING SYSTEM	VERSION	SUPPORTED VIRTUAL PROCESSORS
Windows Server 2008 x64	Standard	1, 2, or 4
	Enterprise	1, 2, or 4
	Datacenter	1, 2, or 4
	Web	1, 2, or 4
	Standard without Hyper-V	1 or 2
	Enterprise without Hyper-V	1, 2, or 4
	Datacenter without Hyper-V	1, 2, or 4
Windows Server 2008 x86	Standard	1 or 2
	Enterprise	1, 2, or 4
	Datacenter	1, 2, or 4
	Web	1 or 2
	Standard without Hyper-V	1 or 2
	Enterprise without Hyper-V	1, 2, or 4
	Datacenter without Hyper-V	1, 2, or 4
Windows Server 2003 x86	Standard with Service Pack 2	1 or 2
	Enterprise with Service Pack 2	1 or 2
	Datacenter with Service Pack 2	1 or 2
	Web with Service Pack 2	1 or 2
Windows Server 2003 x64	Standard with Service Pack 2	1 or 2
	Enterprise with Service Pack 2	1 or 2
	Datacenter with Service Pack 2	1 or 2

OPERATING SYSTEM	VERSION	SUPPORTED VIRTUAL PROCESSORS
Windows Server 2000	Server with Service Pack 4	1
	Advanced Server with Service Pack 4	1
Windows HPC Server 2008		1, 2, or 4
x86 Linux Distributions	SUSE Linux Enterprise Server 10 with Service Pack 2	1
	SUSE Linux Enterprise Server 10 with Service Pack 1	1
X64 Linux Distributions	SUSE Linux Enterprise Server 10 with Service Pack 2	1
	SUSE Linux Enterprise Server 10 with Service Pack 1	1
Client Operating Systems	Windows Vista Business x86 edition with Service Pack 1	1 or 2
	Windows Vista Enterprise x86 edition with Service Pack 1	1 or 2
	Windows Vista Ultimate x86 edition with Service Pack 1	1 or 2
	Windows Vista Business x64 edition with Service Pack 1	1 or 2
	Windows Vista Enterprise x64 edition with Service Pack 1	1 or 2
	Windows Vista Ultimate x64 edition with Service Pack 1	1 or 2
	Windows XP Professional x86 with Service Pack 3	1 or 2
	Windows XP Professional x86 with Service Pack 2	1
	Windows XP Professional x64 with Service Pack 2	1 or 2

Although Microsoft endeavors to update the Hyper-V Integration Components on a regular basis to add support for additional operating systems, currently all other operating systems must run in emulation or legacy mode when running in Hyper-V VMs.



EXAM TIP SUPPORTED GUEST OPERATING SYSTEMS

Pay close attention to the list in Table 1-4: The list of supported guest operating systems and the supported number of virtual processors for each guest operating system are both important parts of the exam.

PRACTICE Understanding Hyper-V Virtual Machines

In this practice, you will obtain a copy of the Windows Server 2008 evaluation in Virtual Hard Drive format. This evaluation machine will be used in later practices as you learn to work with the features of Windows Server 2008 Hyper-V. This practice consists of one exercise.

EXERCISE 1 Obtain a VHD Image for Use with Hyper-V

In this exercise you will download and save VHD images of Windows Server 2008 for later use with Hyper-V. You will need a system with at least 10 GB of free disk space to store the VHD image to perform this exercise. The images together are only 4 GB in size, but you will need additional space to decompress them.

1. On a physical machine with sufficient storage space, launch a copy of Internet Explorer.
2. Type **<http://www.microsoft.com/windowsserver2008/en/us/trial-software.aspx>** in the address bar and press Enter. This takes you to the Microsoft Windows Server 2008 Evaluation Software page on the Microsoft Web site.
3. Click the Get The VHD Image button.
4. On the next page, click the Download It Now button next to If You Are Running Windows Server 2008 And Hyper-V, Download Virtual Hard Drive Images.
5. Review and print the instructions on this page. You will require them in later exercises when you use the VHD image.
6. Download both the full installation and the Server Core installation images. Either select the single image or the multi-part images. Click each link to initiate the download.
7. Save both files into the same folder. You will decompress these files in a later exercise.



Quick Check

1. Name at least four benefits related to the use of a hypervisor.
2. What is the difference between Type 1 and Type 2 hypervisors?
3. What is the difference between Windows Server 2008 Hyper-V x64 and Windows Server 2008 Hyper-V x86?
4. How many virtual processors are supported on virtual machines in Hyper-V?

Quick Check Answers

1. System consolidation, system testing, heterogeneous system operation, hardware optimization, application high availability, resource optimization, service flexibility, and dynamic resource management are some of the benefits you can gain from working with a hypervisor.
2. A Type 1 hypervisor is considered a bare-metal hypervisor and runs directly on top of hardware. A Type 2 hypervisor operates as an application on top of an existing operating system.
3. Windows Server 2008 Hyper-V x64 is the only version that includes the Hyper-V role—a role that is only available with the x64 editions of Windows Server 2008—and Windows Server 2008 Hyper-V x86 only includes the administration function of Hyper-V.
4. Virtual machines running in Hyper-V can rely on up to four virtual processors, but the number supported varies with the operating system installed in the guest VM.

Lesson 2: Evaluating Your Environment

When you prepare to work with Hyper-V in your datacenter, you must begin by evaluating your current environment.

After this lesson, you will understand the assessment process:

- First, you must think about how you will move to a Hyper-V infrastructure.
- Second, you must inventory your environment to determine your current physical server configurations and the services you run on them.
- Third, you must perform an in-depth assessment of the services you currently run to fully understand their requirements once they are virtualized.

These three activities provide the input required to transform the existing services running in your datacenter into virtual machines running on Microsoft Windows Server 2008 Hyper-V.

Estimated lesson time: 30 minutes

Preparing to Deploy Hyper-V

Of all of the different layers of virtualization available in the datacenter, the layer that has the most impact on operations—and on the bottom line—is the server virtualization layer. This is because when you rely on server virtualization, you can dramatically reduce the physical footprint of your servers. This is true for organizations of all sizes. Although the physical consolidation results will be remarkable for large organizations running thousands of physical servers at less than 15 percent utilization, they will still be considerable even for small organizations running only a handful of servers. These small organizations can end up with two host servers running in a failover cluster using shared storage to run all of their services in virtual machines, and because Hyper-V can run on all of the server configurations that have been validated for Windows Server 2008, this configuration can be quite inexpensive.

A good example can be seen with Microsoft's new Windows Essential Business Server 2008 (EBS)—an enhanced service offering built on the original concept of Windows Small Business Server (SBS). Although a Small Business Server configuration runs all processes on a single machine, the EBS configuration separates core services—management, messaging, security, and possibly database—into three or four servers, depending on the edition you select. In addition, organizations wanting to virtualize EBS can easily do so because it is a standard deployment strategy for this product. EBS can be virtualized either on a single server—which can create a single point of failure—or on a pair of host servers, greatly simplifying the deployment and management model for this product.

MORE INFO VIRTUALIZING EBS 2008

For more information on how to proceed when virtualizing Windows Essential Business Server 2008, go to <http://technet.microsoft.com/en-us/library/cc512508.aspx>.

EBS is a good example of how organizations of all sizes are turning to server virtualization to gain better control over the server workloads in their datacenters. As a resource pool administrator, your role in this process is to help determine first how to migrate to a server virtualization infrastructure and then how to transform your physical servers into virtual machines to reap the benefits inherent in such a move. To do this, you must rely on a standard process—a process that will vary slightly depending on where you start from. This process should consist of the following activities:

1. Begin by determining your starting point. The three possible scenarios are:
 - Organizations running a traditional physical infrastructure 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 such as Virtual Server or VMware Server need to implement new host servers running Hyper-V and then, possibly, they need to perform a virtual machine conversion to transform existing virtual machines into Hyper-V VMs.
 - Organizations already using hardware-based server virtualization 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.

In each case, it is important to have a complete assessment of your current environment. This assessment helps you determine exactly where you are starting from and helps you understand how your final configurations should appear.

2. Next, you need to prepare and deploy your host servers. You need to appropriately size these servers and determine how many servers are required. This determines your physical consolidation ratio, identifying how many virtual machines each Hyper-V server will host. Once again, your original assessment will provide valuable input into this process. Keep in mind that host servers should be redundant and should be configured to provide high availability for the virtual machines they run.
3. When the host servers are ready, you should prepare your host server and virtual machine management infrastructure. Depending on your organization size and the number of servers you run, you may opt to use either distributed or centralized host server management tools. Distributed management is performed with the Hyper-V administration console. Centralized management is performed with a tool such as SCVMM. If you opt for centralized management (as most resource pool administrators will), you need to prepare the deployment and configuration of SCVMM. You also need to look at possible automation practices for Hyper-V. Automation is performed with Windows PowerShell.
4. During the implementation of your management structure, you also need to look at securing your host servers and, especially in large datacenters, look to the delegation

of administrative tasks. The latter is performed through the Windows Authorization Manager (AzMan) in Hyper-V.

5. You also need to look at how you will protect host servers and the virtual machines they will eventually run. This involves developing backup policies for both host servers and virtual machines.
6. At this point, you are ready to build new virtual machines or convert existing physical machines into virtual machines. New VMs are required for any new service you need to implement in your network. Conversions are required for the workloads you run. Several approaches are available for this conversion and you need to examine the workload in depth to determine how it should be converted.
7. When all of your end user-facing workloads are converted, you can move on to ongoing resource pool and virtual machine administration. The practices you use here will differ from traditional management practices, mostly because of the introduction of the new resource pool concept into the datacenter.

Consider this process carefully—it is the process all resource pool administrators must rely on to move to server virtualization and reap the most benefits from this move. Many will be tempted to skip several steps and jump right into virtualization, but be wary of this approach. Datacenter management is serious business and should always be approached in a structured and strategic manner.

Keep in mind that all processes should be tested out in a laboratory before being put into production. In fact, the laboratory is the ideal place to begin a server virtualization project because it can also greatly benefit from these technologies.

Finally, rely on this process outline to build your own Hyper-V deployment project. The procedures in this book closely tie in to this process and will help support you each step of the way as well as help you gain the knowledge you need to pass the 70-652 exam.

Inventorying Your Existing Environment

It's simply amazing how few organizations have an updated inventory of the technologies in their datacenters, yet this is the first place to start when you want to move to a Hyper-V infrastructure—you can't convert or migrate what you don't know you have.

Inventories are relatively simple to produce. In fact, many organizations already use tools such as the Microsoft Baseline Security Analyzer (MBSA) to perform security and update assessments on their servers and other systems. As soon as a scan is complete, MBSA provides you with information on each system it scanned, including IP address, operating system, installed applications, and of course, potential vulnerabilities. You can easily turn this valuable data into an inventory by linking the results of any MBSA scan with Microsoft Office Visio through the Microsoft Visio Connector for MBSA. Visio will automatically generate a graphical image of your network and display detailed information on each device when you click it. Combining these two tools makes it very easy to generate an inventory.

MORE INFO WORKING WITH MBSA AND VISIO

For more information on MBSA, go to <http://technet.microsoft.com/en-us/security/cc184924.aspx>. To download the Visio Connector for MBSA, go to <http://technet.microsoft.com/en-us/security/cc184925.aspx>.

Microsoft also offers a similar Visio Connector for System Center Operations Manager. If you already use Operations Manager, you won't need MBSA and you'll be able to use it with Visio to create a visual representation of your network. The same tool also works with System Center Configuration Manager (SCCM, formerly Systems Management Server). Inventory is one of the four core features of this product. Although both Operations Manager and Configuration Manager are more complex tools to roll out than MBSA, they can and do provide constant and ongoing inventory and other status information for all of the systems in your datacenter.

MORE INFO WORKING WITH SC OPERATIONS MANAGER, SC CONFIGURATION MANAGER, AND VISIO

To download the Visio Connector for Operations Manager, go to <http://visiotoolbox.com/en-US/downloads.aspx?resourceid=2&aid=592>.

The tool you use to perform your initial inventory scan doesn't really matter. What does matter is that you discover what is in your datacenter both locally and remotely if your organization also has server technologies in remote sites. When you do, you should pay particular attention to the items listed in Table 1-5.

TABLE 1-5 Key Inventory Factors

ITEM	QUESTIONS TO ANSWER
Server Count	What is the overall server count in your network?
Workloads	How many servers are implemented for a particular workload?
Server Hardware	What type of hardware is each workload running on? Is all hardware from the same generation or manufacturer?
CPU/BIOS Requirements	Which CPUs are running each workload? Are your workloads running on 32-bit or 64-bit processors? If your processors are 64-bit, are the operating systems running on these processors x64 operating systems? How many processors are assigned to each workload?
Memory Requirements	How much RAM is configured on each server? Does the workload actually make use of all of the RAM?

ITEM	QUESTIONS TO ANSWER
Disk/Logical Unit Number (LUN)	Which type of disk subsystems are being used in support of each workload? Are your disk subsystems directly attached or remote? Are remote disks running on network attached storage (NAS) or on storage attached networks (SAN)? How many LUNs are assigned to each workload? Are there remaining LUNs or spare storage in your NAS or SAN infrastructures?
Networking/Network Interface Card (NIC)	What is the networking requirement for each workload? Is there more than one NIC per server and if so, what is the purpose of each NIC?

The questions outlined in Table 1-5 are sample questions that cover the most basic aspect of your inventories, but obtaining the answers to these questions will get you moving forward on your virtualization project.

Using the Microsoft Assessment and Planning Tool

Inventories are not the only information you require when planning to move from an existing infrastructure to a Hyper-V resource pool. Although inventories provide you with the basic information about numbers of machines and workload types, assessments provide you with the operational details for each of the workloads you intend to convert.

Preparing Assessments

Your assessment should include the following activities:

- Consider the various processes running in your datacenter and their dependencies. Understanding the interconnectivity of your running processes and services helps you determine which functions are best suited to virtualization and helps you determine the order of conversion for each workload.
- Determine the number of parent partitions or host servers required to support these workloads. Remember that each Hyper-V server hosts one parent partition, but many child partitions. Determine how resources—processors, memory, hard disks, and network adapters—will be allocated to the parent partitions in support of the number of child partitions it will run.
- Determine the order of conversion for existing workloads. Remember the seven-step process outlined earlier in this lesson. In most cases, you will want to convert both test and development environments as well as performing production physical server consolidation. Begin with the test and development environment because you can

afford to experience downtime in these environments. Then, when you are more familiar with the process, move on to physical server consolidation.

- Determine which workloads will be consolidated on which host servers. Try to consolidate heterogeneous workloads onto each host server. For example, you don't want a host server to run a multitude of virtual Web servers because they will always compete for the same physical resources at the same time. You can also use an application such as SCVMM 2008 to help determine appropriate consolidation candidates based on thresholds such as processor and network usage as well as workload size. Use this information to plan out the workload conversion.
- When the conversion is complete, you will look to the optimization of your infrastructure. Microsoft's Infrastructure Optimization process uses a four-stage model that includes the basic, standardized, rationalized, and dynamic stages. You move from basic to standardized when you convert underutilized physical servers into virtual machines. You move on to a rationalized infrastructure when you implement centralized management tools that control both the physical and the virtual infrastructure. You can complete the process and move on to a dynamic infrastructure when you enable dynamic machine provisioning and implement self-managing systems.
- Complete the optimization process by using the right resources for each job in your datacenter. If a workload requires a 2-processor system with 8 GB of RAM, implementing a host server with 8 processors and 32 GB of RAM is overkill. Try to aim for maximum resource usage in your implementation. Also identify appropriate storage. Host servers operating systems can run off of direct-attached storage, but this storage should be configured for fault tolerance. Use redundant arrays of independent disks (RAID) configurations for both DAS and remote storage. This makes your systems more tolerant to potential device failures. Also, rely on shared storage to place VMs so that they can be accessed by several nodes in a cluster. This renders the VMs more fault tolerant because they will be able to fail over to another cluster node if the current host has a critical failure.
- Finally, use intelligent placement to make the most of your physical resources. When you select which parent partition will run a particular child partition, you perform VM placement. VMs should be placed on the hosts that are most suited to their operation. When you use intelligent placement, you rely on ratings assigned to each host server. SCVMM can centralize this process by identifying all of the hosts in your resource pool and rating them. Hosts are rated based on the number of processors, memory, and other resources such as available hard disk space. Once the hosts are rated, SCVMM can automatically place VMs on appropriate hosts based on existing host workloads and capabilities. This simplifies the VM placement process.

You use special assessment tools in support of these processes. These tools are described in the following sections.

Using the Microsoft Assessment and Planning Tool

Microsoft provides the Microsoft Assessment and Planning (MAP) Toolkit Solution Accelerator in support of this effort. MAP is designed to provide the type of assessments required to begin the conversion process. MAP can be used to scan your entire network for assessments. MAP was formerly released as the Windows Vista Hardware Assessment Tool and was designed to allow organizations to scan their existing PCs to determine their potential for hosting the Windows Vista operating system. But the tool had potential for more—a lot more—and Microsoft soon realized this. If the tool could scan for Windows Vista hardware requirements, it could also scan for a wide variety of other assessments. Therefore, Microsoft changed and adapted the tool to support a whole series of other operations.

MORE INFO DOWNLOAD MAP

To download the MAP tool, go to <http://www.microsoft.com/downloads/details.aspx?FamilyID=67240b76-3148-4e49-943d-4d9ea7f77730&displaylang=en>.

MAP is an agentless analyzer that collects information on all of the identified systems. MAP requires the use of an account that has administrative privileges on each target computer. MAP can be run from any system, but should preferably be installed on an administrative workstation. Installation is performed through a Windows Installer file. Two files are available: one for x86 or 32-bit systems and one for x64 or 64-bit systems. Once installed, MAP will rely on Windows Management Instrumentation (WMI), the Remote Registry Service, the Simple Network Management Protocol (SNMP), Active Directory Domain Services (AD DS), or the Computer Browser service to identify the systems on your network.

Assessment results are in the form of Management Reports (in Microsoft Office Word format) and Report Metrics (in Microsoft Office Excel format). Assessments included in MAP cover the following (see Figure 1-9):

- Systems that can run Windows Vista
- Systems that can run Microsoft Office 2007
- Determining client security settings
- Systems that can run Windows Server 2008
- Server roles that can be migrated to corresponding Windows Server 2008 roles
- Microsoft SQL Server instances that can be upgraded to SQL Server 2008
- Determining how to reduce power consumption for clients and servers
- Determining which applications can benefit from application virtualization through Microsoft Application Virtualization
- Generating performance reports from servers for consolidation purposes
- Server consolidation through virtualization with Hyper-V or Virtual Server
- Determining whether some services can be consolidated online
- Identifying whether you can optimize desktops

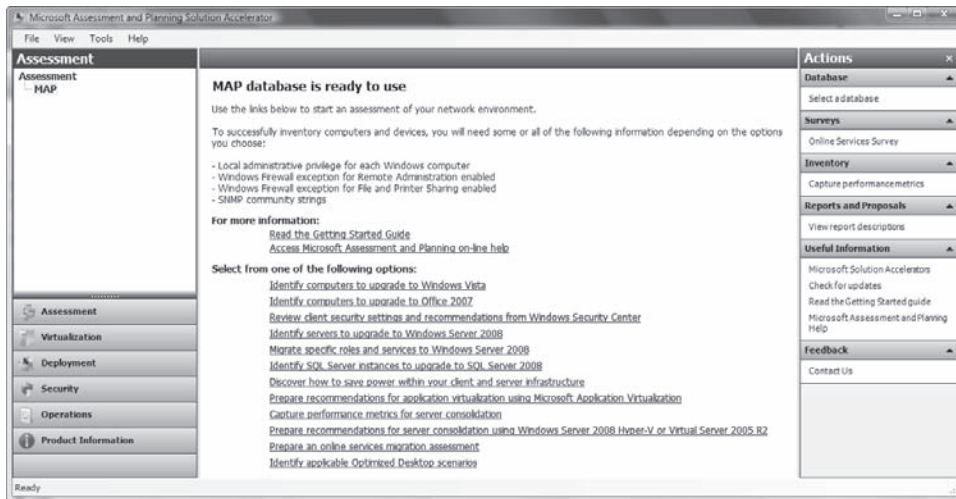


FIGURE 1-9 Using MAP to perform assessments

Each assessment provides a comprehensive series of reports based on the purpose of the assessment. Default reports are in English, but can be translated to French, German, Japanese, Korean, Spanish, and Portuguese (Brazilian). Report details depend on the type of report you use MAP to run. For example, running a MAP report for Windows Server 2008 readiness will include details about approved drivers and required hardware updates. Reports on server virtualization will identify current workloads and potential candidates for virtualization.

MAP stores all data within a SQL database. Data can be reused at any time to generate new reports. In addition, one MAP system can store multiple databases, letting you run assessments for different purposes or even of different environments without mixing the information together. To change databases, click *Select A Database* in the Action pane.

Using MAP to Prepare for Hyper-V

MAP has several uses, but only three components are useful in support of a move to Hyper-V, and the first one is optional:

- Optionally, if you do not have an existing server inventory, you can use the *Identify Servers To Upgrade To Windows Server 2008* assessment in MAP to generate your initial inventory. If you have an existing server inventory, move on to the other two assessments.

NOTE PREPARING FOR THE ASSESSMENTS

When you use MAP to perform assessments for Hyper-V, you must first create a plain text file listing either the NetBIOS or the fully qualified domain names (FQDN) of the servers you want to include in the assessment. Use the inventory you have gathered to prepare this file.

- Use the Capture Performance Metrics For Server Consolidation assessment to analyze the workload on your servers for a given period of time—usually a minimum of two weeks, but much more if possible—to help you identify just how many resources each of your physical workloads requires and let you properly configure the virtual machines you will turn them into. This also lets you determine whether your guests will run as enlightened or legacy virtual machines.
- When performance data has been captured and stored into the MAP database, you use the Prepare Recommendations For Server Consolidation using Windows Server 2008 Hyper-V or Virtual Server 2005 R2 to identify the current workloads of your physical servers and generate recommendations in terms of physical hardware requirements for host servers and how you should virtualize your existing Windows workloads.

Rely on the management reports and report metrics generated by MAP to prepare for your physical server consolidation project and move on to the next stage of your virtualization project.

IMPORTANT CREATE TIMELY REPORTS

Be very careful during this analysis because it will form the basis of your future infrastructure. Properly identifying the required resources for each server workload allows you to appropriately size the hardware you will move these workloads to after you virtualize them. You can never be too careful when you perform a virtualization candidate analysis because once you virtualize your systems, information on physical resource requirements for these workloads is longer available.

In addition, make sure you prepare these reports in a timely fashion. Try to prepare the reports as closely as possible to your actual migration project; otherwise, the data in the reports will not reflect the current status of your network because networks constantly change and grow to meet business requirements.

MORE INFO MAP ASSESSMENT FOR HYPER-V

To view a screencast detailing the steps required to perform a virtualization assessment with MAP, go to <http://go.techtargget.com/r/5927600/30819>.



EXAM TIP ASSESSMENT TOOLS

Note that MAP is not the only tool you can use to perform these types of assessments. Several manufacturers—VMware, CiRBA, and PlateSpin—offer third-party assessment tools. However, the exam only covers the use of MAP. So although you might consider using third-party tools in your own virtualization project, you do not need to know about them for the exam.

In this practice, you will install MAP and prepare a virtualization assessment of an existing environment. This practice, which consists of three exercises, assumes that you already have an existing inventory of the servers you want to assess. The first exercise covers the installation of MAP and all of its prerequisites. The second exercise analyzes the performance of the servers you want to include in your assessment. The third exercise analyzes the performance assessment to determine how your host servers should be sized and how your servers should be virtualized.

EXERCISE 1 Install the Microsoft Assessment and Planning Tool

In this exercise you will download and install the latest version of MAP. Use a workstation to install MAP because MAP requires Microsoft Word and Microsoft Excel to run. The workstation you use can run either Windows XP with Service Pack 2 or Windows Vista.

1. Log on to the workstation with administrative credentials.
2. Use Internet Explorer to download MAP. Go to www.microsoft.com/downloads/details.aspx?familyid=67240B76-3148-4E49-943D-4D9EA7F77730, locate the downloadable files at the bottom of the page, and click the Download button for the appropriate edition (x86 or x64) based on the operating system running on your workstation. Save the file in your Documents folder.
3. When the download is complete, open Windows Explorer, move to your Documents folder, and double-click the downloaded EXE file. If you are running Windows Vista, accept the User Account Control Prompt. The MAP installation begins (see Figure 1-10).

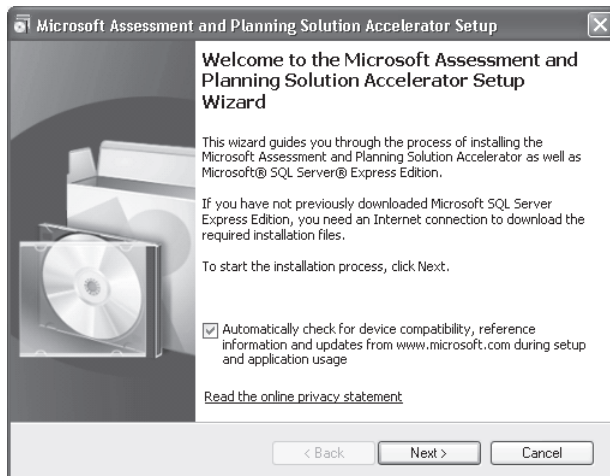


FIGURE 1-10 The MAP Installation Welcome page

4. Proceed with the installation. Click Next on the Welcome page.
5. The MAP installation begins with the verification of prerequisites. If any of the prerequisites are not available, it displays a prerequisite verification page and aborts

the installation (see Figure 1-11). Do not click Finish! Instead, click the links for missing components. This opens an Internet Explorer page and connects you to the appropriate download page. Download and install each of the prerequisites.

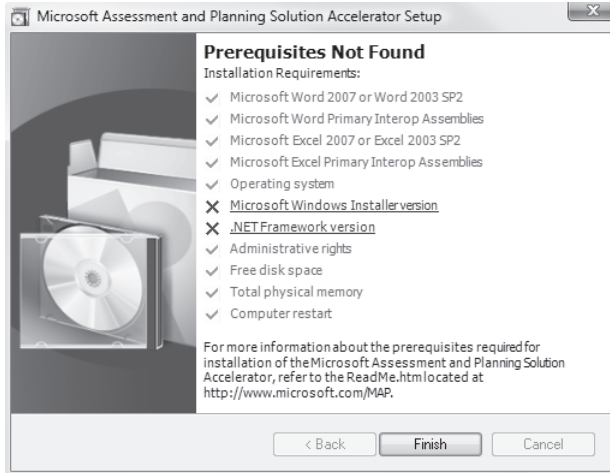


FIGURE 1-11 Locating MAP prerequisites

6. When all of the prerequisites are downloaded and installed, click Finish and launch the MAP installation again.
7. Accept the license agreement and click Next.
8. Choose the installation folder and click Next.
9. MAP requires SQL Server 2008 Express edition to run. If it is not already installed on your machine, select Download And Install and click Next.
10. Accept the SQL Server 2008 Express edition license and click Next.
11. Click Next to proceed with the installation. The MAP installation will download and install SQL Server Express and then install MAP.
12. Make sure the Open The Microsoft Assessment And Planning Solution Accelerator Wizard check box is selected and click Finish when the installation is done.
13. When the MAP Wizard is open, click Select A Database in the Action pane.
14. Select Create An Inventory Database, name it **MAP**, and click OK. You can use this dialog box to manage multiple MAP databases if you need to.
15. MAP is ready to use and all of the assessments are now highlighted in blue.

EXERCISE 2 Assess the Performance of Your Servers with MAP

In this exercise you will capture performance metrics for server consolidation. This exercise relies on the MAP tool you installed to monitor existing servers in your network. You will need access to at least two existing servers to perform this exercise and you will need administrative credentials for these servers. You would normally perform this assessment over a long period

of time to capture peak resource usage for each server, but in the interest of the exercise, you will run the assessment for only one hour.

1. Begin by preparing a text file with the server names you require. Use FQDNs if possible. Launch Notepad (click Start, click Run, type **notepad.exe**, and press Enter) and enter the server names, one per row (see Figure 1-12). Save the file as **ServerNames.txt** in your Documents folder. Close Notepad.

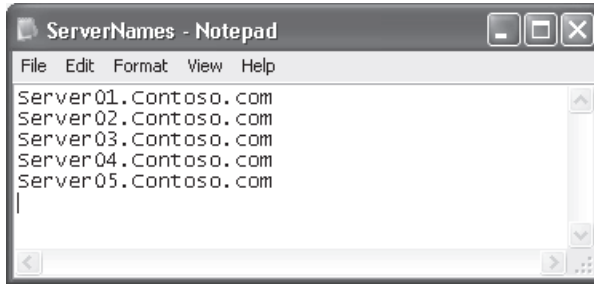


FIGURE 1-12 Creating the list of server names

2. Launch the MAP tool by moving to the Start menu, selecting All Programs, and then selecting Microsoft Assessment And Planning. Click the Microsoft Assessment And Planning shortcut.
3. Click the Capture Performance Metrics For Server Consolidation link in the middle pane of the MAP tool.
4. On the Import Computer Names From A File page, click Browse, move to your Documents folder, select the ServerNames.txt, and click Next. MAP will tell you how many machines will be inventoried. Click OK.
5. On the Enter WMI Credentials page, click New Account. You can use either a domain or a local account to collect information. This account needs local administrative credentials on each machine. Ideally you will be able to use a single account (see Figure 1-13). Enter the credentials and password and click Save. Click Next.

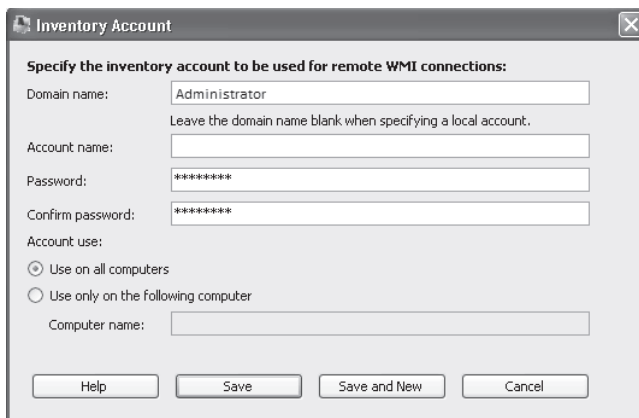


FIGURE 1-13 Entering inventory credentials

6. Collections cannot be automated, but you can run them for significant periods of time. Because of this, you should be careful of which computer you use to run your collection because it will not be available for other activities for the duration of your assessment. In this case, you run the assessment for only one hour, but you would normally run it for a minimum of two weeks, or better yet much more. Set the end time and click Next.
7. Click Finish to begin the collection. The Collection window will open and capture performance metrics. Click Finish when the collection has completed. This information will be stored in the MAP database. Performance information is a prerequisite for being able to run the consolidation assessment.

EXERCISE 3 Perform a Virtualization Recommendation Assessment

In this exercise you will use MAP to prepare recommendations for Hyper-V. You must have performed a performance assessment prior to this assessment or the assessment will not work.

1. Launch the MAP tool by clicking Start, selecting All Programs, and then selecting Microsoft Assessment And Planning. Click the Microsoft Assessment And Planning shortcut if it is not already open.
2. Make sure the appropriate MAP database has been selected. This database must include performance data collected from a previous assessment. Click Prepare Recommendations For Server Consolidation Using Windows Server 2008 Hyper-V Or Virtual Server 2005 R2.
3. Make sure Windows Server 2008 Hyper-V is selected on the first page of the wizard and click Next.
4. On the Model Host CPU page, select your CPU manufacturer, model, number of processors, processor speed, cores per processor, Hyper Threads per core, L2 and L3 Cache sizes, and Bus Speed. If you are not familiar with these values, leave them at the settings automatically entered by the wizard when you choose your processor type (see Figure 1-14). Click Next.

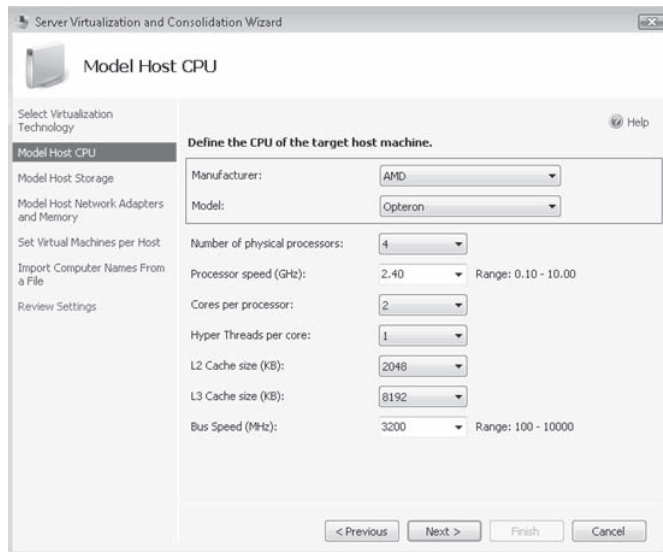


FIGURE 1-14 Selecting Host CPU settings

5. Now, configure projected host server storage. Select the disk type, enter the storage capacity, and then click Select This Option If You Wish To Model An Array Of Disks Using The Single Disk Type Configured Above. Enter the appropriate RAID values. If at all possible, you should use RAID 10 because it provides the fastest response. Note, however, that RAID 10 requires more disks than other RAID types. Click Next.
6. Select the network adapter speed, type in the number of adapters, and enter the total amount of memory in gigabytes for the model host server. Click Next.
7. On the Set Virtual Machines Per Host page, leave all settings blank. Leaving these settings blank lets the wizard determine how many machines should run on the host based on the configuration you entered so far. Click Next.
8. On the Import Computer Names From A File page, click Browse, move to your Documents folder, select the ServerNames.txt, and click Next. MAP will tell you how many machines will be inventoried. Click OK.
9. Review your settings and click Finish to begin the assessment.
10. MAP generates the reports and proposals to meet your configuration. Click Finish when the reports have been generated. Reports are located in the MAP folder under your Documents folder in a folder called MAP_Results. Two reports are created. One is in Excel format and the other is in Word format. The Excel file outlines the recommendations and the Word file outlines the virtualization proposal. Carefully review the contents of each. You can rely on these reports to proceed with your implementation.

NOTE VIRTUALIZATION REPORTS

The reports generated in this practice are based on only one hour of performance data. Make sure you run a long-term performance assessment before you rely on the results from the virtualization reports.

Quick Check

1. What are the three possible scenarios for the deployment of Hyper-V?
2. How can the Microsoft Assessment and Planning tool help in Hyper-V deployment?

Quick Check Answers

1. The three possible scenarios for moving to Hyper-V are:
 - A move from a traditional physical infrastructure to a new server virtualization infrastructure and then the conversion of existing workloads to VMs.
 - Organizations that already use software virtualization (Virtual Server or VMware Server) will implement new host servers with Hyper-V and perform a VM conversion to Hyper-V VMs.

- Organizations that already use hardware virtualization (Citrix XenServer or VMware ESX) will implement new host servers with Hyper-V and perform a VM conversion to Hyper-V VMs.
2. MAP can help Hyper-V implementations in three ways. First, it can scan the entire network to generate a server inventory. Second, it can collect performance information on all of the identified systems. Third, it can provide a Hyper-V server sizing assessment based on the captured performance data.

Lesson 3: Implementing Windows Server 2008 for Hyper-V

When you prepare to deploy Windows Server 2008 Hyper-V, you basically use the same process you would normally use to install Windows Server 2008 x64 on a physical computer. However, since this server will be used as a host server, you need to take special considerations into account.

After this lesson, you will be able to:

- Understand the requirements for a Hyper-V implementation.
- Perform the Windows Server 2008 installation.

Estimated lesson time: 30 minutes

Selecting the Right Hardware for Hyper-V

Another important aspect of any Hyper-V implementation is the proper selection of hardware. Hyper-V is built to run on Designed for Windows Server hardware, and because it runs exclusively on x64 hardware, it requires digitally signed device drivers to operate properly. There is good reason for the signed driver requirement. Signed drivers have passed the validation program Microsoft has designed for all hardware that gains the Designed for Windows logo. This validation program ensures that the drivers are stable and operate properly under any circumstance. After all, you do not want to have your Hyper-V host server fail because of a faulty driver—each host server failure can easily cause multiple virtual machine failures. This is why you need to select appropriate hardware and tested device drivers for your host server configurations.

Validating if an x64 system includes Intel VT or AMD-V

First and foremost, your server hardware must support hardware-assisted virtualization, which means either an Intel VT or an AMD-V processor. In addition, the processor must support DEP because it provides hardware support for detecting and preventing the execution of code in program data areas, stopping the most common buffer overflow errors malicious attackers try to run when they want to take over a system. Note, however, that these settings must be enabled in the system's BIOS before they can be accessed by Hyper-V. It is always good practice to verify that the setting is in fact enabled in the BIOS before performing any Hyper-V installation.

Several free utilities validate whether your server's processor will be able to run Hyper-V. Both the AMD and the SecurAble utilities are executables and do not require installation. The Intel utility is in Windows Installer format and must be installed on a server to run.

AMD offers a free utility that verifies their processors at http://www.amd.com/us-en/assets/content_type/utilities/AMD-V_Hyper-V_Compatibility_Check_Utility.zip. This utility is very useful because it not only tells you whether your processor includes AMD-V, but it also tells you whether it is enabled in the BIOS settings.

Intel offers a similar utility called the Intel Processor Identification Utility. This utility is available at <http://www.intel.com/support/processors/piu>. Use the CPU Technologies tab to verify whether your processor supports Hyper-V.

Another useful utility that examines either AMD or Intel processors is called SecurAble from Gibson Research Corporation. SecurAble checks for three key factors: whether the processor is 64-bit, whether DEP is on, and whether hardware-assisted virtualization is available. Although it is not specifically designed for Hyper-V compatibility verification, it is quite handy. Find it at <http://www.grc.com/securable.htm>.

Determining Hyper-V Characteristics

The actual server hardware you select must meet additional key requirements for Hyper-V. Table 1-6 outlines the characteristics of Hyper-V. Keep these in mind when planning to purchase new systems or refurbish existing systems to run Hyper-V.

TABLE 1-6 Key Hyper-V Characteristics

REQUIREMENT	DESCRIPTION
Windows Server 2008 edition	The Windows Server 2008 edition must include Hyper-V; must be x64; and must be either Standard, Enterprise, or Datacenter.
Free edition	You can also rely on the free Hyper-V server to create host systems.
Processor	Use an x64 processor with hardware-assisted virtualization and DEP. Both must be enabled in the system BIOS. Hyper-V R2 supports CPU core parking which allows it to turn off processor cores that are not in use, reducing the overall host server power consumption.
Number of logical processors	Hyper-V can access up to 24 logical processors—processor cores or hyper-threads—on the host server when running on any edition of Windows Server 2008. Note that this value was changed in October 2008 when Microsoft updated Hyper-V in support of Intel's six-core processors. The original release of Hyper-V could only access 16 logical processors. Hyper-V R2 can access up to 64 logical processors and support new eight-core processors. Also note that this access is different from the capabilities of Windows Server 2008 on its own, which can access several more logical processors when running the Enterprise or Datacenter editions. You can run Hyper-V on configurations with more than 24 logical processors, but these configurations are not supported.
Virtual machines per logical processor	Hyper-V can run up to 8 single-processor virtual machines per processor core. However, each machine must have access to its own independent memory. For example, if your system has four logical processors and can therefore run up to 32 single-processor VMs, the number of VMs will still be limited by the amount of physical RAM on the system and the amount of RAM you assign to each VM.

REQUIREMENT	DESCRIPTION
Number of VMs	Given the appropriate hardware configuration, Hyper-V can support up to 192 concurrent running virtual machines and up to 512 configured VMs per host server. Note that the original number of concurrent VMs was 128 but was updated to 192 when Microsoft updated Hyper-V in October 2008. Hyper-V R2 can run up to 256 concurrent virtual machines.
Virtual machine architecture support	Hyper-V provides support for x86 (32-bit) and x64 (64-bit) virtual machines.
Host server memory	Physical RAM controls the amount of virtual machines a host server can run. The recommended minimum is 8 GB, but Hyper-V hosts running the Standard edition can access up to 32 GB of RAM and host servers running the Enterprise or Datacenter editions can access up to 1 terabyte of RAM. Note that the accessible RAM for the Enterprise and Datacenter editions is different than the accessible RAM for Windows Server 2008 x64 itself, which is 2 terabytes of RAM.
Virtual machine memory	VMs running Windows Server 2008 Enterprise or Datacenter can access up to 64 GB of RAM. VMs running the Standard edition can access up to 31 GB of RAM.
Networking: Adapters	Virtual machines running on Hyper-V can access up to 12 virtual network adapters per machine consisting of 8 synthetic network adapters and 4 emulated network adapters. Each adapter can use either a static or dynamic MAC address. Each can also be assigned a virtual local area network (VLAN) channel to control its traffic.
Networking: Switches	You can create an unlimited number of virtual switches in Hyper-V and you can assign an unlimited number of virtual machines per switch.
Physical storage	Hyper-V can operate with three different types of storage: ■ Direct-attached storage (DAS) can be in the form of Integrated Drive Electronics (IDE), also known as Parallel Advanced Technology Attachment (PATA), Serial Advanced Technology Attachment (SATA), exterior SATA (eSATA), Serial-Attached SCSI (SAS), Small Computer System Interface (SCSI), Universal Serial Bus (USB), or FireWire. ■ Network-attached storage through the server message block (SMB) protocol. ■ Storage Area Networks (SAN) through the iSCSI, Fibre Channel, or SAS protocols. SANs or NAS devices are required for fault-tolerant configurations.

REQUIREMENT	DESCRIPTION
Virtual Hard Disks	Fixed and dynamically expanding virtual hard disks are limited in size to 2,040 GB each. The total amount of storage per VM using virtual hard disks is 512 terabytes. The size of pass-through disks—physical disks that are directly linked to virtual machines—is only limited by the operating system running in the VM.
Virtual Storage Controllers	Up to four IDE connections per VM. At least one IDE device must be assigned to each VM to boot. Up to 4 SCSI connections per VM and up to 64 devices per SCSI connection for a total of 256 possible disk connections.
Virtual Machine Snapshots	Each VM can have up to 50 snapshots.
Virtual CD/DVD	Up to three virtual CD/DVD devices can be assigned to each VM. One IDE controller must be reserved for the boot device. Only one VM can access the physical or pass-through CD/DVD device at a time for security reasons. Hyper-V can also access .iso files as virtual CD/DVD devices.
Virtual Serial (COM) Ports	Each VM can access up to 2 virtual COM ports to communicate with physical devices either locally or remotely through a serial named pipe.
Virtual floppy drive	Each VM supports up to 1 virtual floppy drive. Hyper-V does not support access to physical floppy devices. Floppy devices must be in the form of .vfd files.
Resource pool	Resource pools link host servers together to provide high availability for the VMs they run. Because Hyper-V relies on Windows Server 2008 to create resource pools, the maximum number of hosts in a given resource pool is 16 or 16 nodes in a cluster.



EXAM TIP HYPER-V CHARACTERISTICS

Pay close attention to the items in Table 1-6—they are definitely part of the exam.

UPDATE ALERT HYPER-V CHARACTERISTICS

Microsoft is constantly updating Hyper-V and other virtualization offerings as they compete with other virtualization vendors. Because of this, many of the values in Table 1-6 have been updated to reflect current Hyper-V capabilities. Yet the exam was created based on the original features of Hyper-V. Pay special attention to the original values cited in this table. For example, the number of supported logical processors and the maximum number of concurrent running VMs are both values that have changed since the creation of the exam and these values have also changed with Hyper-V R2.

MORE INFO HYPER-V RAM CALCULATOR

Aidan Finn, an MVP in System Center Configuration Manager, put together a handy spreadsheet outlining how to calculate RAM for host servers running Hyper-V. Find it at <http://joeelway.spaces.live.com/Blog/cns!2095EAC3772C41DB!952.entry>.

Note that although there is a significant performance difference between SCSI and IDE disks on physical systems, there is little difference in a virtual environment running on Hyper-V. The VSC running in enlightened guest operating systems provides highly similar throughput for both storage protocols. Therefore, you can configure virtual machines to boot and operate through virtual IDE drives and expect a higher level of performance than on a physical machine configuration.

Keep the information in Table 1-6 in mind when selecting host hardware. Ideally, you will configure your hosts so that they will support an appropriate number of virtual machines. Although this number is difficult to determine under most circumstances, you can rely on the rule of thumb that many organizations aim for up to 10 VMs per host; or, you can rely on an assessment tool to assist you in determining how many VMs you should assign to each host server. Using this assessment tool is the next topic in this lesson.

Host Server Resource Usage

Given the various characteristics of Hyper-V and given the results of your MAP assessments, you can begin to plan for resource usage of your Hyper-V systems. Although Hyper-V can run up to 192 single-processor virtual machines on a host server configuration that includes 24 logical processors, it is highly unlikely that you will actually do so. This is because you must take into consideration the potential overhead of the parent partition. Remember that the parent partition acts as the coordinating orchestrator for all child partition operations and because of this, it has some resource usage overhead of its own. Table 1-7 outlines considerations for the resource overhead of the parent partition.

TABLE 1-7 Potential Parent Partition Overhead

RESOURCE	REQUIREMENT
Logical processor core	You should reserve at least one logical processor core per host server for the operation of the parent partition. This way, the parent partition will not have to content for processor resources with the child partitions it manages. After all, Hyper-V's parent partition runs Windows Server 2008 and this operating system actually runs best with two logical processor cores when managing other server roles.

RESOURCE	REQUIREMENT
Memory	You should reserve at least 512 MB of RAM for the operation of the parent partition if it is running a Server Core installation of Windows Server 2008. 512 MB of RAM is the bare minimum RAM required for Windows Server 2008. If your parent partition is running the full installation, you should allocate between 768 and 1,024 MB of RAM. Once again, you do not want the parent partition to compete for resources with child partitions. However, Microsoft recommends allocating a minimum of 2 GB of RAM for the parent partition because it also hosts drivers and agents and may require more base RAM to operate. In addition, each child partition you run will require 32 MB of overhead memory as well as 8 MB of RAM for any additional memory it has access to. As a rule of thumb, allocate 2 GB of RAM to the parent partition plus 40 MB for each child partition. This will provide the best operation for your Hyper-V host. Hyper-V R2 can rely on Second Level Address Translation (SLAT) which allows it to leverage new processor features to improve performance and reduce the hypervisor load. This will reduce the hypervisor load to about 1 percent of total system memory, letting you allocate more RAM to VMs.
Network adapters	You should reserve one network adapter for management operations. The parent partition must be connected to this network. A second NIC is required to support virtual machine networking. A third is required if you rely on shared storage for VM storage and you use the iSCSI protocol to access this storage. In addition, if you create a failover cluster, you will need two NICs for the cluster itself: one for public traffic and one for private heartbeat traffic. The public traffic NIC can double as the VM networking NIC.
Storage	The parent partition is installed as the boot operating system for a Hyper-V server. You can choose from two strategies here. If you use DAS, you should at least mirror two local hard disks to provide a first line of protection for the parent partition. Using DAS, however, means that you must use traditional installation procedures to prepare a new server. With Windows Server 2008, you can also boot the parent partition from remote storage. In this case, you can use your remote storage's utilities to generate new parent partitions—through duplication technologies—when a new host server is required.

Keep the considerations in Table 1-7 in mind when you plan for resource usage on your Hyper-V hosts. Reserving some core resources for the parent partition is a good practice that will hold in good stead over time. Host server operation is critical if you want your VMs to remain stable and in good operational health.

Hardware, Software, and Driver Compatibility

Ideally, your host server hardware will be listed in the Windows Server Hardware Catalog (<http://windowsservercatalog.com>). In fact, one of your first preoccupations should be whether you intend to run fault-tolerant host servers to ensure virtual machine availability. If so, you should look to hardware that has been validated for the Failover Clustering service in Windows Server 2008. Fortunately, Microsoft has introduced the Failover Cluster Configuration Program (FCCP) with Windows Server 2008. This program changes the way customers procure hardware for clustering solutions. In this case, manufacturers list validated cluster configurations on their own sites instead of on the Windows Server Catalog site. This helps customers more easily access configurations that have already been completely validated to run Windows Server 2008. A list of partners with validated configurations can be found at <http://www.microsoft.com/windowsserver2008/en/us/clustering-partners.aspx>. Partner configurations range from low-cost two-node clusters to more expensive multi-node datacenter configurations.

In addition, Windows has historically had instability issues related to driver and software design. In an effort to ensure that Windows Vista and Windows Server 2008 are even more stable than any previous releases of Windows, Microsoft has tightened the driver and software signing requirements for this operating system. Driver and software signing ensures the quality of the components administrators install on their servers and workstations. In fact, the following Windows components now require digital signatures:

- x64 versions of Windows Vista and Windows Server 2008 require all components that are loaded into the operating system kernel—the core part of the operating system that runs at ring 0—to include Kernel Mode Code Signing. This ensures that when components operate in the core of the operating system, they are known to behave properly.
- Boot start drivers or drivers that load at boot time must all contain an embedded signature.
- Any components that are downloaded through Internet Explorer for installation must also be digitally signed.
- Any unsigned component requires administrative approval—read operating system procedure override—to install. Therefore, when you choose to install unsigned and potentially unstable software or drivers, you become responsible for making this choice.

Digital signing relies on Public Key Infrastructure (PKI) certificates that are embedded within the component. These certificates must originate from a trusted publisher or a publisher that is included in the default Windows and Internet Explorer list of trusted entities. Self-signed and potentially untrusted certificates are not supported.

Because Hyper-V runs on x64 hardware, it benefits from trusted kernel and other components. Therefore, host servers running Hyper-V should provide stable and robust operation, but only as long as you comply with the guidelines Windows Server 2008 provides. If you opt to install unsigned drivers on your host servers, you can destabilize your host servers. You'll agree that with host servers running multiple VMs in child partitions, introducing any element that can potentially destabilize them is a pointless exercise.



EXAM TIP DIGITAL SIGNATURES

Watch out for questions related to driver and software signing in the exam. Creating potentially unstable host servers is a pitfall that should be avoided at all costs.

Installing Windows Server 2008

As an IT professional focused on Microsoft technologies, you are already familiar with the Windows installation process, and if you have experience with installing Windows Vista, you are also familiar with the installation process for Windows Server 2008. Both use the same installation engine. Windows Server installations are based on the Windows Preinstallation Environment (Windows PE) engine, which is a scaled-down version of Windows that can boot from removable media—CDs, DVDs, or USB disks—and load into RAM to perform bare-metal installation operations.

In addition to moving the installation process to integrate with Windows PE, Microsoft has modified the Windows Vista and Windows Server 2008 installation to remove all barriers to installation completion. In previous versions of Windows, administrators were required to provide input into the installation at various stages of the process. Today all input is provided at the beginning of the installation. As soon as all input data is provided, the installation completes on its own. Administrators only need to provide very basic information:

- Language to install
- Time and currency format
- Keyboard or input method

Then, after you've selected Install Now, you provide the product key for the installation. This product key determines which product will be selected for installation. You then select whether you want to perform a full installation or a Server Core installation, choose the location of the installation—you may have to use advanced functions to create disk partitions—and you're off and running.

Windows now uses an image-based setup (IBS) that copies an installation image to the system disk and then decompresses it to begin the actual configuration based on the discovered devices on the system. Then, when the operating system is installed, you proceed to the actual system configuration: changing administrative passwords, setting firewall configurations, and much more.

Identifying Deployment Options

As you can see, this installation process is fairly basic. But as a resource pool administrator, you need to delve deeper into the installation process. Basically, resource pool administrators need to determine which process they intend to rely on to create host servers when they are required. In the dynamic datacenter, host servers are provisioned on an as-needed basis when the existing pool of servers can no longer provide adequate resources for the virtual machines you run. Because of the dynamic nature of the datacenter, this provisioning process must be as smooth and as efficient as possible. It may be adequate for a small organization to create new host servers manually because the need seldom arises, but it is unacceptable to do so in larger datacenters.

Dynamic systems provisioning must rely on some form of automation. Windows Server 2008 supports four different installation modes:

- Manual installation, which must be used at least once to discover how the installation process actually works. This process is then followed with a manual post-installation system configuration.
- Unattended installation through automated response files. Windows now relies on a single Unattend.xml file for input into all automated installations. This file can be edited and prepared through the Windows System Image Manager which is part of the Windows Automated Installation Kit (WAIK), a downloadable installation support tool. The advantage of using answer files is that they can provide both pre- and post-installation input and configuration settings, making the process simpler for administrators.
- Disk imaging with the System Preparation Tool (SysPrep.exe). This process relies on the creation of a reference computer that is completely configured, then depersonalized through the SysPrep tool. Then, you capture an image of this computer. This image is then used as the installation point for other servers. This process relies on the new Windows image-based installation, but in this case, you use a custom image instead of the default image included in the Windows distribution DVDs. Once again, you rely on the WAIK to create the custom image and an Unattend.xml file or a manual process to customize it each time you deploy it.
- Remote installation through the Windows Deployment Services (WDS), one of the 17 default server roles in Windows Server 2008. WDS also relies on custom images, but can remotely deploy them to bare-metal systems. WDS also relies on Windows PE to boot into the installation process for any server that does not already include an operating system. WDS includes several additional features, such as multicast image deployment, distributed deployment structures for complex environments, and granular distribution control, but in most cases, these features are not required for resource pool creation.

One additional deployment option is available. If the parent partition for a server is hosted on a SAN and the system is configured to boot remotely from SAN, you can use the SAN's logical unit duplication tools to create and depersonalize an image of this parent partition.

Then, when you need to add a new host server, you create a copy of this image, attach it to the new host, customize it, and you have a new host server. In large organizations, this may be the best method to use because it can provide very fast host server provisioning.

Resource pool administrators therefore need to identify which process works best for their environments. Smaller organizations may work well with the Unattended installation process, but medium-sized and larger organizations have to look to either the system image or remote deployment process because of the speed of the deployment.

Identifying Required Host Server Configurations

Resource pool administrators also need to determine how they intend to configure their host servers. Traditionally, host servers are configured in resource pools—or in the case of Windows Server 2008, in failover clusters—so that they can provide high availability for the virtual machines they run. It makes sense: If your host servers run 10 or more virtual machines, you want to make sure that the virtual machines continue to operate no matter what happens to the host server. Using failover clusters, you can move all of these VMs from one cluster node to another through Hyper-V's Quick Migration feature. Some downtime is associated with this move, but it is better to have a few seconds of downtime than to have all virtual machine services fail.

The Windows Server 2008 Failover Cluster service supports two modes (see Figure 1-15):

- **Single-site clusters** Failover clusters use shared storage in a single site to provide high availability. Because all nodes of the cluster are tied to the same shared storage containers, they can provide failover for each other in the event of a hardware failure on a cluster node.
- **Multi-site clusters** Failover cluster nodes are located in different sites and provide multi-site failover services for each other. In this case, each node hosts its own copy of the data and relies on this copy to provide continuity services. Because of this, there is no requirement for shared storage and each node can in fact rely on DAS to host data. Because each node in the cluster must have duplicate data, multi-site clusters must also rely on a replication engine to ensure that all node data is synchronized at all times. This replication engine must be able to duplicate data while it is being used and must therefore be able to replicate open data objects. Right now, multi-site clusters must rely on third-party replication tools.

Multi-site clusters can provide better failover support than single-site clusters because if an entire site fails, your services will continue to operate. In addition, multi-site clusters provide simpler host server configuration designs because they can rely on DAS instead of shared storage. DAS is faster and much easier to implement than shared storage. However, multi-site clusters also require the acquisition and implementation of a third-party replication tool and therefore may be cost-prohibitive for certain organizations.

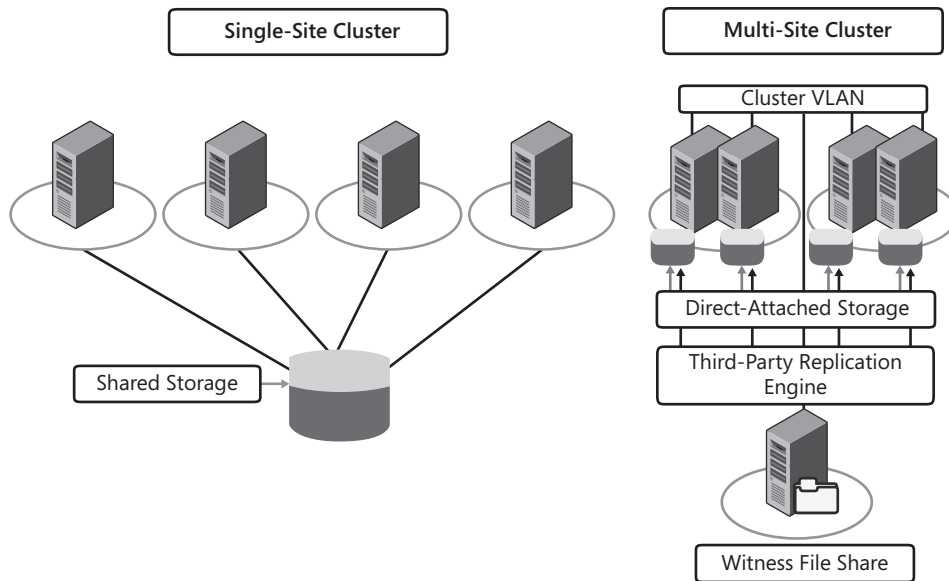


FIGURE 1-15 Single- versus multi-site cluster configurations.

NOTE LIVE MIGRATION

The first iteration of Hyper-V requires downtime to move a VM from one node of the cluster to another. In Windows Server 2008 R2, Microsoft introduces Cluster Shared Volumes (CSV) which will provide support for *live migration*, or the ability to move a virtual machine from one node to another without downtime. CSVs are a function of shared storage, which means that they will only support single-site clusters.

However, resource pool administrators must also take into consideration the support policy for the product they intend to virtualize. Many products find it quite acceptable to rely on host server clustering to provide high availability for the services running in the virtual machine, but some do not. For example, the Microsoft Exchange Server team has posted its official support policy for configuring high availability in virtual machine environments. Remember that virtual machines emulate all of the features of a physical machine and because of this, Windows Server workloads such as Exchange Server can also take advantage of failover clustering within the virtual machines themselves. This is the strategy the Exchange Server team has opted for. They do provide support for both Hyper-V and validated server virtualization platforms, but they do not provide support for host server clustering, nor do they provide support for live migration features. Instead, they provide support for creating a combination of a multi-site cluster in a single site through the Cluster Continuous Replication (CCR) feature of Exchange. CCR provides the replication engine required for the multi-site cluster and all failover processes are maintained by Exchange itself. This strategy limits the

possibility of losing e-mail data. Host clusters that perform a failover are never aware of the state of an application contained in a VM during the transfer and therefore may cause some data loss. When you rely on Exchange to perform the failover, it will always be aware of the latest state of the Exchange mailbox database.

MORE INFO SUPPORTED VIRTUALIZATION FOR EXCHANGE SERVER

For more information on the supported Exchange virtualization strategy, look up <http://go.microsoft.com/fwlink/?LinkId=124624>.

Because of these support policies, resource pool administrators will find that they need to create and maintain three different types of host server configurations:

- Stand-alone hosts will be required to support certain products when virtualized.
- Single-site clusters will be the most common host server configuration.
- Multi-site clusters can provide entire site failure protection.

Take the time to analyze the support policy for the products you want to virtualize before you make your final recommendations on host server configurations. If you decide—as you should—that you want to create single-site clusters for some of your host server configurations, keep in mind that single-site clusters must use shared storage and that clusters in general must be designed to have spare resources so that they can provide failover for other nodes in the event of a hardware malfunction (see Figure 1-16). In addition, take the time to determine the best method to automate Hyper-V deployment given the needs of your organization.

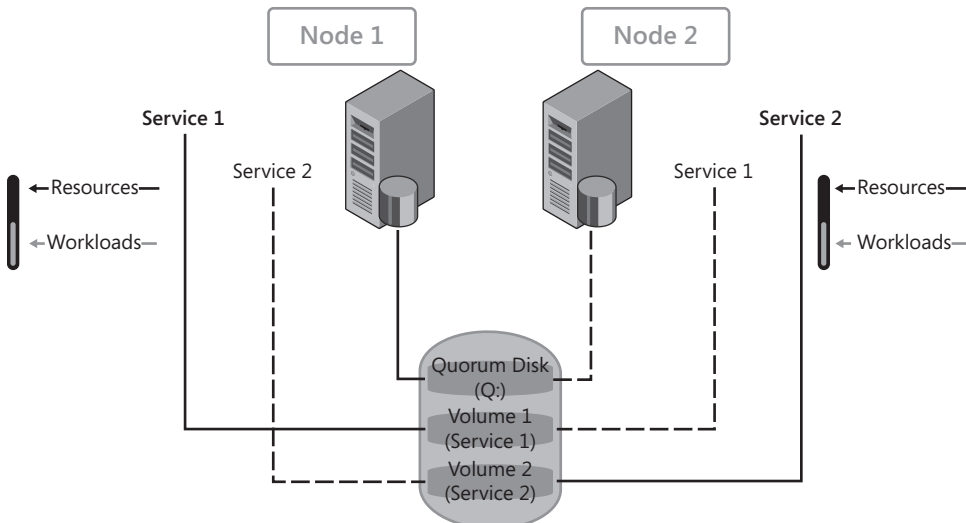


FIGURE 1-16 Single-site clusters rely on shared storage. Clusters in general require spare resources in order to provide failover services.

MORE INFO CLUSTERING HOST SERVERS AND VIRTUAL MACHINES

Fault-tolerance strategies for host servers are covered in Chapter 3, “Completing Resource Pool Configurations,” as you finalize your host server infrastructure. Fault-tolerance strategies for virtual machines are covered in Chapter 10, “Ensuring Virtual Machine High Availability,” as you look to business continuity strategies for your virtualization environment.

PRACTICE Prepare for Hyper-V Deployment

This practice consists of two exercises. The first exercise looks at the full installation of Windows Server 2008 in preparation for the installation and configuration of the Hyper-V role. The second exercise looks at the installation of Server Core on another server in preparation of the installation and configuration of Hyper-V in a Server Core environment. You will rely on these two machines to perform further exercises as you move through the lessons in this guide.

EXERCISE 1 Install Windows Server 2008

In this exercise you will install Windows Server 2008 as a full, graphical installation on a host machine. The host machine should be a physical machine and should be configured according to the recommendations outlined in the Introduction.

1. Obtain an installation DVD for Windows Server 2008. Insert this DVD into the drive of your computer system. Ideally, no pre-existing operating system will be found on this server, but if there is one, use the installation to replace it. Note: You can download an evaluation version of Windows Server 2008 from <http://www.microsoft.com/windowsserver2008/en/us/trial-software.aspx>.
2. Boot the server and select to boot from the DVD at the prompt.
3. When the Windows Setup screen appears, select English as the language to install, English (United States) as the time and currency format, and US as the keyboard or input method. Click Next.
4. Click Install Now.
5. Do not enter a product key at the product key page. This will let you evaluate Windows Server for up to 60 days and can be extended to 240 days, which should be sufficient for the purposes of preparing for the exam. Click Next. Answer No to the product key insertion prompt.
6. Select Windows Server 2008 Enterprise (Full Installation) and select I Have Selected The Edition Of Windows That I Have Purchased. Click Next.
7. Select I Accept The License Terms and click Next.
8. Choose Custom (Advanced).
9. The next screen lets you prepare custom partitions to host the installation. Because this machine should be linked to shared storage, you can use the entire local partition for the installation. Click Next.
10. The installation proceeds and will reboot the server until the installation is complete.

EXERCISE 2 Install Windows Server 2008 Server Core

In this exercise you will install Windows Server 2008 as a Server Core installation on a host machine. The host machine should be a physical machine and should be configured according to the recommendations outlined in the Introduction.

1. Obtain an installation DVD for Windows Server 2008. Insert this DVD into the drive of your computer system. Ideally, no pre-existing operating system will be found on this server, but if there is one, use the installation to replace it.
2. Boot the server and select to boot from the DVD at the prompt.
3. When the Windows Setup screen appears, select English as the language to install, English (United States) as the time and currency format, and US as the keyboard or input method. Click Next.
4. Click Install Now.
5. Do not enter a product key at the product key page. This will let you evaluate Windows Server for up to 60 days and can be extended to 240 days, which should be sufficient for the purposes of preparing for the exam. Click Next. Answer No to the product key insertion prompt.
6. Select Windows Server 2008 Enterprise (Server Core) and select I Have Selected The Edition Of Windows That I Have Purchased. Click Next.
7. Select I Accept The License Terms and click Next.
8. Choose Custom (Advanced).
9. The next screen lets you prepare custom partitions to host the installation. Because this machine should be linked to shared storage, you can use the entire local partition for the installation. Click Next.
10. The installation proceeds and will reboot the server until the installation is complete.

Quick Check

1. Which hardware component is an absolute requirement for Hyper-V and how can you verify that it is enabled before performing a Hyper-V installation?
2. How many single-processor virtual machines can Hyper-V run and how many logical processors can a host server include?
3. What is recommended in terms of memory for the parent partition if it is running on a Server Core installation? If it is running on a Windows Server 2008 full installation?

Quick Check Answers

1. The server processor must support hardware-assisted virtualization, such as Intel VT or AMD-V, and this setting must be enabled in the BIOS before performing a Hyper-V installation.

- 2.** Hyper-V can run up to 192 single-processor virtual machines on a host server configuration that includes 24 logical processors. However, because each machine requires access to its own memory, it is highly unlikely that you would ever use such a configuration.
- 3.** You should reserve at least 512 MB of RAM for the operation of the parent partition if it is running on a Server Core installation of Windows Server 2008. If your parent partition is running on a full installation, you should allocate at least 768 to 1,024 MB of RAM to the parent partition.

Case Scenario: Preparing for Server Virtualization

In the following case scenario, you will apply what you’ve learned about implementing Hyper-V. You can find answers to these questions in the “Answers” section on the companion CD which accompanies this book.

You have been designated as the resource pool administrator for Lucerne Publishing, a medium-sized organization that has offices in New York, Los Angeles, San Remo, Philadelphia, Newark, and Dallas. As part of your first activities, the IT department has asked you to look into Hyper-V as a virtualization platform and to examine the process required to move to a Hyper-V infrastructure. In addition, they have asked you to plan out the configuration of a typical host server. In particular, they want you to outline the number of CPUs, number and type of hard disks, and amount of memory required in a host server that would run up to five virtual machines running various networked services. To facilitate the process, the department has provided you with a table outlining the requirements for the host server as well as the requirements for each of the five virtual machines. Table 1-8 outlines these requirements.

TABLE 1-8 Parent and Child Partition Requirements

PARTITION	REQUIREMENT
Parent partition	CPU: 1 logical processor RAM: 1 GB Disk Space: 40 GB
Child Partition 1	CPU: 2 logical processors RAM: 4 GB Disk Space: 40 GB
Child Partition 2	CPU: 2 logical processors RAM: 2 GB Disk Space: 40 GB
Child Partition 3	CPU: 4 logical processors RAM: 4 GB Disk Space: 100 GB
Child Partition 4	CPU: 1 logical processor RAM: 1 GB Disk Space: 40 GB
Child Partition 5	CPU: 1 logical processor RAM: 2 GB Disk Space: 40 GB

1. What type of system would you recommend?
2. How many CPUs and how many CPU cores are required?
3. What type of storage would you recommend for this host server?
4. How much memory should the host server include?
5. How does your recommendation change if you want to include fault tolerance for the host server?

Suggested Practices

You can perform several practices to prepare for this section of the exam. First, you should review some reference information to complement what you have seen in this chapter. Second, you should take a practice test. Do not take the entire test. Instead, concentrate on the objective in this chapter.

Windows Server 2008 Installation

- **Practice 1** You should take the time to become familiar with both installations of Windows Server 2008—full installation and Server Core.
- **Practice 2** Take a look at the automated deployment mechanisms for Windows Server. If you have taken other IT Pro exams on Windows Server 2008, look up the sections on deployment automation and review the approaches that are available. This will help you better understand how you can deploy Hyper-V servers in your own environment.

Microsoft Assessment and Planning Tool

- **Practice 1** You should also practice performing assessments with the Microsoft Assessment and Planning tool. MAP is a great addition to any Hyper-V implementation because it provides so much input into the process. Play with various lengths of time for performance assessments. Use different values in your host server configurations in the virtualization assessment. Closely examine the results of each assessment to gain a better understanding of how this information can provide input into your own virtualization projects.

Server Hardware Configurations

- **Practice 1** Finally, it is a good idea to look up the systems your hardware manufacturer of choice suggests for the operation of Hyper-V. Most systems range widely in price from very low-cost systems to systems that cost tens of thousands of dollars. Determine which would best suit your organization's needs and become familiar with their potential configurations.

Chapter Summary

- The fully functional Hyper-V role can be found in Windows Server 2008 Standard, Enterprise, and Datacenter x64 editions. This role must run on a 64-bit system with both hardware-assisted virtualization and Data Execution Prevention (DEP) enabled.
- The Hyper-V role can be run on the full installation or the Server Core installation of Windows Server 2008.
- The Hyper-V architecture uses a Virtual Service Provider/Virtual Service Client (VSP/VSC) or client architecture to provide hypervisor services to the virtual machines it supports.
- Microsoft offers a free version of Hyper-V named Microsoft Hyper-V Server 2008. This version is based on the Standard edition of Windows Server 2008 and it is limited to 32 GB of RAM. Hyper-V Server relies on the Server Core interface. Microsoft recommends using this version in test and development environments, for basic server consolidation, or in branch office consolidation scenarios.
- To move to a server virtualization infrastructure you should rely on a process that includes several activities: determining the possible scenarios, preparing and deploying the host servers, preparing the host server and VM management infrastructure, securing and protecting the host servers, and moving on to resource pool and virtual machine administration.
- Before installing Hyper-V you need to select the right hardware based on assessed requirements. In addition, the host server hardware should be listed in the Windows Server Hardware Catalog to provide the very best stability.

Configuring Hyper-V Hosts

The next step in the resource pool planning and deployment process is to configure Hyper-V and prepare it for remote administration. As you saw in Chapter 1, “Implementing Microsoft Hyper-V,” the Hyper-V installation is a multi-part process. Hyper-V was in beta when it shipped with Windows Server 2008, and as such it needs to be updated before you can run the release to manufacturing (RTM) version of the product. This will no longer be necessary when Service Pack 2 for Windows Server 2008 is released, but for any copies of the original, RTM version of Windows Server 2008 released in February 2008, the Hyper-V update is critical.

UPDATE ALERT SERVICE PACK 2

If you use Windows Server 2008 installation media that includes Service Pack 2, you will not need to apply several of the updates mentioned here. Verify the service pack description to make sure the updates mentioned in this chapter are included. Find this information at <http://support.microsoft.com/kb/948465>.

The update process is simple:

- Install Windows Server 2008, either with the full or the Server Core installation.
- Download and install the update.
- Enable the Hyper-V role.
- Configure Hyper-V for operation.
- Configure virtual networks for Hyper-V.

The last step deals with both the configuration of Hyper-V’s local settings—such as libraries for storing virtual hard drives and CD/DVD ISO source images—as well as configuration of the virtual networks Hyper-V uses to support child partition communications. Then, once these elements are configured, you configure Hyper-V for remote administration. Remote administration is an important part of the Hyper-V configuration because as a resource pool administrator, you’ll most likely need to centrally manage all Hyper-V host servers as a resource pool. To do so, each Hyper-V host must be configured to allow remote administration—especially remote access to the Windows Management Instrumentation extensions available in Hyper-V. This is the focus of this chapter.

Exam objectives in this chapter:

- Configure Windows Server 2008 for Hyper-V.
- Configure virtual networking.

Before You Begin

To complete this chapter, you must have:

- Access to a setup as described in the Introduction. At least two computers are required: one running a full installation of Windows Server 2008 and the other running Server Core. You prepared these computers in Lesson 3 of Chapter 1. In this chapter, you will continue the build process and finalize the configuration of these computers.

Lesson 1: Installing the Hyper-V Role

Chapter 1 outlined the requirements for Hyper-V servers as well as some tools, notably the Microsoft Assessment and Planning tool, which can help you better understand the requirements of your host servers. In addition, you performed the basic installation of Windows Server 2008 in preparation for the Hyper-V role. Now you can proceed to the initial configuration of the servers as well as the installation of the Hyper-V role.

After this lesson, you will be able to:

- Perform the initial configuration of Windows Server 2008. This configuration must address both the full and the Server Core installation.
- Obtain the Hyper-V update.
- Install and enable the Hyper-V role.

This lesson also covers the installation and initial configuration of Hyper-V Server, although this topic is not part of the exam.

Estimated lesson time: 30 minutes

Performing the Initial Server Configuration

Each server you deploy requires configuration before use. For example, Windows Server 2008 is installed by default with an Administrator account and a Guest account. The Guest account is disabled and the Administrator account has no password. As part of the initial configuration of your server, you must provide a password to the Administrator account. In fact, this password change is performed at the first logon. Other activities must also be performed before a server is deemed ready to host the Hyper-V role. These activities differ slightly depending on the installation type—full or Server Core—but in general, you must do the following:

- Set the Administrator password at first logon.
- Set the time zone for the server.
- Configure networking.
- Provide a computer name and join a domain.
- Configure automatic updates and update the server.
- Enable the Remote Desktop.
- Configure the Firewall and enable remote administration.
- Add additional features if required. For example, it's a very good idea to use BitLocker full drive encryption on the system drive for host servers that are in unsecured areas. Note, however, that when BitLocker is enabled on a remote server, you may require physical interaction with the server during reboots.

All of these initial tasks are available in a single interface in the full installation, the Initial Configuration Tasks (ICT) screen, which appears at first logon (see Figure 2-1). The ICT screen provides a single interface for the most common initial configuration tasks.

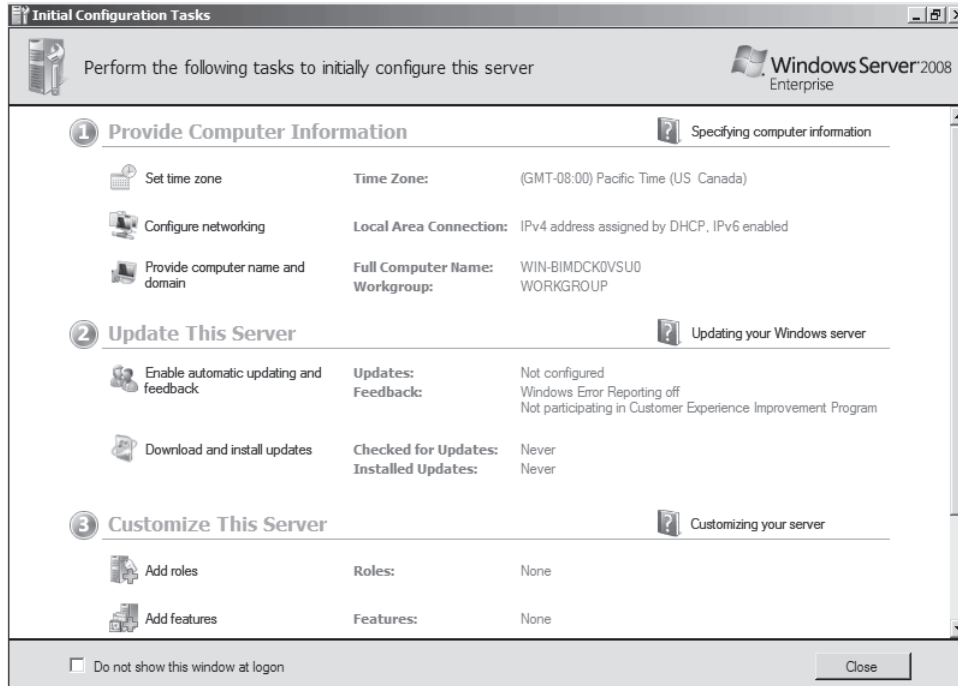


FIGURE 2-1 The Initial Configuration Tasks screen

NOTE SERVER CORE INSTALLATIONS

Because there is no graphical interface in Server Core, there is no correspond interface to the ICT screen. You must, however, perform the same basic configuration tasks on Server Core installations, but all tasks are manual. Note that you can automate this process through the use of answer files during the Server Core installation and thereby reduce the amount of manual configuration required on a Server Core computer.

Although the ICT screen offers a great way to perform some basic configuration tasks, it does not necessarily provide access to all of the interfaces you need to finalize an initial server configuration. Tasks you may want to perform but that are not included in ICT can include the following:

- Server activation.
- Renaming the default Administrator account.
- Creating a backup administrator account if your internal policies allow it or even request it.
- Setting the operating system display time to accelerate the reboot process.

- Setting default recovery options for the parent partition.
- Configuring the page file.
- Performing other required host server configurations. For example, you might need to install the Windows Recovery Environment (WinRE) on the system to simplify server recovery.
- You may also want to add additional administration tools on the server. Note, however, that the Windows Server Remote Server Administration Tools (RSAT) will only work on a full installation.
- Finally, to simplify the use of this system by other users, you might want to configure the user interface and the default user profile. Once again, this activity is only performed on the full installation.

You must perform each of these operations before you are ready to install and enable the Hyper-V role on the server.

Configuring the Full Installation for Hyper-V

Performing these initial configuration tasks on the full installation of Windows Server 2008 is relatively easy because you have access to a graphical interface for each option. At first logon, the system will present the Administrator account and request a password change. By default, the original Administrator password is blank. Log on with this blank password. The system will prompt for a password change (see Figure 2-2). Once the password has been set, you will be allowed to log on to the system and as soon as the logon process is complete, the Initial Configuration Tasks interface will open. Note that you can also create a password reset disk when the system allows you to change the password. Do so only if this is part of your internal security policy.



FIGURE 2-2 Setting the default Administrator password

Proceed as follows:

- Set the time zone for the server by using the link provided on the ICT.
- Configure networking. Once again, rely on the link in the ICT. Configure each of the network adapters on the server. Providing static IP addresses is a good practice on host servers because they manage so many virtual machines. Determine whether you want to use only IPv4 or whether you also want to use IPv6.
- Provide a computer name and join a domain. Once again, use the provided link. It is good practice to join host servers to a domain because domains support central security management for all servers. This facilitates host server access and simplifies role-based administration of the host systems. A reboot is required to complete this change.

NOTE RESOURCE POOL FORESTS

In medium to large organizations, you might consider using a utility forest for the host servers in the resource pool. Using a separate Active Directory Domain Services (AD DS) forest isolates the host servers from the production systems that are running in virtual machines. This limits host server access to resource pool administrators. End users do not need to interact with host servers in any way.

- Configure automatic updates and update the server. Once again, use the link provided in the ICT to perform these tasks. Make sure you enable additional updates and install all required updates.
- Enable the Remote Desktop. Remote Desktop is one of the best administration tools in Windows Server 2008. Enabling it facilitates server administration from any location in your network. Make sure you use the most secure settings for your Remote Desktop connections.
- Configure the firewall and enable remote administration. The Windows Firewall is an important part of the security settings of a host server. It must be enabled and you must make sure that remote server administration is allowed to pass through the firewall; otherwise you will not be able to use remote administration tools such as System Center Virtual Machine Manager 2008 with this host server. Once again, use the link in ICT to make this change.
- Add additional features if required. Keep the additional features on host servers to a minimum. For example, you will need to install and enable Windows Server Backup unless you plan to use a different backup tool. Use the links on the ICT to perform this task.

As soon as all of the tasks that are accessible through the ICT are complete, select the Do Not Show This Window At Logon check box and close the ICT. Proceed to the completion of the tasks that are not available in the ICT interface. As soon as you close the ICT, the Server Manager interface will be launched (see Figure 2-3).

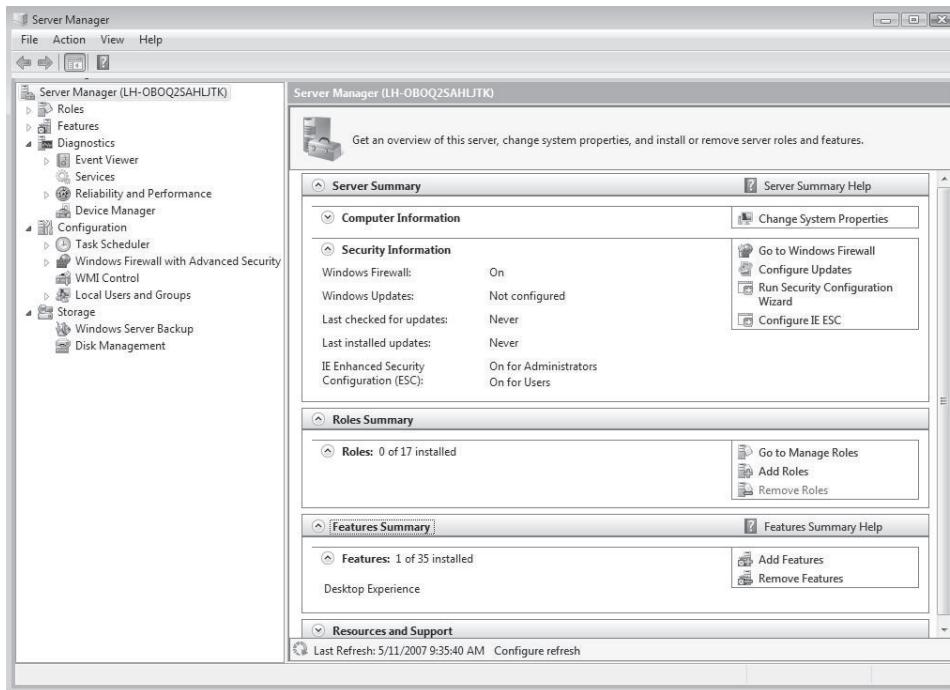


FIGURE 2-3 Using the Server Manager console

You can perform additional activities from this console:

- Server activation is one of the only activities that is not performed through Server Manager. Instead, it is performed in Control Panel by clicking System And Maintenance and then clicking System. This interface lets you both activate your server and change the product key.

Most other activities are performed through the Server Manager console:

- Renaming the default Administrator account is performed under the Configuration | Local Users and Groups | Users node of the Server Manager Tree pane. Use the shortcut menu on the Administrator account object to rename the account. Rename the account according to your organization's requirements.
- While you're in this section of Server Manager, you can create a backup administrator account if your internal policies allow it. The backup account is useful for updating the default user profile but it can also be used if for some reason the system administrator account is locked out. Make sure you make this account part of the local administrators' group.
- Set the operating system display time to accelerate the reboot process as well as the default recovery options for the parent partition. Both settings are found under the Change System Properties link in the Details pane of the home page of Server Manager. Once the System Properties page is open, click the Settings button under the Startup And Recovery section of the Advanced tab. Set the System Failure settings to your organizational standards.

- Use the same tab in System Properties to configure the page file. Click Settings under the Performance section. Click the Advanced tab and select Change. A good practice is to set the page file to an initial size of twice the amount of RAM on the system and set the maximum size to four times the RAM. In host servers that have a very large amount of memory, it is good practice to store page files on separate disk spindles to improve performance. Note that a minimal page file must be located on the system disk.
- Perform other required host server configurations. For example, you might need to install the WinRE on the system to simplify server recovery. This depends on your internal policy for server recovery. In many cases, organizations simply reinstall servers when they use an automated server deployment strategy, and in this case WinRE is not required. However, if you run virtual machines on direct attached storage on the server and you do not have backups or replicated copies of the VMs, a server repair will be essential. This is one more reason why VM placement on remote storage is a good practice. Note that to install WinRE on a host server you need two different partitions on the system drive.
- You may also want to add additional administration tools on the server. These tools are part of the Windows Server 2008 features. Add each feature as required.

NOTE RSAT FOR WINDOWS VISTA SERVICE PACK 1

To run the Remote Server Administration Tools on Windows Vista, you need the RSAT download, which was updated when Hyper-V was released to RTM. The RSAT download is available as part of article number 941314 from the Microsoft Knowledge Base. Download the RSAT update from <http://support.microsoft.com/default.aspx/kb/941314>, apply it to your system, and then add the feature.

- The last step in the configuration is to customize the user interface and update the default user profile. This activity can only be performed on the full installation. Make sure your server interface is updated as you need it, log off of the Administrator profile, and log on to the backup user account you created. Using the Change System Properties link on the Server Manager home page, click the Advanced tab and then click Settings under User Profiles. Copy the Administrator profile to the Default User profile. Accept the change. You can test the change by logging off of the backup administrator account, logging on to Administrator, using the same dialog box to delete the old backup administrator profile, and logging on to the backup administrator account again. It should be using the new profile. This last logon can be performed through the Switch User option instead of logging off of your administrator profile.

The server configuration is now complete. If you created this server as a reference server and intend to use it as a source for disk imaging and further server operating system distributions, it is ready for the system preparation command. Back up the server and keep the image in a safe place.

If this server is intended for production, you are ready to move on to the Hyper-V role installation.

Configuring the Server Core Installation for Hyper-V

The same configuration steps are required for Server Core installations, but because of the very nature of this installation version, the entire process for configuring the server is completely different. Everything is performed through the command line. Although you cannot configure Server Core with the same commands as the full installation, you can configure the full installation with the same commands as you would with Server Core.

MORE INFO SCREENCAST ON HYPER-V CONFIGURATION ON SERVER CORE

To view a screencast on how to configure Hyper-V on a Server Core installation, go to <http://go.techtarget.com/r/5927602/30819>.

You should primarily use Server Core installations for Hyper-V as they guarantee better performance than the full installation. Remember that each child partition must communicate through the parent partition for any response from hardware devices through the VMBus. If the root partition is running the full installation, responses may be delayed. Because Server Core provides a reduced footprint and a minimal set of services as compared to the full installation, its operation is optimized. In addition, because it includes fewer components, there are fewer components to update, providing a simpler and more stable platform for the root partition.

However, because Server Core configuration is performed solely through the command line, it is essential to enable remote administration of the server. This simplifies system administration and lets you control Hyper-V operations through the graphical Hyper-V administration tool.

Although the installation of Server Core is almost identical to that of a full installation, the post-installation configuration differs significantly. After the final reboot during setup, Server Core will ask you to log on and await input. Click **Other User**, type in **Administrator** as the user name, and use a blank password. The system will now ask you to change the password (see Figure 2-4). In this case, you must provide the old password, which is blank. As always, use a strong password. Once you are logged on, you are ready to proceed to the server configuration.

Each configuration operation requires the use of a different command-line script. Remember that Windows PowerShell does not work in Server Core because it relies on the Microsoft .NET Framework, which cannot be installed on Server Core because it has GUI dependencies. Note that Microsoft is changing this for Windows Server 2008 R2, but for now, Windows PowerShell can only perform remote operations on Server Core.

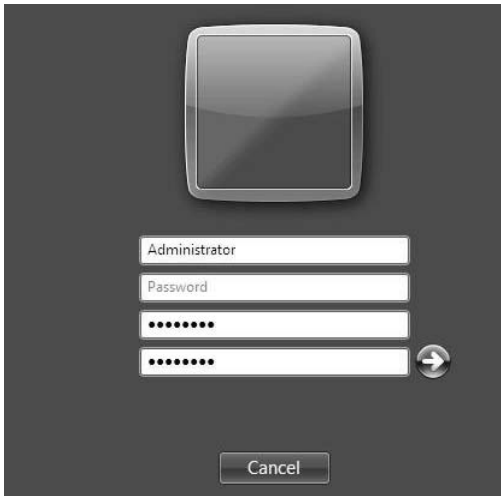


FIGURE 2-4 Server Core requires the old password to change the default Administrator account.

Perform the operations in the same order as for the full installation:

- Begin by setting the time zone and clock for this server. The time zone is changed through a Control Panel applet. This is a bit odd since there really is no graphical interface on Server Core. Use the following command to change the time zone:

```
control timedate.cpl
```

This launches the Time Zone applet and lets you change the time zone and time and date on the server. To view the date and time at the prompt, type the following command:

```
prompt $p$b$b$b$t$b$d$b$g
```

The result displays the user name, time, and date at the prompt (see Figure 2-5). Note that the `$b$b` combination in the prompt command adds a space, a pipe symbol, and another space between each item.

```
C:\Users\administrator | 14:27:08.14 | Mon 01/12/2009>
```

FIGURE 2-5 Displaying time and date at the command prompt

- Next, configure networking. To configure networking, you need to use the `netsh` command. First find out which network interfaces exist, then configure the IP address for the interface, and then assign Domain Name System (DNS) addresses in support of name resolution. In addition, you need to perform this operation for both IPv4 and IPv6. Begin with IPv4:

```
netsh interface ipv4 show interfaces
```

This will provide a list of the available interfaces running IPv4. Note the number shown in the IDX column for each interface. You need this number to configure the interface. Now use the `netsh` command to configure the interface:

```
netsh interface ipv4 set address name="ID" source=static address=staticIPAddress  
mask=SubnetMask gateway=DefaultGateway
```

ID is the number discovered in the previous command, and *staticIPAddress*, *SubnetMask*, and *DefaultGateway* are the values you need to assign for each.

Finally, add a DNS server address for the interface. You would normally configure at least two DNS addresses per interface to ensure redundancy for the name resolution service:

```
netsh interface ipv4 add dnsserver name=ID address=DNSIPAddress index=1
```

ID is the number of the interface and *DNSIPAddress* is the IP address of the DNS server you are adding.

Repeat the same commands for IPv6. Begin by finding the interface ID:

```
netsh interface ipv6 show interfaces
```

Make note of the IDs in the IDX column. Then use the following two commands to set the address and the DNS server(s):

```
netsh interface ipv6 set address interface="ID" address=IPv6Address  
netsh interface ipv6 set dnsserver name="ID" source=static address=DNSIPAddress  
register=both
```

Repeat these commands for each interface you want to configure. You can also review all of the network settings when you're done. Use the following command:

```
ipconfig /all
```

- Now that the network adapters are configured with static addresses, you can provide the computer name and domain:

```
netdom renamecomputer %computername% /newname:NewComputerName
```

You must reboot the computer to make this change take effect. Use the following command:

```
shutdown /r /t 3
```

You use the /t switch with a value of 3 seconds to speed up the process; otherwise, you need to wait a full minute for the shutdown to take effect. Once the system is rebooted, join a domain:

```
netdom join %computername% /domain:DomainName /userD:AdministrativeAccount  
/passwordD:Password
```

DomainName is the name of the domain you want to join, *AdministrativeAccount* is the name of an account with domain administrative privileges (or at least enough privileges to join the computer to the domain), and *Password* is the password for the account. Note that the administrative account should be in user principal name format—for example, *administrator@tandt.ws*. Reboot the computer again once this is done; otherwise, your other commands will not work.

- Enable and check for updates as well as enabling the Remote Desktop. Both of these steps are examples of commands that cannot be performed through the command line only and must rely on a custom script. This is why Server Core includes a custom script to help you perform some of the configuration tasks. This script is located in the System32 folder of your installation. You must change to this folder before using the script because the path to the script will not work otherwise. To find out how the script works, change folders and then type:

```
cd \Windows\System32
cscript scregedit.wsf /?
```

To set both automatic updates and remote administration, type:

```
cscript scregedit.wsf /AU 4
cscript scregedit.wsf /AR 0
```

To view your changes, type:

```
cscript scregedit.wsf /AU /v
cscript scregedit.wsf /AR /v
```

IMPORTANT UPDATES ON SERVER CORE

Updates do not quite operate the same way on Server Core as they do with the full installation, mostly because there is no Web browser in Server Core. One good way to verify updates on Server Core is through the Microsoft Baseline Security Analyzer (MBSA). MBSA can be found at <http://technet.microsoft.com/en-us/security/cc184923.aspx>. Download it and install it on a computer with a full graphic interface, and then use it to scan your Server Core computers. You can also rely on Windows Server Update Services (WSUS) to manage updates internally. Find out more about WSUS at <http://technet.microsoft.com/en-us/wsus/default.aspx>.

IMPORTANT ENABLING UPDATES ON SERVER CORE

The /AU switch in the Server Core Registry Editor script has only two settings: on or off. When you turn automatic updates on, the system automatically applies updates, with the corresponding reboots, of course. Having a Hyper-V server reboot automatically after applying updates is not good practice because it will automatically turn off all virtual machines running on it. It will, however, restart all VMs after it reboots if the VMs were running prior to the shutdown. Note, however, that there is an interruption of service in each running VM. It might be best to disable automatic updates (using *cscript scregedit.wsf /AU 1*) and apply updates manually in maintenance windows to control server reboots more effectively.

- Configure the Firewall on Server Core. You need to do this to make sure you can get into the system from a remote location. Use the following command to enable remote administration through the system's firewall:

```
netsh advfirewall firewall set rule group="Remote Administration" new enable=yes
```

Now you can remotely manage this system. You can also configure access to WMI with this command:

```
netsh advfirewall firewall set rule group="windows management  
instrumentation (wmi)" new enable=yes
```

MORE INFO WORKING WITH THE ADVANCED FIREWALL ON SERVER CORE

You can use two commands with netsh to configure the Windows Firewall on Server Core: netsh firewall and netsh advanced firewall. The advanced firewall command is designed to configure one of three profiles—domain, private, or public—whereas the standard firewall command simply configures single-point settings. To find out more about the differences between the two commands, go to <http://support.microsoft.com/kb/947709>.

MORE INFO REMOTELY MANAGING THE FIREWALL

You can also remotely manage the firewall from a workstation running Windows Vista or a Windows Server 2008 running the full installation. To do so, you must enable remote firewall management by using the following command:

```
netsh advfirewall set currentprofile settings remotemanagement enable
```

- Move on to the final configuration changes for this server. Begin by activating the server. Note that you cannot activate a Server Core installation through a firewall that requires users to log on because there is no Web browser on a Server Core installation. Instead, you can activate by phone, by using a Key Management Service (KMS) server, or remotely by typing the following command at a command prompt of a computer that is running Windows Vista or Windows Server 2008:

```
cscript windows\system32\slmgr.vbs <ServerName> <UserName> <password>:-ato
```

ServerName is the name of the target server, *UserName* is the name of an account with domain administrative privileges, and *Password* is the password for the account.

To activate this server interactively, type:

```
cscript windows\system32\slmgr.vbs -ato
```

If the activation is successful, no message will be presented after the command.

- You should also rename the default administrator account. To do so, type the following command while you are logged on with the local administrator account:

```
wmic UserAccount where Name="%username%" call Rename Name="NewName"
```

%username% is the variable that calls your account name, Administrator, and *NewName* is the name you want to assign to the account. Log off and log on with the new name; otherwise, no other commands will work. The easiest way to do this is to press Ctrl+Alt+Delete and use the Log Off command. You need to reopen a session with the new credentials or your security context will no longer work.

If for some reason you need to change the password again, use:

```
net user  newName  *
```

The asterisk (*) causes the net user command to display a prompt for the password. Type the password, press Enter, retype the password, and press Enter again. Log off and log back on to the computer to begin using the new credentials.

- The last items that need configuration are the paging file and recovery settings. Use the following commands:

```
wmic pagefileset where name="path/filename" set InitialSize=initialsize,  
MaximumSize=maxsize
```

Use the values discussed earlier in the chapter during the full installation configuration. Make sure you create a large enough system drive to hold the page file on host systems—they will have large amounts of RAM. Note that the default page file is located at C:\PAGEFILE.SYS.

One more item may be required. Because you are creating Server Core computers to run virtualized service offerings, you will need to add at least two more disks to the system. As mentioned earlier, these disks should be located in shared storage. But because you may not be sure of the details of these disks at this time, it might be easiest to set up your Server Core computer so that you can remotely manage disks and other components through the Computer Management console on a computer with a full installation of Windows. To do this, you need to run two more commands:

```
net start VDS  
winrm quickconfig
```

The first command starts the virtual disk service (VDS) and lets you manage disks remotely, whereas the second enables the Windows Remote Shell (WinRS) on the system. This means you can now run commands remotely on this system with the WINRS command.

Your configuration of the Server Core host is complete. It is now ready to receive and run the Hyper-V role.

Performing the Hyper-V Role Installation

The activation of the Hyper-V role is very similar on both installation formats. First you need to download and install the Hyper-V RTM code; then you might require the language pack update for Hyper-V; finally, you may need additional updates based on which kind of systems you intend to use to manage Hyper-V. Note that you should also install any required security update as a best practice.

Installing the Hyper-V Role on the Full Installation

By default, Windows Server 2008 is installed in a secure configuration that does not include either enabled features or roles. To apply a specific role to a server, you must first install the role binaries and then activate or configure the role. The same applies to the installation of the Hyper-V role. However, because the original release of Windows Server 2008 was shipped

with a beta version of Hyper-V, you must download and install the appropriate version of update number 950050.

Two updates are available. The x64 update supports host servers running the Hyper-V role as long as the host server configuration meets Hyper-V requirements. Remember that Hyper-V computers must include both hardware-assisted virtualization and Data Execution Prevention (DEP), and that both must be accessible through the system's Binary Input/Output System (BIOS) settings. The x64 update includes the Hyper-V engine, the Hyper-V Manager console, the Virtual Machine Connection tool, and the Integration Services for a variety of operating systems, including:

- Windows Server 2008 (both x86 and x64 versions)
- Windows Server 2003 Service Pack 2 (both x86 and x64 versions)
- Windows 2000 Server Service Pack 4
- Windows Vista Service Pack 1 (both x86 and x64 versions)
- Windows XP Service Pack 3 (for x86 versions only)
- Windows XP Service Pack 2 (for both x86 and x64 versions)

The x86 version of the update includes the Hyper-V management tools. These tools can be installed on 32-bit systems. They are used to update the existing components in a full installation of Windows Server 2008. They include the Hyper-V management console and the Virtual Machine Connection tool.

MORE INFO UPDATE 950050

Obtain update 950050 from Microsoft's download sites at <http://support.microsoft.com/kb/950050>. As a best practice, you should obtain both x86 and x64 versions, although the next release of Windows Server 2008, R2, will only operate in x64 mode.

Download the update and store it on a shared folder. On full installations, you install the update simply by double-clicking it and following the prompts. However, it is always best to copy the update locally to install it. Copy it to the Documents folder and then launch the update. Note that a system reboot is required for the update installation to complete. Also note that this update is a recommended update from the Microsoft Update Web site. If you update your server—as you should—before performing this operation, the update will not be required (see Figure 2-6). You can run Windows Update and check for installed updates through the View Update History command and view whether update KB950050 has already been installed to ensure that you are running the latest version of Hyper-V.

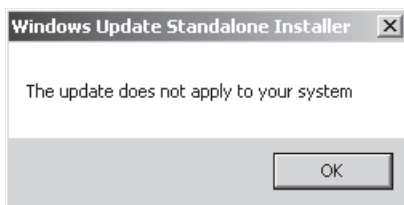


FIGURE 2-6 Hyper-V update not required

UPDATE ALERT UPDATE 950050

Note that the KB950050 update was not available through Windows Update when the exam was written. Keep this in mind as you take it.

If your computer's BIOS has not been modified to enable hardware-assisted virtualization and Data Execution Prevention, the update will give an error message (see Figure 2-7).

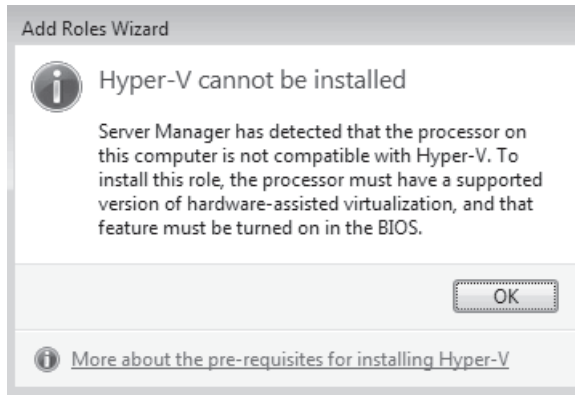


FIGURE 2-7 The BIOS has not been modified to enable hardware-assisted virtualization.

When the update is installed and the server has rebooted, log on with administrative credentials and install the Hyper-V role. The simplest way to install the Hyper-V role is to use the Server Manager console.

1. To open Server Manager, click Start, point to Administrative Tools, and then click Server Manager if it is not already open.
2. In the Server Manager window, click Roles in the left pane and then click Add Roles.
3. Review the information on the Before You Begin page, and then click Next.
4. On the Select Server Roles page, select the Hyper-V check box, and then click Next.
5. To bind the virtual network switch to a network adapter, on the Create Virtual Networks page, select the Local Area Connection check box, and then click Next (see Figure 2-8). Make sure you select only one connection for now. This connection will support the operation of virtual machines whereas the other connection(s) will let you access this server remotely.

NOTE VIRTUAL NETWORK SWITCH CREATION

You must select one network adapter to bind a virtual network switch. It is recommended that at least two network adapters should be available. One can be used for the host communication and the other for the virtual machine communication.

If you are performing the operation remotely and a single network adapter is available, the operation will break the remote connection. This is because when the virtual switch is created, it automatically disables all settings on the network adapter, disabling Remote Desktop Connections. Virtual network switches are covered in Lesson 3 of this chapter.

UPDATE ALERT DEDICATED NETWORK ADAPTERS IN WINDOWS SERVER 2008 R2

The graphical user interface in Windows Server 2008 R2 now provides support for dedicated virtual network adapters. When you create an external virtual network switch, you have the ability to check the new option Allow Management Operating System To Share This Network Adapter. See <http://blogs.msdn.com/taylorb/archive/2009/01/12/hyper-v-v2-guest-only-external-networks-add-roles-wizard-changes.aspx> for more information.

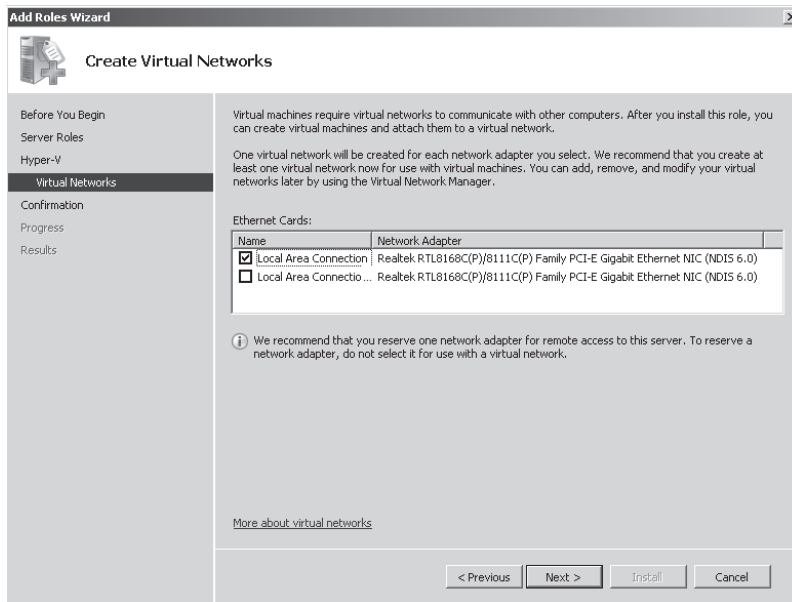


FIGURE 2-8 Creating a virtual network

6. Review your settings and click Install when ready.
7. Click Close when the installation is complete. After a dialog box appears, click Yes to restart the computer.

The Hyper-V role has been installed on this server. As soon as the server reboots, the Role Completion Wizard will open. Click Close to begin using Hyper-V.

You can optionally add another update to the host server. Update number 951636 updates the language pack for Hyper-V administration. Note, however, that this update is only for specific languages, including:

- Czech
- Hungarian
- Korean
- Polish
- Portuguese (Brazil)
- Portuguese (Portugal)
- Russian

- Swedish
- Turkish
- Chinese Simplified
- Chinese Traditional

If you do not use any of these languages, the update is not required.

MORE INFO HYPER-V LANGUAGE PACK

Obtain the Hyper-V language pack at <http://support.microsoft.com/kb/951636>.

UPDATE ALERT HYPER-V LANGUAGE PACK

Note that the Hyper-V language pack is not part of the exam because it was released after the exam was released.

Installing the Hyper-V Role on Server Core

As with the full installation, Server Core must use the updated Hyper-V code to replace the beta code included in the release version of Windows Server 2008. The process is simple:

1. Begin by downloading the update and storing it on a shared folder. Make sure the folder is accessible from your Server Core machine. See the Installing the Hyper-V Role on the Full Installation section for the location of the update.
2. Next, make sure the update has not been installed. The update cannot be removed; therefore, you need to verify whether it has been previously applied to the server you are working on.



EXAM TIP UPDATE VERIFICATION

You do not need to verify whether the update is installed on a full installation because the graphical update installer will automatically detect it and tell you whether it is necessary.

3. Apply the update. The system will reboot after the application of the update.
4. Enable the role on the server.
5. Configure the Hyper-V role.

Use the following commands to perform this installation. Begin by verifying that the update has not been installed:

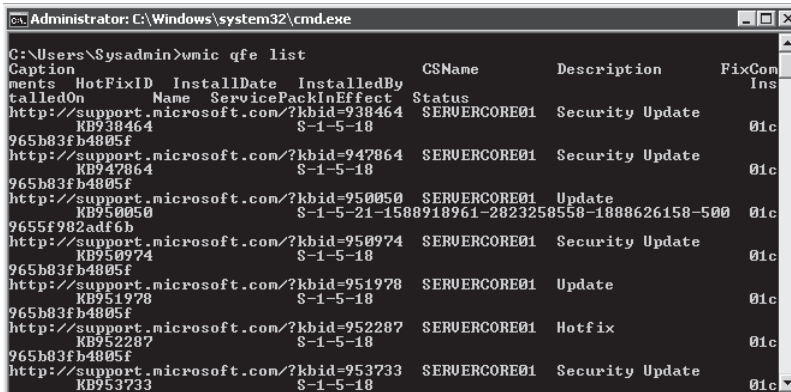
```
wmic qfe list
```

The result should list the KBID for each installed update (see Figure 2-9). Search for KBID 950050. If it is listed, the update has been installed.

If you have enabled automatic updates, the update will be installed automatically on your server. If not, you will need to install the update manually. If the update has not been installed, use the following command to perform the installation:

```
wusa.exe \\ServerShare\Windows6.0-KB950050-x64.msu /quiet
```

ServerShare is the path to the Universal Naming Convention (UNC) path to the server share that includes the update. The server should automatically reboot at the end of the update installation.



Caption	HotFixID	InstallDate	InstalledBy	CSName	Description	FixCom
ments						
talledOn	Name	ServicePackInEffect	Status			
http://support.microsoft.com/?kbid=938464	KB938464	8-1-5-18		SERVERCORE01	Security Update	01c
965b83fb4805f						
http://support.microsoft.com/?kbid=947864	KB947864	8-1-5-18		SERVERCORE01	Security Update	01c
965b83fb4805f						
http://support.microsoft.com/?kbid=950050	KB950050	8-1-5-21-1588918961-2823258558-1888626158-500		SERVERCORE01	Update	01c
9655f982adf6b						
http://support.microsoft.com/?kbid=950974	KB950974	8-1-5-18		SERVERCORE01	Security Update	01c
965b83fb4805f						
http://support.microsoft.com/?kbid=951978	KB951978	8-1-5-18		SERVERCORE01	Update	01c
965b83fb4805f						
http://support.microsoft.com/?kbid=952287	KB952287	8-1-5-18		SERVERCORE01	Hotfix	01c
965b83fb4805f						
http://support.microsoft.com/?kbid=953733	KB953733	8-1-5-18		SERVERCORE01	Security Update	01c

FIGURE 2-9 Verifying existing updates

NOTE ACCESSING A REMOTE SERVER SHARE IN SERVER CORE

Normally, you would need to map a path to the server share, but you can avoid this operation if you are using the same account name and password to log on to the Server Core computer as you would to access the share. This is called *pass-through authentication*.



EXAM TIP USING THE WUSA.EXE COMMAND

It is essential that you add the */quiet* switch at the end of the WUSA.exe command; otherwise, the update will not install on Server Core. Keep an eye out for this on the exam.

You are now ready to add the Hyper-V role. Once again, adding roles on Server Core is different than on the full installation. You must use two commands to work with roles and features on Server Core: OCLIST.exe and OCSETUP.exe. To view what is installed and what is available, type:

```
oclist
```

This command will list installed roles and features. Use the mouse wheel or the command window scroll bar to scroll up and see what is and isn't installed. You can now use the second command: OCSETUP.exe. To get information on setting up operating system roles and features, type:

```
ocsetup /?
```

This command lists the help information on the OCSETUP.exe command (see Figure 2-10).

To install the Windows Hyper-V role, type:

```
start /w ocsetup Microsoft-Hyper-V
```

Using the `/w` switch prevents the command prompt from returning until the command is completed. Otherwise, the only way to know whether a command completed successfully is to run the `OCLIST.exe` command again. Use the same structure for the other features and roles you want to install.

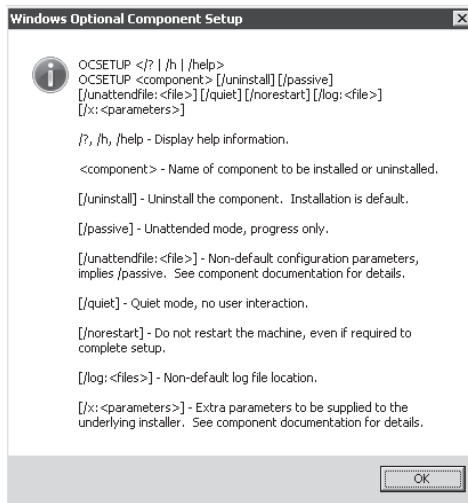


FIGURE 2-10 Viewing OCSETUP.exe Help



EXAM TIP USING THE OCSETUP.EXE COMMAND

The name of each role in OCSETUP.exe is case-sensitive. You must type the command exactly as is to install a role or feature.

The system will display a message warning you of a pending system reboot (see Figure 2-11). Click Yes to restart the system and begin using Hyper-V.

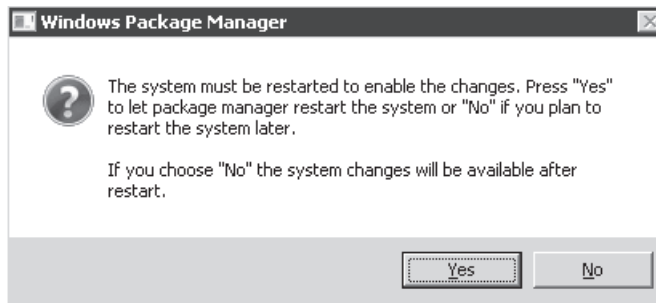


FIGURE 2-11 A reboot is required after adding the Hyper-V role



EXAM TIP THE OC COMMANDS

Keep in mind that the OCSETUP.exe and the OCLIST.exe commands are only available on Server Core. They do not work on the full installation.

Installing Hyper-V Updates

Several updates have been provided for Hyper-V since its release. Table 2-1 outlines the available updates at the time of this writing. Updates are classified according to processor capability (x86 or x64) and whether they apply to either the host, virtual machines, or both.

TABLE 2-1 Hyper-V Update List

KB #	X86	X64	HOST	VM	DESCRIPTION
KB950050		X	X		Use to run the Hyper-V RTM version.
KB950182	X			X	Use to start a VM on a computer that uses a 6-core processor.
KB951308		X	X		Use to increase functionality for Failover Clusters running Hyper-V.
KB951636	X			X	Language Pack Update for Windows Server 2008.
KB952627		X	X	X	RSAT on Windows Vista Service Pack 1 or later using the Hyper-V MMC snap-in.
KB953585		X	X		Use to run Hyper-V VMs running Windows Server 2008 and Windows Vista operating systems on a host that uses non-uniform memory access (NUMA) architecture.
KB953828		X	X		Use for NLB on Windows Server 2008 Hyper-V virtual machines.
KB956386		X			Contains Microsoft Hyper-V Server 2008 ISO files.
KB956589		X	X	X	Use to manage Hyper-V with SCVMM 2008.
KB956697		X	X	X	Use to back up VMs using Volume Shadow Copy (VSS).
KB956710		X	X		If the management operating system has more than 16 logical processors, Hyper-V will be able to support up to 24 logical processors and 192 VMs. Note that Hyper-V R2 supports even more processors than this update provides.
KB956774		X	X	X	Corrects issues where a Background Intelligent Transfer Service (BITS) client cannot handle files that contain the volume GUID in Windows Server 2008.
KB957967		X	X		Use to resolve the following error message: "Stop error message on a Windows Server 2008-based computer that has the Hyper-V role installed:"STOP 0x0000001A"."
KB958065		X	X		Use for a non-Microsoft clustered file system or non-Microsoft replication solutions.
KB958184		X		X	Use to back up a volume that is mounted using a volume GUID.

UPDATE ALERT HYPER-V UPDATES

Because many of the updates for Hyper-V date from well after it was released, none of the features or issues fixed by these updates is mentioned in the exam.

MORE INFO HYPER-V UPDATES

Microsoft regularly releases updates for Hyper-V. Therefore, the list in Table 2-1 is not exhaustive. Go to <http://technet.microsoft.com/en-us/library/dd430893.aspx> to check for the latest updates for Hyper-V.

Make sure you read through the list of updates in Table 2-1. Apply each of the required updates to your host systems before moving them into production.

Hyper-V and Active Directory Domain Services

It is good practice to make your Hyper-V host servers part of an AD DS directory. AD DS directories centralize all access rights to servers and support the delegation of administration services. However, because host servers run a service in support of virtual machines and virtual machines run the services you provide to end users, you might consider using a separate directory for your host server configuration. This second directory is a utility directory that provides a security context only for the host servers.

The security and identity context for the networked services in your production network remains the same as it was, but the security context for your host servers becomes an independent directory. Obviously, this depends on the size of your network, but in anything except very small networks, it is highly recommended to create a separate utility directory for host server environments. This ensures that end users do not live or operate in the same security context as your host servers. Segregating security contexts in this way helps further protect host servers from potential tampering (see Figure 2-12).

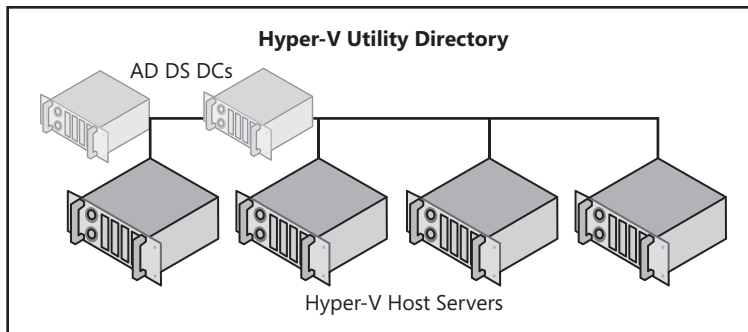


FIGURE 2-12 The Hyper-V host server security context

If you elect to create a separate utility directory, create a single domain forest and run it on at least two domain controllers. These domain controllers can reside in virtual machines, but you must make sure that they are set to start automatically if your entire Hyper-V host

infrastructure is completely shut down; otherwise, you will find it difficult to log on to the Hyper-V host domain.

MORE INFO AD DS

For more information on implementing AD DS and other Active Directory technologies, see *MCTS Self-Paced Training Kit (Exam 70-640): Configuring Windows Server 2008 Active Directory* by Holme, Ruest, and Ruest at <http://www.microsoft.com/learning/en/us/books/11754.aspx>.

Installing Windows Hyper-V Server

A third option you can use to host virtual machines is Windows Hyper-V Server 2008. As mentioned in Chapter 1, Hyper-V Server is a free download from Microsoft. The download is available as an ISO file—a special format that contains a CD or DVD image. Remember that Hyper-V Server is based on the Standard edition of Windows Server 2008 and includes a Server Core installation only. Because it is based on the Standard edition, Hyper-V Server does not include the capability to support fault tolerance in host servers, but in some cases—as per the Exchange Support Team—it is necessary to install stand-alone hosts that do not include fault tolerance to create a supported virtual installation of a Windows Server product. Also remember that because it is free, Hyper-V Server does not include any licenses for the virtualization of Windows Server 2008, unlike the actual Windows Server 2008 editions that support Hyper-V.

UPDATE ALERT HYPER-V SERVER R2

Note that Hyper-V Server R2 is now based on the Enterprise edition of Windows Server 2008 R2 and therefore includes support for more memory, more processors, and failover clustering among other new features. This means it will support both Quick and live migrations.

MORE INFO THE HYPER-V SERVER DOWNLOAD

Find the Hyper-V Server download at <http://www.microsoft.com/downloads/details.aspx?familyid=6067cb24-06cc-483a-af92-b919f699c3a0&displaylang=en&tm>.

The first thing to do to install Hyper-V Server is to convert the ISO file into a DVD. Most DVD burner software can do this, as well as some free utilities such as WinImage. WinImage is a good utility because it also lets you examine the contents of an ISO file. In addition, the latest edition of WinImage even converts virtual hard drives into physical disks, converts physical disks into virtual hard drives, and supports the conversion of virtual disks from VMware to Microsoft virtual hard drive format and vice versa.

MORE INFO WINIMAGE

WinImage is available as a trial edition from Gilles Volant Software at <http://www.winimage.com>.

Burn the DVD for Hyper-V and then move on to the Hyper-V Server installation. Remember that Hyper-V Server has the same hardware requirements as Windows Server 2008 Hyper-V.



EXAM TIP HYPER-V SERVER

Even though Hyper-V Server is an important part of the Hyper-V datacenter, it is not on the exam because it was not available when the exam was released.

Performing the Hyper-V Server Installation

Proceed to the installation. Use the following instructions:

1. Insert the Hyper-V Server DVD into the drive of your computer system. Ideally, no pre-existing operating system will be found on this server, but if there is one, use the installation to replace it.
2. Boot the server and select to boot from the DVD if prompted.
3. When the Windows Hyper-V Server Setup screen appears, select My Language Is English and press Enter (see Figure 2-13).

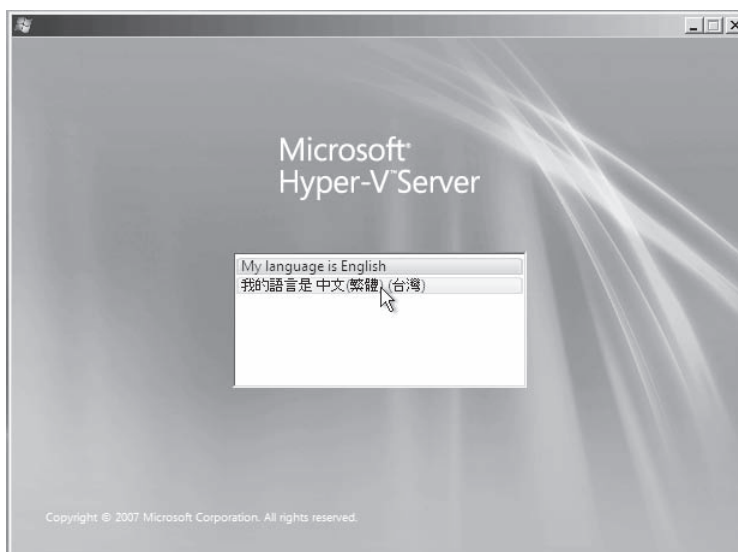


FIGURE 2-13 Selecting the language to install in Hyper-V Server

4. Select English as the language to install, English (United States) or whatever is appropriate as the time and currency format, and US or whatever is appropriate as the keyboard or input method. Click Next.
5. Click Install Now.
6. Accept the license terms and click Next.
7. Select Custom because there is no upgrade path to Hyper-V Server.
8. The next screen lets you prepare custom partitions to host the installation. Because all host servers should be linked to shared storage, you can use the entire local partition for the installation. Click Next.
9. The installation proceeds and will reboot the server until the installation is complete.

Now proceed to the system personalization and preparation. During the first logon after the installation of Hyper-V Server, you will be prompted to enter a user name and create a password. Use the following instructions:

1. Click Other User.
2. In the User Name field type **Administrator** and then press Enter.
3. The system displays a message stating “The user’s password must be changed before logging on the first time”. Click OK.
4. Type a new password in the New Password field. Confirm the password and press Enter.
5. You will see a confirmation that your password has been changed. Click OK.

The system logs you on and displays the Hyper-V Server Configuration Tool.

Using the Hyper-V Configuration Tool

The Hyper-V Configuration Tool is a menu-driven UI that helps you configure Hyper-V Server. The interface starts automatically at system administrator logon or can be started manually. To manually start the Hyper-V configuration tool, make sure you are on the system drive and type:

```
hvconfig.cmd
```

Press Enter to display the interface (see Figure 2-14).

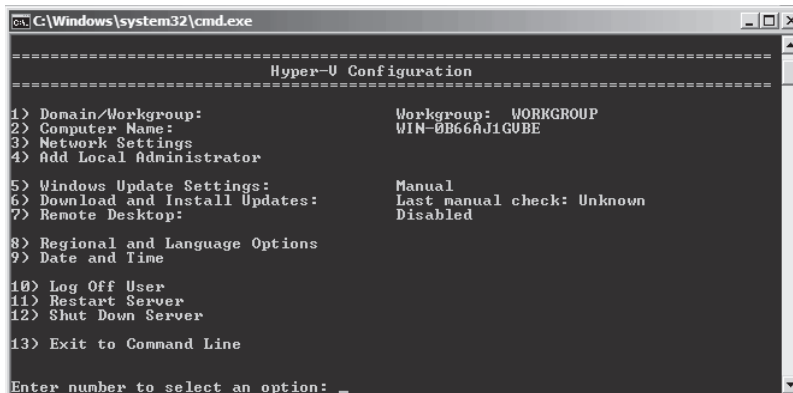


FIGURE 2-14 The Hyper-V Configuration UI

This interface provides some easy access to the system configuration you would normally have to perform from the Server Core command line. Perform the following steps:

1. Change the computer name. Type **2** and press Enter. Name the computer according to your organizational standards and press Enter. A message appears, informing you that the name has been changed. Click OK and then click Yes to restart the computer.
2. Log on again, type **3**, and press Enter to configure network adapters. Host servers should not rely on the Dynamic Host Configuration Protocol (DHCP) and should use

static IP addresses. The interface lists available network cards. Type the Index number for the card you want to modify. For example, type **1** and then press Enter. The system displays the IP settings for the selected adapter (see Figure 2-15). Type **1** and press Enter to modify the IP address. Type **S** and then press Enter to change it to a static address. Enter the IP address and press Enter. Press Enter to apply the default subnet mask. Type the default gateway address and press Enter.

```

-----
Network Adapter Settings
-----
NIC Index           1
Description         Intel 21140-Based PCI Fast Ethernet Adapter <Emulated>
IP Address          192.168.0.61
Subnet Mask         255.255.255.0
DHCP enabled        True
Default Gateway     192.168.0.1
Preferred DNS Server 192.168.0.10
Alternate DNS Server 192.168.0.80

1> Set Network Adapter IP Address
2> Set DNS Servers
3> Clear DNS Server Settings
4> Return to Main Menu

Select option: _

```

FIGURE 2-15 Changing network settings on Hyper-V Server

3. Type **2** and then press Enter to set DNS settings. Enter at least one DNS address, two if possible. Type the IP address of the DNS server and then press Enter. Click OK to close the Successful Change dialog box. Type in the alternate DNS server IP address and then press Enter. Click OK to close the dialog box.
4. Type **4** and then press Enter to return to the main menu. Type **1** and then press Enter to join a domain. Type **D** and then press Enter to join the domain. Type the domain name and then press Enter. Type the name of an appropriate account and then press Enter. Type the account's password and then press Enter. Click Yes to restart the computer.
5. Log on with a domain administrator account. Use the Switch User and Other User buttons and type the account in the *Domain\Username* format.
6. Type **7** and then press Enter to enable the Remote Desktop. Type **E** and then press Enter; then type **1** and press Enter to enable only secure connections. Click OK to close the dialog box telling you that only secure connections are enabled.
7. Type **6** and then press Enter to download and install updates on this server. A new window opens and the system begins searching for updates. Once updates are found, they are listed in the window (see Figure 2-16). Type **y** and then press Enter to download and install updates. The server will need to reboot once the updates are installed. Click Yes to restart the server. You will need to repeat this operation regularly to update this server on a monthly basis.

Your Hyper-V server is ready. Hyper-V Server includes fewer features than Windows Server 2008 with Hyper-V, but it does include some. Use the OCLIST.exe command to view available features on Hyper-V Server (see Figure 2-17).

```

C:\Windows\System32\cscript.exe
1> Cumulative Security Update for Internet Explorer 7 in Windows Server 2008 x64
Edition (KB947864)
2> Update for Windows Server 2008 x64 Edition (KB951978)
3> Security Update for Windows Server 2008 x64 Edition (KB953733)
4> Cumulative Security Update for Internet Explorer 7 in Windows Server 2008 x64
Edition (KB953838)
5> Security Update for Windows Server 2008 x64 Edition (KB950974)
6> Update for Windows Server 2008 x64 Edition (KB952287)
7> Update for Windows Server 2008 x64 Edition (KB955302)
8> Security Update for Windows Server 2008 x64-based Systems (KB938464)
9> Security Update for Windows Server 2008 x64 Edition (KB954211)
10> Security Update for Windows Server 2008 x64 Edition (KB956841)
11> Security Update for Windows Server 2008 x64 Edition (KB958644)
12> Security Update for Windows Server 2008 x64 Edition (KB955069)
13> Security Update for Windows Server 2008 x64 Edition (KB954459)
14> Security Update for Windows Server 2008 x64 Edition (KB957097)
15> Security Update for Windows Server 2008 x64 Edition (KB956802)
16> Security Update for Windows Server 2008 x64 Edition (KB958623)
17> Update for Windows Server 2008 x64 Edition (KB957388)
18> Update for Windows Server 2008 x64 Edition (KB955839)
19> Security Update for Windows Server 2008 x64 Edition (KB958687)
20> Windows Malicious Software Removal Tool x64 - January 2009 (KB890830)

Would you like to download and install updates now? (Y/N)

```

FIGURE 2-16 Checking for updates on Hyper-V Server

```

C:\Users\Administrator>oclist
Use the listed update names with Ocsetup.exe to install/uninstall a server role
or optional feature.

Adding or removing the Active Directory role with OCSetup.exe is not supported.
It can leave your server in an unstable state. Always use DCPromo to install or
uninstall Active Directory.

=====
Microsoft-Windows-ServerCore-Package
Not Installed:BitLocker
Not Installed:BitLocker-RemoteAdminTool
Installed:Microsoft-Hyper-V
Not Installed:Microsoft-Windows-RemovableStorageManagementCore
Not Installed:MultipathIO
Not Installed:NetworkLoadBalancingHeadlessServer
Not Installed:SNMP-SC
Not Installed:TelnetClient
Not Installed:WindowsServerBackup

C:\Users\Administrator>

```

FIGURE 2-17 Viewing available features on Hyper-V Server

PRACTICE Installing the Hyper-V Role

This practice consists of four exercises. These exercises build on the exercises you performed in Lesson 3 in Chapter 1. In this lesson, you installed Windows Server 2008 on two systems. One used the full installation and the other used Server Core. Now you will configure these systems to run Hyper-V. First you will configure the full installation and then you will install the Hyper-V role. Then you will configure the Server Core computer and install the Hyper-V role on this computer.

EXERCISE 1 Configure a Full Installation

In this exercise you will prepare a Windows Server 2008 full installation to host the Hyper-V role.

1. On the computer on which you installed the full installation in the practice in Lesson 3, Chapter 1, "Prepare for Hyper-V Deployment," click the Administrator icon. Type in and confirm a new password and press Enter. Now log on to the system with Administrator and the new password.
2. The system will log you on and launch the Initial Configuration Tasks interface. Click the Set Time Zone link. Set the time zone as needed and click OK.

3. Click the Configure Networking link. This opens the Network Connections window. Right-click each network connection and choose Properties. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties. Enter appropriate networking values for each entry—IP address (**192.168.0.6** and **192.168.0.7**), subnet mask (**255.255.255.0**), default gateway (**192.168.0.1**), and at least one DNS server. Press Enter. Repeat for each network interface card. The IP address for the DNS server should be the IP address for the AD DS domain controller you prepared according to the instructions in the Introduction (**192.168.0.5**). Close Network Connections when done.
4. Click the Provide Computer Name And Domain link in the ICT. Click Change, type in **ServerFull01** as the computer name and **Contoso.com** as the domain, and click OK. The system will warn you that you need to reboot it to make the change take effect. Click OK and then click OK again. Choose to reboot the system now.
5. After the computer is rebooted, log on using **Contoso\Administrator** and click Enable Automatic Updates And Feedback when the ICT screen appears. Select Manually Configure Settings. Under Windows Automatic Updating, click Change Settings. Choose Download Updates But Let Me Choose Whether To Install Them and select Include Recommended Updates When Downloading, Installing Or Notifying About Updates as well as Use Microsoft Update. Click OK and then click Close.
6. Click Download And Install updates and then click Check For Updates. Install all appropriate updates. Make a note to see whether the Hyper-V update (KB950050) is among the updates. Depending on when you perform this installation, you can have more than 30 updates available. However, if your installation included Service Pack 2, the number of required updates will be considerably fewer. Reboot the server when done.
7. When the server reboots, log on and click the Enable Remote Desktop link on the ICT page. Choose Allow Connections Only From Computers Running Remote Desktop With Network Level Authentication (More Secure) and click OK.
8. Click Configure Windows Firewall and choose Change Settings. Make sure the firewall is on, click the Exceptions tab, and choose Remote Service Management, Remote Volume Management, Windows Management Instrumentation (WMI), and Windows Remote Management. Click OK.
9. Select the Do Not Show This Window At Logon check box and click Close to turn off the ICT.
10. Do not activate the server. You have 60 days of evaluation, which should be sufficient time to prepare for the exam.

Although more configuration is required for production Hyper-V servers, it is not necessary for the purposes of this exercise. Your server is ready for Hyper-V.

EXERCISE 2 Install the Hyper-V Role

In this exercise you will install and enable the Hyper-V role. You'll begin by checking for the Hyper-V update and then move on to enabling the Hyper-V role. Use the domain administrator account to perform this exercise.

1. Log on to the computer. The Windows Server Manager console will automatically start.
2. Begin by determining whether the update has been installed. Click Start, then Control Panel. Click Control Panel Home to change to the standard view and click Check For Updates under Security. Click View Update History and scroll through the list to see whether update KB950050 is available. If it is, close the Update windows.
3. If the update has not been installed, launch Internet Explorer from the Quick Launch toolbar. Type **KB950050** in the Live Search bar and press Enter. Click Yes to send information over the Internet. Windows Server 2008 uses IE Enhanced Security Configuration. Add all appropriate Web sites to view the answer to your query. Click the Download Details link for the Hyper-V x64 update and download the update. Accept all appropriate Web sites and save the update in a new folder on drive C: called Updates. Double-click the update to install it and follow the prompts. The system will need to reboot once the update is installed. Log on with the same account.
4. In Server Manager, right-click Roles in the Tree pane and choose Add Role. Review the information on the introduction page and click Next.
5. Select the Hyper-V role and click Next.

IMPORTANT **HARDWARE-ASSISTED VIRTUALIZATION**

A warning will appear if you have not enabled hardware-assisted virtualization in the BIOS of this server. Do so and begin the exercise again.

6. Review the notes on the Hyper-V role and click Next.
7. On the Create Virtual Networks page, select one of the two network adapters and click Next.
8. Review your settings and click Install.
9. Click Close when the installation is complete and click Yes to reboot the server.
10. Log on with the same account and click Close to complete the installation.

Your Windows Server with Hyper-V server is ready.

EXERCISE 3 **Configure a Server Core Installation**

In this exercise you will prepare a Windows Server 2008 Server Core installation to host the Hyper-V role.

1. On the computer on which you installed the Server Core installation in the practice in Lesson 3, Chapter 1, click the Administrator icon. Type in and confirm a new password and press Enter. Now log on to the system with Administrator and the new password.
2. The system will log you on. Begin by setting the time zone. Type the following command, set the time zone as needed, and click OK.

```
control timedate.cpl
```

3. Now configure networking. Use the following commands to set the IPv4 parameters—IP address, subnet mask, default gateway, and at least one DNS server—for each network adapter. Remember, you begin by finding the adapter ID, and then you use this ID to configure the adapter. Repeat this process for each network interface card. The IP address for the DNS server should be the IP address for the AD DS domain controller you prepared according to the instructions in the Introduction.

```
netsh interface ipv4 show interfaces
netsh interface ipv4 set address name=2 source=static address
    =192.168.0.8 mask=255.255.255.0 gateway=192.168.0.1
netsh interface ipv4 add dnsserver name=2 address=192.168.0.5 index=1
netsh interface ipv4 set address name=3 source=static address
    =192.168.0.9 mask=255.255.255.0 gateway=192.168.0.1
netsh interface ipv4 add dnsserver name=3 address=192.168.0.5 index=1
```

4. Now rename the computer. You must restart the computer once the name has been changed.

```
netdom renamecomputer %computername% /newname:ServerCore01
shutdown /r /t 3
```

5. Log on again after the computer has restarted and join the domain. Type in the appropriate password for the Administrator account on the domain. Once again, a reboot is required to complete this operation.

```
netdom join %computername% /domain:Contoso.com /userD:Administrator
    /passwordD:Password
shutdown /r /t 3
```

6. After the computer is rebooted, log on using **Contoso\Administrator**. You can now enable automatic updates and Remote Desktop Connections.

```
cd \Windows\System32
cscript scregedit.wsf /AU 4
cscript scregedit.wsf /AR 0
```

7. Configure the Windows Firewall. You want to enable at least the Remote Service Management and the Windows Management Instrumentation (WMI).

```
netsh advfirewall firewall set rule group="Remote Administration" new enable=yes
netsh advfirewall firewall set rule group="windows management instrumentation
(wmi)" new enable=yes
```

8. You also want to enable Windows Remote Management.

```
winrm quickconfig
```

IMPORTANT WINDOWS REMOTE MANAGEMENT

Although you enable Windows Remote Management on a Server Core installation because it is inconvenient to always manage a server through the command line, you

should also consider running this command on any full installation that you want to manage remotely as well. Make a practice to run the following command on all Hyper-V host servers regardless of the installation type:

```
winrm quickconfig
```

9. Finally, you want to configure, then start the Virtual Disk Service. Note that a space is required before the *auto* value in the first command. When the configuration is complete, you must open the Windows Firewall port for Remote Volume Management on both this server and any remote computer you want to use to manage this server's disk.

```
sc config vds start= auto
net start VDS
netsh advfirewall firewall set rule group="Remote Volume Management"
    new enable=yes
```

IMPORTANT REMOTE VOLUME MANAGEMENT

Make sure you set the firewall rule on your remote server to manage volumes on a Server Core installation. In this case, open an elevated command prompt on ServerFull01 and run the following command on it. Perform this on any computer from which you want to remotely manage volumes.

```
netsh advfirewall firewall set rule group="Remote Volume Management"
    new enable=yes
```

10. Do not activate the server—you have 60 days of evaluation, which should be sufficient time to prepare for the exam.

Although more configuration is required for production Hyper-V servers, it is not necessary for the purposes of this exercise. Your server is ready for Hyper-V.

EXERCISE 4 Install the Hyper-V Role

In this exercise you will install and enable the Hyper-V role. You'll begin by checking for the Hyper-V update and then move on to enabling the Hyper-V role. Use the domain administrator account to perform this exercise.

1. Log on to the computer.
2. Begin by determining whether the update has been installed. Scroll through the list to see whether update KB950050 is available.

```
wmic qfe list
```

3. If the update has not been installed, you need to install it manually. Return to ServerFull01 and launch Windows Explorer by clicking Start, then All Programs, and then Accessories. Move to the C: drive and right-click the Updates folder. Choose Share, then choose Everyone from the drop-down list, and then click Add. Change the Permission Level to Contributor. Click Share and then click Done. You will use this shared folder to install the update on the Server Core computer.

4. Return to the Server Core computer and install the KB950050 update. This update will automatically reboot the computer.

```
wusa.exe \\ServerFull101\Updates\Windows6.0-KB950050-x64.msu /quiet
```

5. Log on with the domain administrator account after the computer has restarted. You will now install and enable the Hyper-V role. The Hyper-V role will require another computer reboot. Click Yes when the reboot dialog box appears.

```
start /w ocsetup Microsoft-Hyper-V
```

Your Windows server with Hyper-V Server will be ready after the reboot.

Quick Check

1. Which tool do you use to activate the server on a full installation?
2. Which kind of scripts can you use to automate Hyper-V operations locally on Server Core?
3. There is a custom script on Server Core designed to help you perform some of the most common configuration tasks. Where is it located?
4. How many settings does Server Core include for the `/AU` switch to enable updates?

Quick Check Answers

1. This is one of the only activities that is not performed through Server Manager. It is performed in Control Panel under System And Maintenance, then System.
2. The command line is used to perform local operations on Server Core. Two script engines can run locally on Server Core: command-line scripts (.cmd) and Visual Basic Scripts (.vbs). You can run Windows PowerShell scripts against Server Core installations, but you must run them from a remote computer because Windows PowerShell requires the .NET Framework to run and this framework does not run on Server Core.
3. Server Core includes a custom script to perform some of the configuration tasks that are located in the System32 folder of the installation. This script is called SCREGEDIT.wsf.
4. There are two settings for the `/AU` switch to enable updates on Server Core: 4 for on and 1 for off.

Lesson 2: Configuring Windows Server Hyper-V

When you prepare to configure your Windows server for Hyper-V, you must begin by understanding the Hyper-V management interfaces as well as the various Hyper-V options.

After this lesson, you will understand:

- The Hyper-V management tools.
- The different settings in Hyper-V.
- The virtual machine file locations.

Estimated lesson time: 30 minutes

Working with the Hyper-V Management Tools

Hyper-V relies on two main consoles for host and virtual machine management. The first console can be found only on the full installation of Windows Server: Server Manager (see Figure 2-18). Remember that Server Manager is a single-instance management console and can only be run on the actual server you are managing. It can be published remotely as a Terminal Services RemoteApp, which lets you run it as a remote application on your desktop, but it cannot connect to remote computers or manage Server Core installations.

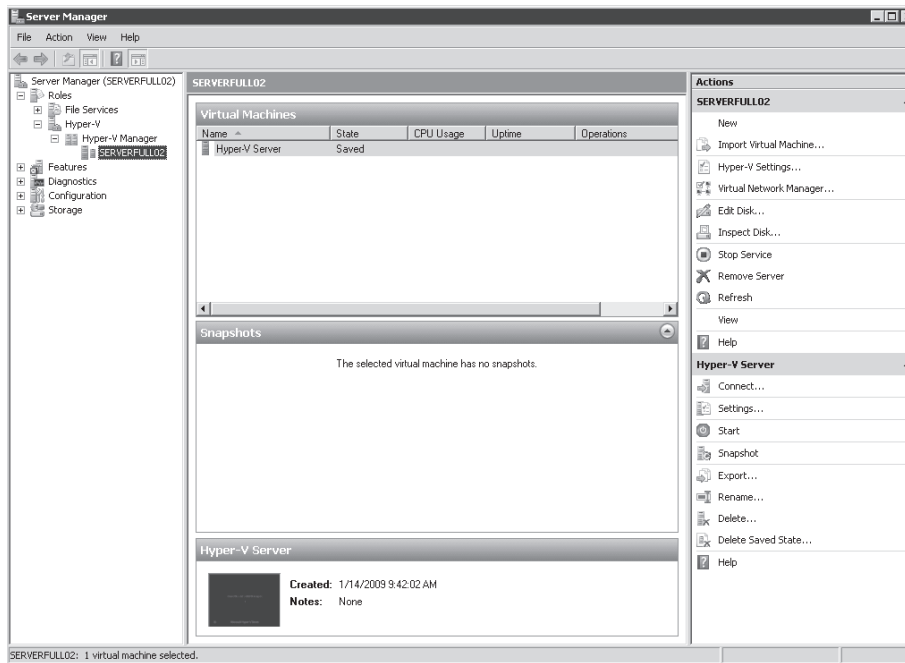


FIGURE 2-18 Working with Hyper-V management in Server Manager



EXAM TIP SERVER MANAGER

Remember that Server Manager is a single-instance console and cannot manage remote servers or Server Core.

The advantage of working with Server Manager is that it provides a single point of access for all server operations. Clicking Server Manager in the tree pane gives you summary information about the status and configuration of your server, letting you view all information in a single place. But this information is only for the local server. Though you can connect to additional Hyper-V servers through the Hyper-V Manager section of Server Manager, you will be limited to Hyper-V Manager functionality on the remote server. You will not have access to the other management functions of Server Manager for the remote computer.

The second management interface for Hyper-V is the Hyper-V Manager console (see Figure 2-19). Like Server Manager, Hyper-V Manager is also based on the Microsoft Management Console (MMC) version 3, but unlike Server Manager, Hyper-V Manager can also be installed independently of Windows Server 2008. Hyper-V Manager can therefore be installed on workstations running Windows Vista with Service Pack 1 or later.

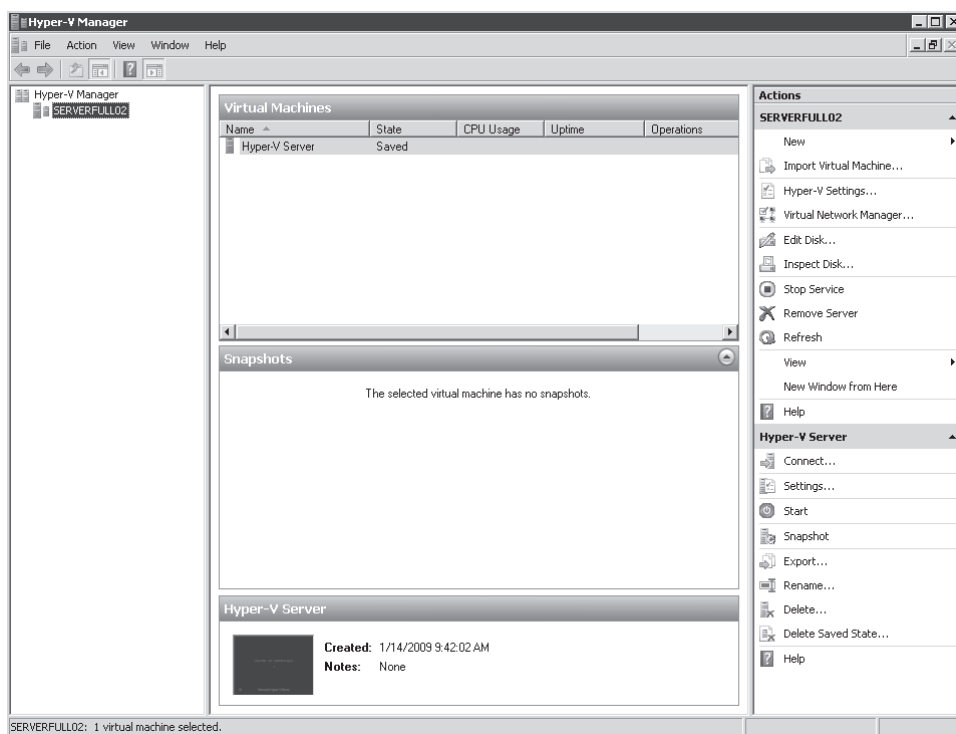


FIGURE 2-19 Working with the stand-alone Hyper-V Manager console

MORE INFO HYPER-V MANAGER ON WINDOWS VISTA AND/OR WINDOWS SERVER 2008 X86

To run Hyper-V Manager on Windows Vista with Service Pack 1 or later, you must download update number KB952627, which you can find at <http://support.microsoft.com/kb/952627>. The console is included in the Windows Server RSAT package. To manage Hyper-V from an x86 installation of Windows Server 2008, you must download the 32-bit version of update number KB950050, which you can find at <http://support.microsoft.com/kb/950050>.

Hyper-V Manager uses a three-pane layout, as do all MMCv3 consoles:

- The leftmost pane is the Tree pane, which displays the hierarchy of managed items.
- The center pane is the Details pane, which displays information on the selected object in the Tree pane. In Hyper-V Manager, this pane includes three sections:
 - Virtual Machines lists the available virtual machines on this server as well as their status. This pane can contain up to 512 virtual machines, but only 192 can run at one time—depending, of course, on your host server’s physical resource availability.
 - Snapshots lists whether the VM includes specific state images of the VM. Snapshots are a powerful feature of Hyper-V that allows you to capture state-in-time images of a VM and return to them if needed. Snapshots are covered in depth later in this lesson.
 - The Hyper-V Server section lists information about the selected VM. In most cases, it displays the VM thumbnail, the creation date for the VM, and any notes attached to the VM. You can double-click the VM thumbnail to open a console letting you interact with the VM.
- The rightmost pane is the Actions pane. The content of this pane is contextual and changes with the selected object in the Details pane. This pane often gives access to the same actions you can find when you right-click an object to view its shortcut menu. In Hyper-V Manager, this pane is divided into two sections:
 - The top section displays actions that can be taken on the selected host server.
 - The bottom section displays actions that can be taken on the selected virtual machine.

Take the time to tour and explore the Hyper-V Manager interface. It will allow you to better understand the various features of Hyper-V.

Understanding Hyper-V Settings

When you launch the Hyper-V console on a newly installed Hyper-V host, you should begin with the configuration of Hyper-V settings. Several settings require modification. Table 2-2 outlines the various settings available in the configuration of a Hyper-V server. Modify these settings before you begin to generate virtual machines on your server.

TABLE 2-2 Hyper-V Settings

SERVER SETTINGS	DESCRIPTION
Virtual Hard Disks	Use this setting to specify the default folder to store virtual hard disk files. The default is C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks.
Virtual Machines	Use this setting to specify the default folder to store virtual machine configuration files. The default is C:\ProgramData\Microsoft\Windows\Hyper-V.
USER SETTINGS	DESCRIPTION
Keyboard	Use this setting to choose how to use Windows key combinations such as Ctrl+Alt+Delete when accessing virtual machines through the Virtual Machine Connection. There are three options: ■ Use On The Physical Computer ■ Use On The Virtual Machine ■ Use On The Virtual Machine Only When Running Full-Screen The default is Use On The Virtual Machine Only When Running Full Screen.
Mouse Release Key	Use this setting to specify the key combination to use to release the mouse when virtual machine drivers are not installed. This key combination is used in Virtual Machine Connection. There are four options: Ctrl+Alt+Left Arrow Ctrl+Alt+Right Arrow Ctrl+Alt+Space Ctrl+Alt+Shift The default is Ctrl+Alt+Left Arrow.
User Credentials	Use this setting to specify whether you want to use your default credentials automatically with Virtual Machine Connection to connect to a running virtual machine. The default credentials are the credentials you used to log on to your current Windows session. Select Use Default Credentials Automatically (No Prompt). To use smart card credentials, you must clear the check box and enter them when you receive a prompt. The default is Allow Default Credentials.
Delete Saved Credentials	Use this setting to delete the credentials that were used to connect to a running virtual machine.
Reset Check Boxes	Use this setting to clear all check boxes that hide pages and messages when selected. This action restores Hyper-V confirmation messages and wizard pages that are hidden by selecting the check boxes.

The settings in Table 2-2 are found in the Hyper-V Settings dialog box (see Figure 2-20), which you can activate by clicking the Hyper-V Settings link in the Actions pane of Hyper-V Manager when a host server is selected in the Tree pane. This dialog box divides settings between servers and users. Server settings such as VHD and VM location apply to the server as a whole. User settings are applied to each user session; therefore, different users can work with different settings.

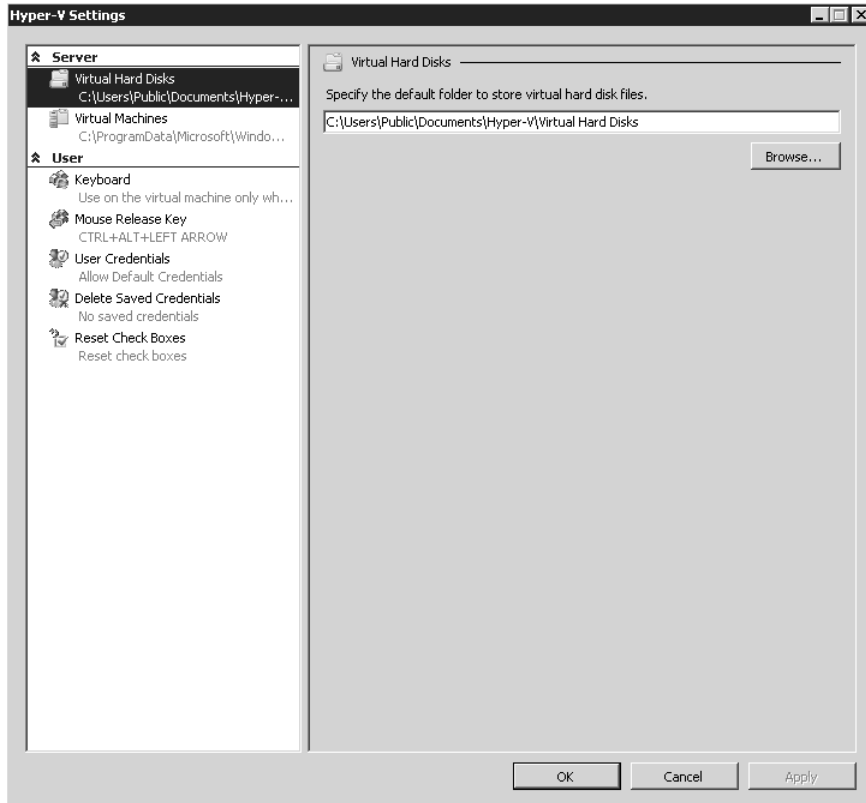


FIGURE 2-20 Working with Hyper-V Manager settings

Working with the Virtual Machine File Locations

As you can see in Table 2-2, the two server settings—Virtual Machine and Virtual Hard Disk Location—are stored by default in either your user profile or in the Windows ProgramData folder. Both locations may be appropriate if you are using Hyper-V on a laptop for personal use only, but when you run Hyper-V in the datacenter as a host environment for a wide variety of virtual machines, these settings are completely inappropriate.

Ideally, your virtual machine settings files and the virtual hard drives they require will be stored in the same folder. After all, the whole idea of a virtual machine is that by transforming

a physical computer into a VM, you transform it into a set of files that should all be located within the same folder. This way, the folder contains all of the components of a given VM. Then when you want to perform operations on the VM—such as backing up the VM—you simply manipulate the entire folder and all of its contents. You want to move the VM from host to host. Move the folder and you're set.

In addition, if you want to provide high availability for your virtual machines through host server clustering, you'll want to store all virtual machine files in a shared storage container—either an iSCSI target or a Storage Area Network (SAN). This way each host has access to the VM files and can take on the operation of the VM without having to wait for the duplication of the files that make it up—a duplication process that can take considerable amounts of time because VM files, specifically the virtual hard drive files, can be many gigabytes in size.

Therefore, you should make sure that the two server-based settings for each Hyper-V server are set to a specific location. By default, both virtual hard drives and virtual configuration files are not in the same container, which makes it difficult at best to locate all of the components of a VM. By default as well, the virtual machine's hard drives are in the public user profile. Storing virtual hard drives in a profile folder is definitely not a best practice. Therefore, you should modify these settings as follows:

- If the host server uses Direct-Attached Storage (DAS) only, create a separate disk configuration on the host server, ideally with separate spindles, configure a RAID mode for these spindles, and use it as VM storage. For example, you might create a separate partition with at least 100 GB in spare space and create a storage folder for all VMs. In this case, you would modify the default location settings to something such as `D:\VirtualMachines`.
- If the host server can access shared storage, create a set of storage logical units (LUNs) and connect them to your host server. Create a default container for VMs on one of the LUNs and name it appropriately. For example, you might change your default settings to `S:\VirtualMachines`.

Make sure you set both the virtual machine configuration files and the virtual hard drives to the same location.

Because the user settings apply to each user that logs on, they can be modified individually. However, it is good practice to keep these settings at the default. This way, your administrators all rely on the same approaches to interacting with virtual machines.



EXAM TIP HYPER-V SETTINGS DEFAULTS

Pay close attention to the default settings listed in Table 2-2. The exam includes several questions on the use of release keys as well as the use of Windows key combinations in virtual machines. Some questions also address default storage paths for VM files.

In this practice, you will begin to work with your two Hyper-V servers and configure their default settings. You will also create and work with your first virtual machines. This practice consists of five exercises. In the first exercise, you begin to work with Hyper-V Manager and your two host servers. In the second exercise, you configure default settings for each of your host servers. In the third exercise, you create your first virtual machine. In the fourth exercise, you import the virtual machine you downloaded from the Microsoft Web site during the practice in Lesson 1 of Chapter 1. Finally, in the fifth exercise you examine how Hyper-V creates and manages the files that make up VMs.

EXERCISE 1 Begin to Work with Hyper-V Manager

In this exercise you will log onto your Windows Server 2008 full installation to begin working with Hyper-V Manager. Use domain administrator credentials to perform this exercise.

1. Log on to ServerFull01 using domain administrator credentials. Server Manager will automatically launch once you are logged on. You can work with either Server Manager or Hyper-V Manager to perform this exercise.
2. To work with Hyper-V Manager, open the console by clicking Start, then Administrative Tools, and then Hyper-V Manager. To work with Server Manager, click Roles, then Hyper-V, then Hyper-V Manager. Note that ServerFull01 is displayed under Hyper-V Manager in the Tree pane.
3. To manage both servers from the same console, you need to connect to your Server Core computer. In Hyper-V Manager, click Connect To Server in the Actions pane. Click Another Computer, type **ServerCore01**, and then click OK. ServerCore01 should appear under Hyper-V Manager in the Tree pane of the console.

Note that you must reconnect to remote servers each time you close and reopen the console.

EXERCISE 2 Configure Hyper-V Settings

In this exercise you will configure the default virtual machine file locations for both host servers.

1. Log on to ServerFull01 using domain administrator credentials. Either go to Server Manager or launch Hyper-V Manager.
2. Begin by creating a storage folder to contain files. This storage folder should be either on a separate set of spindles or on a shared folder, but for the purposes of this exercise, you will use a separate folder on the system disk. Launch Windows Explorer by clicking Start, right-clicking Computer, and then selecting Explore. Select Local Disk (C:) in the Tree pane, move to the Details pane, and right-click to choose New and then Folder. Name the folder **VirtualMachines** and press Enter to complete the change.
3. Now move to the Explorer's address bar and click the disk; the path should change to C:\. Replace the path with **\\ServerCore01\C\$** and press Enter. Move to the Details pane and right-click to choose New and then Folder. Name the folder **VirtualMachines** and press Enter to complete the change.

4. Return to either Server Manager or Hyper-V Manager and expand Hyper-V Manager to view ServerFull01. Click the server name.
5. Click Hyper-V Settings in the Actions pane.
6. Change the path for Virtual Hard Disks to **C:\VirtualMachines**. Click Virtual Machines in the leftmost portion of the dialog box and change the path for Virtual Machines to **C:\VirtualMachines**. Click OK to apply the change.
7. Return to either Server Manager or Hyper-V Manager and expand Hyper-V Manager to view ServerCore01. Click the server name.
8. Click Hyper-V Settings in the Actions pane.
9. Change the path for Virtual Hard Disks to **C:\VirtualMachines**. Click Virtual Machines in the leftmost portion of the dialog box and change the path for Virtual Machines to **C:\VirtualMachines**. Click OK to apply the change.

The virtual machine and virtual hard drive paths have been changed on each host server.

EXERCISE 3 Create Your First VM

In this exercise you will create your first VM on Hyper-V. This operation will be performed on ServerFull01. The VM will not include an operating system, but it will still be useful because it will include all of the components of a VM in Hyper-V.

1. Log on to ServerFull01 using domain administrator credentials. Either go to Server Manager or launch Hyper-V Manager.
2. Return to either Server Manager or Hyper-V Manager and expand Hyper-V Manager to view ServerFull01. Click the server name.
3. Click New and then click Virtual Machine in the Actions pane. The New Virtual Machine Wizard will open. Review the information on the Before You Begin page and click Next.
4. Enter the name for the new VM as **VM01**. Make sure you select Store The Virtual Machine In A Different Location and leave the folder as is (C:\VirtualMachines). This forces Hyper-V to create a new folder called VM01 under the C:\VirtualMachines folder and store all virtual machine components into this folder (see Figure 2-21). It will make it easier to manage the VM afterward. Click Next.



EXAM TIP VM FILE PLACEMENT

Hyper-V does not place VHD and virtual machine configuration files in the same folder by default. When you generate a new VM, Hyper-V creates the VM configuration file in a subfolder called Virtual Machines and places the VHD file directly in the default VHD path. By selecting the Store The Virtual Machine In A Different Location check box, you automatically force Hyper-V to create a new subfolder with the virtual machine name and place all VM files in this folder.

5. On the Assign Memory page, leave the memory at 512 for this VM and click Next. 512 MB is quite sufficient because this VM will not include an operating system.

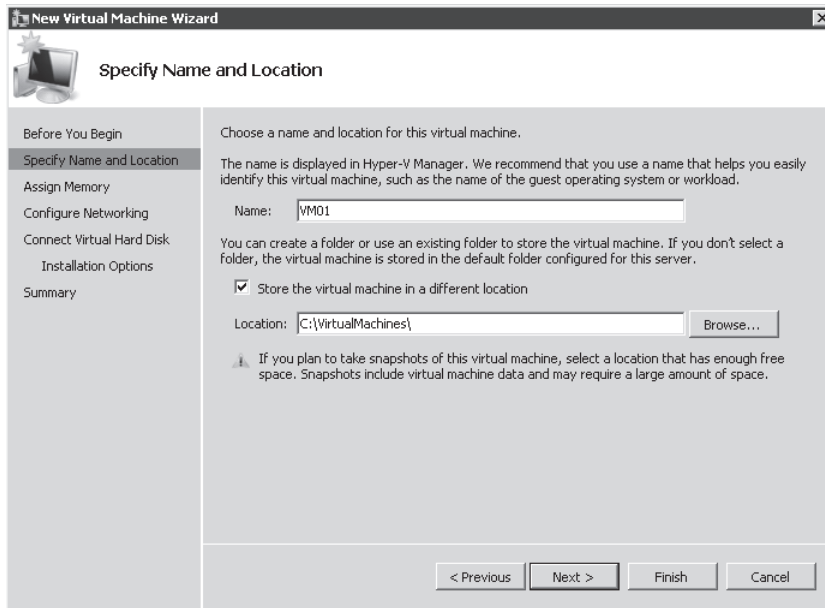


FIGURE 2-21 Naming a VM and storing its files

6. On the Configure Networking page, leave the connection as Not Connected and click Next. You use this page to connect a VM to a virtual network, but because this VM does not include an operating system, no connection is required.
7. On the Connect Virtual Hard Disk page, modify only the size of the virtual hard disk. Change it to **40** GB. Note that Hyper-V will name the VHD file the same as the machine name and use the default VHD location you set earlier. Click Next.



EXAM TIP HYPER-V DEFAULT DISK SIZE

Hyper-V defaults to 127 GB whenever creating a new VHD because 127 is the maximum size of an IDE disk. Because Hyper-V VMs require at least one IDE disk to boot from, this setting has been made the default for all new disks.

8. On the Installation Options page, make sure that Install An Operating System Later is selected and click Next. Note that you can use this page to automatically install an operating system into the VM as you create it (see Figure 2-22).
9. Review your settings and click Finish. You do not need to start this VM once it is created because you will not install an operating system on it.
10. Hyper-V will create the VM and automatically select it in the Details pane once it has been created. Note that the lower portion of the Actions pane now lists commands particular to this VM.

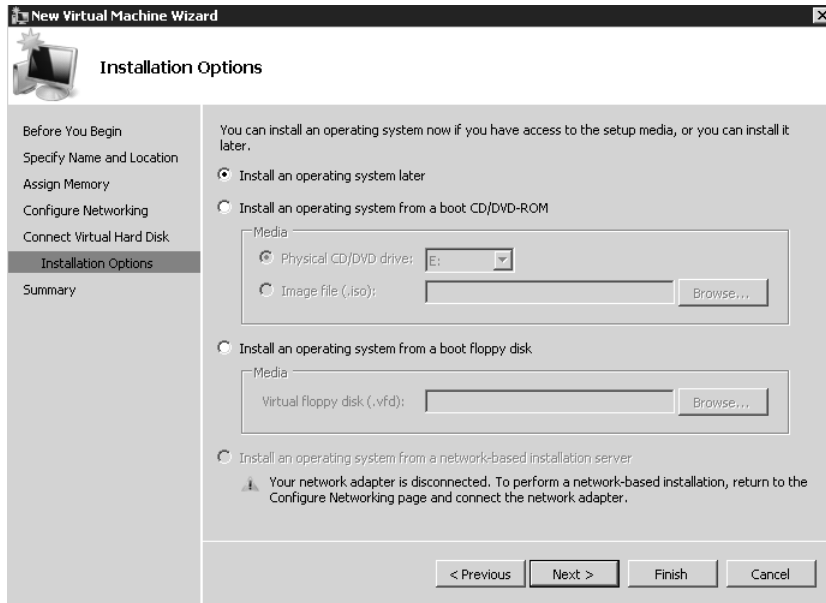


FIGURE 2-22 Choosing to install an operating system on a VM later

EXERCISE 4 Import Your First VMs

In this exercise you will install the two evaluation virtual machines you downloaded in the practice in Lesson 1 of Chapter 1, “Implementing Microsoft Hyper-V”. You will then be able to use them as virtual machines in your Hyper-V environment.

1. In the Practice in Lesson 1 of Chapter 1, you downloaded two files: `HyperV_ServerCorex64_Enterprise.exe` and `WS08_RTM_x64_EnterpriseFull.exe`. Both files include virtual hard drives of machines running Windows Server 2008. Now you will use these files to create the VMs they contain. Begin by making sure the files are located on `ServerFull01` in the `C:\Updates` folder. You shared this folder earlier.
2. Double-click the `WS08_RTM_x64_EnterpriseFull.exe` file and then click **Run**. Click the **Install** button to decompress the VHD file into the `C:\Updates` folder. This places a `WS08_RTM_x64_EnterpriseFull.vhd` file in the folder.
3. Perform the same operation with the `HyperV_ServerCorex64_Enterprise.exe` file. This places a `HyperV_ServerCorex64_Enterprise.vhd` file in the folder.
4. Right-click the `HyperV_ServerCorex64_Enterprise.vhd` and choose **Copy**. Move to the address bar, type `\\ServerCore01\C$`, and press **Enter**. Open the **VirtualMachines** folder and right-click to choose **New** and then **Folder** and name the folder **WS08_Core**. Double-click the new folder name to open the folder. Right-click the folder and choose **Paste**. This will copy the VHD file into the folder.
5. Return to the `C:\Updates` folder of `ServerFull01`. Copy the `WS08_RTM_x64_EnterpriseFull.vhd` file, move to the `C:\VirtualMachines` folder, right-click to choose **New**

and then Folder, and name the folder **WS08_Full**. Double-click the new folder name to enter the folder. Right-click the folder and choose Paste. This will copy the VHD file into the folder.

6. Return to your Hyper-V console. You will now create two VMs—one on ServerFull01 and one on ServerCore01 using these VHD files. Click ServerFull01 in the Tree pane.
7. Click New and then Virtual Machine in the Actions pane. The New Virtual Machine Wizard will open. Review the information on the Before You Begin page and click Next.
8. Enter the name for the new VM as **WS08_Full** and select Store The Virtual Machine In A Different Location. Click Next.
9. On the Assign Memory page, change the memory to **2048** for this VM and click Next.
10. On the Configure Networking page, leave the connection as Not Connected and click Next.
11. On the Connect Virtual Hard Disk page, choose Use An Existing Hard Disk and click Browse to navigate to the C:\VirtualMachines\WS08_Full folder. Select the VHD in this folder, choose Open, and then click Next.
12. Review your settings and click Finish. You do not need to start this VM once it is created because you will work with it later. Hyper-V will create the VM and automatically select it in the Details pane once it has been created.
13. Click ServerCore01 in the Tree pane.
14. Click New and then Virtual Machine in the Actions pane. The New Virtual Machine Wizard will open. Review the information on the Before You Begin page and click Next.
15. Enter the name for the new VM as **WS08_Core** and select Store The Virtual Machine In A Different Location. Click Next.
16. On the Assign Memory page, change the memory to **2048** for this VM and click Next.
17. On the Configure Networking page, leave the connection as Not Connected and click Next.
18. On the Connect Virtual Hard Disk page, choose Use An Existing Hard Disk and click Browse to navigate to the C:\VirtualMachines\WS08_Core folder. Select the VHD in this folder, choose Open, and then click Next.
19. Review your settings and click Finish. You do not need to start this VM once it is created because you will work with it later. Hyper-V will create the VM and automatically select it in the Details pane once it has been created.

You have now created your first VMs from existing VHDs.

EXERCISE 5 Examine VM File Locations

In this exercise you will examine how Hyper-V generates and manages the files that make up a VM.

1. Return to Windows Explorer on ServerFull01 and move to the C:\VirtualMachines folder.
2. Note that this folder contains two folders: VM01 and WS08_Full. Double-click VM01.

3. Note that this folder includes two items: a folder named Virtual Machines and the VM01.vhd file. Double-click the Virtual Machines folder.
4. Note that this folder includes two items: a <GUID>.xml file and a <GUID> folder. The XML file is the configuration file. Double-click it to view its content. Internet Explorer will open. Respond to any warnings.
5. Scroll through the file to view its contents. Note that it outlines all of the properties of the virtual machine (see Figure 2-23). Close Internet Explorer when you are done.

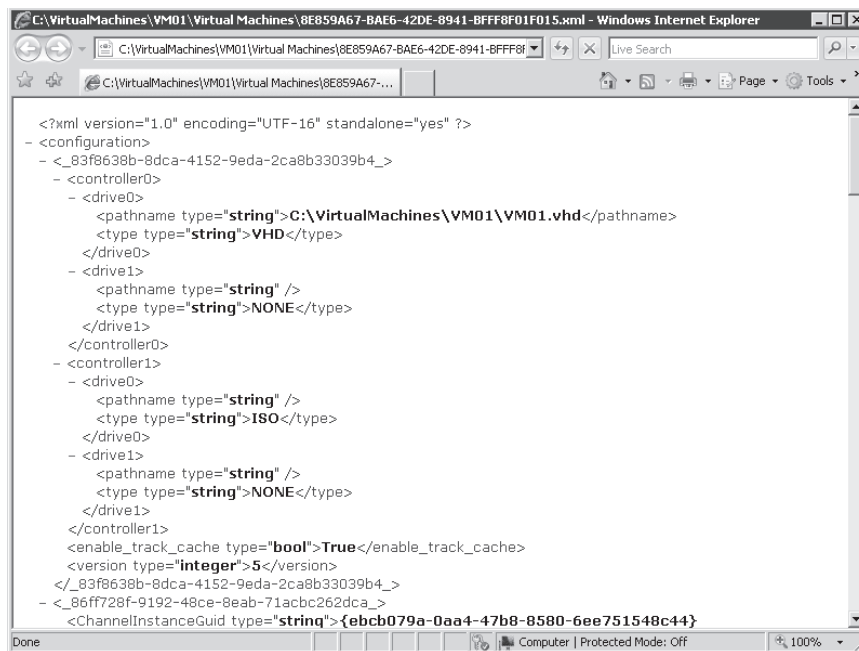


FIGURE 2-23 Examining a VM configuration file



EXAM TIP HYPER-V VM CONFIGURATION FILES

Hyper-V uses Extended Markup Language (XML) files to store virtual machine configurations. Previous versions of Microsoft virtualization technologies such as Virtual Server and Virtual PC used standard text files with a VMC extension. Because of this, you cannot directly transfer VMs from these tools to Hyper-V. Note, however, that virtual hard disk files remain compatible and can be transferred from one to another.



Quick Check

1. What are the two consoles that Hyper-V relies on to manage hosts and virtual machines?
2. What is the default location for virtual machine configuration files and virtual hard drives?

Quick Check Answers

1. The two consoles are the Server Manager console on the full installation and the Hyper-V Manager console on Windows Server 2008 full installations and Windows Vista with Service Pack 1.
2. The default location for virtual machine configuration files is the public user profile; for virtual hard drives, the default location is the Windows ProgramData folder.

Lesson 3: Configuring Virtual Networking

Hyper-V relies on virtual networks to provide networking services to VMs. Each enlightened VM can access up to 12 virtual network cards—8 virtual network adapters and 4 legacy virtual network adapters. Because the virtual network adapters rely on the VMBus to communicate with adapters through the parent partition, they perform much better than the legacy virtual network adapters. Legacy virtual network adapters must use device emulation to communicate with the virtual networks in Hyper-V. Emulation always performs slower than devices relying on the VMBus.

After this lesson, you will understand:

- The virtual network types that Hyper-V supports.
- Hyper-V virtual switches.
- The Virtual Network Manager Tool.
- Virtual local area network (VLAN) tagging.

Each is an important part of virtual networking with Hyper-V.

Estimated lesson time: 30 minutes

Working with Virtual Network Types in Hyper-V

When a virtual machine connects to a network in Hyper-V, it uses either the network adapters or legacy network adapters Hyper-V provides to make the connection. Enlightened VMs can use both network adapter types, but legacy machines—machines that need to use device emulation in Hyper-V—can only access the network through the legacy network adapter type. However, each adapter type can support several types of networking connections (see Figure 2-24).

- **External virtual networks** For creating a connection to a physical network adapter, the virtual machine can access the physical network, other virtual machines on this network, the host server, and all other external machines, virtual or physical, linked to this network. This network type is most often used in production environments where all machines need to communicate with each other, with the host, and with external machines.
- **Internal virtual network** For creating a connection that supports communications between the host server and the VM and other virtual machines on the same network. The internal network is not bound to a physical adapter; because of this, it limits communications. This network type is often used for testing environments where you want VMs to communicate with each other and you need the VMs to communicate with the host server as well. For example, you download updates to the host server and make them available from there to the VMs on the internal network.

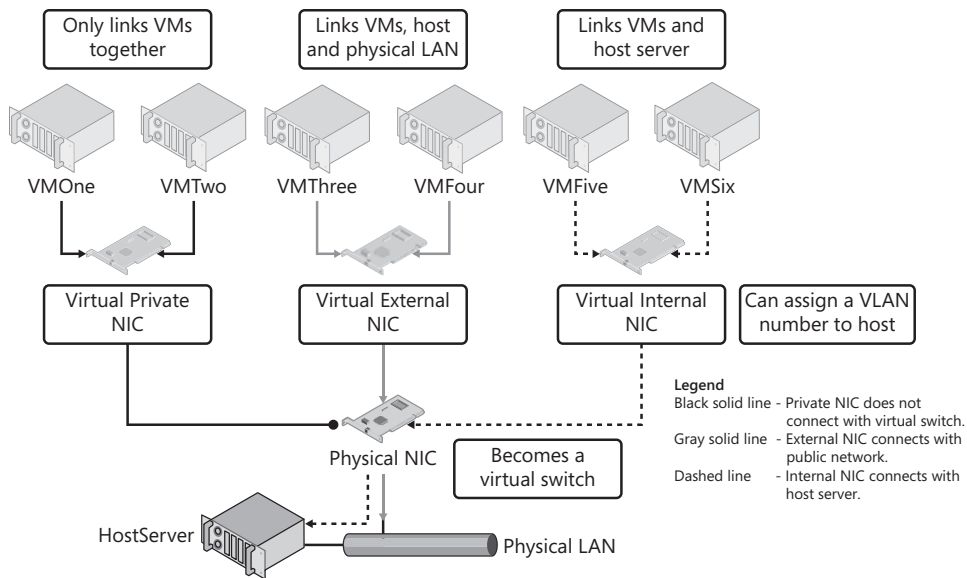


FIGURE 2-24 Virtual network types in Hyper-V

- **Private virtual network** For creating a network that limits communications to other virtual machines on the same network only. This network type is also not bound to a physical adapter. It also does not include a virtual network adapter on the host, which means that it cannot communicate with the host server. Use this network type to isolate traffic to VMs only and cut them off from all other environments. A good example is a perimeter network on a three-homed computer running an isolation environment.

Each virtual machine can be connected to any of the three network types. In addition, you can modify the connection in a virtual machine at any time, even during VM operation. This flexibility gives you full control over how VMs communicate.

MORE INFO SCREENCAST ON HYPER-V NETWORKING

To view a screencast on how to configure virtual networking in Hyper-V, go to <http://go.techtarget.com/r/5927598/30819>.

The graphical interface of Hyper-V Manager gives you access to the three most common network interface types in Hyper-V. There is also a fourth type, which should only be created through Windows Management Instrumentation (WMI) scripting. This fourth network adapter type—the Dedicated adapter—acts like the External type, but the difference is that it is not bound to the parent partition in any way. It is dedicated to virtual machines. VMs that are linked to the dedicated network interface type can communicate with each other and with external machines, but not with the parent partition, or at least not directly with the parent partition. Communications with the parent partition are still possible, but require another physical adapter to which the parent partition is bound. Communications go from

the dedicated virtual network adapter through the virtual switch, out to the external world, and then back into the host system through the second physical network adapter.

MORE INFO MORE ON NETWORKING WITH HYPER-V

John Howard, one of the program managers for the Hyper-V team, has some great postings on virtual networking in Hyper-V, which you can find at <http://blogs.technet.com/jhoward/default.aspx>. One of the most useful posts is about basic networking in Hyper-V: <http://blogs.technet.com/jhoward/archive/2008/06/16/how-does-basic-networking-work-in-hyper-v.aspx>.

UPDATE ALERT NETWORK ADAPTER TEAMING AND TCP CHIMNEY OFFLOAD

Windows Server 2008 does not have official support for *network teaming*—the integration of two network adapters to appear as one and provide redundancy for traffic management—but it does have support for TCP Chimney Offload—the offloading of network data transfer management from the main CPU to a processor on the network adapter. Note that Hyper-V does not support either of these technologies. See Knowledge Base Article number 951037 at <http://support.microsoft.com/kb/951037> for more information. Note that Hyper-V R2 includes support for TCP Chimney Offloads through the use of VM queues. It also includes support for Jumbo frames and network adapter teaming.

When you create a virtual network on Hyper-V, you transform the physical network adapter into a virtual network switch. Hyper-V installs the Microsoft Virtual Network Switch Protocol and activates it. This protocol then becomes the only active protocol on a physical adapter once it is converted to a virtual network switch. All other network adapter settings are automatically deactivated (see Figure 2-25).

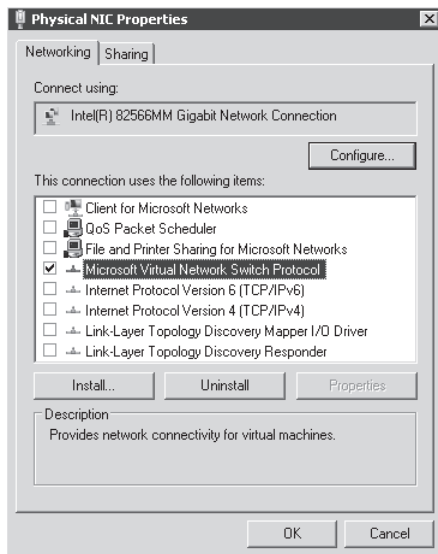


FIGURE 2-25 The Microsoft Virtual Network Switch Protocol is activated.

Because of this, each Hyper-V host should include at least two network adapters and possibly more. Network adapters should be set as follows:

- The first network adapter should be used to create a virtual network switch for virtual machines.
- The second network adapter should be reserved for all management access to the parent partition in Hyper-V.
- Other network adapters should be in place if you use iSCSI connectivity to access remote storage. The number of adapters you use for this will depend on adapter speed and the amount of data you need to transfer, but using two adapters is good practice because they provide redundant paths to the remote storage.
- Other network adapters can be installed to act as additional virtual network switches. The number of adapters you need depends on the number of VMs you intend to run on the host, but having at least two virtual network switches is good practice because it provides redundant paths for your VMs.

As you can see, you need to carefully plan the installation of network adapters in your Hyper-V hosts. Fortunately, network adapters can be added at any time in a Windows Server 2008 computer because of its plug and play capabilities.



EXAM TIP WIRELESS NETWORK ADAPTERS

Hyper-V cannot use wireless network adapters because the parent partition cannot bind them to the Microsoft Virtual Network Switch Protocol. Don't be fooled by this on the exam.

Configuring Hyper-V on Full vs. Server Core Installations

In Lesson 1 of this chapter, you installed and enabled Hyper-V on both a full installation and on a Server Core installation. Remember that when you enable Hyper-V on the full installation, you run through pages in a wizard to complete the operation. One of these pages requests the creation of a virtual network (see Figure 2-26). When you choose to do this, Hyper-V automatically transforms the settings of the physical adapter into a virtual network switch and creates an external virtual network adapter for the parent partition. This virtual network adapter is assigned all of the settings that were previously assigned to the physical network interface. This is why you lose connectivity when you perform this through the Remote Desktop and your Hyper-V host has only one network adapter: The process transforms the existing adapter into a virtual switch and creates the new virtual adapter, and connectivity is temporarily lost.

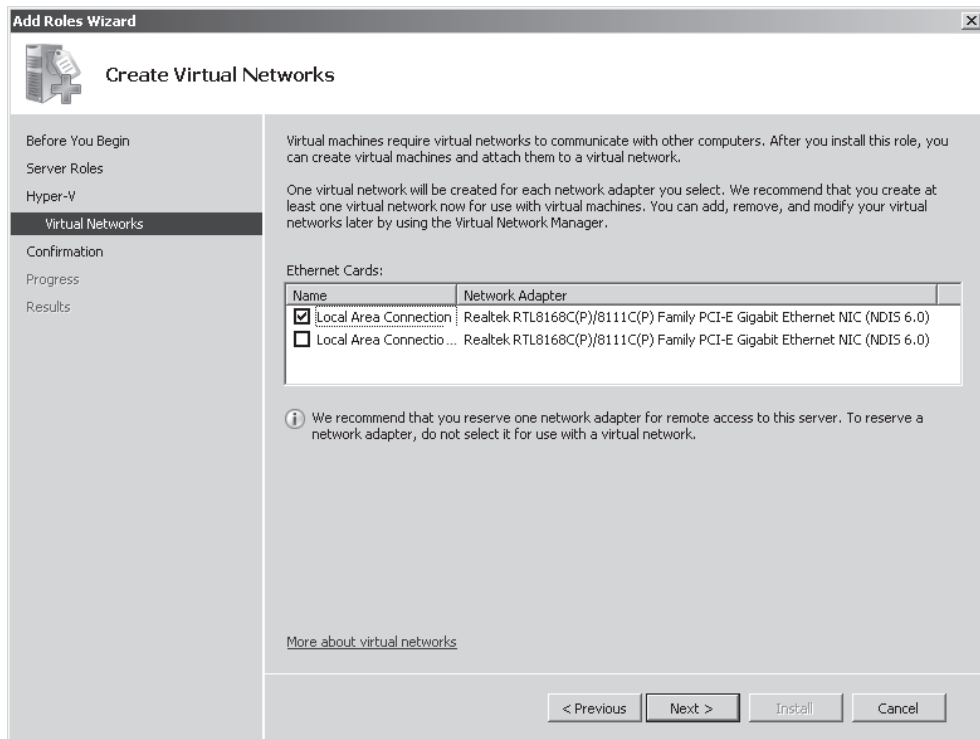


FIGURE 2-26 The Create Virtual Networks page of the Hyper-V role Installation Wizard

After the virtual switch is created, the network adapter begins to act like a normal switch, except that the switch is software-based and ports are added and removed dynamically as needed.

This process is not duplicated when you work with Hyper-V on Server Core. Because you use a command line to add the Hyper-V role, you do not get to create a virtual network switch. Instead, the virtual network switch must be created manually after the role installation and its corresponding reboot.

External connections will automatically be linked to the virtual network switch. In this case, all network traffic is routed through the virtual switch as if it were a physical switch (see Figure 2-27). Because the external connection is linked to a port on the virtual switch, applications within the VM that must connect externally will have all traffic routed through the virtual network adapter to the port on the virtual switch, then through the physical network adapter and out to the external world.

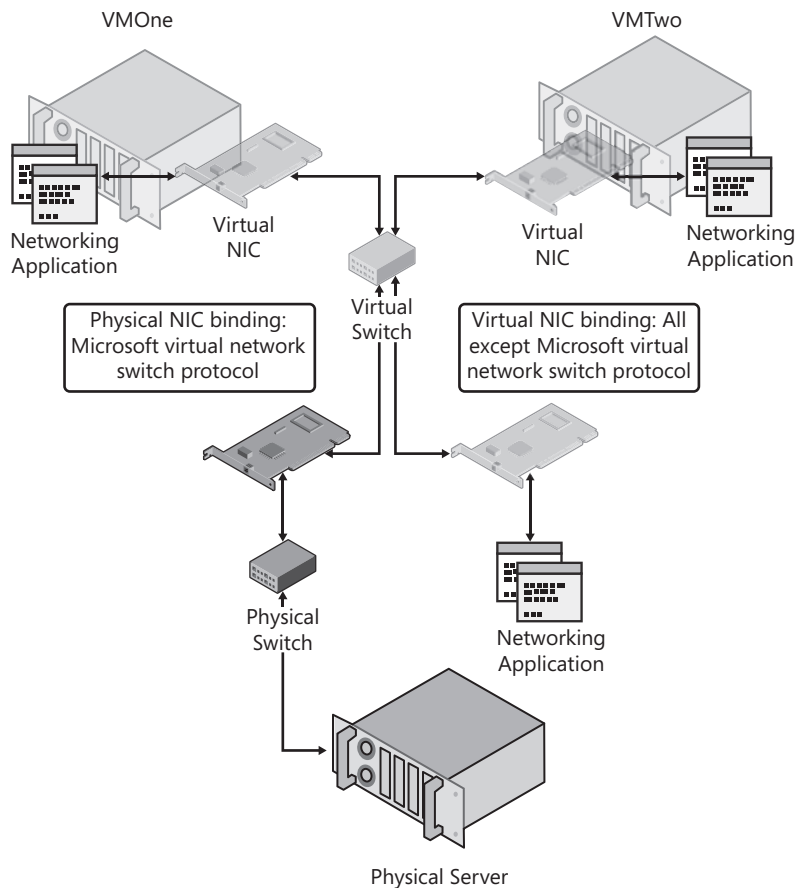


FIGURE 2-27 The operation of an external network in Hyper-V

Internal connections are not linked to the virtual network switch. Because of this, they can only communicate with the host and with other virtual machines bound to the same network (see Figure 2-28).

Private networks are not linked to the virtual network switch either. They only provide access to other virtual machines linked to the same network (see Figure 2-29).

Hyper-V can emulate two different types of network adapters: the network adapter and the legacy network adapter. For virtual machines to be able to work with the network adapter, they must be able to install and run the Hyper-V Integration Services. If the operating system in a VM does not support Integration Services, it must use the legacy network adapter, which emulates an Intel 21140-based PCI Fast Ethernet Adapter. Note that the legacy network adapter is also required if a virtual machine needs to boot from a network, such as when you use the Preboot Execution Environment (PXE) to boot a machine from the network to install an operating system into it. In this example, there is no operating system yet on the VM and thus no Integration Services are installed. This is why only the legacy network adapter works in this case.

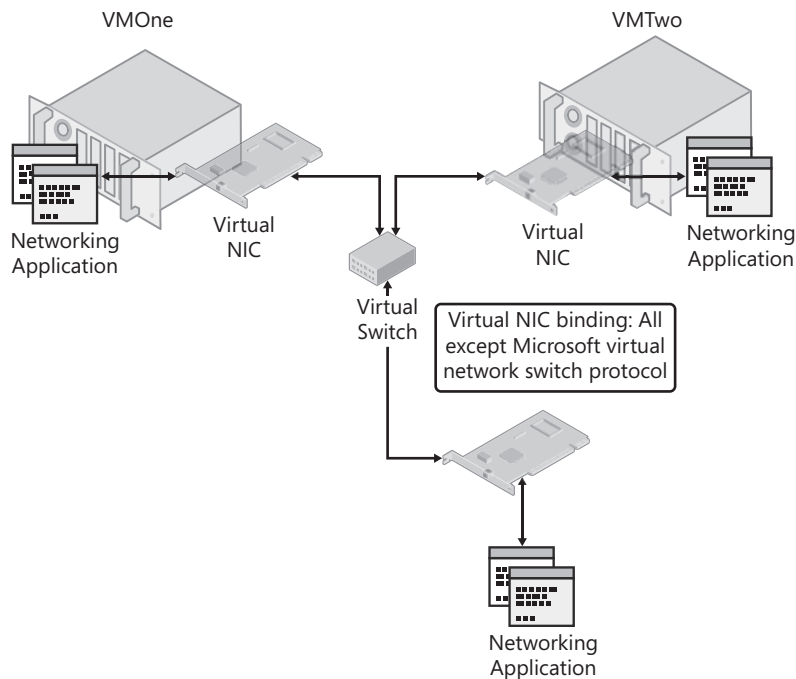


FIGURE 2-28 The operation of an internal network in Hyper-V

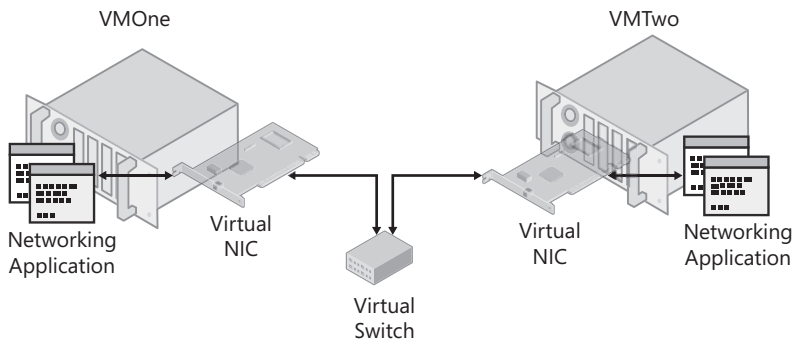


FIGURE 2-29 The operation of a private network in Hyper-V



EXAM TIP LEGACY NETWORK ADAPTERS

Make sure to remember that you must use the legacy network adapter to have a machine boot from the network—this is definitely on the exam.

When VMs need to communicate to the parent partition, they can do so in one of two ways. First, the VM can be linked to an external virtual network adapter that then routes the traffic to the port on the virtual switch and out to the physical adapter. The traffic then returns through a second physical adapter to communicate with the Hyper-V system. Second, the VM can be routed directly through the virtual network adapter to the parent partition. Although this

second method is more efficient because the traffic does not have to loop back into the system, this won't occur until the virtual network uses its built-in algorithm to determine the most efficient port to direct traffic to and then send the traffic to that port. Traffic is sent to all ports by default until the algorithm kicks in and determines the best possible route.

Using the Virtual Network Manager Tool

You rely on the Virtual Network Manager tool within Hyper-V Manager to create and modify virtual networks. As a best practice, you should create at least one of each of the three virtual network adapter types and name them appropriately. This will facilitate your choices when you create or configure virtual machines and you need to attach them to a given network.

As mentioned in the previous section, when you install the Hyper-V role on a full installation and you select to create a virtual network during the installation process, Hyper-V automatically turns the selected physical adapter into a virtual network switch and creates the first external virtual network adapter. However, Hyper-V does not rename either adapter, which can lead to some confusion when working with network adapters on Hyper-V hosts.

Creating virtual network adapters is relatively simple. You use the Virtual Network Manager link in the Actions pane to launch the tool (see Figure 2-30). This tool lets you create any of the three network adapter types as well as rename and modify existing virtual network adapters. If you are using the full installation of Windows Server 2008, the first thing you should do is rename the external virtual network adapter that was automatically created during the installation of the Hyper-V role to a more significant name such as Hyper-V External.

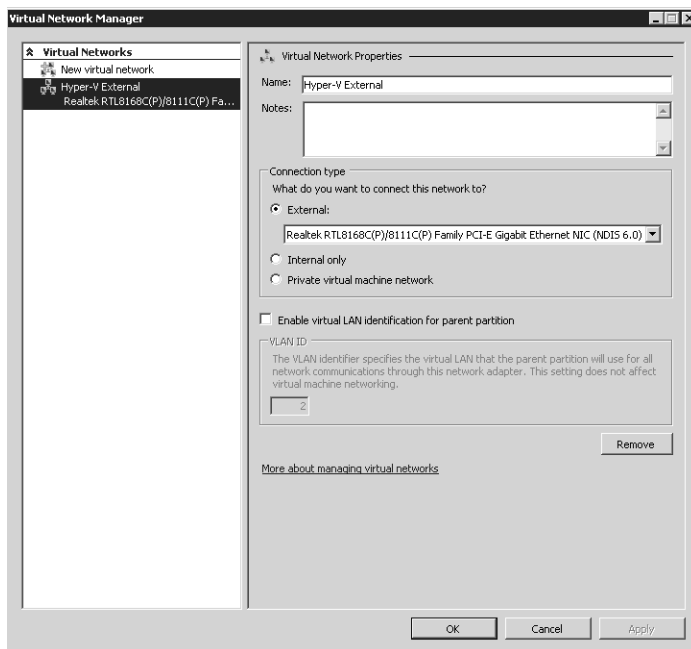


FIGURE 2-30 Using the Virtual Network Manager

You can then proceed to create additional networks. Create at least one of each of the three network adapter types. To do so, you need to click New Virtual Network to the left of the dialog box, choose the type of network you want to create, and then click Add. This creates the network adapter. Name it and provide a description for the adapter. Click Apply to set your changes. Repeat the process for each adapter type.

Note that you can assign a virtual local area network (VLAN) number to both the external and internal network adapter types. This assignment can be done at any time, either during the creation of a network adapter or through reconfiguration once it has been created. This is done through the Enable Virtual LAN Identification For The Parent Partition option and is used to specify an identification number to isolate network traffic from the operating system that runs in the parent partition (see Figure 2-31).

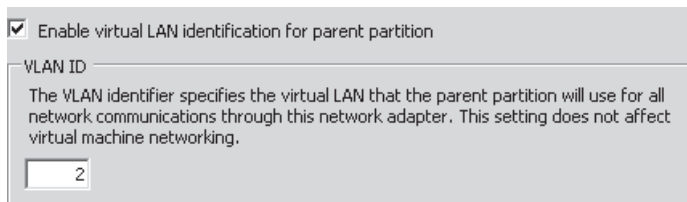


FIGURE 2-31 Assigning a VLAN to the parent partition

You can use virtual LAN identification as a way to isolate network traffic. However, this type of configuration must be supported by the physical network adapter. VLAN tagging isolates all parent partition traffic using this network adapter. This does not affect the operation of a virtual machine in any way, but it segregates parent partition traffic from virtual machine traffic. You can also assign VLANs to virtual machines through the virtual machine configuration (see Figure 2-32). In this case, the traffic initiated by the virtual machine going through this network adapter will be limited to the virtual LAN ID number you assign.

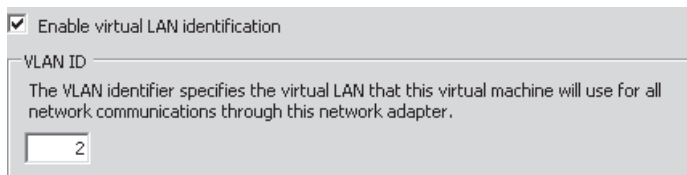


FIGURE 2-32 Assigning a VLAN to a network adapter in a VM

MORE INFO PARENT PARTITION VLAN TAGGING

For more information about configuring virtual LAN identification for the parent partition, see the Hyper-V deployment content at <http://go.microsoft.com/fwlink/?LinkID=108560>.

Note that when you create virtual network adapters, corresponding adapters are created in the network connections of the parent partition. This occurs for both the external and internal network adapter but not for the private network adapter because the private adapter is not bound to the physical adapter in any way.

You should rename the connections created in Network Connections so that you can more easily identify which connection is which (see Figure 2-33). Do this using the Rename command in the shortcut menu for each adapter.

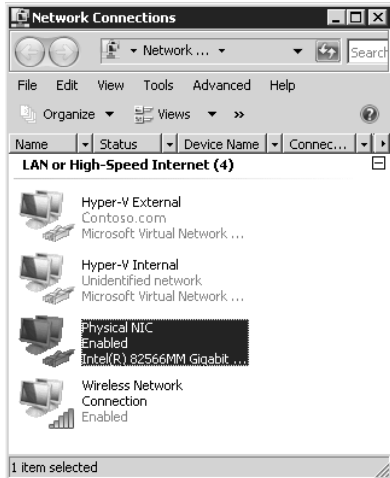


FIGURE 2-33 Renaming adapters to better identify them

PRACTICE Working with Virtual Networks

In this practice, you will configure virtual networking on your two host servers, ServerFull01 and ServerCore01. This practice consists of two exercises. The first focuses on creating additional virtual network adapters on the full installation of Windows Server 2008. In the second, you create a virtual network switch on Server Core and then you create virtual network interface cards on Server Core. When this practice is complete, your host servers will be configured to support all types of networking in Hyper-V.

EXERCISE 1 Create Virtual Network Interface Cards on a Full Installation

In this exercise you will configure additional network adapters on the full installation of Windows Server 2008. This exercise is performed on ServerFull01. Log in 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 network. This network was created when you installed the Hyper-V role.
3. Rename the existing connection. Click the connection in the left pane of the dialog box, select the name in the right pane, and rename it **Hyper-V External**. Click Apply. Note that this network is of an external type and is bound to one of your physical network interfaces.

4. Now create a second virtual adapter. Click New Virtual Network in the left part of the dialog box, choose Internal, and then click Add.
5. Name the adapter **Hyper-V Internal** and make sure Internal Only is selected as the connection type. Note that as with the External connection type, you can assign a VLAN to the parent partition. You do not need to do so at this time. Click Apply.
6. Now create a third virtual adapter. Click New Virtual Network in the left part of the dialog box, choose Internal, and then click Add.
7. Name the adapter **Hyper-V Private** and make sure Private Virtual Machine Network is selected as the connection type. Note that this network type does not allow you to assign a VLAN to the parent partition because there is no link to the parent partition in this network connection type. Click OK. Your three network types have been created.
8. 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 Control Panel. In Control Panel, 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.
9. Rename each connection. You can check each connection's properties to make sure you are renaming the appropriate network. Begin with the new virtual switch, which actually is your physical network adapter. Right-click it and choose Rename. Type **Physical NIC** and press Enter. The properties of this NIC should only list the Microsoft Virtual Network Switch as enabled.
10. Repeat the process with each adapter in the window. Rename the external adapter to **Hyper-V External** and the internal adapter to **Hyper-V Internal**. Your Hyper-V network configuration is complete.

EXERCISE 2 Create a Virtual Switch on a Server Core installation

In this exercise you will create a virtual network switch on Server Core. Note that the Server Core Hyper-V role installation does not create this virtual switch the way the full installation does. You must create this switch interactively. 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. Note that there is no existing network adapter in this interface.
3. The New Virtual Network and the External Network type should already be selected. Click Add.
4. Name this adapter **Hyper-V External**, make sure the External connection type is selected, and make sure the appropriate adapter is selected in the drop-down list.

This adapter should not be the one you are using to remotely connect to Server Core. Do not apply a VLAN to the parent partition at this time. Click Apply. The Apply Networking Changes warning will appear (see Figure 2-34). Click Yes. You shouldn't have issues with this change as long as you selected the appropriate adapter in the drop-down list. If you don't, you will lose connectivity with the Server Core computer.

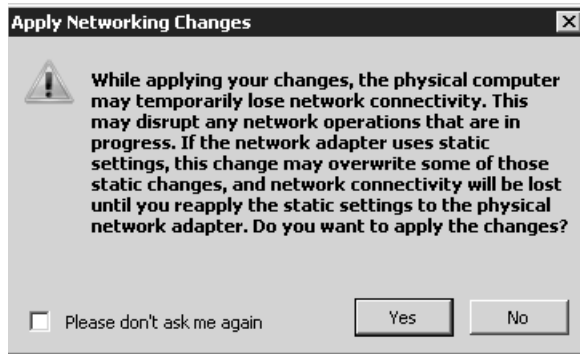


FIGURE 2-34 The Hyper-V Networking Changes warning

5. Create a second virtual adapter. Click New Virtual Network in the left part of the dialog box, choose Internal, and then click Add.
6. Name the adapter **Hyper-V Internal** and make sure Internal Only is selected as the connection type. Note that as with the External connection type, you can assign a VLAN to the parent partition. You do not need to do so at this time. Click Apply.
7. Create a third virtual adapter. Click New Virtual Network in the left part of the dialog box, choose Internal, and then click Add.
8. Name the adapter **Hyper-V Private** and make sure Private Virtual Machine Network is selected as the connection type. Note that this network type does not allow you to assign a VLAN to the parent partition because there is no link to the parent partition in this network connection type. Click OK. Your three network types have been created.
9. You can also rename the network adapters in Server Core to make them easier to manage. To do so, you need to log on to the Server Core machine and use the netsh command to rename each connection. Log on with domain administrator credentials.
10. Begin by listing the adapters, making note of the adapter ID number and then rename each adapter. Use the following commands. In this case, the old connection names were Local Area Connection 3 and Local Area Connection 4. Your connection names may differ from these. This is why you run the show interface command first.

```
netsh interface ipv4 show interface
netsh interface set interface name="Local Area Connection 3" newname
    ="Hyper-V External"
netsh interface set interface name="Local Area Connection 4" newname
    ="Hyper-V Internal"
```


If you run the `show interface` command again (hint: use the up arrow to call the command back), you will see that the interfaces have been renamed. Networking is ready on this server.

✓ Quick Check

1. How many virtual network cards can each enlightened VM access?
2. What is the difference between an external connection and an internal connection?

Quick Check Answers

1. Each enlightened VM can access up to 12 virtual network cards—8 virtual network adapters and 4 legacy virtual network adapters.
2. The external adapter is a connection to a physical network adapter. Machines using this adapter can access a physical network, other virtual machines on this network, the host server, and all other external virtual or physical machines connected to this network. The internal adapter is a connection that only supports communications between the host server and the VM and other virtual machines on the same network.

Case Scenario: Networking Virtual Machines

In the following case scenario, you will apply what you have learned about preparing your Hyper-V host servers. 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 the Graphics Design Institute and you have been asked to prepare the network connections required to host virtual machines on a Hyper-V server. Table 2-3 outlines the VMs you will require and the type of networking traffic each will generate. Your job is to propose which type of virtual network adapter should be used for each VM.

TABLE 2-3 Virtual Machine List

VIRTUAL MACHINE	NETWORK TRAFFIC TYPE
DC01	AD DS for a production forest.
DC02	AD DS for a production forest.
Web01	Web server running Internet Information Services for a public Web site.
File01	Internal production file server.
DCTest01	AD DS for a test forest. This forest should not have any connection to the production forest.
WebTest01	Staging Web server for the production Web site.

1. Based on the information in Table 2-3, which connection type would you use for the production machines?
2. Which connection type should you use for the test machines?
3. The Web production team wants to be able to upload content into the test Web server, and once it passes approval, they want to automatically upload it from the test server to the production server. Which type of connections should each server contain to make this scenario work?

Suggested Practices

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

Windows Server 2008 Configuration

- **Practice 1** Take the time to become thoroughly familiar with the configuration of the full installation. It will be useful for the exam, and also for the configuration of your own servers.

- **Practice 2** Take the time to become thoroughly familiar with the configuration of Server Core installations. It will be useful for the exam and also for the configuration of your own servers.

Hyper-V Role Installation

- **Practice 1** Take the time to become familiar with the process used to enable Hyper-V. There are several intricacies in this process and a few differences between the process you use on the full installation and the Server Core installation.

Virtual Network Configuration

- **Practice 1** Practice installing virtual adapters of each type. Learn the configuration parameters for each. Also take the time to view the settings in each adapter.
- **Practice 2** Practice installing virtual adapters of each type on Server Core. Use the command line to view adapter settings and gain a better understanding of virtual networking on this installation type.

Chapter Summary

- Each server that is deployed should be configured before use. The full installation includes a window called Initial Configuration Tasks (ICT) that provides a single interface to perform several of these configuration activities. Server Core does not have a graphical interface but it is important to perform similar configuration tasks. The entire process in Server Core is performed through the command line.
- The Hyper-V role installation is similar on the full installation and the Server Core installation. You need to download and install the Hyper-V RTM update and install other required updates such as the language pack update or additional updates based on which kind of system you use to manage Hyper-V.
- The machines on which you install Hyper-V must include hardware-assisted virtualization and Data Execution Prevention. They must be accessible from the BIOS system. Both must be enabled for Hyper-V to operate.
- Hyper-V relies on two consoles to manage hosts and virtual machines. The Server Manager console provides a single interface for all server operations. This console includes a server summary, a roles summary, a features summary, and access to additional resources and support. It also includes a Hyper-V Manager section once the role is installed. In addition, you can use the stand-alone Hyper-V Manager console. This console includes controls for virtual machines, VM snapshots, and Hyper-V server. This console can run on Windows Server 2008 or on Windows Vista with Service Pack 1.
- By default, the storage location for virtual machine configuration files and virtual hard drive is not in the same container. The first location is in the public user profile and the second location is in the ProgramData folder. It is good practice to keep all virtual machine files together to simplify VM management.

- In Hyper-V, virtual machines connect to a network using network adapters or legacy network adapters. Enlightened VMs can use both types but legacy machines need to use device emulation. There are several types of networking connections: external, internal, private, and dedicated.
- You use the Virtual Network Manager tool in Hyper-V Manager to manage virtual network cards.
- Don't forget that Hyper-V cannot use wireless network adapters because the parent partition cannot bind them to the virtual switch.
- In Server Core, you use a command line to add the Hyper-V role and because of this, the virtual network switch is not created during this process. You must create it manually later.

Completing Resource Pool Configurations

Your host server infrastructure is almost ready to manage and maintain virtual machines. Only a few elements need to be finalized before this can happen. So far, you have installed and implemented the Hyper-V role on both the full and the Server Core installations of Windows Server 2008. You discovered that Hyper-V required special hardware or x64 hardware that also included processors with hardware-assisted virtualization. You also discovered how Hyper-V's parent and child partitions interact with each other to support virtual machine operation. You learned that Hyper-V manages both enlightened and legacy guest operating systems in virtual machines.

However, one of the most important aspects of a Hyper-V deployment and the transformation of production computers into virtual machines is fault tolerance. When a Hyper-V host runs 10 or more production virtual machines, you simply cannot afford any downtime from the host server. This is why you must cluster your host servers, ensuring that the workloads of each node in the cluster are protected by other nodes in the cluster. If one host fails, all of the virtual workloads on that host are automatically transferred to other nodes in the cluster to ensure service continuity. It's bad enough when you have one server failure. You cannot afford to have multiple virtual workloads failing at the same time because the host server they were running on was not configured to be fault tolerant. Fault tolerance for Hyper-V hosts is provided by the Windows Server 2008 Failover Clustering feature.

In addition, you must ensure that you can manage your host servers from remote systems, especially if you have configured your Hyper-V hosts to run the Server Core installation of Windows Server 2008. Remote management tools include the Hyper-V Manager, which is available as part of the Remote Server Administration Tools (RSAT) for Windows Server. Hyper-V Manager is sufficient to manage a small number of host servers. However, when you begin to create massive farms of host servers all clustered together, you begin to see the failings of Hyper-V Manager and need a more comprehensive tool, one that will let you manage host server farms as a whole. For Hyper-V, this tool is System Center Virtual Machine Manager 2008 (SCVMM). Part of the System Center family of Microsoft management tools, Virtual Machine Manager can manage both Hyper-V and Virtual Server. It also supports the migration of physical computers to virtual machines or virtual machines in another format to Hyper-V VMs. Finally, it lets you manage multiple hypervisors in the event that you have already proceeded with server virtualization and you are running tools such as VMware ESX Server as well as Hyper-V.

Before you move on to populating your host server farm, you need to ensure that your Hyper-V hosts are running at their optimum peak. This ensures that your systems provide the very best platform to host the VMs you use in production. Then and only then can you move your production systems into VMs and transform your data center.

Exam objectives in this chapter:

- Configure Hyper-V to be highly available.
- Configure remote administration.
- Manage and optimize the Hyper-V Server.

Before You Begin

To complete this chapter, you must have:

- Access to a setup as described in the Introduction. At least two machines are required: one running a full installation of Windows Server 2008 and the other running Server Core. These machines were prepared in the practices outlined in Lesson 3 of Chapter 1, "Implementing Microsoft Hyper-V" and then configured with the Hyper-V role in Chapter 2 "Configuring Hyper-V Hosts."
- In this chapter, you will continue the build process for these machines and transform them into a Failover Cluster. You will also create a System Center Virtual Machine Manager machine to manage this cluster.

Lesson 1: Configuring Hyper-V High Availability

High availability is an absolute must for any host server environment because each host server runs several virtual machines. No one can afford the potential loss of productivity that would be caused if all of the production VMs on a host server were to fail because the host server failed. This is why this lesson forms a key element of any resource pool infrastructure.

After this lesson, you will be able to:

- Understand Failover Clustering principles in general.
- Understand Failover Clustering requirements.
- Create a two-node Hyper-V cluster.
- Manage Hyper-V host clusters.

Estimated lesson time: 60 minutes

Understanding Failover Clustering

Microsoft has enhanced the Failover Clustering feature in Windows Server 2008 to better support the concept of host servers. Prior to the release of Windows Server 2008 with Hyper-V, failover clusters were primarily used to protect critical workloads such as Microsoft Exchange e-mail systems, SQL Server database systems, file and print systems, and other workloads that organizations felt required an “always-on” capability. Note, however, that not all Windows workloads are suited to failover clustering. Windows Server 2008 also includes the ability to support fault tolerance through the Network Load Balancing (NLB) feature.

NLB creates a redundant service by using a central Internet Protocol (IP) address for a given service. The NLB service then redirects the traffic it receives on this central address to servers that are part of the NLB farm. When a server fails, the NLB service automatically takes it out of the farm temporarily and redirects all traffic to the other available farm members. Because NLB is a traffic director, all of the computers in an NLB farm must include identical content to provide an identical experience to the end user. This is one reason why front-end Web servers are ideally suited to NLB farms. Web servers often include read-only content that users can browse through. Whether the user is on one server or another does not matter because all of the content is identical. Because of the nature of the NLB service, the services that are best suited to participate in an NLB farm are called *stateless services*—the user does not modify information in a stateless farm and only views it in read-only mode. NLB clusters can include up to 32 nodes (see Figure 3-1).

Failover clusters are different from NLB clusters in that they include *stateful services*—services that support the modification of the information they manage. Database stores, mailbox stores, file stores, and printer stores are all examples of services that manage stateful information—information that is often modified each time a user accesses it. Because of this, the failover cluster does not include machines with identical content. Although each machine includes identical services, the information store they link to will be unique. In addition, because the information store is unique, only one server hosts a particular service at one point in time. This is different from the NLB cluster where each machine provides the same service.

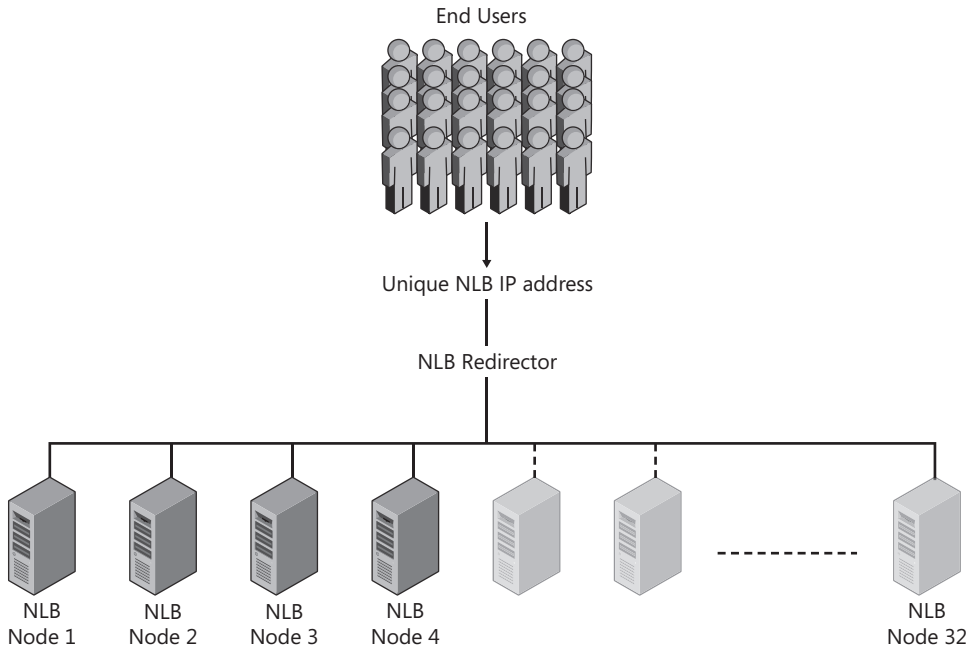


FIGURE 3-1 Stateless NLB clusters can include up to 32 nodes.

Windows Server Failover Clustering supports two types of configurations: the single-site cluster and the multi-site cluster. In a single-site cluster, cluster nodes are linked to a single shared storage matrix (see Figure 3-2). This shared storage container is divided up into several containers, or logical units (LUNs), each of which is tied to a particular service. Each of the nodes in the cluster that provide fault tolerance for a service has linked paths to the LUN that contains the data for the service. For example, if you are running a two-node Exchange Mailbox server cluster, each node will have a linked path to the LUN containing the mailboxes, but only one of the nodes will have an active connection to the LUN at one time. If a failure occurs on this node, the service is automatically failed over to the second node. At that time, the second node's link to the LUN is activated as it takes over the service. This is the *shared-nothing* clustering model—only one node can modify data in the data store of a given service at one time.

UPDATE ALERT HYPER-V SHARED-EVERYTHING CLUSTERS

Microsoft has modified the shared-nothing cluster model for Hyper-V in Windows Server 2008 R2 to change it to a shared-everything model. A new disk volume—the Cluster Shared Volume (CSV)—is available to the Failover Clustering feature in this version of Windows Server.

In addition, the Hyper-V team has developed a new virtual machine migration feature—the live migration feature—to support moving a virtual machine from one host to another with no downtime. This feature will be added to Quick Migration, which is currently available for the movement of machines between nodes of a cluster. Remember that Quick Migration must save the state of the virtual machine before moving it, resulting in some downtime, even if it may be minimal. If you already have a cluster, you only need to update each node to R2 to be able to take advantage of the live migration feature.

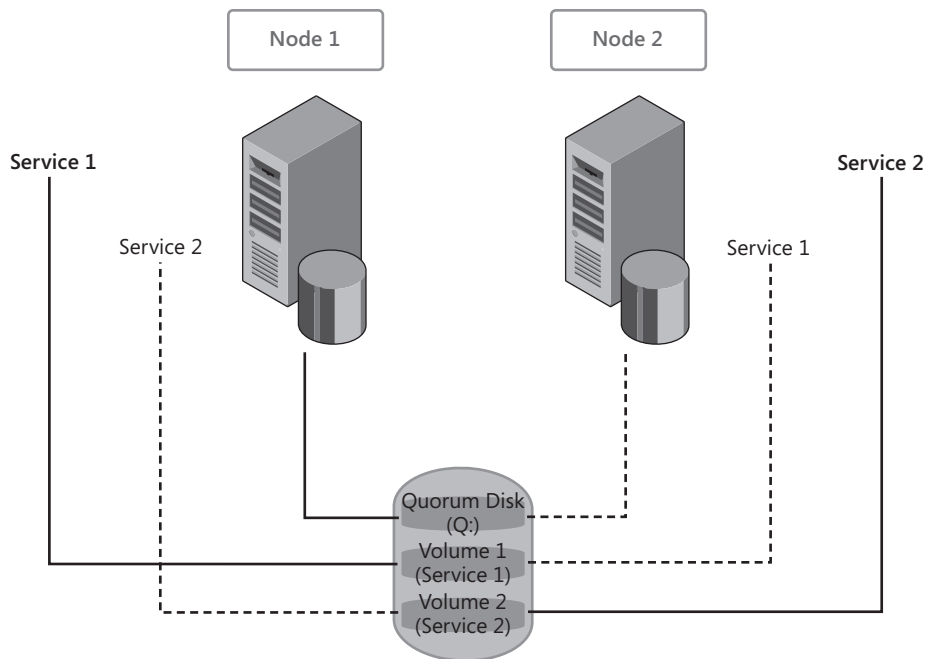


FIGURE 3-2 Single-site clusters use shared storage. Each node must have a linked path to the LUN storing the data for the service it hosts.

This cluster model is called a single-site cluster model because shared storage is local only and must therefore be located in a single site. In addition, because the nodes provide fault tolerance for the same service, they must have spare resources—resources that will be put to use if the node running the service experiences a failure. Several approaches are available for the implementation of single-site clusters:

- **Active-passive clusters** In an active-passive cluster, one node is used to run the service and the other node is used as a backup. Because the second node is a backup to the first, it does not run any services until a failover—the process of moving a service from one cluster node to another—occurs. These clusters usually contain only two nodes.
- **Active-active clusters** In an active-active cluster, each node hosts a service while providing failover services for the services actively running on the other node. In the event of a failure, the partner node in the cluster will host both its own service and the failed service. These clusters can include more than two nodes. In fact, they can include up to 16 nodes. This cluster configuration is more efficient because each node is actually running a service instead of passively waiting for a service to fail. However, it is important to note that active-active cluster nodes must be configured with spare resources. In a simple active-active configuration, a node runs its own service and includes enough spare resources to host a service from a failed node. The simplest configurations include nodes with half of the resources used for the active service and the other half available for failover.

- **Mix-and-match clusters** In a mix-and-match cluster configuration, some nodes are configured as active-active whereas others are configured as active-passive. For example, an Exchange Mailbox service could be configured on two nodes of the cluster in active-passive mode. Three other nodes could be running SQL Server with each server running its own databases, but including enough spare resources to provide failover for the others. Few organizations use this mode. Most organizations will use smaller, single-purpose, two- or three-node clusters where the cluster runs only one service such as e-mail, file sharing, or database services.

In addition to the single-site cluster, the Windows Server Failover Cluster feature can support multi-site clusters. In a multi-site cluster, each host has direct access to the data store that is linked to a protected service. However, because the hosted service is a stateful service—a service that modifies data—there must be a way to ensure that the data store in each site is identical. This is performed through some form of data replication. Each time the data is modified on the active node of the cluster, the modification is replicated to the passive node for that service. The advantage of a multi-site cluster is that the services it hosts are protected not only from equipment failures, but also from disasters affecting an entire site (see Figure 3-3).

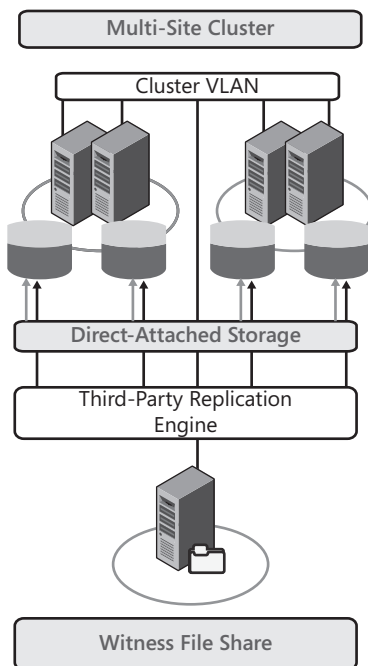


FIGURE 3-3 Multi-site clusters use replication to protect a service's data and ensure that it is identical in all data stores.

Failover Clustering for Hyper-V

When you combine Hyper-V with the Failover Clustering feature, you ensure high availability for the virtual machines you run on host servers because in the event of a hardware failure, the virtual machines will be moved to another host node. However, for this operation to occur, you must also combine the Hyper-V failover cluster with System Center Virtual Machine Manager 2008. This combination of tools supports the need to respond to planned and unplanned downtime on host servers with a minimal service interruption.

Because Hyper-V is a cluster-aware role, it is fully supported in failover clusters. When you run virtual machines in Hyper-V on a failover cluster, you will be able to fail over—move the active service from one node to another—the entire Hyper-V service or individual virtual machines. For example, if you need to update a host node in a Hyper-V cluster, you would fail over all of the virtual machines from this node to another by causing the entire service to fail over. However, if you need to move a single virtual machine from one node to another for some reason, you fail over only the VM itself.

When you prepare for planned downtime on a host node, you manually fail over the service from one node to another. In this case, virtual machine states are saved on one node and restored on the other. When the Failover Clustering service detects a potential hardware failure such as in the case of unplanned downtime, it automatically moves all of the virtual machines on the failing node to another node in the cluster. In this case, the machines actually stop on the failing node and are restarted on another node.

Depending on the cluster model you use—single-site or multi-site—you configure your Hyper-V systems to access all virtual machine files from a storage location that is either shared between the cluster nodes or from a storage location that is replicated from one cluster node to another. The key to Hyper-V failover clustering is that VM files must be in a location that is accessible to all of the nodes of the cluster.

MORE INFO VIRTUAL MACHINE FAILOVER CLUSTERS

Virtual machines running the Windows Server operating system can also run in cluster modes. In fact, both Failover Clustering and Network Load Balancing are supported in virtual machines as long as the configuration of the machines meets the requirement for each service. These machines can be set up in either mode even if the host machines are not clustered. More on this topic is covered in Chapter 10, “Configuring Virtual Machine High Availability.”

Understanding Failover Clustering Requirements

The most common cluster type is the two-node single-site cluster. This cluster requires several components to make it work. Table 3-1 outlines the requirements of this cluster configuration.

TABLE 3-1 Two-Node Cluster Requirements

REQUIREMENT	DESCRIPTION
Hardware Components	The most common cluster configuration requires certified hardware components or components that meet the “Designed for Windows Server” requirements. (See Chapter 1, Lesson 1 for more information.)
Server Hardware	The hardware used for each node in a cluster should be as similar as possible. If one node includes three network adapters, the other node should as well. If one node includes two processors, the other node should as well. When building a two-node cluster, try to purchase the two nodes at the same time.
Network Adapters	To support the cluster configuration, each node in the cluster requires a minimum of two network adapters. The first supports public network traffic—traffic similar to the traffic a non-clustered machine manages. The second supports private heartbeat data—information exchanged between cluster nodes about the health of the nodes in the cluster. This data can flow directly between the nodes of the cluster; for example, you could even use a cross-over cable to connect the private adapters in each cluster node because they only communicate with each other. A third adapter is recommended to support host server management and administration. This adapter would not run virtual machine traffic. Make sure each of the adapters is configured in the same way using identical settings for speed, duplex mode, flow control, and media type.
Network Cabling	The most important aspect of a cluster is the removal of single points of failure. This means that you should use redundant cabling and routing. If you can, use different networks for the public and the private traffic in the cluster. If you use a network-based shared storage system, such as iSCSI, try to assign another separate network for this traffic.
Direct-Attached Storage (DAS)	Many two-node clusters use DAS for the host operating system. Although you can boot Windows Server 2008 from shared storage, it is often simpler to create a mirrored redundant array of independent disks (RAID 1) configuration to store the host operating system. Using RAID 1 protects the operating system in the event of a single disk failure.

REQUIREMENT	DESCRIPTION
Shared Storage Connectivity	Windows Server 2008 supports several shared storage models. Shared storage can be accessed through Fibre Channel using Host Bus Adapters (HBAs), serial attached SCSI (SAS), or network-based SCSI (iSCSI). Whichever method and hardware is used should be identical in each node of the cluster. If you use HBAs or SAS controllers, they should be identical in each node. In addition, the firmware of each controller should be identical. If you use iSCSI, each host node should have at least one dedicated network or HBA to manage this traffic. This network cannot be used to run network communications. Network adapters for iSCSI should support Gigabit Ethernet or better connections. In addition, you cannot use teamed network adapters—two adapters that are teamed as one in a redundant configuration—because they are not supported for iSCSI traffic.
Shared Storage Containers	The shared storage container must be compatible with Windows Server 2008. It should contain at least two separate volumes (LUNs) and both LUNs should be configured at the hardware level. The volumes you create for a cluster should never be exposed to non-clustered servers. The first volume acts as the witness disk, sharing cluster configuration information between the nodes. The second volume acts as the service volume, sharing service data such as virtual machine files between the two cluster nodes. All disks must be formatted as NTFS. Disks should be basic disks, not dynamic volumes. Clustered volumes can use either the master boot record (MBR) or the GUID partition table (GPT) for the partition style of the disk.

NOTE MORE THAN ONE VM ON A CLUSTER

Because you will be running more than one virtual machine in the shared storage container, consider creating a separate volume for each virtual machine's files. This will simplify VM file management and improve overall performance.

NOTE STORAGE DEVICE COMPATIBILITY

Microsoft has modified the cluster service in Windows Server 2008 to improve performance. Because of this, storage containers used with the clustering service must support the standard called SCSI Primary Commands-3 (SPC-3); failover clustering relies on Persistent Reservations as defined by this standard. In addition, the miniport driver used to connect to the storage hardware must work with the Microsoft StorPort storage driver.

As outlined in Table 3-1, you can use several different configurations to run the single-site two-node cluster. Table 3-2 outlines the required components based on the type of storage connectivity you will use.

TABLE 3-2 Network and Storage Component Requirements

COMPONENT	SAS	ISCSI	FIBRE CHANNEL	COMMENTS
Network adapter for network traffic	3	3	3	You should aim to include three network adapters in each host server for network traffic. See Table 3-1 for more information.
Network adapter for storage traffic		2		Use at least two network adapters if the iSCSI connectivity is run through the network. This provides storage path redundancies. Dedicate these adapters to the iSCSI traffic.
Host Bus Adapters for storage traffic	2	2	2	Use at least two HBAs in each host to provide redundant paths to data.

As you can see in Table 3-2, you should make your host computer nodes as redundant as possible both at the component level and at the cluster level. In fact, you should also use multipath Input and Output (I/O) software to create multiple paths to storage through the redundant adapters you include in your host servers. Verify with the storage hardware vendor to obtain the latest multipath I/O device specific module for the device as well as specific advice regarding firmware versions, adapter types, and other required software to make the vendor's solution work with Windows Server 2008.

NOTE WINDOWS SERVER 2008 STORAGE SYSTEMS

You can no longer use parallel SCSI in Windows Server 2008 to provide shared storage connectivity in support of cluster configurations. Parallel SCSI is still supported in Windows Server 2003 clusters, however.

Also make sure your host servers are running the Enterprise or Datacenter editions of Windows Server 2008. Other editions do not include the WSFC feature. Note that Hyper-V

Server 2008 cannot run the Failover Clustering service either because it is based on the Standard edition of Windows Server 2008.

Finally, your configuration must also meet additional requirements:

- The nodes in the cluster must both be part of the same Active Directory Domain Services (AD DS) domain.
- The servers must be using the Domain Name System for name resolution.
- Cluster nodes should not run the domain controller role and should be member servers. The domain controller role is not cluster-aware and cannot take advantage of the clustering feature.
- The account you use to create the cluster must have local administration rights on each node of the cluster. This account should not be a domain administrator, but it must have the Create Computer Objects permission in the domain.
- A unique cluster name—unique both as a DNS name and a NetBIOS name—is required.
- A unique cluster IP address for each public network with which the cluster will interact is required.

Keep these additional requirements in mind when preparing to create the cluster.



EXAM TIP HYPER-V TWO-NODE CLUSTERS

Pay close attention to the requirements and considerations for Hyper-V single-site clusters. They are a definite part of the exam.

Multi-Site Clustering Requirements

Although you can create single-site Hyper-V clusters and you must use shared storage to do so, you'll find that the system requirements are considerably different in a Windows Server 2008 multi-site cluster. In this case, the Hyper-V hosts do not need to rely on shared storage and can actually run virtual machine content directly from Direct-Attached Storage. This provides considerable performance improvement and makes the cluster implementation much simpler.

However, unlike Exchange Server 2007, Hyper-V does not include its own replication engine to ensure that each DAS container includes identical content. Because of this, you must rely on a third-party replication engine. Several such engines are available on the market. FalconStor (<http://www.FalconStor.com>) provides the Network Storage System. SteelEye (<http://www.SteelEye.com>) also provides a software product that supports Hyper-V replication: DataKeeper. DoubleTake Software (<http://www.DoubleTake.com>) also provides a Hyper-V replicator. More are being made available on an ongoing basis.

The major advantage of the multi-site cluster is that it provides a very simple configuration. Another advantage is that it does not need to be deployed in multiple sites. If you want to create a simple Hyper-V failover cluster relying on DAS instead of shared

storage, you can create a multi-site cluster configuration within a single site. You still require the replication engine to ensure that all your host server data stores are identical, but the overall configuration of the host servers and the implementation of the cluster will be simpler and can even be less expensive than a traditional single-site cluster, depending on the configuration you use.

MORE INFO WINDOWS SERVER 2008 MULTI-SITE CLUSTERS

For more information on Windows Server 2008 multi-site clusters, go to <http://www.microsoft.com/windowsserver2008/en/us/clustering-multisite.aspx>. For a full list of partners for Windows Server 2008 clusters, go to <http://www.microsoft.com/windowsserver2008/en/us/clustering-partners.aspx>. For information on what to consider when deploying a multi-site cluster, look up Knowledge Base article number 947048 at <http://support.microsoft.com/default.aspx/kb/947048/en-us>.

Creating a Hyper-V Two-Node Cluster

As you have seen so far, you need specialized hardware to create a two-node cluster. This hardware is not necessarily available to organizations of any size. Small and medium-sized organizations with few virtual machines most likely cannot afford the specialized shared storage that is required for this cluster setup. Storage prices are dropping and may well make this type of configuration available to everyone eventually, but for now, smaller organizations will have to look to other methods such as backup and recovery solutions to ensure that their virtual machines are protected at all times.

However, if your organization believes that high availability is a must for host servers—as they should—it will make sure you have the appropriate budget to acquire and prepare the hardware required for a Hyper-V cluster. When you do obtain this hardware, proceed as follows to create the cluster.

The cluster installation process includes several steps, each of which must be performed in order to create a working cluster. These steps differ slightly on the full installation and the Server Core installation, but generally they proceed similarly. The major difference is that the Server Core cluster must be created remotely. The main steps include:

1. Prepare the physical server nodes.
2. Install the operating system.
3. Install the Hyper-V role.
4. Install the Failover Clustering feature on both nodes.
5. Create a virtual network.
6. Validate the cluster configuration and create the cluster.
7. Create a VM and make it highly available.

Prepare Physical Server Nodes

Integrate all of the required components into each physical server. When the components are all installed, proceed as follows:

1. Connect each device to the networks it requires. Begin by connecting an adapter from each node to the private network the cluster will use for the heartbeat. Connect the second adapter (two adapters are the utmost minimum requirement) to the public network. This network must support communications between the nodes, between the nodes and the domain controllers in your network, and between the nodes and end users.
2. Connect your servers to the shared storage container. You will most likely need to rely on your hardware manufacturer's instructions for this operation because the steps to follow vary based on manufacturer, connection type, and storage type.
3. Prepare and expose the LUNs for the cluster. One LUN is required for cluster information and at least one LUN is required for virtual machine storage. The cluster information LUN can be relatively small but should be a minimum of 10 GB. The LUN you prepare for virtual machine storage should be considerably bigger and should include enough space for all of the disks you will assign to the VM. Expose the LUNs to the server nodes. Use either the manufacturer's storage management application, an iSCSI engine, or Microsoft Storage Manager for SANs (another feature of Windows Server 2008) to expose these LUNs.
4. Install the Windows Server 2008 Enterprise or Datacenter operating system on the nodes in the cluster. Perform the installation as per the instructions in Chapter 2.
5. Make sure the LUNs are formatted with the NTFS format. This file format provides the best cluster performance and is an absolute requirement for the cluster witness disk or the disk containing cluster configuration information. If the disk will be larger than 2 terabytes, you must use the GUID partition table (GPT), not the master boot record (MBR). You can modify this setting in the Disk Management section of Server Manager on one of the cluster nodes. Use the Convert To GPT command, which is available when you select the disk itself. Make sure that all partitions are cleared from the disk before you perform this conversion. Also, make sure your disks are basic disks and not dynamic disks. Dynamic disks do not work with the cluster service.

Your systems are ready for the next step.

Install the Required Role and Feature

If the computers do not already include the appropriate features and the Hyper-V role, you must add them at this time. Begin with the Hyper-V role. Review the instructions in Chapter 2 for the required procedure, depending on which installation mode you selected. Ideally, you will be running the Server Core installation.

NOTE INSTALLING THE HYPER-V ROLE ON THE FULL INSTALLATION

If you are running servers with the full installation, you will be prompted to create a virtual network during the installation of the Hyper-V role. Perform this action only if the two servers include identical network interface cards. If not, skip the virtual network creation and create it in the next step of the process. The virtual network name needs to be identical between the two host servers. If you use the same network card, the name will be identical; if not, they will be different because Hyper-V automatically names the network based on the adapter name when the virtual network is installed during the role installation.

When the Hyper-V role is installed, proceed with the installation of the Failover Clustering feature. On a full installation, use Server Manager to add the feature. Right-click Features in the Tree pane and choose Add Features. Select the Failover Clustering feature and click Next (see Figure 3-4). Click Install to perform the installation of the feature. Click Close when the feature is installed.

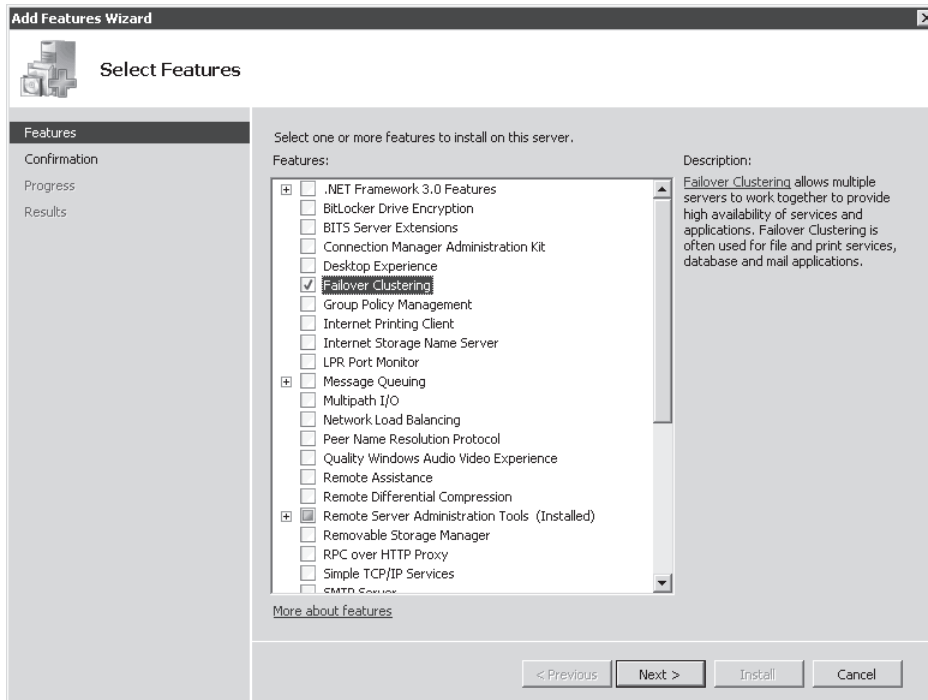


FIGURE 3-4 Adding the Failover Clustering feature

On Server Core, you must use the OCSETUP.exe command to perform this installation. Feature and role names are case-sensitive with this command. Begin with the OCLIST.exe command to view the name of the feature then use the OCSETUP.exe command to install it.

You need to scroll to the top of the list to see the Failover Cluster feature name. Use the following commands:

```
oclist
start /w ocsetup FailoverCluster-Core
```

The last command will wait until the feature has been completely installed to complete.

Microsoft has updated the Failover Clustering service to work with Hyper-V and expose several new features when working with virtual machines on failover clusters (see Figure 3-5).

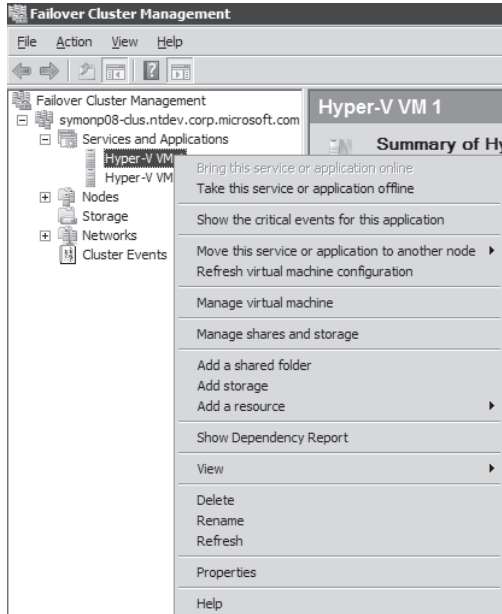


FIGURE 3-5 Managing VMs in Failover Cluster Manager prior to the installation of update 951308

This update is number 951308 and can be found at <http://support.microsoft.com/kb/951308>. The following changes are included in this update (see Figure 3-6):

- Changes to the context-sensitive commands provided when you right-click on a virtual machine
- Improvements to the Quick Migration feature
- Support of more than one VM in a cluster group
- Support of the use of mount points and volumes without using drive letters
- Changes to the refresh behavior in the Cluster user interface (UI)
- Corrections to the clustering service when virtual machines are in a disconnected state
- Corrections in the addition of pass-through disks to VMs
- Corrections in the use of virtual machines including differencing disks
- Corrections to support extensive drive paths, especially with GPT disks

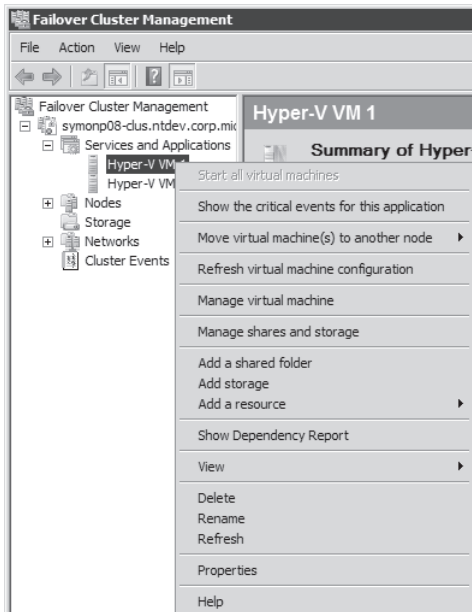


FIGURE 3-6 Managing VMs in Failover Cluster Manager after the installation of update 951308

This update is applicable to any full installation of Windows Server 2008, both x86 and x64, where the Failover Clustering feature is installed or where the Failover Clustering tools have been installed. It is also applicable to Windows Vista with SP1 x86 or x64 systems that include the RSAT or at least the Failover Clustering tools from RSAT. This update is not applicable to Server Core installations because it applies to the graphical UI (GUI) and there is no GUI in Server Core.

Download the update to a location that is accessible to the computer you need to install it on and double-click to install. Click OK to accept the installation (see Figure 3-7) and click Close when the installation is complete.

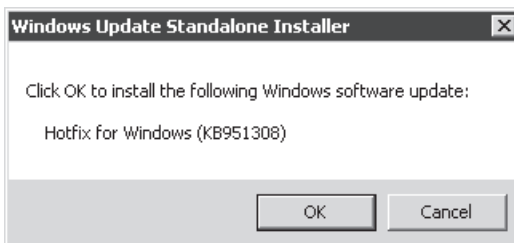


FIGURE 3-7 Adding the Failover Clustering Update for Hyper-V

UPDATE ALERT THE MICROSOFT CLUSTER UPDATE FOR HYPER-V

Note that the UI behavior changes brought about by update number 951308 are not part of the exam. Be sure to read the article at <http://support.microsoft.com/kb/951308> and note the previous behavior to prepare for the exam. Alternatively, you could omit the update on your servers while you prepare for the exam and apply it after you pass the exam.

Perform all operations on each node of the cluster if the installations are full installations. If they are Server Core, perform the role and feature installations but not the update installation. Install the Failover Clustering and Hyper-V management tools and apply the update to the GUI systems you use to manage Hyper-V.

Create a Virtual Network

Now you need to create a virtual network to support virtual machine traffic. You need to perform this action if your servers run the full installation and use different network cards or if your servers run the Server Core installation.

Basically, you need to use the procedures outlined in Chapter 2, Lesson 3 to add a new external virtual network and assign it to a physical network adapter. The key to this operation is that the name of the virtual network you create is identical on both nodes of the cluster. Otherwise, failover will not work because Hyper-V will not be able to bind failed-over VMs to the same network when moving machines from one node to another.

If you create more than one virtual network for the VMs you will host on the cluster, make sure each network has the same name.

Validate and Create the Cluster

The first step you should perform when creating a cluster is to run the Failover Cluster Validation tool. This tool validates all parts of your cluster configuration and points out any potential issues. When all portions of the cluster are validated, you can proceed to the cluster creation.

Perform this operation directly on one of the host servers if you are using a full installation. Perform this operation on a separate system if you are using Server Core installations. Remember to use an account that is Local Administrator on both nodes. Accept all User Account Control (UAC) prompts during this operation if they appear.

1. Begin by launching the Failover Cluster Management console (see Figure 3-8). Click Start, point to Administrative Tools, and click Failover Cluster Management. Take the time to review the information on the start page of the console.
2. Click Validate A Configuration in the Actions pane. The Validation A Configuration Wizard begins. Review the information on the Before You Begin page and click Next.
3. On the Select Servers Or A Cluster page, click Browse, type the name of the two servers separated with a semi-colon, click Check Names, and then click OK. Click Next.

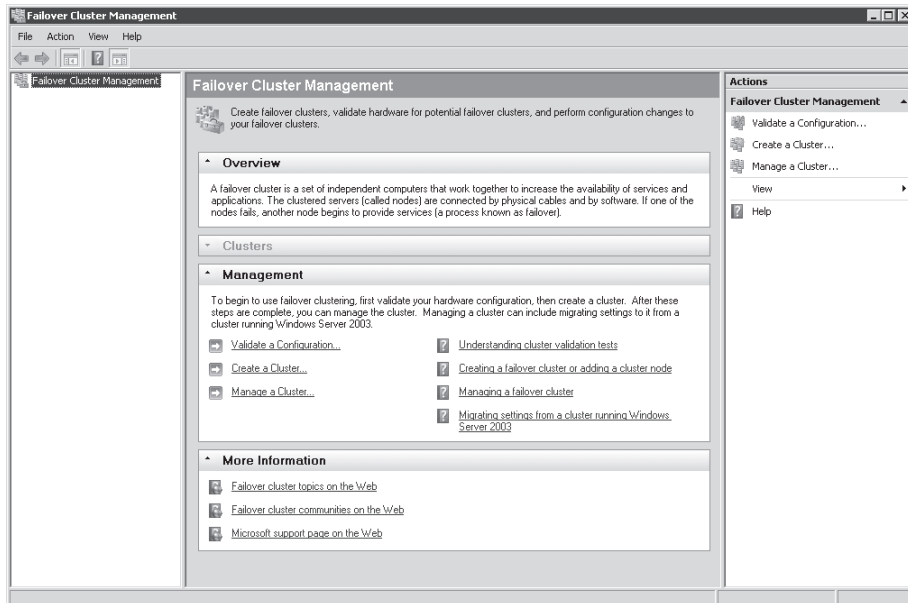


FIGURE 3-8 The Failover Cluster Management console

4. Normally, you should run all tests on the cluster nodes, but because this is the first time you are running this wizard, it is a good idea to select Run Only Tests I Select to view the available tests. Click Next.
5. Take the time to review the available tests and the types of tests the wizard can run (see Figure 3-9). Click Next when ready.

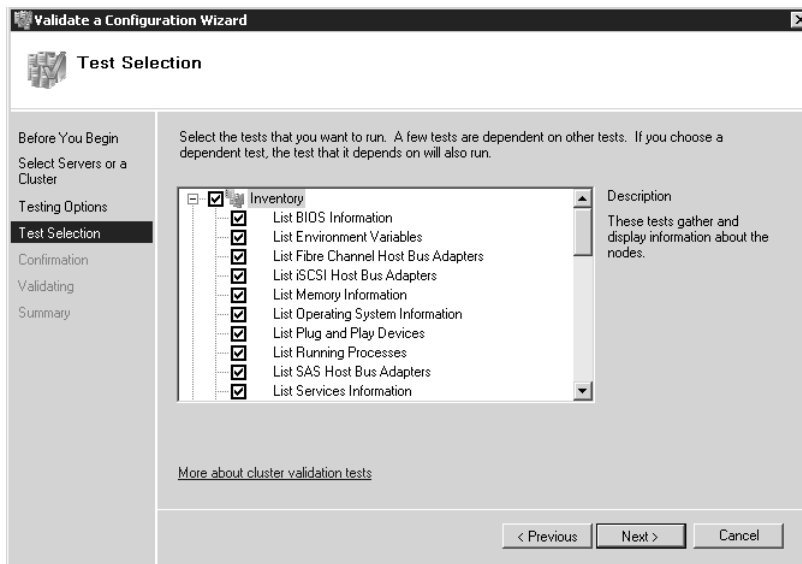


FIGURE 3-9 The list of tests available in the Validation Wizard

6. Confirm the settings and click Next. The tests will begin to run (see Figure 3-10).
7. Review the Report on the final page of the wizard. If you want a copy of the report, click View Report. Reports are saved in your profile under AppData\Local\Temp and are in .mht format. They are visible in Internet Explorer. Click Finish on the last page of the wizard when done.

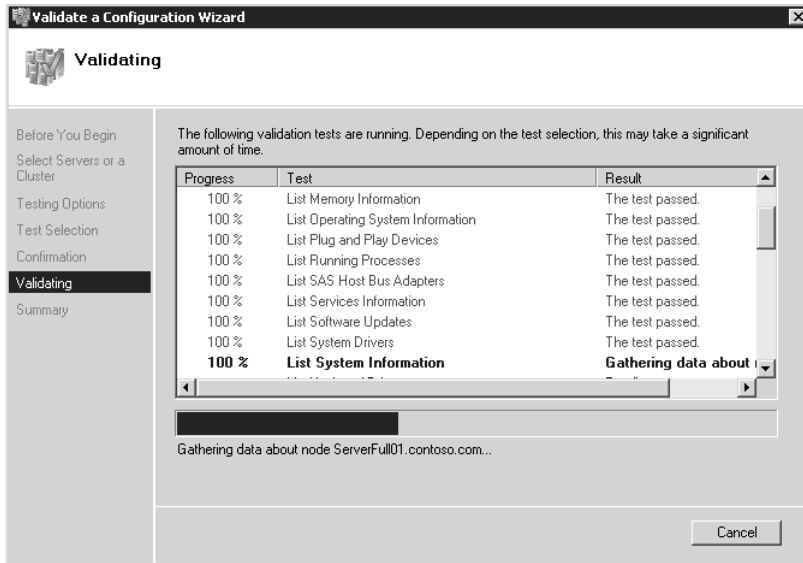


FIGURE 3-10 Running a cluster validation

Note any discrepancies in the report and repair any issues. Items that pass the report appear in green, items that cause warnings appear in yellow, and items that fail appear in red. Repair all failed items and review any warnings to ensure that your systems are ready to support clustering. When all issues are repaired, you are ready to create the cluster.

1. Click Create A Cluster in the Actions pane. Review the information on the Before You Begin page and click Next.
2. On the Select Servers Or A Cluster page, click Browse, type the name of the two servers separated with a semi-colon, and click Check Names. Click OK and then click Next.
3. Because you already ran the validation, choose not to run the Validation Report again and click Next.
4. Name your cluster (for example, **Hyper-V Cluster**), type in an IP address for the cluster for each public network it will access, and click Next.
5. Confirm your settings and click Next. The wizard will proceed with the cluster creation. When the process is complete, you can again view the report and click Finish when done.

During the cluster configuration, the configuration process will create a quorum disk. The quorum disk is the shared storage container that contains the cluster configuration settings for both nodes. In Windows Server 2003, the quorum consisted of only one disk, and because

the quorum model only included a single location for the cluster configuration settings, it could be a single point of failure in the cluster.

Windows Server 2008 includes a new two-node cluster mode called Node and Disk Majority Quorum configuration. In this case, the cluster data is stored on each node as well as on the quorum disk. The cluster continues to work as long as it has quorum or at least two of the three sources for the cluster configuration data are available. You can change quorum disk configurations at any time by selecting the cluster name, clicking More Actions in the Actions pane, and then selecting Configure Cluster Quorum Settings. Windows Server 2008 supports four different quorum modes (see Figure 3-11).

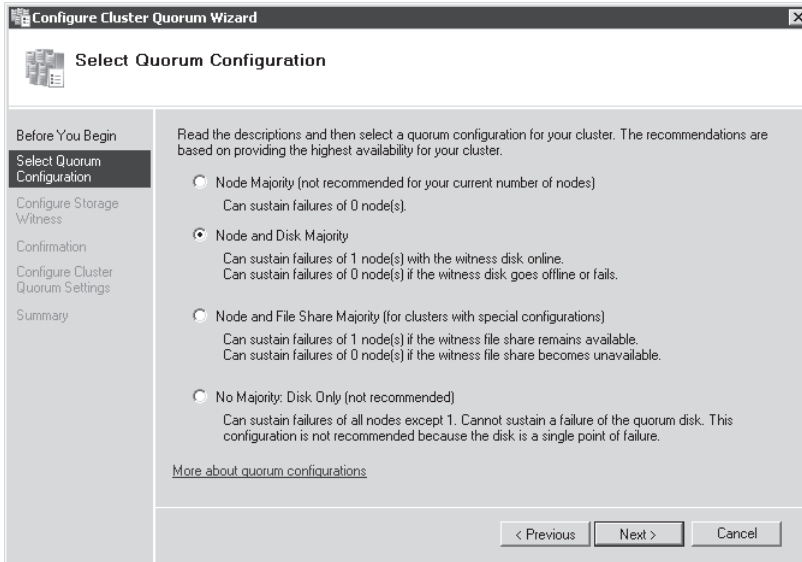


FIGURE 3-11 Supported cluster quorum modes

Your cluster has been created. The Failover Cluster Manager should now include the cluster in the Tree pane. Note that this pane now includes five headings under the cluster name:

- **Services and Applications** This section lists the fault-tolerant applications that have been added to the cluster.
- **Nodes** This section gives you access to the configuration and operation of each node in the cluster.
- **Storage** This section controls shared storage containers. It should list the minimum two LUNs you created and added to the cluster.
- **Networks** This section lists both the private and public networks your cluster nodes have access to.
- **Cluster Events** This section gives you access to all cluster events.

Take the time to explore each section of this console before moving on.

Create a Highly Available VM

Now that your cluster has been prepared, you can move on to create a highly available VM.

1. Open the Hyper-V Manager console. Make sure the Hyper-V Manager console is connected to one of the cluster nodes.
2. Click New and then click Virtual Machine on the Actions pane. Click Next.
3. Name the virtual machine and click Store The Virtual Machine In A Different Location. Use the Browse button to locate the shared storage LUN you created to host virtual machines. Click Next.
4. On the Assign Memory page, assign an appropriate amount of memory for this VM and click Next.
5. On the Configure Networking page, choose an external network connection and click Next.
6. On the Connect Virtual Hard Disk page, make sure Create A New Hard Disk is selected and modify the size of the virtual hard disk. Change it to **40** GB because it will be the system disk. Click Next.



EXAM TIP MAKING AN EXISTING VM HIGHLY AVAILABLE

If you already have a virtual machine and you intend to make it highly available, move the VM's hard disk file(s) to the shared LUN using Windows Explorer, place it in a folder with the machine's name and, when you get to step 3, locate the VM's configuration file in this folder. When you get to step 6, select Use An Existing Virtual Hard Disk, browse to select the disk you moved, and assign it to this VM.

7. On the Installation Options page, make sure that Install An Operating System Later is selected and click Next. Review your settings and click Finish. Do not start this VM once it is created because it must be shut down to make it highly available.
8. Now reset the automatic start action for this VM. By default, Hyper-V sets this action to Automatically Start If It Was Running When The Service Stopped. However, when machines use this setting, they are not managed by the Failover Cluster service. Change the setting by right-clicking the new machine in the Details pane and choosing Settings. Move to the Automatic Start Action in the left pane of the dialog box and change the setting to Nothing (see Figure 3-12). Click OK to apply the change.
9. Configure the VM as highly available. Return to the Failover Cluster Management console and make sure the Hyper-V Cluster is selected. Move to the Services And Applications section of the Tree pane and right-click to select Configure A Service Or Application. Click Next.
10. Choose Virtual Machine (toward the bottom of the list), wait for the cluster to verify whether it can support this application, and click Next.

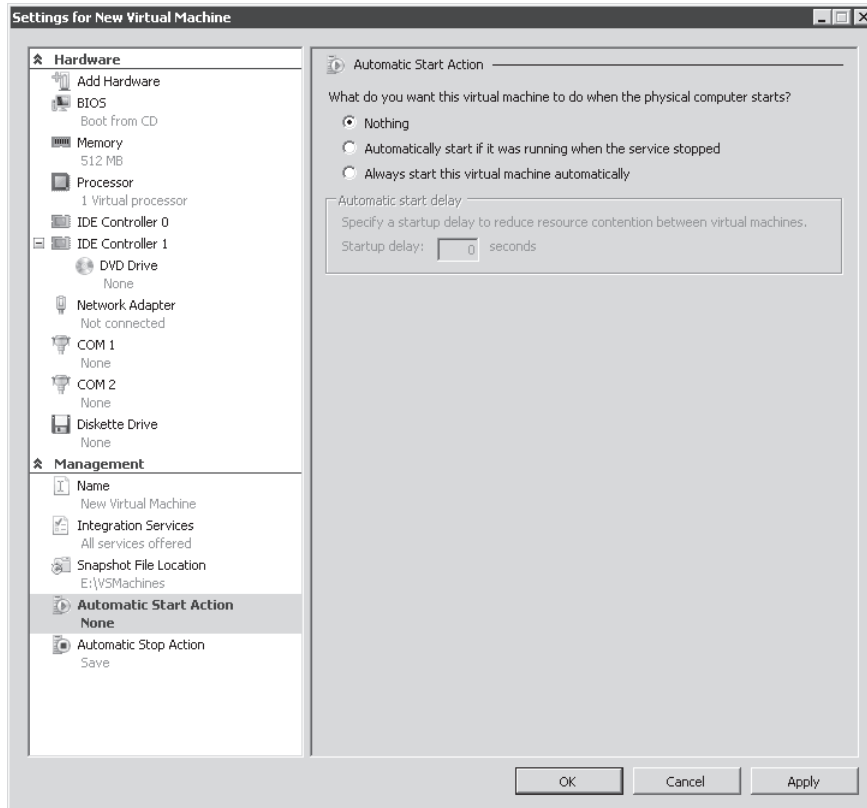


FIGURE 3-12 Setting automatic start actions

- 11.** On the Select Virtual Machine page, select the new virtual machine you just created and click Next.
- 12.** Confirm your settings and click Next. The VM will be configured for high availability and provide a summary report of the operations it completed. Click Finish.

The VM will now appear under the Services And Applications node of the Hyper-V Cluster. You can right-click this VM and tell the Failover Cluster service to bring it online if you are ready to install an operating system in this machine. If you used an existing machine, simply bring it online.

Managing Hyper-V Host Failovers

Failovers are designed to support both planned and unplanned downtime. In the case of Hyper-V, virtual machines are saved on one node and then restarted on another node when you plan the downtime. This works because the machine's saved state is on the shared disk and is therefore available to both cluster nodes.

When an actual failure occurs, the machine is automatically stopped on the failed node and then restarted on the running node. This causes an interruption of service that can vary

in duration. The duration of the service interruption depends greatly on the speed of the spindles in your shared storage container. The speed of the disks determines how fast the VM will restart and be available to service users.

All failover actions are performed from the Failover Cluster Management console. Once again, you rely on the Services And Applications node to manage virtual machine Quick Migrations. To perform a planned failover, you right-click a VM and select Move This Service Or Application To Another Node. To perform an unplanned failover, you simply stop the cluster service on the node hosting the running VM or shut down that host. To stop the service, right-click the name of the node running the VM, select More Actions, and then select Stop Cluster Service. This will cause a cluster failure and automatically move the VM to the other node in your cluster. Alternatively, you can use the Quick Migrate Virtual Machines command, which is available when you right-click a VM in the Services And Applications node. This command shuts down the VM and then restarts it on another node.

Your failover cluster is ready. It is imperative that you manage virtual machine operations through the Failover Cluster Management console from this point on because it gives you control of all fault-tolerant virtual machines. Running VMs in a cluster abstracts VM operation from the actual hosts they run on and lets you manage the host servers as a single resource pool unit.



EXAM TIP UPDATE 951308

Remember that if you installed update 951308, the commands in the cluster UI will be different than the ones listed here. Notably, the Move This Service Or Application command will be renamed Move Virtual Machines and the Quick Migrate Virtual Machines action will no longer be available. The Move Virtual Machines command automatically saves the state of the VM and then moves it to the other node.

MORE INFO QUICK MIGRATION WITH HYPER-V

Microsoft has released a white paper on how to use Quick Migration with Hyper-V. Download it from <http://www.microsoft.com/downloads/details.aspx?FamilyID=fdd083c6-3fc7-470b-8569-7e6a19fb0fdf&DisplayLang=en>.

MORE INFO WORKING WITH FAILOVER CLUSTERING

Microsoft has released an online virtual lab for Windows Server 2008 Enterprise Failover Clustering. If you do not have access to the proper hardware to create a cluster, you can still practice working with a cluster at <http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?EventID=1032345932&EventCategory=3&culture=en-US&CountryCode=US>.

As mentioned in the Introduction, it is difficult for readers preparing for the exam to have full access to the technologies required to create failover clusters because of the prohibitive cost of shared storage or replication engines. However, even if you do not have access to shared storage, it is still possible to create a non-working failover cluster to view the Failover Cluster Management console UI and try out the various operations it supports for Hyper-V. This is the focus of this practice. Note that if you do have access to a full cluster configuration, you should run through the instructions listed in this lesson to review actual cluster operations.

MORE INFO EVALUATION CLUSTER

Although the practice focuses on a non-working cluster, you can create a working cluster using iSCSI target software. You can obtain an evaluation version of StarWind Server from Rocket Division Software to create iSCSI targets for testing failover clustering. Obtain the free version from http://rocketdivision.com/download_starwind.html. This free version will let you create two drives to host clustering; however, note that the evaluation is limited to 2 GB of disk space. As such it is only valid for testing purposes.

This practice consists of three exercises. In the first, you install the failover cluster role and perform a cluster validation. In the second, you install a non-working failover cluster and explore cluster operation. In the third, you break the cluster in order to prepare for future exercises.

EXERCISE 1 Install the Failover Clustering Feature

In this exercise you will install the failover cluster feature on each of your servers and validate the cluster. Perform this exercise with domain administrator credentials.

1. Log on to ServerFull01 and launch Server Manager if it isn't already started. Click Start, point to Administrative Tools, and then click Server Manager.
2. Right-click Features in the Tree pane and choose Add Features.
3. Select the Failover Clustering feature and click Next.
4. Click Install to perform the installation of the feature. Click Close when the feature is installed.
5. Log on to ServerCore01. Type in the following command:

```
start /w ocsetup FailoverCluster-Core
```
6. Wait until the feature has been completely installed. The installation is complete when the prompt returns in the Command window.
7. Return to ServerFull01. Launch Internet Explorer (click Start, point to All Programs, and then click Internet Explorer). Type **KB951308** in the Search bar and press Enter. Download the x64 version of the update for Windows Server 2008 and save it in your Documents folder. Close Internet Explorer.

8. Use the Windows Explorer (click Start, point to All Programs, and then click Windows Explorer) to go to your Documents folder. Double-click the update named Windows6.0-KB951308-v2-x64.msu. Click OK to install the update and click Close when done. This will update the Failover Cluster UI for Hyper-V.



EXAM TIP UPDATE 951308

You can skip step 8 if you want to maintain the Failover Cluster UI in the form that is on the exam.

9. Launch the Failover Cluster Management console. Click Start, point to Administrative Tools, and click Failover Cluster Management. Take the time to review the information on the startup page of the console.
10. Click Validate A Configuration in the Actions pane. The validation wizard begins. Review the information on the Before You Begin page and click Next.
11. On the Select Servers Or A Cluster page, click Browse, type the name of the two servers separated with a semi-colon, click Check Names, and then click OK. Click Next.
12. Because this is the first time you are running this wizard, select Run Only Tests I Select to view the available tests. Click Next.
13. Take the time to review the available tests and the types of tests the wizard can run. Click Next when ready.
14. Confirm the settings and click Next. The tests will begin to run.
15. Review the report on the final page of the wizard. If you want a copy of the report, click View Report. Reports are saved in your profile under AppData\Local\Temp and are in .mht format. They are visible in Internet Explorer. Click Finish on the last page of the wizard when done.

The report will include several errors if your servers do not include shared storage.

EXERCISE 2 Create a Non-working Hyper-V Cluster

In this exercise you will install the cluster service on both nodes even if you do not have access to shared storage. This will let you become familiar with the process and with the Failover Cluster Management console and help you pass this section of the exam. Perform this operation from ServerFull01. Log on with domain administrator credentials.

1. Log on to ServerFull01. Launch the Failover Cluster Management console if it isn't already open. Click Start, point to Administrative Tools, and click Failover Cluster Management. Click Create A cluster in the Actions pane. Review the information on the Before You Begin page and click Next.
2. On the Select Servers Or A Cluster page, click Browse, type the name of the two servers separated with a semi-colon, click Check Names, and then click OK. Click Next.
3. Because you already ran the validation, choose not to run the Validation Report again and click Next.

4. Name your cluster **Hyper-V-Cluster** and type in **192.168.0.10** as the IP address for the cluster for the public network it will access. Click Next.
5. Confirm your settings and click Next. The wizard will proceed with the cluster creation. When the process is complete, you can view the report and click Finish when done.

The cluster will be created even though no storage is available. Now take the time to proceed through the cluster interface and examine the commands and settings you can modify in this tool.

EXERCISE 3 Break the Hyper-V Cluster

In this exercise you will break the cluster and return the host servers to standalone machines in order to prepare for future exercises. Perform this operation from ServerFull01. Log on with domain administrator credentials.

NOTE WORKING CLUSTER

If you have access to the hardware or software required to create a working cluster, you should maintain the cluster as is. It will support all of the remaining exercises in this guide.

1. Log on to ServerFull01. Launch the Failover Cluster Management console if it isn't already open. Click Start, point to Administrative Tools, and click Failover Cluster Management.
2. Make sure the Hyper-V Cluster is selected in the Tree pane.
3. Move to the Actions pane and click on More Actions. Choose Destroy a cluster. A warning dialog box will appear. Click Destroy a cluster.

The cluster will be broken. It is important to break the cluster at this point since it is a non-working cluster. Keeping it as such would cause issues in future exercises. You will proceed through all other exercises with the host servers running as standalone hosts from now on.



Quick Check

1. What are the two types of configurations that are supported in Failover Clusters?
2. Name two different approaches available for the implementation of single-site clusters.
3. Can Hyper Server 2008 run the Failover Clustering service? If no, why not?
4. Which commands do you use in Server Core to view the name of a feature and to install this feature?

Quick Check Answers

1. The two types of configurations supported in Failover Clusters are a single-site cluster or a multi-site cluster.

2. There are several approaches to implementing a single-site cluster:
 - Active-passive clusters
 - Active-active clusters
 - Mix-and-match clusters
3. Hyper-V Server 2008 cannot run the Failover Clustering service because it is based on Windows Server 2008 Standard edition.
4. To view the name of a feature, use the OCLIST.exe command. To install it, use the OCSETUP.exe command with the feature name. It is also a good idea to use `START /w` with the OCSETUP.exe command to force the system to wait until the command is complete before returning the command prompt.

Lesson 2: Working with Hyper-V Host Remote Administration

Your Hyper-V infrastructure is just about complete. Your host servers are all prepared, critical virtual machines will be protected through failover clustering, and you're just about ready to begin the deployment of virtual machines. Only a couple of elements of the Hyper-V infrastructure remain to be prepared. The first is the management infrastructure for both hosts and virtual machines. Whether your organization is small or large, you'll need some form of remote administration tools for your Hyper-V servers, especially if you run the Server Core installation on them. Medium to large organizations will also want to look to System Center Virtual Machine Manager 2008 to create a more comprehensive host and virtual machine management environment.

The second remaining element is the optimization of your servers. This is covered in Lesson 3 of this chapter. This lesson looks at both remote administration and the implementation of a tool such as SCVMM for host and VM administration.

After this lesson, you will understand:

- The installation of the Hyper-V Manager on various platforms.
- The installation of the Failover Cluster Management console on the same platforms.
- The installation of System Center Virtual Machine Manager.
- The upgrade of an existing SCVMM installation to SCVMM.

Estimated lesson time: 60 minutes

Lessons in upcoming chapters will rely on these installations to manage both host servers and the virtual machines they run.

NOTE SYSTEM CENTER VIRTUAL MACHINE MANAGER

Microsoft released the first version of SCVMM as version 2007. Version 2007 only supported the management of host servers running Microsoft Virtual Server. In version 2008, Microsoft added support for the management of Hyper-V and VMware ESX Server hosts. For this reason, this guide only discusses the features of SCVMM 2008 and does not include any information about version 2007. In fact, the 70-652 exam only covers topics related to SCVMM 2008 and not 2007.

Deploying Hyper-V Manager

Hyper-V Manager is available in three locations:

- With the release to manufacturing Hyper-V update, update number 950050. This update comes in both x86 and x64 format.

- With the Remote Server Administration Tools included as a feature within the Windows Server 2008 full installation.
- With the downloadable update available for Windows Vista with Service Pack 1.

So far, you've worked with the Hyper-V update, but you haven't really worked with any of the RSAT versions. However, you have installed the Failover Clustering feature so you are familiar with the feature installation process. Installing the RSAT on a full installation of Windows Server 2008 uses the same process. In Server Manager, right-click Features in the Tree pane and choose Add Feature. Click Next to get to the feature list, move to the Remote Server Administration Tools section, expand the section, expand the Role Administration Tools section, and select Hyper-V Tools (see Figure 3-13). Complete the remaining steps of the wizard.

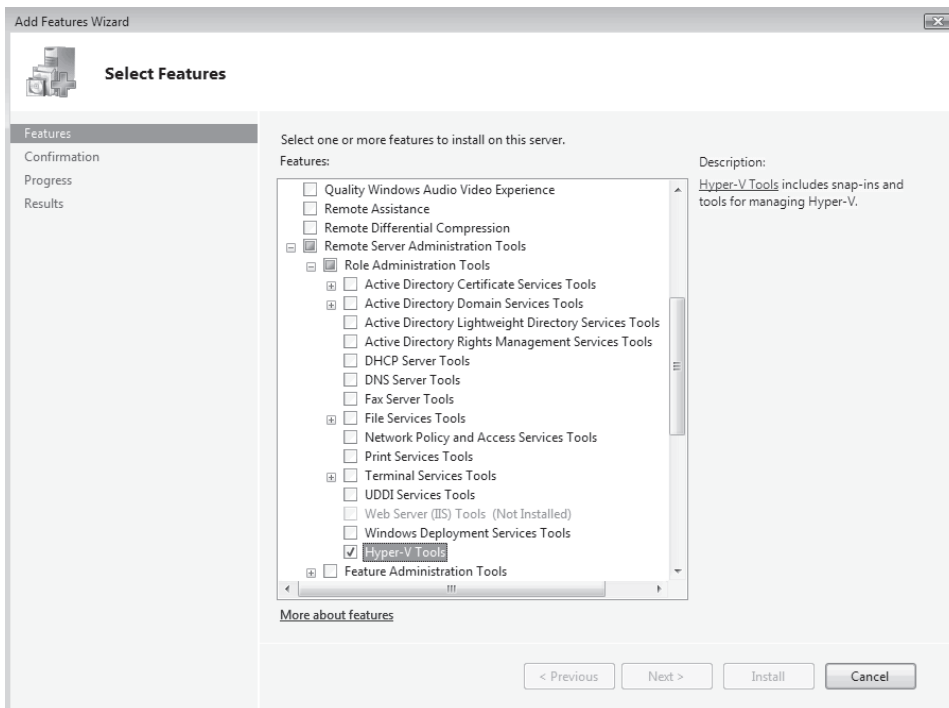


FIGURE 3-13 Installing Hyper-V tools

Remember that this step is only required when your full installation does not already include the Hyper-V role. This applies to servers running an x64 full installation but not Hyper-V, as well as x86 full installations because they do not include the capability to host virtual machines through Hyper-V. Also keep in mind that the RTM update for Hyper-V is required on these servers to have the latest version of these tools.



EXAM TIP THE RSAT FEATURE

Remember that the RSAT feature is not available on Server Core because it does not include a GUI.

In the case of Windows Vista computers, you must download and install an update to gain access to the Hyper-V Manager console. In addition, your Windows Vista computer must be running Service Pack 1; otherwise, the Hyper-V tools will not install and will not be available to you. In addition, you must be running the proper Windows Vista edition. The Hyper-V Manager console is only available for the following editions:

- Windows Vista Ultimate with SP1
- Windows Vista Enterprise with SP1
- Windows Vista Business with SP1

Hyper-V Manager is available for both the 32- and 64-bit versions of these editions of Windows Vista. Installing this console on Windows Vista is performed in two steps. First you download the update and then you install it.

1. Begin by obtaining the update. The update for Hyper-V Manager is available in Knowledge Base article number 952627 at <http://support.microsoft.com/kb/952627>. Download the appropriate update (either x86 or x64) and store it in a folder that is accessible to the workstation you want to install it on.
2. Double-click the downloaded update to launch the installation process. This process requires elevated rights and is performed through the Windows Update Standalone Installer. Click OK to begin the installation and click Close when the installation is complete. When the installation is complete, the local Administration Tools will include a link for the Hyper-V Manager.

NOTE DISPLAYING THE ADMINISTRATIVE TOOLS ON WINDOWS VISTA

The Administrative Tools are not displayed by default on Windows Vista. To display them in the Start menu, right-click Start, choose Properties, and click Customize. Move to the bottom of the list and click Display On The All Programs Menu And The Start Menu Under System Administrative Tools. Click OK twice to close the dialog boxes.

You can also use the Windows Update Standalone Installer (WUSA.exe) to install the update from a command line. You rely on WUSA to install the update using the update file itself. Using the `/quiet` switch performs the operation without user interaction. If you want to see the results, omit this switch.

```
wusa path\Windows6.0-KB952627-x86.msu /quiet
```

path is the location of the update. If you are running an x64 version of Windows Vista, you must use the x64 version of the update package.

This update will install both the Hyper-V Manager console and the Virtual Machine Connection tool or the tool you use to connect remotely to a virtual machine running on Hyper-V from a graphical installation.

NOTE MANAGING SERVER CORE FROM WINDOWS VISTA

Remember that if you intend to manage Server Core installations from Windows Vista, you need to open the Windows Vista firewall ports in the same way you opened them on the full installation of Windows Server 2008 in Chapter 2. For example, if you intend to manage the Virtual Disk Service (VDS) on Server Core from Windows Vista, you must run the following command on your Windows Vista computer from an Elevated Command Prompt:

```
netsh advfirewall firewall set rule group="Remote Volume Management" new  
enable=yes.
```

After the Hyper-V Manager is installed, you must select Hyper-V Manager in the Tree pane and then select Connect To Server in the Actions pane to locate the server you want to connect to. Perform this task to link to all of the servers you want to manage. When you close the console, it will remember the remote server connections you created and reopen with the connections in place.

However, note that Hyper-V Manager is designed to manage each Hyper-V host one at a time. Although this is adequate for small installations that include only a few host servers (see Figure 3-14), it is not adequate for an environment that includes massive numbers of host servers. For these types of environments, you will require the use of a more comprehensive management tool such as SCVMM.

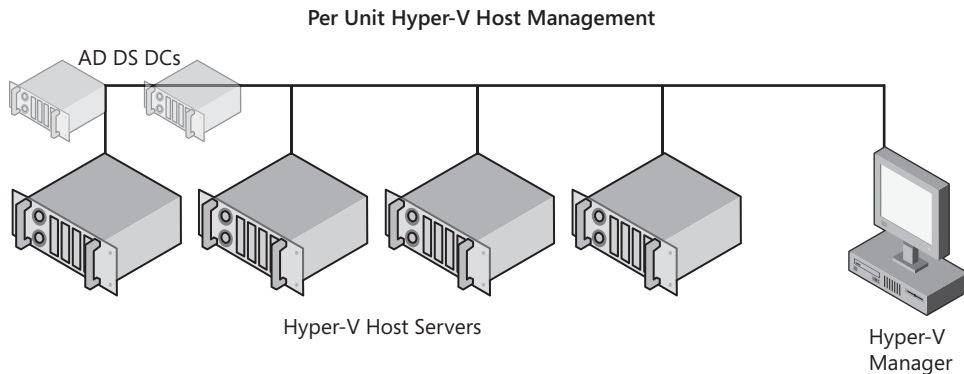


FIGURE 3-14 Managing single Hyper-V hosts may be suitable for small organizations or test environments.

UPDATE ALERT RUNNING THE HYPER-V MANAGER FROM WINDOWS 7

You can also manage Hyper-V remotely from Windows 7; however, you need a different version of the update package. Obtain it from <http://www.microsoft.com/downloads/details.aspx?FamilyID=82516c35-c7dc-4652-b2ea-2df99ea83dbb&displaylang=en>.

MORE INFO USING THE REMOTE DESKTOPS CONSOLE

You can also rely on the Remote Desktops console to manage multiple hosts. For instructions on how to build this console, look up Build The Ultimate RDC Step-by-Step at http://searchwindowsserver.techtarget.com/news/article/0,289142,sid68_gci1243095,00.html#.

Deploying the Failover Cluster Management Console

If you are running failover clusters on your host servers, you will need to install or deploy the Failover Clustering Management console in addition to the Hyper-V Manager. This console is available in two locations:

- With the Remote Server Administration Tools included as a feature within the Windows Server 2008 full installation
- With the downloadable RSAT update available for Windows Vista with Service Pack 1

Installing the Failover Clustering Management console on a full installation of Windows Server 2008 uses the same process as installing Hyper-V Manager. In Server Manager, right-click Features in the Tree pane and choose Add Feature. Click Next to get to the feature list, move to the Remote Server Administration Tools section, expand the section, expand the Feature Administration Tools section, and select Failover Clustering Management. Complete the remaining steps of the wizard.

Remember that this step is only required when your full installation does not already include the failover clustering role. Perform this operation on servers running an x86 or x64 full installation, but not failover clustering. Also keep in mind that the Failover Clustering update for Hyper-V is required on these servers to have the latest version of this console.

In the case of Windows Vista computers, you must download and install an update to gain access to the Failover Clustering Management console. Your Windows Vista computer must be running Service Pack 1 and the proper Windows Vista edition. This update is available for the same editions as for Hyper-V Manager.

The Failover Clustering Management console is available as part of the RSAT for both the 32- and 64-bit versions of these editions of Windows Vista. Installing these tools and the required console on Windows Vista is performed in three steps: download the update, install it, and activate the console.

1. Begin by obtaining the update. The update for RSAT is available in Knowledge Base article number 941314 at <http://support.microsoft.com/kb/941314>. Download the appropriate update (either x86 or x64) and store it in a folder that is accessible to the workstation you want to install it on.
2. Double-click the downloaded update to launch the installation process. This process also requires elevated rights. Click OK to begin the installation, accept the license agreement, and click Close when the installation is complete. The local Administration Tools will now include a link to the RSAT Help File.

3. When the update has been installed, you need to enable the new RSAT Windows tools you want to use. Click Start, click Control Panel, click Programs, and select Turn Windows Features On Or Off. Accept the UAC elevation prompt and scroll down to Remote Server Administration Tools (see Figure 3-15). Note that the RSAT section is divided into two subsections: Feature Administration Tools and Role Administration Tools. Open Feature Administration Tools, select Failover Clustering Tools, and click OK to enable the tool. Note that the Distributed File System And Share And Storage Management Tools are also selected under the Role Administration Tools when you select Failover Clustering Tools.

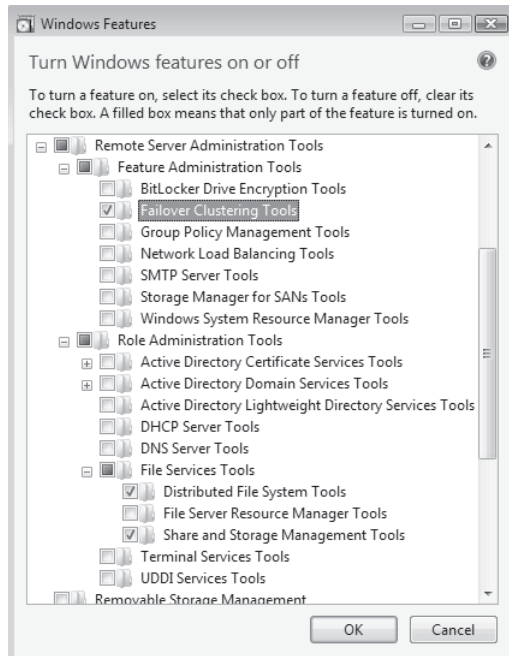


FIGURE 3-15 Installing Failover Clustering Tools

4. Click OK when the operation completes and close Control Panel.

All of these tools will now be listed under the Administrative Tools menu.

You can also perform this operation with the command line with the Windows Update Standalone Installer and the Windows Package Manager (PKGMGR.exe). Begin by installing the update. You can then add the Failover Clustering Tools as part of the Windows Server Administration tools. Note that this command will add all of the Administration Tools except the Internet Information Server (IIS) tools.

```
wusa path\Windows6.0-KB941314-x86.msu /quiet
```

```
start /w pkgmgr /iu:WindowsAdministrationTools
```

path is the location of the update. If you are running an x64 version of Windows Vista, you must use the x64 version of the update package.

When the operation is complete, you can launch the Failover Cluster Management console and select **Connect To Cluster** or **Connect To Server** in the **Actions** pane to locate the cluster or server you want to connect to. Perform this task to link to all of the clusters or servers you want to manage. When you close the console, it will remember the remote server connections you created and reopen with the connections in place.

From this point on, you should manage virtual machine operations from the Failover Cluster Management console because this will abstract VM operations from the individual host servers that make up the cluster (see Figure 3-16). However, even though you can now manage virtual machines independently of the host servers, you will only be able to manage the operation of the VM—startup, shutdown, saved state, and transfers to other hosts. The Failover Cluster Management console does not give you access to the commands required to create and populate VMs. You still need to return to the Hyper-V Manager to perform these operations.

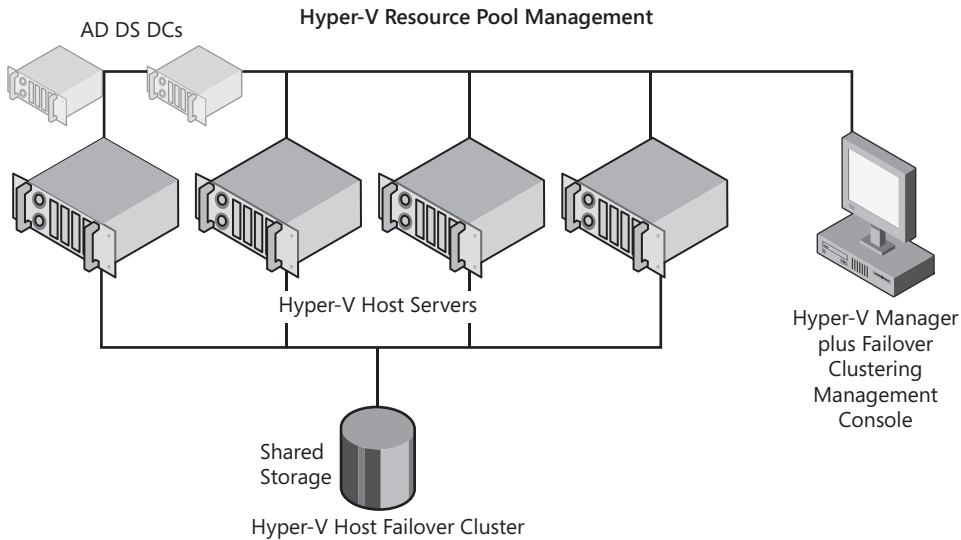


FIGURE 3-16 Managing Hyper-V host clusters may be suitable for small to medium organizations.

Understanding System Center Virtual Machine Manager

As you have seen, Hyper-V Manager provides management capabilities for single hosts and the virtual machines they maintain. Failover Cluster Management gives you a broader view of your Hyper-V hosts by linking them into resource pools and letting you manage the VMs contained in the resource pool independently of the individual host servers. SCVMM comes in where both of these consoles leave off.

SCVMM offers a complete and comprehensive host and virtual machine management interface (see Figure 3-17). The goal of SCVMM is to support dynamic datacenter operations through an in-depth view of host servers as resource pools and virtual machines as entities that are independent of the underlying host infrastructure. It provides access to all of the operations you can perform with Hyper-V Manager as well as all of the operations you can perform with Failover Clustering Management together in a single interface. In addition, it lets you manage several different virtualization engines:

- Virtual Server 2005 R2
- Windows Server 2008 with Hyper-V
- Hyper-V Server 2008
- VMware ESX Server and ESXi Server
- VMware ESX or ESXi servers that are part of a VMware Virtual Infrastructure 3 or greater cluster

Because of this capability, SCVMM can be used to create a single management interface into a heterogeneous host server environment. Remember that Virtual Server 2005 R2 can run on both x86 and x64 versions of Windows Server 2003 SP2 and 2008 with or without Hyper-V; however, it does not have the ability to run x64 VMs, only x86 VMs. Windows Server 2008 with Hyper-V can create fault-tolerant x64 host server infrastructures. Hyper-V Server 2008 can create standalone x64 host servers and is a free download. VMware ESX Server can run fault tolerant infrastructures on both x86 and x64 host server infrastructures

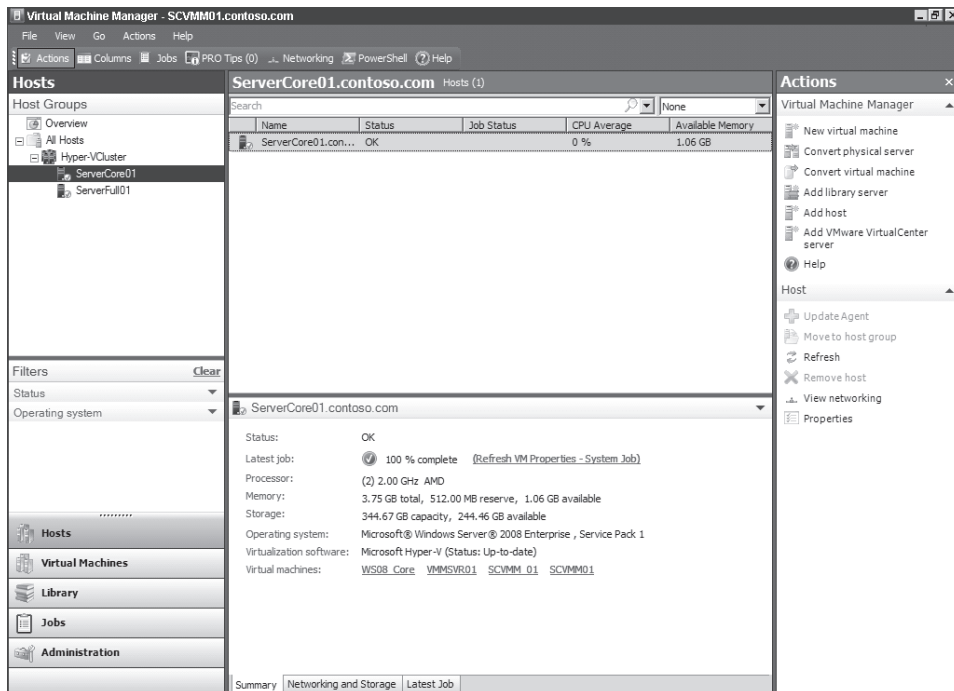


FIGURE 3-17 The SCVMM interface

and ESXi Server is, like Hyper-V Server, a free download that can create standalone x86 or x64 host server infrastructures. With SCVMM as the top-layer management engine, even the most eclectic host server infrastructures can appear as a single, integrated resource pool.

UPDATE ALERT SCVMM R2

In order to manage Windows Server 2008 with Hyper-V R2 or Hyper-V R2 features such as live migration, hot add/remove of VHDs and virtual machine queues or TCP chimneys, you must be using SCVMM R2. SCVMM R2 also supports a new maintenance mode for host servers that will make it easier to update host servers that are in a failover cluster without disrupting the VMs they run. Finally, it includes new support for VMware vCenter and Virtual Desktop Infrastructure as well as supporting the management of host servers in disjointed domains.

MORE INFO ACQUIRING SCVMM 2008

System Center Virtual Machine Manager can be acquired in two different ways. The first is through a System Center package called the Server Management Suite Enterprise (SMSE). SMSE includes four System Center Products: System Center Configuration Manager, System Center Operations Manager, System Center Data Protection Manager, and SCVMM. This option is quite useful for medium to large organizations. The second way to obtain SCVMM is on its own in either the Workgroup or Enterprise versions. Find out more at <http://www.microsoft.com/systemcenter/virtualmachinemanager/en/us/pricing-licensing.aspx>.

Because it is part of System Center, SCVMM provides a familiar interface for host and VM management. The SCVMM GUI includes a series of panes, taskbars, filters, and view buttons. Each view you select displays a Tree pane, a Results pane, a Details pane, and an Actions pane. The different views and commands available in SCVMM depend on the components you choose to install. Table 3-3 outlines the various components displayed in the SCVMM console.

TABLE 3-3 SCVMM Administrator Console Views

VIEW PANE	POSSIBLE ADMINISTRATIVE TASKS
Hosts View	■ Add, remove, and monitor the status of virtual machine hosts. ■ Configure virtual networks, placement options, virtual machine paths, and custom properties on a host. ■ Enable remote connections to virtual machines. Register existing virtual machines on a host. ■ Create and delete host groups for ease of monitoring and managing hosts. ■ Configure host reserves and self-service policies for host groups.
Virtual Machines View	■ Create, deploy, migrate, operate, connect to, clone, repair, store, and remove virtual machines. ■ Create checkpoints so that you can restore virtual machines to a previous state.

VIEW PANE	POSSIBLE ADMINISTRATIVE TASKS
Library View	■ Add file-based resources for use in creating virtual machines. ■ Add Library servers and Library shares. ■ Refresh a library share to immediately index its files in Virtual Machine Manager. By default all library shares are refreshed once per hour. ■ Configure guest operating system profiles, hardware profiles, and virtual machine templates for use in virtual machine creation.
Jobs View	■ Monitor, cancel, restart, search, sort, filter, and group jobs. ■ View the changes that a job made to objects.
Administrative View	■ Overview View graphical summary information of the environment (hosts, virtual machines, recent jobs, and library resources). ■ General Configure global VMM settings: Remote Control and PRO. ■ Managed Computers Manage Virtual Machine Manager agents on managed hosts and Library servers, update the agent, remove agent roles, and re-associate agents with the current VMM Server. ■ Networking View the MAC address range used by VMM across all managed hosts. ■ User Roles View all existing user roles grouped by profile type. ■ System Center View reports generated by System Center Operations Manager. ■ Virtualization Managers View all available virtualization managers: Virtual Machine Manager and VMware VirtualCenter Server.
Reporting View	■ View and open reports This option is available only if you have configured Operations Manager to work with SCVMM.
Diagram View	■ Display the health of the Virtual Machine Manager Server, database server, Library servers, hosts, virtual machines, and VMware VirtualCenter Server servers. This option is available only if you have configured Operations Manager.

Use the filters in SCVMM to reduce the amount of information displayed in each view and focus on the machines and objects you need to work with. SCVMM will provide a comprehensive list of features for host and VM management. Table 3-4 provides a comprehensive list of the SCVMM feature set.

TABLE 3-4 SCVMM Features

FEATURE	DESCRIPTION
Active Directory Domain Services Integration	SCVMM integrates with AD DS to provide secure virtual machine management. However, even when it is integrated with one AD DS forest, SCVMM can work with non-AD DS environments and even other, untrusted AD DS domains.
Centralized Resource Optimization (CRO)	SCVMM provides a unique, centralized interface for the administration of both hosts and VMs. It also supports the tuning of VM or host resources as well as the migration of VMs from one host to another, whether or not the hosts are configured in a failover cluster. If the hosts are not configured in a failover cluster, SCVMM must move the VM files from one host to another. This process takes considerably more time than on a cluster because VM files can be extremely large in size.
Consolidation	A process that examines existing physical servers, analyzing hardware configuration and performance data to identify the best candidates for virtualization. This process requires an integration with System Center Operations Manager 2007 (OpsMgr).
Deployment	SCVMM can support several VM deployment options from isolated, standalone host server setups to geographically distributed, fault-tolerant environments. The deployment options can include: ■ Workgroup Setups All SCVMM components run on the same physical hardware as the host server and VMs. This setup uses a local SQL Server 2005 or 2008 database to store library files. ■ Co-Located or Distributed Data Center Setups SCVMM components are distributed across different systems. The database is installed in a fault-tolerant configuration running SQL Server in a failover cluster. SCVMM is deployed on several servers independent of hosts and VMs. This setup can manage thousands of VMs distributed across various environments. It can also support the management of host servers in a perimeter network as well as in non-trusted AD DS domains.

FEATURE	DESCRIPTION
Failover Cluster	SCVMM is cluster-aware and can manage and configure Hyper-V hosts that are part of a failover cluster. It can also create all of the resource groups and dependencies for fault-tolerant VMs running on these clusters.
Guest OS Profile	The Guest OS Profile is a collection of settings that can be applied to the operating system running in a VM. The profile is similar to a setup answer file and provides automation for the following: ■ System settings ■ Administrator account ■ Domain to join The profile is saved in the SCVMM library and is used to quickly apply the settings to an operating system in a new virtual machine that is created from a template.
Hardware Profile	The Hardware Profile contains the settings that define the hardware characteristics of a VM, including: ■ Processors ■ Memory ■ Floppy Drive ■ Network Adapters ■ DVD drive(s) ■ Priority setting for the VM As with the Guest OS Profile, the Hardware Profile is stored in the library and can be applied as you create new VMS from templates.
Host Servers	SCVMM can manage several different host types: ■ Windows Server 2008 with Hyper-V ■ Hyper-V Server 2008 ■ Virtual Server 2005 R2 ■ VMware ESX Server ■ VMware ESXi Server ■ VMware Virtual Infrastructure Managed hosts are added to the SCVMM resource pool through the Add Hosts Wizard in the SCVMM Administrator Console.

FEATURE	DESCRIPTION
Intelligent Placement	You use Intelligent Placement to determine which host is best suited to run a new VM. Decisions are based on several inputs such as host system configuration data, past workload performance history, administrator-defined business requirements, available resources on the host, and virtual machine resource requirements. This feature can be used with all host servers managed by SCVMM.
Library Server	The Library Server is used to store different items in a virtual infrastructure. SCVMM provides a single interface to manage these components, which include: ■ Stored virtual machines ■ Virtual hard disks ■ Virtual floppy disks ■ .iso files ■ Post-deployment customization scripts ■ Hardware profiles ■ Virtual machine templates ■ Sysprep answer files ■ Post-deployment customization scripts ■ Guest operating system profiles
Managed Host	A host becomes managed when it has been added to the SCVMM library. Multiple hosts can be added to the library and can be managed from one centralized location. A given host can be managed by only one SCVMM server at a time.
Performance and Resource Optimization (PRO)	PRO is a feature that becomes available when you link OpsMgr's capabilities to monitor host status and send alerts within the SCVMM interface about host health. PRO can be used to dynamically manage host resource pools.
Physical to Virtual (P2V) Conversion	A process that converts a physical machine into a virtual machine. SCVMM will also convert physical machine drivers to virtual machine drivers during the conversion process.
Role-Based Administration	SCVMM supports the delegation of specific administrative functions to other members of the resource pool administration team.
Storage Area Network (SAN) Integration	SCVMM can auto-detect SAN infrastructures and use them to store library and other components. It can also use Fibre Channel connections to copy VM components at very fast speeds.

FEATURE	DESCRIPTION
Self-Service Portal	SCVMM includes a self-service portal that allows authorized users to deploy and manage their own virtual machines through a Web portal. Users are constrained to selected host servers or host groups and all VMs are generated from templates stored in the SCVMM library.
Stored virtual machine	The components that make up a VM, such as .vhd files and VM properties, are stored in the SCVMM library. When you use a stored VM to deploy a new VM, SCVMM generates a configuration file from this data for the new VM.
System Center GUI	SCVMM uses the System Center graphical user interface to provide a familiar management environment for resource pool administrators.
Template	Templates are models that can be used to generate new VMs. Templates include three key elements: ■ Guest operating system profile ■ Hardware profile ■ One or more .vhd files
Virtual to Virtual (V2V) Conversion	A process that converts a virtual machine in one format into a virtual machine in Hyper-V format. For example, you can use V2V to convert VMware VMs to Hyper-V VMs or convert Virtual Server 2005 R2 VMs to Hyper-V VMs. SCVMM will also convert virtual machine drivers from one format to another during the conversion process.
Windows PowerShell Integration	SCVMM uses the Windows PowerShell scripting language to generate all SCVMM operations and commands. Rely on the GUI to prepare operations through wizards and then capture the scripts that are generated by the GUI to automate future operations.

When you deploy SCVMM, you to deploy several different components to create a fully managed resource pool infrastructure. The various components, both required and optional, are listed in Table 3-5.

Each of the components listed in Table 3-5 work together to create the SCVMM implementation. This implementation can be used in homogeneous environments where all hosts run Hyper-V either through Windows Server with Hyper-V or through Hyper-V Server (see Figure 3-18 on page 163). Homogeneous environments are the type of environment you should aim for because they are the simplest to manage and deploy.

TABLE 3-5 SCVMM Components

COMPONENT	DESCRIPTION
SCVMM Server	The SCVMM Server is the central SCVMM component. It must be installed before any other component. By default, it includes a Library Server.
Virtual Machine Manager (VMM) Service	When you install the SCVMM Server, you also install the VMM service that controls the components of the resource pool. The VMM service is used to run commands and transfer files as well as control communications with other SCVMM components, hosts, and SCVMM Library servers.
Microsoft SQL Server	The SCVMM server relies on a Microsoft SQL Server database to store all SCVMM configuration information. This database can be based on either a SQL Server Express installation or a full installation of a fault tolerant SQL Server cluster. The Express edition should only be used in very small environments. SCVMM can work with SQL Server 2005 or SQL Server 2008. However, the SCVMM installation files only include SQL Server 2005 Express.
Administrator Console	An independent MMC console that can be installed on the same computer as the SCVMM server or on a different server or workstation. The console requires the installation of Windows PowerShell to operate. It supports the following operations: ■ Manage global SCVMM configuration settings. ■ Manage and monitor hosts and library servers. ■ Create, deploy, and manage virtual machines.
Library Server	This server maintains a catalog of resources that can be used to generate new VMs in the resource pool.
SCVMM Agent	The agent must be installed on all hosts within the resource pool as well as on the SCVMM server and Library servers. It provides communications between other SCVMM components to manage virtual machines on the hosts and allow VMs, hosts, and Library servers to communicate with the SCVMM server.
Self-Service Portal	This portal is a Web-based component that supports self-service VM creation and management. This component is optional in an SCVMM deployment. It includes policies to control: ■ Which templates self-service users can use to create VMs ■ How many VMs can be created per user ■ Which hosts the users will be able to use to run VMs ■ Which actions users can perform on the VMs they have access to
Windows PowerShell	Windows PowerShell is required to operate the Administrator Console and must be deployed with the console.

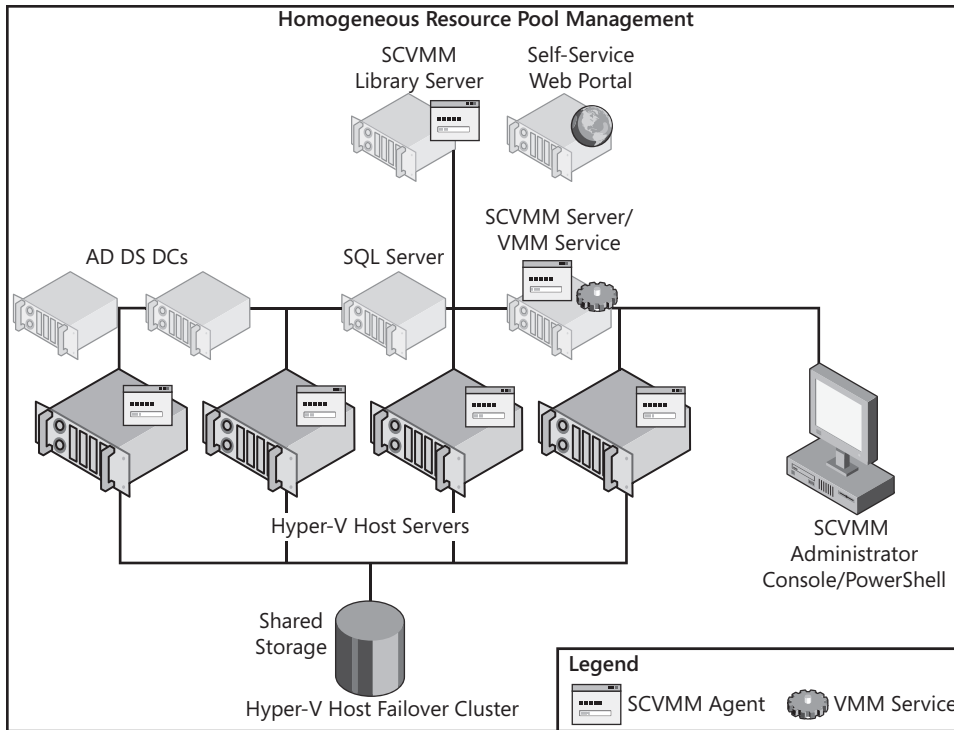


FIGURE 3-18 Managing homogeneous resource pools with SCVMM is suitable for medium to large organizations.

NOTE SCVMM AND OPSMGR

If you intend to integrate SCVMM with OpsMgr to use the SCVMM Reporting feature, you must install the SCVMM Administrator Console on the OpsMgr server because the Virtual Machine Management Pack—the component that integrates OpsMgr with SCVMM—requires access to the Windows PowerShell commands provided by the Administrator Console to generate these reports.

However, many organizations have already invested in server virtualization to some degree. Some may be using Virtual Server 2005 R2 on x86 hosts. Virtual Server is a good platform to use if you want to recover the investment you have in 32-bit server hardware, although these systems should eventually be replaced with x64 hardware and Hyper-V because of the performance and stability Hyper-V brings to VM hosting. Other organizations may have already begun using a hypervisor in the resource pool through the implementation of VMware's free ESXi or paid ESX Server. In both cases, organizations will be running heterogeneous host server infrastructures. Once again, the introduction of SCVMM will provide a single integrated management environment (see Figure 3-19).

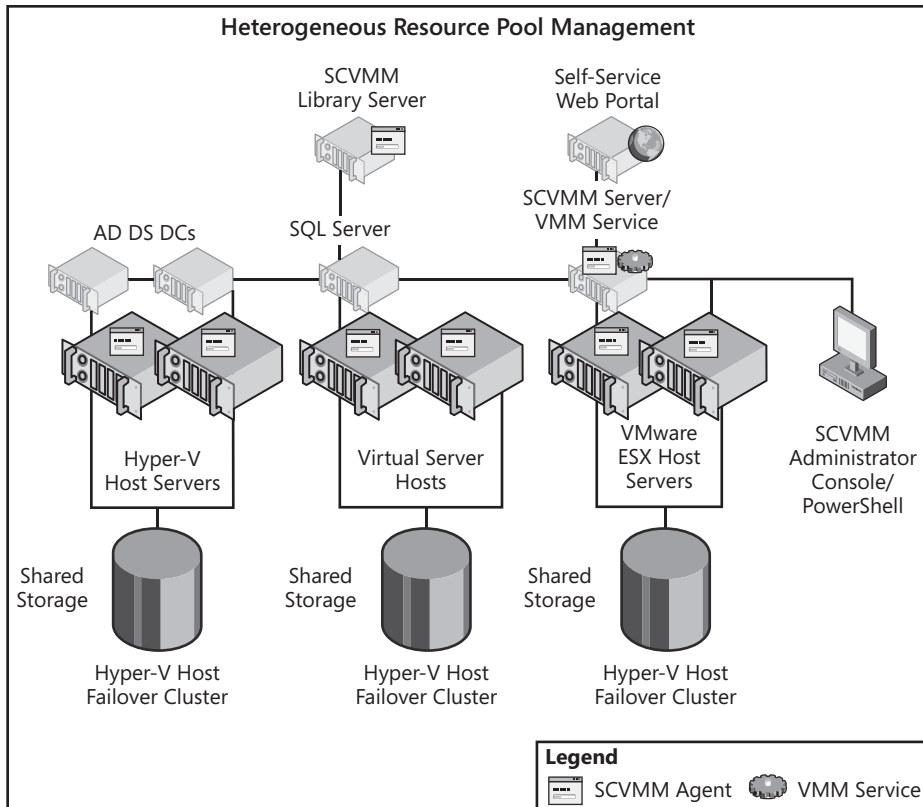


FIGURE 3-19 Managing heterogeneous resource pools with SCVMM is suitable for organizations that have already invested in some form of server virtualization.

Understanding the SCVMM Architecture

To accomplish the management of homogeneous and heterogeneous resource pools, SCVMM must rely on a three-layer architecture (see Figure 3-20).

The first layer—the Managed Computer Layer—uses a variety of communications protocols to interact with the hypervisors or virtual machine engines, physical computers that are used as sources for P2V conversions, the Library, and VMware ESX and ESXi.

- For Hyper-V and Virtual Server 2005 R2 hosts, SCVMM uses the Windows Remote Management (WinRM) protocol, an implementation of Web Service Management Protocol (WS-Management) focused on Windows. WS-Management is a Simple Object Access Protocol (SOAP) that uses common HyperText Transfer Protocol (HTTP) ports such as 80 and 443 to communicate with hardware and operating systems from different vendors. WinRM consists of an HTTP listener on the management server that awaits calls from WinRM clients. The advantage of using HTTP-based management protocols is that the communications can safely traverse firewalls without having to open additional ports.

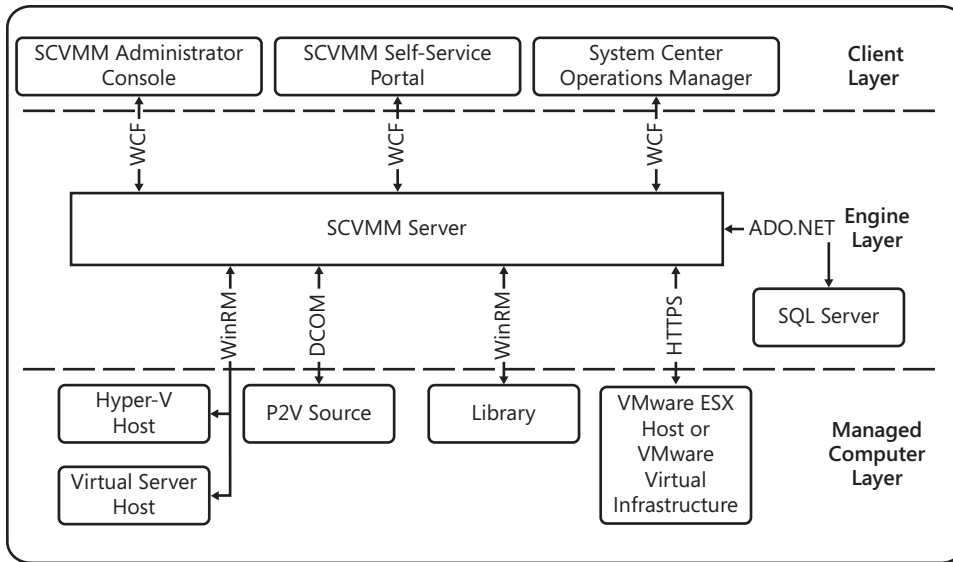


FIGURE 3-20 The three layers of the SCVMM architecture

- For physical computers in P2V operations, SCVMM uses the Distributed Component Object Model (DCOM), a proprietary protocol used to communicate among Windows objects. SCVMM relies on this protocol to send Windows Management Instrumentation (WMI) calls to physical computers during the conversion process.
- For the Library, SCVMM uses WinRM.
- For third-party hypervisors such as VMware ESX and ESXi, SCVMM uses Secure HTTP (HTTPS) with the Secure Sockets Layer (SSL) on port 443 to communicate. In particular, it uses this protocol to communicate with the VMware Virtual Infrastructure Application Programming Interface (API) to manage VMware host servers.

The second layer—the Engine Layer—is the layer that manages all of the SCVMM components. It relies on ADO.NET to communicate with stored data in the SQL Server database and uses the Windows Communications Foundation (WCF), which is part of the .NET Framework 3.0, to interact with the Client Layer.

The third layer—the Client Layer—is the layer that hosts the Administrator Console, the Self-Service Web Portal, and System Center OpsMgr when it is integrated to the SCVMM deployment.



EXAM TIP THE SCVMM ARCHITECTURE

Pay close attention to the SCVMM architecture and its components. They are an important part of the exam.

Understanding SCVMM Communications Ports

Communication between the three layers of the architecture relies on common ports. In many cases, these ports are firewall-friendly. Firewall-friendly ports can support the management of host servers in perimeter networks. In other cases, the ports are used only for internal communications and do not need to traverse firewalls. However, if the Windows Firewall is enabled on hosts running either Hyper-V or Virtual Server 2005 R2, the installation of the SCVMM agent will automatically open the appropriate ports on the host server.

Table 3-6 outlines the various communications ports SCVMM relies on to communicate between the three layers of the SCVMM architecture.

TABLE 3-6 SCVMM Communications Ports

COMMUNICATION	TRANSPORT	PORT
SCVMM Server to SCVMM Agent (control)	Windows Remote Management	80
SCVMM Administrator Console to SCVMM Self-Service Portal	Windows Communications Foundation	80
SCVMM Library to Physical Host	Background Intelligent Transfer Service (BITS)	80
Physical Host to Physical Host	BITS	80
SCVMM Administrator Console reporting view to System Center Operations Manager Reporting Server	HyperText Transfer Protocol	80
SCVMM Server to P2V Source	WinRM	135
SCVMM Server to SCVMM Agent (data)	BITS	443
SCVMM Server to Remote Database	HTTP	1433
VMConnect on Hyper-V hosts for single-class console view	Custom TCP/IP Port	2179
SCVMM Self-Service Portal user Internet Explorer session to Hyper-V host	Remote Desktop Protocol (RDP)	3389
SCVMM Self-Service Portal user Internet Explorer session to Virtual Server host	Virtual Machine Remote Control (VMRC)	5900
SCVMM Administrator Console to SCVMM Server	WCF	8100

In reverse, each SCVMM also interacts with other components through TCP/IP ports. Table 3-7 outlines which ports are used by which SCVMM component.

TABLE 3-7 SCVMM Component Ports

COMPONENT	TRANSPORT	PORT
SCVMM Server	Hypertext Transfer Protocol (HTTP)	80
	Windows Management (WS-MAN)	
	Secure Hypertext Transfer Protocol (HTTPS)	443
	Background Intelligent Transfer Service (BITS)	
	Windows Communication Foundation (WCF) connections to Windows PowerShell or Administrator Console	8100
SCVMM Library Server and Physical Hosts	HTTP	80
	WS-MAN	
	HTTPS	443
	BITS	
	Remote Desktop Protocol (RDP)	3389
	VMConnect on Hyper-V hosts	2179
	Virtual Machine Remote Client (VMRC) on Virtual Server hosts	5900
Microsoft SQL Server	Remote SQL instance connection	1433
	SQL browser service (only needed for initial setup)	1434
VMware Virtual Center Server and VMware ESX Hosts	HTTPS for calling Virtual Infrastructure Web Services APIs	443
	Secure Shell (SSH) for Secure File Transfer Protocol (SFTP) files to or from ESX hosts (not needed for ESX version 3.5i)	22

As you can see, an SCVMM implementation in a heterogeneous environment uses many more protocols than a homogeneous SCVMM/Hyper-V implementation. Because of this, homogeneous implementations are simpler to manage and secure.

Preparing for SCVMM Implementation

When you prepare to deploy SCVMM, you must first understand the various requirements SCVMM requires to operate, including both software and hardware elements. As with the Hyper-V installation, you must prepare these components before you proceed with the SCVMM deployment. Table 3-8 outlines the software requirements for SCVMM.

TABLE 3-8 Software Requirements

COMPONENT	SOFTWARE	DESCRIPTION
SCVMM Server	Operating System	Windows Server 2008 x64 on a physical or a virtual machine. If you use a physical machine, you can co-host SCVMM with the Hyper-V role.
	Database	If no database is available, the SCVMM installation will install Microsoft SQL Server 2005 Express Edition SP1 with its Toolkit and create an instance called MICROSOFT\$VMM\$ on the local computer. You can also use a local or remote database using: ■ Microsoft SQL Server 2005 Standard edition SP1 or SP2 ■ Microsoft SQL Server 2005 Enterprise edition SP1 or SP2 ■ Microsoft SQL Server 2008 ■ Microsoft SQL Server 2008 Standard edition ■ Microsoft SQL Server 2008 Enterprise edition
	Other Software	Microsoft .NET Framework 2.0 which, if not installed, can be installed from the Setup Wizard. Microsoft .NET Framework 3.0 which, if not installed, will be installed automatically. Microsoft Core XML Services (MSXML) 6.0 which, if not installed, can be installed from the Setup Wizard. The existing WinRM on the server operating system.
	For P2V or V2V Support	You must install the Windows Automated Installation Kit 1.1 to support P2V or V2V operations. This kit is installed automatically by SCVMM.

COMPONENT	SOFTWARE	DESCRIPTION
SCVMM Administrator Console	Operating System	Microsoft Windows Server 2008 Microsoft Windows Server 2003 Microsoft Windows Vista SP1 Microsoft Windows XP SP3
	Other Software	Windows PowerShell 1.0. If not installed, download the software from http://go.microsoft.com/fwlink/?LinkId=77521 . On Windows Server 2003, Windows Vista or XP, Microsoft .NET Framework 2.0—which, if not installed, can be installed from the Setup Wizard. On Windows Server 2008, Microsoft .NET Framework 3.0.
SCVMM Self-Service Portal	Operating System	Microsoft Windows Server 2008 Microsoft Windows Server 2003 SP2
	Other Software	For Windows Server 2003, Microsoft .NET Framework 2.0 For Windows Server 2008, Microsoft .NET Framework 3.0 Windows PowerShell 1.0 Internet Information Services (IIS). In Windows Server 2003, install IIS 6 from the Control Panel in Add/Remote Windows Components. In Windows Server 2008, install IIS 7 from Server Manager using the Application Server in the Add Roles Wizard.
SCVMM Agent on Host Servers	Operating System	Windows Server 2003 SP1 or above; x86 or x64 with Virtual Server 2005 R2. Windows Server 2008 with Hyper-V
	Other Software	Windows Remote Management (WinRM) needs to be installed before you add a host or a library in the Administrator Console and also before you install an agent locally on a host. Microsoft Core XML Services (MSXML) 6.0. If not installed, download the software from http://go.microsoft.com/fwlink/?LinkId=84599 . (Note: Use this link for Windows Server 2003 R2—installing it from Add/Remove Windows Components installs the wrong version.)

COMPONENT	SOFTWARE	DESCRIPTION
SCVMM Monitoring and Reporting	System Center Software	To monitor and report in SCVMM, use System Center Operations Manager 2007. To monitor and report on virtual servers, you need to install: ■ System Center Operations Manager 2007 ■ System Center Operations Manager Reporting Server ■ Virtualization Management Pack for System Center Operations Manager 2007

As you can see from the items listed in Table 3-8, preparing for an SCVMM installation requires several different software components, especially if you want to include all of the optional components that are available.

NOTE THE SCVMM LIBRARY

By default, SCVMM will install a Library Server with the SCVMM Server. If you do not intend to use a separate Library Server, you must make sure your SCVMM Server includes enough additional space to host Library items. Virtual hard disk drives and ISO files can require considerable space. Make sure you plan appropriately for this space.

Similarly, you must prepare appropriate hardware requirements. Table 3-9 outlines the hardware requirements for an SCVMM installation.

TABLE 3-9 Hardware Requirements

COMPONENT	PROCESSOR	RAM	DISK SPACE
SCVMM Server minimum requirements	CPU 2.8 GHz or faster (x64)	2 GB	7 GB if using the default local SQL Server 2005 Express database. 1 GB if using a remote SQL Server database. 200 GB if using SCVMM Server as Library Server. If using an existing local instance of SQL Server, plan for at least 7 GB.
SCVMM Server with fewer than 150 hosts	Dual-processor or dual-core processor at 3.2 GHz or faster (x64)	4 GB	160 GB with 40 GB allocated to the system drive and 120 GB allocated to the local Library Server.

COMPONENT	PROCESSOR	RAM	DISK SPACE
			If the SQL database is installed locally, add 10 GB to the system drive (50 GB total).
SCCVMM Server with more than 150 hosts	Dual-processor or dual-core processor at 3.66 GHz or faster (x64)	8 GB	50 GB with the Library Server running on a separate system.
SCVMM Administrator Console	Pentium 4, 550 MHz	512 MB	512 MB
SCVMM Self-Service Portal	Pentium 4, 2.8 GHz	2 GB	512 MB
SCVMM Agent	The requirements for host servers depend on the number and type of VMs, the applications installed on the VMs, and the anticipated workload for the host server. For more information see the Hyper-V Planning and Deployment Guide at http://download.microsoft.com/download/8/1/5/81556693-1f05-494-a-8d45-cdeeb6d735e0/HyperV_Deploy.doc. If the host is running Virtual Server, look up the Virtual Server 2005 Deployment Guide at http://www.microsoft.com/technet/prodtechnol/virtualserver/2005/proddocs/vs_deploy.msp?mfr=true.		
Library Server	The requirements depend on the number and size of VM templates, virtual hard disks, virtual floppy disks, ISO images, scripts, hardware profiles, guest operating system profiles, and stored VMs in the Library. The minimum recommended hard disk capacity is 200 GB. More may be required in large host farms.		



EXAM TIP LOCAL SCVMM DATABASE WITH SQL SERVER EXPRESS

The use of SQL Server Express limits the size of the SCVMM database to a maximum of 4 GB. If you anticipate needing more, you need to use a full version of SQL Server.

Once again, the implementation of SCVMM requires several different hardware components. Finally, SCVMM also has custom networking requirements, which are listed in Table 3-10.

TABLE 3-10 Networking Requirements

REQUIREMENT	DESCRIPTION
Connection	At least a 100-MB Ethernet connection. A 1-GB Ethernet ensures more adequate bandwidth and improved performance.
Domain	The SCVMM Server must be part of a domain in AD DS. Physical host servers may or may not be part of a domain. Join internal hosts to the same domain as SCVMM and keep perimeter hosts in a workgroup. If you include VMware ESX hosts, they do not need to be part of a domain.
Firewall	Both ports 80 and 443 are required to manage hosts through firewalls. These ports are opened automatically when you install the agent on a Windows system. They must be opened manually on hardware or non-Microsoft firewalls, but ports 80 and 443 are commonly open by default on most firewalls.

Note that the details listed in Tables 3-8, 3-9, and 3-10 are minimum requirements. For improved performance, install SCVMM components on systems with more powerful resources than those listed in these tables.

MORE INFO SCVMM REQUIREMENTS LIST

For more information on SCVMM requirements, go to <http://technet.microsoft.com/en-ca/library/cc764328.aspx>.

Microsoft also sets a hard limit of 150 host servers for SCVMM installation recommendations. If your SCVMM installation is managing fewer than 150 host servers, you can install SCVMM on a single server and run the Library from the same server. If you are managing more than 150 hosts, you should use dedicated Library and SCVMM servers, separating the two functions. SQL Server should also be running on a separate system. It is also a good practice to use a clustered SQL Server instance on separate systems to ensure high availability of the SCVMM database.

When you plan for your own implementation of SCVMM, you should at least double the system recommendations. This will ensure that you have sufficient space and capacity for growth and proper operation in peak loads.

MORE INFO THE SCVMM DECISION FLOW

Microsoft has put together a flow chart that outlines the decision-making process for SCVMM implementations. Find it at <http://technet.microsoft.com/en-ca/scvmm/cc835256.aspx>.



EXAM TIP SCVMM CONFIGURATION ANALYZER

SCVMM offers a Configuration Analyzer that can scan your system prior to an SCVMM deployment. The Analyzer will identify any potential issues with your system configuration and provide information on best practices for use with SCVMM deployments. Find the Analyzer at <http://www.microsoft.com/downloads/details.aspx?FamilyID=ae7c6a09-e8df-4adc-8686-f4d140a3a3f4&displaylang=en>. Note, however, that the Analyzer is not part of the exam because it was not released until December 2008.

You must install and run the Analyzer on the computer that either currently is or will become your SCVMM Server. Before you install the Analyzer, you must download and install the 64-bit version of Microsoft Baseline Configuration Analyzer (MBCA). To download the MBCASetup64.msi file, go to <http://go.microsoft.com/fwlink/?LinkID=97952>.

You should use this version of the Analyzer with Virtual Machine Manager 2008 only. To download the Analyzer for Virtual Machine Manager 2007, go to <http://go.microsoft.com/fwlink/?LinkID=132136>.

IMPORTANT INSTALLING SCVMM ON A SERVER RUNNING HYPER-V

You can install SCVMM Server on a computer running Hyper-V; however, it is not a recommended practice because your Hyper-V servers should only run the Hyper-V role to achieve optimal performance (see Lesson 3 of this chapter). If you still decide to do so, you must install two important updates on the co-hosting Hyper-V server.

The first update will update the Hyper-V service to work with a local copy of SCVMM. It is update number KB956589 and can be found at <http://support.microsoft.com/kb/956589>. You should install this update on every Hyper-V host managed by SCVMM as a best practice.

The second update is required to modify the BITS client on the local computer. It is update number KB956774 and can be found at <http://support.microsoft.com/kb/956774>.

If you do not install these updates, your Hyper-V host will always display a status of Needs Attention and will never resolve to OK.

Distributed SCVMM Implementation Recommendations

When you install SCVMM in very large environments, you should consider the following:

- If you plan to run SCVMM in a multiple AD DS forest environment, and SCVMM operations will traverse these forests, you must establish a two-way Forest Trust relationship.
- If your SCVMM will traverse multiple forests, but only interact with specific domains in each forest, you can implement a two-way trust between each affected domain.
- When you use remote installations of SQL Server, you must use a named account—often called a service account—to run the SQL Server Service. You cannot use the Local System account.

- When you use SCVMM with Virtual Server, it will rely on the Virtual Machine Remote Control protocol to control VMs. By default this protocol is not encrypted. You should use SSL to encrypt this protocol to protect the information your administrators send to these VMs.

In addition, you need to keep several considerations in mind after SCVMM is installed:

- Run your VMs under a specific service account instead of the default account of the user that launched the VM. Limit the level of privileges of this service account.
- Make your VM administrators part of the local Virtual Machine Manager Administrator security group. They do not need local administrative rights on the machine to do this.
- Secure your Library servers at the file system level. Assign only the SCVMM administrators and the Virtual Machine Manager Servers account at the NTFS security level to Library folders. Where appropriate, assign specific self-service users—ideally through a custom group—if you implemented the Self-Service Portal.
- The SCVMM installation automatically creates a local account called Virtual Machine Manager Servers as a local administrator of the machine. Make sure this account is not removed through Restricted Groups settings in Group Policy; otherwise, the SCVMM Server will be unable to operate.

Keep these elements in mind when customizing your SCVMM installation.

Upgrading from SCVMM 2007 to SCVMM 2008

Many organizations will already be using SCVMM 2007 to manage Virtual Server 2005 R2 hosts. If you want to upgrade your SCVMM 2007 installation to 2008, you must take special steps to protect your existing information. Also note the following:

- Begin by creating a backup of the SCVMM 2007 database using SQL Server Management Studio, not SCVMM database backup. SCVMM 2007 database backup is not compatible with SCVMM 2008.

NOTE DATABASE BACKUP

For more information on how to back up the database with SQL Server Management Studio, see <http://msdn.microsoft.com/en-us/library/ms187510.aspx>.

- The upgrade will lose all passwords and product keys for VM templates, VM Profiles, Hardware Profiles, and those stored in the Jobs Table.
- Self-Service information and custom fields for VMs and hosts are maintained.

Make note of any potentially lost data and then proceed as follows to perform the upgrade:

1. Begin by creating a backup of your SCVMM 2007 database with SQL Server Management Studio. Restore the database on the server that will host the SCVMM 2008 database. This can be the local SCVMM Server or a remote SQL Server.

2. Install SCVMM. During the installation, specify the existing database in the SQL Server Settings page. Setup will automatically upgrade the database.
3. Install the SCVMM 2008 Administrator Console and connect to the SCVMM Server.
4. In the Administrative View of the console, click Managed Computers. Your SCVMM 2007 hosts should appear with an agent communication status of Access Denied.
5. Use the Results Pane to select the disconnected hosts and click Re-associate in the Actions pane. This will change the host status to Unsupported.
6. Select the hosts again and click Update Agent in the Actions pane. Hosts will change status to Responding and list an up-to-date agent status. Your host upgrade is complete.

NOTE SCVMM HOST UPDATES

Update hosts in batches of 10 to 25, first associating the hosts with the SCVMM 2008 server and then updating the agents on the hosts, until all hosts have been updated. This will improve the upgrade performance.

7. Repeat steps 5 and 6 with any or all Library Servers.
8. Some hosts may still have a status of Needs Attention. Click Refresh to make sure the status is updated. Virtual Server 2005 R2 hosts managed by SCVMM 2008 must have update number KB948515 installed before the host status will change to OK. If your hosts still list as Needs Attention, you must apply the update to them.

NOTE THE VIRTUAL SERVER 2005 R2 SP1 UPDATE

Download the Virtual Server R2 SP1 update at <http://go.microsoft.com/fwlink/?LinkId=120488>.

9. Select the hosts that still list as Needs Attention and click Update Virtual Server in the Actions pane. The host will have a host status of OK. This indicates the upgrade for the hosts is complete.
10. Review all other systems in your SCVMM management group to ensure that their status is listed as OK. When all hosts are listed as OK, your upgrade is complete.

MORE INFO CITRIX ESSENTIALS FOR HYPER-V MANAGEMENT

As a long-standing partner with Microsoft, Citrix has released several different tools to support Microsoft virtualization products. One of the most interesting is Citrix Essentials for Hyper-V Management. Essentials links with SCVMM and Hyper-V hosts to provide additional management functionality. For example, with Essentials, you will gain more granular control over resource pool storage foundations, gain dynamic provisioning services for VMs, and gain lifecycle management features, allowing you to control the

generation of entire environments through authorization workflows. Organizations working with massive numbers of host servers and VMs should look to this product for additional functionality. Find out more at <http://www.citrix.com/English/ps2/products/feature.asp?contentID=1686941>.

PRACTICE Installing SCVMM

In this practice you will perform the installation of SCVMM in a virtual machine running on one of your two Hyper-V hosts. You will use this SCVMM installation later on to manage your Hyper-V environment. This practice consists of seven exercises. In Exercise 1, you export a virtual machine from ServerFull01 so that you can import it later on ServerCore01. In Exercise 2, you add an external disk to ServerCore01. You will use this disk to store the virtual machines you run on this server. Then you will copy the exported files that make up the WS08_Full virtual machine you created in Lesson 2 in Chapter 2 from ServerFull01 to the new disk you added to ServerCore01. In Exercise 3, you will import the VM on ServerCore01. In Exercise 4, you will add a new virtual hard drive to this machine to support the installation of SCVMM and prepare the new virtual machine for the SCVMM installation. In Exercise 5, you install SCVMM using the guidelines for an installation for fewer than 150 host servers. In Exercise 6, you install the SCVMM Administrator Console. And finally, in Exercise 7, you add the SCVMM agent to your Hyper-V hosts.

NOTE INSTALLING SCVMM VS. USING AN SCVMM VHD

This exercise takes you through the steps required to install SCVMM on your own virtual machine. Alternatively, you could simply download the evaluation virtual hard disk for SCVMM. This VHD includes a pre-installed version of SCVMM which is ready to run. Find the evaluation VHD at <http://www.microsoft.com/downloads/details.aspx?FamilyID=4a27e89c-2d73-4f57-a62c-83afb4c953f0&DisplayLang=en>.

EXERCISE 1 Export a Virtual Machine

In this exercise you will export a VM from ServerFull01 so that you can import it on ServerCore01 later. The export process packages a VM in a special transportable format that Hyper-V understands.

1. Log on to ServerFull01 and launch Hyper-V Manager. You can either use the standalone console or perform the action through Server Manager. Make sure you can see ServerCore01 in the Hyper-V console.
2. Click ServerFull01 in the Tree pane of the console.
3. Right-click WS08_Full and choose Export from the shortcut menu.
4. Click Browse and move to C:\VirtualMachines on ServerFull01. Create a new folder called **WS08_FullExport** and click Select Folder.

5. Click Export to begin the process. An export status will appear next to the VM name in the Details pane under the Operations heading. Wait until the export is complete before proceeding with Exercise 2.

Exporting a virtual machine brings all of the files that make up the VM into a single folder. This includes virtual machine configuration, virtual hard drive(s), and potential snapshots that may belong to the VM. It then makes it easier to transport the VM from one Hyper-V host to another.

EXERCISE 2 Add an External Disk to ServerCore01

In this exercise you will add an external disk to your Server Core Hyper-V host. As outlined in the Introduction, you need an external USB hard disk drive that is at least 100 GB in size. Once again, perform this operation with domain administrator credentials. Only local administrative credentials are required, but using domain administrator credentials simplifies the process.

1. Begin by plugging in the external hard disk into a USB port on ServerCore01. The system will recognize the disk and add it to the system's configuration.
2. Log on to ServerFull01. Click, Start, point to Administrative Tools, and click Computer Management. You will use this tool to configure the disk remotely on ServerCore01.
3. Right-click Computer Management (Local) and select Connect To Another Computer. Type in **ServerCore01** and click OK.
4. Move to the Storage node in the Tree pane and click Disk Management. Locate the new disk and make sure it is formatted and assigned to the D: drive. If it is not formatted, right-click the partition and choose Format to format it in the NTFS format and assign the D letter. Name the disk **VMDData**. If it is already formatted, right-click the partition, select Change Drive Letter And Paths, click Change to choose D from the drop-down list, and then click OK twice.

NOTE DRIVE LETTER ASSIGNMENTS

The Server Core system may already have assigned the D letter to the DVD drive. If so, you must change the DVD drive to E before you can assign D to the new disk.

5. Open Windows Explorer and move to the address bar. Type **\\ServerCore01\D\$** and press Enter. Create a folder called **VirtualMachines** in the root of the ServerCore01 D: drive.
6. Move to drive C: on ServerFull01 in Windows Explorer, open the VirtualMachines folder, right-click the WS08_FullExport folder, and choose Copy.
7. Move back to the D:\VirtualMachines folder on ServerCore01 and right-click and choose Paste. This will copy the files that make up the exported WS08_Full virtual machine to ServerCore01.

Your computer is ready when the copy completes.

EXERCISE 3 Import a Virtual Machine on ServerCore01

In this exercise you will import a virtual machine in Hyper-V on ServerCore01. Again, log on with domain administrator credentials.

1. Log on to ServerFull01 and launch Hyper-V Manager. You can either use the stand-alone console or perform the action through Server Manager. Make sure you can see ServerCore01 in the Hyper-V console.
2. Click ServerCore01 in the Tree pane and select Import Virtual Machine from the Actions pane.
3. Click Browse to go to D:\VirtualMachines\WS08_FullExport\WS08_Full. Choose Select Folder. Note that you must use the VM subfolder to import the VM. The machine is imported into ServerCore01 and is ready to run from this system.
4. Finish the process by renaming the machine and examining its settings. Right-click WS08_Full in the Details pane of ServerCore01 and choose Rename. Type **SCVMM01** and press Enter.
5. Right-click SCVMM01 and choose Settings. Move to Network Adapter, assign Hyper-V External to the adapter, and click Apply.
6. Click IDE Controller 0, choose Hard Drive in the right pane, and then click Add. This will add a hard drive connection to IDE Controller 0 and assign 1 (in use) as the Location.
7. Click New under Virtual Hard Disk (.vhd) File. Click Next.
8. Under Choose Disk Type, make sure Dynamically Expanding is selected and click Next.
9. Type **SCVMM01DiskD.vhd** as the name and click Browse to go to D:\VirtualMachines\WS08_FullExport\WS08_Full. Click Select Folder and then click Next.
10. Choose Create A New Blank Virtual Hard Disk and set it to 60 GB. Normally, your SCVMM Library Server should use 100 GB or more, but for the purposes of this exercise, 60 GB will be sufficient. Click Next and then click Finish. Click OK to close the settings box.

Your new VM is ready.

EXERCISE 4 Prepare for the SCVMM Server Installation

In this exercise you will install an SCVMM Server into your new VM. You will open the VM, add it to the Contoso domain, configure its D: drive, and then proceed to the installation of SCVMM. Use domain administrator credentials to perform this activity. In this case, domain administrator privileges are required for this operation.

1. Log on to ServerFull01 using the domain administrator account.
2. Open Internet Explorer and connect to the Microsoft System Center Virtual Machine Manager 2008 Evaluation site at <http://www.microsoft.com/downloads/details.aspx?FamilyID=ED012990-6E86-4B43-9842-DA5C02FF1C83&displaylang=en>. Click Continue, select whether you want to register, and click Continue.

3. The download consists of three files. Click the download button for the first file and then click Save. Type in **\\ServerCore01\D\$** as the save path and create a new folder in the root of the disk called **SourceFiles**. Click Save. Repeat for the two other files. The download will take some time. Meanwhile, you can continue preparing your virtual machine.
4. In Hyper-V Manager, make sure ServerCore01 is selected and click SCVMM01. Click Start in the Actions pane.
5. Double-click the SCVMM01 thumbnail at the bottom of the Details pane. This will open the Hyper-V VM Console and let you interact with the VM. Make sure the VM starts in normal mode.
6. When the VM is started, click the first button in the Virtual Machine Connection (VMC) console to send a Ctrl+Alt+Delete to the machine. Log on with **Administrator** and use **pass@word1** for the password.
7. When you log on, Windows will have discovered new hardware and will request a driver disk. Click Cancel or press Esc. The Initial Configurations Tasks (ICT) Wizard will launch. Move the cursor to the Action menu in the VMC console and choose Insert Integration Services Setup Disk. This will link the Integration Services ISO to the machine's DVD drive and launch AutoPlay. Click inside the console window in the AutoPlay dialog box and press Enter. This will launch the setup. A previous version of the drivers exists and a message will display to announce that an upgrade will be performed (see Figure 3-21). Press Enter or select OK and click Yes when a reboot is requested. This will upgrade the Integration Services and allow your mouse to work in the console even in Remote Desktop Connections.

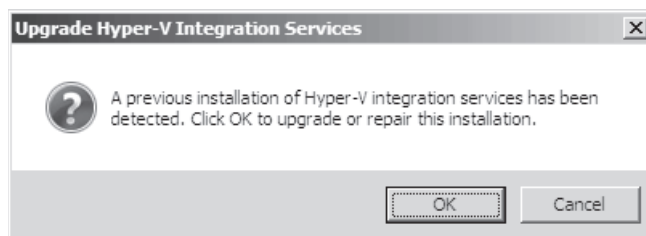


FIGURE 3-21 Upgrading Integration Services

8. Log on to the machine again when the reboot is complete. This time, a Terminal Services Licensing Configuration message will appear. Close it to proceed. You must perform several activities before this server is ready to host SCVMM. First, you must give it an IP address, rename it, and join it to the domain. Move to ICT, click Configure Networking, right-click the connection, and then select Properties. Select Internet Protocol Version 4 and click Properties. Assign **192.168.0.11** as the IP address, **255.255.255.0** as the subnet mask, **192.168.0.1** as the gateway, and **192.168.0.5** as the DNS server. Click Advanced and then click the DNS tab. Type in **Contoso.com** in the DNS suffix for this connection and select Use This Connection's DNS Suffix In DNS registration and click OK three times. Close the Network Connections window.



EXAM TIP DNS SERVER NAME

The SCVMM Server installation will fail if you do not use a fully qualified domain name (FQDN) for the server because it does not support NetBIOS names. Make sure your SCVMM server includes a DNS suffix in its TCP/IP properties.

9. In ICT, click Provide Computer Name And Domain. Click Change, name the computer **SCVMM01** and join the Contoso.com domain. Type in your domain administrator credentials and password and click OK. Click OK in the Welcome To The Contoso Domain dialog box and then click OK to restart the computer. Click Close to close the dialog box and restart.
10. When the reboot is completed, log on as the Contoso domain administrator. Click Switch User and provide your domain administrator credentials with a preceding **Contoso** to make sure you log on to the domain.
11. Now you will change the roles assigned to this machine. Select Do Not Show This Window At Logon and close ICT. When Server Manager launches, right-click Roles and select Remove Roles. Click Next.

NOTE SECURITY UPDATES

Note that you should configure and install updates on this computer as you would with any running machine in your network.

12. Clear Active Directory Domain Services, Network Policy And Access Services, and Terminal Services. Click Remove Dependent Role Services whenever it pops up, click Next, and then click Remove. Click Close when the removal is complete and click Yes to restart the machine.
13. When the machine restarts, log on as domain administrator. When Server Manager starts, move to the Storage and then Disk Management node in the Tree pane. Click OK to initialize the new disk. Right-click the DVD drive, choose Change Drive Letter Or Path, and change it to E:. Click OK and then click Yes.
14. Right-click the blank partition and choose New Simple Volume, then click Next. Choose the entire partition and click Next. Select the D: letter and click Next. Name the volume **SCVMMData**, make sure NTFS is selected, and choose Perform A Quick Format. Click Next and then click Finish.
15. Move to Configuration | Local Users And Groups | Groups and double-click Administrators. Click Add, type in **SCVMM_Service**, click Check Names, and then OK twice.

Your machine is ready for the installation of SCVMM.

EXERCISE 5 Install SCVMM Server

In this exercise you will install an SCVMM Server into your new VM. You will open the VM and proceed to the installation of SCVMM. Use domain administrator credentials to perform this activity. In this case, domain administrator privileges are required for the operation.

1. Log on to ServerFull01 and move to ServerCore01 in Hyper-V Manager. Start SCVMM01 if it is not already started. Once the machine is started, double-click the SCVMM01 thumbnail and log on to SCVMM01 with domain administrator credentials.
2. Open Windows Explorer (click Start, right-click Computer, and select Explore) and move to the address bar. Type in `\\ServerCore01\D$` as the save path and move to the SourceFiles folder. Double-click SCVMM2008_Eval.part1.exe. This will decompress the SCVMM installation files. Click Run and then click Run again. This will decompress all of the files making up the evaluation. When the installer asks if you want to run SETUP.exe, click OK and then click Run. SCVMM Setup will launch (see Figure 3-22).

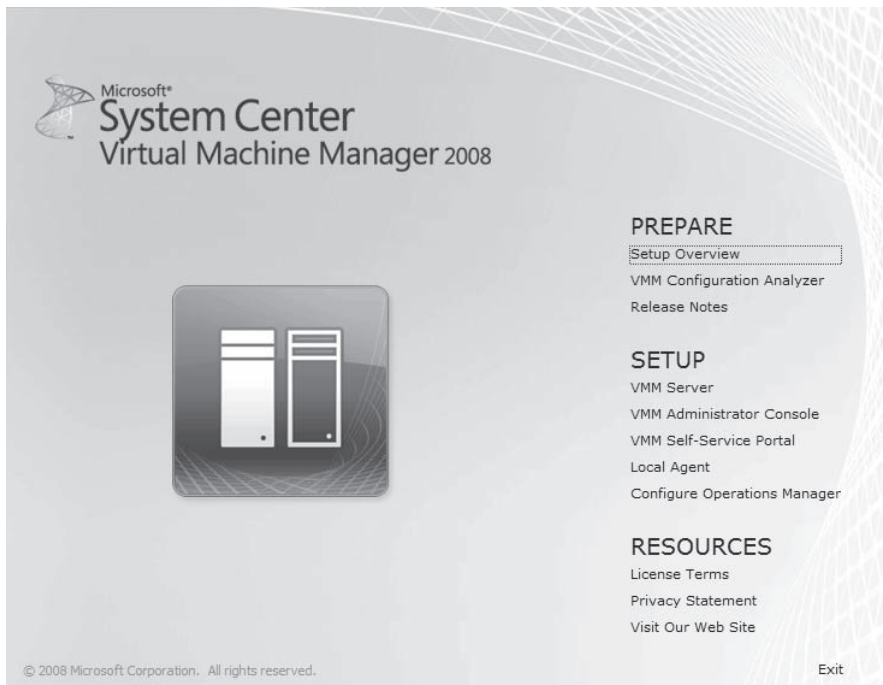


FIGURE 3-22 Running SCVMM Setup

This setup page includes several options:

- The Prepare section outlines three options. Setup Overview lets you review the SCVMM Setup requirements. VMM Configuration Analyzer points you to the download site for the Analyzer, which lets you scan the system you are installing SCVMM into and provides best practices for configuration. Release Notes lets you find the latest information related to the SCVMM setup.

- The Setup section outlines five options: VMM Server, VMM Administrator Console, Self-Service Portal, Local Agent, and Configure Operations Manager.
 - The Resources section outlines three options. License Terms lets you read about SCVMM licensing requirements. Privacy Statement lists privacy information about SCVMM. Visit Our Web Site links you to the SCVMM site on Microsoft TechNet.
3. Click VMM Server to launch the Server installation, click Install Server, and accept the License Terms. Click Next.
 4. On the Microsoft Update page select Use Microsoft Update and click Next. This will update SCVMM installation files if updates are available. Click No on the Customer Experience Improvement Page and click Next.
 5. On the Product Registration page, enter your name and your organization's name.
 6. On the Prerequisites Check page, SCVMM Setup will verify that both hardware and software prerequisites are met. When they pass, click Next. On the Installation Location page, keep the default location, and click Next.
 7. On the SQL Server Settings page, select Install SQL Server 2005 Express Edition, and click Browse, move to drive D: and click Make New Folder, type **VMMDB** as the folder name and press Enter, then OK. Click Next.
 8. On the Library Share Settings page, select Create A New Library, click Change to locate the library on drive D:, create a new folder called **SCVMM_Library**, and click OK. Click Next. Note that once the Library is created on this system, you can no longer move it (see Figure 3-23).

NOTE LIBRARY SHARE

During the installation, the Setup Wizard will create a folder named VHDs and two virtual hard disks, one of 16 GB and the other of 60 GB. These disks can be used as sources for new VM system drives or simply as additional disk drives on existing VMs.

9. On the Installation Settings page, keep the default ports. Note the ports that will be used—you will need to use the same ports for all other component installations. You can refer to Table 3-6 for additional port information. Click Other Account and type in **Contoso\SCVMM_Service** and its password. Click Next.
10. On the Summary of Settings page, review your changes and click Install. The installation begins. Click Run when prompted to run the SQL Server Express Setup and click Run again for the SQL Server Tools. Note that the system will install SQL Server, SQL Server Tools, .NET Framework 3.0, Windows Automated Installation Kit 1.1, and the SCVMM Server. Once the installation is complete, you can check for any available updates. Clear this option. Click Close.

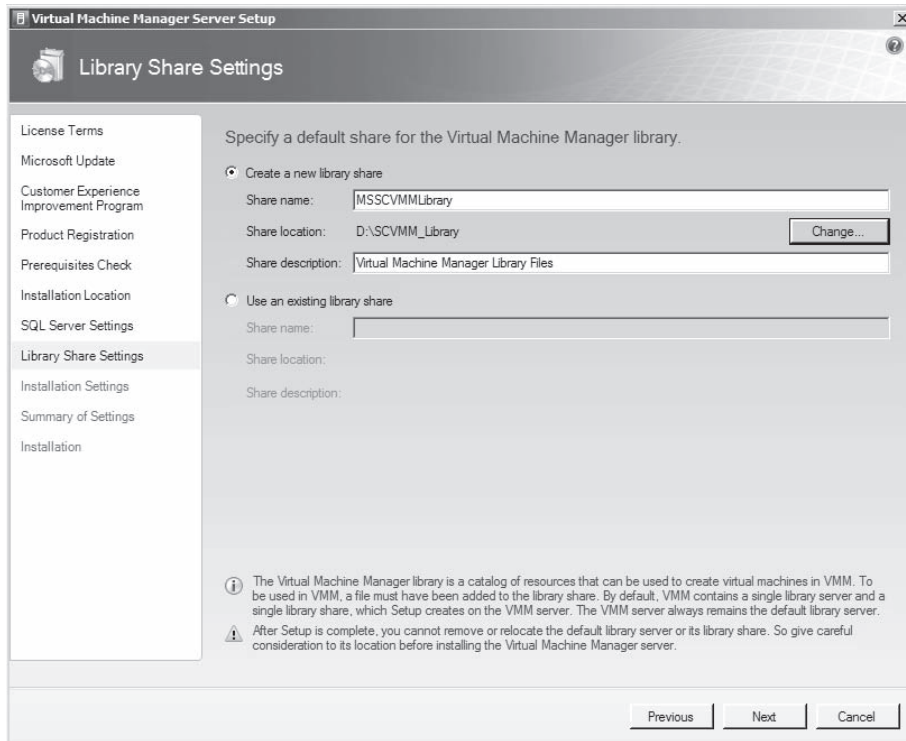


FIGURE 3-23 Creating the Library Share

EXERCISE 6 Install the SCVMM Administrator Console

In this exercise you will install the SCVMM Administrator Console. This console will be installed on the same computer as the SCVMM Server. The installation of the Administrator Console will also install Windows PowerShell.

NOTE INSTALLING WITH SC OpsMgr

If you use the Operations Manager Administrator Console to perform tasks on the hosts and virtual machines from the Virtualization Management Pack, you must install the console on the same computer as the Operations Manager Server.

1. Launch Setup.exe and click VMM Administrator Console. Accept the License Terms. Click Next.
2. On the Microsoft Update page select Use Microsoft Update and click Next. Note the information on the Customer Experience Improvement Page and click Next.
3. Note that the prerequisites passed and click Next. Accept the default path and click Next.

4. On the Port Assignment page, use the default port (8100) and click Next. On the Summary Of Settings page, review your settings and click Install.
5. When the installation is complete, you can check for any available updates. Clear this option. You can also add a shortcut to your desktop and launch the console. Click Open The VMM Administrator Console When The Wizard Closes and click Close.
6. The first time you open the console, the Connect To Server dialog box opens. Click Connect. The connection to the local SCVMM Server will occur using the default port 8100. Click Connect. When you connect to a remote server, replace Localhost with the FQDN of the server name in the form of **Servername:8100**, where *Servername* is the name of the server that runs SCVMM Server.

EXERCISE 7 Deploy the SCVMM Agent

Each host server that is part of an SCVMM farm must include an agent. Agent deployment can be done locally or remotely through the Windows Installer for the agent files. The agent is not required on the SCVMM Server because it is part of the installation of the Server. Use the installation files to install on your other servers. Perform this operation on ServerFull01.

1. Log on to ServerFull01 with domain administrator credentials. Link to the SCVMM installation files and launch Setup.exe.
2. Click Local Agent.
3. Click Next to accept the default installation location and click Next again to accept the default port settings configuration.
4. On the Security File Folder page, ensure that the This Host Is On A Perimeter Network check box is cleared. Click Next.
5. On the Host Network Name page, click Next to have SCVMM contact the host by using its local computer name, click Next, and then click Install.

NOTE ADDING AGENTS TO PERIMETER NETWORKS

When a SCVMM agent is installed host in a perimeter network, the Agent Setup Wizard prompts you for an encryption key and other information required to access and manage the host and its VMs. The wizard generates a set of credentials for the local agent-access information and stores them in a security file. You must transfer this security file to the server on which an SCVMM Administrator Console is installed. When the file is transferred, you can use the console to add the host and SCVMM will use these credentials to communicate with the agent on the host. This file is named *SecurityFile.txt* and is located in %SystemRoot%\Program Files\Microsoft System Center SCVMM 2008.

Your systems are ready. You will deploy the agent on ServerCore01 from the Administrator Console in the next chapter.



Quick Check

1. Where can you find the Hyper-V Manager installation files?
2. When you install the administration tools using the command line, which tools will not be installed?
3. Which commands are available in the Failover Clustering Management Console to manage the VM operations?
4. Which are the different virtualization engines that can be managed by SCVMM?
5. Which feature becomes available when you link OpsMgr's capabilities with SCVMM?

Quick Check Answers

1. You can find Hyper-V Manager in three locations:
 - The Hyper-V Update, KB950050, for both x86 and x64 setups
 - From the Remote Server Administration Tools included as a feature in Windows Server 2008 full installation
 - From the downloadable update for Windows Vista with SP1
2. When you are using the command line to install the administration tools, all the tools will be installed except the Internet Information Server tools.
3. The commands available to manage VM operations are startup, shutdown, saved state, and transfer to another host. You cannot create or populate VMs in this console.
4. SCVMM can manage Virtual Server 2005 R2, Windows Server 2008 with Hyper-V, Hyper-V Server 2008, VMware ESX Server and ESXi Server, and VMware ESX or ESXi servers that are part of a VMware Virtual Infrastructure 3 or greater cluster.
5. When you use OpsMgr and SCVMM to manage the environment, Performance and Resource Optimization (PRO) can be used to dynamically manage host resource pools.

Lesson 3: Optimizing Hyper-V Hosts

You are now ready to optimize the performance of your Hyper-V machines. When you optimize Microsoft Windows Server 2008 systems, you need to begin by reviewing the server performance and then make appropriate modifications. When you use proper installation and creation procedures, your Hyper-V servers should just work. Hyper-V is a very solid and stable service and is among the most stable services available in Windows Server 2008.

However, you'll find that despite this stability, things can still go wrong, whether they are related to system error or human error. And when things do go wrong, you need to be ready to identify the issues quickly and take appropriate steps to correct the situation. The best way to do this is to perform proactive performance management. When you do so, you are forewarned when untoward events might occur. This is the crux of this lesson.

After this lesson, you will be able to:

- Monitor performance in Window Server 2008.
- Work with key Hyper-V Performance Monitor Counters.
- Use the Reliability and Performance monitor.

Each will help you ensure that your Hyper-V systems run at their optimum.

Estimated lesson time: 45 minutes

Managing Windows Server 2008 System Resources

Windows Server includes several tools that help identify potential issues with system resources. When systems are not configured properly and are not assigned appropriate resources such as CPU, RAM, or disk space, systems monitoring will help you identify where bottlenecks occur. When you identify these bottlenecks, you then assign additional resources to the system. If the system is physical, this most often means shutting down the system, installing new resources (for example, additional memory chips), and then restarting the system. If the system is virtual, depending on the component you want to change, you might be able to allocate new resources while the virtual machine is still running. If not, shut it down, allocate new resources (for example, an additional CPU and additional RAM), and then restart it. After the system is restarted, monitor its performance again to identify whether the new resources solved the problem.

The tools you can rely on to identify performance bottlenecks in Windows Server 2008 include:

- Task Manager, which displays current system resource usage.
- Event Viewer, which logs specific events, including performance-related events.

- Reliability Monitor, which tracks changes brought to the system, enabling you to identify whether a change could be the cause of a new bottleneck.
- Performance Monitor, which collects data in either real time or at specific intervals to identify potential issues.

You can use other tools as well, such as Microsoft System Center Operations Manager, to monitor the state of a system continuously and automatically correct well-known issues. Operations Manager relies on custom management packs to monitor specific applications and is designed to integrate with SCVMM in support of host server optimization.

Using Task Manager

The simplest of all tools to use is Task Manager. This tool provides real-time system status information and covers several key aspects of a system's performance, including:

- Running applications
- Running processes
- Running services
- Performance, including CPU and memory usage
- Networking, including network interface card (NIC) utilization
- Currently logged-on users

Task Manager is accessed in a variety of ways, the most common of which is to right-click the taskbar and select Task Manager. Another common method is to use the Ctrl+Alt+Delete key combination and click Task Manager when the menu choices appear. For example, that is how you would access Task Manager on Server Core, which does not include a taskbar. You can also type **Taskmgr.exe** at a command prompt.

When you access information regarding system performance, the Performance tab is the most useful tab (see Figure 3-24). This tab displays complete information about your system's key resource usage. It details physical and kernel memory usage. This tab also includes a button that gives you access to Resource Monitor. Clicking this button launches Resource Monitor while keeping Task Manager open.

Resource Monitor is a *super* Task Manager because it brings together the CPU, disk, memory, and network usage graphs in a single view (see Figure 3-25). In addition, Resource Monitor includes expandable components for each resource, displaying details of each component so that you can identify which processes might be the culprits if issues are evident. These two tools are ideal for on-the-spot verifications of resource usage. You should rely on them if you need to identify immediately whether something is wrong with a server.

For example, if the system does not have enough memory, you will immediately see that memory usage is constantly high. In this case, Windows will be forced to use on-disk virtual memory and will need to swap or page memory contents constantly between physical and virtual memory. Constant paging is a typical issue that servers with insufficient physical memory face and is often indicated by slow system behavior. One good indicator of insufficient memory is slow Server Manager operation.

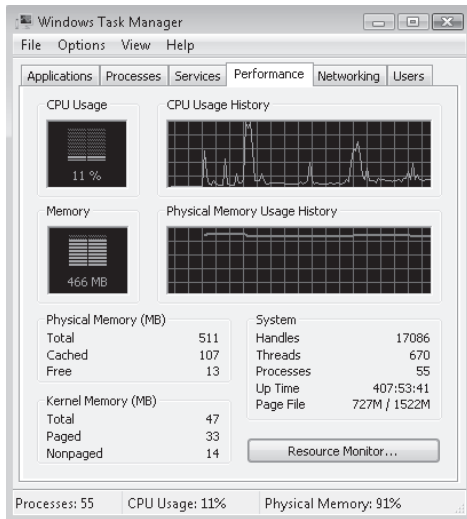


FIGURE 3-24 Viewing real-time performance information in Task Manager

MORE INFO RESOURCE MONITOR

For more information on Resource Monitor, see Scenario 1 in “Windows Server 2008 Performance and Reliability Monitoring Step-by-Step Guide” at <http://technet2.microsoft.com/windowsserver2008/en/library/7e17a3be-f24e-4fdd-9e38-a88e2c8fb4d81033.mspx?mfr=true>.

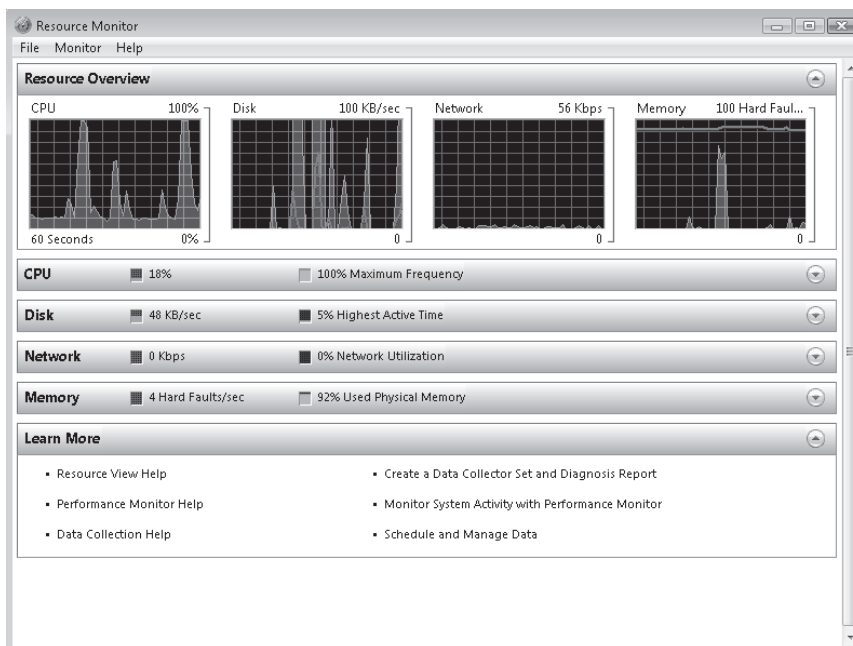


FIGURE 3-25 Viewing real-time performance information in Resource Monitor



EXAM TIP MONITORING HYPER-V PERFORMANCE

Note that the Task Manager and the Resource Monitor live in the parent partition of Hyper-V and therefore do not provide accurate information on the processor and memory usage of child partitions or virtual machines. They are useful for a quick view of machine resource status, but should not be used to gauge the ongoing performance of a host server. To obtain accurate information on Hyper-V performance, you must use the Performance and Reliability Monitor, which is detailed further in this lesson. Remember this when you take the exam.

Working with Event Viewer

Another excellent indicator of system health is Windows Event Log. Windows maintains several event logs to collect information about each of the services running on a server. By default, these include the Application, Security, Setup, System, and Forwarded Events logs, all located in the Windows Logs folder. However, on a Hyper-V server, you also have an additional log that is specifically related to Hyper-V operation. This log is located in a special Server Roles node under the Event Viewer and is called Hyper-V. It contains all Hyper-V-specific information.

However, one of the best features of Event Log is related to Server Manager. Because Server Manager acts as the central management location for each of the roles included in Windows Server 2008, it provides custom log views that percolate all the events related to a specific server role. For example, if you click the Hyper-V Manager role, Server Manager provides you with a log view that includes, among other things, a summary view of key events related to this service (see Figure 3-26).

Event Log lists three types of events: Information, Warning, and Errors. By default, the summary view displayed under the server role lists Errors with a high priority, Warnings with a medium priority, and Information messages with the lowest priority. Therefore, Errors always appear at the top of the summary, alerting you immediately if there is an issue with your system. To drill down and see the event details, either double-click the event itself or move to the Event Viewer section under the Diagnostics node of the Tree pane in Server Manager.

Events provide much more information in Windows Server 2008 and Windows Vista than ever before. In previous versions of Windows, events were arcane items that provided very little information about an issue. Today, you get a full explanation of an event in Event Viewer, and you can link to an online database maintained by Microsoft for each event. You can look up an event in this database by clicking the Event Log Online Help link in the event's Properties dialog box. You will be prompted to send information about the event to Microsoft. Click Yes if you want information specifically about this event.

This database does not provide information about every event in Windows, but it covers the most frequently viewed events. You can also use third-party event log databases to view information about events.

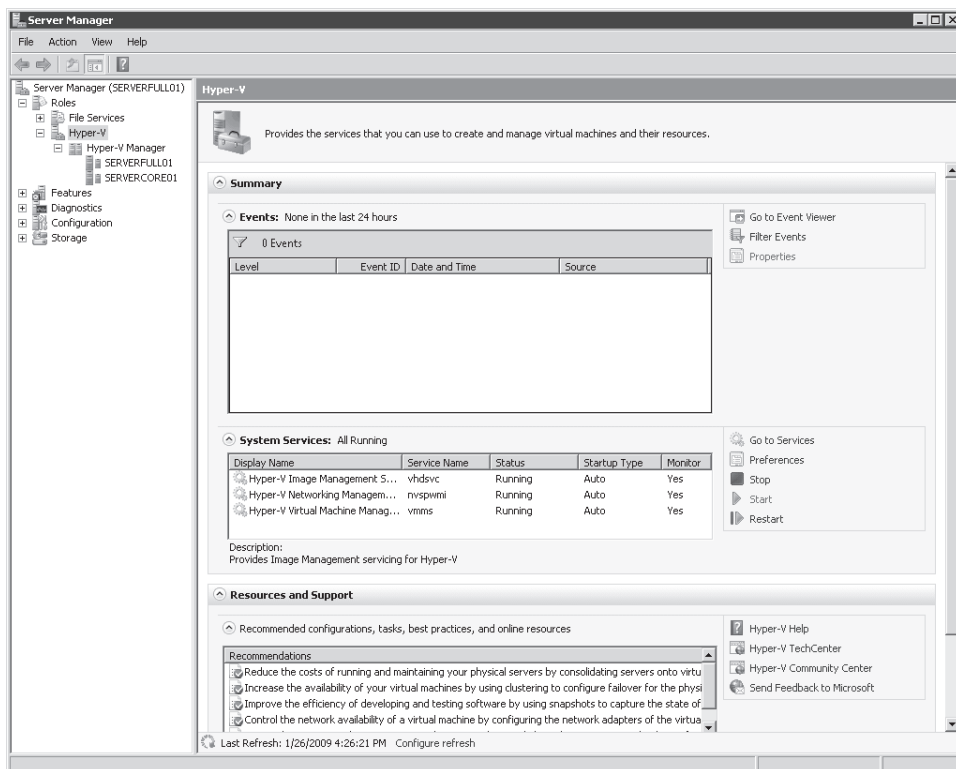


FIGURE 3-26 Viewing summary events for Hyper-V in Server Manager

MORE INFO WINDOWS EVENT IDs

To access a free database of Windows event IDs, go to <http://kb.prismmicrosys.com/index.asp>.

The more information you know about Windows events, the easier it is to deal with the issue. You can rely on the Microsoft online event database and free third-party event databases and supplement this information with online searches through tools such as Windows Live Search to locate information about an issue. Searching on the event ID will return the most results.

MORE INFO NEW FEATURES OF THE EVENT LOG

For more information on working with Event Log, download "Tracking Change" in Windows Vista at <http://www.reso-net.com/download.asp?Fichier=A195>. This multi-page article details the new features of Event Log and how it can be integrated with Task Manager to automate actions based on specific events as well as forward key events to a central collection system.

Working with Windows Reliability Monitor

Another useful tool to identify potential issues on a system is Reliability Monitor. This tool, located under the Diagnostic, then Reliability and Performance, then Monitoring Tools node in Server Manager, is designed to track changes that are made to a system. Each time a change is performed on the system, it is logged in Reliability Monitor (see Figure 3-27). Tracked changes include system changes, software installs or uninstalls, application failures, hardware failures, and Windows failures.

If an issue arises, one of the first places you should check is Reliability Monitor because it tracks every change to your system and reveals what might have happened to make your system unresponsive. For example, if the change is a new driver for a device, it might be a good idea to roll back the device installation and see whether the system becomes more responsive. Verify Reliability Monitor whenever an issue affecting performance arises on a server.

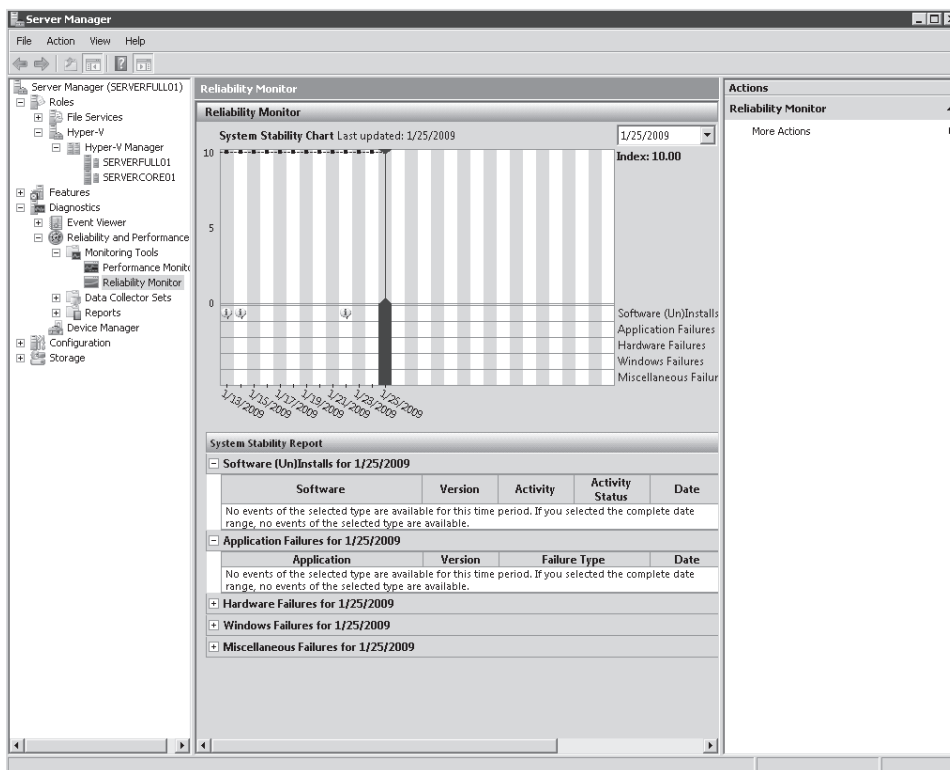


FIGURE 3-27 Viewing system changes in Reliability Monitor



EXAM TIP MONITORING RESOURCES

Work with Task Manager, Event Viewer, and Reliability Monitor. All are an important part of the exam.

Working with Windows Performance Monitor

Sometimes problems and issues are not immediately recognizable and require further research to identify them. In this case, you need to rely on Performance Monitor. This tool, located under the Diagnostic, then Reliability and Performance, then Monitoring Tools node in Server Manager, is designed to track performance data on a system. You use Performance Monitor to track particular system components either in real time or on a scheduled basis.

If you are familiar with previous versions of Windows Server, you'll quickly note that Windows Server 2008 Performance Monitor brings together several tools you might be familiar with: Performance Logs and Alerts, Server Performance Advisor, and System Monitor. If you are new to Windows Server with the 2008 release, you'll quickly find that when it comes to performance management and analysis, Performance Monitor is the tool to use. Using Performance Monitor, you create interactive collections of system counters or create reusable data collector sets. Performance Monitor is part of Windows Reliability and Performance Monitor (WRPM). Table 3-11 outlines each of the tools in WRPM that supports performance monitoring and the access rights required to work with them.

TABLE 3-11 WRPM Tools and Access Rights

TOOL	DESCRIPTION	REQUIRED MEMBERSHIP
Monitoring Tools, Performance Monitor	Use to view performance data in real time or from log files. The performance data can be viewed in a graph, histogram, or report.	Local Performance Log Users group
Monitoring Tools, Reliability Monitor	Use to view the system stability and the events that affect reliability.	Local Administrators group
Data collector sets	Groups data collectors into reusable elements that can be used to review or log performance. Contains three types of data collectors: performance counts, event trace data, and system configuration information.	Local Performance Log Users group with the Log on as a batch user right
Reports	Includes preconfigured performance and diagnosis reports. Can also be used to generate reports from data collected using any data collector set.	Local Performance Log Users group with the Log on as a batch job user right

Windows Server 2008 includes a new built-in group called Performance Log Users, which allows server administrators who are not members of the local Administrators group to perform tasks related to performance monitoring and logging. For this group to be able to initiate data logging or modify data collector sets, it must have the Log On As A Batch Job user right. Note that this user right is assigned to this group by default.

In addition, Windows Server 2008 will create custom Data Collector Set templates when a role is installed. These templates are located under the System node of the Data Collector Sets node of WRPM. For example, with the Hyper-V role, three collector sets are created:

- The LAN Diagnostics set collects data from network interface cards, registry keys, and other system hardware to identify issues related to network traffic on the local host.
- The System Diagnostics set collects data from local hardware resources to generate data that helps streamline system performance on the local host.
- The System Performance set focuses on the status of hardware resources and system response times and processes on the local host.

You can also create your own personalized data set. Hyper-V includes a wide variety of counters for this very purpose. Table 3-12 outlines the counter set name and the number of counters in each set. Hyper-V includes 24 counter sets.

TABLE 3-12 Hyper-V Performance Counter Sets

COUNTER SET CATEGORY	NUMBER OF COUNTERS	DESCRIPTION
Hyper-V Hypervisor	5	Information on the hypervisor.
Hyper-V Hypervisor Logical Processors	18	Information on logical processors.
Hyper-V Hypervisor Partition	7	Information on virtual machines.
Hyper-V Hypervisor Root Partition	7	Information on virtual machines.
Hyper-V Hypervisor Root Virtual Processor	69	Information on virtual processors.
Hyper-V Hypervisor Virtual Processor	69	Information on virtual processors.
Hyper-V Legacy Network Adapter	6	Performance counters for a virtual machine's Ethernet controller.
Hyper-V Task Manager Detail	72	The summary statistics for the Virtual Machine Management Service's Task Manager.
Hyper-V Virtual IDE Controller	4	Performance counters for a virtual machine's IDE Controller.
Hyper-V Virtual Machine Bus	3	The statistics for the virtual machine bus.

COUNTER SET CATEGORY	NUMBER OF COUNTERS	DESCRIPTION
Hyper-V Virtual Machine Health Summary	2	The health summary statistics for the Virtual Machine Management Service.
Hyper-V Virtual Machine Summary	18	The summary statistics for the Virtual Machine Management Service.
Hyper-V Virtual Network Adapter	12	The statistics for the Hyper-V network adapter.
Hyper-V Virtual Storage Device	6	The total number of packets per second traversing the network adapter.
Hyper-V Virtual Switch	18	The statistics for the Hyper-V switch.
Hyper-V Virtual Switch Port	12	The statistics for the Hyper-V switch port.
Hyper-V VM IP APIC	1	Assertions are the number of interrupt assertions the I/O Apic device sent to the Virtual Machine.
Hyper-V VM Remoting	2	Performance counters for a virtual machine's remoting system.
Hyper-V VM Save, Snapshot, and Restore	6	Performance counters for a virtual machine's save and snapshot systems.
Hyper-V VM VID Driver	39	Performance counters for the virtualization infrastructure driver (VID) root level.
Hyper-V VM VID Message Queue	8	Performance counters for a VID message queue object.
Hyper-V VM VID NUMA Node	3	Performance counters for a non-uniform access (NUMA) node.
Hyper-V VM VID Partition	51	Performance counters for a VID partition object.
Hyper-V VM Worker Process Memory Management	12	Performance counters for a worker process memory manager.

To add counters to Performance Monitor, simply click the plus sign (+) in the toolbar at the top of the details pane. This displays the Add Counters dialog box (see Figure 3-28). Scroll through the counters to identify which ones you need. In some cases, you will need subcounters under a specific counter set; in other cases, you need the entire subset of counters. When you need a subcounter, click the down arrow beside the heading, locate the subcounter, and click Add. When you need the entire counter set, click the counter set and then click Add. This adds the counter set with a star heading below it, indicating that all subcounters have been added.

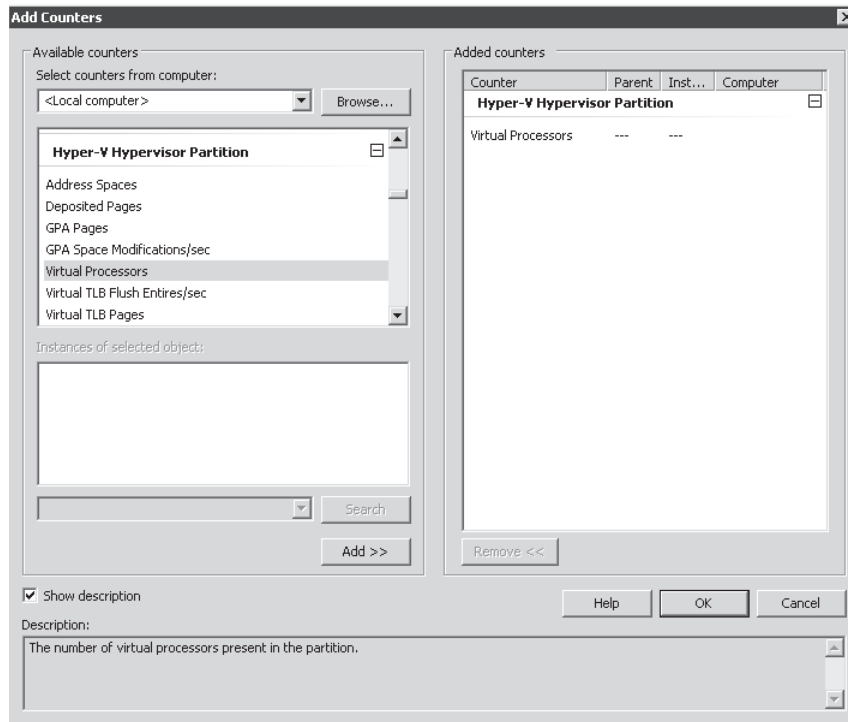


FIGURE 3-28 Adding Hyper-V counters to Performance Monitor

Working with the Windows Server 2008 Interface

When you use the classic interface in Windows Server 2008, you access subcounters by clicking plus signs. When you use the Desktop Experience feature in Windows Server 2008 (which simulates the Windows Vista interface), you access subcounters by clicking down arrows.

To obtain information about a counter, click Show Description. Then, when you click any counter or subcounter, a short description will appear at the bottom of the dialog box.

As soon as you are finished adding counters and you click OK, Performance Monitor starts tracking them in real time. Each counter you added will be assigned a line of a specific color. To remove a counter, click the counter and then click the Delete button (X) on the toolbar at the top of the details pane.

You can start and stop Performance Monitor much like a media player, using the same type of buttons. When Performance Monitor runs, it automatically overwrites data as it collects more; therefore, it is more practical for real-time monitoring.

If you want to capture the counters you added into a custom data set, right-click Performance Monitor, select New, and then choose New Data Collector Set. Follow the prompts to save your counter selections so that you can reuse them later.



EXAM TIP SERVER PERFORMANCE ADVISOR

Work with Performance Monitor because it is an important part of the exam. Also, note that there is no Server Performance Advisor (SPA) in Windows Server 2008. This Windows Server 2003 tool has been rolled into Windows Reliability and Performance Monitor. Don't get caught on questions regarding SPA on the exam.

Creating Baselines for Hyper-V

For long-term system monitoring, you must create data collector sets. These sets run automated collections at scheduled times. When you first install a system, it is a good idea to create a performance baseline for that system. As load increases on the system, you can compare the current load with the baseline and see what has changed. This helps you identify whether additional resources are required for your systems to provide optimal performance. For example, when working with Hyper-V servers, it is a good idea to log performance at peak and nonpeak times. Peak times are when users access the virtual machines you are running on the hosts; non-peak times are when VMs are at rest. To create a performance baseline, you need to take samples of counter values for 30 to 45 minutes for at least a week during peak, low, and normal operations.

However, note that it is difficult to get an accurate view of some of the resources in a Hyper-V host because VM resource usage happens in various places. For example, when you look at CPU uses, note the following:

- VMs consume resources within the child partition. You can view individual VM CPU resource usage within Hyper-V Manager. You can also look at the % Guest Run Time counter under the Hyper-V Hypervisor Virtual Processor section of Performance Monitor.
- CPU resources are also consumed when the hypervisor is managing intercepts, connecting contexts, and performing other VM communication tasks. You can track this through the % Hypervisor Run Time counter under the Hyper-V Hypervisor Virtual Processor section.
- Look at the worker process in the parent partition. Each VM is assigned a worker process. These processes manage operations such as starting or stopping VMs or even taking snapshots of the VM. These processes also manage emulated devices.
- You can allocate more processors to VMs than are actually available in the physical computer because the parent partition virtualizes logical processors. In this case, it is extremely difficult to measure processor utilization because processor access is controlled directly by the parent partition.

Keep the concept of different locations in mind when you try to track resource usage in Hyper-V. Also remember the following:

- Disk Latency is an important potential bottleneck in Hyper-V. Many of the Hyper-V operations are related to disk access because each VM is nothing but a set of files on a disk and requires disk read-write operations to operate. Use the Logical Disk, Average Disk second/Read, and Average second/Write counters on all disks to measure this performance. A problem exists if average response times are greater than 15 milliseconds (ms). Ideally, your seek times will be between 1 and 15 ms. If your seek times are 26 ms or greater, your system has a critical problem.
- Guest operating systems have the same counters. You can measure their disk seek times by running the same performance counters in Windows VMs.
- Memory is a critical resource in host computers. Use the Memory, Available Megabytes counters on the parent partition to view how the host is using memory. If more than 50 percent of memory is available, your system is healthy. If 25 percent or less is available, monitor memory closely. If 10 percent or less is available, your system will start having poor performance. If memory levels fall significantly below 10 percent, your systems have a problem and require more memory or fewer workloads.
- Use Memory, Pages/second counters to determine the rate at which pages of memory are read by the system. This measures memory swapping from the hard disk to RAM. High levels will negatively impact your system operation. If the value is less than 500, the system is healthy. If it is between 500 and 1000, monitor the system. If it is greater than 1000, your system requires more memory or fewer workloads.
- You can use the same counters within VMs running Windows operating systems.
- Next, focus on networking performance since VMs must rely on the parent partition and the VMBus to access networks. You can perform a simple ping test against each of your VMs to view its network performance. If the response times are greater than 1 ms, you may need to resolve an issue. You can also use the PATHPING.exe command to identify whether packets are being lost when transferred from VMs to other systems. You can use network file transfers to test network performance. Copying a 100-MB file from one system to another is a good test of network performance. On a 100-Mbit network, this transfer should take between 10 to 20 seconds; it should take about 3 seconds on a 1-Gbit network.
- You can use the Network Interfaces, Bytes Total/second counters on each adapter in the parent partition. If utilization is less than 40 percent, the system is healthy. If it is between 41 and 64 percent, monitor the system. If it is between 65 and 100 percent, an issue is indicated and more adapters may be required.
- Use the Network Interface, Output Queue Length counters to identify the number of threads waiting for transfer on the adapter. 0 is a healthy value, 1 to 2 requires monitoring, and greater than 2 is an issue.
- You can use the same counters within the Windows VMs.

- Processors are a key resource in host systems and must be monitored closely. Use the Hyper-V Hypervisor Logical Processor (_Total), Percent Total Run Time counter to measure processor usage by host and guest operating systems. If the values are less than 60 percent, the system is healthy. Monitor the system if the values are between 60 and 89 percent. Add resources or reduce workloads if the value is over 90 percent. You can also rely on the same values with the Hyper-V Hypervisor Virtual Processor settings to differentiate between logical and virtual processor utilization. If the Logical Processor is high and a Virtual Processor is low, your VM may be using more processors than are physically available. You can then use the Hyper-V Hypervisor Virtual Processor, Percent Guest Run Time to identify which virtual processors are causing the bottleneck. When the reverse occurs and Logical Processor is low while Virtual Processor is high, it means that you have available logical processors that can be allocated to the VM. When both values are high, you must add resources to the physical host or reduce the number of workloads.

MORE INFO EVALUATING PERFORMANCE IN HYPER-V

For more information on evaluating performance in Hyper-V, look up “Measuring Performance on Hyper-V” at <http://technet.microsoft.com/en-us/library/cc768535.aspx>.

The general steps for creating a baseline include:

1. Identify resources to track.
2. Capture data at specific times.
3. Store the captured data for long-term access.

IMPORTANT PERFORMANCE MONITORING AFFECTS PERFORMANCE

Taking performance snapshots also affects system performance. The object with the worst impact on performance is the logical disk object, especially if logical disk counters are enabled. However, because this affects snapshots at any time, even with major loads on the server, the baseline is still valid.

When you are ready to view the results of your collection, you can rely on the Reports section of the Windows Reliability and Performance node. Right-click the collector set for which you want to view the report (either User Defined or System) and select Latest Report. This will generate the report if it isn't already available and provide extensive information on the status of your DC.

MORE INFO PERFORMANCE MONITOR SCENARIOS

For more information on Performance Monitor, see the scenarios in the Windows Server 2008 Performance and Reliability Monitoring Step-by-Step Guide at <http://technet2.microsoft.com/windowsserver2008/en/library/7e17a3be-f24e-4fdd-9e38-a88e2c8fb4d81033.mspx?mfr=true>.

Optimizing Hyper-V Operations

After you have collected information on Hyper-V server performance, you can move on to optimizing the systems. In terms of guest operating systems, Hyper-V provides the possibility of configuring a network heartbeat service called the VM heartbeat. The VM heartbeat service is available when enlightened guests are running Hyper-V Integration Services. This service is enabled by default when you install or upgrade the Integration Services on each guest VM (see Figure 3-29). Note that the heartbeat service is not available for legacy VMs. Hyper-V relies on this service to ensure that the VM is operating properly. Make sure this service is enabled on each enlightened VM.

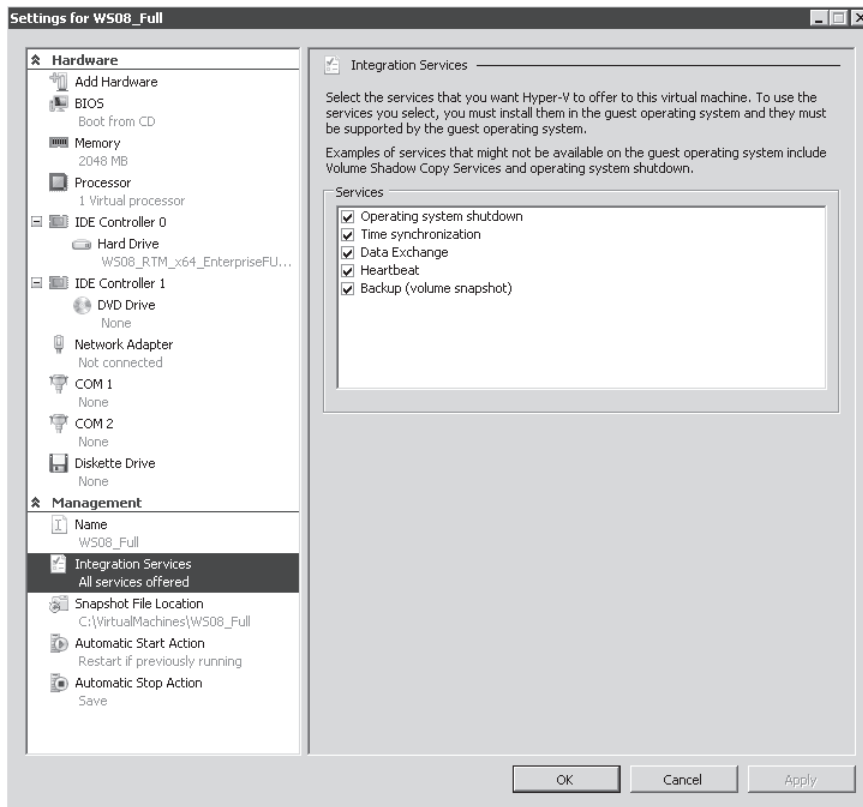


FIGURE 3-29 Viewing the VM heartbeat service in Integration Services

Other optimization goals should include the following:

- **Allocate 110 to 125 percent of resources to VMs** If a system recommendation for a physical installation of a server application recommends using 4 GB of RAM, allocate 5 GB of RAM to the installation of the same application within a VM. Configuring the VM with additional resources ensures that its performance will be on par and possibly better than a corresponding hardware installation. Do the same for all hardware resources.

- **Minimize the roles in the parent partition** Keep the parent partition as lean as possible. This partition should only run the Hyper-V role and possibly the Failover Clustering feature. This will ensure that most resources are available to VMs.
- **Run enlightened VMs as much as possible** Enlightened VMs with the Integration Services provide the best performance for guest operating systems running on Hyper-V.
- **Run Hyper-V on Server Core** Running on Server Core minimizes the resources used by the parent partition and improves VM operations.
- **Optimize disk resources in VMs** Consider using pass-through disks in VMs. A pass-through disk is a physical disk partition that is attached to the VM. Pass-through disks provide better performance because there is no conversion between the virtual disk and the physical disk. Also consider using SCSI connectors for these disks. Although there is little difference between the IDE and the SCSI connector when working with a virtual hard drive, SCSI provides better performance when working with pass-through disks. Note that the SCSI connector is only available to enlightened guests.
- **Configure your host server with sufficient** Memory is one of the most important resources on host servers. Ensuring that you have sufficient memory on your hosts allows them to support more VMs. Also remember that the parent partition and each VM has memory overhead when you calculate the amount of RAM required for your hosts.
- **Run VMs with x64 operating systems** x64 operating systems provide the best performance because they break the memory barriers inherent in x86 systems.
- **Use Network Adapters instead of Legacy Network Adapters** Network Adapters run through the VMBus and provide the best performance to VMs.
- **Configure 1-to-1 mappings for logical to virtual processors** Even though Hyper-V supports up to eight virtual processors per logical processor, configure only one virtual processor per logical processor for ultimate performance.
- **Use modern operating systems in your guest VMs** Modern operating systems such as SUSE Linux 10 and Windows Server 2008 are optimized for operation within virtual machines and will perform better than older operating systems.
- **Avoid using Hyper-V Snapshots in VMs** Using snapshots transforms virtual disk drives into differencing disks that provide poorer performance than other virtual hard drive types. More on this topic is covered in Chapter 4, "Creating Virtual Machines."

MORE INFO PERFORMANCE OPTIMIZATION ON HYPER-V

For more information on tuning Hyper-V, look up the "Performance Tuning for Virtualization Servers" section of the Performance Tuning Guidelines for Windows Server 2008 document at <http://go.microsoft.com/fwlink/?LinkId=121171>. You can also look up the "Recommendations for Configuring and Optimizing Hyper-V" section of Performance and Capacity Requirements for Hyper-V at <http://technet.microsoft.com/en-us/library/dd277865.aspx#section2>.

MORE INFO USING A VISTA GADGET TO MONITOR HYPER-V

You can also monitor Hyper-V performance through a custom Vista Gadget. Find it at <http://mindre.net/post/Hyper-V-Monitor-Gadget-for-Windows-Sidebar.aspx>.

Finally, you can also rely on SCVMM to improve both Hyper-V and VM performance. SCVMM can help in a number of ways:

- **Identify virtualization candidates** SCVMM can scan physical computer systems to identify potential virtualization candidates.
- **Allocate VMs** SCVMM can compute chargeback costs for VMs and apply them to specific cost centers.
- **VM usage** SCVMM can provide comprehensive reports on VM resource utilization.
- **Host usage** SCVMM can provide comprehensive reports on host server utilization.
- **Host usage patterns** SCVMM can also show the growth patterns for host server resource utilization.

Using SCVMM to centrally scan and manage resource utilization is a good way to optimize your Hyper-V environments. This will be covered in more detail as you begin to work with virtual machines in the remaining chapters of this book.

PRACTICE AD DS Performance Analysis

In this practice, you will use WRPM to view the performance of your host servers. This practice consists of one exercise. You will create a custom collector set. After the collector set is created, you will run it and view the diagnostics report. These exercises rely on ServerFull01.

EXERCISE 1 Create a Data Collector Set

A data collector set is the core building block of performance monitoring and reporting in WRPM. You can create a combination of data collectors and save them as a single data collector set. This is the task you will perform in this exercise.

1. Log on to ServerFull01 with the domain administrator account. You only need to be a member of the Performance Log Users group with the Log On As A Batch Job user right, but for the purpose of this exercise, you will use the domain administrator account.
2. In Server Manager, expand Diagnostics, expand Reliability and Performance, expand Monitoring Tools, and then click Performance Monitor.
3. Begin by adding counters in the Performance Monitor. Your goal is to monitor the parent partition performance. To add a counter, click the plus sign in Performance Monitor, scroll down to locate the required counter set, click the plus sign to expand it, locate the appropriate counter, and click Add. You can also select Show Description to view the description of each counter as you add it. Add the following counters (see Figure 3-30):
 - Hyper-V Hypervisor Logical Processor (_Total), Percent Total Run Time
 - Hyper-V Hypervisor Virtual Processor (_Total), Percent Total Run Time

- Hyper-V Hypervisor Virtual Processor (_Total), Percent Guest Run Time
- Logical Disk (_Total), Average Disk second/Read for all disks
- Logical Disk (_Total), Average second/Write for all disks
- Memory, Available Megabytes
- Memory, Pages/second
- Network Interfaces, Bytes Total/second for all interfaces
- Network Interface, Output Queue Length for all interfaces

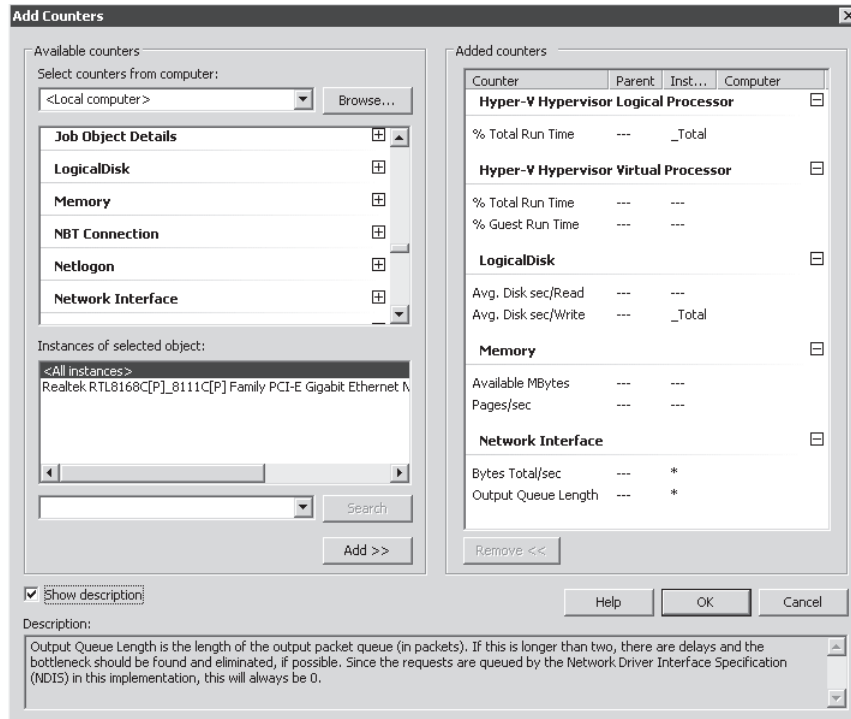


FIGURE 3-30 Adding performance counters

4. Click OK. Performance Monitor will begin monitoring the local system. Click the plus sign again and then click Browse to type in **ServerCore01**. Click Check Names, click OK, and then add the same counters as in step 3. The result will display Performance Monitor monitoring both host servers.
5. Save these counters into a data collector set. Right-click Performance Monitor in the Tree pane, select New, and then select Data Collector Set. On the Create Data Collector Set page, type **Custom Hyper-V Collector Set**, make sure Create From A Template (Recommended) is selected, and click Next.
6. By default, the wizard selects %systemdrive%\PerfLogs\Admin as the root directory. You can use the Browse button to change this if you need to. Click Next.

7. On the Create The Data Collector Set page, in the Run As field, leave the defaults and click Finish.

When you create collector sets for long-term use, use a special account that is both a member of the Performance Log Users group and has the Log On As A Batch Job user right to run your collector sets. Note that the Performance Log Users group has this right assigned to it by default.

When you finish the New Collector Set Wizard, you are given three options:

- **Open Properties Data For This Data Collector Set** Select this option to view the properties of the data collector set or to make additional modifications (in this case, this option is not available).
- **Start This Data Collector Set Now** Select this option to run the data collector set immediately.
- **Save And Close** Select this option to save the data collector set without starting the collection.

Your custom data collector set has been created. Notice that it is located in the Data Collector Sets, User Defined section of the Tree pane and it is stopped. To schedule the Start condition for your data collector set, use the following procedure:

1. Right-click Custom Hyper-V Collector Set and choose Properties.
2. Click the Schedule tab and then click Add to create a start date, time, or day schedule.
3. In the Folder Action dialog box, make sure that today's date is the beginning date, select the Expiration Date check box, and set it as one week from today. Also, make sure that the report time is set to the current time. Click OK.

You must set the start date of the schedule to Now for the collection set to work.

If not, you will not be able to generate reports in later steps.

Note that you can create quite a modular schedule in this dialog box. Also note that selecting an expiration date will not stop data collection in progress on that date. It will only prevent new instances of data collection from starting after the expiration date. You must use the Stop Condition tab to configure how data collection is stopped.

4. Click the Stop Condition tab, select the Overall Duration check box, make sure it lists 5 minutes, and select the Stop When All Data Collectors Have Finished check box. Click OK.

You select the Stop When All Data Collectors Have Finished check box to enable all data collectors to finish recording the most recent values before the data collector set is stopped if you have also configured an overall duration.

You can also set limits on your collection. However, note that when an overall duration is configured, it will override any limits you set. If you do want to set limits, make sure the Overall Duration check box is cleared and define the following limits:

- **Select When A Limit Is Reached, Restart The Data Collector Set** to segment data collections into separate logs.

- To configure a time period for data collection to write to a single log file, select the Duration check box and set its value.
- To restart the data collector set or to stop collecting data when the log file reaches a specific limit, select the Maximum Size check box and set its value.

Collector sets will generate a large amount of data if you allow them to run unmonitored. To configure data management for a data collector set, use the following procedure:

1. Right-click Custom Hyper-V Data Collector Set and choose Data Manager.
2. On the Data Manager tab, you can accept the default values or change them according to your data retention policy. Keep the defaults.
 - Select the Minimum Free Disk or Maximum Folders check boxes to delete previous data according to the resource policy you choose from the drop-down list (Delete Largest or Delete Oldest).
 - Select the Apply Policy Before The Data Collector Set Starts check box to delete previous data sets according to your selections before the data collector set creates its next log file.
 - Select the Maximum Root Path Size check box to delete previous data according to your selections when the root log folder size limit is reached.
3. On the Actions tab, you can set specific data management actions for this collector set. Note that three policies already exist. Click 1 Day(s) policy and then click Edit.

Folder actions enable you to choose how data is archived before it is permanently deleted. You can decide to disable the Data Manager limits in favor of managing all data according to these folder action rules. For example, you could copy all collection sets to a central file share before deleting them on the local server.
4. Click OK and then click OK again.

Your collector set is ready to run. Wait until the scheduled time occurs for the report to run. However, if you want to view an immediate report, proceed as follows:

1. Right-click the Custom Hyper-V Collector Set and choose Start. This automatically moves you to the Reports, User Defined section of WRPM and highlight the Custom Hyper-V Collector Set folder. You will see that the collection set is generating a report.
2. Click the report name. You will see that the report is currently running (see Figure 3-31).
3. Return to the Custom Hyper-V Collector Set to right-click it and choose Stop.
4. The report that was generated by your collector set will be displayed in the Data Collector Sets, User Defined, Custom Hyper-V Collector Set folder.

This procedure lets you capture a quick view of the status of your systems. Use these collector sets to perform ongoing monitoring of your Hyper-V systems performance.

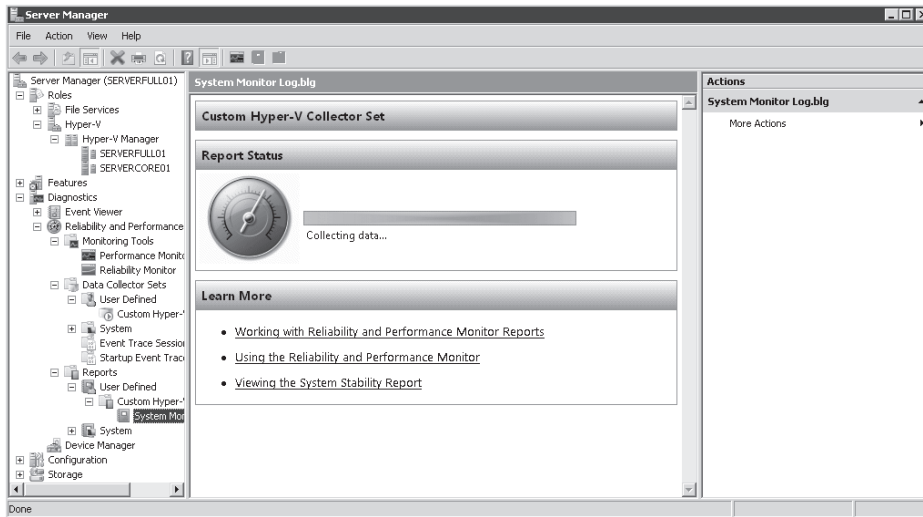


FIGURE 3-31 Running a data collector set



Quick Check

1. You want to view potential error messages about the Hyper-V service. Where can you find this information?
2. How do you generate a custom data collector set for Hyper-V?

Quick Check Answers

1. View potential error messages about the Hyper-V service in Event Log. You can view this information in two places. The first is by clicking the server role name in the Tree pane of Server Manager. This will display a summary view of Hyper-V service events if there are any. The second is by going to the Hyper-V log itself, under Event Viewer, Custom Views, Server Roles. This will display all the events related to the Hyper-V service.
2. The easiest way to generate a custom data collector set for Hyper-V is to prepare a collector set in Performance Monitor interactively and then capture this collection into a new data collector set.

Case Scenario: Deploying SCVMM on Physical or Virtual Platforms

In the following case scenario, you will apply what you've learned about SCVMM in this chapter. 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 Contoso Ltd. Your organization runs 100 virtual machines on 10 Hyper-V hosts running Server Core in one single failover cluster. Note that you do not anticipate any growth in terms of machine numbers for the foreseeable future. So far, you have been working with both the Hyper-V Manager and the Failover Clustering Management console to manage both the host servers and the VMs they run. You requested that a Microsoft representative introduce SCVMM to your management staff, and now they have finally been convinced that it would be a good addition to your management tool set.

However, they want to minimize costs as much as possible. Because of this, they have requested that you prepare a proposal for SCVMM deployment. Particularly, they want you to respond to the following questions:

1. Which deployment model should you use for SCVMM?
2. Should SCVMM be deployed on a physical computer? If so, what are some advantages and what are some drawbacks?
3. Should SCVMM be deployed on a virtual computer? If so, what are the advantages and what are some drawbacks?
4. If SCVMM is deployed in a virtual machine, are there any other factors you should take into consideration to improve performance?

Suggested Practices

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

Failover Clustering

- **Practice 1** Even though you do not have the proper shared storage, you should practice the installation of Failover Clustering Services because it exposes you to the process.
- **Practice 2** After the Failover Clustering feature is installed and configured, work through the Failover Clustering console and its options as well as the Tree structure of the service. This will be useful for the exam.

SCVMM Installation

- **Practice 1** Take the time to install the SCVMM components as outlined in the practice in Lesson 2. SCVMM is a very important part of the exam and therefore requires extensive examination.
- **Practice 2** Take the time to browse through the SCVMM Administrator console. It will be used in future chapters, but you can never be too familiar with this important aspect of the exam.

Performance Monitoring

- **Practice 1** Work with the Hyper-V monitoring tools. Use Task Manager, Event Viewer, and the Windows Reliability and Performance Monitor views. Try as many of the various options as possible to become familiar with how they work. Look up the suggested article for Event Log management and apply its principles to your servers.

Chapter Summary

- Microsoft Windows Server 2008 includes Failover Clustering and Network Load Balancing (NLB) to support the concept of fault-tolerant servers. Stateless services are best suited to participate in an NLB farm. Applications suitable for failover clusters include stateful services or services that write data to disk.
- The two types of failover clusters are single-site and multi-site clusters. The Failover Clustering feature combines with Hyper-V to ensure high availability for the virtual machines that run on the host server. But when you use a multi-site cluster, Hyper-V does not include its own replication engine and you have to rely on a third-party replication engine to make the cluster work.
- Hyper-V Manager can be obtained from the Hyper-V update or from the Remote Server Administration Tools as well as from the update for Windows Vista SP1. After the Hyper-V Manager is installed you need to select Connect To Server in the Actions pane to locate which server you want to manage. This console is designed to manage each Hyper-V host one at a time.
- Hyper-V Manager can manage single hosts and virtual machines. Failover Clustering Management can view the Hyper-V hosts by linking them in the resource pools, thereby giving you the ability to manage the VMs contained in the resource pool independently of the individual host servers. System Center Virtual Machine Manager (SCVMM) supports dynamic datacenter operations through the management of both host servers and virtual machines.

- SCVMM uses a single management interface that includes several views. It also includes several components: SCVMM Server, the VMM Service, Microsoft SQL Server, SCVMM Administrator console, Library Server, an Agent, Self-Service Portal, and Windows PowerShell.
- The SCVMM architecture includes three layers: the Managed Computer Layer, the Engine Layer, and the Client Layer. These layers rely on common communication ports such as 80 and 443 and do not require the opening of custom ports in firewalls.
- When performance issues arise, Windows Server 2008 provides a series of tools for analysis and problem correction. These include both real-time and scheduled analysis tools. Real-time tools include Task Manager, Resource Monitor, and Performance Monitor. Scheduled or tracking tools include Event Log, Reliability Monitor, and scheduled data collection sets in Performance Monitor.

Creating Virtual Machines

Now that your host infrastructure is ready, you can move on to begin working with virtual machines. You have already worked with virtual machines to some degree because it is hard to work with host servers without having to deal with virtual machines in some way, shape, or form. Now you will begin to work with the VMs in full force.

Remember the seven-step process outlined in Chapter 1, “Implementing Microsoft Hyper-V.” This process basically outlined how to build and create your virtual infrastructure:

1. You begin by determining your starting point. You performed this task in Chapter 1.
2. You prepare and deploy your host servers. You performed this task in Chapter 2, “Configuring Hyper-V Hosts.”
3. You prepare your management infrastructure. You performed this task in Chapter 3, “Completing Resource Pool Configurations.”
4. You secure the host server infrastructure. You will perform this task in Chapter 8, “Securing Hosts and Virtual Machines.”
5. You then need to put a data protections strategy in place. You will perform this task in Chapter 9, “Protecting Hyper-V Resource Pools.”
6. You can then build your production virtual machines. This task begins in this chapter.
7. Finally, you look to update your management practices to ensure proper separation of tasks between the resource pool and the virtual workloads it runs. This task is ongoing in the remaining chapters.

This chapter and the following two chapters look at virtual machines in depth. This chapter will examine the makeup of a VM and its components. Chapter 5, “Automating Virtual Machine Creation,” will look at VM creation and operation automation and optimization. Chapter 6, “Migrating to Hyper-V,” then looks at migration scenarios. As outlined in Chapter 1, there are three migration scenarios:

- Some organizations are new to virtualization and need to migrate from physical machines.
- Some organizations are already using a virtual infrastructure based on software virtualization products and need to transform both host servers and the virtual machines they run.
- Some organizations are already using other hardware virtualization products and need to transform both host servers and the virtual machines they run.

Of course, some organizations are in a hybrid state, running some production systems as VMs and some as physical servers. These organizations need to determine whether Hyper-V is stable enough to migrate all your production workloads into VMs.

First you need to prepare for virtual machine operation, which is the focus of this chapter.

Exam objectives in this chapter:

- Create or clone a virtual machine.
- Create a virtual disk.
- Manage and optimize the Hyper-V Server.
- Manage virtual machine settings.

Before You Begin

To complete this chapter, you must have:

- Experience with Windows Server 2003 or Windows Server 2008.
- Experience with some form of guest operating system virtualization.
- Access to a setup as described in the Introduction. If not, your experience with Hyper-V will be limited.

Lesson 1: Discovering Virtual Machines

Virtual machines run as applications on top of a hypervisor. As such, they can consume several different type of resources. Understanding these resources and the relationship between the virtual machine and the hypervisor is the focus of this lesson.

After this lesson, you understand:

- Hyper-V child partitions and how they interact with the parent partition.
- Virtual machine components, both basic and advanced.
- Virtual machine configuration settings.
- Integration Services installation.
- Virtual machine states.

Estimated lesson time: 40 minutes

Working with Hyper-V Child Partitions

You've already worked with Hyper-V child or guest partitions as you worked with the host or parent partition. You've seen that creating a child partition or virtual machine is performed through the New Virtual Machine Wizard in Hyper-V Manager. This wizard takes you through the steps required to create the basic components of a virtual machine. But much more is involved when you need to run more sophisticated implementations of both operating systems and applications within a virtual environment. When this occurs, you need to work with the Virtual Machine Settings to modify existing components and add additional components to the VM.

Another aspect of virtual machine creation and operation is the nature of the child partition itself. As you've learned so far, Hyper-V supports both enlightened and legacy guest operating systems. Enlightened guest operating systems perform better on Windows Server Hyper-V because they use the VMBus to communicate through the parent partition with machines outside the host. Legacy machines must use emulated device drivers, which draw additional resources from the host server and affect performance.

Finally, virtual machines running in Windows Hyper-V can run any number of operating systems, but the only ones that can draw upon the highest levels of integration are the newest versions of Windows and special editions of Linux, editions that have been updated to interact with Hyper-V through the Hypercall Adapter. This means that when you are working with Hyper-V, you will be running potentially three different types of VMs:

- Machines running Hyper-V-aware Windows operating systems
- Machines running Hyper-V-aware non-Windows operating systems
- Machines running non-Hyper-V-aware operating systems

The last category includes both Windows and non-Windows operating systems that do not understand the Hyper-V architecture. Remember that these machines do not support Hyper-V's Integration Services and therefore run everything through emulated device drivers (see Figure 4-1).

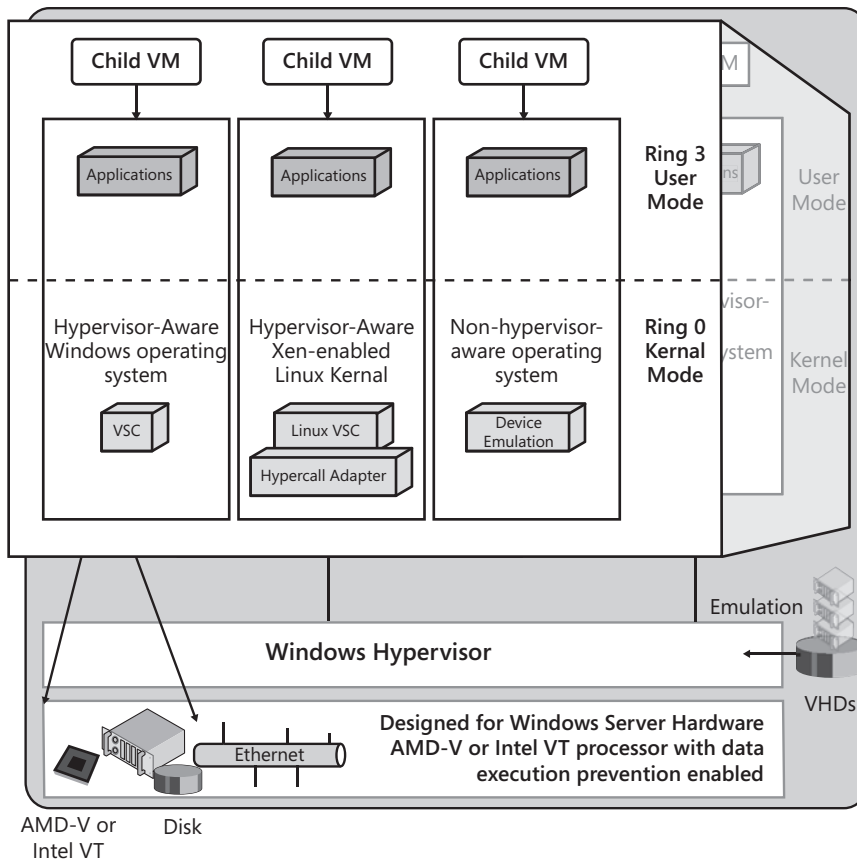


FIGURE 4-1 Child partitions in Hyper-V

Hyper-V Integration Services

While performing the various exercises in the previous chapters, you used and installed Integration Services in the VMs you created. Integration Services are special components that Hyper-V provides to enlightened guest operating systems. These services provide additional integration capabilities to operating systems that have been made aware of the fact they are running within a virtual environment. The Hyper-V Integration Services are made up of two core components: services and drivers. The services are made up of several components, including:

- **Operating System Shutdown** Lets the parent partition send shutdown requests to the child partition, turning off the operating system properly instead of simply turning off the machine.
- **Time Synchronization** Ensures that the time in the child partition is synchronized with the time on the parent partition.

- **Data Exchange** When the parent and child partitions exchange key and value pairs as registry values, they rely on this service to do so. This is mostly used by management tools that control VM operations.
- **Heartbeat** A service used by the parent partition to verify that the child partition is available and can respond to requests. You viewed this service in Lesson 3 of Chapter 3 when you looked at improving the performance of Hyper-V and the guests it runs.
- **Backup (volume snapshot)** Relies on the Volume Shadow Copy Service (VSS) in the parent partition to ensure that any backups of the virtual machine are consistent with the state of the VM when the backup is taken.

These services are enabled by default when they are installed in a guest operating system. However, you can control whether they are available to the guest through the virtual machine's settings (see Figure 4-2).

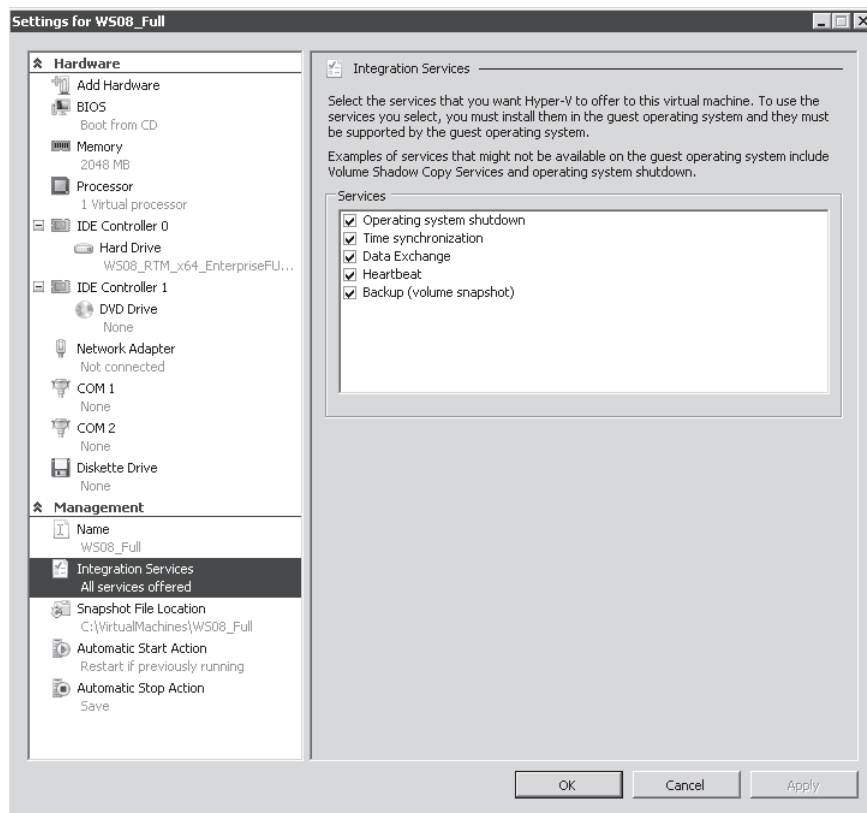


FIGURE 4-2 Working with Integration Services

In terms of drivers, Integration Services can provide several types of enlightenments to guest operating systems, including storage (IDE or SCSI), networking, graphics (video), and input (keyboard and mouse).



EXAM TIP HYPER-V INTEGRATION SERVICES DRIVERS

Note that the Hyper-V enlightenments included as drivers within Integration Services do not include USB devices. Make sure you don't get caught on this in the exam.

Running Enlightened Windows Guests

When a Windows operating system such as Windows Server 2008, Windows Server 2003 with SP2, Windows 2000 Server with SP4, Windows HPC Server 2008, Windows Vista with SP1, or Windows XP with SP2 is running within a Windows Server Hyper-V child partition, it runs core services within the kernel mode of Windows.

The first of these is the Virtualization Service Client (VSC). VSCs are basically synthetic devices that are installed within the child partition. These synthetic devices call upon the host server's hardware resources through communications with the Virtualization Service Provider (VSP) that resides within the parent partition. VSCs and VSPs communicate through the VMBus.

When you first install one of the aforementioned operating systems within a child partition, it behaves as follows:

- If the operating system does not include Hyper-V Integration Services, it relies on emulated hardware drivers just as a non-Hyper-V-aware operating system would.
- If the operating system includes a version of Hyper-V Integration Services, the operating system can begin to consume synthetic devices through VSCs immediately.

In most cases, you'll need to either install or upgrade Hyper-V Integration Services within the child partition to convert the operation of the operating system from a non-Hyper-V-aware operating system to a Hyper-V-aware operating system. For example, the original release of Windows Server 2008 already includes a version of the Hyper-V Integration Services, but because the release to manufacturing (RTM) version of Hyper-V was not available when Windows Server 2008 was released, the version of the Integration Services contained within the code is not up to date. Therefore, you will need to upgrade Integration Services to the RTM version of Hyper-V (see Figure 4-3). Remember that you performed this task in Exercise 4 of Lesson 2 in Chapter 3.

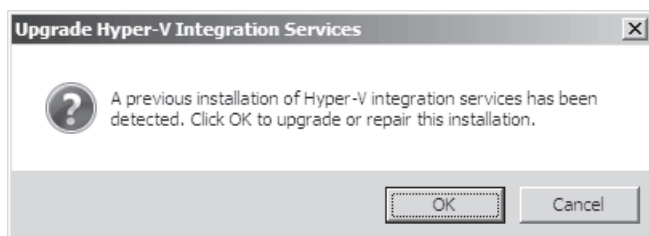


FIGURE 4-3 Upgrading Integration Services

In the case of other enlightened Windows operating systems, you simply need to install Integration Services because they are not present in the system's code. Future Windows

operating systems will include up-to-date Integration Services and will therefore be able to natively run in child partitions on Hyper-V.

The ability to use Integration Services to create VSCs in child partitions comes from enlightenments—updates to the core operating system code, which make the operating system aware that it is running in a virtual machine on top of a hypervisor. This is why Hyper-V–aware Windows operating systems prior to Windows Server 2008 all require a service pack to become Hyper-V–aware. The code in the service pack modifies the operating system so that it can detect that it is running within a VM.



EXAM TIP WINDOWS 2000 SERVER

Note that the drivers included in the Integration Services enlightenments for Windows 2000 Server do not include support for the SCSI storage driver, only for IDE.

Running Enlightened non-Windows Guests

The same kind of process as an enlightened Windows guest can occur with non-Windows operating systems that are Hyper-V–aware. Once again, these operating systems will use VSCs to communicate with VSPs through the VMBus. However, because the operating system is not Windows, these VSCs are third-party VSCs. In fact, these VSCs do not interact with VSPs in exactly the same way as Windows-based VSCs. They must use a Hypercall Adapter to perform the communication because the operating system does not include the Hypercall code. Microsoft has generated the Hypercall Adapter and made its application programming interface (API) freely available through its Open Specifications Promise. This allows third parties and the entire open source community to develop high-quality virtualization solutions that deliver true interoperability between Windows and Linux.

MORE INFO THE MICROSOFT OPEN SPECIFICATION PROMISE

Find out more about the Microsoft Open Specification Promise, go to <http://www.microsoft.com/interop/osp/default.mspx>.

Microsoft also provides Integration Components for Linux, which will provide additional functionality within the guest operating system. These components include:

- Driver support for synthetic devices, including both the network controller and the storage controller, allowing them to interact directly through the VMBus just as Hyper-V–aware Windows operating systems would.
- The Hypercall Adapter, which is an adapter that sits underneath the Xen-enabled Linux kernel and translates all Xen-specific virtualization function calls to Microsoft Hyper-V calls.

The integration of both components results in faster Linux operating system performance when installed in Hyper-V child partitions.

In the first version of Hyper-V, only select versions of Linux can call upon the Linux Integration Components (LIC) to run as enlightened guests—SUSE Linux Enterprise Server 10 with SP2. However, both x86 and x64 versions of this operating system can run as Hyper-V–aware VMs. This is because Microsoft has a tight collaboration program with Novell, the manufacturer of this operating system. Microsoft is also working on Red Hat Enterprise Linux versions of the Integration Services and will release them when they become available.

Also note that the LIC are not included with Hyper-V—not even in the RTM update for Hyper-V—and must be obtained via a separate download.



EXAM TIP LINUX INTEGRATION COMPONENTS

Note that the enlightenments for Linux are called *Integration Components*, not Integration Services. This is because the LIC only include drivers and not services. Also keep in mind that the drivers include support for IDE and SCSI storage, networking, and keyboard and mouse. They do not offer graphics (video) support.

MORE INFO LINUX INTEGRATION COMPONENTS

While the LIC were in beta at the writing of the exam, they have now officially been released. Find them at <http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=ab7f4983-93c5-4a70-8c79-0642f0d59ec2>.

Running Legacy Guests

When you run a non-Hyper-V–aware guest operating system in a child partition, its performance suffers from the fact that it does not include enlightenments and therefore does not detect that it is running in a VM. Operating systems that fall within this category include any Microsoft operating system that has not been updated and any non-Microsoft operating system for which Integration Services have not been developed. In the Microsoft realm, this includes DOS, Windows 3.x, Windows NT, and others. In the non-Microsoft realm, this includes any x86 or x64 operating system for which Integration Services do not exist.

IMPORTANT WINDOWS NT

Although Windows NT is not an enlightened guest operating system, it is a special case, as you will discover when you examine the advanced settings for virtual machines in Hyper-V.

IMPORTANT HYPER-V PERFORMANCE

If your network adapters include advanced interface settings, do not run enlightened and legacy VMs on the same host server. Legacy VMs can only work with the legacy network adapter. This adapter might require you to deactivate the advanced features of your physical network adapters, which could impact the performance of the enlightened VMs. Because enlightened VMS use virtual network adapters through VSCs, they can take advantage of all of the features of your physical network adapters.

Using the Hyper-V Input Release Keys

One of the impacts of working with a Legacy guest operating system in Hyper-V is evident when you work with the Virtual Machine Connection for the VM. You use the Virtual Machine Connection (VMC) when you interact with the virtual machine and you access it by double-clicking the virtual machine's thumbnail image in Hyper-V Manager. This gives you access to the VM's guest operating system and lets you interact with all of the functions available within the VM. However, when you work with an enlightened guest that includes Integration Services, the experience is transparent, especially when you use the mouse. The mouse can be active both within the VM in the VMC and outside the VM when you move it outside of the VMC.

But when you work with a legacy guest operating system, there are no Integration Services; therefore, your mouse becomes "trapped" when you click the VMC to access the VM's functions. To release it, you must use the special Hyper-V Release Key. By default, this key is Ctrl+Alt+Left Arrow, but you can modify it for several other key combinations through the Hyper-V Settings dialog box (see Figure 4-4). You will learn to use this key combination whenever you work with legacy VMs and the VMC interface.

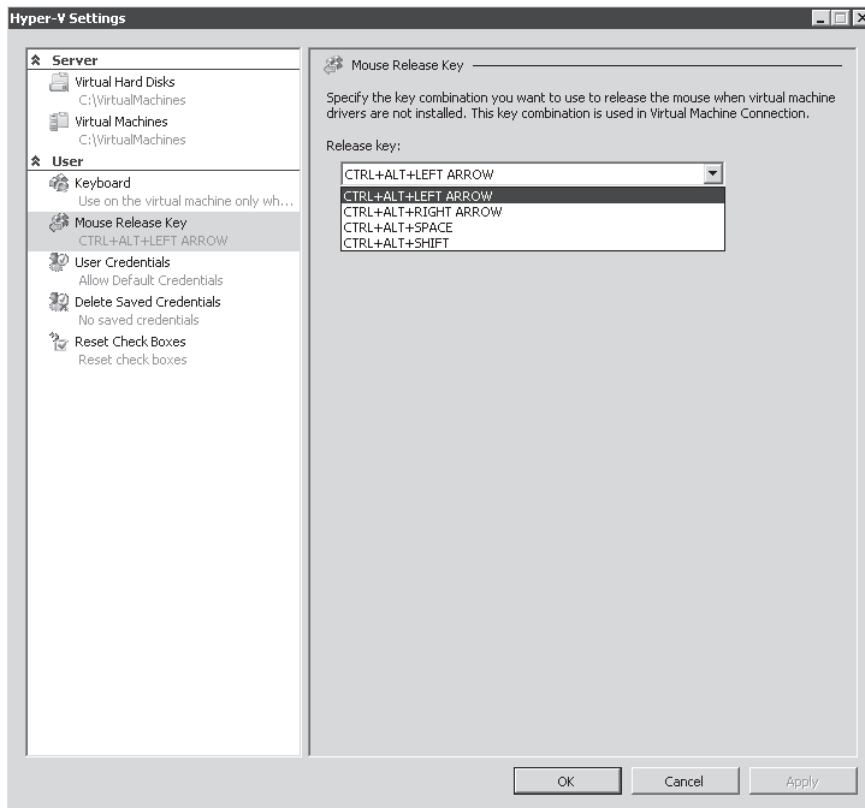


FIGURE 4-4 Modifying the Hyper-V Input Release Key



EXAM TIP LEGACY VMs, HYPER-V, AND TERMINAL SERVICES

When you access a legacy VM or a VM that does not yet include Integration Services by accessing the Hyper-V server through Terminal Services or the Remote Desktop Connection and then launching the VM's VMC, the mouse will not be available and all operations will need to be performed through the keyboard only. Note, however, that when you access the VM directly through Terminal Services or the Remote Desktop, the mouse will work just fine.

Creating a Virtual Machine

Creating a virtual machine in Hyper-V is a very straightforward process:

1. Determine the requirements for the operating system you intend to run in the VM.
2. Determine whether this operating system can support Hyper-V's Integration Services. Look up Table 1-4 in Chapter 1, "Implementing Microsoft Hyper-V" to review supported operating systems. This will help you determine which type of virtual components the machine will require.
3. Add the potential requirements for the application this operating system will support.
4. Determine which type of disks are required for the virtual machine. For example, a database server should have at least three disk volumes:
 - The first volume will run the operating system.
 - The second volume will run the database itself.
 - The third volume will run the transaction logs required to update the database.Other applications will require different disk structures. Make sure you understand them fully before you proceed; otherwise, the structure of the VM you create may impact the performance of the application(s) it hosts.
5. Create the basic VM, assigning the base components.
6. Use the VM Settings dialog box and tools to modify the configuration of the basic VM, adding components and changing other settings.
7. Launch the VM and begin the installation and configuration process for both the operating system and the application(s) it will host.

From that point on you monitor the operation of the VM to ensure that it continues to meet the service levels you have outlined to your user base.

As you work with VMs, you'll discover specific categories of machines that you work with. At that point in time, you'll begin creating template virtual machines—machines that are already prepared to some degree and that you can use to seed new operational VMs. This is when you'll begin to reap some of the most powerful benefits of virtualization: creating VMs from templates is a very fast process that is limited only by the speed of the disk when duplicating virtual hard drive images. In some cases, it can take as little as 20 minutes from start to finish. Compare this to deploying physical systems. In fact, even in the very best

deployment infrastructures, there is little comparison between creating a physical machine and generating a copy of a virtual machine from a template.

Creating a Basic Virtual Machine

A basic virtual machine is a machine as it is after you have generated the virtual machine through the Hyper-V New Virtual Machine Wizard. You can create a basic virtual machine in two ways:

- The first is to start the New Virtual Machine Wizard and immediately click Finish on the Before You Begin page. This generates a virtual machine with all default settings. These settings are discussed in the following section.
- The second is to start the New Virtual Machine Wizard and go through each page. You have already used this wizard to run through this process when you performed Exercise 3 in Lesson 2 of Chapter 2. Remember that this process asks you to specify the following items:
 - Specify the VM name and location.
 - Assign memory to the VM.
 - Configure networking for the VM. Note that only a single network adapter is available for the VM at this time.
 - Connect a virtual hard disk. By default, a new IDE virtual hard disk is created with a proposed size of 127 GB.



EXAM TIP HYPER-V IDE DISKS

Hyper-V proposes an IDE disk and not a SCSI disk by default because Hyper-V machines must use an IDE disk to boot. SCSI disks can only be added after the machine has been created. This is why the proposed default disk size is 127 GB—this is the maximum size of IDE disks.

- Review the installation options and create the VM.

This generates a VM with default settings.

Exploring the Settings of a Default VM

When you create a VM with default settings—basically opening the wizard and clicking Finish—Hyper-V creates a VM with the following properties:

- Under the Hardware category:
 - VM memory is set at 512 MB; maximum VM RAM depends on the Guest operating system, but you can only enter up to 3836 in this dialog box.
 - One processor with no reserve, a virtual machine limit of 100, and a relative weight of 100.
 - One hard drive assigned to IDE controller 0 with a location of 0 (in use).

- One DVD drive assigned to IDE controller 1 with a location of 0 (in use) and media set to None.
- One virtual hard disk (.vhd) file located under either the default path (the Public User Profile) if the path has not been changed in Hyper-V settings or in the location of the last VHD file you created. This VHD will be called New Virtual Machine.vhd and be a dynamically expanding disk with a size of 127 GB.
- Two COM ports, both set to None.
- One diskette drive with media set to None.
- Under the Management category:
 - The default name is New Virtual Machine with no description.
 - All the Integration Services are selected, but are not available to the VM until they have been installed.
 - The snapshot file location is either the default setting of the system drive's ProgramData folder or the setting you assigned when you configured the VHD location in Hyper-V settings.
 - The Automatic Start Action is set to Automatically start if it was running when the service stopped and is set to No startup delay.
 - The Automatic Stop Action is set to Save The Virtual Machine State.

In addition, the virtual machine's configuration file will be located either in the default location (the ProgramData folder) or the location you set when you configured the Hyper-V settings.

MORE INFO CONFIGURING VIRTUAL MACHINES

For more information on configuring virtual machines, look up the screen cast *Configuring Virtual Machines* at <http://go.techtargget.com/r/5927601/30819>.

Exploring Virtual Machine File Makeup

Hyper-V virtual machines are composed of several files and file types, including:

- **Virtual machine configuration file** The Hyper-V virtual machine configuration file is an Extended Markup Language (XML) file that contains all of the information pertaining to the VM's settings. This file is stored in a subfolder called Virtual Machines and is named with a Globally Unique Identifier (GUID) instead of the VM's name. Because the file is named with a GUID, it is difficult to identify which configuration file is tied to which VM. By default all virtual machine configuration files are stored in the Virtual Machines folder under the default configuration path file you set in Hyper-V Settings. When all VM configuration files are in the same location like this and all are named as GUIDs, it becomes extremely difficult to identify which file belongs to which VM. However, if you create a special subfolder for the VM and if you select Store The Virtual Machine In A Different Location During The Creation Of The VM, Hyper-V

creates a new subfolder named with the VM name you assign during creation, creates a subfolder named Virtual Machines within this folder, and then stores the GUID configuration file within this folder (see Figure 4-5). You used this method in Exercise 3 in Lesson 2 in Chapter 2 when you created your first VM. Hyper-V will also create a folder with the same GUID. The purpose of this folder is detailed later in this section. You can view the contents of the configuration file in Internet Explorer, which is the default program for files with the XML extension (see Figure 4-6) or in Notepad if you need to modify it. However, be very wary of directly editing VM configuration files because you may break the VM if you make a mistake.

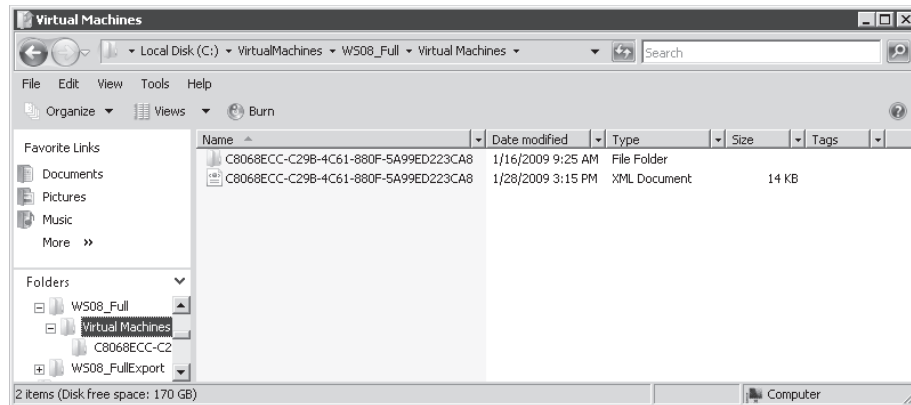


FIGURE 4-5 Viewing the VM's configuration file location



EXAM TIP VIRTUAL SERVER CONFIGURATION FILES

Microsoft Virtual Server 2005 creates VMs and automatically stores all VM files in a single folder named with the VM name. In addition, VM configuration files are named after the name you give to the VM and use a .vmc extension. Keep this in mind during the exam. Virtual Server and Hyper-V do not use the same structure for VM file location and do not use the same convention for VM file naming. This is one reason why Virtual Server virtual machine configuration files are not compatible with Hyper-V. Note, however, that Virtual Server VHDs are compatible with Hyper-V. More on this topic is covered in Chapter 6, "Migrating to Hyper-V".

- **Virtual machine hard disk files** VM VHDs are stored in the Public User Profile by default, but this setting can and should be changed in Hyper-V Settings. As a best practice, you should never store VHDs on the system disk because VM operation will be seriously impacted. You should also avoid storing VHDs on a second partition of the same physical disk as the operating system because it will also impact VM operation. Once again, if you select Store The Virtual Machine In A Different Location During The Creation Of The VM and you create a new disk for the VM, it will be stored in the same folder as the Virtual Machines folder (which contains the VM's GUID configuration file). This procedure keeps all of the VM's makeup files together.

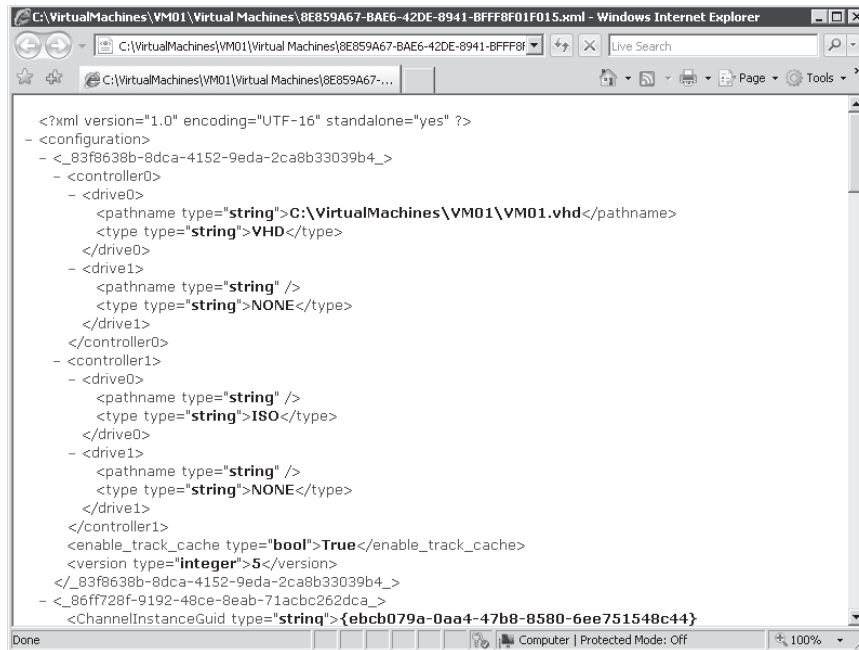


FIGURE 4-6 Viewing the content of a VM's configuration file

- **Virtual machine snapshots** Hyper-V has the ability to capture a point-in-time image of a virtual machine state. These images are called Hyper-V snapshots. Hyper-V snapshots are not to be confused with the snapshots created by the Volume Shadow Copy Service (VSS) in Windows Server 2008. VSS is used to prepare a backup image of a virtual machine whereas Hyper-V snapshots are used to support the return to a specific point in time of a VM. Hyper-V snapshot images are also named with GUIDs—but with no file extension—and stored in the same location as the VM's configuration file. Hyper-V snapshots will be covered in more detail in the next lesson.
- **Virtual machine saved states** One of the greatest features of a hypervisor is the ability to save virtual machine states. A VM saved state is very much like a physical machine hibernation state. When you hibernate a physical machine, you copy all of the machine's in-memory content and store it on the machine's hard disk. Then, when you restart the machine, instead of running through the entire boot process, the machine will simply restore in-memory contents to RAM and start—a process that is much faster than the normal boot process. The same thing occurs when you save the state of a VM: all VM in-memory contents are written to saved state files, which use .vsv and .bin extensions and are stored within the folder that is created when you first generate the VM's configuration file. This folder is named with the same GUID as the VM's configuration file and is a subfolder of the Virtual Machines folder containing the GUID XML configuration file.
 - VSV files contain the supporting process information on the VM state.
 - BIN files contain the actual memory contents.

These file types make up Hyper-V VMs. As you can see, if you do not select Store The Virtual Machine In A Different Location During Its Creation, the files that make up a given VM will be scattered in different locations. However, because most VMs are nothing but a set of files—XML configuration files, VHDs, and possibly, snapshots—it makes the most sense to gather them all within a single folder. Gathering all VM makeup files in a single folder makes it much easier to manage VMs in the long run.

Advanced VM Setting Configurations

In most cases, you will rely on the Hyper-V New Virtual Machine Wizard to create a new VM and then use the VM Settings dialog box to further modify the VM's properties. Table 4-1 outlines the settings you can control and modify when you change a VM's configuration. Most settings changes require you to turn off the VM, but in some cases, you can change settings while the VM is running. Settings you can change while the VM is running are called *variable resources*. Settings you cannot change while the VM is running are called *fixed resources*. Also note that the Settings dialog box is divided into two sections: Hardware and Management (see Figure 4-7). The Hardware section covers all of the virtual components of the VM. The Management section covers how the VM will behave given specific conditions.

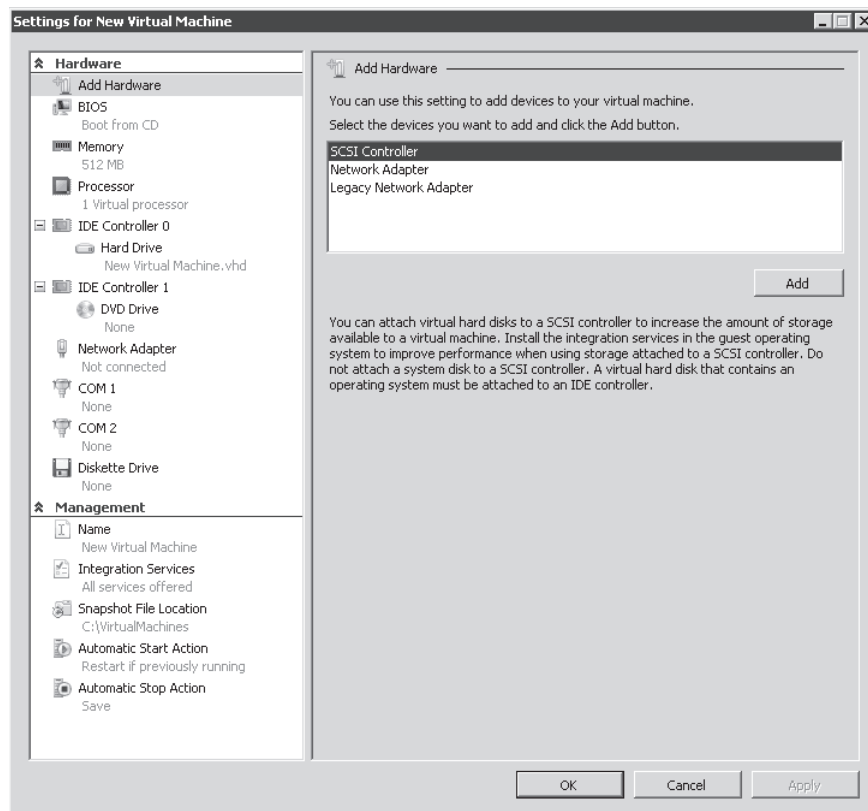


FIGURE 4-7 Viewing the content of a VM's configuration file

TABLE 4-1 Virtual Machine Settings

CATEGORY	SETTING	DESCRIPTION	OPTIONS	FIXED RESOURCE	VARIABLE RESOURCE
Hardware	Add Hardware	Used to add devices.	SCSI controller	X	
			Network adapter		
			Legacy network adapter		
	BIOS Boot form CD	Used to modify the startup order of the devices in the basic input/output system (BIOS) or turning Num Lock on or off.	The default order is:	X	
			■ CD		
			■ IDE		
			■ Legacy network adapter		
			■ Floppy		
	Memory	Used to change the amount of random access memory (RAM) allocated to the virtual machine.	Between 8 and the maximum amount of memory available on the host minus minor Hyper-V overhead.	X	
Processor	Used to modify the number of virtual processors based on the number of logical processors on the physical machine. Can also be used to modify other resource control settings.	Used to limit processor functionality to run an older operating system such as Windows NT on the virtual machine.	Number of logical processors	X	
			Resource Control:		
			■ VM reserve (%)		X
			■ % of total system resources	X	
			■ VM limit (%)		X
			■ % of total system resources	X	
			■ Relative weight	X	
			■ Limit processor functionality	X	

IDE Controller 0	Used to add hard drives or CD/DVD drives to the IDE controller.	Hard Drive DVD Drive	X X
Hard Drive (VHD)	Hard Drive: Used to change how the VHD is attached to the VM. Media: Used to compact or convert the VHD by editing the .vhd file.	Controller Location Specify the full path. (.vhd file) New Edit Inspect Browse Physical hard disk Remove	X X X X X X X X X
IDE Controller 1	Used to add hard drives or CD/DVD drives to the IDE controller.	Hard Drive DVD Drive	X X

CATEGORY	SETTING	DESCRIPTION	OPTIONS	FIXED RESOURCE	VARIABLE RESOURCE
		DVD Drive:	Controller	X	
		Used to select the controller and the location on the controller to attach the CD/DVD drive.	Location	X	
		Media:			
		Used to specify which media to use with the virtual CD/DVD drive.	None		X
			Image file: Browse		X
			Physical CD/DVD drive	X	
			To remove the virtual CD/DVD drive from the VM	X	
			Network:		
			Not Connected		X
			Internal		X
Network Adapter	Used to specify the configuration of the network adapter or to remove the network adapter.		External		X
			Private		X
			MAC Address:		
			Dynamic	X	
			Static	X	
			VLAN ID		X
		Used to enable virtual LAN identification.			
		Used to remove the network adapter from the VM.		X	

COM 1 COM 2	Used to configure the virtual COM port to communicate with the physical machine (parent partition) through a named pipe.	Attachment:		
		None		X
		Named pipe, if on a remote computer, must specify the computer name		
		Pipe name		X
Diskette Drive	Used to specify a 1.4-MB virtual floppy disk file.	Remote computer		X
		Media:		
		None		X
Management	Name	Virtual floppy disk (.vfd file)		X
		Name		X
		Notes		X
Integration Services	Used to edit the name of the VM. Used to record notes about the VM. Used to view the services that have been installed and are currently running. Must be installed and supported in the guest operating system.			
		Operating system shutdown		X
		Time synchronization		X
		Data Exchange		X
		Heartbeat		X
		Backup (volume snapshot)		X

CATEGORY	SETTING	DESCRIPTION	OPTIONS	FIXED RESOURCE	VARIABLE RESOURCE
	Snapshot File Location	Used to specify the folder to store the snapshot files for the VM.	Location		X
	Automatic Start Action	Used to specify what the VM should do when the physical computer starts.	Nothing Automatically start if it was running when the service stopped Always start this virtual machine automatically		X X X
		Used to specify a startup delay to reduce resource contention between VMs.	Startup delay		X
	Automatic Stop Action	Used to specify what the VM should do when the physical computer shuts down.	Save the virtual machine state Turn off the virtual machine Shut down the guest operating system		X X X

UPDATE ALERT FIXED VS. VARIABLE RESOURCES

The nature of resources and VMs is apt to change over time as Microsoft adds functionality to Hyper-V. As time goes by, more and more resources will change from fixed to variable in nature. For example, in Hyper-V 2.0 (R2), VHDs become variable resources since they can be added or removed while the machine is running.

**EXAM TIP SCSI VS. IDE**

Hyper-V virtual machines can only boot from IDE drives. Because of this, every VM must have at least one IDE disk drive.

**EXAM TIP SNAPSHOT LOCATION**

The Snapshot location in VM Settings is a variable resource until you take the first snapshot. As soon as a snapshot has been captured, the resource changes from variable to fixed.

UPDATE ALERT CHANGE IN THE VM SETTINGS UI IN WINDOWS SERVER 2008 R2

In Hyper-V R2, Microsoft added a new toolbar to the VM settings user interface. You can use the new toolbar to move from the settings of one virtual machine to another by either selecting the new virtual machine from the drop-down list or by using the forward and back arrows to move through VMs. This toolbar also lets you change the settings of more than one VM at a time. For more information, see http://blogs.msdn.com/virtual_pc_guy/archive/2009/01/26/hyper-v-r2-changes-to-the-virtual-machine-settings-ui.aspx.

UPDATE ALERT MAC ADDRESS MANAGEMENT IN WINDOWS SERVER 2008 R2

Microsoft has added a new section to the Virtual Network Manager in Hyper-V R2 that allows you to configure the range of MAC addresses that Hyper-V will use for dynamic MAC addresses generation. For more information, see http://blogs.msdn.com/virtual_pc_guy/archive/2009/01/20/hyper-v-r2-mac-address-management.aspx.

Note also that the information visible in the left pane of the VM Settings dialog box can be controlled through the Hyper-V UI. If you right-click the left pane, you will be presented with the option of turning two options on or off (see Figure 4-8). The two options are:

- **Show Summary** By default, the Settings dialog box displays summary information beneath each item in the VM. If you clear this option, the summary information will disappear.
- **Highlight Changes** By default, the dialog box highlights each change you make. If you clear this option, changes will no longer be highlighted.

Be aware of these two options. If they are turned off by mistake, you can always turn them back on.

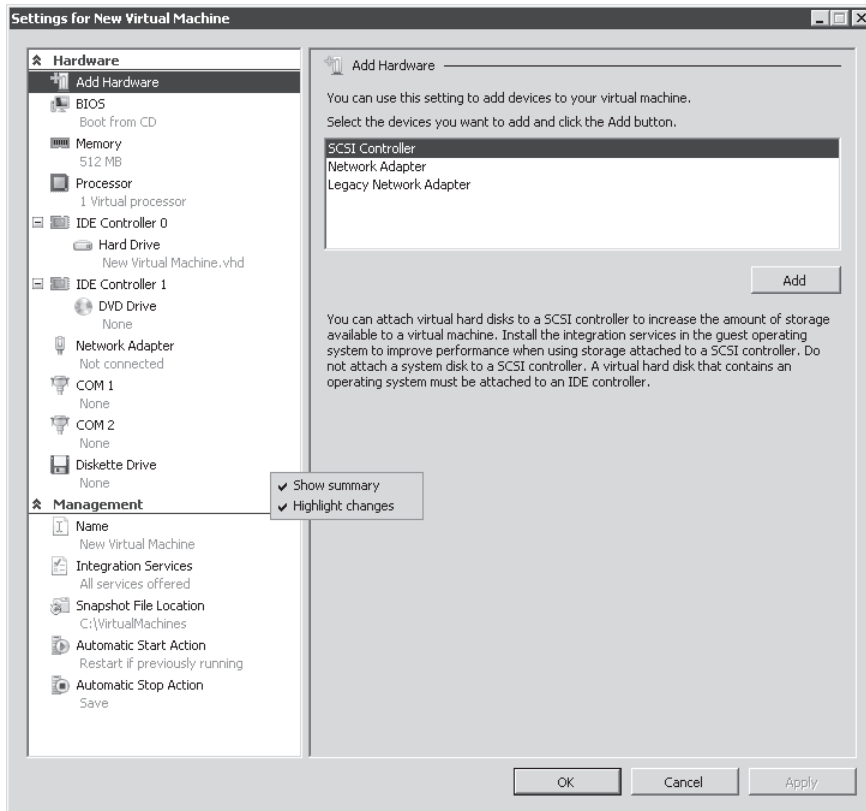


FIGURE 4-8 Controlling the UI options in the Settings dialog box

Installing a Legacy Guest

Although Hyper-V works best with enlightened guest operating systems and you should try to use these operating systems as much as you can to obtain peak VM performance, you may find yourself in a situation that requires the operation of a legacy VM. Legacy VMs can be one of two types of operating systems:

- Older Windows operating system** If you try to run an operating system such as Windows NT or MS-DOS in a VM on Hyper-V, the VM may not operate properly because modern processors include functionality that is not supported by the operating system. In this case, you must use the Limit Processor Functionality (LPF) setting in the VM's settings (see Figure 4-9). This setting reduces the command set of the processor and changes its behavior to support the older operating system. For example, NT was not aware of multi-core processors. Using the LPF setting will let NT treat the processor as a single-core processor. In addition, this setting reduces the possibility of NT crashing because of the high central processing unit identification (CPUID). Make sure you make this change before you install the operating system to avoid any potential problems during installation.

- **Newer non-Windows non-Hyper-V-aware operating system** If you try to run a modern Linux operating system that is not supported through Hyper-V Integration Components—for example, running Red Hat Linux before Microsoft releases the Integration Components for it—your operating system will need to run using only legacy devices through emulation. For example, to have your operating system communicate through the network adapter, you must use a Legacy Network Adapter and not the enlightened Network Adapter or the machine will not be able to detect the virtual device. In this case, you must modify the settings of a VM—ideally before you install the operating system—remove the Network Adapter that is added during VM creation, and replace it with a Legacy Network Adapter. Use the Add Hardware option available at the beginning of the VM Settings dialog box to do so.

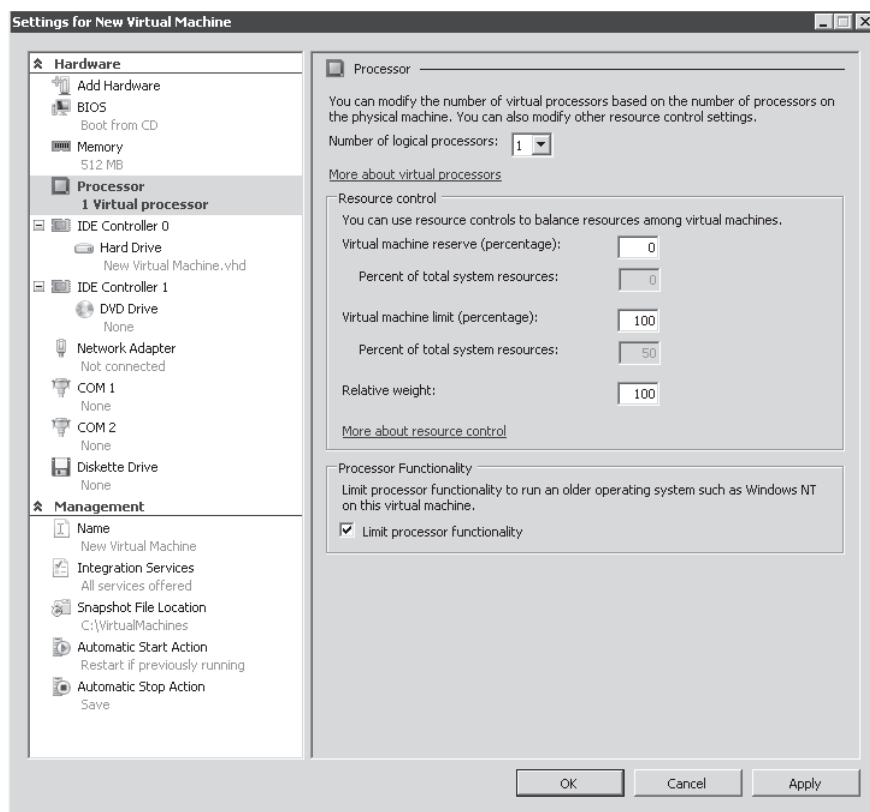


FIGURE 4-9 Using LPF for a Legacy VM

Remember that you should not run legacy VMs on the same hosts as enlightened VMs because legacy VMs rely on emulated hardware while enlightened VMs use the VMBus. Using both on the same system could force you to reduce the functionality of some of your hardware devices—such as disabling some settings in physical network adapters—and throttle the performance of the component.

Examining Virtual Machine States

The virtual machines you run in Hyper-V can exist in a wide variety of states throughout their life cycle. States are displayed under the State column within the Details pane of Hyper-V Manager. These potential states are outlined in Table 4-2. This table also includes the corresponding commands in Hyper-V Manager. VM states are controlled by selecting the VM and applying the appropriate command from the Actions pane in Hyper-V Manager.

TABLE 4-2 Virtual Machine States

STATE	COMMAND	DESCRIPTION
Applying Snapshot	Apply	Used to apply a point-in-time image to a virtual machine, returning the contents of the VM to the point-in-time image. Requires confirmation in the Apply Snapshot dialog box. Can also take a snapshot and then apply the image to the VM.
Creating Snapshot	Snapshot	Used to create a point-in-time image of a virtual machine. Can be performed while the machine is either Running, Off, or Saved.
None	Delete Snapshot	Used to remove a point-in-time image from a VM and return the VM to its current status by merging the snapshot contents. Requires confirmation in the Delete Snapshot dialog box.
None	Delete Snapshot Tree	Used to remove a hierarchy of point-in-time images from a VM and return the VM to its current status by merging snapshot contents. Requires confirmation in the Delete Snapshot Tree dialog box.
None	Delete Saved State	Used to discard the state that was saved for a virtual machine that is in a saved state, and turn off the virtual machine. Requires confirmation in the Delete Saved State dialog box.
Paused	Pause	Used to suspend execution of a virtual machine and keep all virtual machine states in memory. This is the same as putting a physical machine on Standby. If the power fails, the VM state is lost.
Saving/Saved	Save	Used to suspend execution of a virtual machine and save the current virtual machine state to disk to release memory and CPU resources for other virtual machines. When restored from the saved state, the VM is returned to the condition that it was in when its state was saved. This is the same as hibernating a physical machine.
Starting/Running	Start	Used to start a virtual machine that is stopped, paused, or in saved state.

STATE	COMMAND	DESCRIPTION
Stopping/Off	Shut Down	Used to shut down the guest operating system on the virtual machine. This is the same as using the Shut Down command from within a guest operating system. Requires a confirmation in the Stop Machine dialog box.
Stopping/Off	Turn Off	Used to stop a virtual machine and does not save any state information. This has the same effect on a virtual machine as does pulling the plug on a physical server.
Stopping/Running	Reset	Used to shut down and restart a guest operating system on the virtual machine. This is the same as using Restart within the guest operating system. Requires a confirmation in the Reset Machine dialog box.



EXAM TIP MACHINE STATES

Keep the various machine states and their corresponding commands in mind—they are an important part of the exam.

PRACTICE Working with non-Windows VMs

In this practice, you will install a new VM to host a non-Windows operating system. The operating system you will install is Novell's SUSE Linux Enterprise Server 10 SP2. This practice consists of a single exercise. Perform this exercise on ServerFull01. Log on with domain administrator credentials to simplify the process.

EXERCISE 1 Create a Linux VM

In this exercise you will create a SUSE Linux Enterprise Server 10 SP2 x86 virtual machine. Make sure you have an ISO file of a SUSE distribution from Novell. You will need to create a Novell account to download the bits. Go to https://secure-www.novell.com/center/regadmin/jsp/eval_app.jsp?buildid=xWohTS2zkSs to obtain them. Also make sure you download the Linux Integration Components file from Microsoft. Store the ISO file and the LIC in the SourceFiles folder. Execute the downloaded file to extract the LinuxIC.iso from it. Store the extracted files in the SourceFiles folder. Also take the time to review the Linux ICs for Hyper-V file for additional and updated instructions.

1. Create a virtual machine with 1 GB of RAM and a new 60-GB VHD. Name the machine **Linux01** and make sure you tell Hyper-V to store the VM files in a different location during the machine creation. You can follow the steps in Exercise 3 in Lesson 2 of Chapter 2 to refresh your memory on how to perform this task. Do not start the VM at the end of the wizard. You need to modify its settings first.

2. Right-click Linux01 and choose Settings. In the Add Hardware section of the Settings dialog box, click Legacy Network Adapter and then click Add. Choose which network to attach the Legacy Network Adapter to. In this case, select Hyper-V External and click Apply. The Legacy Network Adapter is necessary to provide VM networking functionality before the Linux Integration Components are installed.
3. Move to DVD Drive. Click Image file, click Browse, move to the folder where you stored the SUSE Linux ISO file, and click OK twice. You can now move on to the Linux installation.
4. Right-click Linux01 and choose Start. This will start the VM and begin the installation process for SUSE Linux.

IMPORTANT INTEL PROCESSORS AND LINUX VMs ON HYPER-V

It is possible that the graphical boot loader will fail on an Intel platform during the setup and during VM operation. AMD processors have no similar issue. To avoid this issue, you must pass a parameter to the Linux kernel to specify screen resolution and depth. For example, to use a 1024 x 768 screen resolution with 16-bit color, type **linux vga=0x317** at the install prompt.

5. Make sure you choose to install the development packages (C/C++ Compiler and Tools) and the kernel sources (Xen Virtual Machine Host Server) during the installation. The development packages are required to build and install the LIC. The kernel sources are required to install the synthetic device drivers in the VM.
6. Reboot as required, log on to the VM with root access, and complete any first boot configuration in the VM.
7. Use the command prompt to mount the installation media from the DVD and install the Xen-enabled kernel from the distribution you are using.
8. Replace the Linux installation DVD in the VM with the LinuxIC.iso file. Use the VM settings in Hyper-V Manager. You can do this while the machine is running because DVD settings are a variable resource in Hyper-V VMs. Unmount the installation media and mount the LinuxIC.iso file in Linux. Copy the Integration Components to the hard disk in the Linux machine. Place them in the LinuxIC folder.
9. Now install the Linux Integration Components into your x86 machine. Use a perl command to do so:

```
$ perl /opt/linucic/setup.pl x2v /boot/grub/menu.lst
```

10. Reboot Linux. When the reboot is complete, log on with root access and finish the installation by installing the synthetic drivers. Use the following command:

```
$ perl /opt/linucic/setup.pl drivers
```

The Integration Components are installed. You will now need to configure networking in the VM using the Network Adapter. You can also remove the Legacy Network Adapter now that the LIC are installed and running. In the VM Settings dialog box, select the Legacy Network Adapter, click Remove, and then click OK. Your VM is ready.

✓ Quick Check

1. What are the three types of virtual machines you can work with in Hyper-V?
2. What is the type of virtual machine in Hyper-V that does not support Hyper-V Integration Services?
3. What are the components (services and drivers) included in the Hyper-V Integration Services?
4. What are the additional components included in the Integration Components for Linux?
5. What are the files and file types that comprise a Hyper-V virtual machine?

Quick Check Answers

1. Hyper-V can run three types of virtual machines:
 - a. Machines running Hyper-V–aware Windows operating systems
 - b. Machines running Hyper-V–aware non-Windows operating systems
 - c. Machines running non-Hyper-V–aware operating systems
2. The machines running non-Hyper-V–aware operating systems will not support Hyper-V Integration Services; these machines will run everything through emulated device drivers.
3. Integration Services include two components: services and drivers. Services include operating system shutdown, time synchronization, data exchange, heartbeat, and backup (volume snapshot); these are enabled by default when they are installed in the guest operating system. Drivers include storage, networking, graphics, and input. No USB devices are included in the drivers.
4. Linux Integration Components (LIC) include only drivers and the Hypercall Adapter. Driver support for synthetic devices includes both a network controller and a storage controller. The Hypercall Adapter is an additional component included in the Integration Components for Linux and used to provide a communication channel between the synthetic drivers and the VMBus.
5. The files and file types of a Hyper-V virtual machine include:
 - a. A virtual machine configuration file (XML) named with a GUID and stored in a subfolder called Virtual Machines.
 - b. Virtual machine hard disk files (VHDs) stored in the Public User Profile by default.
 - c. Virtual machine snapshots called Hyper-V snapshots.
 - d. Virtual machine saved states.

Lesson 2: Working Virtual Hard Drives

A key part of virtual machine functionality is the virtual hard disk. VHDs are the component that make VMs so malleable transforming physical machines into a set of files in a folder. This is the focus of this lesson.

After this lesson, you will understand:

- Virtual hard disk types.
- The Virtual Hard Disk Wizard.
- Editing and inspecting a virtual hard disk.

Estimated lesson time: 40 minutes

Understanding Virtual Hard Disks

Hyper-V, like Virtual Server and Citrix XenServer, relies on virtual hard drives (VHD) files to store virtual machine disk contents. VHD files basically use a flat file format to write disk content. As outlined in Table 4-3, several different types of virtual hard disk drives are available in Hyper-V. Each type is accessible through the New Hard Disk Wizard in Hyper-V Manager.

TABLE 4-3 Virtual Hard Disk Drive Types

DISK TYPE	DESCRIPTION
Dynamically Expanding	The dynamically expanding virtual hard disk type is a disk that is created with a set size, but that does not take up this set size at creation. Instead, the set size acts as a limit for disk growth. The disk slowly expands as information is written to it. For example, if you create a dynamically expanding disk and set its size to 40 GB, but it only contains 10 MB of information, the size of the disk will be 10 MB plus a minor amount of space for disk management overhead. Dynamically expanding disks are very similar to the thin provisioning concept in storage virtualization technologies. When you use thin provisioning, you assign a set size to a logical unit (LUN) of storage, but the storage system only consumes the actual amount of space used in the LUN. If you create a LUN of 100 GB but there is only 10 GB of used space, the actual space requirements will be 10 GB plus some minor disk management overhead. Then, when the disk grows and requires more space, the storage system alerts the operator to add more spindles to support LUN growth. In this way, organizations can save on required spindles because they do not need to purchase them until the spindles are actually required.

DISK TYPE	DESCRIPTION
Fixed Size	Note, however, that using a dynamically expanding disk can cause virtual machine performance issues because there is some performance overhead in the parent partition of Hyper-V to actually expand the disk as the virtual machine runs. Therefore, dynamically expanding disks are most often used in test or development environments, in training environments, and in production environments for low-performance VMs. Fixed size disks are disks that are produced with a given size at disk creation. When you create a fixed size disk, Hyper-V automatically allocates all of the disk size on the spindle that hosts the disk. If the disk is 100 GB, then Hyper-V creates a storage container of 100 GB on the spindles to host the disk. The fixed size disk will be 100 GB regardless of the amount of information stored within the disk. Fixed size disks are similar to traditional LUNs in shared storage containers. When you create a traditional LUN, all of the space of the LUN is allocated at creation time and all of the spindles required to host the LUN must be present. Because fixed size disks are of a set size at creation time, they tend to perform better than dynamically expanding disks. Fixed size disks are often used in production environments where you want to gain the very best performance from a virtual hard drive. Note that fixed size disks take much longer to create than dynamically expanding disks because Hyper-V must reserve all of the space for the fixed disk. When a dynamically expanding disk is created, Hyper-V only needs to create the placeholder for the disk, which occurs much faster.
Differencing	Differencing disks are disks that use a parent-child relationship. One disk—the parent—contains the base information for the contents of the virtual machine. The other disk (or disks as the case may be)—the child—contain new information that has changed since the parent-child relationship was created. Parent differencing disks can be either fixed size or dynamically expanding disks, but when the parent-child relationship is created, the parent disk automatically becomes a locked disk; that is, a disk that no longer supports any changes. If changes are brought to the parent disk, it will automatically break the parent-child relationship. Note that one parent disk can have multiple child disks.

DISK TYPE	DESCRIPTION
	Differencing disks are used in a wide number of situations. For example, Microsoft Learning uses the differencing disk concept to create all of the training machines used in the courses they deliver. In the case of a course requiring several machines working together, such as a Microsoft Windows SharePoint course, one parent disk is created with a core installation of Windows Server 2008 and multiple child disks are created with the required server roles such as one for Active Directory Domain Services, one for Exchange Server, one for SQL Server, one for SharePoint Server, and so on. When the entire environment runs, each server role boots from the core parent disk and then the child disks run to create the required environment. Because differencing disks are based on a single parent, performance can be very poor unless you run differencing disks on the fastest spindles you have access to. However, because of the parent-child relationship, differencing disks can save significant amounts of actual disk space because the parent disk is the disk that requires the largest amount of space and the child disks only store actual differences or changes made beyond the base parent disk. In the case of the MS Learning disk example, you can often create very complex environments with only a few gigabytes of used space. A parent can have multiple different and unrelated child disks such as in the case of installing different products on different child disks or it can have a hierarchical relationship to child disks, with each child becoming the parent of the next child disk as new child disks are created. The latter is what happens when you use the Hyper-V Snapshot feature because you automatically turn the existing VHD into a set of differencing disks. Each time you create a snapshot, you create a new parent-child relationship between the VHDs. Differencing disks are often best used in training, testing, or development environments because they always allow you to go back in time by breaking the parent-child relationship and return to a given state of the VM.

The three disk types listed in Table 4-3 make up the different types of disks you will normally work with in Hyper-V (see Figure 4-10).

MORE INFO VIRTUAL HARD DISKS

For more information on working with virtual hard disks, look up the screen cast *Working with VHDs* at <http://go.techtarget.com/r/5927599/30819>.

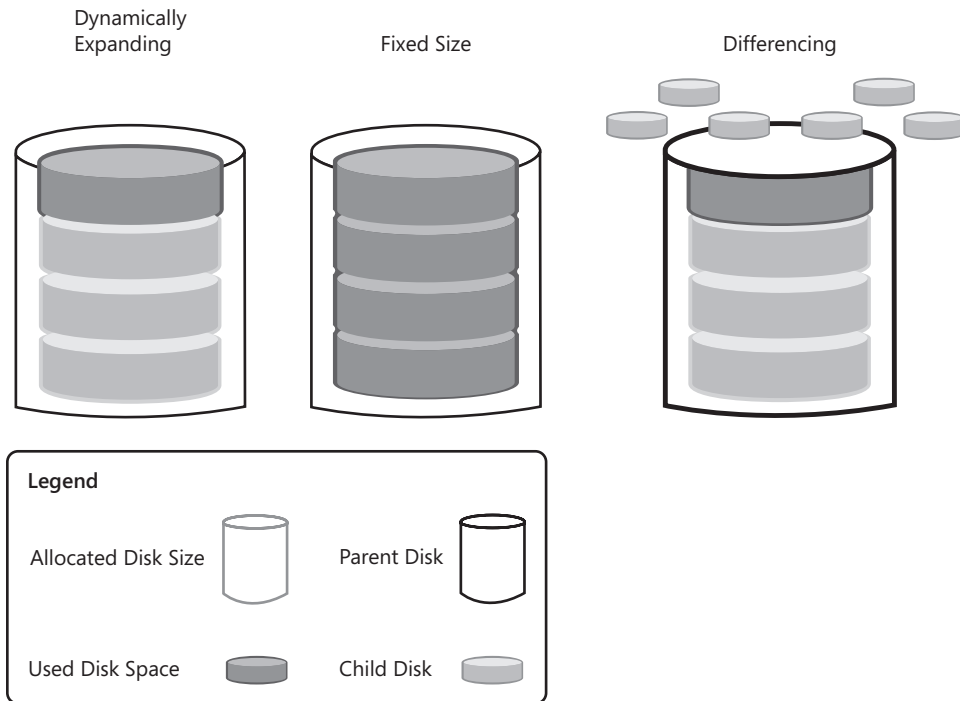


FIGURE 4-10 Hyper-V VHD types

UPDATE ALERT HOT ADD VHDS

VHDS are now a standard part of Windows Server 2008 R2 and Windows 7. For example, when you add a new disk in Disk Manager, you can create, format and consume VHDS directly from the interface. Because of this, you can now dynamically add or remove VHDS to running VMs. Note however that VHDS must be tied to SCSI controllers to use this feature. You can also add or remove pass-through disks to running VMs so long as the disks are tied to SCSI controllers. Windows Server 2008 R2 and Windows 7 can also boot from VHDS making it easier to consume this powerful disk format directly from the OS.

You can store any of the three VHD types on physical hard disk volumes that can be in either direct-attached storage (DAS), network-attached storage (NAS), or storage area network (SAN) in nature. However, you must store them on partitions that are formatted with NTFS. You cannot store Hyper-V VHDS in folders that use the Encrypting File System (EFS) because EFS is an encrypting system that is usually tied to particular users, and storing VHDS in user profiles does not make them highly available because they must run in a single user's context.

If security is an issue, you can store VHDS on partitions that use the BitLocker full drive encryption system. However, note that BitLocker adds some overhead to disk operations, which may impact VHD I/O operations and therefore virtual machine performance. Use BitLocker encryption only in highly secure environments or in environments where the possibility of theft

is present. The latter could occur in remote sites or in branch office locations where access to host servers cannot be secured because of the lack of a lockable storage room for servers.

Ideally, your VHDs will be stored on a high-speed shared storage container that is accessible by multiple Hyper-V hosts. Using this strategy ensures virtual machine fault tolerance because the VM can run on any of the hosts that have access to the shared storage LUN without having to actually duplicate or replicate the VHDs from one location to another. VHD replication can take considerable time because they can range in size from 40 to many hundreds of gigabytes. Note that the maximum size of a VHD in Hyper-V is almost 2 terabytes and is set at 2,040 GB.



EXAM TIP MAXIMUM VHD SIZE

Remember that the maximum VHD size in Hyper-V is actually 8 GB short of 2 terabytes and is set to 2,040 GB instead of 2,048 GB. This item will definitely be in the questions you'll find on the exam.

Avoid running VHDs on system disks that are used to run the parent partition.

Working with Pass-through Disks

A fourth type of disk you can use in support of virtual machines in Hyper-V is the pass-through disk. Pass-through disks are physical disk partitions that are assigned to a virtual machine. Instead of using a virtual hard disk, you assign an actual physical partition to the VHD. Pass-through disks have the following features:

- **Performance** Pass-through disks will give your VMs the utmost performance because Hyper-V does not need to manage the virtual disk during the operation of the virtual machine. When a VM runs, Hyper-V is only responsible for the actual operation of the VM and only needs to assign processor, memory, and networking resources to the VM.
- **Hybrid VMs** When you use pass-through disks, you can create a hybrid VM using a VHD as the system disk and using pass-through disks for the data disks. For example, if you created a VM to host Exchange Mailbox Server, you might store the operating system on a small VHD tied to the IDE controller, then install all Exchange services on a second drive that is a pass-through disk. You could then assign additional pass-through disks for the messaging database and the transaction logs, ensuring the best performance for the Exchange Mailbox Service.
- **Pass-through Disk Connections** Hyper-V VMs must boot from an IDE drive. Fortunately, you can assign a pass-through disk to a VM's IDE controller. You can also assign pass-through disks to both SCSI and iSCSI controllers, but they must be for disks other than the boot or system disk.
- **Locked-in VMs** Using pass-through disks locks the VM into the physical configuration you use to create it. The whole point of a virtual machine is that it is nothing but a set of files in a folder. When this is the case, you can create a VM in London, copy its files to New York, and then run the VM in New York. But when you use pass-through disks, you limit

the VM's mobility in much the same way you limit the mobility of a physical machine when you install an operating system physically. You must then find a way to move the contents of the physical disks the VM is composed of to another location to move the VM. To do this, you will often have to re-create the VM in its destination location or at the very least change its disk connections in the VM settings because they will no longer be the same.

- **Hybrid Pass-through Disks** You can also create hybrid pass-through disks. For example, you cannot boot a VM from an iSCSI controller, but you can boot a VM from an IDE controller that is tied to an iSCSI pass-through disk. Here's how:
 1. Create a LUN in your shared storage container to host the boot and system partitions for the VM.
 2. Use iSCSI to attach the LUN to the parent partition of a Hyper-V host. To avoid contention for the disk between the host and the VM, make sure the new LUN is offline on the host server.
 3. Create your new VM and choose to create the disk drives that will run it after the VM is created.
 4. Move to the VM's settings and select IDE Controller 0 and Location 0 (In Use) and assign it to a Physical Hard Disk. Select the disk you attached through the iSCSI LUN.
 5. Save your changes and boot the VM. The VM will boot from the iSCSI LUN. You can then install an operating system and run it from the iSCSI LUN.
- **Enlightened or Legacy Guests** Both enlightened and legacy guest operating systems can use pass-through disks; however, legacy guests are limited to IDE functionality and cannot use SCSI pass-through disks.

As you can see, pass-through disks can provide a viable option for several system configurations, but they limit VM functionality and do not give you access to any of the VHD capabilities that make VMs so much more exciting than physical machines.



EXAM TIP **MAXIMUM PASS-THROUGH DISK SIZE**

Remember that the maximum pass-through disk size in a VM is limited only by the limitations of the operating system running in the VM, not by Hyper-V's limitations.

Using IDE or SCSI Disks

When you attached disks to VMs, you must select how to attach the disk to the VM. Three possibilities exist:

- **Integrated Drive Electronics (IDE)** When you attach a disk—either VHD or pass-through—to a VM through an IDE controller, you attach a virtual Advanced Technology Attachment (ATA) disk to the VM. You can attach up to four virtual IDE disks to a VM. Note that IDE controllers are created automatically when you create a VM. Both enlightened and legacy guest operating systems can use IDE controllers in Hyper-V. Also note that Hyper-V VMs must boot from a virtual IDE disk.

- **Small Computing System Interface (SCSI)** When you attach a disk to a VM through the SCSI controller, you attach a virtual SCSI disk to the VM. However, because SCSI controllers are not created automatically during VM creation, you must create them after the VM has been generated through the New Machine Wizard in Hyper-V. This is done through the VM's Settings dialog box under Add Hardware and then SCSI Controller. You can attach up to four SCSI controllers to a VM. Each SCSI controller can support 64 disks for a maximum of 256 virtual SCSI disks on a guest operating system. Note, however, that SCSI controllers are only available to enlightened guest operating systems that have Integration Services installed.



EXAM TIP LINUX INTEGRATION COMPONENTS

Remember that LIC contain support for SCSI controllers just as the Integration Services do for Hyper-V-aware Windows guest operating systems, but do not include graphics drivers.

- **Internet SCSI (iSCSI)** You can also attach disks directly to VMs through iSCSI initiators. For example, Windows Server 2008 includes the iSCSI initiator directly within the operating system. You can use this initiator to bypass the host operating system completely and expose a disk only to the VM it runs. You do this by loading the iSCSI initiator directly within the guest operating system and correctly configuring the target disk.

The disk controller used in VMs does not have to correspond to the disk controller used in the host computer. For example, you can use Serial-Attached SCSI (SAS) devices on the host server and expose them as virtual IDE devices to VMs. You can also use both virtual IDE and virtual SCSI devices in a VM at the same time. However, because both devices are virtual and use the same optimizations in Hyper-V, their performance is similar even though IDE and SCSI performance in the physical realm is considerably different.

Keep the following rules in mind when you work with disk controllers in Hyper-V VMs:

- Use IDE only if you need four or fewer drives in the VM.
- Use IDE to boot legacy VMs from VHDs or VMs that do not include Integration Services yet.
- Use IDE and SCSI if your VM boots from a VHD, but you need more than four virtual drives in your VM.
- Use pass-through disks to boot from iSCSI within the guest operating system. Make sure the disk is set to offline on the host's parent partition.

These guidelines will help you determine which method to use to connect a VM based on the requirements of that VM.

MORE INFO DISK CONNECTIONS IN VMs

For more information on disk connections within VMs, look up Windows Server Hyper-V Storage at <http://blogs.microsoft.co.il/blogs/dario/archive/2008/08/26/windows-server-2008-hyper-v-storage.aspx>.

MORE INFO iSCSI INITIATOR CONFIGURATION

For instructions on how to perform iSCSI connections in Hyper-V, go to <http://blogs.technet.com/josebda/archive/2009/01/31/step-by-step-using-the-microsoft-iscsi-software-target-with-hyper-v-standalone-full-vhd.aspx>. For more information on iSCSI and Windows Server 2008, go to <http://technet.microsoft.com/en-us/library/cc771740.aspx>.

Working with the Virtual Hard Disk Wizard

Disk operations are performed through several different Hyper-V Manager interfaces. The first interface that gives you access to disk creation is the New Virtual Machine Wizard. Disk creation comes on the fifth page of this wizard, the Connect Virtual Hard Disk page (see Figure 4-11). The available options are:

- **Create A Virtual Hard Disk** This lets you generate a new VHD. The VHD will be a dynamically expanding VHD by default.
- **Use An Existing Virtual Hard Disk** This lets you connect to a previously created VHD. This VHD can be any of the three VHD types.
- **Attach A Virtual Hard Disk Later** This lets you create the VM without a hard disk and attach it later by editing the VM's settings. For example, you use this option when you want to connect the VM to a pass-through disk.

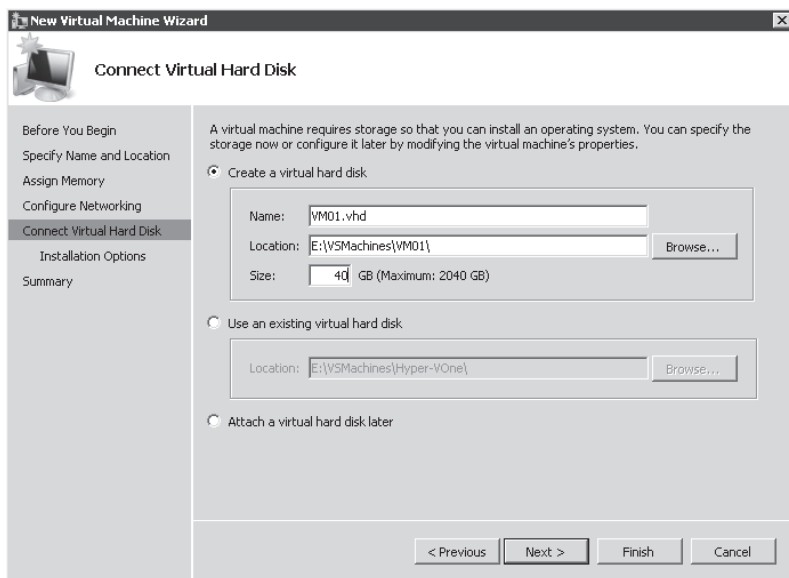


FIGURE 4-11 Creating a VHD during VM creation

VHD creation is performed through the New Hard Disk Wizard. This wizard gives you several options and lets you create disks in a wide variety of styles, choosing any one of the three VHD types (see Figure 4-12). The wizard can be accessed either through the Actions pane in Hyper-V Manager or through the VM Settings dialog box under the controller sections.

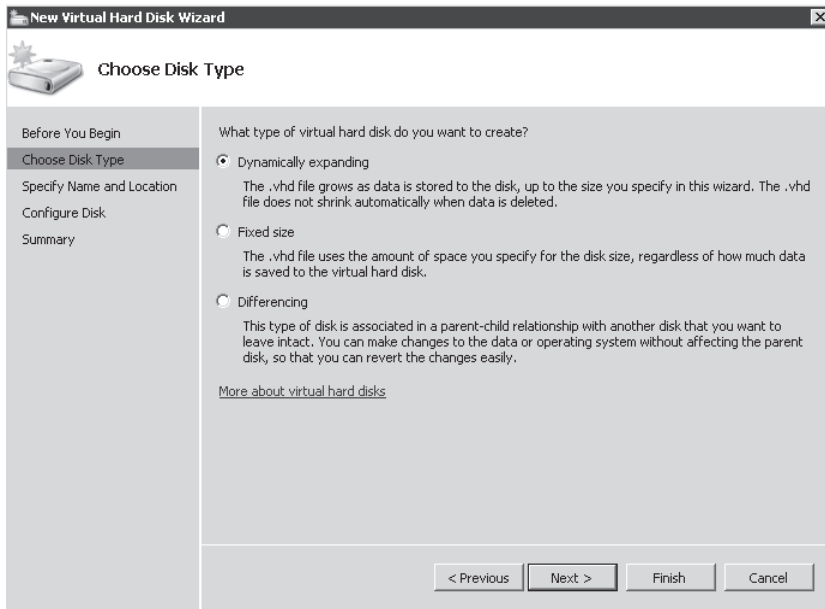


FIGURE 4-12 Creating a new VHD

If you choose a dynamically expanding or a fixed size disk, the wizard prompts you to name the disk, choose a location for it, and then identify the size of the disk to create. It also gives you the option to copy the contents of a physical hard drive into the newly created VHD (see Figure 4-13). In this case, the size of the disk will be the same size as the disk you are copying.

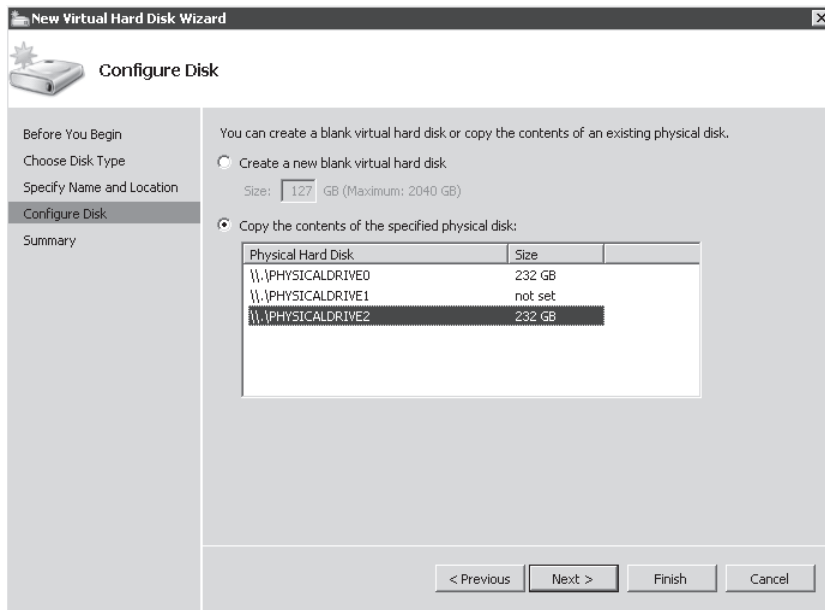


FIGURE 4-13 Copying a physical disk into a new VHD

If you choose to create a differencing disk in the New Virtual Disk Wizard, you will have to specify the location of the parent disk you want to use (see Figure 4-14). Remember that as soon as you identify a disk as a parent disk, it should be locked and used as read-only from that point on because if the parent disk changes, the parent-child relationship will be broken.

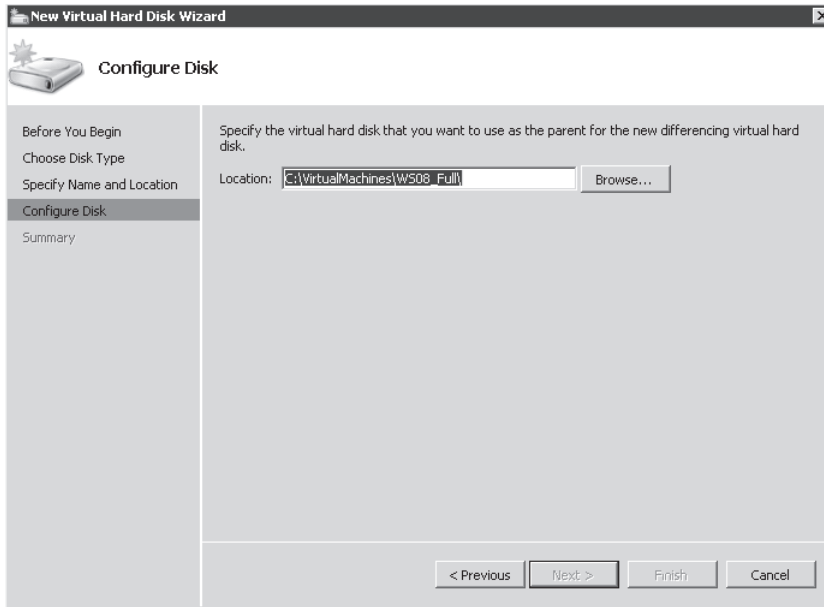


FIGURE 4-14 Specifying the location of a parent disk for a new differencing VHD

Another interface you can use to work with VHDs and pass-through disks is the Virtual Machine Settings dialog box (see Figure 4-15). In this case, you must begin by adding a new hard disk. You do this by selecting the controller you want to connect the disk to, choosing Hard Drive, and then choosing Add. After the hard drive has been connected to the controller—which can be either IDE or SCSI—you can configure the type of hard drive you want to connect. In this case you are given several choices:

- You can control both the controller and the location the virtual hard disk will be connected to.
- You can select the media type:
 - When you select Virtual hard disk (.vhd) file, you can either create the disk by clicking New or connect to an existing disk by either typing the path to the VHD file or clicking Browse to locate the existing VHD file. Clicking New launches the New Virtual Hard Disk Wizard.
 - When you select Physical hard disk, you must select the disk from a list of available partitions. Disks are listed as Disk 2, Disk 3, and so on. Disk 1 is usually assigned to the parent partition. Remember that the disk should be offline in the parent partition to avoid contention for disk reads and writes between the parent and the child partitions.

- You can also use this interface to remove a disk from a VM's configuration. Note that this does not delete the VHD from the host's hard drives; it only removes the VHD from the VM's configuration.

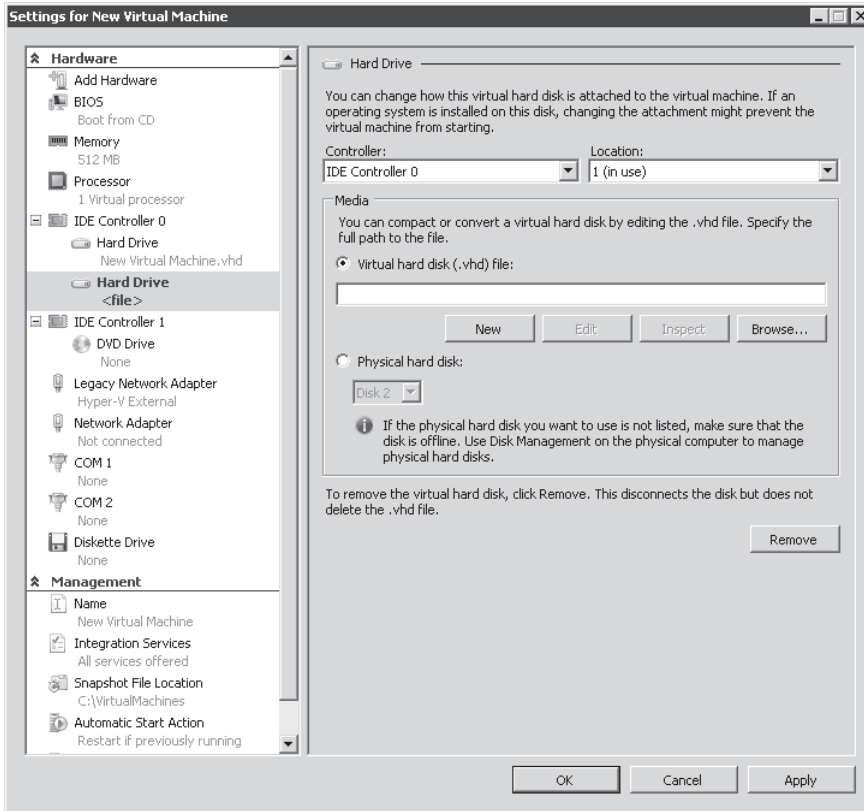


FIGURE 4-15 Attaching disks to a VM

You use the same interface to attach and create DVD drives to VMs (see Figure 4-16).

This interface also gives you several options:

- You can control both the controller and the location the DVD will be connected to.
- You can select the media type:
 - New DVDs are connected to None by default.
 - You can also connect the media to an ISO image file. ISO is a special, non-proprietary archive format used to represent the integral contents of a hard drive, CD, or DVD. For example, many software vendors deliver their software products in ISO format. You can use a DVD creation tool or a tool such as WinImage to convert the ISO image into another medium such as a DVD, but vendors are relying on the ISO more and more because it is one of the best mediums for populating virtual machines.

- You can connect the virtual DVD to the Physical CD/DVD drive.
- You can also use this interface to remove a DVD from a VM's configuration.

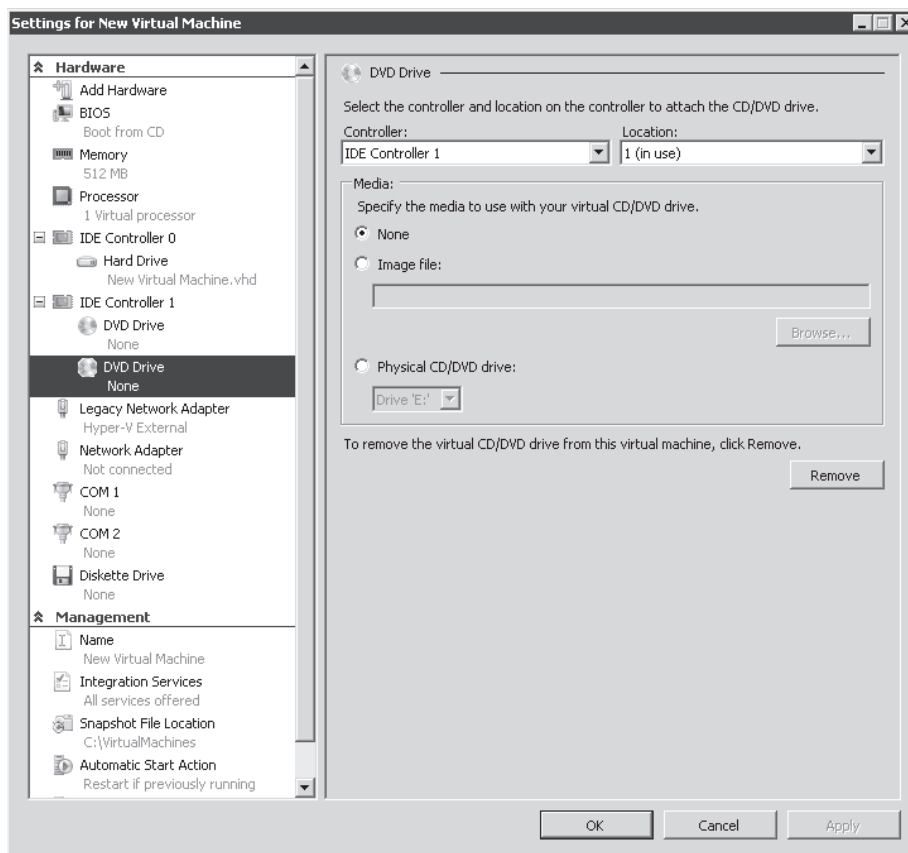


FIGURE 4-16 Attaching a DVD to a VM

MORE INFO WINIMAGE

Obtain WinImage from Gilles Volant Software at <http://www.winimage.com>.

The VM Settings dialog box is also used to add or remove SCSI connectors to the VM's configuration. In this case, you move to the Add Hardware option at the top of the left pane in the dialog box, select SCSI Controller, and click Add. As soon as you add the SCSI controller, the new SCSI controller is highlighted and you are given the option to add a hard drive to the VM's configuration (see Figure 4-17).

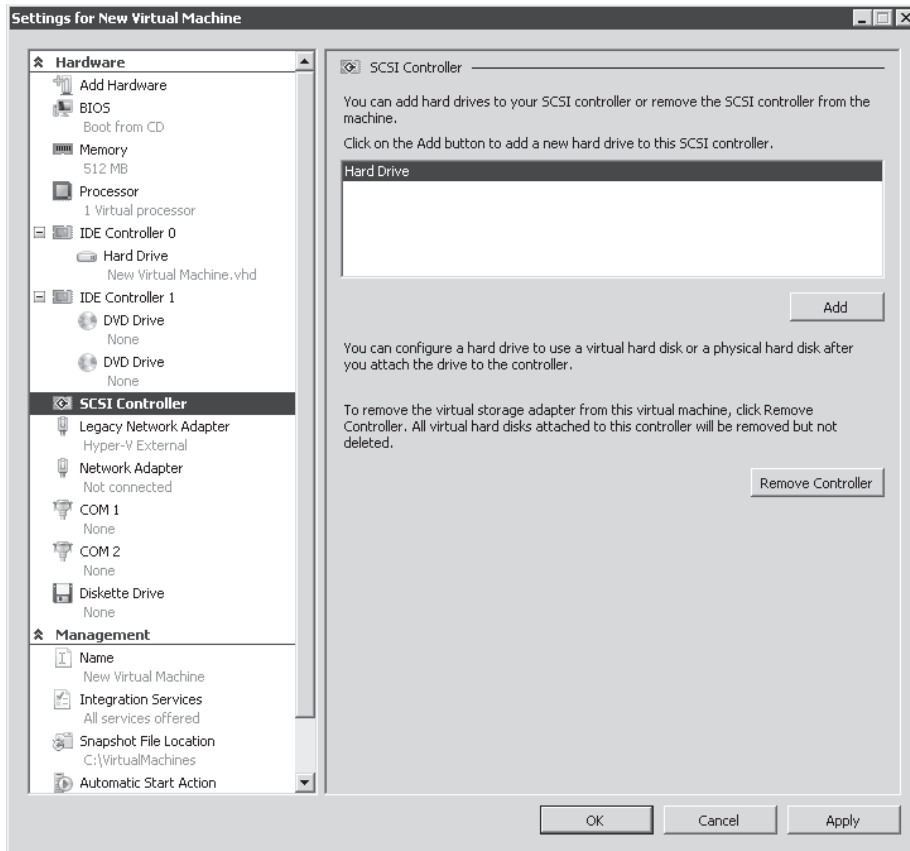


FIGURE 4-17 Adding a SCSI Controller to a VM

IMPORTANT NETWORK ADAPTERS AND VIRTUAL NETWORK ADAPTERS

Note that you also use the Add Hardware option in the VM Settings dialog box to add either network adapters or legacy network adapters. Remember that you can add up to 8 network adapters and 4 legacy network adapters for a total of 12 adapters per VM.

After the hard drive is added, you are given the same choices as when you add a hard drive to a virtual IDE controller. The only difference is the amount of possible locations for the drive because Hyper-V's virtual SCSI controllers support up to 64 locations each (see Figure 4-18).

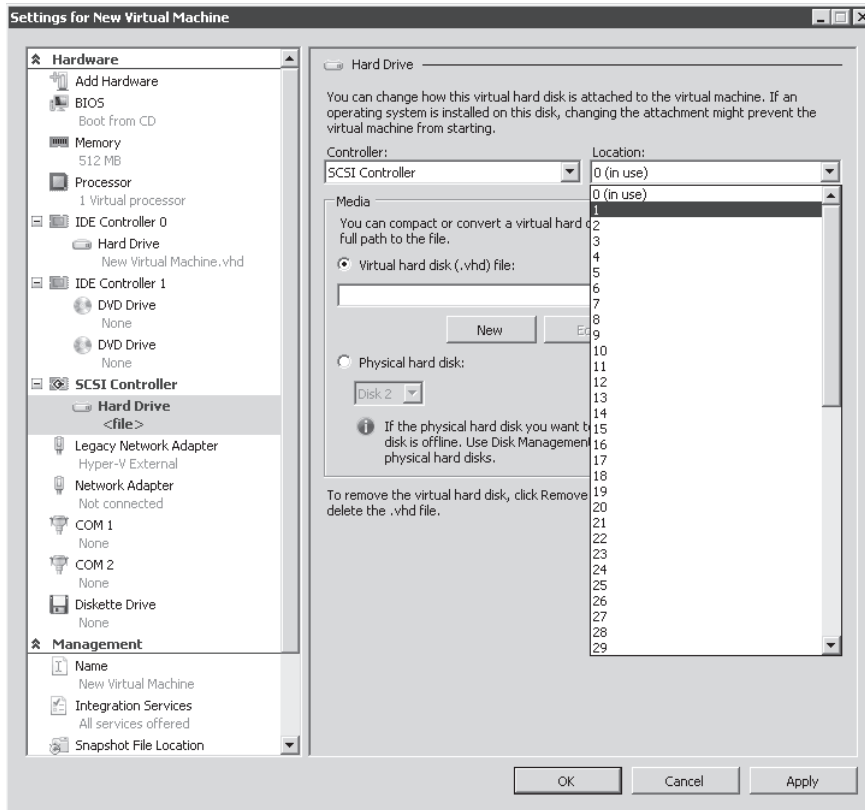


FIGURE 4-18 Choosing the location for a hard drive on a SCSI Controller

Editing a Virtual Hard Disk

Virtual hard disks are much more malleable than physical hard disks or even pass-through disks because they are captured and stored within the VHD file format. The best way to find this out is to use the Edit Disk command in the Actions pane of Hyper-V Manager. Edit Disk is once again a wizard that gives you complete control over a VHD. The wizard's operation will differ based on the type of VHD you are working with. Its operation is simple:

1. Click Edit Disk in the Action pane.
2. Click Next after reading the information on the Before You Begin page.
3. In the Locate Virtual Hard Disk page, type the path to the disk you want to edit or click Browse to select it. Note the warning on this page concerning parent hard disks (see Figure 4-19). As you know, parent hard disks should never be modified or the parent-child relationship will be broken.

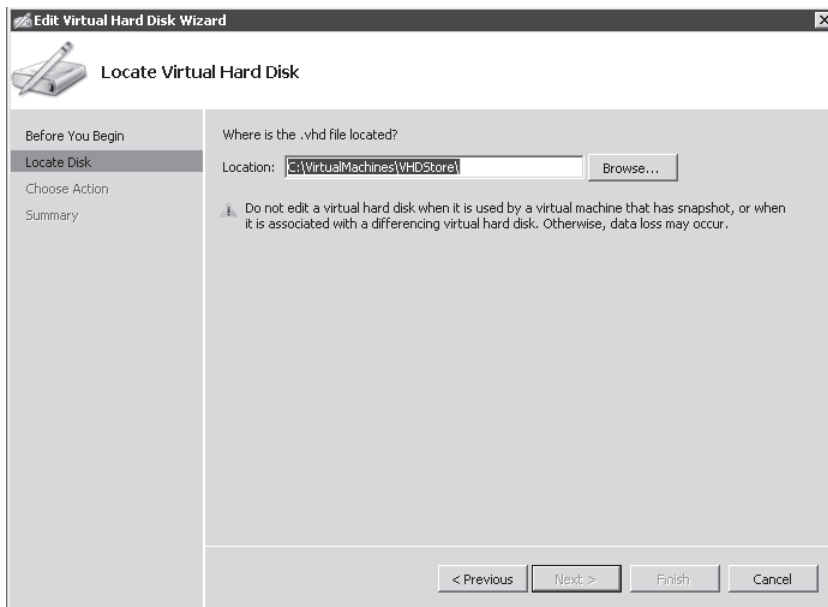


FIGURE 4-19 Parent hard disk modification warning

When you select the type of disk you want to modify, the wizard inspects the selected disk and provides various options based on the results of this inspection. The available options (see Figures 4-20 through 4-24, see pages 252-254) are outlined in Table 4-4.

TABLE 4-4 Edit VHD Options

VHD TYPE	OPTION	DESCRIPTION
Dynamically Expanding Disk	Compact	Shrinks a VHD file by removing blank space that is not removed when you delete content within the disk file. VHDs are much like database files and do not remove space used by deleted data when the data is removed; therefore, you must compact the disk to recover empty space within the VHD file.
	Convert	This converts the VHD file from dynamically expanding to fixed disk size. You must specify the location of the new fixed disk, then Hyper-V copies the contents of the dynamically expanding disk to the new fixed size disk. Note that you must have enough space to store both disks during the conversion.
	Expand	Increases the size of the VHD by a given amount. You must specify the new disk size. By default, Hyper-V sets the new size at 1 GB greater than the current disk size.

VHD TYPE	OPTION	DESCRIPTION
Fixed Size	Convert	This converts the VHD file from fixed size to a dynamically expanding disk. You must specify the location of the new dynamically expanding disk. Hyper-V then copies the contents of the fixed size disk to the new dynamically expanding disk. Note that you must have enough space to store both disks during the conversion.
	Expand	Increases the size of the VHD by a given amount. You must specify the new disk size. By default, Hyper-V sets the new size at 1 GB greater than the current disk size.
Differencing	Compact	Shrinks a VHD file by removing blank space that is not removed when you delete content within the disk file. By default, all child disks are dynamically expanding disks and therefore support the compacting action.
	Merge	Captures the changes from the child disk and merges them into the parent disk or another disk. Changes can be merged to the parent disk, expanding the size of the parent disk. Changes can also be merged to a new, third disk. In this case, you must specify the name and the location of the new disk as well as the type of disk: dynamically expanding or fixed size. Note that you must have enough space to store all three disks during the merge operation.
	Reconnect (see Figure 4-24)	Appears only when a parent-child relationship is broken and lets you reconnect the child with the parent. You must specify the location of the parent VHD during the reconnection.

IMPORTANT COMPACTING NON-NTFS DISKS

When you compact a disk that is in NTFS format, compacting is performed without advanced preparation. But when you compact a disk that uses a format other than NTFS, such as FAT or FAT32, you must use a non-Microsoft disk utility to replace the blank space in the VHD with zeros. The zeros are then removed during compaction. Virtual Server 2005 R2 SP1 includes such a utility even though Hyper-V does not. You can download Virtual Server, uncompress the Virtual Server files, and extract the PreCompact.ISO file from the Virtual Server installation files. Then attach this file to your non-NTFS VHD and run the pre-compaction tool on your hard drive before compacting it. Obtain Virtual Server from Microsoft at <http://technet.microsoft.com/en-us/evalcenter/bb738033.aspx>.

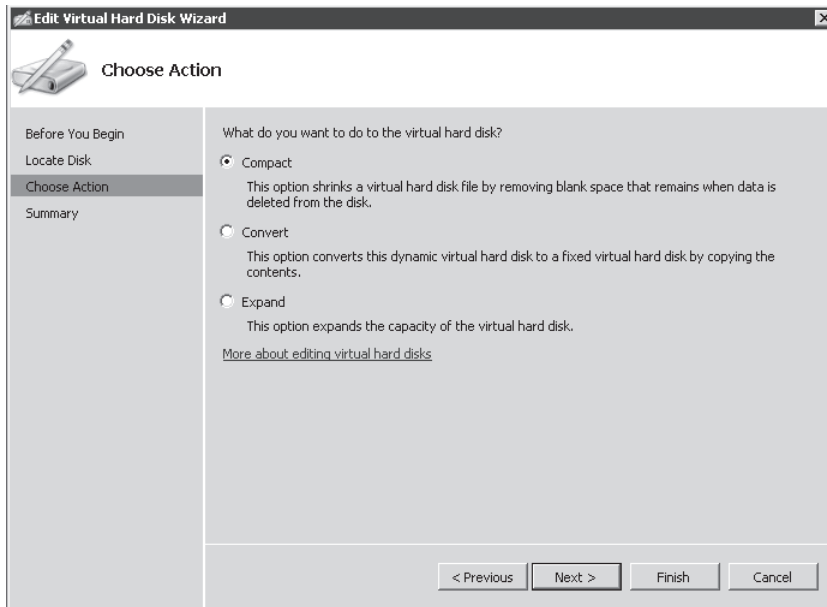


FIGURE 4-20 Available actions for dynamically expanding VHDs

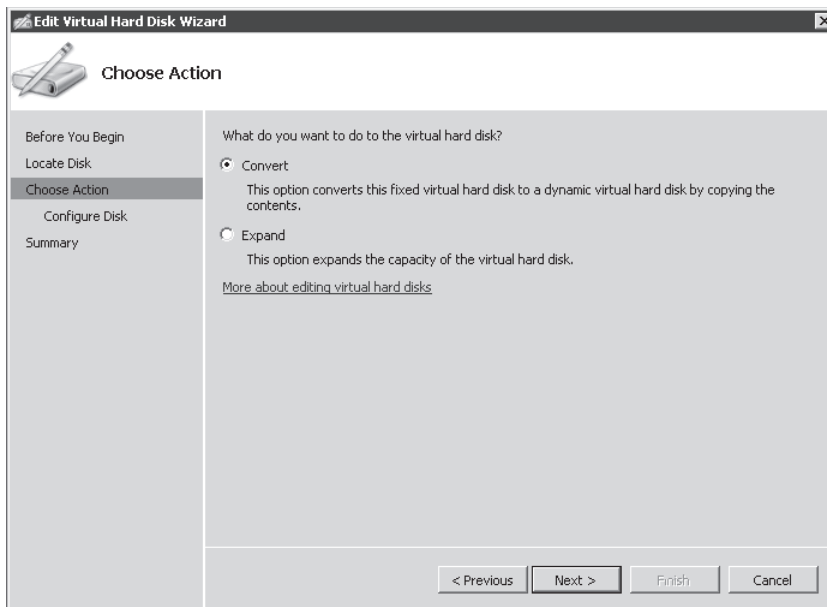


FIGURE 4-21 Available actions for fixed size VHDs

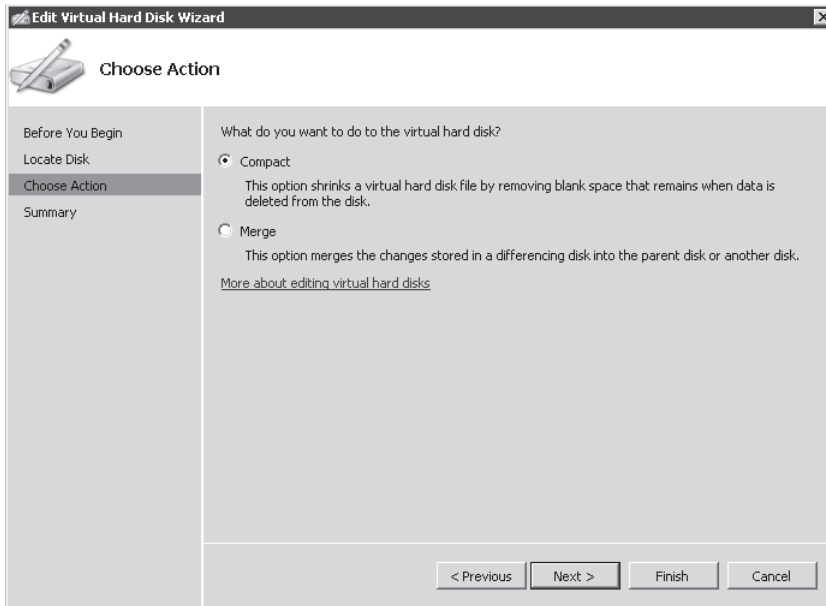


FIGURE 4-22 Available actions for differencing VHDs

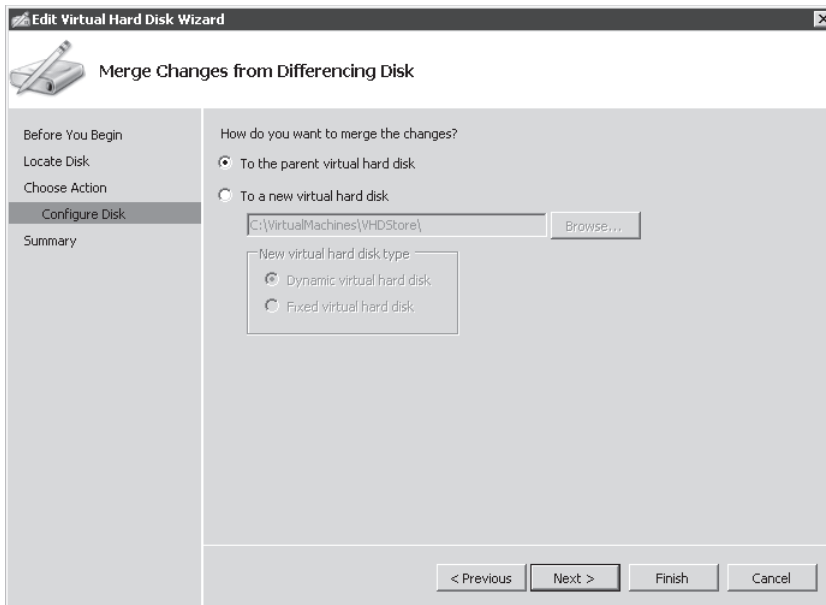


FIGURE 4-23 Choosing merge options

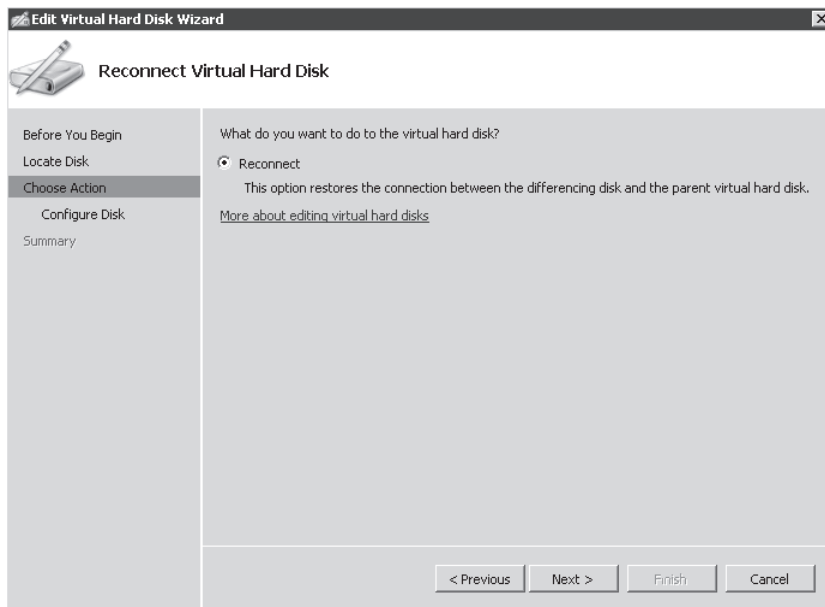


FIGURE 4-24 Reconnecting an orphan child disk

Inspecting a Virtual Hard Disk

In addition to editing VHDs, you have access to a VHD inspection tool. Inspecting VHDs is relatively simple. Note that inspecting can only be used to identify the status of a disk, not to determine whether the disk is working correctly or whether it is possible to repair damage on the disk. To repair a disk, you must use the operating system's own repair tools within the guest operating system in the VM.

Inspection can be performed through the Actions pane in Hyper-V Manager or through the VM Settings dialog box when the VHD is highlighted. The results of the inspection tell you what kind of disk it is and where it is located (see Figure 4-25).

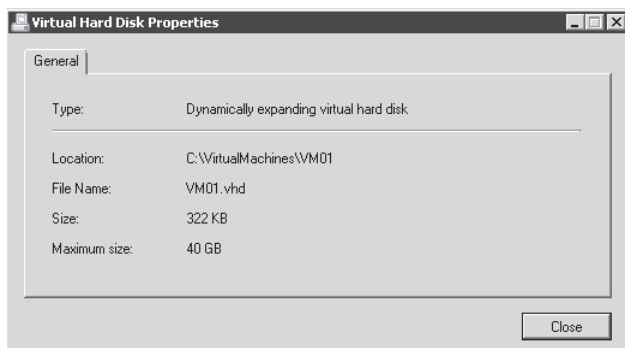


FIGURE 4-25 Inspecting a VHD

Despite the fact that inspection only gives you information about a disk, it is still quite a useful tool because it allows you locate virtual hard disks and identify their status. In resource pools of all sizes, you will find that this tool is very useful when:

- You forget what the original size was of a dynamically expanding VHD file.
- You forget where a VHD is located, especially if it wasn't stored with the VM configuration file.
- You want to know how much space has been used in a dynamically expanding VHD file.
- You want to know to which parent disk a child disk is tied.

In all of these cases, Inspect Disk is often the only answer to your questions.

Working with Hyper-V Snapshots

Virtual machine snapshots are a new feature of Window Server 2008 Hyper-V, as you saw in Chapter 1. As you know, a snapshot is a point-in-time version of a VM. You can take VM snapshots when a VM is running, when it is saved, or when it is stopped. Note that you cannot generate a Hyper-V snapshot of a VM when it is in a paused state.



EXAM TIP CREATING SNAPSHOTS

Remember that you cannot capture a snapshot when a VM is in a paused state.

Each time you take a snapshot, you capture a specific point in time for a VM. For example, when a developer is working with new code and testing the operation of the code, he or she can take snapshots of the VMs running the new application whenever a result is positive. This way, the developer can return to a stable machine state in the event that a test does not work.

Another excellent example of a snapshot process is when an IT professional is performing a complex configuration in a VM. For example, when you install Windows Server 2008, Active Directory Domain Services, Exchange Server, SQL Server, and SharePoint Server in the same VM, you can take snapshots of the VM each time you finish installing and configuring a given component. This way, you can always go back to a given state if configuration errors occur during the process. And then, when the configuration is complete, you can merge all of the changes into a single VHD to have an operating VHD including all of the installed components.

When you revert back to a given snapshot, you revert to an exact point in time for the VM. This means that memory contents, virtual hardware, processes, machine state, and so forth are exactly the same as when you took the snapshot. When a snapshot is generated, it creates a specific set of files, including:

- A copy of the virtual machine configuration .xml file.
- Any save state files (.vsv and .bin).
- A differencing disk—a file with an .avhd extension—which becomes a child to the original VHD for the VM, which in turn becomes the parent for the child disk. The new AVHD file becomes the working disk for all future writes to the VM.

When you create snapshots one after the other without ever applying them, you create a *snapshot hierarchy*, which is a snapshot tree with a single branch. When you apply a snapshot within this hierarchy to revert to a given state in the VM and then generate new snapshots once again, you generate a new branch to the snapshot tree (see Figure 4-26).

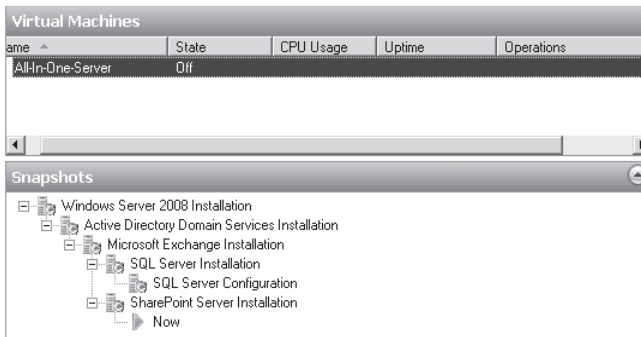


FIGURE 4-26 Working with a complex snapshot hierarchy

Snapshots are stored within the Snapshots folder that is created when you generate a new VM in a specific folder. Each snapshot is stored within a folder named after the GUID assigned to the snapshot (see Figure 4-27). Remember that the original XML configuration file for the VM is stored within the Virtual Machines folder that is also created when you generate a VM. Once again, the configuration file is named with a unique GUID and saved state files are stored within a subfolder of the Virtual Machines folder that uses the same GUID as the original VM configuration filename.

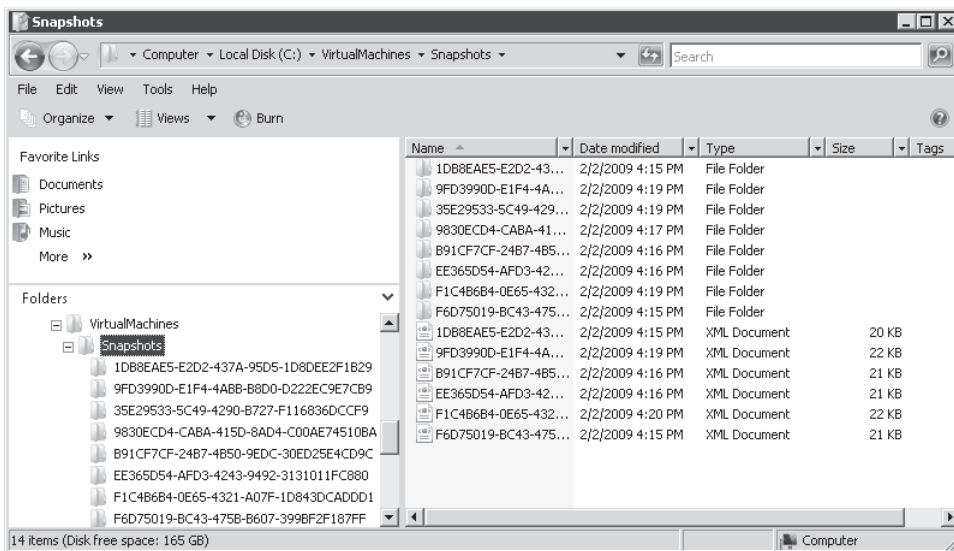


FIGURE 4-27 Examining snapshot file locations

Creating VM Snapshots

You can create a snapshot in two ways: when the virtual machine is running and when the virtual machine is turned off or in a saved state.

When you create a new VM, two subfolders are created in the VM's folder. For example, if you created a VM called VMOne on the D: drive and stored it in a folder named D:\VMOne, the process will create two subfolders to D:\VMOne—D:\VMOne\Snapshots and D:\VMOne\Virtual Machines. D:\VMOne\Snapshots is an empty folder, but D:\VMOne\Virtual Machines contains the original XML configuration file saved with a GUID name and a directory using the same GUID name that will contain potential save state files (.vsv and .bin), which are in-memory files.

Now if you create a snapshot when VMOne is turned off, the following process occurs:

1. Two folders are created in the D:\VMOne\Snapshots folder:
 - VM GUID: a folder that will store all the .avhd files for all the snapshots. Note that this folder creation only occurs for the first snapshot because all future AVHD files will be stored here. These .avhd files are named with the machine name, plus another GUID in the format of MachineName_OtherGUID.avhd.
 - New GUID: a folder that will store the memory save state for this snapshot. In this case, the New GUID folder will be empty since the VM is powered off and there is no memory state.
2. A copy of the VM's .xml configuration file is saved with the New GUID name.
3. An .avhd file is created and is stored in the D:\VMOne\Snapshots\VM GUID folder. This becomes the working .avhd file. This file is named with the machine name, plus another GUID in the format of MachineName_OtherGUID.avhd.
4. A pointer is added to the VM's original .xml configuration file to identify the other GUID .avhd file as the current VHD for the VM.

When you create a snapshot with the VM powered on or if the machine is in a saved state, the exact same process occurs, except that the VM's in-memory state is captured to .vsv and .bin files. These two files are stored within the folder named after the snapshot's GUID.

If you take another snapshot of the VM, the same process occurs except that a new AVHD file is created and this new AVHD file becomes the child to the latest running AVHD and the latest running AVHD becomes its parent. This process is repeated each time a new snapshot is created (see Figure 4-28).

When you choose to apply a snapshot to a VM, the VM reverts to the state captured within the snapshot and a new AVHD file is created. This new AVHD file becomes the child of the .AVHD file you applied and future changes are stored within this AVHD file.

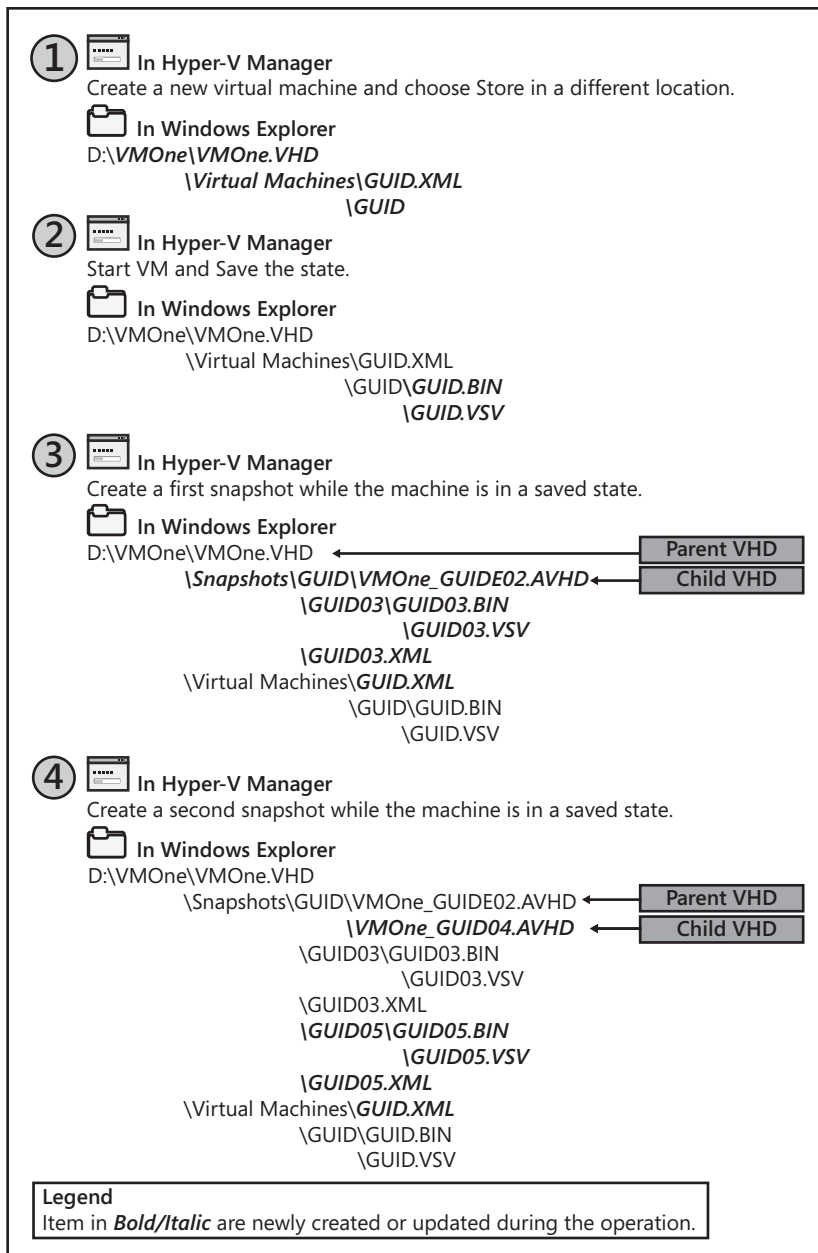


FIGURE 4-28 The snapshot process in Hyper-V

When you revert to the original VM state through the Revert command, the current AVHD file is deleted and a new one is created to capture all changes moving forward. If the snapshot was captured when the machine was running, the saved state files are applied to the VM and the VM is restarted using these files. If the VM was stopped when the snapshot was captured, the VM would remain in a turned off state.

MORE INFO HYPER-V SNAPSHOTS

For more information on working with Hyper-V snapshots, look up the screen cast *Working with Snapshots* at <http://go.techtarget.com/r/5927603/30819>.

IMPORTANT APPLICATIONS AND SNAPSHOTS

Some applications do not support Hyper-V snapshots. In addition, each time you take a snapshot, your VHD is turned into a differencing disk and you can no longer directly modify the parent disk.

PRACTICE Working with VM Disks

In this practice you will work with virtual hard disks. This practice consists of three exercises. In the first, you create a dynamically expanding disk. In the second, you expand the size of this disk to make it larger. In the third, you attach a physical disk to a VM as a pass-through disk. All of the exercises are performed on ServerFull01. You log on with domain administrator credentials to facilitate the exercise even though all you need is Hyper-V administration rights.

EXERCISE 1 Create a Dynamically Expanding Virtual Disk

In this exercise you will create a dynamically expanding disk. This exercise is performed on ServerFull01.

1. Begin by logging on to ServerFull01. Move to Server Manager and then to the Hyper-V Manager node. Select ServerFull01.
2. Move to the Actions pane, select New, and then select Hard Disk. Click Next.
3. Choose Dynamically Expanding and click Next.
4. Name the virtual hard disk **Dynamic.vhd** and store it in a new folder in the root of the C: drive called VHDFiles. Use the Browse button to move to the C: drive, click New Folder, type **VHDFiles**, and press Enter. Click Select Folder and click Next.
5. Set the VHD size to **10** GB and click Finish.

Your new dynamically expanding VHD has been created. Note how little time it takes the wizard to close. Open Windows Explorer (click Start and right-click Computer to select Explore), move to the C:\VHDFiles folder, and examine the size of the new VHD. It should be approximately 82 KB in size. This disk is very small because all it contains is the placeholder for the disk and does not yet contain data.

EXERCISE 2 Expand a Hard Disk

In this exercise you will choose the disk you created in Exercise 1 and expand it. Once again, you perform this exercise on ServerFull01.

1. Return to Server Manager and then to the Hyper-V Manager node. Select ServerFull01.
2. Move to the Actions pane and select Edit Disk. Click Next.
3. Click the Browse button to select the Dynamic.vhd file in C:\VHDFiles. Click Open and then click Next. The system inspects the disk to discover its properties.
4. Click Expand and then click Next.
5. Note that the wizard adds 1 GB to the disk size by default. Change the value to **40 GB** and click Finish.

The wizard closes very quickly once again. Open Windows Explorer (click Start and right-click Computer to select Explore), move to the C:\VHDFiles folder, and examine the size of the modified VHD. It should be approximately 322 KB in size. More data about the disk was added to the file, but it still does not contain any actual data, which is why it is so small.

EXERCISE 3 Connect a Pass-through Disk

In this exercise you will connect an external hard drive to ServerFull01 and use it to create a pass-through disk for one of your VMs. Perform this exercise on ServerFull01. To perform this exercise, you need the second external USB disk as outlined in the requirements in the Introduction.

1. Begin by plugging in your USB disk into a USB port on ServerFull01. Cancel the Autoplay dialog box if it opens.
2. Move to Server Manager and go to the Storage, Disk Management node and click Disk Management. If a dialog box appears to initialize the new volume, click OK.
3. The new disk should appear as Disk 2 and should be online. Right-click Disk 2, not on its partition, and choose Offline. The result should be a blank disk that is offline (see Figure 4-29). The disk is ready to be used in Hyper-V. You set the disk offline to make sure the parent partition does not try to access it while a VM is using it.
4. Move to the Hyper-V Manager node in Server Manager. Make sure ServerFull01 is selected.
5. Select WS08_Full in the Details pane and make sure it is turned off. If not, click Shut Down in the VM section of the Actions pane.
6. Make sure WS08_Full is selected and click Settings in the VM section of the Actions pane. This opens the Settings dialog box.
7. Make sure Add Hardware is selected in the left pane and SCSI Controller is selected in the right pane and click Add. This adds a virtual SCSI controller and moves you to the SCSI Controller section.
8. Click Add to add a new hard drive.
9. Make sure SCSI Controller and 0 (In Use) are selected in the Controller and Location sections of the right pane and click Physical hard disk to select Disk 2 (see Figure 4-30). Click OK to apply your changes. This adds the physical hard drive to the WS08_Full virtual machine as a physical disk connected to the virtual SCSI controller.
10. The disk will appear in the VM when you launch the VM. You can then use the VM's internal tools to format and partition the disk.

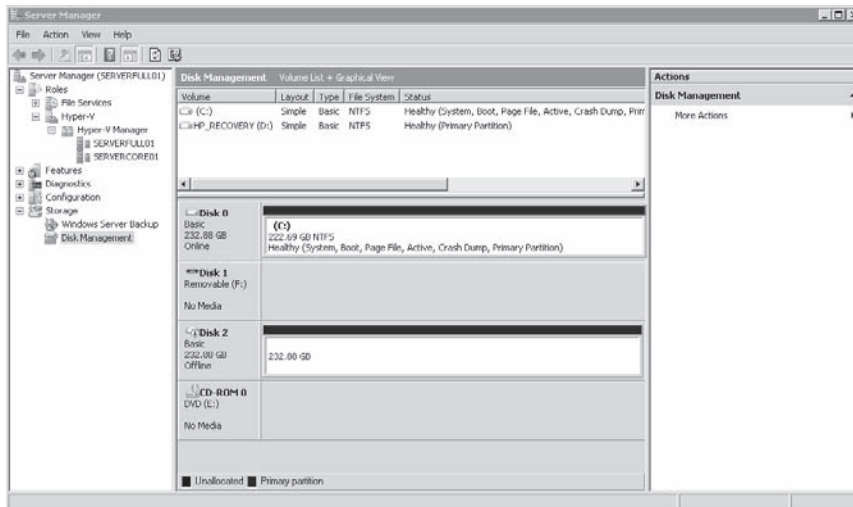


FIGURE 4-29 Setting the disk as offline

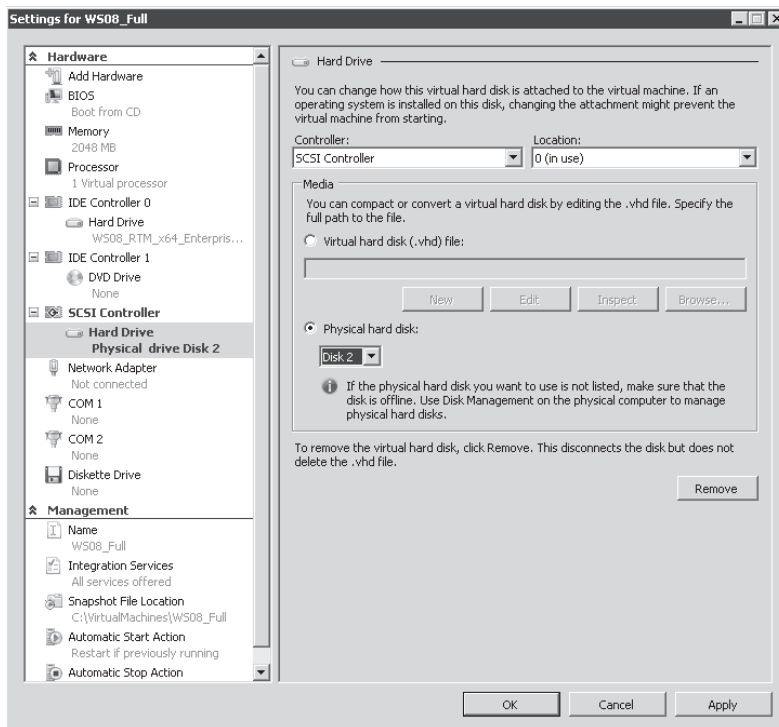


FIGURE 4-30 Attaching a physical hard disk

You have now attached a physical drive to a virtual machine.

✓ Quick Check

1. Into which hard disk partition formats can you store a virtual hard disk?
 - a. FAT format.
 - b. Encrypting File System.
 - c. NTFS format.
 - d. The partition does not need to be formatted.
2. Is it possible to store VHDs in folders that use the Encrypting File System? If not, why?
3. What are the possibilities that you can select to attach disks to VMs?
4. What are the options available when you edit a dynamically expanding virtual hard disk?
5. Which VM state does not allow you to take a snapshot of a virtual machine?

Quick Check Answers

1. The correct answer is C. The partition that stores a virtual hard disk should be formatted with NTFS.
2. You cannot store VHDs in folders that use EFS because EFS is tied to particular users and does not provide high availability because VMS stored within user profiles must run in a single user's context.
3. Three possibilities exist when you want to attach disks to VMs: Integrated Drive Electronics (IDE), Small Computing System Interface (SCSI), and Internet SCSI (iSCSI).
4. When you edit a dynamically expanding virtual hard disk, you have three options: compact, convert, and expand.
5. You cannot take a snapshot when the virtual machine is in a paused state.

Case Scenario: Moving a Virtual Machine

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

Contoso Ltd. has been operating from several different offices around the world for several years, but with the economic downturn, things are tight and Contoso management has had to make some tough decisions. Fortunately, they have focused on reducing expenditures rather than reducing staff. This is why they have decided to close down the London office and relocate all personnel to New York. This also means relocating the London datacenter.

They have asked you, as resource pool administrator, to move your VMs from the London datacenter to the New York datacenter. Most of the virtual machines are straightforward to move because they are nothing but a set of files in a folder. All you have to do is copy them from one location to the other. Of course, it will require considerable bandwidth and time, but it is really a simple operation. However, you are concerned about the custom banking application Contoso uses in London. This VM was created using three pass-through disks linked to a storage area network. Your job is to prepare a plan to migrate this VM from London to New York. During the migration, you may need to change the nature of the VM and management is conscious of that, but they want you to provide the utmost in performance after the move because the VM is running a critical application. Specifically, they want you to answer the following questions:

1. How can you move the pass-through disks?
2. How will the transfer of the complete virtual machine occur?
3. How will you provide the best performance for the VM once it has been moved?

Suggested Practices

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

Creating and Working with VMs

- **Practice 1** Take the time to create basic VMs and then examine the results. It is important to understand the Hyper-V defaults and know what they are.
- **Practice 2** Take the time to work with advanced VM settings. It is important to understand the potential settings you can assign to VMs and know what they are.
- **Practice 3** Work with various VM states. Start, stop, and reset VMs. Save VM states, pause VMs, and restart them. Work to understand each state and its impact on a VM.

Creating and Working with VHDs

- **Practice 1** Take the time to create each type of VHD. Create a dynamically expanding VHD, a fixed size VHD, and a differencing VHD. Name each VHD with the disk type and then examine the results in Windows Explorer. You'll need to create a parent VHD before you create a differencing VHD. Name each parent and child to understand their relationship.
- **Practice 2** Spend considerable time with VHD snapshots. The snapshot process is a complex process and requires thorough examination in preparation for the exam. Create multiple snapshots from one VM with it in all three states: started, stopped, and saved. Examine the results each time in Windows Explorer. Apply one of the snapshots and continue the snapshot creation process. Make sure you understand this process fully before you take the exam.

Chapter Summary

- Hyper-V can run several different operating systems including the newest versions of Windows and special editions of Linux that have been updated to interact with it through Hypercall Adapter. In addition, Hyper-V includes Integration Services to provide additional capabilities to operating systems that are aware of the virtual environment.
- Hyper-V provides Linux Integration Components to enhance Linux operating system performance when installed in Hyper-V child partitions.
- Hyper-V can run legacy guests such as DOS, Windows 3.x, Windows NT, and others. Legacy virtual machines are older Windows operating systems or new non-Windows non-Hyper-V-aware operating systems.
- You must use the Hyper-V Input Release Key with a legacy guest operating system to exit from a Virtual Machine Connection because these operating systems do not support Integration Services.
- To create a basic virtual machine you use the New Virtual Machine Wizard. The new virtual machine includes several default settings:
 - 512 MB of RAM
 - One processor with no reserve
 - One hard drive connection and one DVD drive connection
 - One virtual hard disk (.vhd) file
 - Two COM ports
 - One diskette drive

- Virtual machines have several advanced configuration settings that can be modified or controlled through the VM's settings. Most of the setting changes require the machine to be turned off.
- Virtual machines can have a variety of states, and they can be controlled by selecting the virtual machine and applying the appropriate command in Hyper-V Manager.
- There are three virtual hard disk (VHD) types: dynamically expanding, fixed size, and differencing. These three types can be stored in direct-attached storage (DAS), network-attached storage (NAS), or storage area networks (SAN).
- VHDs cannot be stored in a folder using EFS, but can be stored on partitions that use BitLocker for added security issues.
- When you create a VHD using the New Virtual Machine Wizard you have three options: Create A Virtual Hard Disk, Use An Existing Virtual Hard Disk, or Attach A Virtual Hard Disk Later.
- A snapshot of a virtual machine creates a set of files that includes a copy of the VM configuration .xml file, any save state files (.vsv and .bin), and a differencing disk with an .avhd extension. You can create a snapshot when the virtual machine is running or when the virtual machine is powered off or in a saved state.

Automating Virtual Machine Creation

The great advantage of working with virtual machines is that they can be deployed on an as-needed basis almost in the blink of an eye. Because most virtual machines are nothing but a set of files in a folder—this includes any VM that uses VHDs and excludes VMs using pass-through disks—duplicating a VM is really as easy as copying the files that make it up and booting the new VM. Of course, if you do not want an exact duplicate of a VM, you must prepare the guest operating system through tools such as the Windows System Preparation Tool (SysPrep.exe) to depersonalize the new copy. But overall, this process can take as little as twenty minutes. Compare that to the physical machine creation process: you must first initiate the acquisition process, configure the hardware when it comes in, and then use a physical deployment strategy to put the server in place. Physical server deployments can easily take weeks, whereas virtual server deployment can take minutes (see Figure 5-1).

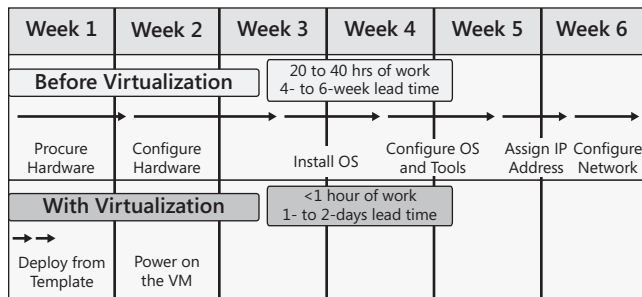


FIGURE 5-1 Deployment timeframes: physical machines vs. virtual machine

This is why virtual machine management and operation fully support the dynamic datacenter model. If you can respond in minutes to a new business requirement, you can dynamically provide IT services to respond to changing business conditions.

In addition, virtual machines can be much more volatile than physical machines. You can spin up a virtual machine to meet a peak in business requirements and then turn it off or simply destroy it once the need has been met. For example, if your business has seasonal fluctuations, you can create virtual machines that run desktop operating systems to support temporary employees when they come in and simply make the VMs disappear once the

seasonal flux is over. A good example of this is a governmental revenue agency that requires hundreds, if not thousands, of temporary employees come tax time, but that no longer needs these employees once all income tax returns have been filed.

Using virtual machine management automation, you can even power up new server VMs to support peaks in Web site access and then destroy them once the peak is over, all through automated processes that simply respond when performance measurements meet specific thresholds. This is the power of virtual machine management in dynamic datacenters.

But to move on to dynamic virtual machine management, you need both the proper tools and the proper processes. This is the gist of this chapter.



EXAM TIP COVERED EXAMS

Remember that 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.

Exam objectives in this chapter:

- Manage templates, profile, and the image library by using SCVMM.
- Create or clone a virtual machine.

Before You Begin

To complete this chapter, you must have:

- Ideally, access to a setup as described in the Introduction. In this chapter, you will begin to work with SCVMM in earnest, and to do so you must have access to the hardware required to support host servers and VM automation.

Lesson 1: Exploring System Center Virtual Machine Manager

System Center Virtual Machine Manager is a very powerful resource pool and virtual service offering management tool. It provides support for VM creation automation and host server management.

After this lesson, you will understand:

- The SCVMM user interface (UI).
- The Hyper-V through SCVMM.
- The SCVMM add-ons.

Estimated lesson time: 35 minutes

Working with Hyper-V Through SCVMM

You installed SCVMM in Chapter 3, “Completing Resource Pool Configurations.” This is where you learned how powerful this tool could be to manage Hyper-V and other server virtualization hosts. The central tool for host server management with SCVMM is the SCVMM Administrator Console. This console provides several management capabilities when linked to Hyper-V:

- You can use it to deploy virtual machines regardless of the host server they will reside on.
- You can use it to convert physical machines into virtual machines (P2V).
- You can use it to convert virtual machines in a non-Hyper-V format into Hyper-V virtual machines (V2V).
- You can use it to manage virtual machines regardless of the host the VM is located on, as long as the host has been added to the SCVMM resource pool (see Figure 5-2).
- You can use it to view the status of virtual machines, regardless of host.
- You can use it to manage template virtual machines that can be used as sources for new VMs.
- You can use it to regroup the components you need to generate new VMs and install guest operating systems within them through the SCVMM Library.
- You can use it to assign tasks to other members of your organization. For example, you can delegate SCVMM tasks to other members of the IT group through the Administrator Console. Or you can use it to delegate tasks to non-IT personnel through the Self-Service Portal.

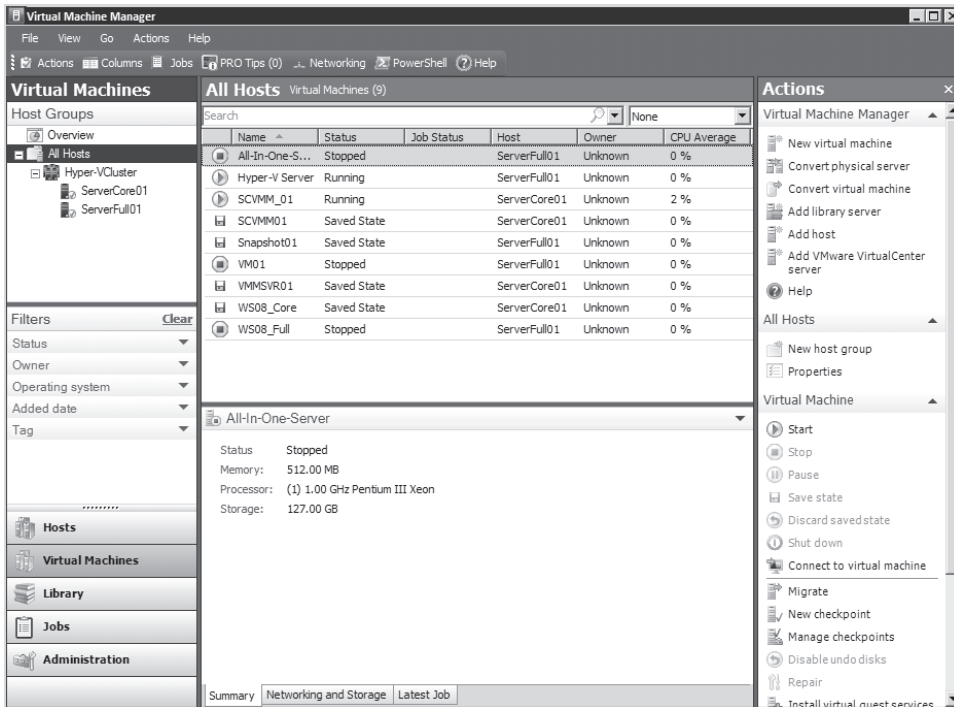


FIGURE 5-2 Working with multiple VMs in SCVMM

As you can see, the SCVMM Administrator Console offers more functionality than the Hyper-V Manager Console. Whereas Hyper-V Manager only lets you work with one host server at a time, the SCVMM Administrator Console lets you work with resource pools as a whole even beyond the 16 possible nodes in a Hyper-V Failover Cluster. SCVMM supports the management of hundreds of host servers and thousands of VMs if you need it. This is one reason why the SCVMM Administrator Console includes filters. Filters let you quickly sift through thousands of systems to focus on the ones you need to work with at the time.

When you install SCVMM and the SCVMM Administrator Console, specific executives are installed within the %ProgramFiles%\Microsoft System Center Virtual Machine Manager 2008\Bin folder. They include:

- **VMMAdmin.exe** The engine for the console itself. This is the controller engine that can call upon all of the different console engines. Different console engines are used to access virtual machines from Hyper-V, Virtual Server 2005 R2 SP1, and VMware ESX Server or VMware Virtual Infrastructure. This engine also includes a Virtual Machine Remote Control ActiveX Control (VMRCActiveXClient.dll), which is used to view what is happening in a VM from within the console. This Dynamic-Link Library (DLL) is used to display the thumbnail of the VM within the console. Note that this DLL does not allow you to interact with the VM, it will only view what is happening within the VM.

- **VirtualMachineViewer.exe** The engine used to open a remote control session on a virtual machine running in a Hyper-V environment. This viewer relies on the Terminal Services ActiveX Control (MSTSCAX.dll) to open a Remote Desktop Connection to interact with virtual machines running on servers using Hyper-V. You'll remember that this communication relies on port 2179. This engine is called upon automatically when you launch a remote session on a machine running on Hyper-V, but you can also use it through the command line with one of the following command structures:

```
virtualmachineviewer.exe /host Hostname
```

```
virtualmachineviewer.exe /computername VirtualMachineName
```

For more information on the various switches you can use with the Virtual Machine Viewer command, use the following command (see Figure 5-3):

```
virtualmachineviewer.exe /?
```

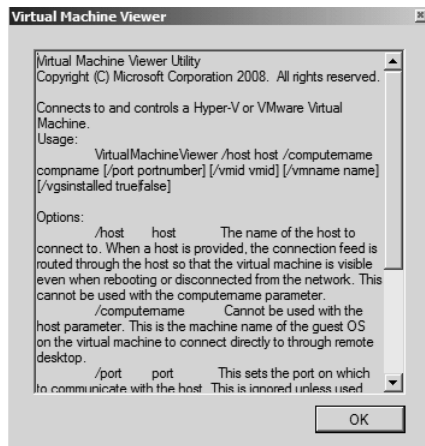


FIGURE 5-3 Finding out more information on the Virtual Machine Viewer command

- **VMRC.exe** The engine used to open a remote connection to a virtual machine running on Virtual Server 2005 R2 SP1. The Virtual Machine Remote Control process relies on the Virtual Network Computing (VNC) protocol to connect to VMs running on Virtual Server. You can also launch this command directly using the following structure:

```
vmrc.exe HostURL
```

For more information on the various switches you can use with the Virtual Machine Remote Control command, use the following command (see Figure 5-4):

```
vmrc.exe /?
```

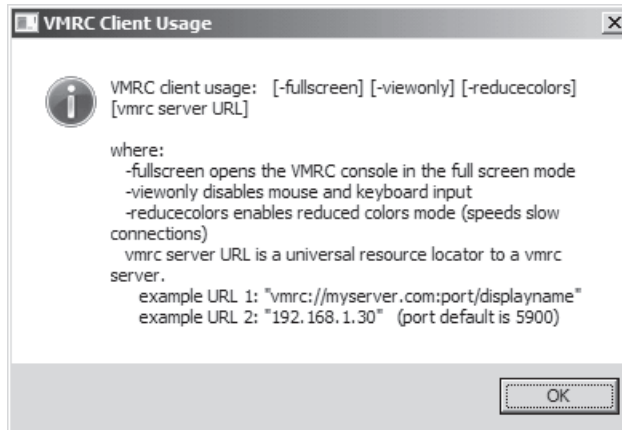


FIGURE 5-4 Finding out more information on the Virtual Machine Remote Control command



EXAM TIP MANAGING VIRTUAL SERVER HOSTS

One great advantage of being able to manage Virtual Server hosts with SCVMM is that you can give extended life to x86 physical machines or x64 machines whose processors do not include hardware-assisted virtualization because Virtual Server also runs on 32-bit operating systems. When it runs on 64-bit systems, it does not have the same requirements as Hyper-V. Remember, however, that Virtual Server can only create and run 32-bit VMs.

- **VMwareViewer.exe** The engine used to open a remote connection to a VM running on VMware ESX or ESXi. The VMware Viewer Process relies on the VMware WebCenter Remote MKS Plug-in control to open a remote console to the VM.

If you intend to use either the Virtual Machine Viewer or the Virtual Machine Remote Control tools through the command line, you should consider adding the C:\Program Files\Microsoft System Center Virtual Machine Manager\Bin folder in the path of the machine you use to run the SCVMM Administrator Console. Use the following procedure to do so:

1. Click Start, right-click Computer, and choose Properties.
2. Click Advanced System Settings on the left side of the Computer Properties window. Accept the UAC prompt if it appears.
3. Click Environment Variables on the Advanced tab of System Properties.
4. Select Path in the lower section of the dialog box and click Edit.
5. Press the End key to move to the end of the current path string and type **;"C:\Program Files\Microsoft System Center Virtual Machine Manager 2008\Bin"** (see Figure 5-5). Click OK twice. You use the leading semi-colon to separate this folder from other folders in the path string; you use quotation marks because this folder name includes spaces. Close all Control Panel windows.

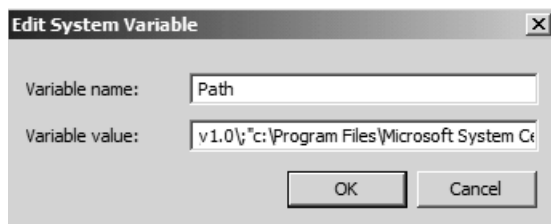


FIGURE 5-5 Adding the SCVMM Bin folder to the path string

The Bin folder is added to the current path string. You can now type either the VMRC.exe or the VirtualMachineViewer.exe command at any prompt and have it work properly.

Exploring the SCVMM Administrator Console User Interface

You use the SCVMM Administrator Console to interact with the SCVMM Server and manage both host servers and the virtual machines they run. Because the console is an independent component, you can install it on a wide variety of platforms. In fact, although you should install it on the server in case you need to work interactively on the server and want to use SCVMM, you should also install the console on your administrative systems, preferably workstations, so that you can interact with the Server without having to open a Remote Desktop Connection. Table 5-1 outlines the various supported operating systems for the installation of the Administrator Console.

TABLE 5-1 Supported Platforms for the SCVMM Console

PLATFORM
Windows Server 2008 with Hyper-V x64 Standard, Enterprise, and Datacenter editions
Windows Server 2008 without Hyper-V x64 Standard, Enterprise, and Datacenter editions
Windows Server 2008 without Hyper-V x86 Standard, Enterprise, and Datacenter editions
Windows Server 2003 x86 with Service Pack 2 Standard, Enterprise, and Datacenter editions
Windows Server 2003 x64 with Service Pack 2 Standard, Enterprise, and Datacenter editions
Windows Server 2003 x86 R2 with Service Pack 2 Standard, Enterprise, and Datacenter editions
Windows Server 2003 x64 R2 with Service Pack 2 Standard, Enterprise, and Datacenter editions
Windows Vista with Service Pack 1
Windows XP Professional x86 with Service Pack 2 or 3
Windows XP Professional x64 with Service Pack 2

Note that the Console can only be installed on Full Installations of Windows Server 2008.

Once installed, the console uses Port 8100 to communicate with the SCVMM Server whether the communication is local or remote. Once you connect to the SCVMM Server, you are presented with several different views within the console (see Figure 5-6).

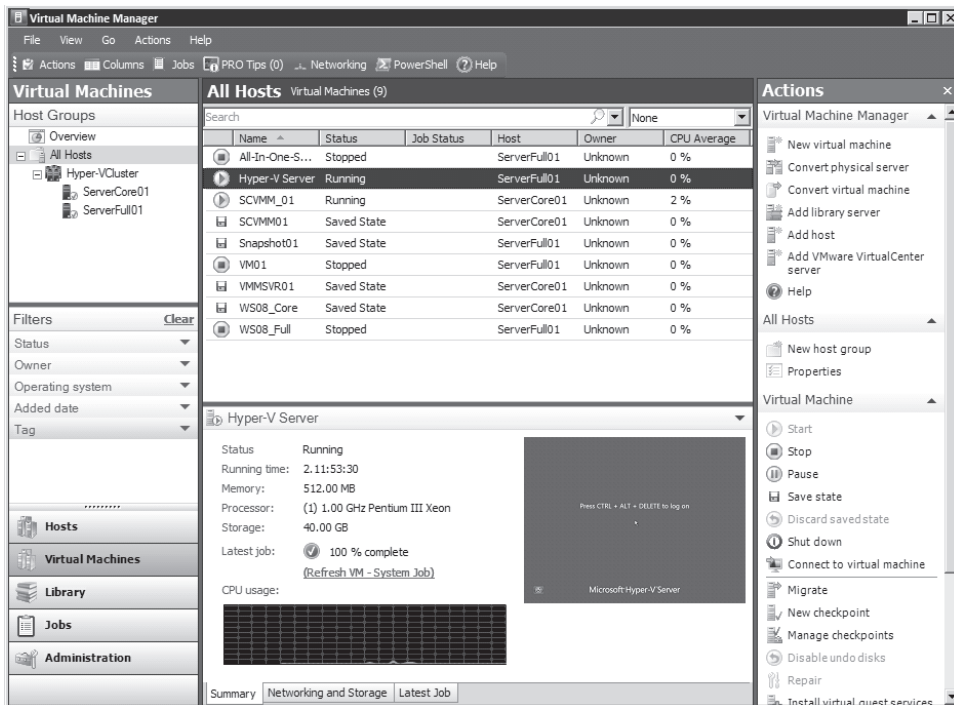


FIGURE 5-6 The SCVMM Administrator Console in Virtual Machines view

Once again, this console uses the standard Microsoft Management Console version 3 structure, which is made up of Tree, Details, and Actions panes. In addition, it uses the standard System Center management tools console structure. Each of the three panes includes the following:

- The Tree pane includes three sections:
 - The top portion lists the name of the current view and the tree structure of the available nodes in this view.
 - The middle portion gives you access to filters. Although you might not use these filters when your resource pool consists of 2 host servers and 10 virtual machines, these filters become extremely useful when you manage hundreds of hosts and thousands of virtual machines because they reduce the amount of information displayed in the Details pane.
 - The bottom portion controls which view is currently active. You change views by clicking the view name in this section of the Tree pane.

- The Details pane includes two sections:
 - The top portion displays the results of a combination of the selected view along with any filter you have applied. If no filter is applied, you see all of the results of this current view.
 - The bottom section displays pertinent information about the selected object in the top portion.
- The Actions pane also includes three sections:
 - The top portion displays commands related to the host server. This is the Virtual Machine Manager (VMM) section. The VMM contents change based on whether the host is running Hyper-V, Virtual Server, or VMware ESX Server.
 - The middle portion displays commands related to the type of object displayed within the current view in the Tree pane. If the object type is a host server, host server commands are displayed. If the object type is a VM or the Library, appropriate commands are displayed and so on.
 - The bottom portion displays commands based on sub-objects controlled by the object type in the selected view. For example, if the object type is the Library, this section displays commands that apply to virtual hard disks. If the object type is Virtual Machines, the commands apply to VMs.

Take the time to explore the different views available in the SCVMM Administrator Console and examine the changes in the console when you change the view. You'll find that several different operations are available through this console interface. Table 5-2 outlines the different operations you can perform based on the view type.

TABLE 5-2 Available Operations Based on Selected View

VIEW	OPERATIONS
Hosts	■ Add or remove hosts. ■ View host status. ■ Configure virtual networks. ■ Configure virtual machine placement options. ■ Configure VM paths. ■ Configure host server properties. ■ Register existing VMs on a host. ■ Access existing VMs through remote connections. ■ Create or delete host groups. ■ Monitor and manage hosts through host groups. ■ Configure host reserves. ■ Configure self-service policies for a given host group.

VIEW	OPERATIONS
Virtual Machines	■ Create or delete virtual machines. ■ Deploy VMs from templates. ■ Connect to and operate a VM. ■ Clone a VM. ■ Migrate a VM from one host to another. ■ Repair a VM. ■ Store a VM in a given storage container. ■ Create checkpoints for a VM. Checkpoints in SCVMM are like Hyper-V Snapshots and capture the state of a VM at a given time.
Library	■ Control library resources. ■ Add or remove ISO files. ■ Add or remove executables in support of VM creation and configuration. ■ Add or remove shares to the Library. ■ Add or remove additional Library servers. ■ Control the Library Index by refreshing the contents of a Library. If no manual refresh is performed, the Library is automatically re-indexed every hour by default. ■ Create, configure, or remove guest operating system profiles. ■ Create, configure, or remove hardware profiles. ■ Create, configure, or remove virtual machine templates.
Jobs	■ Monitor jobs. ■ Sort, filter, or group jobs. ■ Search through existing jobs. ■ Cancel or restart a job. ■ View job results.
Administration	This view includes several subviews: ■ Overview Provides a graphical summary of all of the components managed by SCVMM. ■ General Configures SCVMM Properties. ■ Managed Computers Control SCVMM agents on hosts and Library servers. ■ Networking Provides a view to the Media Address Control (MAC) address range used by SCVMM.

VIEW	OPERATIONS
	■ User Roles View all user roles by profile type. ■ System Center Views reports from System Center Operations Manager (OpsMgr) if it is integrated with SCVMM. ■ Virtualization Managers View available virtualization managers. In SCVMM 2008, two managers are listed. Virtual Machine Manager is used for Hyper-V and Virtual Server. VMware VirtualCenter Server is used for VMware ESX servers.
Reporting View	■ Available only when the OpsMgr reporting feature has been configured to work with SCVMM. ■ View and open OpsMgr reports in SCVMM.
Diagram View	■ Available only once OpsMgr has been configured to work with SCVMM. ■ Display health status for all of the components that make up the SCVMM environment.

As you can see from the items listed in Table 5-2, the SCVMM Administrator Console gives you access to many more controls than Hyper-V Manager can on its own. It also gives you more control than the Failover Clustering Management console does because it can also manage Hyper-V failover clusters as part of the various host groups it can control.

Controlling Hyper-V with SCVMM

When you use SCVMM to manage Hyper-V servers, the Hyper-V systems become managed hosts within the SCVMM infrastructure. Remember that you must deploy SCVMM agents on the Hyper-V hosts just as you would deploy agents on either Virtual Server or VMware ESX hosts.

In Chapter 3, you learned that you could regroup Hyper-V hosts into failover clusters to provide high availability for the virtual machines you run. The Failover Clustering feature of Windows Server 2008 lets you regroup up to 16 host servers together into a single resource pool. In addition, the Failover Clustering feature lets you regroup servers in single or multi-site clusters. SCVMM also lets you regroup host servers, but this time in the format of host groups.

Host groups provide a simple, logical way to regroup host servers. SCVMM includes a default host group: All Hosts. This group is created by default because all hosts must belong to a group. Host groups are very useful because they can simplify host purpose identification. For example, even if you use only two types of host servers in your datacenter—production and testing hosts—regrouping them into host groups called Production and Testing makes it very easy for you to quickly identify which host is used for which purpose. Larger organizations will find it useful to create regional or departmental host groups to simplify

both the administration of these hosts and the delegation of host management activities. In more complex environments, you'll find that nesting groups to create host group hierarchies will make it even easier to manage your resource pools.

Adding host groups is as simple as clicking the New Host Group link in the Actions pane under the Hosts view. All new host groups are created under the All Hosts group and are named New Host Group by default. Change the name to a more descriptive term and press Enter to rename the group. To remove a group, right-click the group name and select Delete. A warning will be displayed to tell you that all child host groups will also be deleted (see Figure 5-7). You can also move host groups to nest them into other groups by dragging and dropping the host group to the new location.

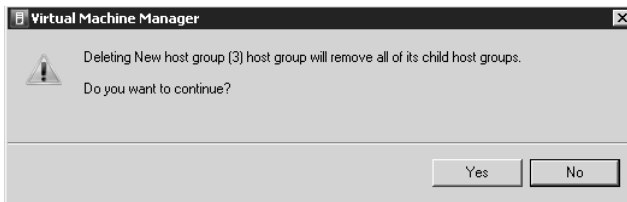


FIGURE 5-7 Confirming a host group deletion

After a new host group is created, you can move existing managed hosts by dragging them into the new host group. New hosts are added through the Add Host Wizard (see Figure 5-8). This wizard will let you add either Hyper-V, Virtual Server, or VMware ESX hosts; however, you need appropriate credentials to perform the operation. Added hosts can be within the Active Directory Domain Services domain to which SCVMM belongs, trusted domains, or in workgroups such as in the case of host servers running in perimeter networks.

When a host is added to an SCVMM group, SCVMM will automatically install the appropriate SCVMM agent on the host. However, you can also pre-deploy the agent using the standalone agent installation package to simplify the host integration process when massive numbers of hosts need to be added at once.

When you remove a host from the managed hosts in SCVMM, SCVMM will automatically remove the agent from the host. In some cases, you have to remove hosts that no longer respond. You can force host removal with Windows PowerShell. This operation is covered in Chapter 7, "Automating Hyper-V with Windows PowerShell."

Host groups include properties that allow you to control how the host group should behave. To access host group properties, click the Properties command in the Actions pane under the Host view after selecting the host group you want to modify. The host group Property dialog box includes three tabs. The General tab provides general information about the group, which is much the same as the information displayed in the Details pane when the group is selected. The Host Reserves tab lets you determine how many physical resources you will reserve for the host (see Figure 5-9).

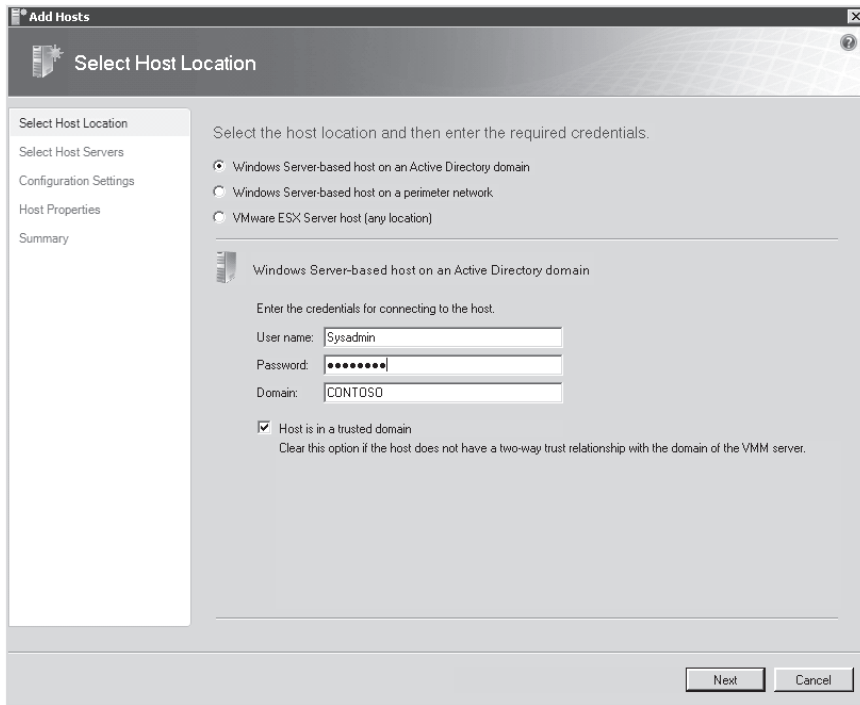


FIGURE 5-8 Using the Add Host Wizard

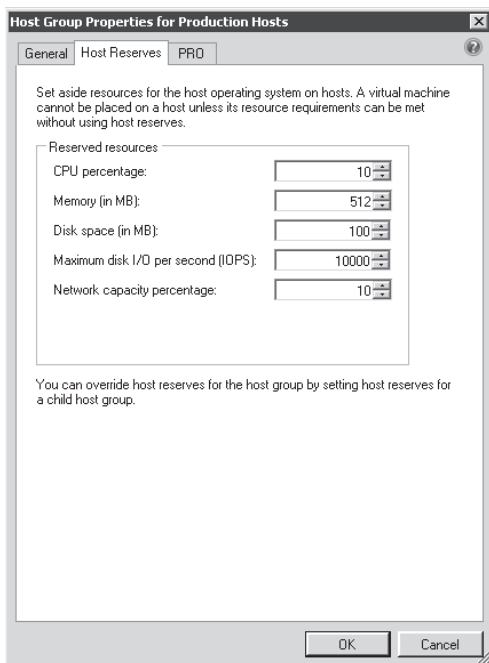


FIGURE 5-9 Configuring host reserves for a host group

In the case of Hyper-V, this is the amount of resources reserved for the parent partition. By default, SCVMM reserves 10 percent of the CPU resources, 512 MB of RAM, 100 MB of disk space, 10,000 Input and Output operations per second (IOPS), and 10 percent of network bandwidth for Hyper-V hosts. The PRO tab controls the behavior of Performance Resource and Optimization (PRO) for the group. PRO is enabled when SCVMM is linked to OpsMgr.

Note that the SCVMM Administrator Console provides access to the same type of commands in regards to hosts that you find in Hyper-V Manager. However, because SCVMM can manage three different kinds of hosts, the terminology used in SCVMM is not quite the same as that used in Hyper-V Manager. For example, in Hyper-V Manager, hosts have settings; in SCVMM, they have properties. In addition, host properties in SCVMM provide control over more properties than the Hyper-V Manager Hyper-V Settings dialog box does. For example, you can determine whether a host is available for VM placement through its properties in SCVMM (see Figure 5-10). If the host requires maintenance, you can set it as not available for placement and SCVMM will automatically exclude it from the available hosts when a new VM is generated.

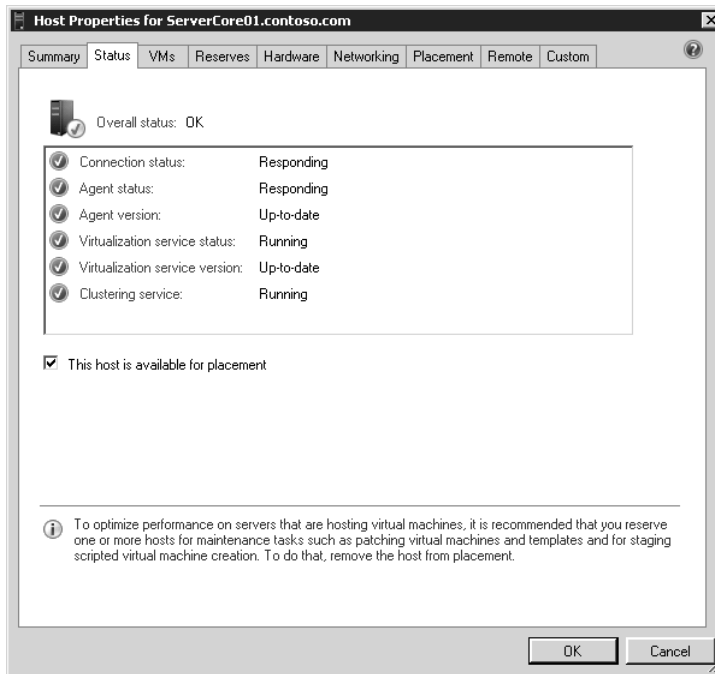


FIGURE 5-10 Viewing host properties in SCVMM

Remote Connections in Hyper-V Manager vs. SCVMM

Opening a remote connection in the SCVMM Administrator Console is performed using the same process as in Hyper-V Manager: just double-click the VM's thumbnail in the Details pane. However, note that the remote connection provided by Hyper-V Manager includes more settings and commands than that provided by SCVMM's Virtual Machine Viewer.

Hyper-V Manager's Virtual Machine Connection includes both a toolbar and a menu bar (see Figure 5-11).

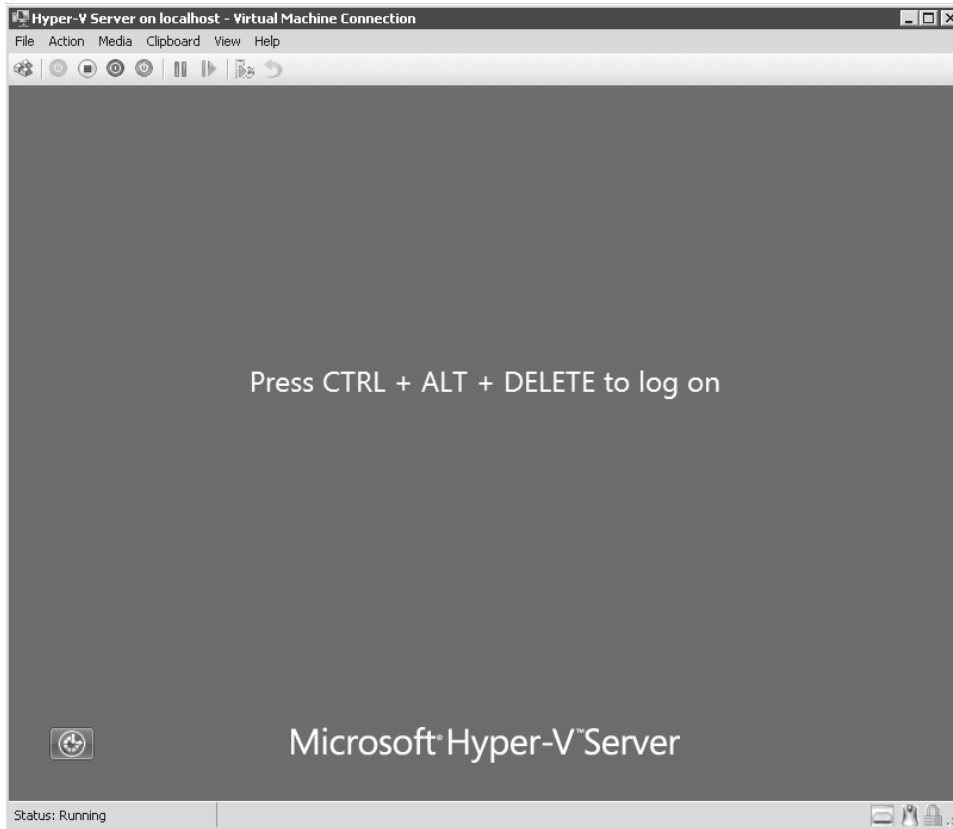


FIGURE 5-11 Using the Virtual Machine Connection in Hyper-V

The toolbar includes many more settings than the one in the Virtual Machine Viewer. The menu bar also includes several commands:

- The File menu gives you access to the VM's settings.
- The Action menu includes all of the items on the toolbar, as well as access to the Insertion of the Integration Services Setup Disk. The Virtual Machine Viewer does not give you access to Integration Services. Instead, you use the SCVMM Administrator Console's Actions pane when the VM is selected to choose Install Virtual Guest Services. Once again, this is because SCVMM manages multiple host platforms.
- The Media menu lets you control access to the virtual diskette drive and the virtual DVD drive for the VM.
- The Clipboard menu lets you capture text or screen images from the VM.
- The View menu controls the display of the toolbar as well as the change from windowed to FULL SCREEN mode.
- The Help menu gives you access to help related to the Virtual Machine Connection tool.

These items are not the same in the Virtual Machine Viewer. In fact, this connection window only includes two menus: File and Action and two items on the toolbar (see Figure 5-12).

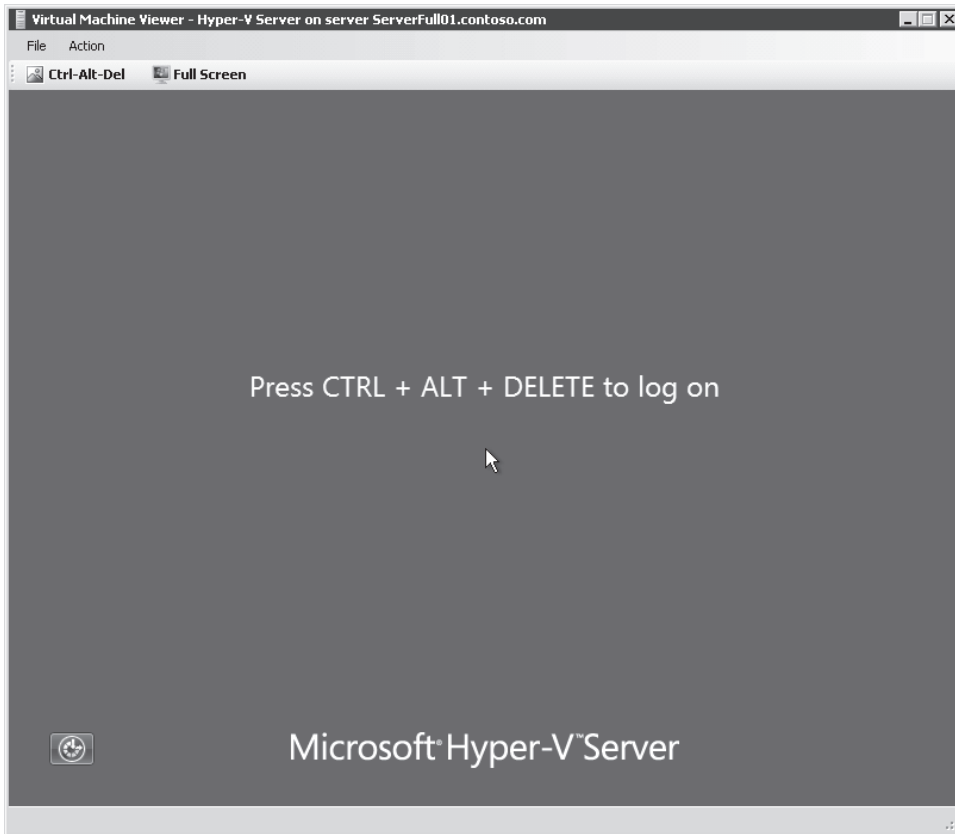


FIGURE 5-12 Using the Virtual Machine Viewer in SCVMM

In each case, only a single connection can be made to the virtual machine. Each time you connect from either Hyper-V Manager or SCVMM, the other connection is cancelled if it already exists. In addition, the thumbnail in the SCVMM Administrator Console is disconnected and can no longer be viewed by other administrators. You must click the Reconnect link in the bottom part of the Details pane to view the VM's thumbnail again.

Differences also exist in virtual machine properties. When you view a virtual machine's properties in SCVMM, you will see that the dialog box is laid out in a different manner than the similar dialog box in Hyper-V Manager. Yet a little exploration of the settings in the dialog boxes will quickly show you that you still have access to the same options and parameters that you did in Hyper-V Manager.

However, there is one significant difference between Hyper-V Manager and SCVMM. Because SCVMM relies on an agent to work with a host server, the Host Properties dialog box will display information that the agent collects from the host machine and transmits to the SCVMM Server.

You'll find the Host Properties dialog box under the Status tab (see Figure 5-10 again). Several different status values can be displayed in each of the categories listed in this tab. Table 5-3 outlines the possible values and their impact on host management.

TABLE 5-3 Host Status Values

STATUS CATEGORY	VALUE	DESCRIPTION
Overall	OK	There are no issues with the host.
	OK (Limited)	Applies to VMware ESX servers only and occurs when additional credentials and security certificates are required to support full control of the host.
	Needs Attention	An issue exists with the host.
Connection Status	Responding	Communications are operating normally.
	Not Responding	Communications between the host and the server are down.
	Access Denied	The VMM Agent is not associated with this server anymore.
Agent Version	Up-to-date	The Agent is OK.
	Upgrade Available	The versions of the server and the Agent are out of synch.
	Unsupported	The Agent does not work with this version of the server.
Virtualization Service Status	Running	The hypervisor is started.
	Stopped	The hypervisor is stopped.
Virtualization Service Version	Up-to-date	The hypervisor version is OK.
	Upgrade Available	The versions of the server and the hypervisor are out of synch and updates must be installed on the host.
	Unsupported	The hypervisor does not work with this version of the server.

Another major difference is the availability of filters within the SCVMM Administrator Console. Filters reduce the number of results displayed in the Details pane when the Host, Virtual Machine, Library, or Jobs views are selected. Filters are predefined and will vary based on the type of object available in the selected view. To enable a filter, simply select the check box for the filter. For example, to view all running virtual machines in the resource pool, proceed as follows:

1. Click Virtual Machines in the Tree pane to enable the Virtual Machines View.
2. Click the Status Filter list in the Filters section of the Tree pane.
3. Select the Running filter. This will filter the VMs listed in the Details pane and display only running VMs.

You can use multiple filters together—just select more filters. To clear all filters, click the Clear link in the Filters section.



EXAM TIP THE SCVMM ADMINISTRATOR CONSOLE

Take the time to explore every aspect of the SCVMM Administrator Console as it is an important part of the exam.



EXAM TIP USING FILTERS

Filters are useful to reduce the number of items displayed in the Details pane; however, they can also limit what you see. For example, if you are working in the Library and you are looking for a specific type of object but cannot locate it, check to see whether any filters are enabled. Clearing all filters will let you see all objects.

Managing the SCVMM Library

The SCVMM Library is a special data store that will include the components you need to generate and build new virtual machines. The Library is, in fact, a managed shared folder that is controlled through the SCVMM Server. The Library can be installed on a number of different Windows Server platforms. Table 5-4 outlines which server operating systems support the Library role.

TABLE 5-4 Supported Platforms for the SCVMM Library

PLATFORM
Windows Server 2008 with Hyper-V x64 Standard, Enterprise, and Datacenter editions
Windows Server 2008 without Hyper-V x64 Standard, Enterprise, and Datacenter editions
Windows Server 2008 without Hyper-V x86 Standard, Enterprise, and Datacenter editions
Server Core installations of Windows Server 2008
Windows Server 2003 x86 with Service Pack 2 Standard, Enterprise, and Datacenter editions
Windows Server 2003 x64 with Service Pack 2 Standard, Enterprise, and Datacenter editions
Windows Server 2003 x86 R2 with Service Pack 2 Standard, Enterprise, and Datacenter editions
Windows Server 2003 x64 R2 with Service Pack 2 Standard, Enterprise, and Datacenter editions

The Library acts as a catalog that hosts file-based resources. These resources include ISO images, virtual hard disks, virtual machine templates, installation scripts, unattended installation answer files, and any other file object that can be used in support of virtual machine and guest operating system deployment. Although most objects are stored within

the file system, some, such as guest operating system and hardware profiles, are stored within the SCVMM database yet are still accessed through the Library.

Remember that a Library Server is automatically installed when you install the SCVMM Server. By default this Library Server is installed in the %SystemRoot%\ProgramData\Virtual Machine Library Files folder, but this path can be changed at installation. This default Library is shared as MSSCVMMLibrary wherever it is actually located. When this Library is created, it automatically includes two blank VHDs: Blank Disk Small (16 GB) and Blank Disk Large (60 GB). Both are dynamically expanding VHDs and are stored within the VHDs folder under the library share.

When you work with the Library, you create additional subfolders to store different types of file-based resources. For example, you might create a new folder called ISOStore to store all of the ISOs you need to install both the operating systems and the applications you will run within your virtual machines. You can do the same for custom Windows PowerShell scripts, unattended installation files, source virtual machines, and more.

Because each SCVMM Server is also a Library Server by default, you should make sure you include at least two disks in the server configuration. This way, you can store the Library on a separate spindle from the operating system partition that will host the SCVMM service. Library objects such as VHDs and ISO files can be quite large in nature and will impact the SCVMM Server performance if they are stored on the same partition or even on the same spindles.

Ideally, you will store the Library Server on the same shared storage container—usually a storage area network (SAN)—as the virtual machines you run. This way, you can use SAN duplication speeds to duplicate VHDs when you create new virtual machines from stored virtual hard disk drives. In addition, because a Library Server is mostly a managed file share, you can host it on servers running the Windows Server Failover Clustering feature to make sure that the Library remains highly available at all times.

You can add new Library Servers at any time. However, because Library Servers rely on file shares to provide access to the file-based resources they store, you should take the time to create the folder structure and the shares you want to use before you add the server as a Library Server.

Use the following procedure to add a new Library Server once the shares have been created:

1. Click Add Library in the Actions pane under the Virtual Machine Manager section.
2. Begin by entering the credentials required to add the server. You must have local administrative rights on the target server or cluster to add it as a Library Server.
3. Type in the name of the server you want to add and click Add. SCVMM will perform an Active Directory Domain Services lookup to locate the server name you enter. Add all of the servers you want to include.
4. Select the shares you want to use (see Figure 5-13). These shares should have been prepared previously. Select all applicable shares.
5. Complete the operation.

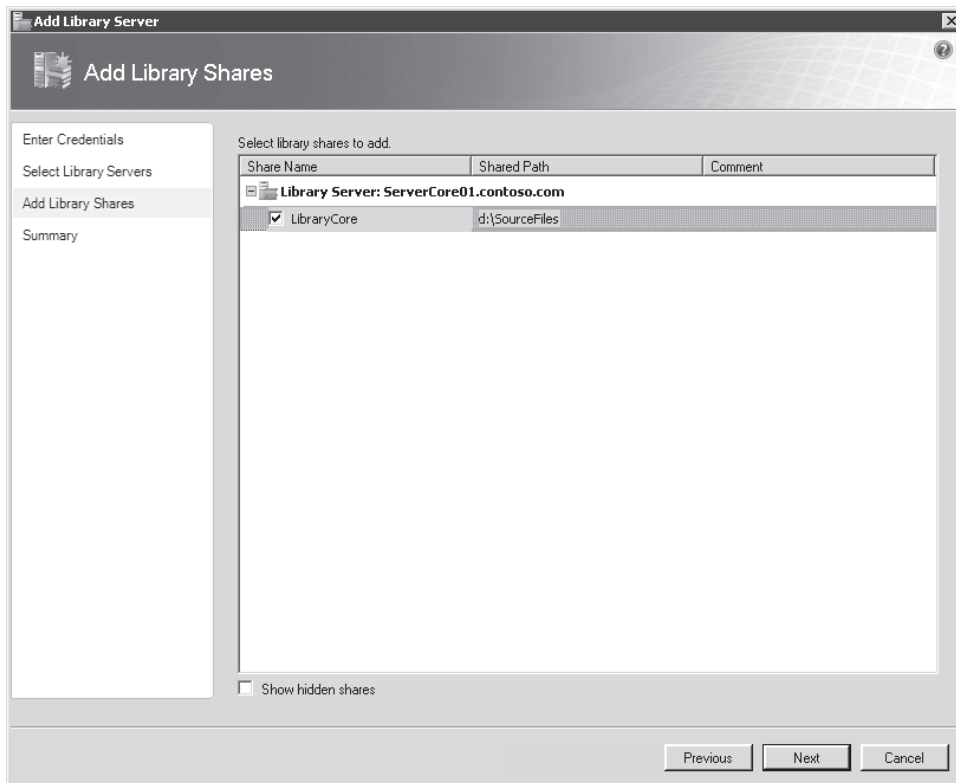


FIGURE 5-13 Selecting shares on the new Library Server

Note that the last page of the wizard displays a View Script button. When you click this button, SCVMM will display the Windows PowerShell script it will use to perform the operation (see Figure 5-14). The advantage of using a tool that is built on Windows PowerShell is that it always generates a script to perform an operation. If you copy the script and save it to a new location, you can later use it as the basis for a completely automated operation that repeats the operation you just performed. This is scripting without needing to know how to program. This is perhaps one of the most powerful features of SCVMM.

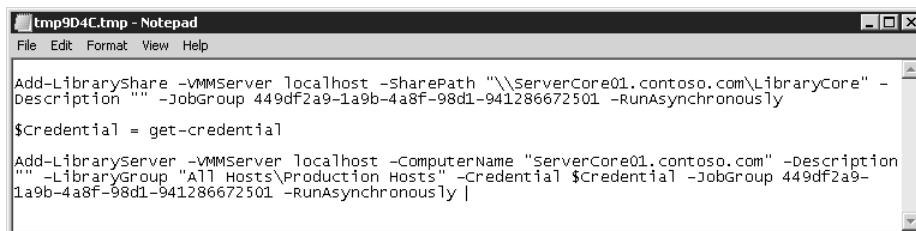


FIGURE 5-14 Viewing the Windows PowerShell Script

When the wizard closes, the Jobs window will automatically open to display the progress of the operation you just completed (see Figure 5-15). You can close this window after the operation has been completed by SCVMM. You can also view job results by clicking the Job view.

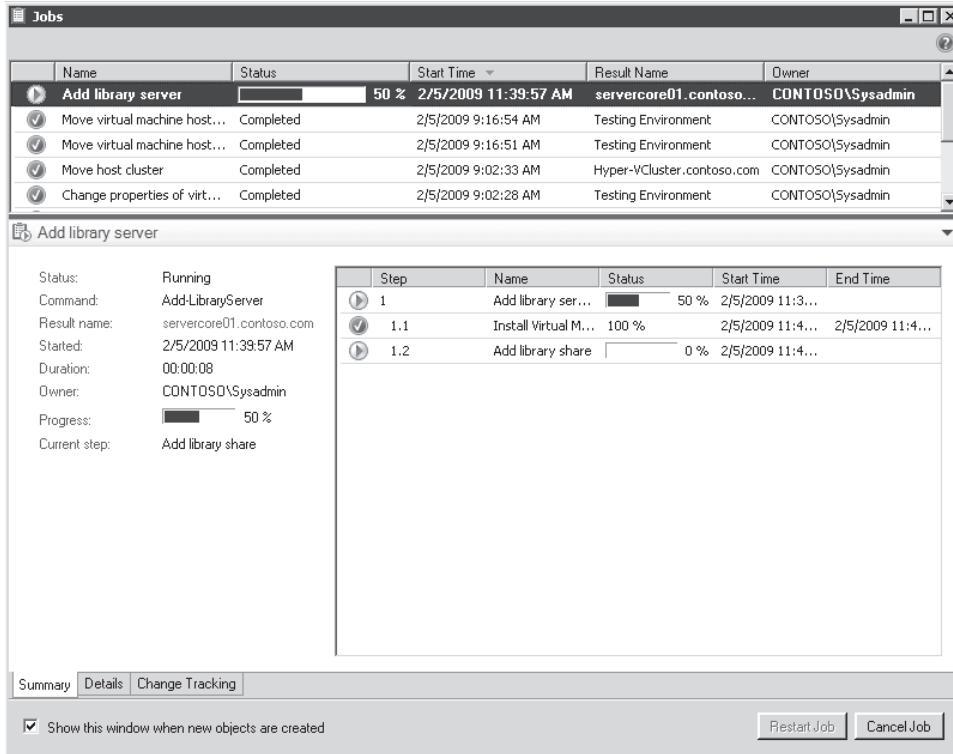


FIGURE 5-15 Viewing the job status

Note that once again, SCVMM will create two blank VHDs in the new Library Server.

Managing Library Contents

You use the Administrator Console to manage Library contents. Although the Library is mostly a file share, it should not be managed through Windows Explorer because many of the items you create within the Library are linked together. For example, to generate a new VM, you need five items:

- A source VHD that may already contain a guest operating system.
- A guest operating system profile that will act as the information source for the configuration of the guest operating system.
- A hardware profile that will act as the source for the new VM's settings.
- An automated operating system configuration answer file that will serve to personalize the guest operating system.
- A VM template that brings together the various components required for the creation of the new VM.

If you delete or move any of these items through the Windows Explorer, the others may break and will require repair. However, if you make a modification through the Administrator Console, the consistency of the object links will remain intact and the objects will continue to work.

When you work with Library contents, you will work with the following file types:

- **ISO Image Files** ISO files are images that most often include installation components for either an operating system or an application. Microsoft provides all of its products in ISO format. ISO files use a .iso extension. These files are indexed by SCVMM.
- **Virtual Hard Disks** SCVMM stores and indexes virtual hard disks in both Microsoft (.vhd) and VMware (.vmdk) format.
- **Virtual Floppy Disks** SCVMM stores and indexes virtual floppy disks in both Microsoft (.vfd) and VMware (.flp) format.
- **Scripts** SCVMM stores and indexes Windows PowerShell (.ps1).
- **Answer Files** SCVMM stores and indexes unattended installation answer files (either .inf or .xml format).
- **VMware Templates** SCVMM stores and indexes templates in the VMware (.vmtx) format.
- **SCVMM Templates** SCVMM stores and indexes virtual machine templates. Templates are depersonalized VMs that are used as sources for the generation of new VMs. Templates can be captured from existing VMs or created from scratch. Templates can be composed of several files: ISO images, scripts, answer files, virtual hard disks, and virtual floppy disks.
- **Guest Operating System Profiles** SCVMM stores and indexes guest operating system profiles. Guest operating system profiles contain the configuration of a guest operating system when installed in a new VM. These profiles can be composed of two file types: scripts and answer files.
- **Hardware Profiles** SCVMM stores and indexes hardware profiles. Hardware profiles contain the configuration settings for new VMs. These profiles can contain two file types: ISO images or virtual floppy disks.

In addition, the Library will store the following file types but will not make them available as resources because they are tied to specific VMs:

- **Virtual Machines** SCVMM stores and indexes complete virtual machines. These machines can include configuration files, virtual floppy disks, or virtual hard disks. Note, however, that the files that make up VMs are not displayed in the Library because they are tied to a specific VM.
- **Hyper-V VMs** Additional files can be included in Hyper-V VMs. These include the export format for a VM configuration (.exp) and the saved state files for a VM (.vsv and .bin).
- **Virtual Server VMs** Additional files can be included in Virtual Server VMs. These include the VM configuration file (.vmc) and the saved state file (.vsv).
- **VMware VMs** Additional files can be included in VMware VMs. These include the VM configuration file (.vmx) and the export format for a VM configuration (.vmtx).

Although your Library will most likely not include all of these formats, it will certainly include at least one template, one guest operating system profile, and one hardware profile. It may also include several source VHDs. And, depending on your organization's requirements, you might include templates for different virtual machine types. In large organizations, you might consider including preconfigured VMs for several different types of machines. In fact, any machine that supports the installation of an application and then the depersonalization of the machine image could be included in your system templates. This could include anything from a generic Windows Server 2008 machine to a Web server, a SQL server, a Windows Deployment Services (WDS) server, a machine with the Active Directory Domain Services role installed but not configured, and so on. By having these VMs preconfigured but depersonalized through the System Preparation Tool, you can quickly deploy a new VM with a given role whenever your organization requires it.

Be careful, however, of VM sprawl! Just because you can deploy a new VM within 20 minutes does not mean you need to proliferate VMs. The reason you are moving to virtualization is in support of physical server consolidation, so don't make the mistake of generating too many VMs just because they are easy to create. Continue to use a proper administrative authorization process for all machines, both virtual and physical, and you will control the number of systems you run in your datacenter.

Working with SCVMM Add-Ons

Because SCVMM is a tool you can use to both manage and deploy virtual machines, you'll find yourself working with SCVMM add-ons—add-ons that are designed to support the new machine creation process. In fact, SCVMM includes one add-on and can work with another:

- **The Windows Automated Installation Kit (WAIK)** The WAIK included in SCVMM is automatically installed when you deploy a SCVMM Server. This tool is composed of a series of utilities that support automated installation of Windows operating systems.
- **Windows Deployment Services (WDS)** WDS is a role in Windows Server 2008 that is designed to support the remote deployment of operating systems. It includes both an operating system image management component and a multicast deployment component. The latter supports the deployment of an operating system image through a single stream of data to multiple endpoints.

Both tools are used when you need to deploy massive numbers of servers. In fact, both tools can support the deployment of either physical hosts running the Hyper-V role and virtual machines running any Windows Server 2008 role.

MORE INFO AUTOMATING VIRTUAL MACHINE AND HOST DEPLOYMENT

For an excellent overview of how both tools can be used to install both hosts and VMs with assigned roles, look up "Automating Virtual Machine and Host Deployment" at <http://technet.microsoft.com/en-us/magazine/2009.02.hyperv.aspx>.

Working with the Windows Automated Installation Kit

The WAIK includes a set of utilities in support of Windows operating system deployment, including:

- **Windows System Image Manager (Windows SIM)** Windows SIM is used to build and customize automated installation answer files, which provide installation and configuration settings as the installation is performed. Answer files are created on a source computer and then transferred to the reference computer before its system image is captured. The startup file for this tool is called `ImgMgr.exe` and is located in the Image Manager folder of the `%ProgramFiles%\Windows AIK\Tools` folder.
- **Windows Preinstallation Environment (WinPE)** WinPE is a short-lived operating system that has only a 72-hour duration at any given time—it can only run for a maximum of 72 hours at a time, though it can be rebooted any number of times—and includes a limited set of services. However, it does not require installation and can run from various removable media. WinPE is aimed at preinstallation and deployment of Windows Vista and Windows Server 2008. WinPE is included in the PETools folder of the `%ProgramFiles%\Windows AIK\Tools` folder. You must use the `PEImg.exe` tool to build a WinPE image for the hardware platform you are targeting (x86 or x64).
- **ImageX** ImageX is a command-line tool that supports the creation and manipulation of system images for installation and deployment. Use `ImageX.exe` in the appropriate folder for the hardware platform you are targeting under the `%ProgramFiles%\Windows AIK\Tools` folder. Use AMD64 for x64 systems, x86 for x86 systems, and IA64 for Itanium systems. Note that only the ADM64 or the x86 versions apply to virtual machines.
- **System Preparation Tool (SysPrep.exe)** The Windows Server 2008, Windows Vista, and Windows 7 System Preparation Tool is not actually part of the WAIK because it is now located in both the Windows Vista and the Windows Server 2008 operating systems, but it is necessary to depersonalize a system image for replication to multiple computers or servers. Note that the WAIK includes a version of this tool for use with older versions of Windows. Look to the `%SystemRoot%\System32\SysPrep` folder to locate the tool on Windows Vista and Windows Server 2008 in both x86 and x64 installations.

These tools will be useful as you generate new VMs through SCVMM.

Working with Windows Deployment Services

Windows Server 2008 includes a core operating system deployment technology: Windows Deployment Services (WDS). WDS can be used for both servers and workstations. WDS relies on the use of a Preboot Execution Environment (PXE) network card. This means that you can start a new machine that does not include an operating system, press F12 during the boot sequence, boot from the network interface adapter, and select the operating system to install from the menu choices that have been previously prepared with WDS. WDS works in both Windows Server 2008 and in Windows Server 2003, replacing a previous role Windows Server 2003 included called Remote Installation Services (RIS). WDS is a role in Windows Server 2008, but must be downloaded for Windows Server 2003. In addition, RIS must be installed on Windows Server 2003 and then upgraded to WDS.

Remote installation is a very promising automated installation method because it provides the ability to install Windows operating systems on bare metal machines—both virtual and physical. WDS can also repair a faulty operating system installation.

Both RIS and WDS require a significant infrastructure to run. They need a working Active Directory Domain Services to provide authorization for the service in a domain, as well as a Dynamic Host Configuration Protocol (DHCP) server to provide automatic IP addressing during the system installation process. Once these services are in place, you can rely on the WDS process to deploy servers.

The WDS process is made up of four major stages:

- Installing the WDS role and preparing the WDS server
- Preparing system images on the WDS server
- Preparing answer files for use with WDS (if required)
- Deploying WDS system images

Once these tasks are complete, you will be able to support remote deployments of Windows Server 2008 and Windows Vista as well as other Windows operating systems.

MORE INFO UPGRADING RIS TO WDS

If you already have a Windows Server 2003 network in place, you already have the required infrastructure for this service. In this case, look up how to upgrade your RIS servers to WDS on the Microsoft Web site at <http://technet2.microsoft.com/WindowsVista/en/library/9e197135-6711-4c20-bfad-fc80fc2151301033.mspx?mfr=true>.

MORE INFO WINDOWS SERVER DEPLOYMENT GUIDANCE

Microsoft has released guidance that helps you step through the Windows server installation and deployment process. Look for this guidance on the Microsoft Windows Server 2008 Web site at <http://www.microsoft.com/windowsserver2008/default.mspx>.

WDS works with Windows PE to deploy operating systems to bare-metal machines. Because WDS uses the boot sequence of a network card to contact the machine to be staged, it must supply this machine with an IP address, much in the way DHCP does. Because of this, WDS must also be authorized in Active Directory Domain Services to function.

Installing WDS

Because it is a network infrastructure service, WDS requires certain components to be present before it can be installed and configured. These include:

- Active Directory Domain Services, which is already installed.
- DNS, which is part of the installation of each DC in your network.
- DHCP, which is also already deployed.
- NTFS partitions, which should be the only partition type you use on your servers.

Like other roles, WDS is installed through Server Manager via the following steps:

1. Select the Windows Deployment Services role and click Next.
2. Now select the services for the role. WDS includes two services: Deployment Server and Transport Server. Deployment Server includes the full functionality of WDS. Transport Server includes only a subset and is useful for large networks, where you need to transport data from a central location to remote offices. For example, this service would be available in the remote office to support system image deployment across the WAN. Because this is the first server in the network, select both services.
3. Click Install to perform the installation.

You're ready to begin working with WDS.

MORE INFO WDS ROLE INSTALLATION

For more information on deploying this role, go to <http://go.microsoft.com/fwlink/?linkid=84628>.

Working with WDS

You can work with WDS in one of two ways: with the Windows Deployment Services Configuration Wizard or through the WDSUTIL.exe command. When you configure WDS, you need to:

- Create a shared folder that contains the following files:
 - Files needed for PXE boot
 - Files for booting Windows PE into a RAM disk
 - Windows PE boot images
 - System images for Windows Vista or Windows Server 2008
- Upload system images of Windows Vista, Windows Server 2008, Windows Server 2003, or Windows XP in Windows Imaging Format (WIM) format.
- Configure the settings for the PXE listener to control how the server services incoming client boot requests.

Here's how to proceed:

1. Launch the WDS console once the role is installed. Click Start, then Administrative Tools, and then Windows Deployment Services.
2. Expand the nodes in the left pane once the console is open, right-click the server name, and select Configure Server from the shortcut menu.
3. On the Remote Installation Folder Location page, type the path to the shared folder containing system images—for example, **D:\RemoteInstall**.
4. If your WDS server is also a DHCP server, you must select the two options in the next screen: Do Not Listen On Port 67 and Configure DHCP Option Tag 60 To 'PXEClient'.

5. Configure your PXE listener options. Ideally, you will select Respond Only To Known Clients. This means you will need to pre-stage all computer accounts in Active Directory Domain Services before you can use WDS to deploy system images to them. Clear the Add Images option and click Finish.

Your server is ready. You can add images and learn to use WDS when you need to work with PC system image deployment.

PRACTICE Working with the SCVMM Library

In this practice, you will create a new Library Server and begin to populate its contents with the components you use to generate new VMs. This practice consists of five exercises. In the first exercise, you install a new Library Server. In the second exercise, you populate the server with a new ISO file. In the third exercise, you use the newly downloaded ISO file to create an unattended installation file for Windows Server 2008. In the fourth exercise, you use this file to create a new guest operating system profile. In the fifth exercise, you create a new Hardware Profile.

EXERCISE 1 Create a New Library Share and Add a New Library Server

In this exercise you will create a new share on ServerCore01 and use it to create a new Library Server. This exercise is performed on ServerCore01, ServerFull01, and SCVMM01. You will use domain administrator credentials in all cases to facilitate the exercise.

1. Begin by logging on to ServerCore01. In Exercise 4 of Lesson 2 in Chapter 3, you created a new folder called SourceFiles on the external disk you added to this server. You will now share this folder and grant everyone full permissions to the share.
2. Type the following command in ServerCore01:

```
net share LibraryCore=d:\SourceFiles /Grant:Everyone,Fu1l
```
3. The result should be a new shared folder called LibraryCore. Move to ServerFull01.
4. In Server Manager, move to the Hyper-V Manager node and make sure ServerCore01 is selected. If the SCVMM01 virtual machine is not running, start it. Double-click the SCVMM01 thumbnail once the machine is started.
5. Log on to SCVMM01 and launch the SCVMM Administrator Console if it is not already started. Click the Library view.
6. Click Add Library Server in the Actions pane. This launches the Add Library Server Wizard.
7. Type in your credentials. Your logon information should already be displayed and you should only need to type your password. Click Next.
8. Type in **ServerCore01** and click Add. SCVMM will display a message noting that this server is part of a cluster and ask if you want to continue adding it as a single node (see Figure 5-16). Click Yes and then click Next.

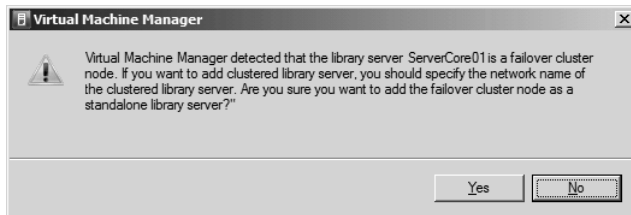


FIGURE 5-16 Adding only one node of a cluster as a Library Server

9. Click LibraryCore as the share to use and click Next.
10. Review the summary of your operation. You can click View Script to open a Notepad window with the Windows PowerShell script that will be used. Click Add Library Servers when ready.

The Jobs window will open and display the actions SCVMM is undertaking. Close the window when the operation is complete.

EXERCISE 2 Download and Store a Windows Server 2008 ISO File

In this exercise you will download an ISO image of the Windows Server 2008 installation DVD and store it in your new Library Server. Perform this exercise from SCVMM01.

1. In the SCVMM Administrator Console, select the new Library Share you added. Right-click the Library Share and click Explore. This opens Windows Explorer and puts the focus on the \\ServerCore01\\LibraryCore share.
2. Right-click in the Details pane and select New, and then Folder. Name the folder **ISOStore** and press Enter. Minimize Windows Explorer.
3. Open Internet Explorer and type **Windows Server 2008 Evaluation ISO** in the search bar. Press Enter. Click Yes to send the information over the Internet. Close all of the warning dialog boxes. Click the second download link on the page listing Download Details: Windows Server 2008 Enterprise. This link should be <http://www.microsoft.com/downloads/details.aspx?FamilyID=13C7300E-935C-415A-A79C-538E933D5424&displaylang=en>. Close all warning dialog boxes.
4. Move to the bottom of the page and click Download beside the first link, which should be 2539.9 MB in size. This is the AMD64 version of Windows Server 2008. Click Add to add Download.Microsoft.com to your trusted sites and click Add again. Click Close and then click the Download link again.
5. Click Save, then click Browse Folders. Move to the Address Bar, type **\\ServerCore01\\LibraryCore** and press Enter. Double-click the ISOStore Folder and click Save.

This will begin the download of the ISO file. This download will take some time. Wait until it completes before you move on to the next exercise.

EXERCISE 3 Create an Unattended Installation File

In this exercise you will create a unattend.xml file. The unattended installation customizes and automates a default Windows installation. To do this, you need to use the Windows System

Image Manager (Windows SIM) to generate the answer file. Windows SIM is part of the Windows AIK and should now be installed on SCVMM01.

1. Log on to SCVMM01 and make sure the SCVMM Administrator Console is open. Make sure you are in Library view, right-click LibraryCore, and choose Refresh. This will update the library index and include the new ISO file you copied. Click ISOStore beneath LibraryCore and wait for your new ISO image to appear.
2. Move to the Virtual Machines view. Right-click SCVMM01 and choose Properties.
3. Move to the Hardware Configuration tab and click Virtual DVD under Bus Configuration. Make sure Existing Image File is selected and click Browse. Select the 6001.1800.080118-1840_ADM64FRE_Server_EN-US-KRMSXFRE_EN_DVD.ISO file and click OK twice. This connects the new DVD image to your VM. Wait until the machine is updated. Cancel the Autoplay dialog box when it appears.
4. Open Windows Explorer. Move to drive D and create a new folder called **Sources**. Move to the DVD drive and go to the /SOURCES folder. Locate the INSTALL.WIM file and copy it to the D:\Sources folder.
5. In Windows Explorer, move to drive C. Select Program Files, click Start, click All Programs, click Windows AIK, click Tools, and finally click Image Manager. Double-click ImgMgr.exe to open Windows System Image Manager.
6. Go to the File menu and click Select Windows Image. Open D:\Sources\INSTALL.wim.
7. In the Select An Image In The Windows Image File dialog box, choose the Windows Longhorn Enterprise image (see Figure 5-17), and click OK. When you get an error message stating that you do not have a valid catalog file, click Yes to create it (see Figure 5-18). The system will create it for you. Each version of Windows needs its own catalog file.

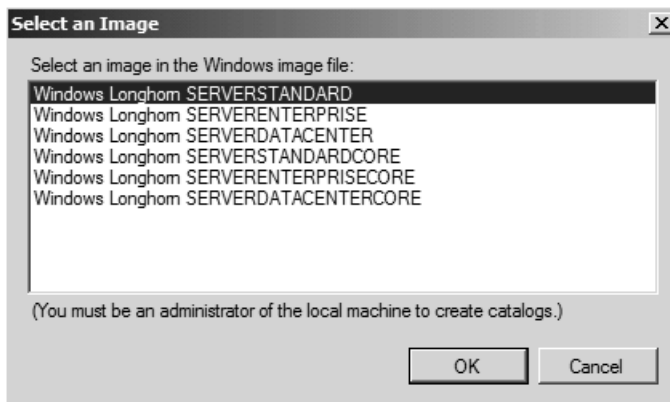


FIGURE 5-17 Choosing an image

8. The image is open and you are ready to proceed. Opening the image may take some time. Now create and modify the answer file. On the File menu, choose New Answer File. This populates the Answer File pane with an untitled file.

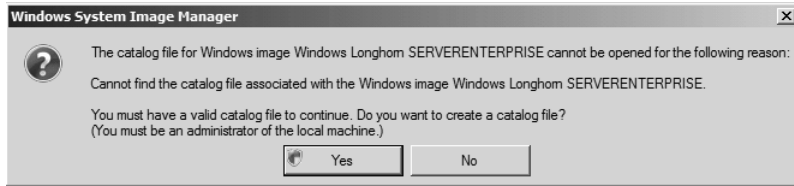


FIGURE 5-18 Creating a new catalog file

9. On the File menu, choose Save Answer File. Name it **WS08_Enterprise** and click Save. Now you will make changes to the answer file to create a basic virtual machine setup. This setup will:
 - Create a setup for a 64-bit machine.
 - Create a 40-GB partition for the operating system and format it in NTFS.
 - Install Windows Server 2008 on the partition.
 - Automatically provide the product key during installation.
10. Go to the Windows Image pane and expand the Component node.
11. In the Component node, locate the AMD64_Microsoft-International-Core_6.0.6001.18000_neutral node. Right-click the node name and select Add Setting To Pass 4 Specialize.
12. Repeat step 11 for the AMD64_Microsoft-International-Core-WinPE_6.0.6001.18000_neutral node, but this time click the plus sign beside the node, right-click SetupUILanguage, and choose Add Setting To Pass 1 Windows PE.
13. Under the AMD64_Microsoft-Windows-Setup_6.0.6001.18000_neutral node, expand the node and add the following items. Once again, expand each of the following items and right-click it to choose the available Add command. Each item will be added to the answer file.
 - DiskConfiguration, then Disk, CreatePartitions, and then CreatePartition.
 - DiskConfiguration, then Disk, then ModifyPartitions, and then ModifyPartition.
 - ImageInstall, then OSImage, and then InstallTo.
 - UserData, then ProductKey.
14. Under AMD64_Microsoft-Windows-Shell-Setup_6.0.6001.18000_neutral add: OOBE. This time choose Add Setting To Pass 7 oobeSystem.
15. On the Answer File pane, add the following settings to each listed component. Unlisted components do not need settings; they will use the default. To add each setting, click the component name in the Answer File pane, move to the Properties pane, click the setting, and select the appropriate value from the drop-down arrow or type the value out.

Pass 1 — International Core WinPE

InputLocale: **0409:00000409**

LayeredDriver: none

SystemLocale: **en-US**

UILanguage: en-US
UILanguageFallback: none
UserLocale: en-US

Pass 1 — International Core WinPE, then SetupUILanguage

UILanguage: en-US
WillShowUI: OnError

Pass 1 — DiskConfiguration

WillShowUI: OnError

Pass 1 — DiskConfiguration, then Disk

DiskID: 0
WillWipeDisk: True

Pass 1 — DiskConfiguration, then Disk, then CreatePartitions, and then CreatePartition

Order: 1
Size: 127000
Type: Primary

Pass 1 — DiskConfiguration, then Disk, then ModifyPartitions, and then ModifyPartition

Active: True
Extend: False
Format: NTFS
Label: SystemDisk
Letter: C
Order: 1
PartitionID: 1

Pass 1 — ImageInstall, and then OSImage

WillShowUI: OnError

Pass 1 — ImageInstall, then OSImage, and then InstallTo

DiskID: 0
PartitionID: 1

Pass 1 — UserData

AcceptEULA: True
FullName: Resource Pool Administrator
Organization: Contoso.com

Pass 1 — UserData | ProductKey

Key: You enter your organization's product key; if no key is available, leave blank
WillShowUI: OnError

Pass 4 — International Core

InputLocale: 0409:00000409
SystemLocale: en-US

UILanguage: **en-US**
UILanguageFallback: none
UserLocale: **en-US**

Pass 7 — OOBE

HideEULAPage: **True**
NetworkLocation: **Work**
ProtectYourPC: **3**
SkipMachineOOBE: blank (the server setup does not have a machine out of box experience)
SkipUserOOBE: **True**

16. Save the answer file when done.
17. Validate the answer file to make sure it works. On the Tools menu, select Validate Answer File. If your entries are correct, you should have no warnings or errors in the Messages pane. If not, review the settings listed here and compare them to yours. If you have discrepancies, modify your settings. If you cannot modify your settings, delete the component from the answer file by right-clicking it, and then add it again and reapply the settings. Save the file again.
18. Save a new copy of the file. Name it **AUTOUNATTEND.xml**. This file will be used to automate your installation. Windows Setup automatically searches removable drives, such as floppy and USB drives, for a file named AUTOUNATTEND.XML during setup. If Windows Setup locates the file, it uses the file to apply settings during installation. Close Windows SIM.
19. Complete the process by saving the file to a floppy disk or USB thumb drive. In ServerFull01, go to Server Manager and then the Hyper-V Manager node. Make sure ServerCore01 is selected. Click New and then click Floppy Disk in the Actions pane.
20. Click Browse Folders and move to \\ServerCore01\\LibraryCore. Create a new folder called **FloppyDisks**. Name the new floppy disk **WS08_Install.vfd** and click Create.
21. Return to SCVMM01 and the SCVMM Administrator Console. In the Library view, right-click LibraryCore and then choose Refresh. This updates the library index and includes the new floppy disk file you created. Wait for it to appear in the Details pane.
22. Move to the Virtual Machines view. Right-click SCVMM01 and choose Properties.
23. On the Hardware Configuration tab, click Floppy Drive under Hardware Profile. Make sure Existing Virtual Floppy Disk File is selected and click Browse. Select the WS08_Install.vdf file and click OK twice. This connects the new floppy image to your VM. Wait until the machine is updated.
24. Return to Windows Explorer. Move to the D:\\Sources folder on SCVMM01 and locate the AutoUnattend.xml file.
25. Copy this file to the floppy disk. When you click the floppy disk drive on SCVMM01, you will be prompted to format the diskette (see Figure 5-19). Click Format Disk. Click Quick Format and then click Start. Click OK to accept the warning and then click OK

when the format is complete. Click Close to close the format dialog box. Paste the AutoUnattend.xml file on your floppy disk.

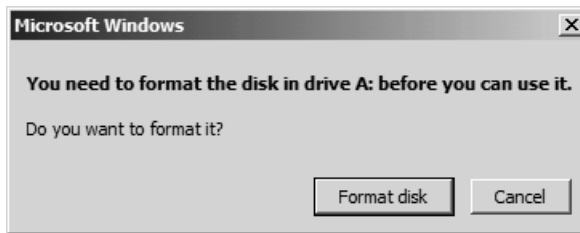


FIGURE 5-19 Formatting a virtual floppy disk

Your unattended file is ready and is on a virtual floppy image, which allows you to use it with any new VM. Repeat the process if you need to update the XML file.

EXERCISE 4 Create a Guest OS Profile

In this exercise you will add the unattended installation file to the Library on ServerCore01 and use it to create a Guest OS Profile. Perform this operation from SCVMM01, which is accessed from ServerFull01.

1. Log on to SCVMM01 and launch Windows Explorer. Go to the D:\Sources drive and copy WS08_Enterprise.xml to the clipboard. Right-click the file and choose Copy.
2. Move to \\ServerCore01\LibraryCore and create a new folder called **UnattendedInstalls**.
3. Paste the XML file into this new folder.
4. Return to the SCVMM Administrator Console. In the Library view, right-click LibraryCore and choose Refresh. This updates the library index and includes the new unattended installation file you just added. Wait for it to appear in the Details pane.
5. Click New Guest OS Profile in the Actions pane. Type **WS08_Enterprise** as the name and give it a short description.
6. Move to the Guest OS tab. Click Identity Information under General Settings. Leave the computer name as is and enter **Resource Pool Administrator** as the full name and **Contoso Ltd.** as the organization's name.
7. In the Administrator Password text box, type and then confirm your password of choice.
8. Move to Operating System and choose 64-bit edition Of Windows Server 2008 Enterprise from the drop-down list (see Figure 5-20). This step is necessary because this option controls the type of unattended answer file SCVMM looks for when you get to the next step.
9. Move to Answer File under the Scripts section and click Browse. Select WS08_Enterprise.xml from the list and click OK.
10. SCVMM will ask you if you want to populate the Guest OS Profile with values from your answer file (see Figure 5-21). Click Yes. Click OK to generate the Guest OS Profile.

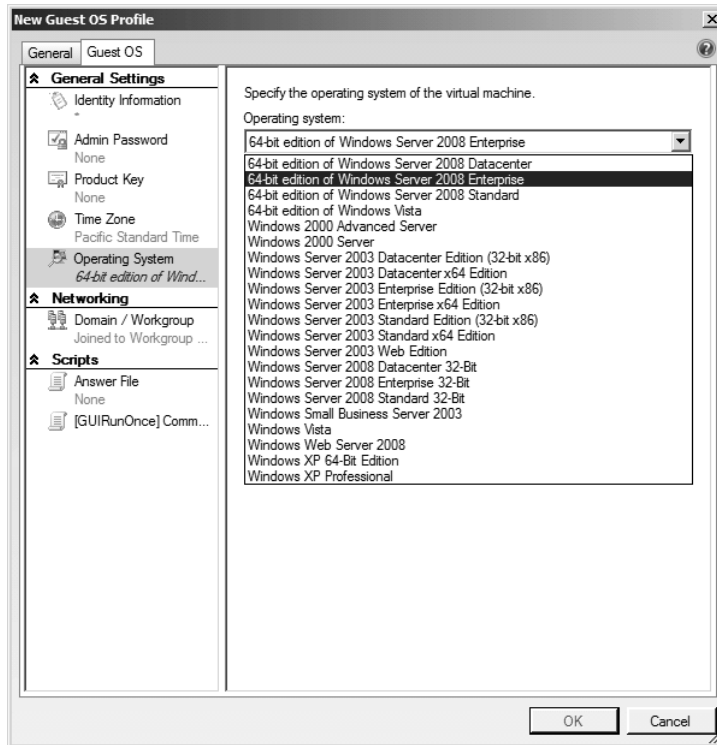


FIGURE 5-20 Choosing the target operating system for a Guest OS Profile

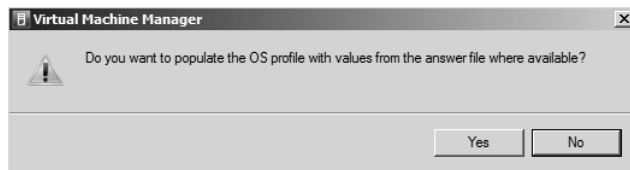


FIGURE 5-21 Populating a Guest OS from an answer file

Your profile is ready and can be used to install a guest operating system in a blank VM.

EXERCISE 5 Create a Hardware Profile

In this exercise you will create a hardware profile to be used in the generation of new virtual machines. This exercise is performed on SCVMM01. Access SCVMM01 from ServerFull01.

1. Log on to SCVMM01 and open the SCVMM Administrator Console. Make sure you are in Library view.
2. Click New Hardware Profile in the Actions pane.
3. Name the new profile **x64_VM** and provide a short description.

4. On the Hardware Settings tab, click Processor and select 2.40 GHz Opteron (see Figure 5-22). Opteron processors are from AMD. All AMD processors are x64 processors and will therefore support an x64 operating system.
5. Click Memory and assign 1024 MB of RAM. Click OK to generate the hardware profile.

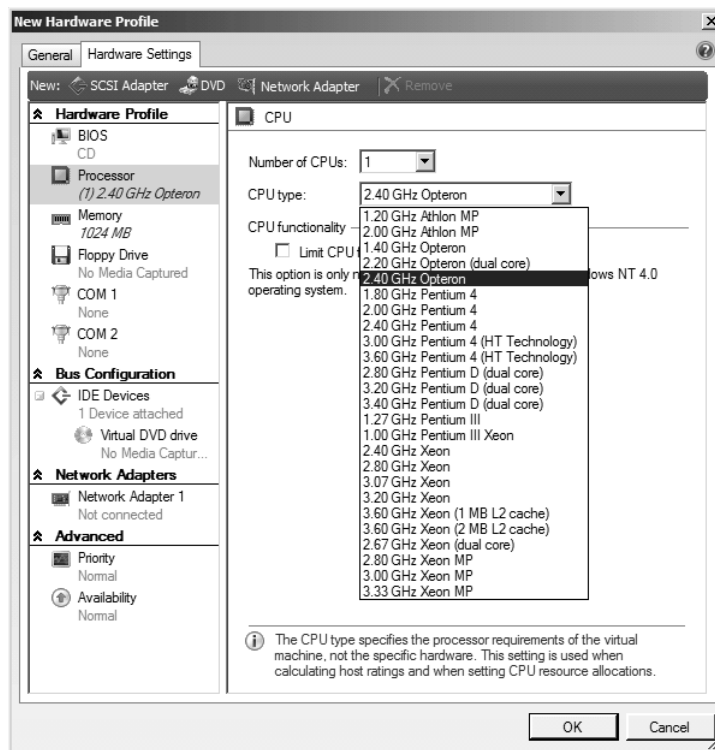


FIGURE 5-22 Choosing the processor type in a hardware profile

Note that you can make several additional changes in the New Hardware Profile dialog box. The Availability option allows you to automatically place the VM on a failover cluster. In addition, you can add additional network adapters—even legacy network adapters. Remember that you need a legacy network adapter if you want to use WDS to install an operating system into the VM because legacy network adapters are the only ones that support PXE booting or booting from the network before an operating system is installed. Note that in SCVMM, legacy network adapters are called *emulated network adapters* and enlightened network adapters are called *synthetic network adapters*. Finally, you can also change the priority of the VM. Priority controls the amount of resources the hypervisor dedicates to the VM. If VMs based on this profile run business critical applications, you probably want to give them a higher priority than Normal, which is the default. Your hardware profile is ready for use.

Quick Check

1. Name at least three management capabilities of the System Center Virtual Machine Management Administrator Console.
2. Which four specific executives are installed in the %ProgramFiles%\Microsoft System Center Virtual Machine Manager 2008\Bin folder when you install SCVMM and the Administrator Console?
3. Which port does the SCVMM Administrator Console use to communicate with the SCVMM Server whether locally or remotely?
4. What are the settings that the SCVMM will reserve by default for the parent partition?
5. What are the two blank virtual hard disks that are created during the SCVMM Library Server installation and what is their size?

Quick Check Answers

1. Several management actions can be performed through the SCVMM Administrator Console:
 - Deploy VMs from any host server.
 - Convert physical machines into virtual machines (P2V).
 - Convert virtual machines in a non-Hyper-V format into Hyper-V virtual machines (V2V).
 - Manage VMs from any host server that has been added to the SCVMM resource pool.
 - View VM status on any host server.
 - Manage template VMs that can be used as sources for new VMs.
 - Regroup components that are needed to generate new VMs and install a guest operating system through the SCVMM Library.
 - Assign tasks to other members of the organization.
2. Four executives are installed:
 - VMMAAdmin.exe launches the console itself.
 - VirtualMachineViewer.exe opens a remote control session on a virtual machine running in a Hyper-V environment.
 - VMRC.exe opens a remote connection to a virtual machine running on Virtual Server 2005 R2 SP1.
 - VMwareViewer.exe opens a remote connection to a VM running on VMware ESX or ESXi.

- 3.** The SCVMM Administrator Console uses port 8100 to communicate with SCVMM Server.
- 4.** SCVMM reserves 10 percent of CPU, 512 MB of RAM, 100 MB of disk space, 10,000 I/O operations per second, and 10 percent of network bandwidth for Hyper-V Hosts.
- 5.** The SCVMM Library installation creates two blank VHDs: Blank Disk Small (16 GB) and Blank Disk Large (60 GB).

Lesson 2: Automating Virtual Machine Creation

Now that you understand how to use SCVMM, you can move on to discover the SCVMM features related to virtual machine creation and management. You've already seen that virtual machine creation with Hyper-V Manager is mostly an interactive process. Now you'll learn how to rely on existing virtual machines to generate new VMs. You'll also learn how to rely on templates to generate new VMs. Templates greatly reduce the time it takes to generate a VM because they build VMs from files that already contain guest operating systems and even applications if the applications lend themselves to the duplication process.

After this lesson, you will understand:

- How to duplicate a virtual machine by copying virtual hard disks.
- How to clone a virtual machine.
- How to depersonalize the VM clone image by using the System Preparation Tool.
- How to install a guest operating system in a VM by using the PXE boot process.
- How to create and manage templates.
- How to deploy a virtual machine from the SCVMM library.
- How to allow end users to generate their own VMs through the SCVMM Self-Service portal.

Estimated lesson time: 40 minutes

Manually Creating a Duplicate Virtual Machine

When you manage multiple virtual machines, you quickly learn that generating a new VM from scratch can take considerable time—not nearly as much time as generating a new physical machine, but time nevertheless. Yet, when you consider that a VM is mostly composed of virtual hard disks and all you need to do to generate a new VM is copy the virtual hard disks to another folder, you begin to see the impact server virtualization has on standard datacenter operations. Even better, if you can automate the process or make it available through self-service, you turn your datacenter into a dynamic environment that can quickly respond to changing business needs.

Generating a new VM from an existing VM can be a simple process, but like physical machines, virtual machines must be depersonalized before you can use a duplicate of the system image to create a new machine. In the physical world, duplicating a machine uses the following process:

1. You create a reference computer. The reference computer is a computer that includes an operating system and possibly an application such as a Web server or a database engine. In addition, the reference computer has been personalized and configured to the organization's standards. This includes any utilities or security components such as antivirus and antimalware engines.

2. You depersonalize the reference computer. This involves using the Microsoft System Preparation Tool to remove items such as computer name, security identifier (SID), administrative account, and more. This generalizes the installation so that it can be reused without any conflicts within the same environment. Depersonalization renders the machine unusable until it has been repersonalized.
3. You capture a disk or file image copy of the disks that make up the reference computer. This capture can be performed through the ImageX tool that is included in the Windows Automated Installation Kit. ImageX captures a file-based image of the disk and stores it in a WIM format. In many cases, you only need to capture the operating system disk. You store the image on a file share that is accessible by the other computers on which you want to install the new image.
4. You deploy the image to new or existing computers. If the target computer does not include an operating system, you use either components from the Windows AIK or the Windows Deployment Services to send the image to the new systems. If you use WDS, you need to boot the system from the network interface through the PXE process (the F12 key), connect to a WDS server, and download the image. Both processes—interactive image copying with WAIK tools and remote image copying through WDS—rely on Windows PE to boot to a temporary operating system, copy the image, and then reboot into the newly installed operating system.
5. After the system is booted into the newly installed operating system, the operating system is repersonalized, generating a new SID, reassigning the administrative account, naming the computer, and possibly joining a Windows domain. This process can either be interactive or automated through unattended response files. At this point the computer is ready to take on a new role within your infrastructure.

The advantage of this process is that you do not need to run through a standard installation and configuration each time you deploy a new computer. However, it has some disadvantages:

- When you work with physical computers, you must destroy the reference computer to generate a depersonalized version of the newly configured operating system.
- When it is time to update the reference system—which occurs each time new updates are available for operating system and other components on the configured system—you must re-create the reference computer by re-copying the image to the system, personalizing it, updating the system, depersonalizing the system once again, and then regenerating the source image.

When you work with virtual machines, you'll find that working with reference systems is much easier than in the physical world. For one thing, you never need to regenerate the reference system. Instead of depersonalizing the reference computer, you generate a clone of the reference computer and depersonalize the clone. This way, you can always rely on the original reference computer to install updates and regenerate a depersonalized image. Of course, you must shut down the reference computer when you depersonalize the cloned version to ensure that the two systems do not conflict with each other.

Another major advantage of virtual machines is that you do not need to generate an image of the disk drives that make up the machine because the disk drives are already in file format (using the VHD format). This also saves considerable time. Therefore, the same duplication process is simplified when applied to virtual machines (see Figure 5-23):

1. You create a reference VM. You set it up the same way you would create a reference physical system. Shut down the VM.
2. You copy the VHDs that make up the reference computer. This can be as simple as copying the VHDs from one folder to another. The process will be much faster if the VHDs are dynamically expanding VHDs because they will only include the actual used space in the VHD.
3. In Hyper-V Manager, you create a new VM based on the existing VHD copies.
4. You boot the new VM to depersonalize it, making sure the reference computer is still off. Once again, you use the System Preparation Tool to do this.
5. To deploy a new VM, you duplicate the VHDs that make up the depersonalized computer.
6. In Hyper-V Manager, you create a new VM based on the existing VHD copies and boot it up.
7. When the system is booted, you proceed with the repersonalization. At this point the computer is ready to take on a new role within your infrastructure.

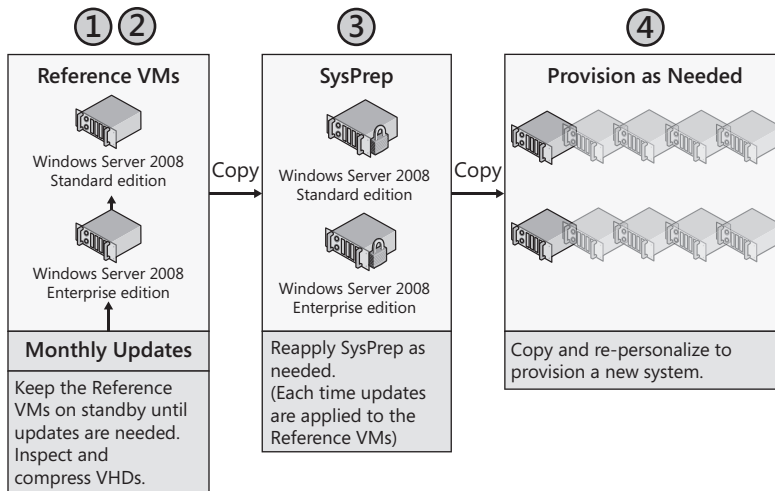


FIGURE 5-23 Managing reference and source VMs

The major advantage of this process is that it only takes a few minutes and your reference computer remains intact throughout the process. When updates are available, all you need to do is launch the reference computer, update it, repeat step 2—copying the updated VHDs to the depersonalized machine's folder—and then repeat step 4 to depersonalize it again.

MORE INFO OFFLINE VHD SERVICING

Microsoft also offers an offline virtual machine servicing tool that lets you install updates on virtual machines that are turned off while stored in the SCVMM Library. Find it at <http://www.microsoft.com/downloads/details.aspx?FamilyID=8408ecf5-7afe-47ec-a697-eb433027df73&DisplayLang=en>.



EXAM TIP DUPLICATION VS. EXPORT

When you generate a VM to use as a source or seed machine, do not use the Hyper-V Export tool. This tool does not generate a copy of the VM. Instead, it exports the actual virtual machine and the exported virtual machine is no longer usable until it has been imported. Note, however, that the exported machine is still available on the original host.

Cloning a Virtual Machine

When you perform the VM duplication process in Hyper-V alone, you need to use manual processes to make the copies of the VMs. However, when you use SCVMM, you can use a special process called VM cloning to prepare the machine duplicate. Cloning is much faster than manually duplicating the VHDs because it copies the entire VM including configuration and any other files that may be part of the VM.

Cloning is useful when you need to generate a copy of a reference computer or when you simply want to generate a backup of a virtual machine. You can only clone a VM when it is stopped. The VM can either be on a host or in the SCVMM Library.

To clone a VM, you use the Virtual Machines view and then the Clone command. This command is listed at the bottom of the Actions pane and is only available when the VM is stopped. This command launches the New Virtual Machine Wizard, which takes you through the steps required to modify the parameters of the new VM (see Figure 5-24).

Note that when you clone a new VM, the following occurs:

- The guest operating system within the new VM is identical to the source VM. This is fine for seed machines because you will later depersonalize the VM.
- The hardware settings for the VM can be modified during the cloning process.
- You can also move the VM to a new host during the cloning process.

Be wary of cloning VMs. Several other tools are available for generating new VMs in SCVMM and they may be more appropriate if your purpose is not to generate a new seed machine.

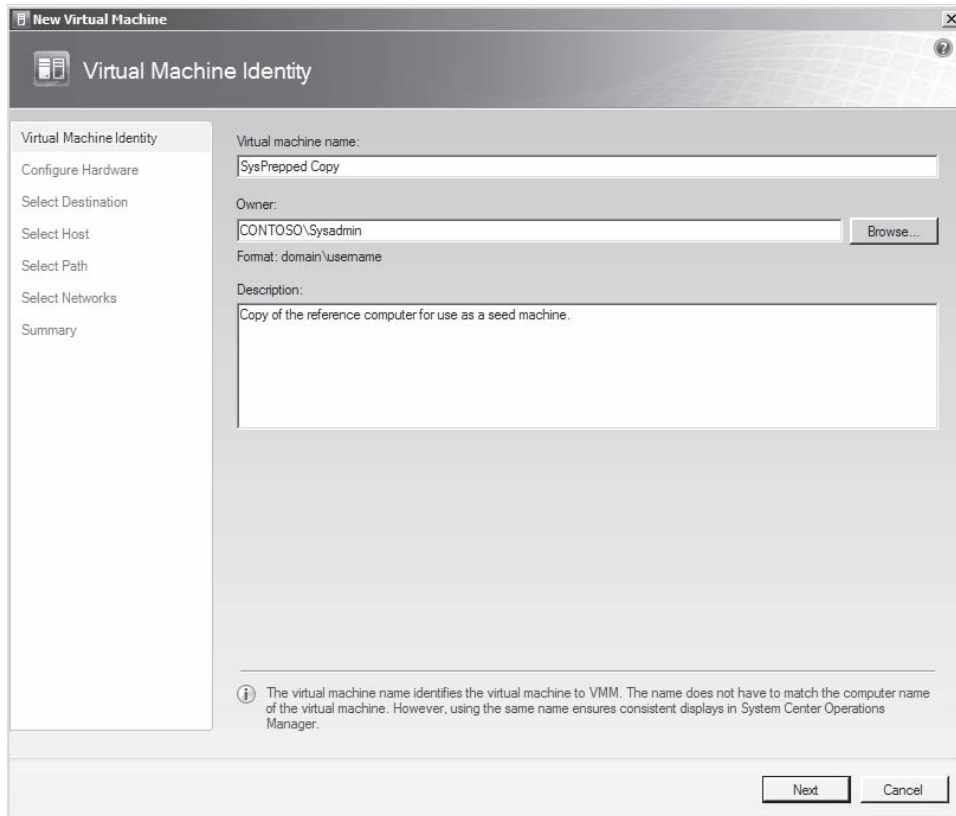


FIGURE 5-24 Cloning a VM with the New Virtual Machine Wizard

Using Sysprep to Prepare a Virtual Machine for Duplication

After the VM has been cloned, you can use the System Preparation Tool within the cloned VM to turn it into a seed VM by following these steps:

1. Boot the cloned VM and log on with local administrative credentials.
2. Open Windows Explorer and go to %SYSTEMROOT%\SYSTEM32\SYSPREP.
3. Launch SYSPREP.exe.
4. In the Sysprep dialog box, select the following options (see Figure 5-25):
 - System Cleanup Action: Enter System Out-of-Box Experience (OOBE)
 - Select the Generalize option
 - Shutdown Options: Shutdown
5. Click OK. Sysprep will depersonalize the system and shut it down.

Your cloned VM system is ready for duplication. You can use the cloning process once again to generate a new working VM from this seed machine.

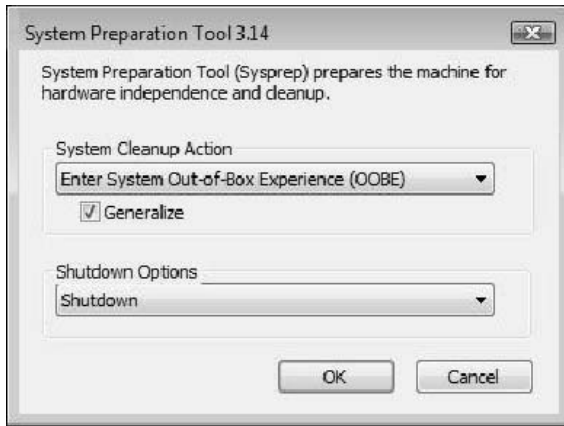


FIGURE 5-25 Using the System Preparation Tool

You can also run the System Preparation Tool through the command line with the following command:

```
C:\Windows\System32\Sysprep.exe /oobe /generalize /shutdown
```

Creating and Managing VM Templates

Although you can clone a VM and then depersonalize the VM using the System Preparation Tool, you can also perform this task automatically through the Administrator Console in SCVMM by generating a VM template. When you generate a template VM, SCVMM automatically transforms the VM into a depersonalized virtual machine to be used as a seed machine for the generation of new VMs.

The template generation process automatically applies the System Preparation Tool to a VM that already includes a Windows operating system. The template will also be stored in the Library to support the generation of new VMs from a central source. In fact, several activities are performed when you generate a template (see Figure 5-26).

Step	Name	Status	Start Time	End Time
✓ 1	Create template	100 %	2/9/2009 5:02:...	2/9/2009 5:27:...
✓ 1.1	Sysprep virtual machine	100 %	2/9/2009 5:02:...	2/9/2009 5:07:...
✓ 1.1.1	Start virtual machine for sysprep	100 %	2/9/2009 5:03:...	2/9/2009 5:03:...
✓ 1.1.2	Stop virtual machine	100 %	2/9/2009 5:07:...	2/9/2009 5:07:...
✓ 1.2	Store virtual machine from ServerFull01.contoso.com to servercore01.co...	100 %	2/9/2009 5:07:...	2/9/2009 5:27:...
✓ 1.2.1	Run pre checks for transfer	100 %	2/9/2009 5:07:...	2/9/2009 5:07:...
✓ 1.2.2	Change virtual machine status	100 %	2/9/2009 5:07:...	2/9/2009 5:07:...
✓ 1.2.3	Deploy file (using LAN)	100 %	2/9/2009 5:07:...	2/9/2009 5:07:...
✓ 1.2.4	Export Hyper-V virtual machine	100 %	2/9/2009 5:07:...	2/9/2009 5:07:...
✓ 1.2.5	Deploy file (using LAN)	100 %	2/9/2009 5:07:...	2/9/2009 5:26:...
✓ 1.2.6	Remove virtual machine	100 %	2/9/2009 5:26:...	2/9/2009 5:27:...
✓ 1.2.7	Fix up differencing disks	100 %	2/9/2009 5:27:...	2/9/2009 5:27:...

FIGURE 5-26 The tasks performed during the creation of a template

You should create as many templates as you need. For example, if your datacenter runs two versions of Windows Server, the Standard and the Enterprise editions, you should have a VM template for each. This way, you can quickly provision new VMs whenever you need them.

IMPORTANT USING SCVMM ON SANs

Storage area networks usually include special tools that support high-speed duplication of information from one location to another within the SAN through the SAN Transfer feature. If you store the SCVMM Library on a SAN, SCVMM will be able to use these tools to perform high-speed VM duplications. This will greatly speed up the generation of VMs from templates and the cloning or duplication of VMs, which can be quite large in file size.



EXAM TIP CREATING TEMPLATES

Remember that templates can only be created from VMs that are stopped.

Creating and Managing VMs with SCVMM

As you’ve seen, SCVMM offers several tools for VM management and administration that are not available in either Hyper-V Manager or the Failover Clustering Management console. In fact, any organization that must manage VMs on an ongoing basis should seriously consider running SCVMM as well as Hyper-V in their environment.

Creating a New VM with SCVMM

The process of creating a new VM in SCVMM—even (and especially) a new VM from scratch—is considerably different from the same process in Hyper-V Manager. It proceeds as follows:

1. Launch the SCVMM Administrator Console and select the Virtual Machines view.
2. In the Actions pane, select New Virtual Machine.

The New Virtual Machine Wizard will launch, and several actions will be presented.

3. Follow the directions in the wizard.

Table 5-5 outlines the major differences you will find when creating a new VM in SCVMM compared to Hyper-V. Figures 5-27 through 5-29 illustrate some of the available options.

TABLE 5-5 The SCVMM New Virtual Machine Wizard

WIZARD PAGE	ACTION
Select Source	Two actions are available and offer different options. ■ Use An Existing Virtual Machine, Template, Or Virtual Hard Disk This lets you generate a new VM from an existing VM.

WIZARD PAGE	ACTION
	■ Create The New Virtual Machine With A Blank Virtual Hard Disk Select this option to create a new virtual machine from scratch. Note that you do not need to use a blank disk and can use an existing hard disk that already includes a guest operating system.
Virtual Machine Identity	This is where you name the VM and provide a description for it. Descriptions are very useful, especially when you run hundreds of VMs.
Configure Hardware	When you configure hardware, you can create a brand new profile for the VM or you can draw upon an existing hardware profile that was pre-created and stored in the Library. Hardware profiles are provided in a drop-down list.
Select Destination	Once again, this page gives you two options: ■ Place The Virtual Machine On A Host This copies the files associated with the VM to the target host. You can even start the VM immediately. ■ Store The Virtual Machine In The Library This stores the VM in the library for later use. You then need to deploy the VM from the Library to a host before you can start it.
Select Host (Host Only)	When you choose to place the VM on a host, SCVMM uses Intelligent Placement to locate an appropriate host from your pool of hosts. Hosts do not need to be in a failover cluster to belong to this pool. Intelligent Placement is based on special host ratings. You can customize these ratings on this page. To do so, select Customize Ratings. This presents a special dialog box that includes two tabs. Note that changes in this dialog box only change the ratings for this particular placement. To change the ratings for all placements, you must access this dialog box through the Administration View. Placement Options tab Configures how host ratings are calculated. ■ Placement Goal Load Balancing or Resource Maximization. ■ Resource Importance You can modify CPU usage, memory free, disk I/O, and network utilization on each host. VM Load tab ■ Lets you refine host ratings based on the anticipated resource utilization of this VM. When the VM is based on an existing VM, the displayed settings are based on past performance of the source VM.

WIZARD PAGE	ACTION
	When you return to the Select Host page, you will see that SCVMM presents available hosts based on the Intelligent Placement settings. Hosts are rated with a five-star method. Hosts with the most resources are displayed first. You can choose which host offers the most resources to place your VM.
Select Library Server (Library Placement Only)	When you choose to place the VM in the Library, you will be given the option to store the VM in one of the Library shares. If you placed the Library on a SAN, you will be able to use SAN Transfer. If SAN Transfer is not available, this page will tell you why.
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. When you place the VM in the Library, you choose where to place the VM in the folder structure of the Library share.
Select Networks (Host Placement Only)	Lets you choose which network to attach to the VM's adapter(s).
Additional Properties (Host Placement Only)	Configures which actions will be applied to the VM.
Summary	Lets you view and copy the Windows PowerShell script to be used to generate the new VM.

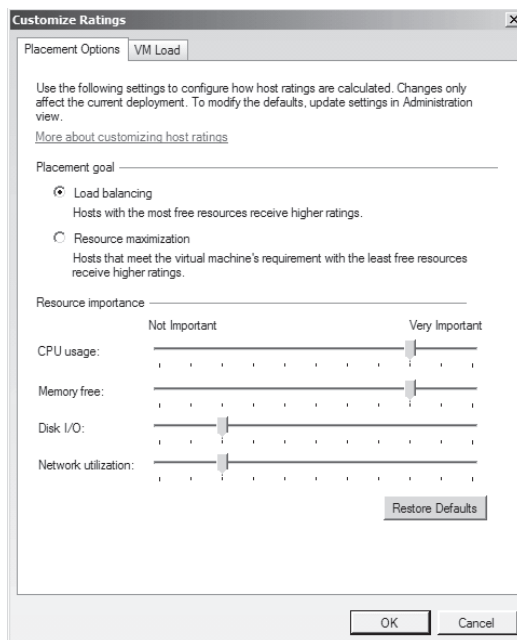


FIGURE 5-27 Customizing placement ratings

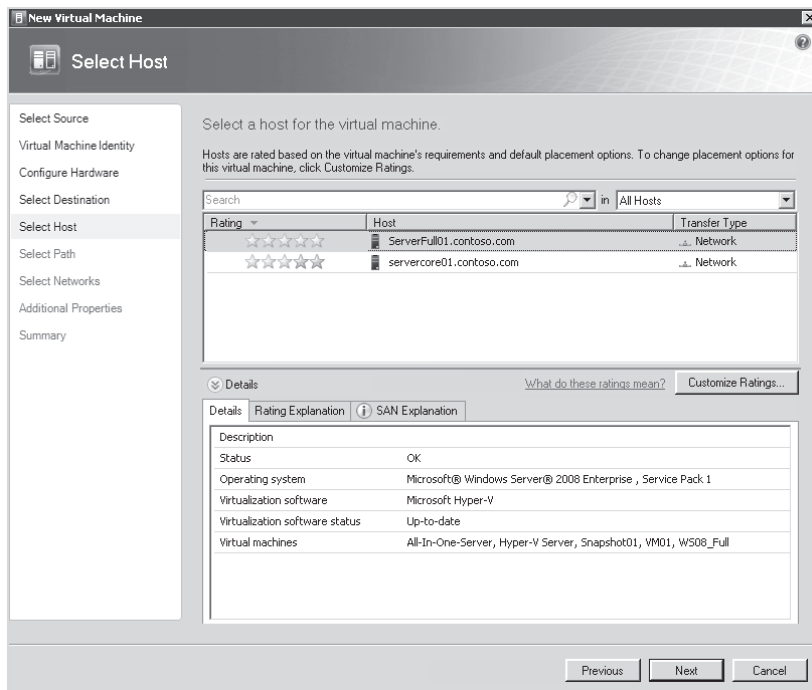


FIGURE 5-28 Using Intelligent Placement to deploy a new VM

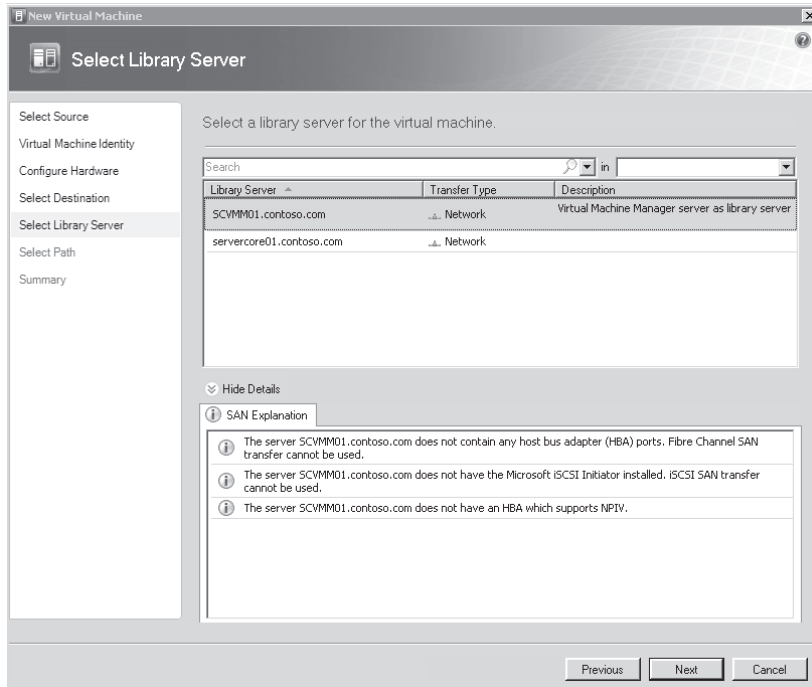


FIGURE 5-29 Placing a new VM in the Library

IMPORTANT NEW VMS IN SCVMM

When you create a new VM from a template, you will be able to customize both the hardware and the guest operating system profiles. If you choose an existing VM, you will only be able to customize the hardware profile.

MORE INFO DEPLOYING VIRTUAL MACHINES WITH SCVMM

For more information on VM placement and deployment rules and guidelines, go to <http://technet.microsoft.com/en-us/library/bb740797.aspx>.

Moving VMs with SCVMM

In Chapter 3, “Completing Resource Pool Configurations”, you learned that one of the advantages of running Hyper-V in a failover cluster is that it supported VM movement from one host to another, either by making the VM highly available or by using the Quick Migration feature of Hyper-V. The same applies to SCVMM when you manage Hyper-V or other hosts that are deployed in a fault-tolerant configuration. However, you can also move VMs from one host to another even if the hosts are not fault tolerant.

In this case, SCVMM will move the files that make up the VM from one host to another. Once again, the VM must be stopped to support the movement. Although you must export and then import a VM in Hyper-V Manager to perform this type of operation, you can simply move the VM in SCVMM to achieve the same result.

When you are not using a cluster, VM movement in SCVMM is performed through the Migrate command in the Actions pane while in the Virtual Machines view. To move VMs, you must make sure they are stopped. If VMs are in a saved state mode, the processors between the host servers must be identical. This means they must use identical stepping and have identical capabilities. If not, SCVMM will give you a warning (see Figure 5-30).

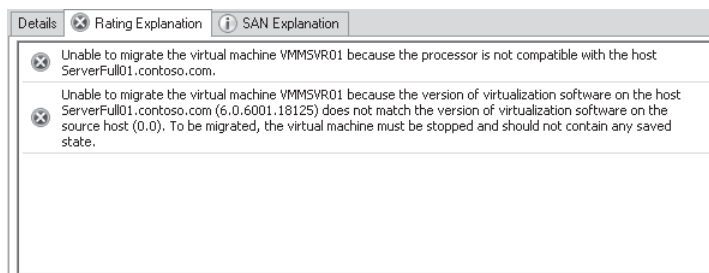


FIGURE 5-30 Migration is not available when processors are not identical.

MORE INFO DETERMINING STEPPING IN PROCESSORS

You can download a useful tool, CPU-Z.exe, for determining the characteristics of your processors. CPU-Z.exe examines all of the features of a processor and displays the information. Obtain CPU-Z at <http://www.cpuid.com/cpuz.php>.

When you choose a machine that is turned off, you can migrate or move that virtual machine from one host to another even if the hosts are not clustered. If the hosts are not clustered and if the VMs are not stored on a SAN, then the migration process will be performed over the network (see Figure 5-31).

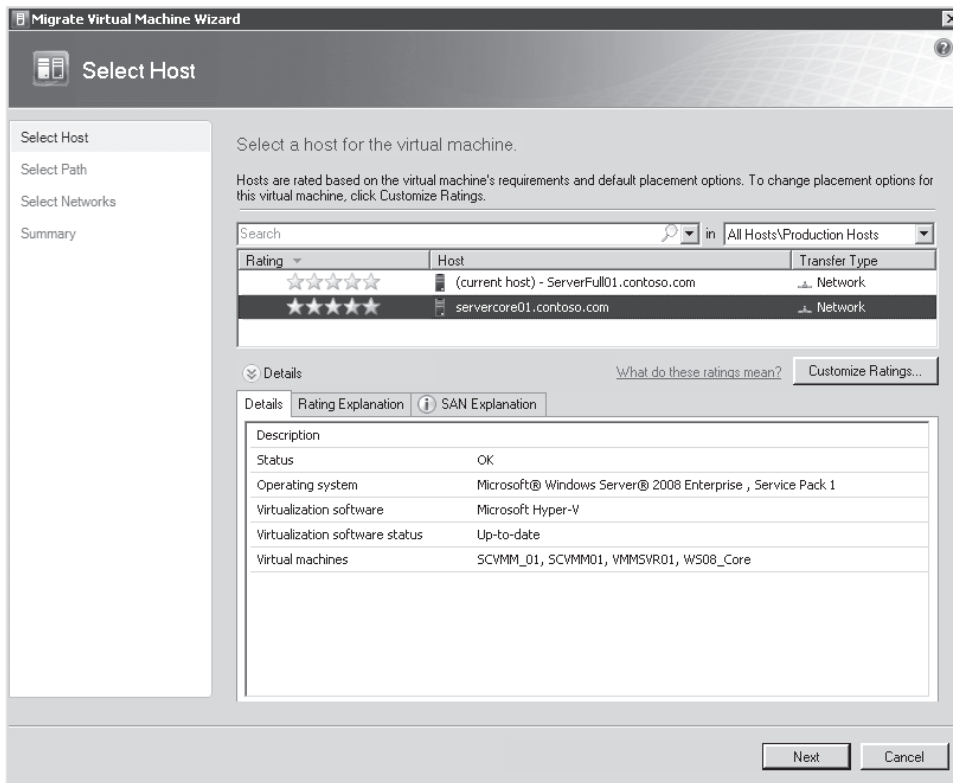


FIGURE 5-31 Migration is performed over the network when VMs are not on a SAN.

Managing the VMM Self-Service Portal

Another component of SCVMM that can be useful in larger organizations is the Self-Service Portal. The Self-Service Portal is a Web page running an ASP.NET application that allows authorized users to create and manage their own VMs. You can create a custom set of host servers and place them in a special host group. Then you can allow end users such as developers, trainers, or testers to deploy and manage their own VMs without your interaction. The Self-Service Portal relies on custom VM templates that you generate and store within the Library. You then create a special usage policy and assign it to the targeted users. This policy controls which kind of operations they can perform on their VMs as well as control how many VMs they can create, how long the VMs will last, and other standard VM parameters. Basically, the Self-Service Portal provides a controlled environment for the use of virtual machines by authorized users.

Installing the SCVMM Self-Service Portal

The SCVMM Self-Service Portal must be installed on a server operating system that includes Internet Information Services (IIS). This installation can be on a number of platforms. Table 5-6 outlines the available platforms for portal installation.

TABLE 5-6 Supported Platforms for the SCVMM Self-Service Portal

PLATFORM
Windows Server 2008 with Hyper-V x64 Standard, Enterprise, and Datacenter editions
Windows Server 2008 without Hyper-V x64 Standard, Enterprise, and Datacenter editions
Windows Server 2008 without Hyper-V x86 Standard, Enterprise, and Datacenter editions
Windows Server 2008 Web Server edition
Windows Server 2003 x86 with Service Pack 2 Standard, Enterprise, and Datacenter editions
Windows Server 2003 x64 with Service Pack 2 Standard, Enterprise, and Datacenter editions
Windows Server 2003 x86 R2 with Service Pack 2 Standard, Enterprise, and Datacenter editions
Windows Server 2003 x64 R2 with Service Pack 2 Standard, Enterprise, and Datacenter editions

When you set up the Self-Service Portal, you must perform the following tasks:

1. Select the target system to host the Self-Service Portal. This can be a VM, but it must include the IIS role.
2. Install the Self-Service Portal from the SCVMM installation files.
3. Create a custom host group for use with the portal. Portals are most often used in testing, development, or training environments. For this reason, you should dedicate host servers to this role and this group. Move the dedicated host servers to the new host group. You dedicate these hosts to this task to avoid interference from testing, development, training, or other volatile VMs with production VMs.
4. Create VM templates and assign them to portal use.
5. Create Self-Service User roles to allow users access to the portal and its VMs.
6. Identify the e-mail address of the administrator responsible for the portal.
7. Make the Web address for the Self-Service Portal available to authorized users.

Users will access the Self-Service Portal through a simple Web browser. When they first connect to the portal page, they log on. After they log on, they can view and access the VMs you have granted them permissions to.

Managing Self-Service Portal Policies

To manage and create Self-Service Portal policies, you must first create Self-Service User Roles. These user roles are created from the Administration view. Use the following procedure.

1. Click Users Roles in Administration view.
2. Click New User Role in the Actions pane.
3. Name the new user role. For example, if you are creating a Self-Service Portal for the training group in your organization, call it **Trainers**. You can also give it a description. Make sure the Self-Service User option is selected from the drop-down list. Click Next.
4. Click Add and type in the name of the domain group that will be assigned to this role. You use a group to simplify the addition process. After you assign the group to this role, you can add new users simply by adding them to the group in Active Directory Domain Services. Click Next.
5. Select the host group the users will be able to interact with. Click Next.
6. Select the actions you want this group to be able to perform on VMs (see Figure 5-32). Click Next.

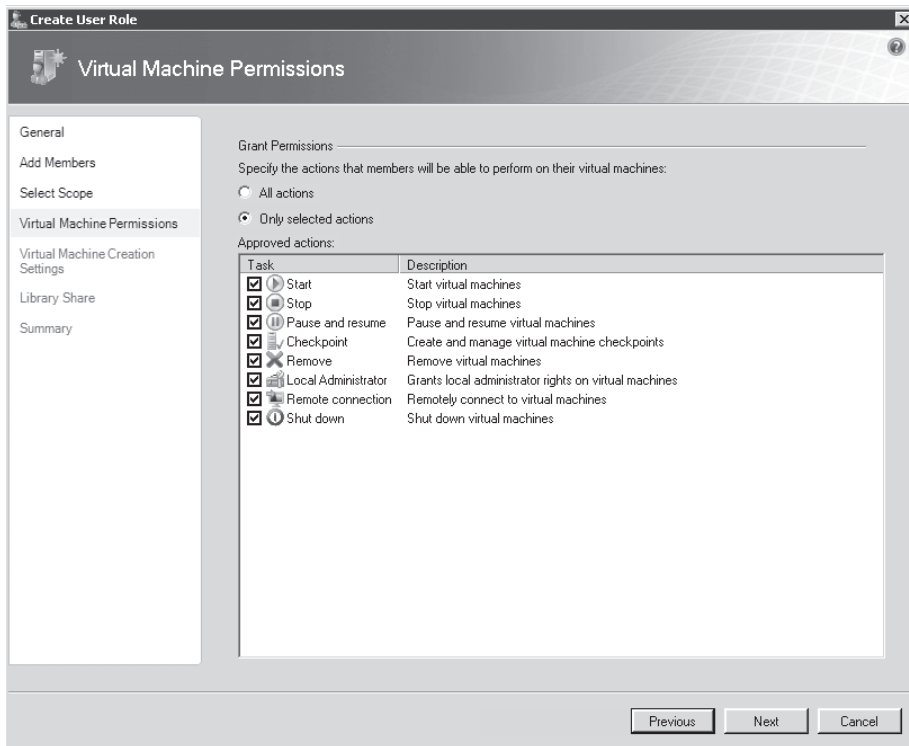
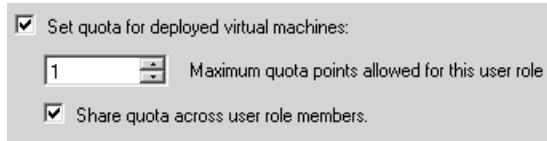


FIGURE 5-32 Users can perform several actions on Self-Service Portal VMs.

7. Select the template users will be allowed to use to generate new VMs. You can also assign quotas to users. Quotas can be assigned to individuals or can be shared among the entire group (see Figure 5-33). Click Next.



☒ Set quota for deployed virtual machines:

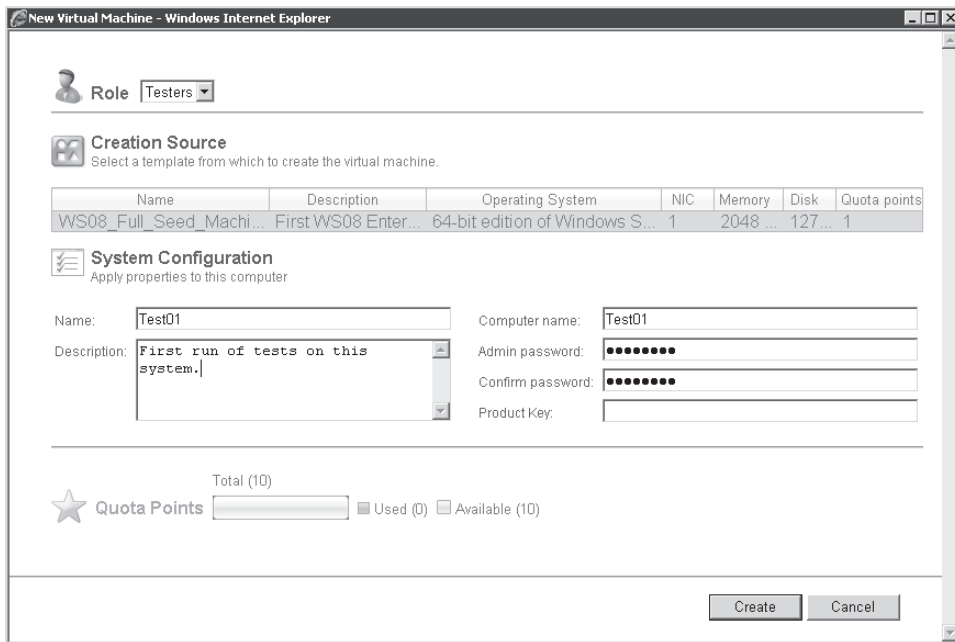
Maximum quota points allowed for this user role

☒ Share quota across user role members.

FIGURE 5-33 You can assign quotas to users in the Self-Service Portal.

8. Identify the Library share to use as the source for the generation of the VMs. Click Next.
9. Review your changes and click Create. The group is created.
10. Communicate with the users to let them know they are now able to create VMs in the Portal.

Users will now be able to interact with the portal through their browser. For example, they will be able to generate new VMs from the templates you assigned them (see Figure 5-34).



Name	Description	Operating System	NIC	Memory	Disk	Quota points
WS08_Full_Seal_Machi...	First WS08 Enter...	64-bit edition of Windows S...	1	2048 ...	127 ...	1

FIGURE 5-34 Users can generate their own VMs through the Self-Service Portal.

PRACTICE Managing Virtual Machine Templates

In this practice, which consists of five exercises, you will add a new hard disk to ServerFull01 and use it to generate a clone of the WS08_Full VM. This clone will then be used to generate a template. You will customize this template and then use it to deploy a new VM. This practice

is performed on both ServerFull01 and on SCVMM01. Log on with domain administrator credentials to facilitate the exercise.

EXERCISE 1 Add an External Hard Disk

In this exercise, you will add an external hard disk to ServerFull01.

1. Plug the external hard disk into a USB port on ServerFull01. The system will recognize the disk and add it to the system's configuration.
2. Log on to ServerFull01, click Start, point to Administrative Tools, and click Computer Management. You will use this tool to configure the new disk.
3. Move to the Storage node in the Tree pane and click Disk Management. Locate the new disk and make sure it is formatted and assigned to drive D. If it is not formatted, right-click the partition and choose Format to format it in the NTFS format and assign the D letter. Name the disk **VMData**. If it is already formatted, right-click the partition, select Change Drive Letter And Paths, and then click Change to choose D from the drop-down list. Click OK twice.

NOTE DRIVE LETTER ASSIGNMENTS

ServerFull01 may already have assigned the D letter to the DVD drive. If so, you must change the DVD drive to E before you can assign D to the new disk.

4. Open Windows Explorer and move to the new drive D. Create a folder called **VirtualMachines** in the root of this drive.
5. Move to SCVMM01. Log on with domain administrator credentials and open the Administrator Console.
6. Choose the Hosts view, right-click ServerFull01, and choose Properties.
7. Click the Placement tab and choose Add. Expand drive D and select VirtualMachines. Click OK twice. This adds the new disk as a potential placement disk to the ServerFull01 host.

Your computer is ready.

EXERCISE 2 Clone a VM

In this exercise you will create a clone of the WS08_Full VM. Perform this exercise from SCVMM01. Continue to use domain administrator credentials.

1. Log on to SCVMM01, go to the SCVMM Administrator Console, and move to the Virtual Machines View.
2. Click WS08_Full. In the Actions pane, click Clone under the Virtual Machine section. You may have to scroll to the bottom of the Actions pane to locate the Clone command.
3. On the Virtual Machine Identity page, in the Virtual machine name text box, type **WS08_Full_Seed_Machine**, leave the default owner, and type a short description—for example, **First Seed Machine**. Click Next.

4. On the Configure Hardware page, choose the x64 Hardware Profile you created in Lesson 1 from the drop-down list. This will assign the existing hardware profile to the cloned VM. Click Next.
5. On the Select Destination page, select Place The Virtual Machine On A Host and click Next.
6. On the Select Host page, choose ServerFull01.contoso.com in the host list and click Next.
7. On the Select Path page, select D:\VirtualMachines from the Virtual Machine Path drop-down list and click Next.
8. On the Select Networks page, do not select a network connection, leave the adapter at Not Connected and click Next.
9. On the Additional Properties page, leave the defaults and click Next.
10. Review your changes and click Create.

The Jobs window will appear and begin the cloning process. The machine will be cloned when the process is complete (see Figure 5-35).

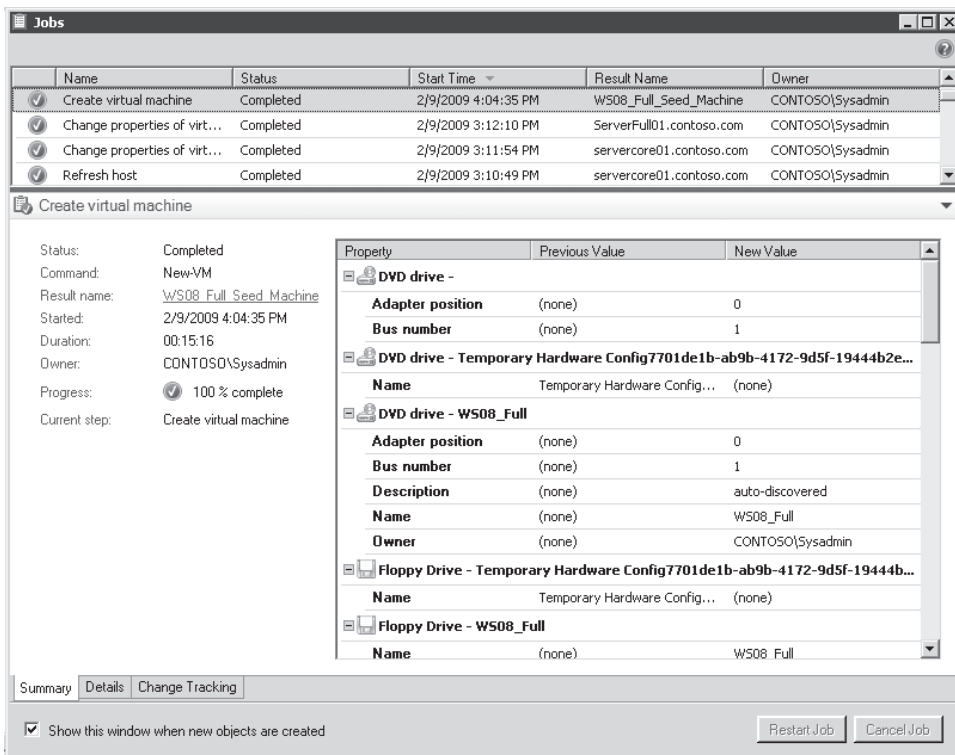


FIGURE 5-35 The cloning job is finished.

EXERCISE 3 Generate a Template from a Cloned VM

In this exercise you will generate your first template. When you create a template, SCVMM automatically depersonalizes the VM in the template. You will use the VM you cloned in the previous exercise to generate the template. You use a cloned VM to generate the template because when you create a template, it destroys the source VM (see Figure 5-36).

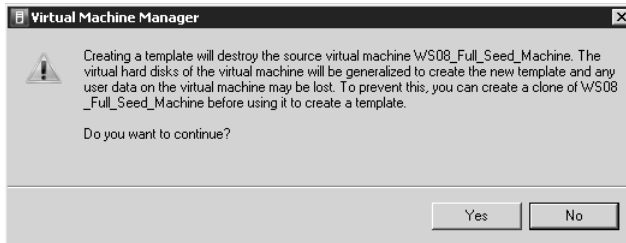


FIGURE 5-36 Creating a template destroys the source VM.

1. Log on to SCVMM01 with domain administrator credentials. Open the SCVMM Administrator Console and move to the Virtual Machines view. Click WS08_Full_Seed_Machine and choose New Template from the Actions menu. You may have to scroll through the Actions menu to locate this command.
2. SCVMM warns you that the source VM will be destroyed. Click Yes.
3. Leave the name as is and add a short description, such as **First WS08 Enterprise Seed Template of a full installation**. Click Next.
4. Choose the x64 Hardware Profile from the drop-down list and click Next.
5. Choose the WS08_Enterprise Guest OS Profile from the drop-down list and click Next. You created this profile in Lesson 1 and can now apply it to new VMs generated from this template.
6. Choose ServerCore01 as the Library Server and click Next. This will store the template within this server's Library share.
7. Click Browse to choose the storage path. Click the plus sign (+) to expand the folder structure under this Library share and choose the VHDStore folder. Click OK and then click Next.
8. Review your changes and click Create to begin the process.

The Jobs window opens and runs a multipart job to create the template. Wait until the job completes before you proceed to the next exercise. This may take some time because the VM must be copied from one host server to the other. Also note that the job will give you a warning but will still complete properly. Warning number 10666 indicates that you cannot change hardware settings during the creation of the template (see Figure 5-37). This is due to the fact that the WS08_Full VM is allocated 2048 MB of RAM and the x64 Hardware Profile is allocated only 1024 MB. These values cannot be changed during template creation and must be changed afterwards.

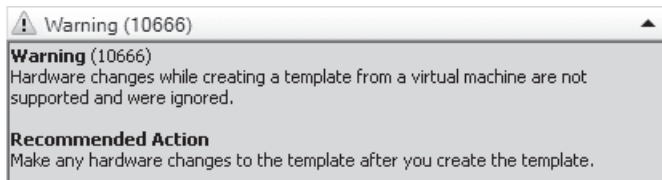


FIGURE 5-37 Warning message 10666

EXERCISE 4 Customize a Template

In this exercise you will customize the new template you just generated. This exercise is performed on SCVMM01. Log on with domain administrator credentials to facilitate the exercise.

1. Log in to SCVMM01 and open the SCVMM Administrator Console. Move to the Library view.
2. Select VMs And Templates in the tree view of the LibraryCore Library on ServerCore01. The Details pane will display your new template.
3. Select WS08_Full_Seed_Machine and click Properties in the Actions pane under Template. This opens the Properties dialog box. Move to the Hardware Configuration tab.
4. Select Memory and change the setting from 2048 to 1024. Click OS Configuration and note that the settings here reflect the settings applied using the WS08 Enterprise guest OS profile. Move to the Settings tab.
5. This tab displays the number of points assigned to a VM when used through the Self-Service Portal. These points are tabulated against a user's quota and help control how many VMs users can run in their Portal profile. Change the quota value to 2 and click OK.

The template is ready for deployment.

EXERCISE 5 Generate a New VM from a Template

In this exercise you will use the template you created and customized to deploy a new VM. Perform this exercise on SCVMM01 and log on with domain administrator credentials.

1. Log on to SCVMM01 and open the SCVMM Administrator Console. Move to the Virtual Machines view.
2. Click New Virtual Machine. Make sure that Use An Existing Virtual Machine, Template Or Virtual Hard Disk is selected, and click Browse.
3. Select your new template: WS08_Full_Seed_Machine, click OK, and then click Next.
4. Name the new VM **Template_Test** and click Next.
5. Review the hardware configuration. Note that the memory setting is set at 1024 MB according to your customizations of the template. Click Next.
6. Review the Guest OS Profile that will be assigned. Note that it is using the answer file you created in Lesson 1. Click Identity and change the name to **Template_Test**.

7. Click Product Key and note that the current product key is to be supplied by the answer file. However, you did not add a product key in the answer file. Click Next. SCVMM gives you an error message (see Figure 5-38). You must assign a product key to be able to use this template to generate VMs. If you do not have a product key, stop the exercise at this stage. If you do have a product key, click OK to close the error message, clear the Product Key Provided By Answer File check box and type in your product key. Click Next.

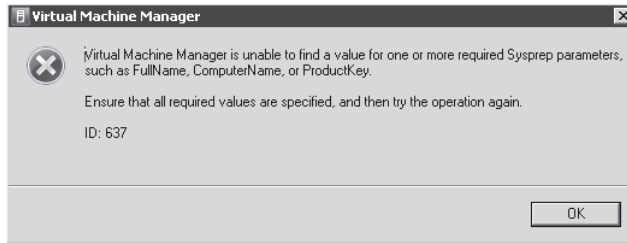


FIGURE 5-38 You need a product key to deploy a VM from a template.



EXAM TIP PRODUCT KEYS AND TEMPLATES

Keep in mind that to use templates in support of Self-Service Portal users, you must enter the product key into the answer file, but when you deploy a template interactively, you can supply the product key on your own.

8. Make sure Place The Virtual Machine On A Host is selected and Click Next. Assign the VM to ServerCore01 and click Next.
9. Select the path on drive D and click Next. Assign the network adapter to Hyper-V External and click Next.
10. Leave Automatic Actions as is and click Next. Review the Summary page. You can opt to start the VM after it is created if you want to at this stage, but for this exercise do not select this option. Click Create.

The Jobs window will open and generate your new VM. This will also take some time because the VHD file that makes up the VM is quite large.

✓ Quick Check

1. In which state can you clone a virtual machine?
2. What happens when you clone a new virtual machine?
3. When you move a VM from one host to another, how does the process differ in Hyper-V Manager and SCVMM?
4. What kind of control does a Self-Service Portal policy offer?

Quick Check Answers

1. Virtual machines need to be in stopped state to be cloned.
2. When you clone a virtual machine, the following occurs:
 - The guest operating system of the new VM is identical to the source VM.
 - The hardware settings for the VM can be modified during the cloning process.
 - The VM may be moved to a new host during the cloning process.
3. In Hyper-V Manager you must export and then import the VM. In SCVMM you only need to move or migrate the VM.
4. A Self-Service Portal policy controls which kind of operations end users can perform on their VMs, how many VMs they can create, how long the VMs will last, and other standard VM parameters.

Case Scenario: Provisioning Virtual Machines

In the following case scenario, you will apply what you've learned about automating virtual machine creation. 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. Your manager has read about virtual machine technologies and has decided that you need to set up a complex provisioning system to generate new VMs in the future. You already own System Center Virtual Machine Manager and you use it to manage your 15 host servers. But your manager has decided that you need to implement a Windows Deployment Services server to support virtual machine creation. He also wants you to use this WDS system to generate the operating system installation process within each of the new VMs you create. Specifically, he wants you to answer the following questions:

1. What does your VM Hardware Profile need to include to support operating system installations with WDS?
2. What is one consequence of using WDS to install new operating systems in bare-metal VMs?
3. Is WDS the best method to use to generate new VMs?
4. What is your final recommendation to your manager?

Suggested Practices

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

Working with SCVMM

- **Practice 1** Take the time to compare the remote connection differences between SCVMM and Hyper-V Manager. Note the available toolbars and menu items.
- **Practice 2** Examine the SCVMM Administrator Console in depth. Take the time to examine the features and commands available in each view.
- **Practice 3** Take the time to look through the available features and commands related to the SCVMM Library. Note how the Library stores various items such as templates, VHDs, profiles, and more.

Working with VMs with SCVMM

- **Practice 1** Create VMs with SCVMM and move through every option and each creation path, storing VMs on hosts and in the Library.
- **Practice 2** Clone VMs, move VMs, and copy VHDs. Learn how SCVMM gives you complete control over the VMs you manage on various hosts.

- **Practice 3** Generate templates from your VMs. Examine each step SCVMM performs when it creates and deploys templates. Also work with answer files to become familiar with their structure.

Working with the SCVMM Self-Service Portal

- **Practice 1** Install all of the prerequisites for the portal and then install the portal. Note the processes involved in the installation.
- **Practice 2** Create a user role and examine all of the features you can assign to the Self-Service Portal user role.
- **Practice 3** Log on to the Self-Service Portal as a user and perform user-oriented tasks. This will help you become familiar with the Self-Service Portal user experience.

Chapter Summary

- System Center Virtual Machine Manager allows you to manage several host systems and virtual machines at the same time and offers more functionality than Hyper-V Manager or the Failover Cluster Management console. Hyper-V Manager in particular only lets you work with one host server at a time. However, to be able to manage host servers with SCVMM, you need to deploy SCVMM agents.
- The SCVMM Administrator Console can be installed on various operating systems, but the console can only be installed on full installations when you deploy it on Windows Server 2008.
- Several operations are available in the SCVMM Administrator Console, depending on the selected view. You must always select the appropriate view first before performing an operation on a given object.
- SCVMM includes a default host group called All Hosts. Each host server you add is added to this group by default. However, you can and should create your own custom host groups and move host servers to these groups either through the Move command or by dragging and dropping.
- The SCVMM Library Server serves as a catalog for host file-based resources. The Library Server is installed automatically with the SCVMM Server during installation. A default Library folder is created under the %SystemRoot%\ProgramData\Virtual Machine Library Files folder and is shared as MSCVMMLibrary.
- The default Library also automatically creates two blank VHDs. Both are dynamically expanding VHDs.
- SCVMM includes one add-on called the Windows Automated Installation Kit (WAIK). SCVMM can also work with Windows Deployment Services (WDS). These tools are used to deploy massive numbers of servers. WAIK includes several utilities such as the Windows SIM, WinPE, and Sysprep.

- The process used to generate a new virtual machine from a reference computer is easier than the one used to generate a physical computer. You never have to regenerate the reference system; instead, you generate a clone of the reference computer and use the clone to depersonalize it. You also don't have to generate an image of the disk drives because the disk drives are already in file format.
- To clone a virtual machine in Hyper-V Manager you need to use a manual process. In SCVMM you use a process called VM cloning. This process copies the entire VM including configuration and any other files that may be part of the VM. After the VM is cloned you can use Sysprep to prepare a VM for duplication or use the clone to generate a VM template in SCVMM.
- The Self-Service Portal allows end users to deploy and manage their own VMs. The Self-Service Portal needs to be installed on a server operating system that includes IIS. The Self-Service Portal relies on custom VM templates that are stored in the Library. You need to create a special usage policy and assign it to the targeted users to allow them access to the Self-Service Portal. To manage and create policies, you must first create Self-Service User roles.

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?editorialid=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.

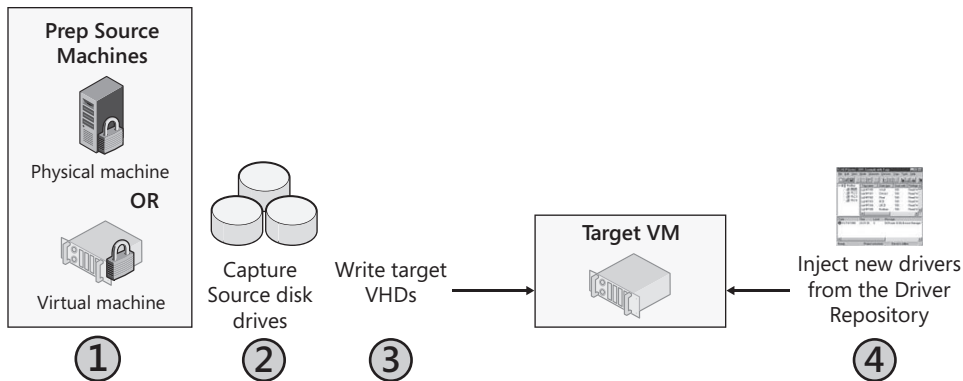


FIGURE 6-1 The key to P2V/V2V conversions is proper driver injection.

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 continues 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-8AE5-949DFBE59C4&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



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.

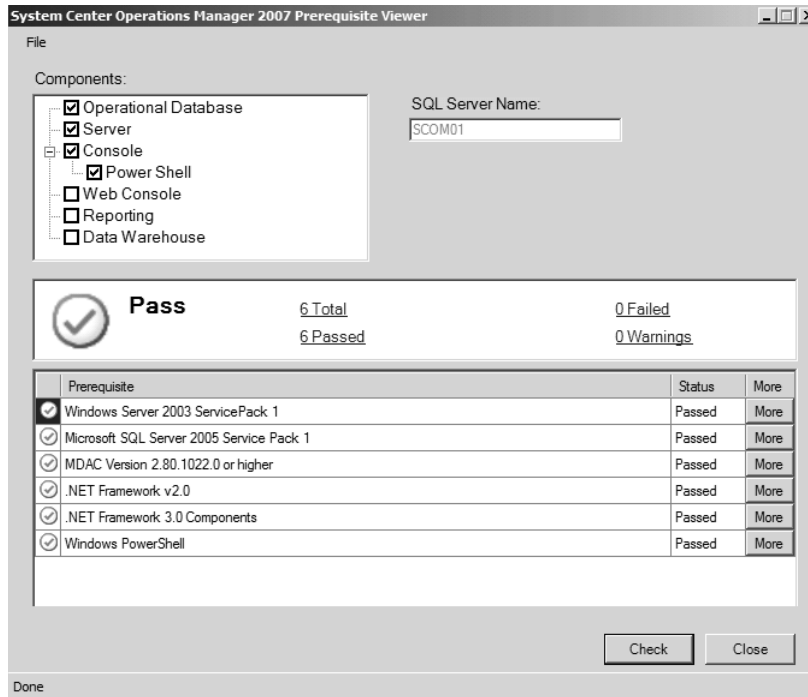


FIGURE 6-3 Verifying the OpsMgr 2007 SP1 prerequisites

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.

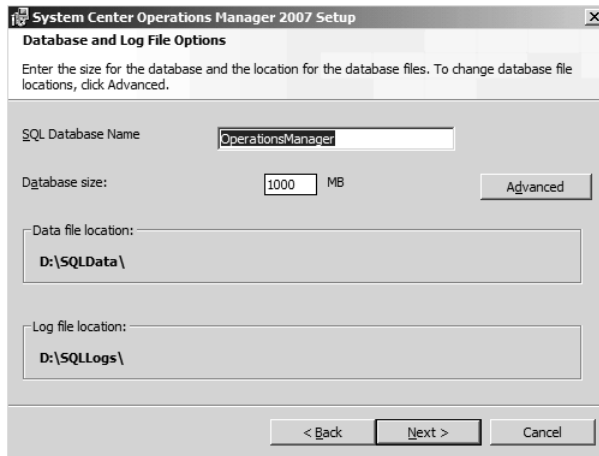


FIGURE 6-4 Choosing database settings for OpsMgr

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.

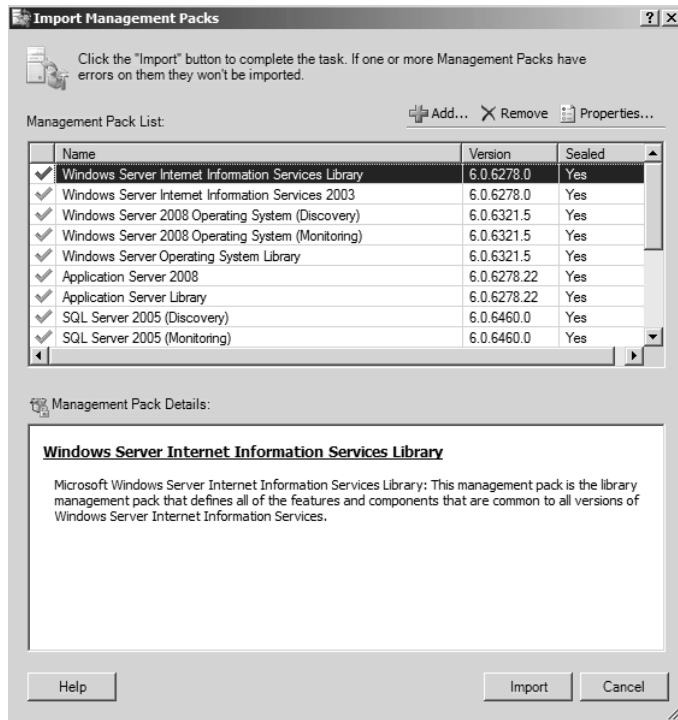


FIGURE 6-5 Importing management packs

- 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 SP1Upgrade.exe and then click Run to start the program.

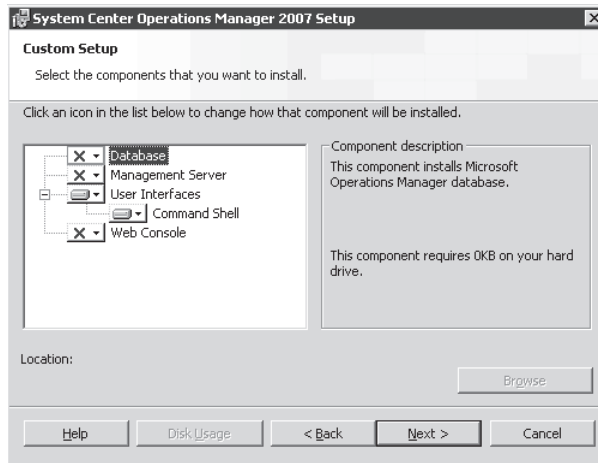


FIGURE 6-6 Installing the OpsMgr console

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 integration. 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.

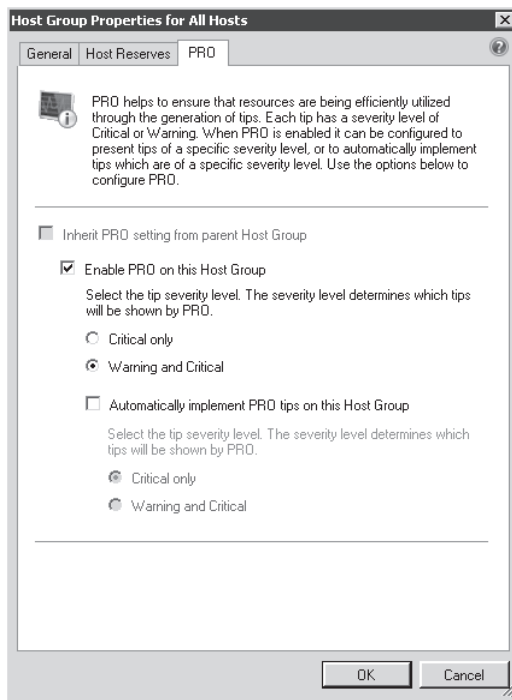


FIGURE 6-7 Enabling PRO

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

i 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.

i Virtual Machine Manager provides limited management of newly imported VMware ESX Server hosts.
[What restrictions apply?](#) [How do I enable full management?](#)

OK Cancel

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.

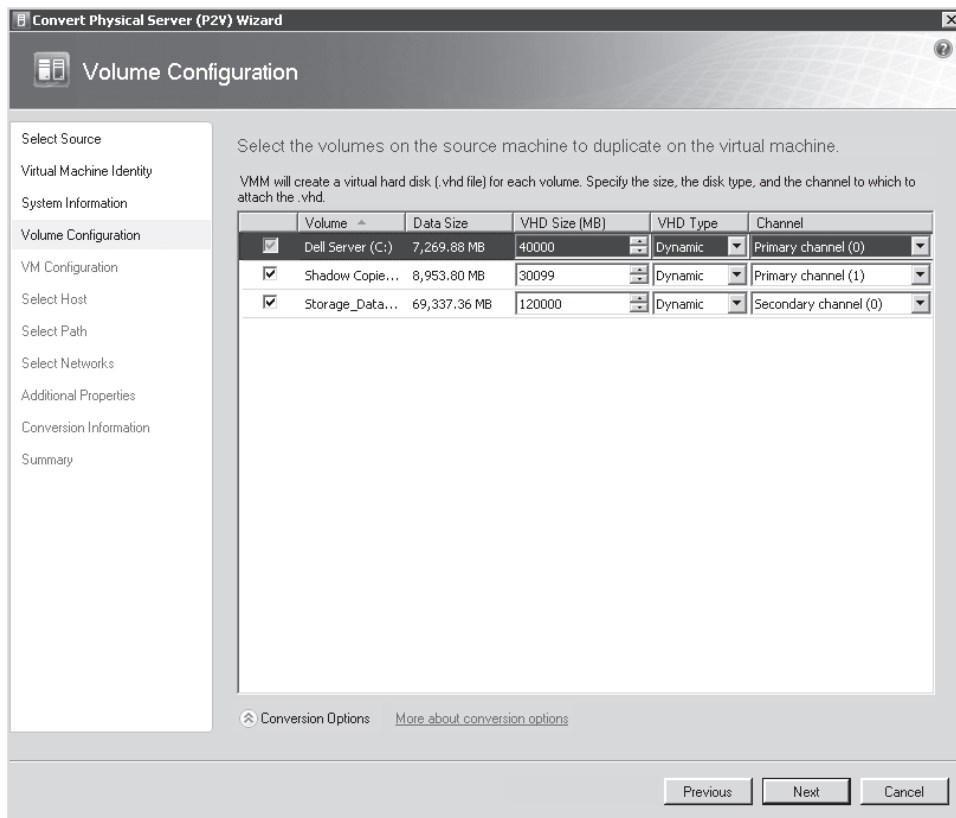


FIGURE 6-9 Resizing target VHDs

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.

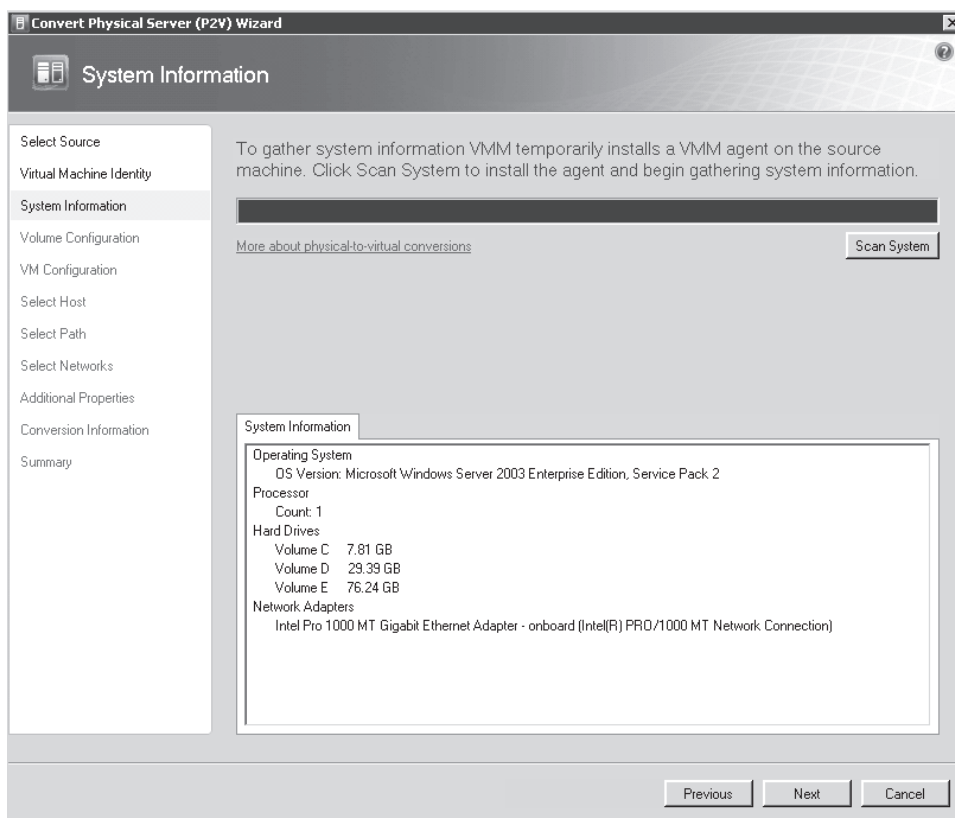


FIGURE 6-10 System information captured by the SCVMM P2V Agent

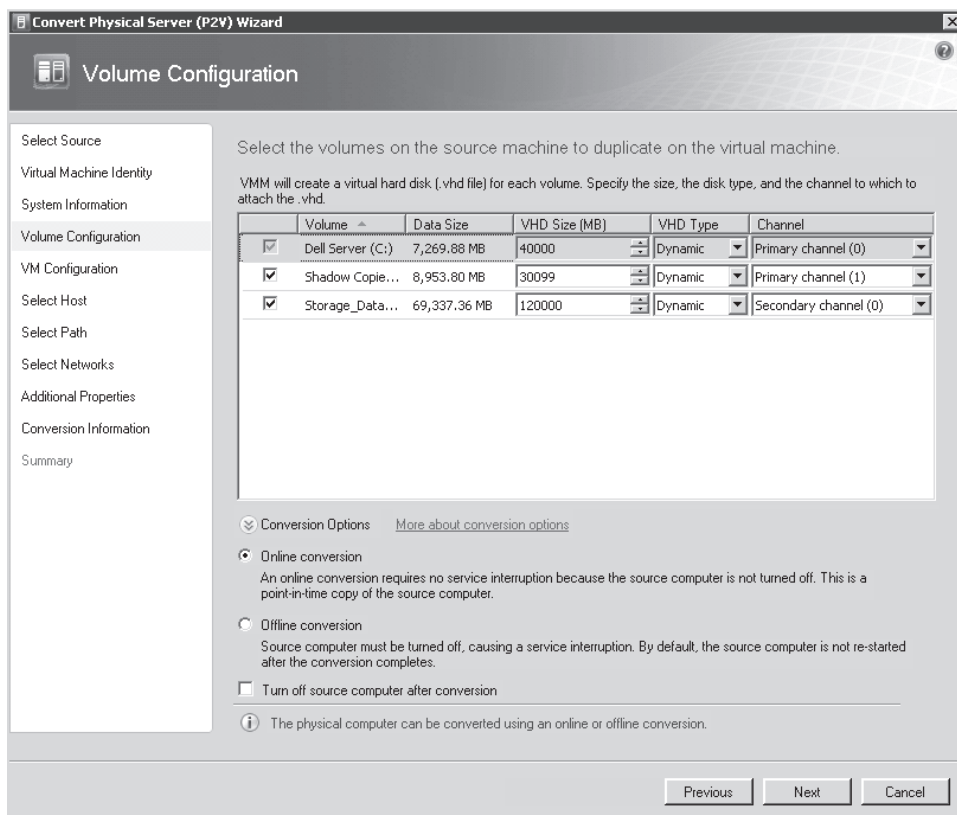


FIGURE 6-11 Choosing between online and offline conversions

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.

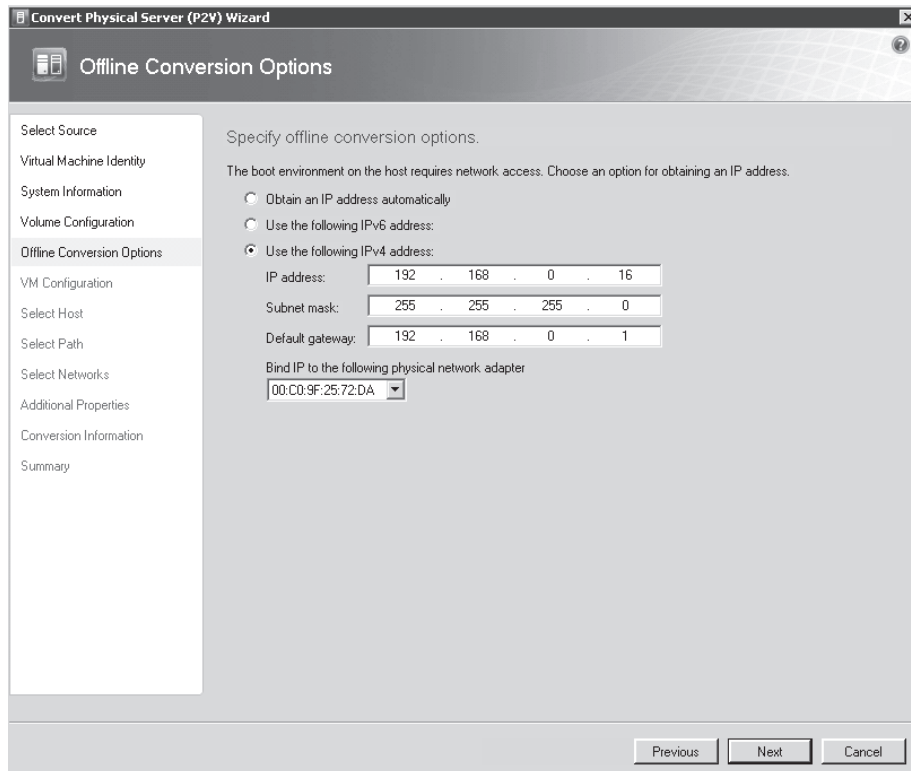


FIGURE 6-12 Assigning an IP address and network adapter for Windows PE

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.

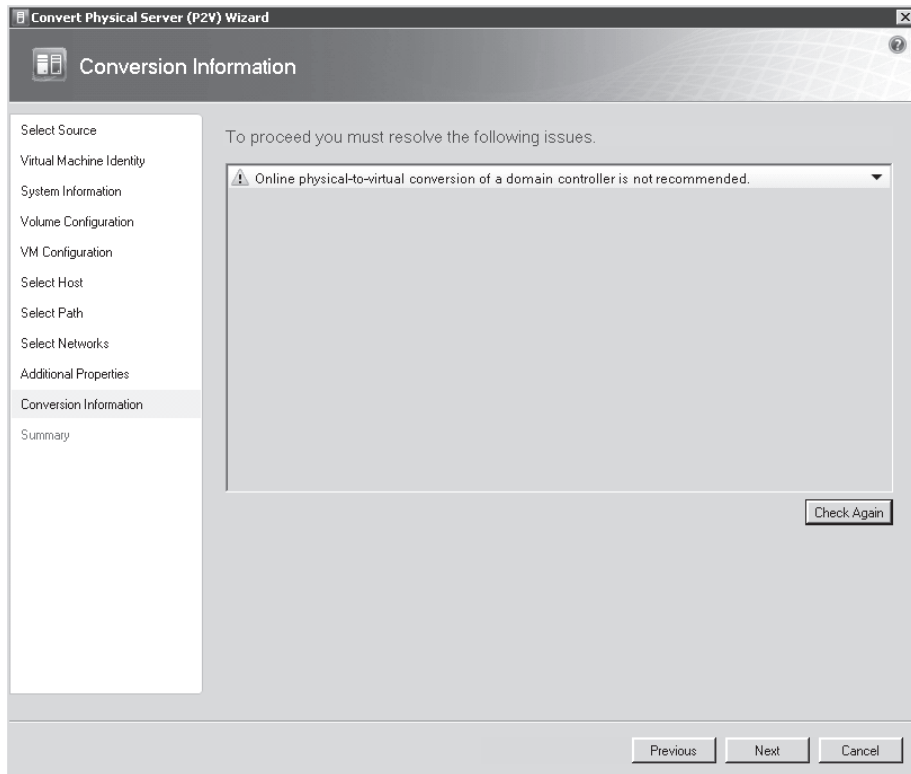


FIGURE 6-13 SCVMM does not recommend an online conversion for domain controllers.

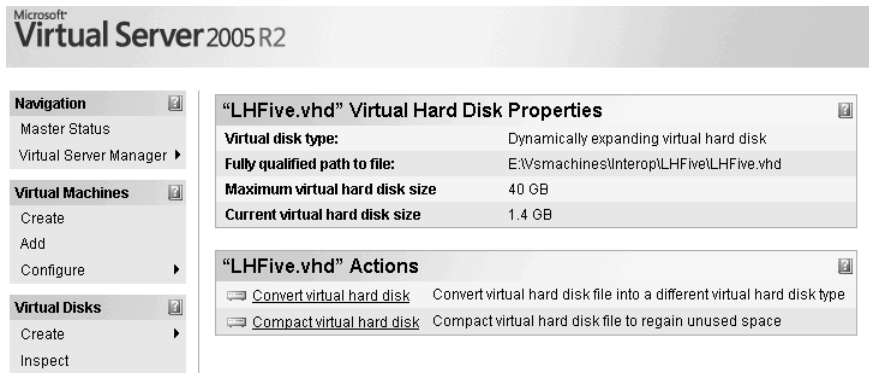


FIGURE 6-14 Preparing a VHD drive in Virtual Server

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.

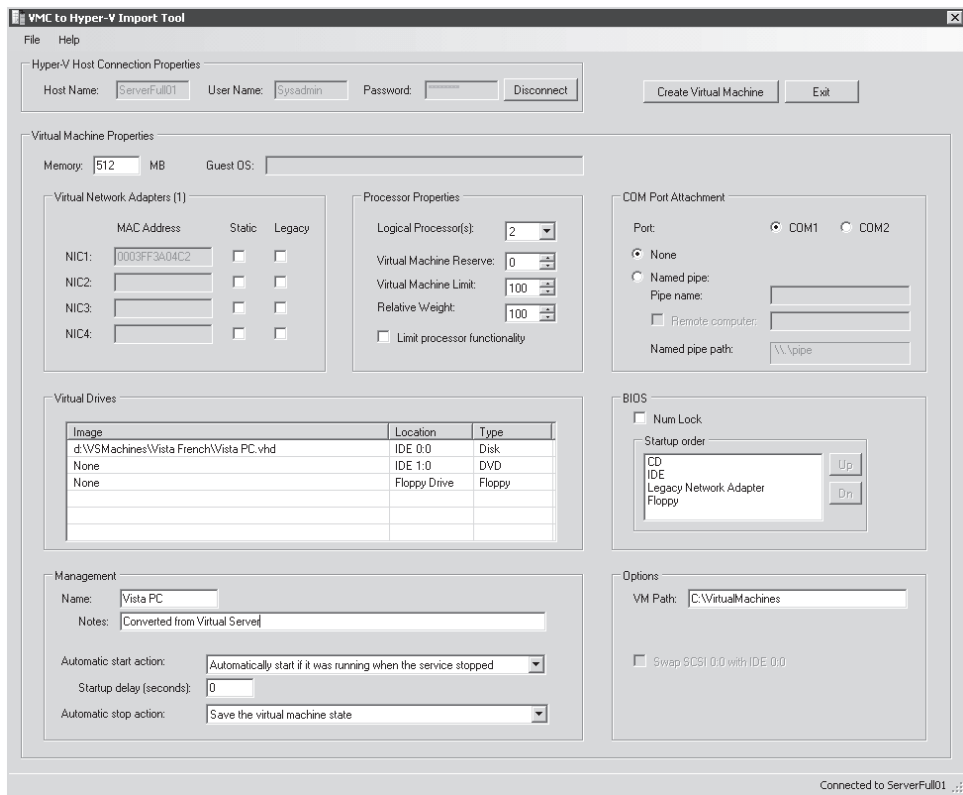


FIGURE 6-15 Converting a VMC to Hyper-V

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.

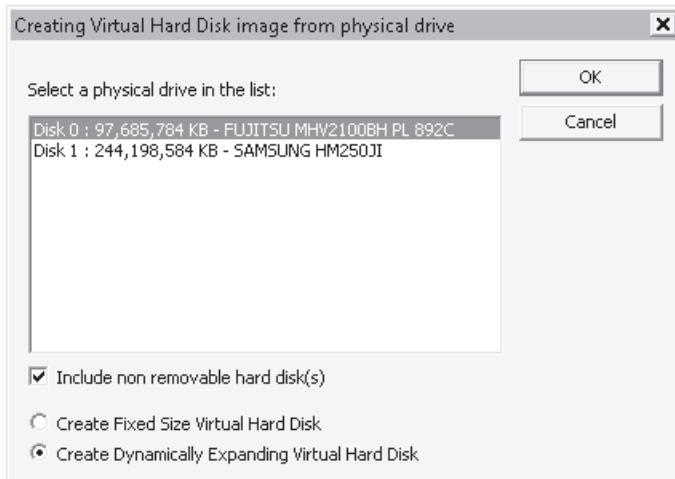


FIGURE 6-16 Using WinImage to convert a physical drive to a VHD

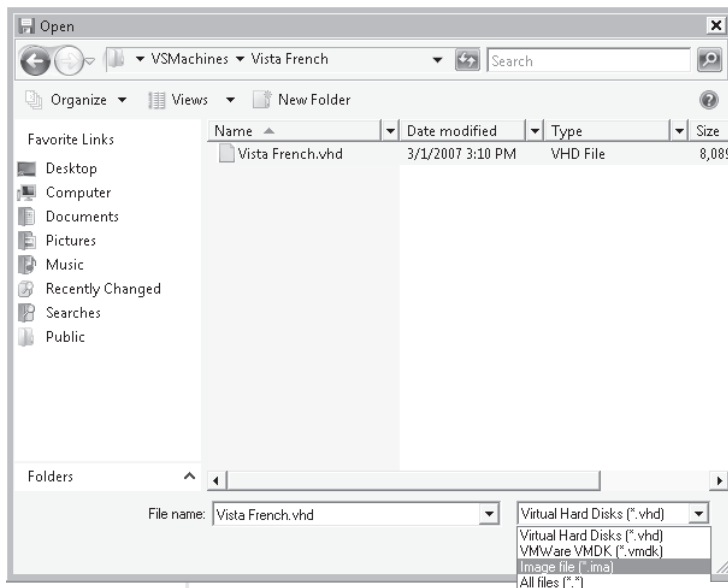


FIGURE 6-17 Using WinImage to convert a disk image to a virtual disk format

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.

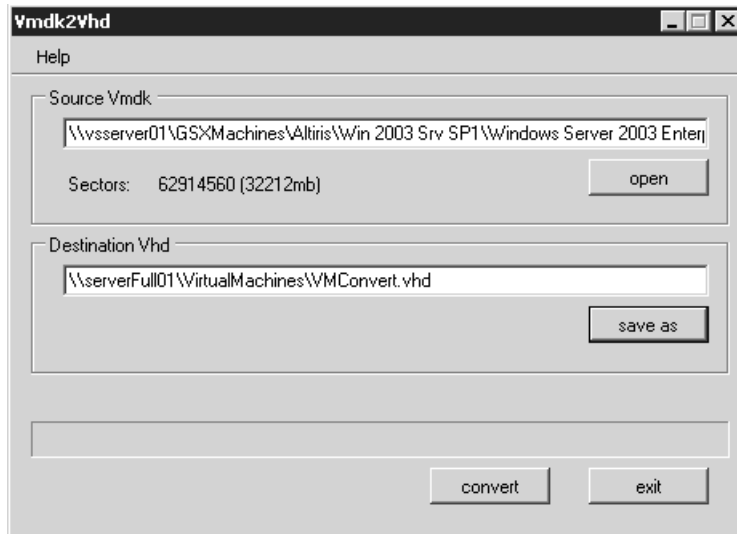


FIGURE 6-18 Converting a VMware disk to a virtual hard disk

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>.

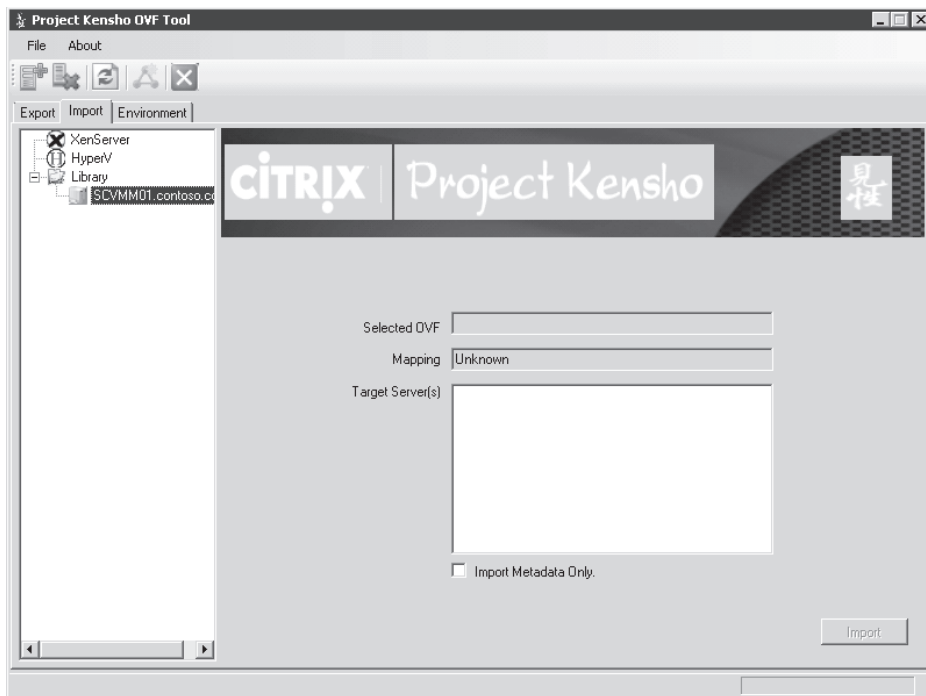


FIGURE 6-19 Running Project Kensho to convert OVF files

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).

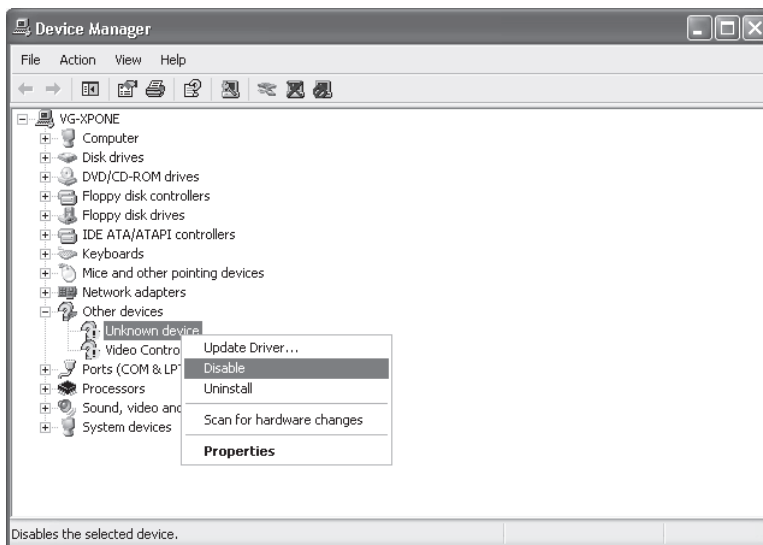


FIGURE 6-20 Disabling unknown devices in Windows XP

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.

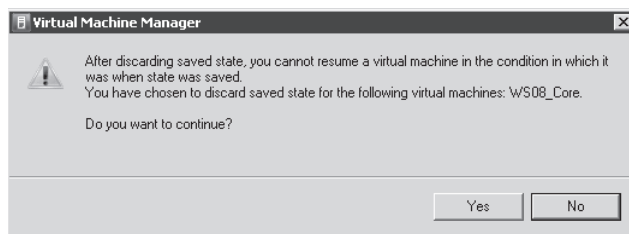


FIGURE 6-21 Discarding a saved state

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).

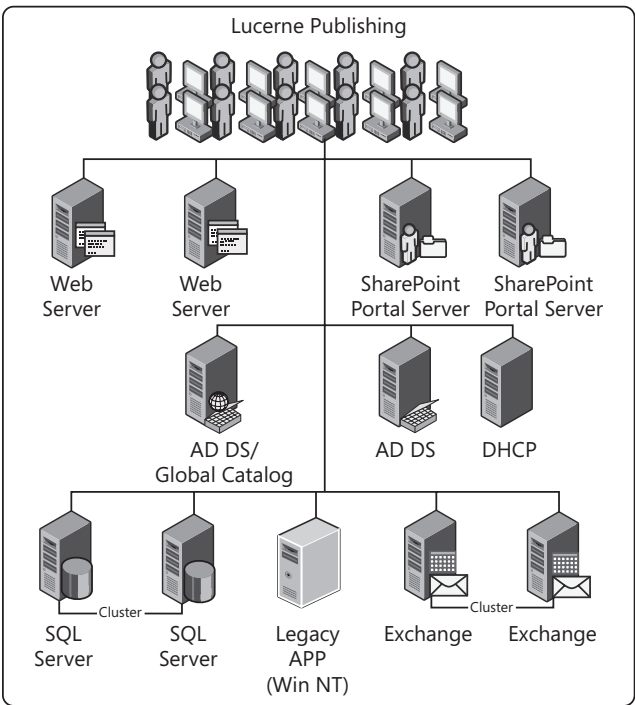


FIGURE 6-22 The Lucerne Publishing network

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.

Automating VM Management with Windows PowerShell

Administrators of small resource pools can easily get by with interactive operation of both the host servers and the VMs they manage, but administrators of medium to large resource pools need some form of automation to facilitate their daily operations workload. This is where Windows PowerShell can help. Windows PowerShell is a relatively new scripting environment developed solely for the Windows environment. Although Windows offered scripting through Microsoft Visual Basic, this scripting engine has had a rocky past. In addition, many viruses were generated and run using Visual Basic Scripting (VBS). This is one reason why many organizations shy away from VBS and another reason why Microsoft felt the need to develop a new extensible command-shell and associated scripting language: Windows PowerShell.

The Windows PowerShell environment is secure by default and will not allow unknown scripts to run. In addition—and this may be Windows PowerShell’s very best feature—more and more Microsoft products use graphical administration interfaces that are built on top of Windows PowerShell. The first of these was Microsoft Exchange Server 2007, but several others now exist: System Center Operations Manager 2007, System Center Virtual Machine Manager 2008, Microsoft SQL Server 2008, and more. What makes these interfaces so great is that each time you run through an operation using a wizard, the wizard generates a Windows PowerShell script that can be captured at the end of the operation and then reused to automate the operation; such is the case with SCVMM when you use the View Script button in any of its wizards (see Figure 7-1).

This means that you no longer need to be a developer or programmer to be able to script in Windows. All you need to do is use the graphical user interface to generate the script and then modify it to run against your systems. This greatly facilitates the scripting process.

However, if you want to become proficient in Windows PowerShell, you still need to learn its rudiments. Another great feature of Windows PowerShell is community support. Several organizations and individuals have added to the Windows PowerShell workspace. This has generated a whole series of tools and additional commands—or rather, cmdlets, because PowerShell is not a traditional command shell—for use by administrators everywhere that depend on Windows PowerShell to run their Windows networks. This also includes third-party organizations. For example, VMware offers a Virtual Infrastructure Toolkit powered by Windows PowerShell to manage its virtual infrastructures.

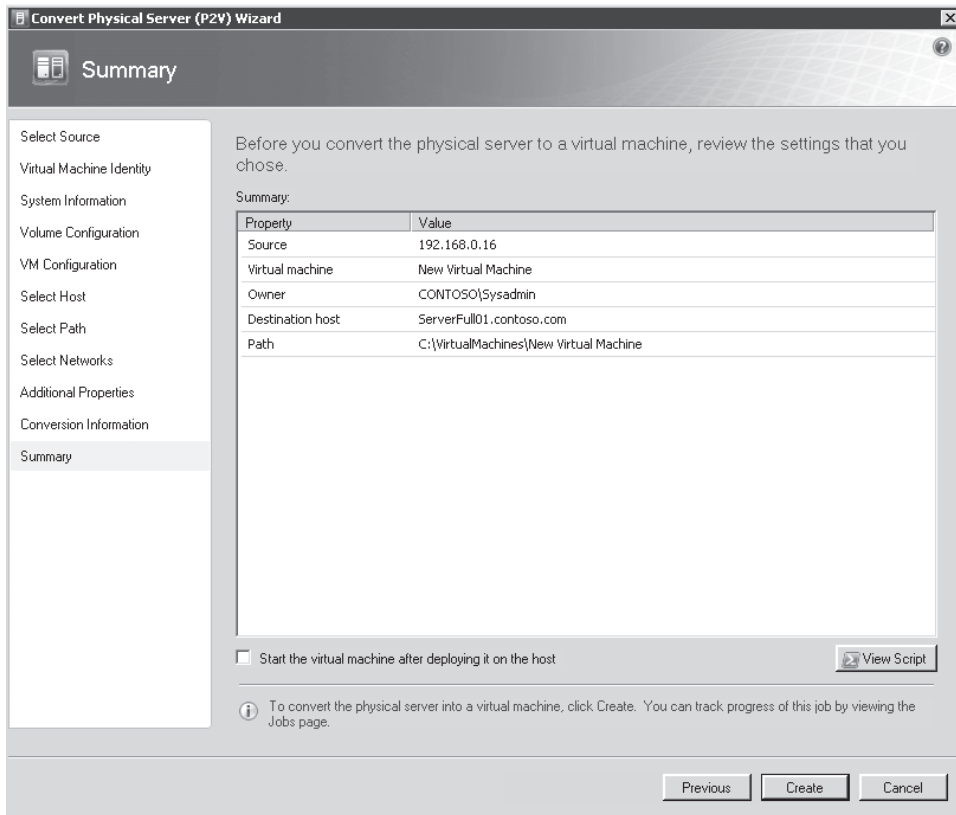


FIGURE 7-1 All SCVMM Scripts can be captured using the View Script button.

Without a doubt, Windows PowerShell is here to stay and is one of the very best tools you can learn to automate Windows workloads both on host servers and in virtual machines.

Exam objectives in this chapter:

- Manage and optimize the Hyper-V server.
- Monitor and optimize virtual machines.

Before You Begin

To complete this chapter, you must have:

- Access to a setup as described in the Introduction. In this case, you will automate Hyper-V operations with the Windows PowerShell scripting engine.
- Experience with some form of Windows scripting.

Lesson 1: Automating Hyper-V Operations with Windows PowerShell

Windows PowerShell helps automate operations within Hyper-V resource pools. As such, it proves to be a great addition to any Hyper-V management infrastructure.

After this lesson, you will understand:

- Windows PowerShell requirements.
- The benefits of using Windows PowerShell.
- The interaction of Windows PowerShell and the Windows Management Instrumentation (WMI).
- Windows PowerShell cmdlets for Hyper-V.
- Windows PowerShell cmdlets for SCVMM.
- Host and VM automation with Windows PowerShell.

Estimated lesson time: 50 minutes

Understanding Windows PowerShell

Windows PowerShell is a command interpreter built on top of the Microsoft .NET Framework, which—because of its access to .NET objects—can provide much more comprehensive programming capabilities than the basic command prompt ever will. Windows PowerShell is not installed by default on any platform. It does, however, get installed when you deploy tools such as Operations Manager, SCVMM, and Exchange, which are based on the Windows PowerShell engine. It is integrated into Windows Server 2008 as one of several features that are available for the platform.



EXAM TIP WINDOWS POWERSHELL AND HYPER-V

This chapter introduces you to Windows PowerShell and Hyper-V automation so that you can become familiar with this powerful tool. However, you are not expected to create Windows PowerShell scripts on the 70-652 exam. You should be able to recognize cmdlets for basic Hyper-V tasks such as those described in this chapter. For more complete information on Windows PowerShell, refer to *Windows PowerShell Scripting Guide* by Ed Wilson (Microsoft Press, 2008). You can also rely on the Windows PowerShell Documentation Pack, which is available for free at <http://www.microsoft.com/downloads/details.aspx?FamilyId=B4720B00-9A66-430F-BD56-EC48BFCA154F&displaylang=en>.

Windows PowerShell is both a command-line shell and a scripting language that includes more than 130 command-line tools that are called cmdlets (pronounced *command-lets*). Windows PowerShell provides both an interactive command prompt and

a scripting environment to perform and to automate administrative tasks. Cmdlets follow a very consistent syntax and naming convention. Windows PowerShell can be extended with custom cmdlets, which makes it a very powerful engine because its list of capabilities continues to grow.

Unlike the traditional command environment that is called upon when you run the CMD.exe engine in Windows, Windows PowerShell performs direct manipulation of .NET Framework objects at the command line. Windows PowerShell is also extensible because additional cmdlets can be created and loaded as a snap-in dynamic-link library (DLL).

Windows PowerShell is installed as a feature of Windows Server 2008. You can rely on either Server Manager or the Initial Configuration Tasks page in the full installation of Windows Server 2008 to add this feature. When Windows PowerShell is selected, Windows Server 2008 automatically selects the .NET Framework 3.0 feature in support of Windows PowerShell operation. This is one reason why Windows PowerShell does not execute on Server Core: the .NET Framework does not run on Server Core in this edition of Windows Server.

UPDATE ALERT WINDOWS POWERSHELL AND SERVER CORE

Microsoft has worked very hard to prepare a special version of the .NET Framework for operation on Server Core in Windows Server 2008 R2. The current version of the .NET Framework has graphical user interface dependencies that block it from running on Server Core. The version in Windows Server 2008 R2 no longer has these dependencies and can therefore run on Server Core. Because of this, you can run Windows PowerShell on Server Core in Windows Server 2008 R2.

After Windows PowerShell is installed, it can be accessed through the Start menu under All Programs. However, it is good practice to create a shortcut on the Quick Launch toolbar for this tool because it must be launched to be able to run cmdlets against it. Do not confuse the Windows PowerShell command window with CMD.exe. By default, the CMD.exe window uses a black background and lists the current folder at the command prompt. The Windows PowerShell window uses a dark blue background and precedes the command prompt with the letters *PS* (see Figure 7-2).

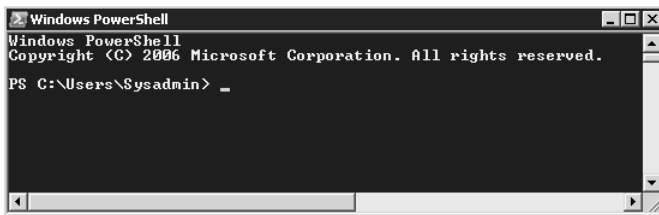


FIGURE 7-2 The Windows PowerShell command window

Note that two Windows PowerShell shortcuts are available when you run Windows PowerShell on an x64 platform such as a Hyper-V host. The first lists Windows PowerShell and the second lists Windows PowerShell (x86). The latter lets you run 32-bit commands only. You may need to use it if you still run 32-bit systems on your network.

MORE INFO WINDOWS POWERSHELL AND OTHER WINDOWS PLATFORMS

Windows Server 2008 is the only Windows platform that includes Windows PowerShell by default. If you want to run Windows PowerShell from your workstation or on other server versions of Windows, you must download it. Windows PowerShell is available in both 32-bit and 64-bit formats. It can be obtained from <http://www.microsoft.com/windowsserver2003/technologies/management/powershell/download.mspx>. Make sure you obtain the appropriate version for your target system.

Although you can't run Windows PowerShell on Server Core, you can still execute Windows PowerShell cmdlets against Server Core installations remotely. Windows PowerShell can run commands on the local machine as well as on remote machines. In addition, although the Windows PowerShell command window is not the same as the CMD.exe window, it is backward compatible, which means that all of the CMD.exe commands you are familiar with will continue to run in Windows PowerShell. Although the Windows PowerShell cmdlet syntax is not the same as the Windows command syntax, Windows PowerShell supports the creation of *aliases*—shortcuts that can be added to a Windows PowerShell environment at any time—and includes many of these by default. For example, although the *dir* command is not a cmdlet, you can still type **dir** at the Windows PowerShell prompt and get the same results that you would get at the command prompt. When you use an alias, it automatically calls the corresponding cmdlet.

When you work with the familiar command prompt in Windows, you issue commands based on utilities that are built into the Windows shell or you work with executable programs such as *xcopy.exe*. Both the utilities and the executables accept parameters and return results in the form of output or error codes.

In Windows PowerShell, you issue directives through cmdlets—single-feature commands that manipulate a specific object. Cmdlets use a Verb-Noun syntax; that is, they rely on a verb associated with a noun and separated with a hyphen. For example, to list information on a service, you use *Get-Service* and to start a service, you use *Start-Service*.

An object is a programming construct that provides a virtual representation of a resource of some type. A .NET object is an instance of a .NET class that consists of data and the operations associated with that data. For example, the *Get-Service* cmdlet returns one or more objects representing services. An object can have properties that represent data or attributes maintained by the resource. The service object in the *Get-Service* example has properties for the service name and its startup state. When you get a property, you retrieve the data for the resource, and when you set a property, you write data to that resource.

An object can also have methods—actions that can be performed on the object. For example, the *service* object has *start* and *stop* methods. Performing a method on an object that represents a resource performs the action on the resource itself.

Cmdlets can be typed in Windows PowerShell interactively or saved in a script file that can then be executed by Windows PowerShell. Windows PowerShell script files are pure text files that use a .PS1 extension. Cmdlets are simple and can work in combination with

other cmdlets. For example, a cmdlet using the *Get* verb retrieves data about an object, and a cmdlet using the *Set* verb specifies or changes data for the target object. If you type the **Get-Service** cmdlet, Windows PowerShell returns a collection of objects for all services because no explicit service is specified. The result is displayed as a table showing the service's status, name, and display name (see Figure 7-3).

```

Windows PowerShell (X86)
Windows PowerShell
Copyright (C) 2006 Microsoft Corporation. All rights reserved.

PS C:\Users\Sysadmin> Get-Service

Status      Name                DisplayName
-----
Stopped     AdtAgent            Operations Manager Audit Forwarding...
Running     AeLookupSvc        Application Experience
Stopped     ALG                Application Layer Gateway Service
Running     AppHostSvc         Application Host Helper Service
Running     Appinfo            Application Information
Stopped     AppMgmt            Application Management
Stopped     aspnet_state       ASP.NET State Service
Stopped     AudioEndpointBu... Windows Audio Endpoint Builder
Stopped     AudioSrv           Windows Audio
Running     BFE                Base Filtering Engine
Running     BITS               Background Intelligent Transfer Ser...
Stopped     Browser            Computer Browser
Running     CertPropSvc        Certificate Propagation
Stopped     clr_optimizatio... Microsoft .NET Framework NGEN v2.0....
Stopped     clr_optimizatio... Microsoft .NET Framework NGEN v2.0....
Running     COMSysApp          COM+ System Application
Running     CryptSvc           Cryptographic Services
Stopped     CscService         Offline Files
Running     DcomLaunch         DCOM Server Process Launcher
Running     Dhcp               DHCP Client
Running     Dnscache           DNS Client
Stopped     dot3svc            Wired AutoConfig

```

FIGURE 7-3 The results of the *Get-Service* cmdlet

Windows PowerShell directives can include one or more cmdlets. They can also contain one or more cmdlet parameters or other elements. For example, you can use the pipe character (*|*) to pass the output of one cmdlet to another cmdlet to produce a different result (see Figure 7-4).

```

Windows PowerShell (X86)
PS C:\Users\Sysadmin> Get-Service | Format-List

Name                : AdtAgent
DisplayName          : Operations Manager Audit Forwarding Service
Status              : Stopped
DependentServices   : {}
ServicesDependedOn  : {eventlog, dnscache}
CanPauseAndContinue : False
CanShutdown         : False
CanStop             : False
ServiceType         : Win32OwnProcess

Name                : AeLookupSvc
DisplayName          : Application Experience
Status              : Running
DependentServices   : {}
ServicesDependedOn  : {}
CanPauseAndContinue : False
CanShutdown         : False
CanStop             : True
ServiceType         : Win32ShareProcess

Name                : ALG
DisplayName          : Application Layer Gateway Service
Status              : Stopped
DependentServices   : {}
ServicesDependedOn  : {}
CanPauseAndContinue : False

```

FIGURE 7-4 The *Get-Service | Format-List* cmdlet result

For example:

Get-Service | Format-List

This directive provides much more detail on the objects and the attributes of the services. As you can see, the `Get-Service` cmdlet not only returns a static list of results, but it also returns data on the objects representing the services. This means that when you apply the `Format-List` cmdlet to the results of `Get-Service`, the second cmdlet can work directly with the returned objects and display the attributes of the services.

In this case, the `Format-List` cmdlet makes decisions about which attributes to display. You can force it to show all properties by adding a parameter or property to the cmdlet and assign a value of all—by using the asterisk character (*)—to the property. The result is a list of all available properties for all services (see Figure 7-5). The cmdlet structure is as follows:

Get-Service | Format-List -Property *

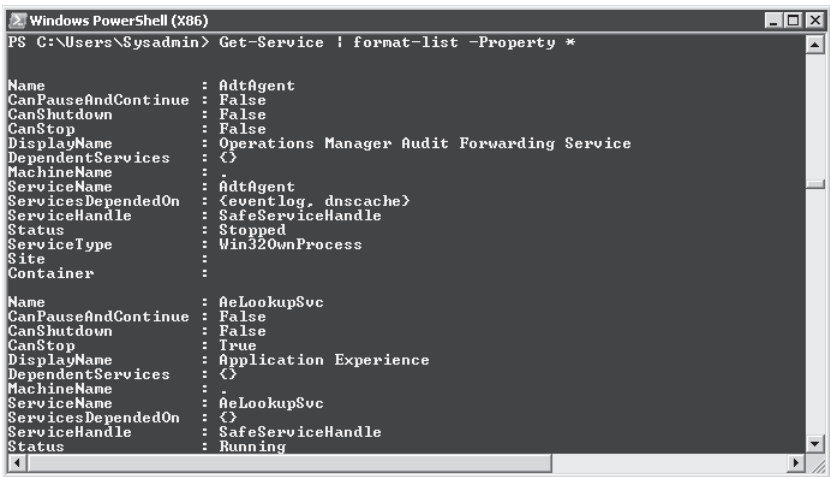


FIGURE 7-5 The `Get-Service | Format-List -property *` cmdlet result

Understanding the Makeup of Windows PowerShell

When you work with Windows PowerShell, you need to work with several different constructs. Table 7-1 outlines some of the most important constructs you will work with.

TABLE 7-1 Essential PowerShell Constructs

CONSTRUCT	DESCRIPTION	CMDLET
Creating variables	When you repeatedly use the same path or object definition in a cmdlet, you can save considerable time by assigning it to a variable. Variables always begin with a dollar sign (\$). For example, instead of typing Get-Service DNS over and over again, you can assign DNS to a variable.	<code>\$DNS=</code> <code>get-service DNS</code>

CONSTRUCT	DESCRIPTION	CMDLET
Using variables	When you assign a variable, you create an object reference, and once you have an object reference, you can use the dot (.) properties to obtain information about the object referenced in the variable. For example, you can use your variable with <code>.status</code> to obtain the status of the service.	<code>\$DNS.status</code>
Special variables	You can use a special pipeline variable as a placeholder for the current object within the current pipeline. This pipeline variable is <code>\$_</code> . Use this to qualify the output you are looking for. For example, you can use the pipeline variable to obtain a list containing only running services.	<code>get-service where-object { \$_.status -eq "Running" }</code>
Using aliases	Aliases are shorthand representations of cmdlets and are designed to shorten the amount of text required in a cmdlet as well as simplifying how to learn Windows PowerShell. For example, <i>Where-Object</i> has an alias of <i>Where</i> . This means that the previous cmdlet can be shortened.	<code>get-service where { \$_.status -eq "Running" }</code>
Aliases vs. cmdlets	Many aliases have been created in Windows PowerShell to simplify the learning curve for this powerful tool. For example, <i>Get-ChildItem</i> is the cmdlet you use to list the contents of a folder. However, this cmdlet also has an alias of <i>dir</i> . To get the same result as <i>Get-ChildItem</i> , you simply type dir .	<code>dir</code>
Finding aliases	There are several aliases in Windows PowerShell. To determine whether a cmdlet is an alias, you can precede it with the <i>alias</i> cmdlet.	<code>alias dir</code>
Aliases vs. commands	Even though aliases have been created to simplify learning Windows PowerShell, they do not work the same way in Windows PowerShell as they do in the Command Prompt window. For example, you cannot use <i>dir /s</i> to obtain a list of the contents of the current folder and all its subfolders. You must use a structure that Windows PowerShell understands.	<code>dir -recurse</code>

CONSTRUCT	DESCRIPTION	CMDLET
Using PSDrives	When you work with a cmdlet, you use the cmdlet against a namespace—a specific naming context that is created by a particular provider. The Windows file system and the registry are both providers that generate namespaces. Instead of representing the namespace in the same way as you would in the file system—using a drive letter for either a local or a networked drive—or for a registry hive, Windows PowerShell assigns it to a PSDrive. For example, instead of using <i>HKey_Local_Machine</i> to access a hive in the registry, Windows PowerShell uses the HKLM PSDrive. This shortens the way you access the object and lets you treat it in more familiar ways. To view the contents of the registry, you can use the cmdlet/alias structure in the next column to treat it as a drive.	<i>Cd hklm:\software</i> <i>dir</i>
Finding PSDrives	Windows PowerShell creates several PSDrives when it is launched. You can use the cmdlet in the next column to find out which PSDrives have been assigned (see Figure 7-6).	<i>Get-PSDrive</i>

```

Windows PowerShell (X86)
PS C:\Users\Sysadmin> get-psdrive

Name      Provider      Root
-----
A         FileSystem    A:\
Alias     Alias         C:\
C         FileSystem    C:\
cert      Certificate    \
D         FileSystem    D:\
E         FileSystem    E:\
Env       Environment
Function  Function
HKCU      Registry      HKEY_CURRENT_USER
HKLM      Registry      HKEY_LOCAL_MACHINE
Variable  Variable
PS C:\Users\Sysadmin> _

```

FIGURE 7-6 Listing PSDrives

As you can see, Windows PowerShell provides a much richer automation and administration environment than the command prompt ever will.

Using Windows PowerShell

Just like the command prompt, you need to open a Windows PowerShell interpreter to run cmdlets. After Windows PowerShell is installed, you click Start, click All Programs, click Windows PowerShell 1.0, and then click Windows PowerShell to open a PowerShell prompt.

Use the Documents folder within the Windows PowerShell Start menu item to access Windows PowerShell documentation and reference information.

Table 7-2 lists the various cmdlets and aliases you can find in a default implementation of Windows PowerShell. Use this table as a reference to locate the cmdlets you need.

TABLE 7-2 Default Windows PowerShell Cmdlets

CMDLET	DESCRIPTION
<i>Add-Content</i>	Use to add contents to a specified item.
<i>Add-History</i>	Use to add a list of commands used during a current session to the end of the session history.
<i>Add-Member</i>	Use to add a user-defined custom member to an instance of a Windows PowerShell object.
<i>Add-PSSnapin</i>	Use to add one or more Windows PowerShell snap-ins to a current console.
<i>Clear-Content</i>	Use to delete the contents of an item.
<i>Clear-Item</i>	Use to delete the contents of an item.
<i>Clear-ItemProperty</i>	Use to delete a value of a property.
<i>Clear-Variable</i>	Use to delete a value of a variable.
<i>Compare-Object</i>	Use to compare two sets of objects.
<i>ConvertFrom-SecureString</i>	Use to convert a secure string into an encrypted standard string.
<i>Convert-Path</i>	Use to convert a Windows PowerShell path to a Windows PowerShell provider path.
<i>ConvertTo-Html</i>	Use to create an HTML page that represents an object or a set of objects.
<i>ConvertTo-SecureString</i>	Use to convert encrypted standard strings to secure strings; converts plain text to secure strings. Use with <i>ConvertFrom-SecureString</i> and <i>Read-Host</i> .
<i>Copy-Item</i>	Use to copy an item from one location to another within a namespace.
<i>Copy-ItemProperty</i>	Use to copy a property value from a specified location to another.
<i>Export-Alias</i>	Use to export information about currently defined aliases to a file.
<i>Export-Clixml</i>	Use to create an XML-based representation of an object(s) and stores it in a file.

CMDLET	DESCRIPTION
<i>Export-Console</i>	Use to export the configuration of a current console to a file to be reused or shared.
<i>Export-Csv</i>	Use to create a comma-separated values (CSV) file that represents the input objects.
<i>ForEach-Object</i>	Use to perform an operation against each of a set of input objects.
<i>Format-Custom</i>	Use for a customized view to format the output.
<i>Format-List</i>	Use to format the output as a list of properties in which each property appears on a new line.
<i>Format-Table</i>	Use to format the output as a table.
<i>Format-Wide</i>	Use to format objects as a wide table that displays only one property of each object.
<i>Get-Acl</i>	Use to get the security descriptor for a resource, such as a file or registry key.
<i>Get-Alias</i>	Use to get the aliases for a current session.
<i>Get-AuthenticodeSignature</i>	Use to get information about the Authenticode signature in a file.
<i>Get-ChildItem</i>	Use to get the items and child items in one or more specified locations.
<i>Get-Command</i>	Use to get basic information about cmdlets and other elements of Windows PowerShell commands.
<i>Get-Content</i>	Use to get the content of an item at the specified location.
<i>Get-Credential</i>	Use to get a credential object based on a user name and password.
<i>Get-Culture</i>	Use to get information about the regional settings on a computer.
<i>Get-Date</i>	Use to get the current date and time.
<i>Get-EventLog</i>	Use to get information about local event logs or their entries.
<i>Get-ExecutionPolicy</i>	Use to get the current execution policy for the shell.
<i>Get-Help</i>	Use to display information on Windows PowerShell cmdlets and concepts.
<i>Get-History</i>	Use to get a list of the commands entered during a current session.

CMDLET	DESCRIPTION
<i>Get-Host</i>	Use to get a reference to a current console host object. Displays Windows PowerShell version and regional information by default.
<i>Get-Item</i>	Use to get an item at a specified location.
<i>Get-ItemProperty</i>	Use to retrieve the properties of a specified item.
<i>Get-Location</i>	Use to get information on a current working location.
<i>Get-Member</i>	Use to get information about objects or collections of objects.
<i>Get-PfxCertificate</i>	Use to get information on .pfx certificate files on a computer.
<i>Get-Process</i>	Use to get processes that are running on a local computer.
<i>Get-PSDrive</i>	Use to get information on Windows PowerShell drives.
<i>Get-PSProvider</i>	Use to get information on a specified Windows PowerShell provider.
<i>Get-PSSnapin</i>	Use to get the Windows PowerShell snap-ins on a computer.
<i>Get-Service</i>	Use to get a service on a local computer.
<i>Get-TraceSource</i>	Use to get Windows PowerShell components that are instrumented for tracing.
<i>Get-UIThread</i>	Use to get information on the current user interface culture for Windows PowerShell.
<i>Get-Unique</i>	Use to return a unique items from a sorted list.
<i>Get-Variable</i>	Use to get variables in a current console.
<i>Get-WmiObject</i>	Use to get instances of WMI classes or information about available classes.
<i>Group-Object</i>	Use to group objects that contain the same value for specified properties.
<i>Import-Alias</i>	Use to import an alias list from a file.
<i>Import-Clixml</i>	Use to import a CLIXML file and to create corresponding objects within Windows PowerShell.
<i>Import-Csv</i>	Use to import comma-separated value (CSV) files in the format produced by the <i>Export-CSV</i> cmdlet and return objects that correspond to the objects represented in that CSV file.
<i>Invoke-Expression</i>	Use to run a Windows PowerShell expression that is provided in the form of a string.

CMDLET	DESCRIPTION
<i>Invoke-History</i>	Use to run commands from a session history.
<i>Invoke-Item</i>	Use to invoke a provider-specific default action on a specified item.
<i>Join-Path</i>	Use to combine a path and child-path into a single path. The provider supplies the path delimiters.
<i>Measure-Command</i>	Use to measure the time it takes to run script blocks and cmdlets.
<i>Measure-Object</i>	Use to measure characteristics of objects and their properties.
<i>Move-Item</i>	Use to move an item from one location to another.
<i>Move-ItemProperty</i>	Use to move a property from one location to another.
<i>New-Alias</i>	Use to create a new alias.
<i>New-Item</i>	Use to create a new item in a namespace.
<i>New-ItemProperty</i>	Use to set a new property of an item at a location.
<i>New-Object</i>	Use to create an instance of a .NET or COM object.
<i>New-PSDrive</i>	Use to install a new Windows PowerShell drive.
<i>New-Service</i>	Use to create a new entry for a Windows Service in the registry and the Service Database.
<i>New-TimeSpan</i>	Use to create a <i>TimeSpan</i> object.
<i>New-Variable</i>	Use to create a new variable.
<i>Out-Default</i>	Use to send an output to the default formatter and the default output cmdlet.
<i>Out-File</i>	Use to send output to a file.
<i>Out-Host</i>	Use to send output to a command line.
<i>Out-Null</i>	Use to delete output instead of sending it to a console.
<i>Out-Printer</i>	Use to send output to a printer.
<i>Out-String</i>	Use to send objects to a host as a series of strings.
<i>Pop-Location</i>	Use to change the current location to a location most recently pushed onto the stack.
<i>Push-Location</i>	Use to push a current location onto the stack.
<i>Read-Host</i>	Use to read a line of input from a console.
<i>Remove-Item</i>	Use to delete a specified items.
<i>Remove-ItemProperty</i>	Use to delete a property and its value from an item.

CMDLET	DESCRIPTION
<i>Remove-PSDrive</i>	Use to delete a Windows PowerShell drive from its location.
<i>Remove-PSSnapin</i>	Use to remove Windows PowerShell snap-ins from current location.
<i>Remove-Variable</i>	Use to delete a variable and its value.
<i>Rename-Item</i>	Use to rename an item in a Windows PowerShell provider namespace.
<i>Rename-ItemProperty</i>	Use to rename a property of an item.
<i>Resolve-Path</i>	Use to resolve a wildcard character in a path and to display the path contents.
<i>Restart-Service</i>	Use to stop and then start one or more services.
<i>Resume-Service</i>	Use to resume one or more paused services.
<i>Select-Object</i>	Use to select specified properties of an object or set of objects.
<i>Select-String</i>	Use to identify patterns in strings.
<i>Set-Acl</i>	Use to change the security descriptor of a specified resource, such as a file or registry key.
<i>Set-Alias</i>	Use to create or change an alias for a cmdlet or other command element in a current Windows PowerShell session.
<i>Set-AuthenticodeSignature</i>	Use an Authenticode signature to sign a Windows PowerShell script or other file.
<i>Set-Content</i>	Use to write or replace the content in an item with new content.
<i>Set-Date</i>	Use to change the system time on a computer.
<i>Set-ExecutionPolicy</i>	Use to change user preference for the execution policy of the shell.
<i>Set-Item</i>	Use to change the values of an item to the value specified in a command.
<i>Set-ItemProperty</i>	Use to set the values of a property at the specified location.
<i>Set-Location</i>	Use to set a current working location to a specified location.
<i>Set-PSDebug</i>	Use to turn script debugging features on and off, to set the trace level, and toggles Strict mode.
<i>Set-Service</i>	Use to change a display name and description, or starts the mode of a service.

CMDLET	DESCRIPTION
<i>Set-TraceSource</i>	Use to configure, start, and stop a trace of Windows PowerShell components.
<i>Set-Variable</i>	Use to set a value of a variable and to create a variable if one with the requested name does not exist.
<i>Sort-Object</i>	Use to sort objects by property values.
<i>Split-Path</i>	Use to return to a specified part of a path.
<i>Start-Service</i>	Use to start one or more stopped services.
<i>Start-Sleep</i>	Use to suspend shell, script, or run space activity for a specified period of time.
<i>Start-Transcript</i>	Use to create a record of all or part of a Windows PowerShell session in a text file.
<i>Stop-Process</i>	Use to stop one or more running processes.
<i>Stop-Service</i>	Use to stop one or more running services.
<i>Stop-Transcript</i>	Use to stop a transcript.
<i>Suspend-Service</i>	Use to pause one or more running services.
<i>Tee-Object</i>	Use to pipe object input to a file or variable, then pass the input along the pipeline.
<i>Test-Path</i>	Use to determine whether all elements of a path exist.
<i>Trace-Command</i>	Use to configure and start a trace of a specified expression or command.
<i>Update-FormatData</i>	Use to update and append format data files.
<i>Update-TypeData</i>	Use to update a current extended type configuration by reloading the *.types.ps1xml files into memory.
<i>Where-Object</i>	Use to create a filter that controls which objects are passed along a command pipeline.
<i>Write-Debug</i>	Use to write a debug message to a host display.
<i>Write-Error</i>	Writes an object to an error pipeline.
<i>Write-Host</i>	Use to display objects by using a host user interface.
<i>Write-Output</i>	Use to write objects to a success pipeline.
<i>Write-Progress</i>	Use to display a progress bar within a Windows PowerShell command window.
<i>Write-Verbose</i>	Use to write a string to a verbose display of a host.
<i>Write-Warning</i>	Use to write a warning message.

When you want to learn more about a cmdlet or get help on the cmdlet's syntax, you can use the *Get-Help* cmdlet or simply the *Help* alias along with the cmdlet you need help with. For example, using the following cmdlet will produce information on *Get-Service*:

```
Get-Help Get-Service
```

You can also qualify the *Get-Help* cmdlet with the *Detailed* or *Full* parameters to obtain more detailed information:

```
Get-Help Get-Service -Full
```

```
Get-Help Get-Service -Detailed
```

Get-Help also supports the *Example*, *Syntax*, *Property*, and *Parameter* parameters.

MORE INFO TYPING CMDLETS

Note that cmdlets are not case sensitive. Typing **Get-Service** will produce exactly the same results as typing **get-service**.

Running Windows PowerShell Scripts

Although you need to install Windows PowerShell on your computer to be able to create and run Windows PowerShell scripts, you do not need to install it on remote systems to be able to execute Windows PowerShell scripts against them. That is because the script actually executes on your own system and only executes operations on the remote system. This makes it easier to work with Windows PowerShell scripts in a Windows environment, especially if you have Server Core installations, as you should with the resource pool.

By default, Windows PowerShell does not support the ability to run scripts. This is because its execution policy—the policy that runs scripts—is set to *Restricted* by default, which means that no scripts are allowed to run. To enable scripting on your system, open the PowerShell prompt and then use the following Windows PowerShell cmdlets to set your Windows PowerShell policy:

```
Get-ExecutionPolicy
```

```
Set-ExecutionPolicy RemoteSigned
```

The first command lists the current policy. The second command lets all of your own scripts run, but will run downloaded scripts only if they are digitally signed. This is the best policy, because allowing scripts to run has security implications.

MORE INFO MORE ON SCRIPTING WITH WINDOWS POWERSHELL

To find out more information on Windows PowerShell scripting, go to <http://www.microsoft.com/technet/scriptcenter/topics/winpsch/manual/run.mspix>.

Now you can run scripts. Note that to run a Windows PowerShell script, you need to type its full pathname along with the script file name. For example, to run a script, type:

```
C:\foldername\scriptname.ps1
```

The script name and the folder name list the complete location of the script. If the folder name or the script name includes blank spaces—for example, if the folder name is PowerShell Scripts—you must add an ampersand before the script name and you must put the script name and path in double quotes:

```
& "C:\foldername\scriptname.ps1"
```

You do this because Windows PowerShell is particular about running scripts. These commands run scripts inside the Windows PowerShell command shell. To run scripts outside Windows PowerShell, you need to call the PowerShell prompt first:

```
powershell.exe "c:\foldername\scriptname.ps1"
```

You can run this command either in the *Run* command in the Start menu or simply in a standard Command Prompt window—or even through the Task Scheduler if you want to schedule the script to run. Use double quotes to surround the path name as a best practice to make sure your scripts always run.

MORE INFO ELEVATING WINDOWS POWERSHELL SCRIPTS

To run scripts with administrative privileges, you need to use an elevated command prompt because there is no elevation command that can do so directly. However, you can use a series of very useful utilities written by Michael Murgolo, a consultant with Microsoft Consulting Services, that does just that. Download it at <http://technet.microsoft.com/en-ca/magazine/2007.06.utilityspotlight.aspx>.

Working with Windows PowerShell

Now that you know how to run scripts, you need to learn how to build them. Learning a new scripting language is a significant task and teaching it is beyond the scope of this book, but you can take shortcuts:

- Use the Windows PowerShell Owner's Manual to learn some basics. Access the manual at <http://www.microsoft.com/technet/scriptcenter/topics/winpsch/manual/default.aspx>.
- Rely on prewritten or sample scripts. Microsoft hosts the Microsoft TechNet Script Center, which lists a whole series of Windows PowerShell scripts, all oriented toward administration tasks at <http://www.microsoft.com/technet/scriptcenter/topics/msh/cmdlets/index.aspx>.
- Learn to use the *Get-* cmdlet. Just type **Get-** at the PowerShell prompt and then press the Tab key. This will automatically scroll through the available commands associated with *Get-*. Press Shift+Tab to go backward in the list. This also works with the *Set-* cmdlet. Table 7-3 lists all of the shortcut keys you can use within Windows PowerShell.
- Get PowerShell Help from Sapien Technologies. Sapien is the maker of PrimalScript, a graphical scripting engine that supports several scripting languages. PowerShell Help offers help on all of the Windows PowerShell commands in a nice graphical layout (see Figure 7-7). PowerShell Help is available for free at http://www.primalscript.com/Free_Tools/index.asp.

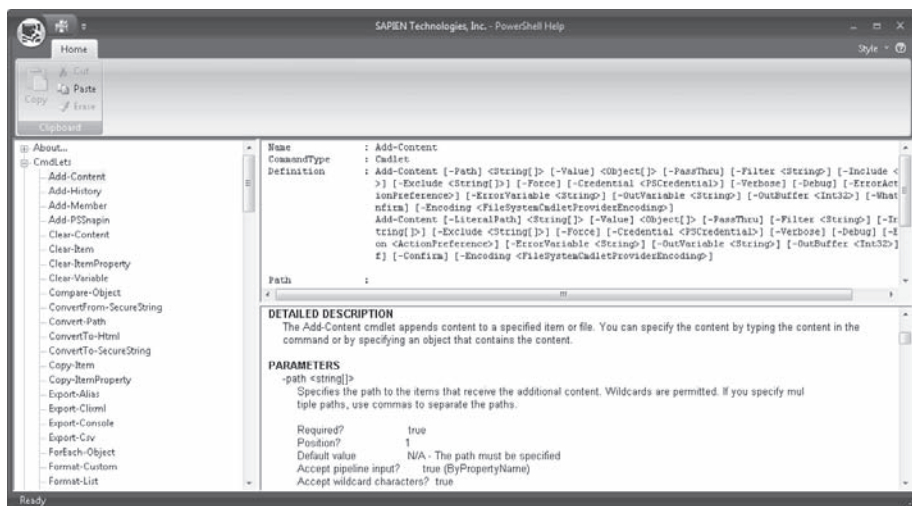


FIGURE 7-7 Using PowerShell Help

- Get the free PowerGUI. PowerGUI is a free graphical user interface for Windows PowerShell script development. In addition, Quest, the makers of PowerGUI, has built a community of users that keep adding functionality to PowerGUI. Find the community and download PowerGUI from <http://powergui.org>. PowerGUI can save you a lot of time (see Figure 7-8).

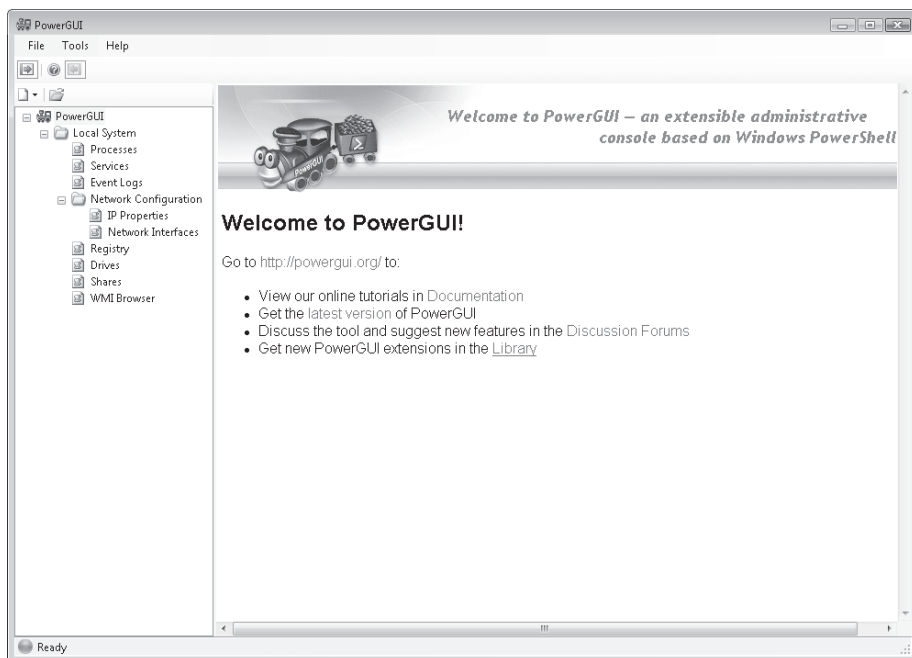


FIGURE 7-8 Using PowerGUI

- You can also learn to work with Windows PowerShell through a guided, online virtual lab hosted by Microsoft. Locate the virtual lab at <http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?culture=en-US&EventID=1032314395&EventCategory=3>.

Finally, just as there is no default way to normally generate a command prompt at the location where you are, there is no default way to do this with Windows PowerShell. This means you need to use a special utility to do so. You can use the utilities developed by Michael Murgolo at Microsoft to create custom entries in the Windows Explorer shortcut menu. Michael’s files are not in REG format; they are in INF format. This means that you must right-click the appropriate file and select Install to get it to modify the shortcut menu. Once the utility is installed, you will have appropriate prompts in the context menu of any folder through Windows Explorer (see Figure 7-9).

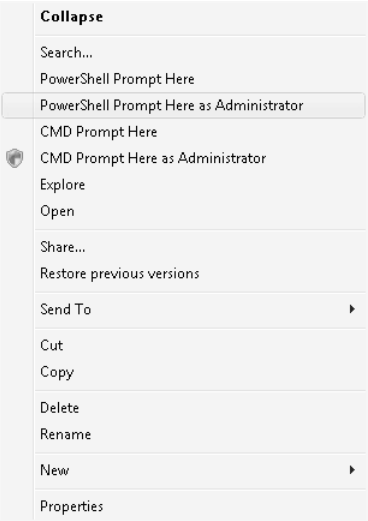


FIGURE 7-9 Using PowerShell Prompt Here as Administrator

TABLE 7-3 Windows PowerShell Shortcut Keys

KEY	DESCRIPTION
Up Arrow, F5, or Down Arrow	Use to move backward or forward through the command history.
Page Up or Page Down	Use to display the first or last command in the command history.
Left Arrow or Right Arrow	Use to move cursor one character to the left or to the right on the command line.
Home or End	Use to move the cursor to the beginning or to the end of the command line.
Control+Right Arrow or Control+Left Arrow	Use to move the cursor one word to the right or to the left on the command line.

KEY	DESCRIPTION
Control+C	Use to cancel the current command.
F2	Use to create a new command line from the partial contents of the last command.
F3	Use to display the previous command.
F4	From the current cursor position, use to delete characters up to the specified character.
F7	Use to display a dialog box that allows you to select a command from a command history (see Figure 7-10).
F8	Use to move backward through the command history, but only displays commands matching text typed at the command prompt.
F9	Use to run a specific command from the command history.

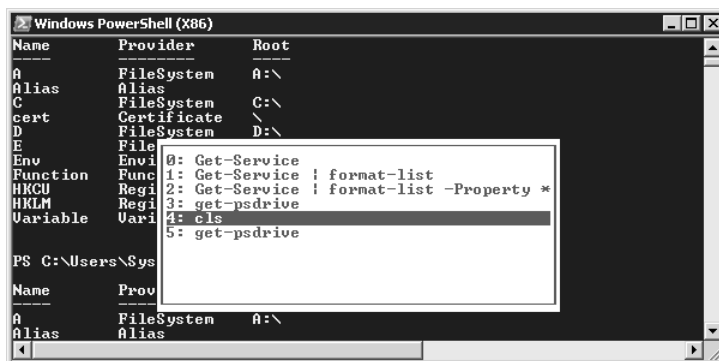


FIGURE 7-10 Using F7 to view a list of past cmdlets

Managing Hyper-V Operations with Windows PowerShell

As displayed in the Hyper-V architecture in Chapter 1, “Implementing Microsoft Hyper-V,” the parent partition in Hyper-V includes a Windows Management Instrumentation (WMI) provider. This provider enables third-party application service providers (ASPs) or scripters to generate custom tools, utilities, or scripts for operation with Hyper-V. This WMI provider is designed to expose the Hyper-V WMI classes for the following object categories:

- BIOS
- Input
- Integration Services or Components
- Memory
- Networking

- Processor
- Profile Registration
- Resource Management
- Serial Devices
- Storage
- Video
- Virtual System
- Virtual System Management

For example, when you work with Integration Services or Components, you can rely on WMI to expose information about each of the services. `MSVN_HeartbeatComponent` exposes information about the monitoring state of a virtual machine by reporting a heartbeat at regular intervals. Using this component programmatically allows you to obtain information about the state of a running VM.

MORE INFO HYPER-V WMI PROVIDER

Find out more about the Hyper-V WMI provider at [http://msdn.microsoft.com/en-us/library/cc136992\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/cc136992(VS.85).aspx).

WMI is one of the most important components in Hyper-V for automation and remote administration. For example, although Hyper-V includes a graphical interface for administration—the Hyper-V Manager—it does not include a corresponding command-line tool, unlike many other server roles or Windows Server System applications. For this reason, you must rely on Windows PowerShell and WMI to perform command-line activities on Hyper-V servers.

In addition, Windows PowerShell can be used to manage Hyper-V virtual machines that run Server Core, but only remotely because it does not execute on Server Core. You have to run the scripts remotely from a computer with Windows PowerShell installed. This can be any workstation or server that supports Windows PowerShell. The scripts will only access the WMI interface on the target Server Core computer because there is no .NET Framework library of objects. This means that the primary cmdlet you will use to manage virtual machines running on Server Core is the `Get-WmiObject` or its associated `gwmi` alias. After the cmdlet retrieves the WMI object, its properties and methods are available to a Windows PowerShell script.

MORE INFO HYPER-V WINDOWS POWERSHELL LIBRARY

There are no specific commands for Hyper-V in the version of Windows PowerShell that is shipped with Windows Server 2008, and the RTM update for Hyper-V does not add any either. But James O'Neil, an IT Pro Evangelist for Microsoft UK, has set about developing a Windows PowerShell library for Hyper-V. This library is available on Microsoft's CodePlex project-hosting Web site at <http://www.codeplex.com/PSHyperv>.

UPDATE ALERT SERVER CORE AND WINDOWS POWERSHELL

Windows Server 2008 R2 will allow you to run Windows PowerShell on Server Core and on Hyper-V Server (which is based on Server Core). For more information, look up http://blogs.msdn.com/virtual_pc_guy/archive/2009/02/10/enabling-powershell-on-hyper-v-server-2008-r2.aspx.

But the easiest way to work with Hyper-V through Windows PowerShell is to install the Hyper-V PowerShell Library. Begin by installing the Windows PowerShell Feature. Do this on a full installation of Windows Server 2008. To do so, use Server Manager and right-click the Features node. Select Add Features. Scroll down to select Windows PowerShell, click Next, and then click Install. Click Close when the installation completes. Next, obtain the Hyper-V PowerShell Library from <http://pshyperv.codeplex.com/>. This download includes two files. HyperV.zip is a compressed file that includes two items; PSHyperv.pdf documents the contents of the package. Save both files in an appropriate location, such as your Documents folder.

Using Windows Explorer, uncompress the two files from HyperV.zip. Store both files in your Documents folder. The two files include a script, Hyperv.ps1, and an XML document, Hyperv.Format.ps1xml. The latter is a format file that is used by the library to generate proper Hyper-V output. To install the library, you need to run the script. If you just installed Windows PowerShell, you'll need to enable scripts. Launch the PowerShell prompt with elevated rights. Right-click the PowerShell shortcut on the Start menu, select Run As Administrator, and accept the prompts. Then type the following cmdlet. The PowerShell prompt is launched by clicking Start, clicking All Programs, clicking Windows PowerShell, and then clicking Windows PowerShell.

```
Set-ExecutionPolicy Unrestricted
```

You must use the unrestricted policy because this script is not digitally signed. Change to your Documents folder and run the script. However, you must *dot source* the script. Dot sourcing is a procedure that makes all variables in the script global variables or variables that will be available in any context, even after you close the PowerShell prompt. If you do not dot source the script, all variables will disappear as soon as the PowerShell prompt is closed. Dot sourcing is performed by placing a period (.) followed by a space to precede the script. Use the following cmdlets to enable the new library, where *username* is your user name:

```
cd documents
. c:\Users\username\Documents\hyperv.ps1
```

The Windows PowerShell engine will warn you about executing scripts (see Figure 7-11). Press **R** and then press Enter to run the script once only, and then press **R** and Enter again to run the Hyperv.Format script. Then type the following cmdlet to reset your scripting environment:

```
Set-ExecutionPolicy RemoteSigned
```



The screenshot shows a PowerShell security warning. The text reads: "Security Warning: Run only scripts that you trust. While scripts from the Internet can be useful, this script can potentially harm your computer. Do you want to run C:\Users\Sysadmin\Documents\hyperv.ps1? [D] Do not run [R] Run once [S] Suspend [?] Help (default is 'D'):". The 'R' key is highlighted, indicating the user's response.

FIGURE 7-11 Windows PowerShell warns you about potential harm from unsigned scripts.

The execution of the script will list all of the new functions that have been enabled by this library. Table 7-4 outlines all of the cmdlets that are enabled by this library.

TABLE 7-4 Cmdlets included in the Hyper-V Windows PowerShell Library

CMDLET	DESCRIPTION
<i>Add-VMDisk</i>	Use to mount a DVD or hard disk image into a drive.
<i>Add-VMDrive</i>	Use to connect a hard disk drive or DVD drive to a controller.
<i>Add-VMFloppyDisk</i>	Use to mount a floppy disk image file.
<i>Add-VMKVP</i>	Use to add a key/value pair to the list sent to VMs by the host.
<i>Add-VMNewHardDisk</i>	Use to attach a new virtual hard disk image to a drive.
<i>Add-VMNIC</i>	Use to add a NIC to a virtual machine.
<i>Add-VMSCSIController</i>	Use to add a synthetic SCSI controller to a virtual machine.
<i>Apply-VMSnapshot</i>	Use to apply a snapshot to a virtual machine.
<i>Choose-VM</i>	Use to select virtual machines from a list.
<i>Choose-VMExternalEthernet</i>	Use to select a host network card.
<i>Choose-VMNIC</i>	Use to select a NIC attached to a virtual machine.
<i>Choose-VMSnapshot</i>	Use to choose a snapshot.
<i>Choose-VMSwitch</i>	Use to choose a virtual switch.
<i>Compact-VHD</i>	Use to compact a dynamic VHD file to save space on the host.
<i>Convert-VHD</i>	Use to change a VHD from one type to another.
<i>Convert-VMState</i>	Use to convert the number for a virtual machine state into the state's name.
<i>Expand-VHD</i>	Use to expand the size of virtual hard disk.
<i>Export-VM</i>	Use to invoke the Hyper-V export process.
<i>Get-VHDDefaultPath</i>	Use to get the default path used by Hyper-V for VHD files.
<i>Get-VHDInfo</i>	Use to get information about a VHD, such as its parent or size on a disk.
<i>Get-VM</i>	Use to return WMI objects representing virtual machines.
<i>Get-VMBackupScript</i>	Use to get a script used to back up one or more virtual machines.

CMDLET	DESCRIPTION
<i>Get-VMByMACAddress</i>	Use to discover a virtual machine from its MAC address.
<i>Get-VMCPUCount</i>	Use to get the number and weighting of processors assigned to VMs.
<i>Get-VMDisk</i>	Use to get a list of virtual disk images in use.
<i>Get- VMDiskByDrive</i>	Use to get the virtual machine disk image attached to a drive.
<i>Get- VMDiskController</i>	Use to get an IDE or SCSI controller. Note the IDE controllers can't be changed.
<i>Get-VMDriveByController</i>	Use to get the drives attached to a controller.
<i>Get-VMFloppyDisk</i>	Use to return information about the mounted floppy disk.
<i>Get-VMHost</i>	Use to get a list from Active Directory of hosts running Hyper-V.
<i>Get-VMJPEG</i>	Use to get a JPEG image of the current virtual machine screen.
<i>Get-VMKVP</i>	Use to get the key/value pair information sent to the host by virtual machines.
<i>Get-VMMemory</i>	Use to return the amount of memory assigned to a virtual machine.
<i>Get-VMNIC</i>	Use to return information about network cards.
<i>Get- VMNICPort</i>	Use to get the virtual switch port attached to a NIC.
<i>Get- VMNICSwitch</i>	Use to return the virtual switch a NIC is connected to.
<i>Get-VMProcessor</i>	Use to get active virtual processors and their load data.
<i>Get-VMSerialPort</i>	Use to return information about serial ports.
<i>Get-VMSettingData</i>	Use to return the settings data object for the virtual machine.
<i>Get-VMSnapshot</i>	Use to get information about snapshots.
<i>Get-VMSnapshotTree</i>	Use to get information about snapshot trees.
<i>Get-VMSummary</i>	Use to return a summary for each virtual machine.
<i>Get-VMSwitch</i>	Use to return information about virtual switches.
<i>Import-VM</i>	Use to invoke Hyper-V's import process.
<i>Merge-VHD</i>	Use to merge a child VHD with its parent to form a new disk.
<i>Mount-VHD</i>	Use to make the VHD file appear as a local disk on the host.

CMDLET	DESCRIPTION
<i>New-VFD</i>	Use to create a new floppy disk image file.
<i>New-VHD</i>	Use to create a new VHD file.
<i>New-VM</i>	Use to create a new virtual machine.
<i>New-VMConnectSession</i>	Use to launch a virtual machine connect session to a virtual machine.
<i>New-VMExternalSwitch</i>	Use to create a virtual switch connected to a host network card.
<i>New-VMInternalSwitch</i>	Use to create a virtual switch accessible to virtual machines and the host.
<i>New-VMPrivateSwitch</i>	Use to create a virtual switch accessible to virtual machines.
<i>New-VMRasd</i>	Use to create objects used by other functions to describe virtual machine components.
<i>New-VMSnapshot</i>	Use to create a new snapshot of a virtual machine.
<i>New-VMSwitchPort</i>	Use to define a new port on a virtual switch.
<i>Ping-VM</i>	Use to ping FQDNs found via the key/value pair (KVP) exchange integration component.
<i>Remove-VM</i>	Use to delete a virtual machine.
<i>Remove-VMDrive</i>	Use to remove a hard disk drive or DVD drive from a controller.
<i>Remove-VMFloppyDisk</i>	Use to eject any floppy disk from the drive of a virtual machine.
<i>Remove-VMKVP</i>	Use to remove a key/value pair from the list sent to virtual machines by the host.
<i>Remove-VMNIC</i>	Use to remove a NIC attached to a virtual machine.
<i>Remove-VMSCSIController</i>	Use to remove a synthetic SCSI controller from a virtual machine.
<i>Remove-VMSnapshot</i>	Use to delete a snapshot or tree of snapshots.
<i>Rename-VMSnapshot</i>	Use to rename a snapshot.
<i>Set-VM</i>	Use to set the properties of an existing virtual machine.
<i>Set-VMCPUCount</i>	Use to set the number of virtual processors assigned to virtual machines.
<i>Set-VMDisk</i>	Use to change the disk image attached to a drive.

CMDLET	DESCRIPTION
<i>Set-VMMemory</i>	Use to set the amount of memory assigned to a virtual machine.
<i>Set-VMNICAddress</i>	Use to set the MAC address for a NIC.
<i>Set-VMNICSwitch</i>	Use to connect a NIC to a virtual switch.
<i>Set-VMSerialPort</i>	Use to map serial ports on a virtual machine to named pipes.
<i>Set-VMState</i>	Use to set a requested state on a virtual machine. These states can be started, stopped, and suspended.
<i>Shutdown-VM</i>	Use to shut down a virtual machine's operating system cleanly via the shutdown integration component.
<i>Start-VM</i>	Use to start a virtual machine or to restart a saved one.
<i>Stop-VM</i>	Use to turn off a virtual machine without asking the operating system to shut down first.
<i>Suspend-VM</i>	Use to put a virtual machine into a saved state.
<i>Test-VHD</i>	Use to test whether a VHD can be mounted and whether its parent is mountable.
<i>Test-VMHeartBeat</i>	Use to test the responses from the heartbeat integration components.
<i>Test-WMIJob</i>	Use to check on the state of a job—can wait until it completes.
<i>UnMount-VHD</i>	Use to reverse the mount process so that the VHD can be used by a virtual machine.
<i>Update-VMSnapshot</i>	Use to delete a snapshot and create a new one with the same name.

MORE INFO DOT SOURCING A SCRIPT

For more information on Windows PowerShell scripts and how to dot source a script, look up “Running Windows PowerShell Scripts” at <http://www.microsoft.com/technet/scriptcenter/topics/winps/sh/manual/run.mspix>.

Given these new cmdlets, you can now generate almost any object in a Hyper-V and you can also do it on a Server Core installation because each one of the cmdlets in this library supports the *-server* parameter to let you name the remote server.

But even better than the Hyper-V Windows PowerShell Library is the PowerGUI. Like the Hyper-V Windows PowerShell Library, PowerGUI can add custom cmdlets for Hyper-V

management, but the advantage is that as soon as they are loaded, you can simply use drag and drop and generate a Windows PowerShell script to manage Hyper-V objects in a graphical interface.

PowerPacks extend the PowerGUI interface with a set of folders, nodes, links, and actions to manage new objects. For example, you can obtain a PowerPack for Exchange Server, Active Directory Domain Services, and much more. The requirements to run PowerGUI are:

- **Operating systems** Windows Vista, Windows Server 2008 full installation, or Windows 7
- Tools and utilities
 - Hyper-V Remote Management Update, which may be installed on its own on Windows Vista or installed through the Remote Server Administration Tools on Windows Server 2008.
 - PowerGUI itself, which is available at <http://www.powergui.org>. Version 1.6 or later is required to work with Hyper-V.
 - The Quest ActiveRoles Management Shell for Active Directory, which can be downloaded at <http://www.quest.com/powershell/activeroles-server.aspx>. This PowerPack is required to let you locate Hyper-V servers in Active Directory Domain Services.
 - The Network PowerPack, which is included with PowerGUI at <http://www.powergui.org/servlet/KbServlet/download/2142-102-3068/Hyper-V.powerpack>.
 - The Hyper-V PowerPack, which is also available from the PowerGUI Web site at <http://powergui.org/entry!default.jspa?categoryID=290&externalID=2142&printable=true>.

When you have each of these tools in hand, you can proceed to the generation of new Windows PowerShell scripts for use with Hyper-V. You will perform this task in the Practice at the end of this lesson.

Using Windows PowerShell with SCVMM

When you install SCVMM, Windows PowerShell is installed by default. Note, however, that SCVMM adds a new link to Windows PowerShell, one that is different from the default link provided when you add the Windows PowerShell feature. This new link is added because the context created by SCVMM is enabled in the SCVMM PowerShell prompt, not the default Windows PowerShell prompt.

To launch the SCVMM PowerShell Prompt, click Start, click All Programs, click Microsoft System Center, and then click Virtual Machine Manager 2008. This is where you will find the Windows PowerShell – Virtual Machine Manager shortcut (see Figure 7-12).

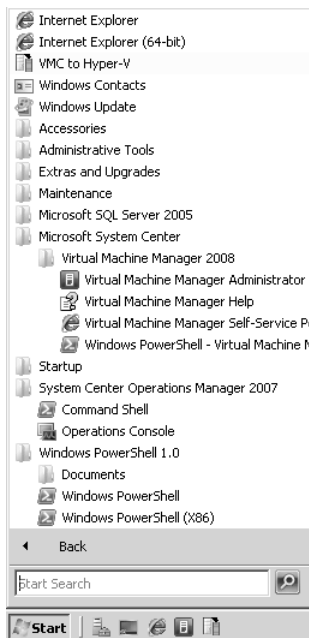


FIGURE 7-12 The SCVMM PowerShell shortcut on the Start menu

You can also launch the SCVMM PowerShell prompt from a command prompt. Use the following command:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -PSConsoleFile "C:\Program Files\Microsoft System Center Virtual Machine Manager 2008\bin\cli.psc1" -NoExit
```

This command starts Windows PowerShell and specifies the SCVMM console file `Cli.PSC1`. This console file is an XML file that contains a few elements as well as the reference to the `Microsoft.SystemCenter.VirtualMachineManager.dll`. The result is a custom SCVMM PowerShell prompt (see Figure 7-13). Note that this prompt uses a black window background and lists Virtual Machine Manager in the title bar to avoid confusion with the default Windows PowerShell prompt.

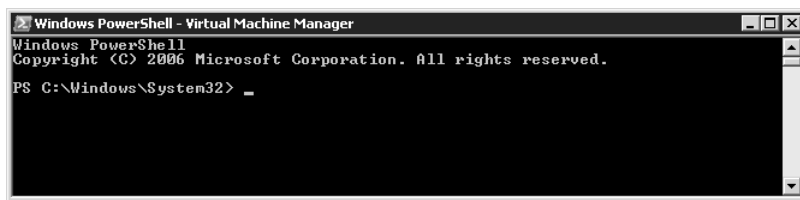


FIGURE 7-13 The SCVMM PowerShell prompt

You can use this console to manage virtual machine hosts, library servers, virtual machines, and other SCVMM components by using cmdlets or scripts. The scripts you create can be based on standard Windows PowerShell and SCVMM cmdlets because the SCVMM PowerShell

prompt includes all of the standard Windows PowerShell cmdlets as well as a set of cmdlets specially designed for SCVMM. Note that when you launch the default Windows PowerShell prompt that is installed in Windows Server 2008—or on any other platform—it does not include the cmdlets for SCVMM because it does not call on the SCVMM PowerShell DLL when it launches.

Configuring Windows PowerShell for Use with SCVMM 2008

You need to configure four elements to be able to use Windows PowerShell with SCVMM: an application-specific profile, an application-specific snap-in, the security context, and the application context. The first two are snap-ins and are configured automatically when the `Cli.PSC1` SCVMM PowerShell console file is loaded. As with the default Windows PowerShell prompt, the security context of the SCVMM PowerShell prompt must be configured manually. As you have seen before, the script execution mode in Windows PowerShell is set to `Restricted` by default. Including `Restricted`, there are four possible values:

- **Restricted** The default context for the Windows PowerShell execution policy: All script execution is disabled, but Windows PowerShell can still be used as an interactive command interpreter.
- **AllSigned** Only Authenticode-signed scripts can be executed. The user is prompted each time a script is run to see if he or she wants to trust the signer of the script.
- **RemoteSigned** All scripts that are downloaded from a remote location must be Authenticode-signed before they can be executed.
- **Unrestricted** Any script can be executed. This setting is the least secure. The user is still prompted to trust the signer if the script is downloaded from a remote location.

Once again, the script execution policy is managed by the `Get-ExecutionPolicy` cmdlet (view the current execution policy) and the `Set-ExecutionPolicy` cmdlet (change the execution policy).



EXAM TIP ELEVATED RIGHTS IN POWERSHELL

Remember that you must use elevated rights when you want to change a global context in Windows PowerShell, such as when you want to change the script execution policy. To do so, right-click the Windows PowerShell shortcut, select **Run As Administrator**, and then accept the prompt.

The fourth context, which is the application context, refers to the specific instance of the SCVMM Server against which the requested script is to be run. By default, no context—not even the local server context—is set when you launch the SCVMM PowerShell Prompt. Before you can execute any SCVMM Windows PowerShell cmdlets, you must set the application context using the following command, where *FQDNComputerName* is the fully qualified domain name for the SCVMM Server you want to use, such as `ServerFull01.Contoso.com`:

```
Get-VMMServer -ComputerName <FQDNComputername>
```


Make sure you begin each SCVMM PowerShell session with this cmdlet first or use the following cmdlet if you are working locally on the SCVMM Server:

```
Get-VMMServer -Computename localhost
```

MORE INFO WORKING WITH THE SCVMM ADMINISTRATOR CONSOLE

Note that you do not need to set the four elements for Windows PowerShell execution when you use the SCVMM Administrator Console because the console runs the Windows PowerShell cmdlets internally and does not rely on PowerShell.exe to execute its scripts.

You can use the SCVMM cmdlets to manage several actions in SCVMM, such as:

- Add and work with virtual machine hosts and host groups.
- Add an SCVMM Library and maintain the resources inside the library.
- Create and work with virtual machines that are deployed on a host.
- Manage the virtual machine environment.
- Create virtual machine checkpoints.
- Back up and restore the SCVMM database.

The SCVMM Windows PowerShell DLL also includes several cmdlets for Performance and Resource Optimization.

Windows PowerShell Commands for SCVMM

All SVMM cmdlets are included in the Microsoft.SystemCenter.VirtualMachineManager.DLL that is loaded when you launch the SCVMM PowerShell Prompt. This DLL is considered a Windows PowerShell snap-in. To view all of the cmdlets included in this DLL, open the SCVMM PowerShell prompt and type the following cmdlet:

```
Get-Command -PSSnapin Microsoft.SystemCenter.VirtualMachineManager
```

The results are displayed in Table 7-5. The SCVMM PowerShell prompt includes these cmdlets in addition to the standard cmdlets included in Windows PowerShell version 1.0. Note that there are some minor differences between some cmdlets for SCVMM 2007 and 2008. Where differences exist, they have been identified with the version number of SCVMM.

TABLE 7-5 Virtual Machine Manager Windows PowerShell Cmdlets

CMDLET	DESCRIPTION
<i>Add-LibraryServer</i>	Use to add a computer as a library server to SCVMM.
<i>Add-LibraryShare</i>	Use to add Windows shares on the file system of a library server as library shares to the SCVMM Library.
<i>Add-Patch</i>	Use to add information about updates, hotfix packages and binaries to the SCVMM update, and hotfix package cache.

CMDLET	DESCRIPTION
<i>Add-VirtualizationManager</i>	Use to add a VMware VirtualCenter Server to SCVMM.
<i>Add-VMHost</i>	Use to add a computer as a managed host to the SCVMM database.
<i>Add-VMHostCluster</i>	Use to add an object to SCVMM that represents a host cluster.
<i>Add-VMHostNetworkAdapter</i>	Use to add a physical network adapter on a host server managed by SCVMM to a virtual network.
<i>Associate-VMHost</i>	Use to associate a VMware ESX Server with SCVMM as a managed host and specify credentials to manage this host.
<i>Backup-VMMServer</i>	Use to back up the SCVMM database.
<i>Compress-VirtualDiskDrive</i>	Use to compress a dynamically expanding virtual hard disk attached to a virtual disk drive object on a stopped virtual machine on a Windows-based host managed by SCVMM.
<i>Convert-VirtualDiskDrive</i>	Use to convert an existing virtual hard disk attached to a virtual disk drive object from dynamic to fixed or from fixed to dynamic, or to convert a pass-through disk attached to a virtual disk drive object to a virtual hard disk.
<i>Copy-HardDisk</i>	Use to copy a volume of a physical hard disk on a source computer to a Windows-based VHD file on the specified SCVMM host.
<i>Copy-VMDK</i>	Use to copy a VMware VMDK file to a Microsoft-compatible VHD file and to convert the VHD for use in a SCVMM environment.
<i>DisableUndoDisk-VM</i>	Use to merge or discard undo disks associated with a virtual machine on a Virtual Server host managed by SCVMM.
<i>DiscardSavedState-VM</i>	Use to discard the saved state of a VM managed by SCVMM.
<i>Discover-Cluster</i>	Use to discover the specified failover cluster in an SCVMM environment.
<i>Discover-Computer</i>	Use to discover computers by querying Active Directory and to return the computer objects.
<i>Discover-LibraryShare</i>	Use to discover all of the shares on the specified computer or Library Server managed by SCVMM.
<i>Expand-VirtualDiskDrive</i>	Use to expand a VHD attached to a virtual disk drive object on a stopped VM deployed on a host managed by SCVMM.

CMDLET	DESCRIPTION
<i>Get-Certificate</i>	Use to get a security certificate object from a VMware VirtualCenter server or from an ESX Server.
<i>Get-CPUType</i>	Use to get objects that represent CPU types for use in VMs, or for use in templates or hardware profiles used to create VM.
<i>Get-DependentLibraryObject</i>	Use to identify dependencies between SCVMM objects.
<i>Get-DirectoryChildItem</i>	Use to get all files and subdirectories in the specified directory on a virtual machine host or on a library server managed by SCVMM.
<i>Get-GuestOSProfile</i>	Use to get guest operating system profile objects from the SCVMM Library.
<i>Get-HardwareProfile</i>	Use to get hardware profile objects from the SCVMM Library.
<i>Get-ISO</i>	Use to get ISO objects from the SCVMM Library.
<i>Get-Job</i>	Use to get SCVMM job objects on an SCVMM Server.
<i>Get-LibraryRating</i>	Use to calculate the placement rating of VM libraries managed by SCVMM to determine whether a SAN Transfer can be used to transfer a VM from a host to the library.
<i>Get-LibraryServer</i>	Use to get Library Server objects from the SCVMM database.
<i>Get-LibraryShare</i>	Use to get library share objects from SCVMM Library.
<i>Get-MachineConfig</i>	Use to get physical machine configuration objects from the SCVMM database.
<i>Get-NetworkLocation</i>	Use to get the list of network locations that the specified SCVMM Server can access.
<i>Get-OperatingSystem</i>	Use to get valid operating system objects from the SCVMM database.
<i>Get-Script</i>	Use to get script objects from the SCVMM Library. With appropriate permissions, you can also use this cmdlet to view or edit any script, or you can use it to view, edit, or run a Windows PowerShell script.
<i>Get-SshPublicKey</i>	Use to get the public key object from a VMware ESX Server that you want SCVMM to manage.
<i>Get-Step</i>	Use to get the steps for the specified job on an SCVMM Server.
<i>Get-Template</i>	Use to get VM template objects from the SCVMM Library.

CMDLET	DESCRIPTION
<i>Get-VirtualCOMPort</i>	Use to get SCVMM virtual communication (COM) port objects from a virtual machine, template, or hardware profile.
<i>Get-VirtualDiskDrive</i>	Use to get virtual disk drive objects on templates or on virtual machines managed by SCVMM.
<i>Get-VirtualDVDDrive</i>	Use to get SCVMM virtual DVD drive objects from a virtual machine, template, or hardware profile.
<i>Get-VirtualFloppyDisk</i>	Use to get virtual floppy disk objects from the SCVMM Library.
<i>Get-VirtualFloppyDrive</i>	Use to get SCVMM virtual floppy drive objects from a virtual machine, template, or hardware profile.
<i>Get-VirtualHardDisk</i>	Use to get virtual hard disk objects from a virtual machine, template, or standalone file stored in the SCVMM Library.
<i>Get-VirtualizationManager</i>	Use to get objects that represent VMware VirtualCenter Servers managed by SCVMM from the SCVMM database.
<i>Get-VirtualNetwork</i>	Use to get virtual network objects configured on a host managed by SCVMM.
<i>Get-VirtualNetworkAdapter</i>	Use to get SCVMM virtual network adapter objects from a virtual machine, template, or hardware profile.
<i>Get-VirtualSCSIAdapter</i>	Use to change properties of a virtual SCSI adapter used in SCVMM.
<i>Get-VM</i>	Use to get virtual machine objects from the SCVMM database.
<i>Get-VMCheckpoint</i>	Use to get virtual machine checkpoint objects from the SCVMM database.
<i>Get-VMHost</i>	Use to get virtual machine host objects from the SCVMM database.
<i>Get-VMHostCluster</i>	Use to get a host cluster object or an array of host cluster objects from the SCVMM database.
<i>Get-VMHostDisk</i>	Use to get a hard disk drive object for the specified host from the SCVMM database.
<i>Get-VMHostGroup</i>	Use to get a host group object from the SCVMM database.
<i>Get-VMHostNetworkAdapter</i>	Use to get physical network adapter objects on a host managed by SCVMM.
<i>Get-VMHostRating</i>	Use to calculate the placement rating for one or more virtual machine hosts managed by SCVMM on which you might want to deploy a specific virtual machine.

CMDLET	DESCRIPTION
<i>Get-VMHostVolume</i>	Use to get drive volume objects from a host managed by SCVMM.
<i>Get-VMManagedComputer</i>	Use to get managed computer objects from the SCVMM database.
<i>Get-VMMServer</i>	Use to connect to an SCVMM (if a connection does not already exist) and to retrieve the object that represents this server from the SCVMM database.
<i>Get-VMUserRole</i>	Use to get an object that represents an SCVMM user role.
<i>Get-VMPerformance</i>	Use to get performance data for a specific virtual machine deployed on a host managed by SCVMM.
<i>Get-VMwareResourcePool</i>	Use to get a VMware resource pool from the SCVMM database.
<i>Get-VMXMachineConfig</i>	Use to get VMX machine configuration objects that are associated with one or more VMware-based VMs in the SCVMM database.
<i>Move-VirtualHardDisk</i>	Use to move a Windows-based VHD file from one location to another on the same host.
<i>Move-VM</i>	Use to move a VM currently stored in the SCVMM Library or deployed on a host server to a new location on a host server.
<i>Move-VMHost</i>	Use to move a host object managed by SCVMM from one host group to another.
<i>Move-VMHostCluster</i>	Use to move a Windows Server 2008 host cluster object managed by SCVMM from one host group to another.
<i>Move-VMHostGroup</i>	Use to move a host group object managed by SCVMM from the current location to a new location under a different host group parent.
<i>New-GuestOSProfile</i>	Use to create a guest operating system profile for use in SCVMM.
<i>New-HardwareProfile</i>	Use to create a hardware profile for use in SCVMM.
<i>New-MachineConfig</i>	Use to create a machine configuration object by gathering machine configuration information from a physical source machine that you plan to convert to a virtual machine managed by SCVMM.
<i>New-P2V</i>	Use to convert a physical machine to a VM on a Windows-based host (Hyper-V or Virtual Server) managed by SCVMM.

CMDLET	DESCRIPTION
<i>New-PhysicalAddress</i>	Use to return the next available physical address (MAC address) if a range of MAC addresses has been configured for your SCVMM environment.
<i>New-Template</i>	Use to create a VM template used to create VMs managed by SCVMM.
<i>New-V2V</i>	Use to convert a virtual machine created on a VMware ESX Server host to a virtual machine deployed on a Windows-based host—Hyper-V or Virtual Server—managed by SCVMM.
<i>New-VirtualDiskDrive</i>	Use to create a virtual disk drive on a VM deployed on a host managed by SCVMM or on a template in the SCVMM Library.
<i>New-VirtualDVDDrive</i>	Use to create a virtual DVD drive on a virtual machine, template, or hardware profile used in SCVMM.
<i>New-VirtualNetwork</i>	Use to create a virtual network object on a host managed by SCVMM.
<i>New-VirtualNetworkAdapter</i>	Use to create a virtual network adapter on a virtual machine, template, or hardware profile used in SCVMM.
<i>New-VirtualSCSIAdapter</i>	Use to create a virtual SCSI adapter on a virtual machine, template, or hardware profile used in SCVMM.
<i>New-VM</i>	Use to create a virtual machine to be managed by SCVMM.
<i>New-VMCheckpoint</i>	Use to create a virtual machine checkpoint object for a virtual machine deployed on a host managed by SCVMM.
<i>New-VMHostGroup</i>	Use to create an SCVMM host group object that can contain virtual machine host servers, other host groups, or host clusters.
<i>New-VMUserRole</i>	Use to create a Self-Service or a Delegated Administrator user role for a group of SCVMM users.
<i>New-VMRCCertificateRequest</i>	Use to generate a request for a signed certificate that SCVMM can use to secure Virtual Machine Remote Control (VMRC) communications by encrypting information exchanged between a user and a virtual machine on a Virtual Server host.
<i>New-VMXMachineConfig</i>	Use to create a VMX machine configuration object by gathering VM configuration information from a virtual machine created in VMware that you plan to convert to a virtual machine deployed on a Windows-based host managed by SCVMM.

CMDLET	DESCRIPTION
<i>Reassociate-VMManagedComputer</i>	Use to reassociate a managed computer on which SCVMM agent software is installed—either a Windows-based host or a library server—with a different SCVMM Server.
<i>Refresh-LibraryShare</i>	Use to refresh the state and metadata of SCVMM Library objects stored in a library share.
<i>Refresh-VirtualizationManager</i>	Use to refresh the properties of a VMware VirtualCenter Server so that the SCVMM Administrator Console displays updated information about entities in VirtualCenter Server.
<i>Refresh-VM</i>	Use to refresh the properties of a virtual machine so that the SCVMM Administrator Console displays updated information about the virtual machine.
<i>Refresh-VMHost</i>	Use to refresh virtual machine host properties in the SCVMM Administrator Console.
<i>Refresh-VMHostCluster</i>	Use to refresh host cluster properties in the SCVMM Administrator Console.
<i>Register-VM</i>	Use to register an existing virtual machine with SCVMM that is not currently registered with the virtualization platform (Virtual Server, Hyper-V, or VMware) of any host managed by SCVMM and is not stored in the SCVMM Library.
<i>Remove-GuestOSProfile</i>	Use to remove a guest operating system profile object from SCVMM.
<i>Remove-HardwareProfile</i>	Use to remove a hardware profile object from SCVMM.
<i>Remove-ISO</i>	Use to remove an ISO object from the SCVMM Library.
<i>Remove-LibraryServer</i>	Use to remove a library server object from SCVMM.
<i>Remove-LibraryShare</i>	Use to remove a library share object from SCVMM but not delete the share from the Windows file system.
<i>Remove-MachineConfig</i>	Use to remove a machine configuration object from SCVMM.
<i>Remove-Script</i>	Use to remove a script object from SCVMM.
<i>Remove-Template</i>	Use to get VM template objects from the SCVMM Library.
<i>Remove-VirtualDiskDrive</i>	Use to remove a virtual disk drive object from a template or a virtual machine in SCVMM environment.
<i>Remove-VirtualDVDDrive</i>	Use to remove a virtual DVD drive object from SCVMM.
<i>Remove-VirtualFloppyDisk</i>	Use to remove a virtual floppy disk object from SCVMM.

CMDLET	DESCRIPTION
<i>Remove-VirtualHardDisk</i>	Use to remove a virtual hard disk from a virtual machine or template or from SCVMM Library.
<i>Remove-VirtualizationManager</i>	Use to remove a VMware VirtualCenter Server from SCVMM.
<i>Remove-VirtualNetwork</i>	Use to remove a virtual network object from a host managed by SCVMM.
<i>Remove-VirtualNetworkAdapter</i>	Use to remove a virtual network adapter object from SCVMM.
<i>Remove-VirtualSCSIAdapter</i>	Use to get SCVMM virtual SCSI objects from a virtual machine, template, or hardware profile.
<i>Remove-VM</i>	Use to remove a virtual machine object from SCVMM.
<i>Remove-VMCheckpoint (2008)</i> <i>Merge-VMCheckpoint (2007)</i>	Use to remove a virtual machine checkpoint object from the SCVMM database.
<i>Remove-VMHost</i>	Use to remove a managed host from SCVMM.
<i>Remove-VMHostCluster</i>	Use to remove a host cluster object from SCVMM.
<i>Remove-VMHostGroup</i>	Use to remove a host group object from SCVMM.
<i>Remove-VMHostNetworkAdapter</i>	Use to remove a physical host network adapter object from a virtual network that is configured on a host managed by SCVMM.
<i>Remove-VMMUserRole</i>	Use to remove an existing Self-Service or Delegated Administrator user role from SCVMM.
<i>Remove-VMXMachineConfig</i>	Use to remove a VMX machine configuration object from SCVMM.
<i>Repair-VM</i>	Use to repair a virtual machine on a host managed by SCVMM if the virtual machine is in a failed state.
<i>Restart-Job</i>	Use to restart a failed or canceled SCVMM job.
<i>Restore-VMCheckpoint</i>	Use to restore a virtual machine on a host managed by SCVMM to the specified checkpoint.
<i>Resume-VM</i>	Use to restart paused virtual machines managed by SCVMM.
<i>SaveState-VM</i>	Use to save the state of a virtual machine managed by SCVMM.
<i>Set-GuestOSProfile</i>	Use to change properties of a guest operating system profile used in SCVMM.
<i>Set-HardwareProfile</i>	Use to change the properties of a hardware profile used in SCVMM.

CMDLET	DESCRIPTION
<i>Set-ISO</i>	Use to change properties of an ISO used in SCVMM.
<i>Set-LibraryServer</i>	Use to change specific properties of an SCVMM Library Server object.
<i>Set-LibraryShare</i>	Use to change the description property of a SCVMM Library share object.
<i>Set-Script</i>	Use to change properties of a script stored in the SCVMM Library.
<i>Set-Template</i>	Use to change properties of a template used in SCVMM.
<i>Set-VirtualCOMPort</i>	Use to change properties of a virtual COM port associated with a virtual machine, template, or hardware profile used in SCVMM.
<i>Set-VirtualDiskDrive</i>	Use to modify settings on a virtual disk drive object on template or on virtual machine in the SCVMM environment.
<i>Set-VirtualDVDDrive</i>	Use to change properties of a virtual DVD drive associated with a virtual machine, template, or hardware profile used in SCVMM.
<i>Set-VirtualFloppyDisk</i>	Use to change properties of a virtual floppy disk used in SCVMM.
<i>Set-VirtualFloppyDrive</i>	Use to change properties of a virtual floppy drive associated with a virtual machine, template, or hardware profile used in SCVMM.
<i>Set-VirtualHardDisk</i>	Use to change properties of a virtual hard disk used in SCVMM.
<i>Set-VirtualizationManager</i>	Use to change properties of a VMware VirtualCenter Server that is managed by SCVMM.
<i>Set-VirtualNetwork</i>	Use to change the properties of a virtual network on a virtual machine host managed by SCVMM.
<i>Set-VirtualNetworkAdapter</i>	Use to change properties of a virtual network adapter associated with a virtual machine, template, or hardware profile used to create virtual machine in SCVMM.
<i>Set-VirtualSCSIAdapter</i>	Use to change properties of a virtual SCSI adapter used in SCVMM.
<i>Set-VM</i>	Use to change properties of a virtual machine managed by SCVMM.
<i>Set-VMCheckpoint</i>	Use to change the description properties of a virtual machine checkpoint object in SCVMM.

CMDLET	DESCRIPTION
<i>Set-VMHost</i>	Use to change the properties of a virtual machine host managed by SCVMM.
<i>Set-VMHostCluster</i>	Use to modify the properties of a virtual machine host cluster managed by SCVMM.
<i>Set-VMHostGroup</i>	Use to change properties of a host group in SCVMM.
<i>Set-VMHostNetworkAdapter</i>	Use to change network-related properties of the specified physical network adapter on a host managed by SCVMM.
<i>Set-VMHostVolume</i>	Use to modify the setting for a volume on a host server that enables SCVMM to evaluate that volume as available storage during the virtual machine placement process.
<i>Set-VMMServer</i>	Use to change the properties of the SCVMM Server.
<i>Set-VMMSUserRole</i>	Use to modify the settings for an existing SCVMM user role.
<i>Shutdown-VM</i>	Use to shut down a running virtual machine managed by SCVMM.
<i>Start-VM</i>	Use to start virtual machines managed by SCVMM.
<i>Stop-Job</i>	Use to stop running jobs in SCVMM.
<i>Stop-VM</i>	Use to stop virtual machines on hosts managed by SCVMM.
<i>Store-VM</i>	Use to store a virtual machine currently deployed on a virtual machine host by migrating it from the host to the SCVMM Library.
<i>Suspend-VM</i>	Use to suspend execution on virtual machine managed by SCVMM.
<i>Update-VMHost</i>	Use to update Virtual Server 2005 R2 software installed on a host to the latest version of Virtual Server supported by SCVMM.
<i>Update-VMManagedComputer</i>	Use to update SCVMM agent software installed on a Windows-based managed computer.
<i>Get-PROTip</i>	Use to get Performance and Resource Optimization (PRO) tip objects from the SCVMM database.
<i>Dismiss-PROTip</i>	Use to dismiss a PRO tip object that is no longer needed in SCVMM.
<i>Invoke-PROTip</i>	Use to perform the action recommended by a PRO tip. You can use this cmdlet to manually invoke the action recommended by a PRO tip that is not set to be implemented automatically.
<i>Set-PROTip</i>	Use to set the status of a PRO tip object.

Managing SCVMM Operations with Windows PowerShell

You can work with SCVMM through both the SCVMM PowerShell prompt and the default Windows PowerShell prompt. However, because the default Windows PowerShell prompt does not include the SCVMM cmdlets, you must run the following cmdlet as soon as you start the default Windows PowerShell prompt:

```
Add-PSSnapin Microsoft.SystemCenter.VirtualMachineManager
```

This adds the SCVMM PowerShell snap-in and adds all of the SCVMM cmdlets to the current console.

But the best way to work with Windows PowerShell and SCVMM is to get the SCVMM Administrator Console to generate a script. For example, if you want to generate a script that creates a new virtual machine and places it on a host, you simply run through the operation once in the SCVMM Administrator Console and then, when you've reached the end of the wizard, click View Script, save the text from the script with a .PS1 extension—for example, **NewVMScript.PS1**—and then cancel the job.

The following script is captured from the New Virtual Machine Wizard. It creates a new VM from a blank 40-GB disk and places it on ServerFull01. Because the VM is generated from a blank disk, it requires the installation of a guest operating system. Ideally, you want to create the VM from a template that is stored in the SCVMM Library.

```
# -----
# New Virtual Machine Script
# -----
# Script generated on Friday, February 20, 2009 9:24:45 AM by Virtual Machine Manager
#
# For additional help on cmdlet usage, type get-help <cmdlet name>
# -----

New-VirtualNetworkAdapter -VMMServer localhost -JobGroup 35d5539a-78ca-47ee-
    -8073-b398d6390a95 -PhysicalAddressType Dynamic -VirtualNetwork "Hyper-V External"
    -VLanEnabled $false

New-VirtualDVDDrive -VMMServer localhost -JobGroup 35d5539a-78ca-47ee-8073-
    b398d6390a95 -Bus 1 -LUN 0

$CPUType = Get-CPUType -VMMServer localhost | where {$_.Name -eq "1.20 GHz Athlon MP"}

New-HardwareProfile -VMMServer localhost -Owner "CONTOSO\Sysadmin" -CPUType $CPUType
    -Name "Profile1e99423a-34db-4d4f-ae73-92f79b50e881" -Description "Profile used to
    create a VM/Template" -CPUCount 1 -MemoryMB 1024 -RelativeWeight 100 -HighlyAvailable
    $false -NumLock $false -BootOrder "CD", "IdeHardDrive", "PxeBoot", "Floppy"
    -LimitCPUFunctionality $false -JobGroup 35d5539a-78ca-47ee-8073-b398d6390a95

New-VirtualDiskDrive -VMMServer localhost -IDE -Bus 0 -LUN 0 -JobGroup 35d5539a-
    78ca-47ee-8073-b398d6390a95 -Size 40960 -Dynamic -Filename "VM00_disk_1"

$VMHost = Get-VMHost -VMMServer localhost | where {$_.Name -eq "ServerFull01
    .contoso.com"}

$HardwareProfile = Get-HardwareProfile -VMMServer localhost | where {$_.Name
    -eq "Profile1e99423a-34db-4d4f-ae73-92f79b50e881"}
```

```
$OperatingSystem = Get-OperatingSystem -VMMServer localhost | where {$_.Name
    -eq "Windows Server 2003 Enterprise x64 Edition"}
New-VM -VMMServer localhost -Name "VM00" -Description "VM created from a script."
    -Owner "CONTOSO\Sysadmin" -VMHost $VMHost -Path "G:\VirtualMachines"
    -HardwareProfile $HardwareProfile -JobGroup 35d5539a-78ca-47ee-8073-b398d6390a95
    -RunAsynchronously -OperatingSystem $OperatingSystem -RunAsSystem -StartAction
    NeverAutoTurnOnVM -StopAction SaveVM
```

If you look through the script, you can see that it is relatively easy to reuse this script to generate another new VM. Just change the name of the VM, the name of its VHD, and run the script. Both items have been highlighted in **bold** in the sample script.

However, if you want to reuse this script in a simpler way and pass the name of the new VM as well as the name of its VHD to the script as you launch it, you need to make a couple of modifications. Open the script in Notepad and begin by adding the following entries just under the help entry at the top of the script:

```
# For additional help on cmdlet usage, type get-help <cmdlet name>
# -----
# Define variables
# -----
$VMName = $args[0]
$VHDName = $args[1]
# -----
```

This adds two new arguments to the script. Because they are arguments, you can type the values for each argument as you call the script. But first, you need to replace the actual values in the script with the variables you just created. Two values need to be changed:

```
New-VirtualDiskDrive -VMMServer localhost -IDE -Bus 0 -LUN 0 -JobGroup 35d5539a
    -78ca-47ee-8073-b398d6390a95 -Size 40960 -Dynamic -Filename "$VHDName"
```

And:

```
New-VM -VMMServer localhost -Name "$VMName" -Description "VM created from a script."
    -Owner "CONTOSO\Sysadmin" -VMHost $VMHost -Path "G:\VirtualMachines"
    -HardwareProfile $HardwareProfile -JobGroup 35d5539a-78ca-47ee-8073-b398d6390a95
    -RunAsynchronously -OperatingSystem $OperatingSystem -RunAsSystem -StartAction
    NeverAutoTurnOnVM -StopAction SaveVM
```

Close Notepad and save the script. Now open the SCVMM PowerShell prompt, move to your Documents folder, and execute the script to generate a new VM:

```
cd \Documents
.\NewVMScript.ps1 "VM02" "VM02_Disk_1"
```

This will create a new VM named VM02 and assign a blank VHD named VM02_Disk_1 to the new VM. Using these methods with SCVMM-generated scripts will save you a lot of time when you want to automate operations on your VMs and hosts.

PRACTICE Using Windows PowerShell to Automate VM Management

In this practice, you will install PowerGUI and begin to use it to generate and run Windows PowerShell cmdlets against ServerFull01. This practice consists of three exercises. In the first exercise, you install PowerGUI and enable the Hyper-V PowerPack. In the second exercise, you obtain the server names from Active Directory Domain Services and begin to examine the type of functions you can perform with PowerGUI. In the third exercise, you perform your first PowerGUI actions against a VM.

EXERCISE 1 Install PowerGUI

In this exercise you will prepare ServerFull01 to run PowerGUI with the Hyper-V PowerPack. Perform this operation with domain administrator credentials.

1. Log on to ServerFull01 with domain administrative credentials. Launch Internet Explorer, go to <http://www.powergui.org/downloads.jspa>, and obtain a copy of PowerGUI.msi as well as the Active Directory cmdlets, which will be from the Quest Web site (ActiveRoles Management Shell for Active Directory 64-bits). Save everything in your Documents folder. You can also download a manual from the Quest Web site. Accept any prompts you get from the Internet Explorer's Security mode. Finally, return to <http://www.powergui.org> and download the Hyper-V PowerPack from the PowerGUI Library at <http://www.powergui.org/kbcategory.jspa?categoryid=21> and click the Virtualization link. Note that there are several useful PowerPacks here. Download the Hyper-V PowerPack by clicking the link, right-clicking Hyper-V.PowerPack under How to Install, choosing Save Target As, and then clicking Save. Close Internet Explorer.
2. Open Windows Explorer and move to your Documents folder. Begin by installing the Management Shell for Active Directory. Double-click ManagementShellforActiveDirectory64bit_112.msi, click Run, and then click Next. Accept the license agreement and click Next. Type in your name and the organization's name and click Next. Click Next to begin the installation and click Finish when the installation is complete. Click Yes to restart your computer.
3. Log on to ServerFull01 with domain administrator credentials. Open Windows Explorer and move to your Documents folder. Install PowerGUI by double-clicking the link, clicking Run, and then clicking Next. Accept the license agreement and click Next. Type in your name and the organization's name and click Next. Select to install the following items (see Figure 7-14):
 - PowerGUI
 - PowerGUI Script Editor
 - Active Directory (under PowerPacks)
 - Local System (under PowerPacks)
 - Network (under PowerPacks)
 - User Interface Localization

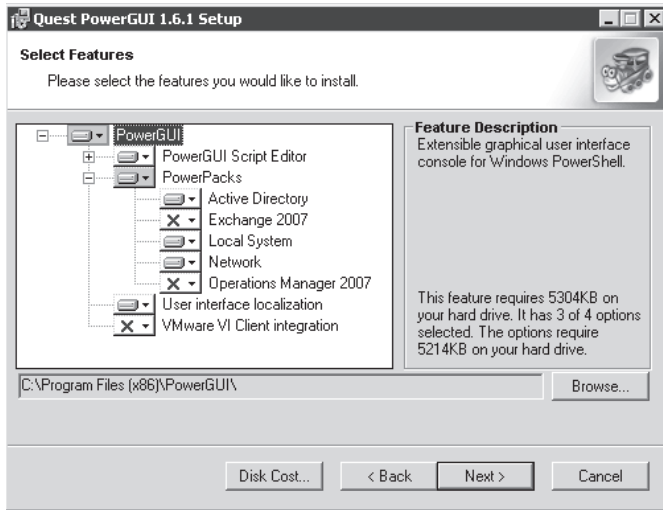


FIGURE 7-14 Installing PowerGUI

4. Click Next when ready and click Next again to install. Click Finish when done. Make sure that Start PowerGUI After I Finish is selected.

You are ready to move on to the next exercise.

EXERCISE 2 Prepare PowerGUI to Support Hyper-V

In this exercise you will prepare PowerGUI to work with Hyper-V. Continue to perform this exercise on ServerFull01.

1. When the PowerGUI Administrative Console is open, right-click the root node (PowerGUI) and select Import. This opens the Import dialog box and puts you in the Documents folder. Select Hyper-V.PowerPack and click Open. This adds the Hyper-V node at the bottom of the PowerGUI tree.
2. Expand the Hyper-V node and select Find Hyper-V Servers to search Active Directory for Hyper-V servers. This opens the Where Would You Like To Search window. Move the cursor to Domain DNS Name, type **Contoso.com**, and click OK. This will use your current credentials to search AD DS for Hyper-V servers. If your servers are not part of a domain, you can perform the same task using the Managed Hyper-V Servers node—use the Add Connection command in the Action pane to add individual Hyper-V servers. The search results should display the servers you have installed with the Hyper-V role (see Figure 7-15).
3. The search was performed using Windows PowerShell code. To view the code that was used, click the PowerShell Code tab at the bottom of the Details pane (see Figure 7-16). Return to the UI by clicking the UI tab at the bottom of the Details pane.

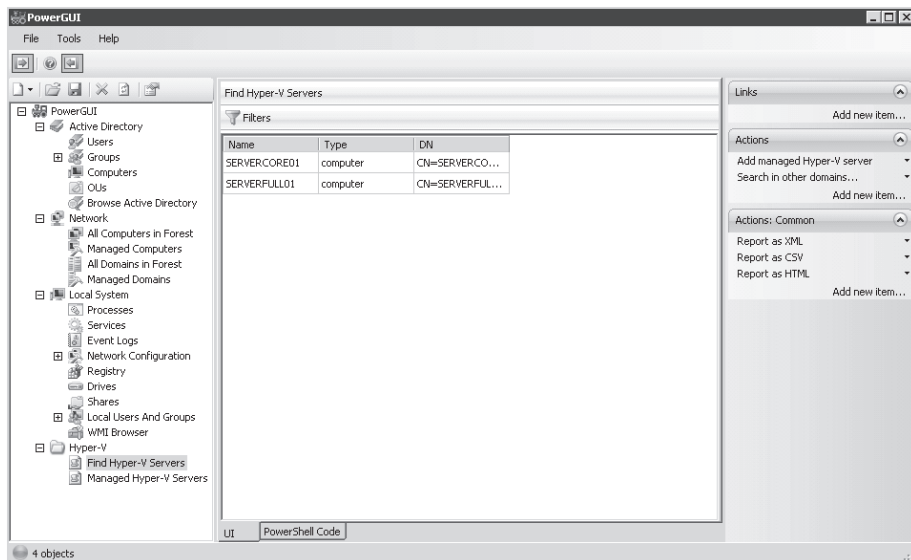


FIGURE 7-15 Finding Hyper-V servers

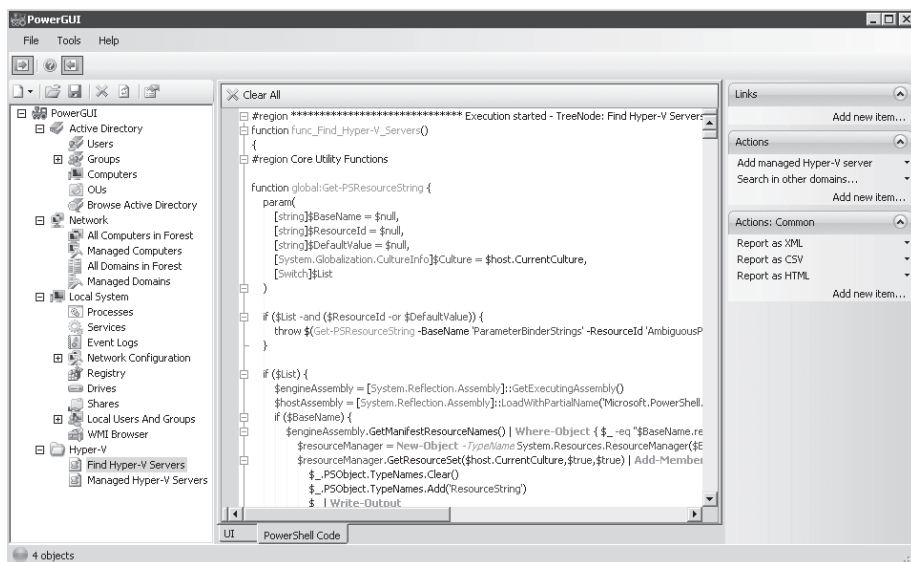


FIGURE 7-16 Viewing the Windows PowerShell script

4. Right-click ServerCore01 and select Actions, and then select Add Managed Hyper-V Server. Type in the name of your domain administrator account—for example, **Contoso\Administrator**—and click OK. Type in your password and click OK. You do not need to repeat the operation for ServerFull01 because the Local System is managed automatically.

You are now ready to manage your Hyper-V servers and the VMs they run with PowerGUI. As you can see, it was relatively easy to generate the code required to locate and add your host servers.

EXERCISE 3 Manage a VM

In this exercise you will use PowerGUI to manage VMs on Hyper-V servers. You will set one of the VMs located on ServerFull01 to a saved state. Perform this exercise from ServerFull01.

1. In the PowerGUI Console, click Managed Hyper-V Servers under the Hyper-V node in the Tree pane. It may take the console a moment to respond.
2. Click Local System when it appears in the Tree pane. Note that it is now a branch that includes several sub-items.
3. Click Hyper-V Manager under Local System. Once again, the node expands.
4. Click Virtual Machines. This will list the VMs hosted on ServerFull01.
5. Move to the Details pane and click SCOM01. Note how the Actions pane is populated with potential commands. Also note that SCOM01 is the only running machine.
6. Click Save in the Actions pane. This will save the state of the VM. Now click the PowerShell Code tab. View the code used for this execution. The code begins at `#region*****` ... and ends with the line containing `#endregion*****` ... (see Figure 7-17).

```
#region ***** Execution started - TreeNode: Virtual Machines ****
function func_Virtual_Machines()
{
    &{
        param(
            $ComputerName = '.') Get-HyperVVirtualMachine -ComputerName $ComputerName | ForEach-Object {
                Add-PowerGUIHyperVVirtualMachineContainerNodes -VirtualMachine $_ -ComputerName $ComputerName
            }
        }
    }
}

function action()
{
    $input | ForEach-Object {
        $job = $_.Save()
    }
}

func_Virtual_Machines | where { $_.Name -eq 'SCOM01' } | action

#endregion ***** Execution completed - TreeNode: Virtual Machine
```

FIGURE 7-17 Verifying a Windows PowerShell script

7. Change back to the UI tab. Make sure SCOM01 is still selected and click Start to start it.

You can continue to explore all of the various tasks you can perform on both VMs and servers in PowerGUI. As you can see, a lot of actions are supported by the Hyper-V PowerPack.

MORE INFO WORKING WITH THE HYPER-V POWERPACK

To view a video on how to work with the Hyper-V PowerPack, go to http://powergui.org/shares/powergui/sbin/docs/Introduction_to_the_HyperV_PowerPack/Introduction_to_the_HyperV_PowerPack.html.

Quick Check

1. How do you install Windows PowerShell on Windows Server 2008 and which feature is a requirement for it?
2. What kind of syntax is used in Windows PowerShell?
3. What is the default script execution policy for Windows PowerShell?
4. Which cmdlet enables scripting in PowerShell?

Quick Check Answers

1. Windows PowerShell is installed on Windows Server 2008 by adding a feature from the Server Manager console. The .NET Framework will be installed automatically because it is required to support Windows PowerShell operations.
2. Windows PowerShell uses a Verb-Noun syntax.
3. The execution policy by default for Windows PowerShell is set to Restricted. No scripts can run by default.
4. The cmdlet is *Set-ExecutionPolicy RemoteSigned*. You can view the results with the following cmdlet: *Get-ExecutionPolicy*.

Case Scenario: Automating Hyper-V Operations

In the following case scenario, you will apply what you've learned about automating VM management with Windows PowerShell. You can find answers to these questions in the "Answers" section on the companion CD that accompanies this book.

You are the resource pool administrator for Lucerne Publishing. You have already implemented your host environment and have begun converting production physical machines into virtual machines. Now your management has decided that it is time to implement a new laboratory in support of a new development project. The development group will require up to 20 virtual machines in support of their project. These machines only need to be base Windows Server 2008 machines because the development team will install and configure additional roles on these machines on their own. These machines will run on two Server Core installations of Windows Server 2008 with Hyper-V. In addition, these machines will be using differential disks because the development team wants to generate at least two snapshots per day for each of the VMs.

Management is concerned, however, that preparing this environment will take too much of your time and take you away from the conversion of the production systems, thereby delaying that project. Note, however, that the two host servers are already up and running and you will not need to spend time preparing them. In addition, the machines are already integrated within a Development host group in System Center Virtual Machine Manager. In addition, you already have a Windows Server 2008 template VM stored within the SCVMM Library.

Specifically, management wants you to answer the following questions before they give the OK to proceed with the development project.

1. How can you prepare the 20 machines that are required for the development team without losing too much time?
2. How can you monitor the 20 machines?
3. How can you ensure that two snapshots are taken every day on each VM without taking too much of your time?

Suggested Practices

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

Automating Hyper-V Tasks

- **Practice 1** Install the Hyper-V PowerShell Library and explore the cmdlets it gives you for managing Hyper-V operations. Perform as many interactive tasks with PowerShell as possible.

- **Practice 2** Install the PowerGUI and the Hyper-V PowerPack and explore the cmdlets it gives you for managing Hyper-V operations. Generate as many scripts with Windows PowerShell as possible.
- **Practice 3** Use the SCVMM wizards to generate scripts. Copy them with the View Script command and adapt them to run generically. Perform this with as many scripts as possible.
- **Practice 4** Take the time to go through the WMI reference Web site for Windows Server 2008 with Hyper-V. Familiarize yourself with the names of all of the exposed classes and how they can be used. Read about the Hyper-V WMI provider at [http://msdn.microsoft.com/en-us/library/cc136992\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/cc136992(VS.85).aspx).

Chapter Summary

- Windows PowerShell is built on top of the .NET Framework, and is not installed by default on Windows Server 2008. It cannot be installed on Windows Server 2008 Server Core, but you can execute cmdlets remotely against Server Core installations.
- Windows PowerShell works with several constructs. It contains various cmdlets and aliases in the default implementation. However, it does not support the ability to run scripts by default because its execution policy is set to Restricted.
- Windows PowerShell can be used to manage Hyper-V virtual machines. The easiest way to work with it is to install the Hyper-V PowerShell Library.

You can also use PowerGUI, a graphical interface for the generation of PowerShell cmdlets, because it also includes custom cmdlets to manage Hyper-V hosts and virtual machines. With PowerGUI you can obtain different PowerPacks that can be used to manage several additional Windows applications.
- Windows PowerShell can also be used to work with System Center Virtual Machine Manager (SCVMM). Windows PowerShell is installed by default with SCVMM. It can manage virtual machine hosts, library servers, virtual machines, and other SCVMM components and it is the default execution engine for SCVMM.

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).

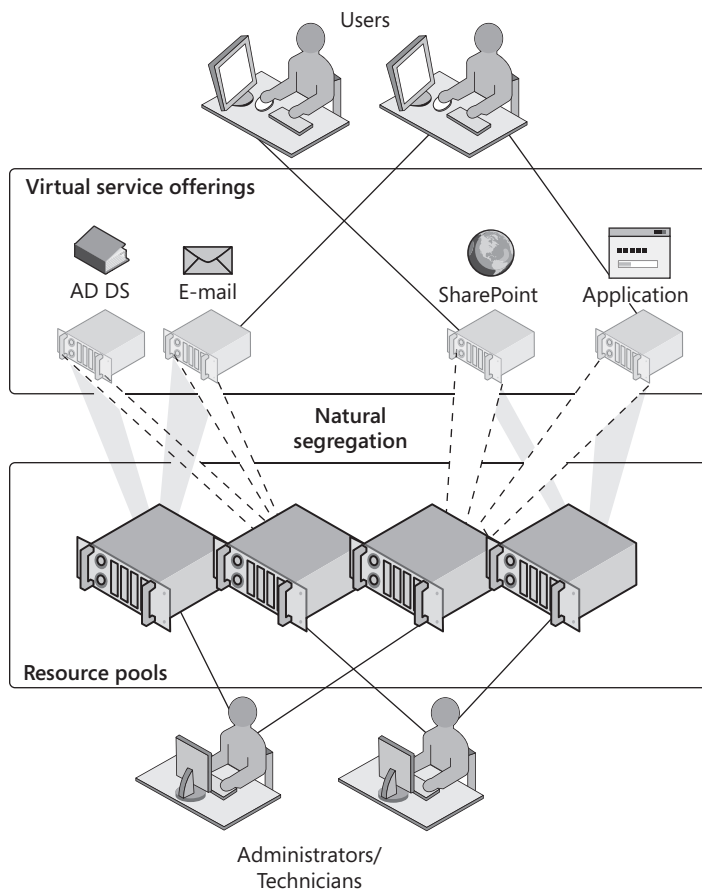


FIGURE 8-1 The natural segregation of resource pools and virtual service offerings

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.

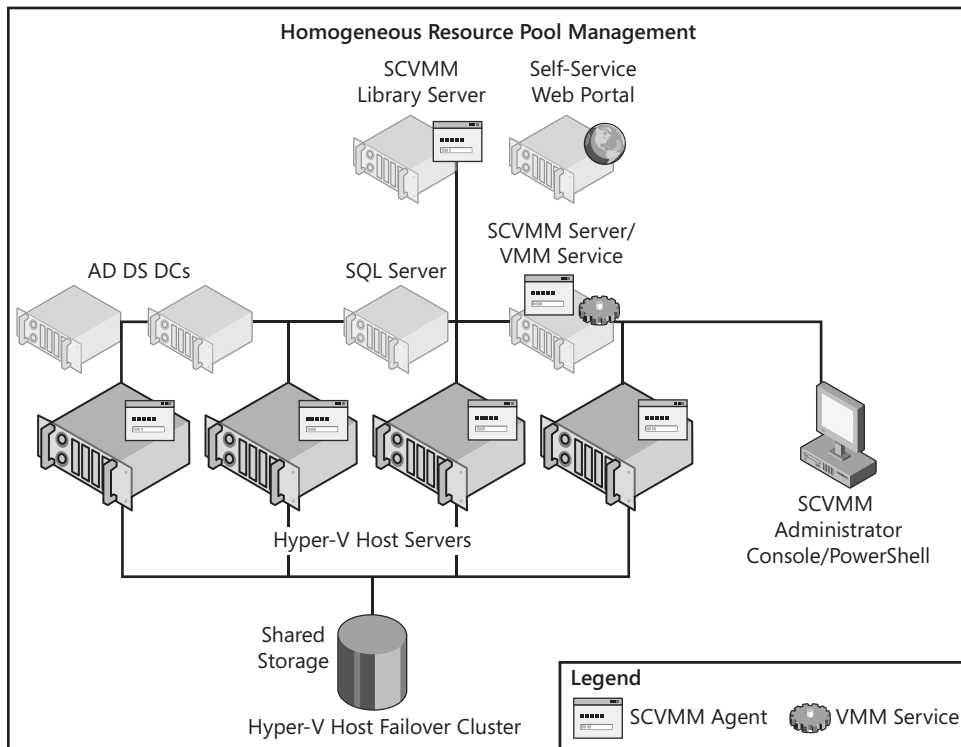


FIGURE 8-2 A homogeneous resource pool configuration

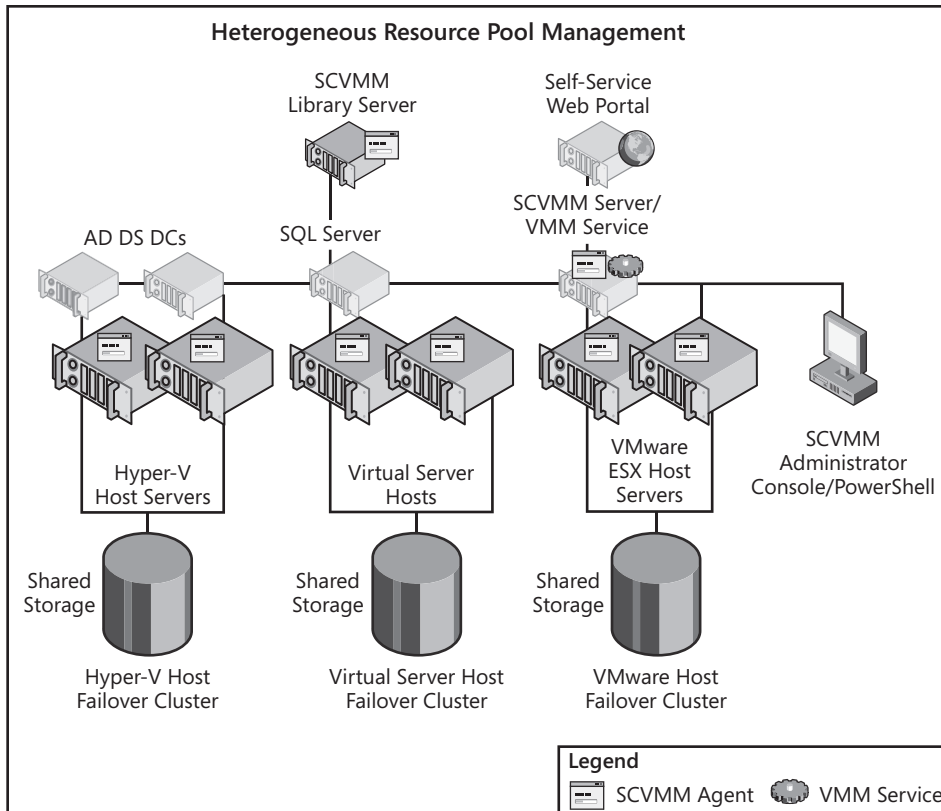


FIGURE 8-3 A heterogeneous resource pool configuration

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 <i>Hyper-V Security Guide</i> 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.

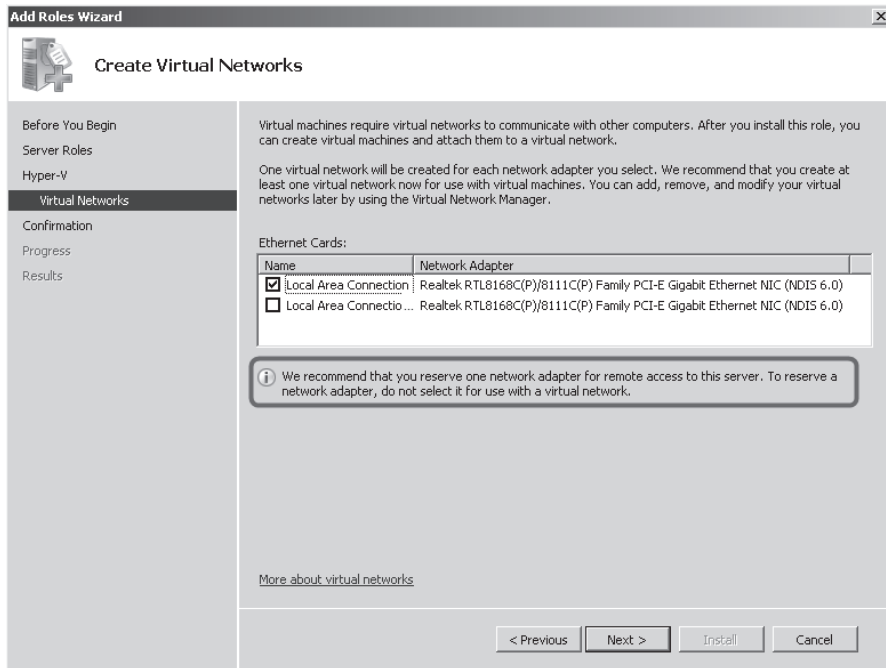


FIGURE 8-4 The Hyper-V Installation Wizard recommends reserving one adapter for management purposes.

- 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).

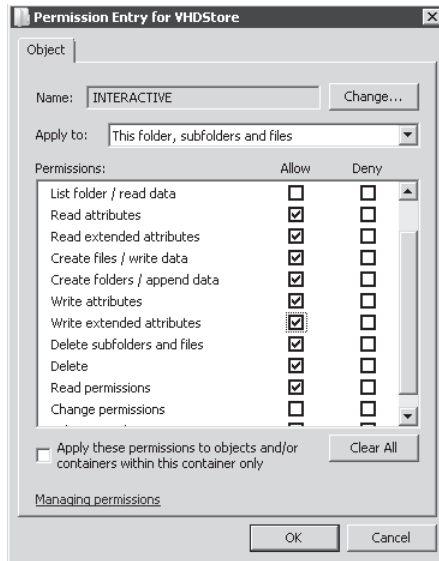


FIGURE 8-5 Assigning proper permissions to the three special accounts: Interactive, Batch, and Service

- 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.

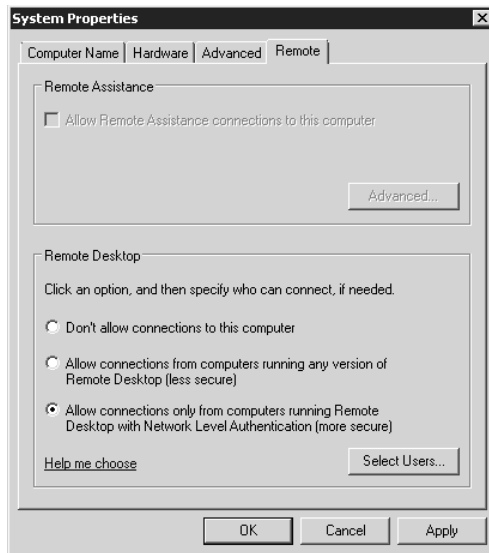


FIGURE 8-6 Using secure communications for the Remote Desktop

- **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.

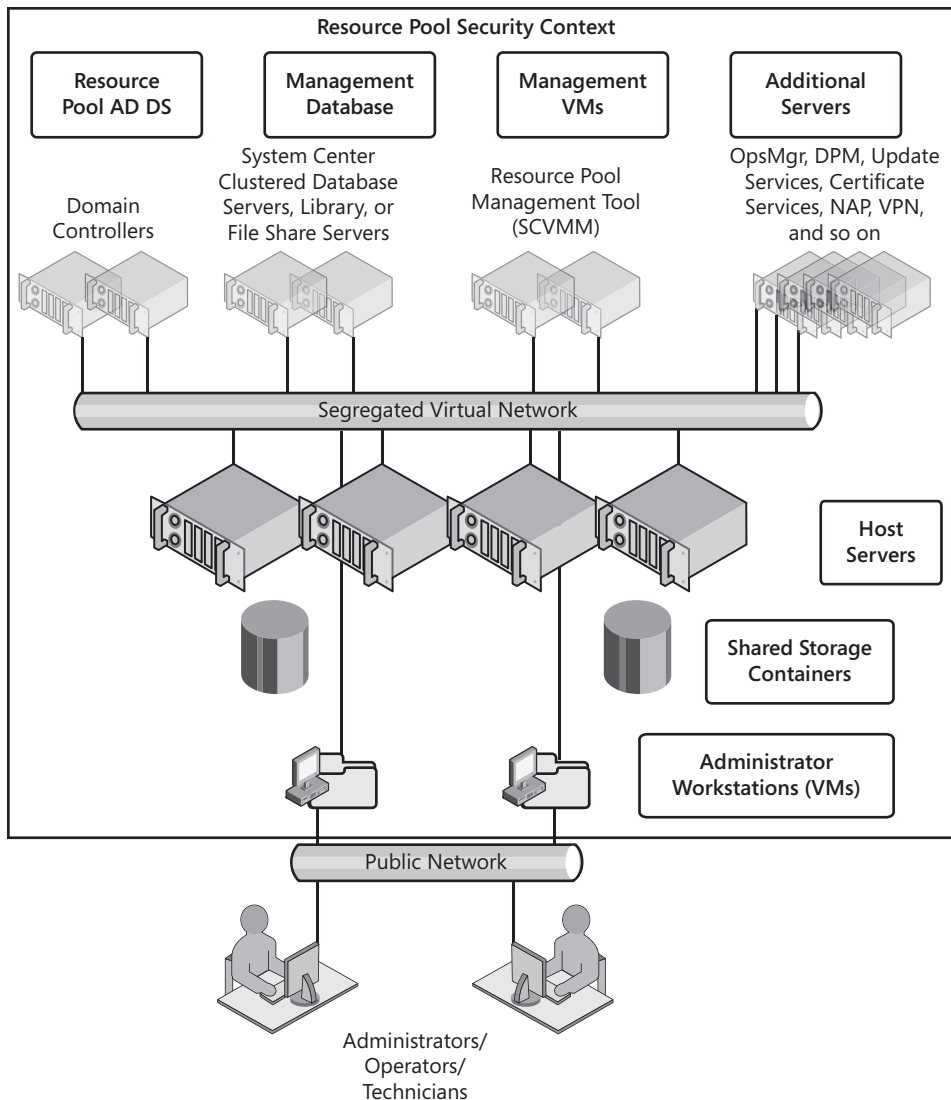


FIGURE 8-7 A resource pool including required and optional components

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).

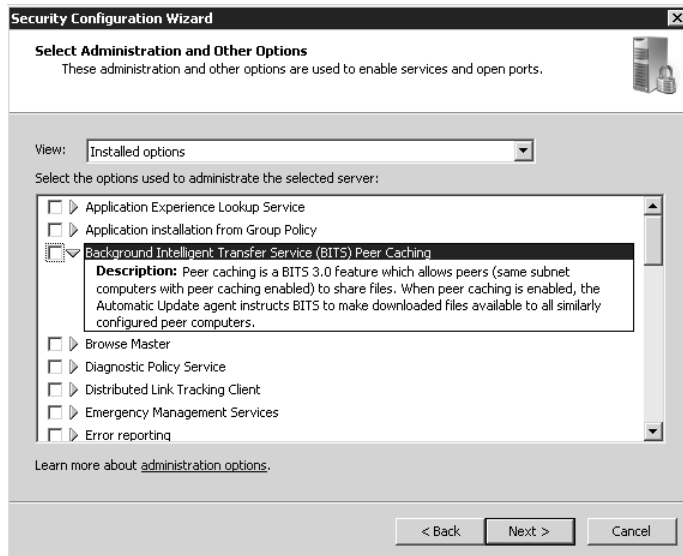


FIGURE 8-8 Obtaining additional information from the Security Configuration Wizard

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.

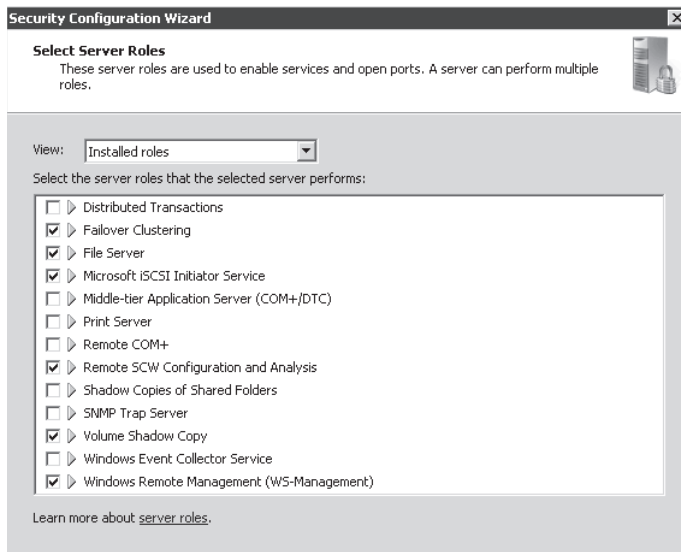


FIGURE 8-9 The Security Configuration Wizard does not include specific information on the Hyper-V role even if it is installed.

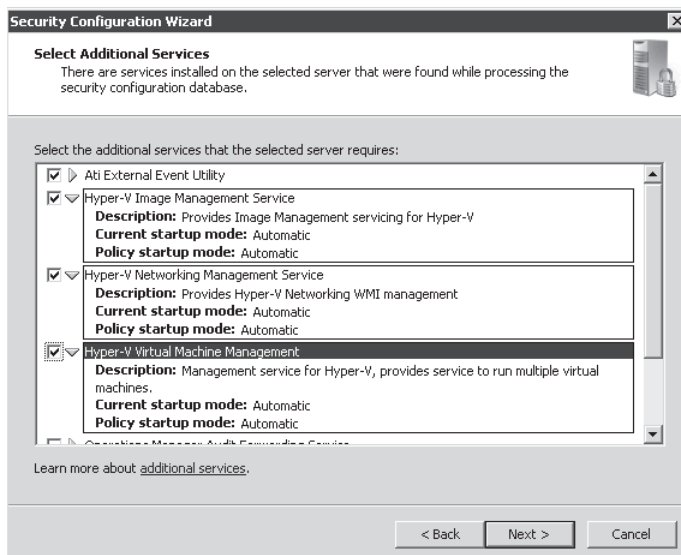


FIGURE 8-10 The Security Configuration Wizard understands Hyper-V services.

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.

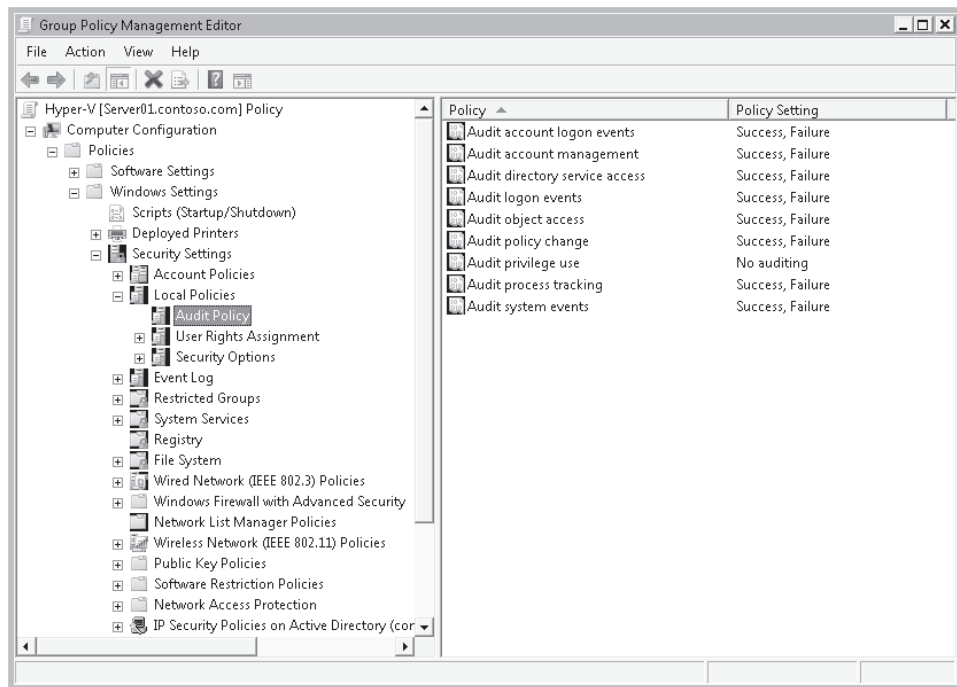


FIGURE 8-11 The Audit section of a security policy generated through SCW and then converted to a GPO

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.msp?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.

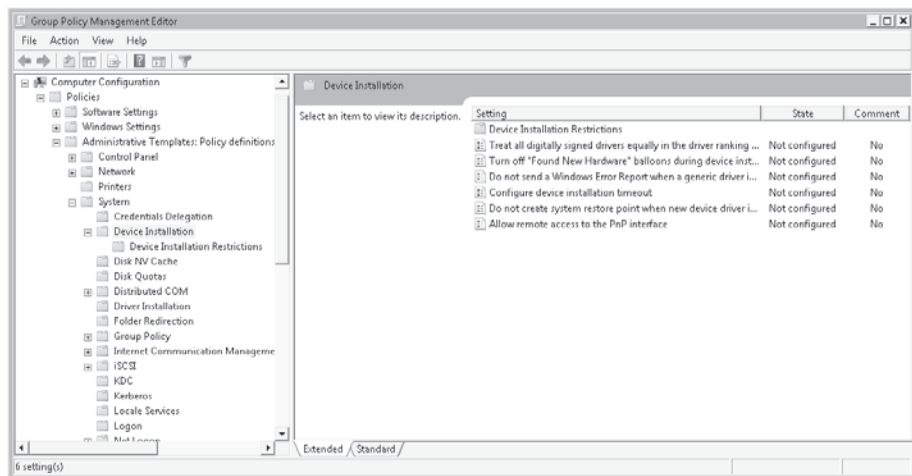


FIGURE 8-12 Setting device restrictions in a GPO

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.

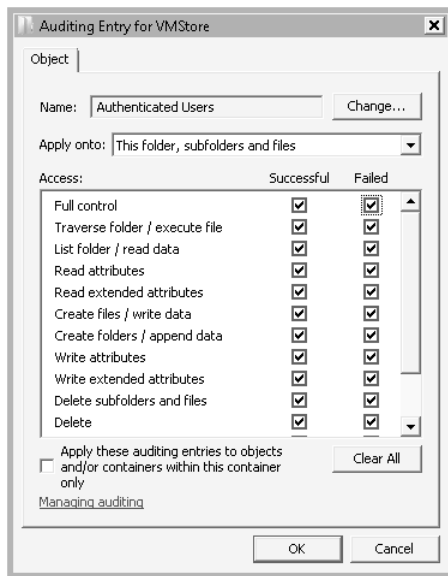


FIGURE 8-13 Auditing changes in a VM storage folder

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.

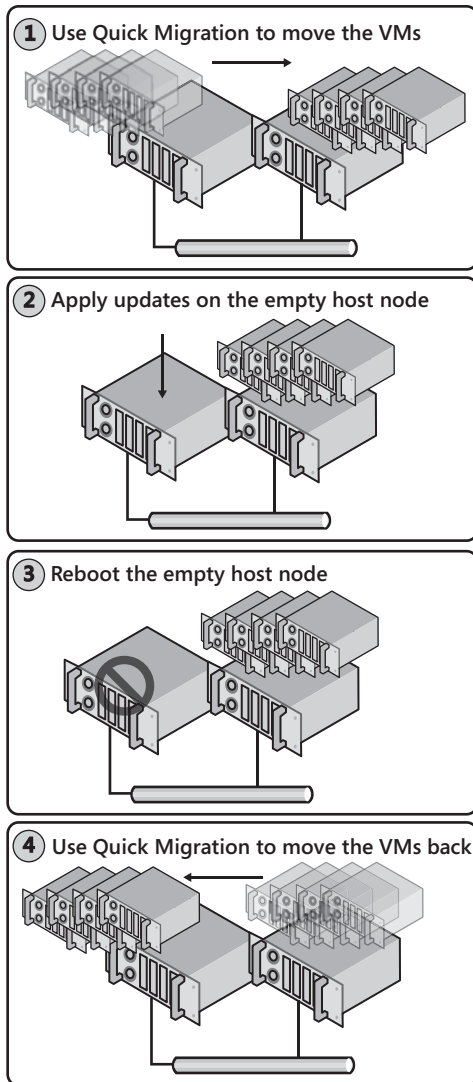


FIGURE 8-14 Updating clustered hosts

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.

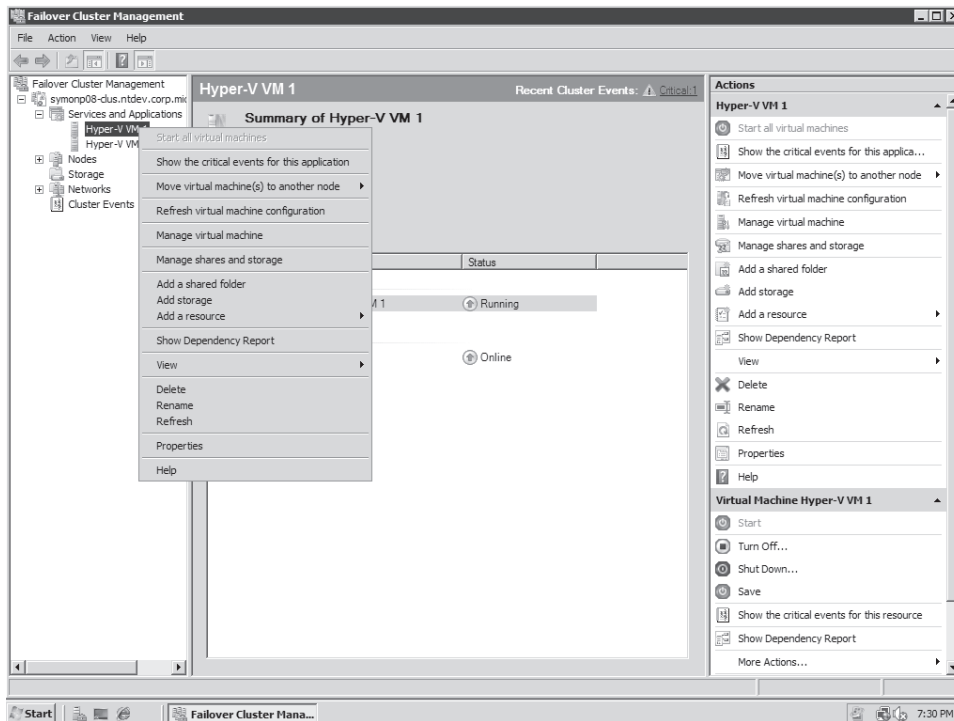


FIGURE 8-15 Moving VMs to another cluster node

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.

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).

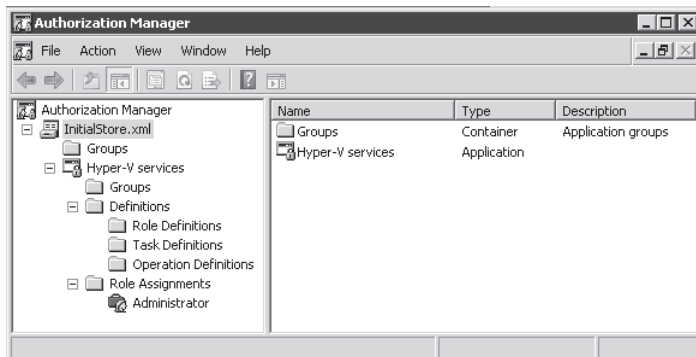


FIGURE 8-17 The structure of the Hyper-V initial store

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.

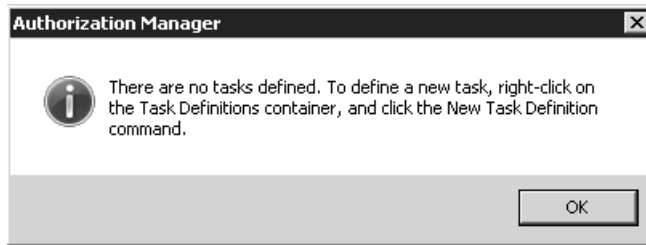


FIGURE 8-18 The No Tasks Defined warning

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

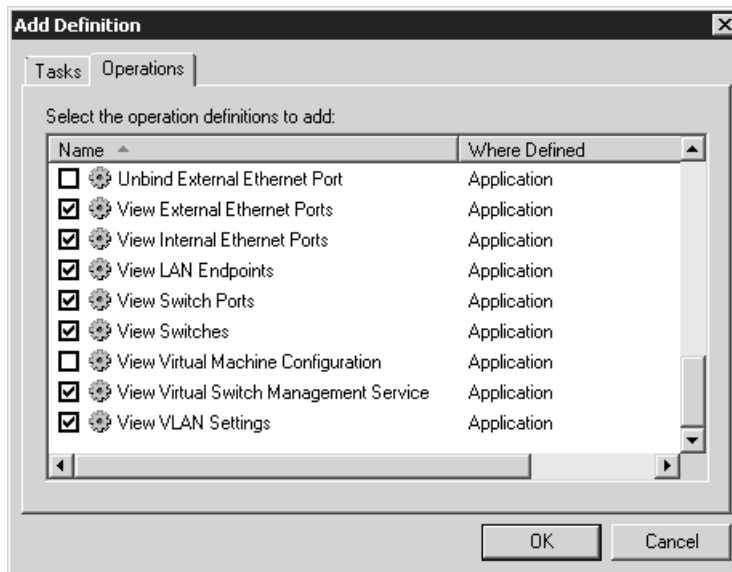


FIGURE 8-19 Assigning operations to tasks

- 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.

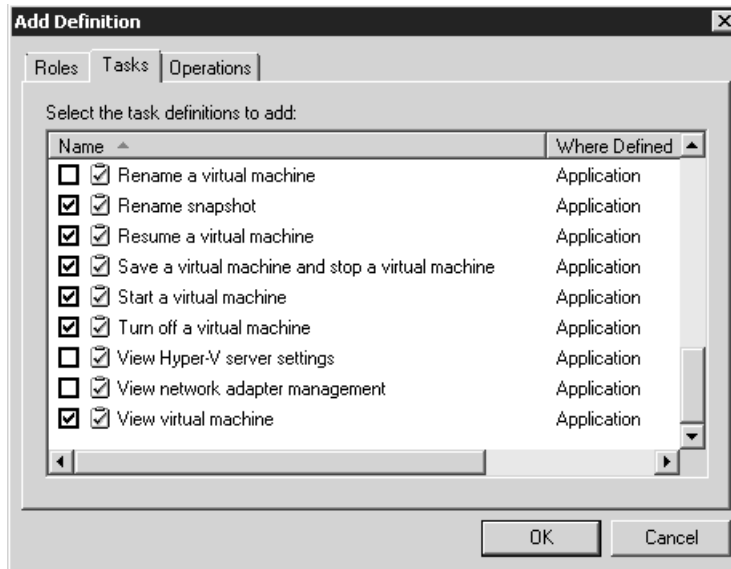


FIGURE 8-20 Assigning tasks to role definitions

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

- 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.

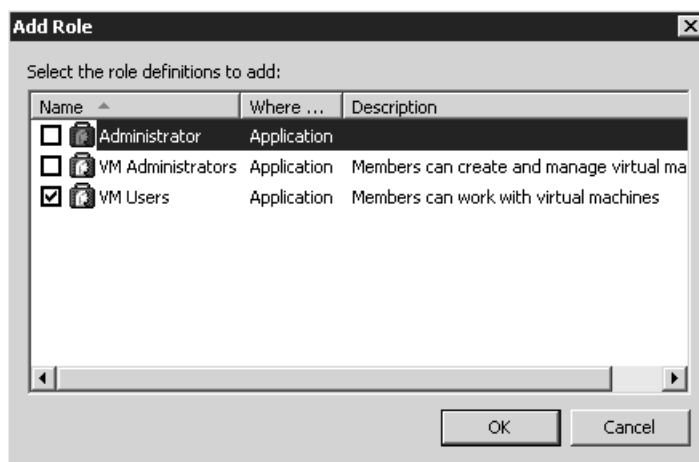


FIGURE 8-21 Assigning role definitions to role assignments

- 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).

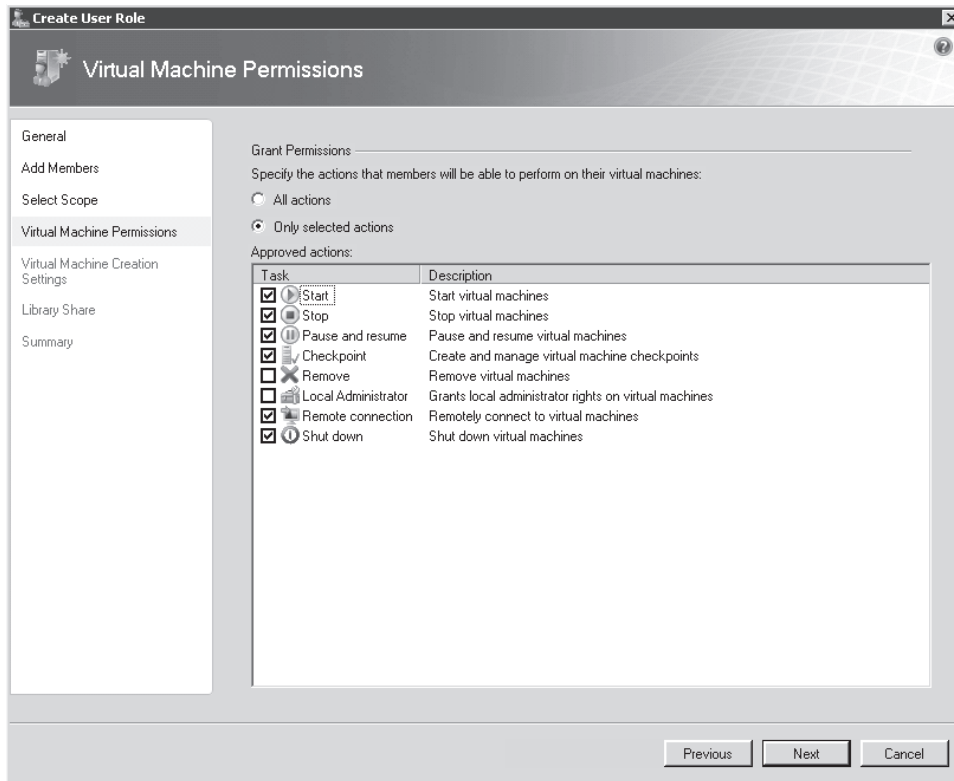


FIGURE 8-22 Controlling self-service user rights in SCVMM

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.

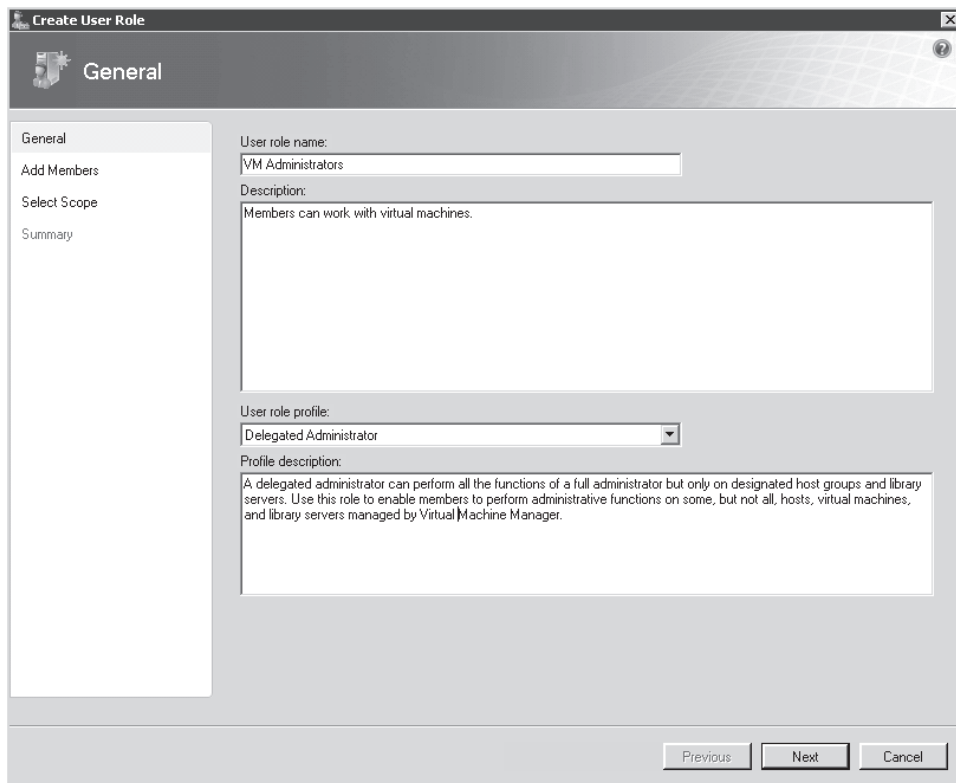


FIGURE 8-23 Delegating administrative tasks in SCVMM

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).

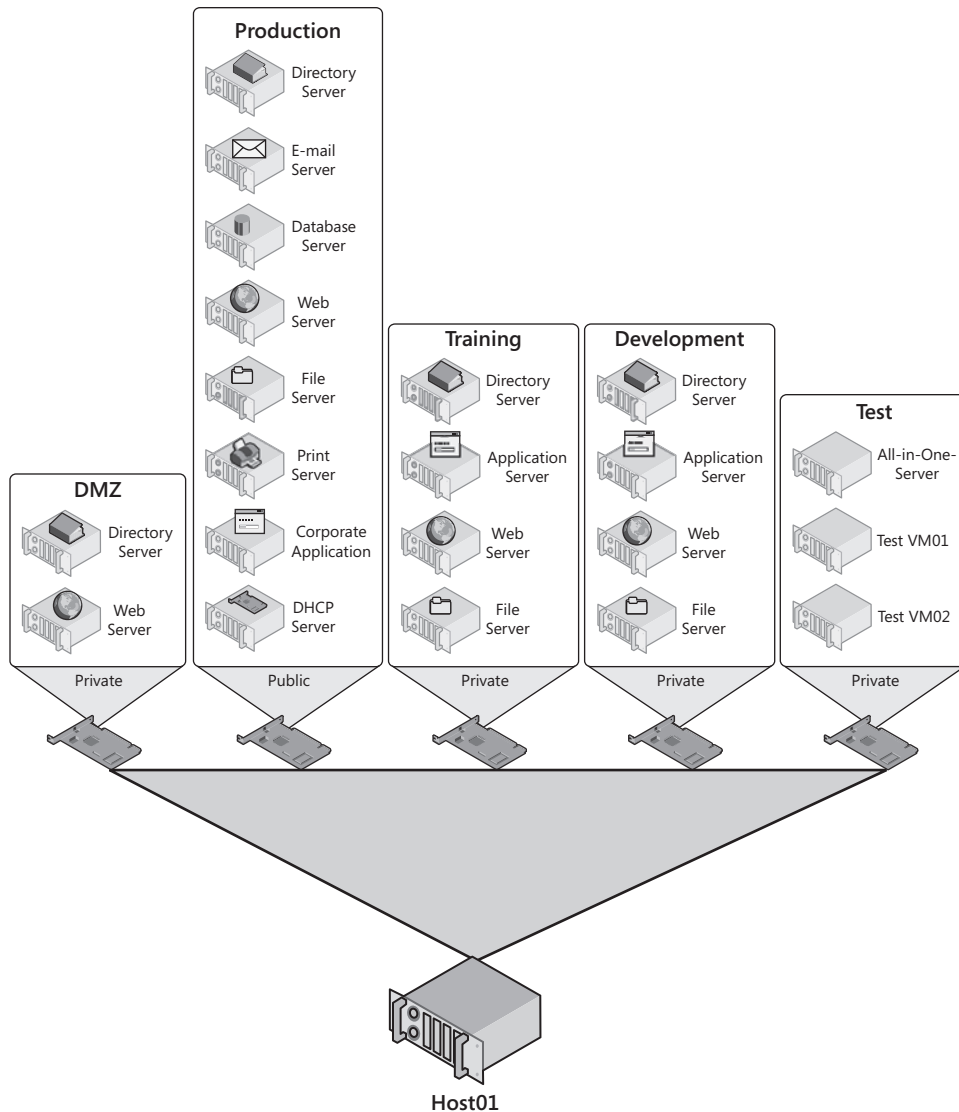


FIGURE 8-24 Controlling VM connectivity through Hyper-V virtual networks

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.

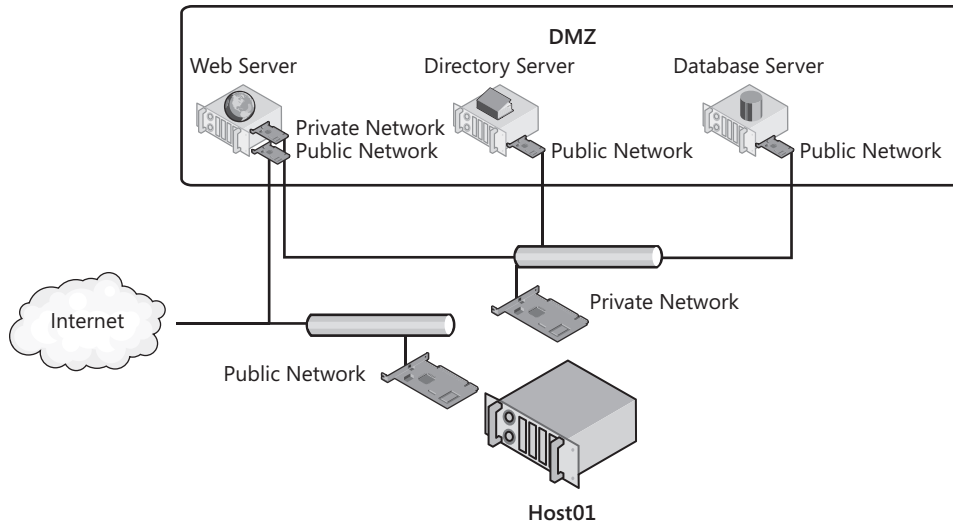


FIGURE 8-25 Creating a perimeter network in a virtual environment

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).

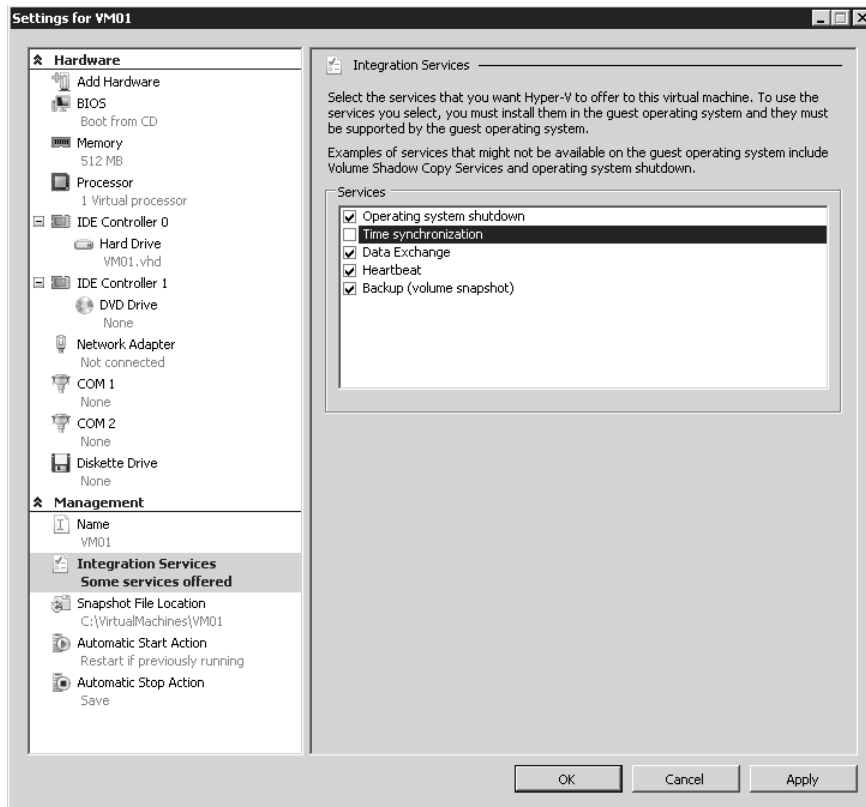


FIGURE 8-26 Setting time synchronization settings for a VM

- 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.

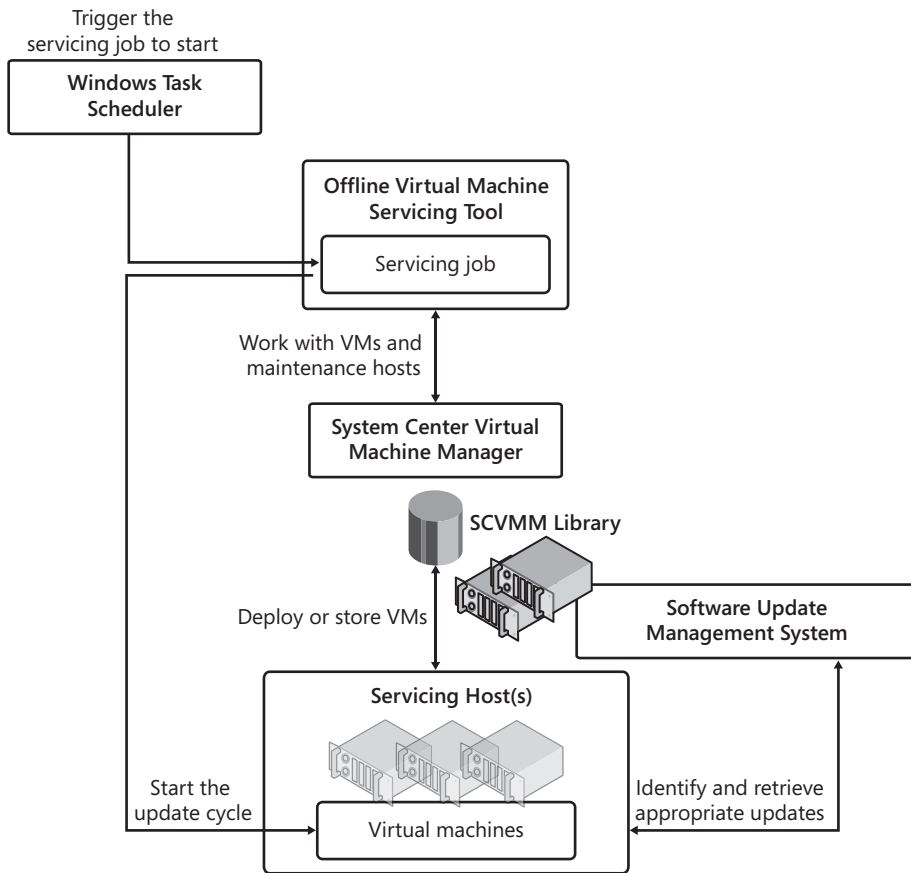


FIGURE 8-27 The OVMST update process

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.

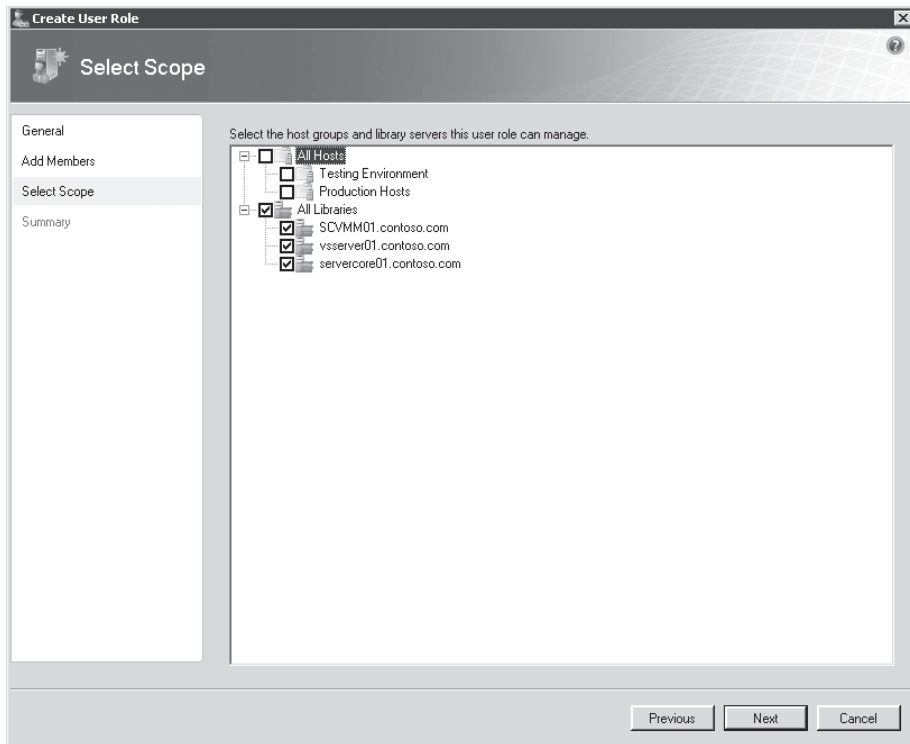


FIGURE 8-28 Selecting the scope of delegation

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).

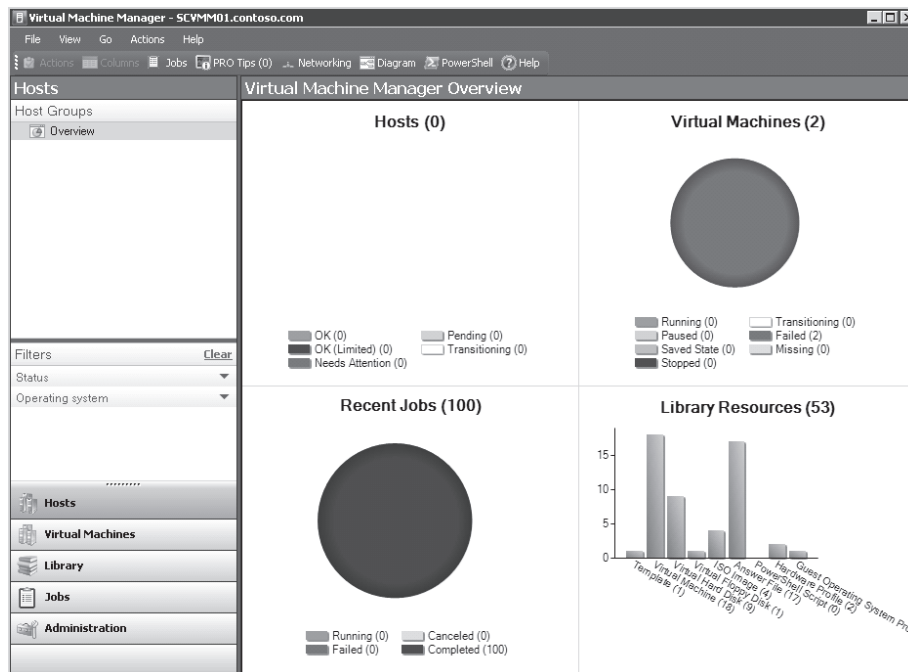


FIGURE 8-29 Viewing a delegated console

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.

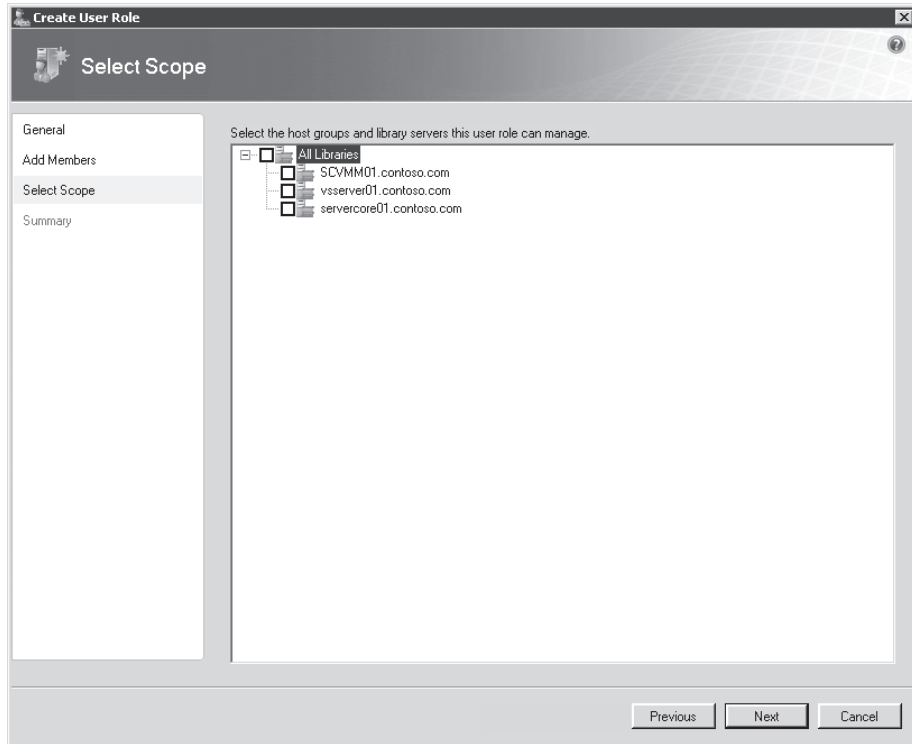


FIGURE 8-30 Delegated administrators only have control over their own delegation scope.

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.

Protecting Hyper-V Resource Pools

Data protection is one of the most important aspects of any resource pool because of the very nature of the pool itself: It is composed of host servers running virtual workloads. Running your production workloads in virtual machines transforms the way you work with production machines, but it also has both positive and negative impacts on your protection strategies.

First of all, you need to design a protections strategy for your host servers. As you know, if a host server fails and it is not protected, all of the virtual workloads on that server will also fail. However, if you run the host server on a failover cluster, the workloads on the host server will automatically be transferred to another host. If you don't run the host server on a failover cluster—for example, if you are running a Standard edition of Windows Server 2008 with Hyper-V or if you are running Windows Hyper-V Server—all of the workloads fail. What is worse is that you cannot transfer the virtual machines from a failed Hyper-V to another host server because even if you can access the VMs—for example, if they are stored on a shared folder running on a separate server or in a storage area network—you cannot open an existing VM within Hyper-V. Hyper-V only supports the exporting and importing of a VM, but if the host server has failed, you cannot export the VM from the original host.

This means that you must have protection mechanisms for both the virtual machines you run and the hosts themselves. If for some reason you run standalone hosts, you must have a solid backup and recovery strategy for the host.

MORE INFO HYPER-V FAILOVER CLUSTERS

More information on creating and deploying both single-site and multi-site Hyper-V failover clusters can be found in Chapter 3, “Completing Resource Pool Configurations.”

These protection mechanisms range from simple backups to disks to complex systems that automatically store all information offsite. The mechanisms you choose for your environment will depend on the size of your organization, the recovery policies your organization has in place, and the complexity of your resource pool. Keep the following considerations in mind as you plan for your own recovery strategy:

- If you are running standalone host servers, you must protect each and every host server through regular backups. These backups must be tested regularly to ensure that they are consistent and provide a valid restoration method.
- If you are running clustered host servers, you should try to have as many redundant nodes as possible to avoid single points of failure. If VMs are hosted on a resource group that includes more than two nodes, the likelihood of having all nodes fail at once is considerably reduced and your virtual machines are well protected. They should still be backed up, however. To protect the hosts even more, you should have a means of quickly re-creating a host and introducing it into the cluster to replace failed nodes.
- If you are using a single-site cluster, make sure your shared storage container is not a single point of failure. If you are using a storage area network, rely on the SAN's own capabilities to create duplicates of the data your cluster manages—that data being, in fact, the VMs you run.
- If you are running multi-site host clusters, you are already replicating the virtual machine data offsite and are protected. Once again, you still need a means to back up the virtual machines themselves as well as a simple means to introduce new hosts into the cluster if required.
- If you are running a resource pool management tool such as System Center Virtual Machine Manager, you need to make sure you protect this system as well as the database it relies on.
- If your resource pool is using a utility directory—as it should—you must protect the domain controllers it relies on. If they are VMs, you can use normal VM protection strategies as defined in this chapter.
- If you are using Library Servers, you need to protect these systems so that they can be quickly recovered if a mishap occurs.

As you can see, your protection plan must cover more than just the host servers or the virtual machines they run. It must protect the entire resource pool, it must be tested, and it must be documented so that you know what to do in the event of a disaster.

MORE INFO HYPER-V PROTECTION STRATEGIES

For more information on Hyper-V protection strategies, look up “Backup and Disaster Recovery for Server Virtualization” at <http://technet.microsoft.com/en-us/magazine/2008.10.disasterr.aspx>.

Specifically in terms of backup, your disaster recovery strategy must consider how you intend to protect your systems. You have three choices:

- Back up entire host systems. This will back up both the host systems and the virtual machines running on them.
- Back up the files that make up the virtual machines as files only. This captures a VM as it is during its operation.
- Back up files and folders within each of the VMs.

Each method will have an impact on your recovery operations. In addition, you are faced with a potential issue that you do not face in physical environments: Because your resource pools are clustered together and because Hyper-V supports Quick Migration, the VMs that are on one host on Monday may very well not be the same VMs that are on the same host on Tuesday. This means that VMs are moving targets. Your protection strategy must take virtual machine mobility into account.

Exam objective in this chapter:

- Manage snapshots and backups.

Before You Begin

To complete this chapter, you must have:

- Experience with Windows Server 2003 and or Windows Server 2008 disaster recovery implementations.
- Access to a setup as described in the Introduction. In this case, you will be using the third USB disk, which was listed as a requirement.

Lesson 1: Protecting Your Resource Pools

Backing up a single server is a simple operation. However, backing up a host server that includes a multitude of virtual machines is a completely different operation. Will you back up just the host and then just the files that make up the VMs, or will you perform internal VM backups? Determining which strategy to use is the focus of this chapter.

After this lesson, you will understand:

- How to plan a backup solution.
- How to perform backups for the hosts.
- How to manage backups for the hosts.
- How to recover host servers.
- How to perform live backups using VSS and DPM.
- How to perform a backup within a VM.
- When to use backups vs. snapshots.
- How to restore VMs.

Estimated lesson time: 60 minutes

Understanding Hyper-V Host Protection Strategies

Backing up host servers means backing up three different types of objects:

- **Operating System** The partition that makes up the system drive and runs the host server parent partition.
- **Data Partitions** The data drive(s) that contains the virtual service offerings.
- **Virtual Machine Contents** The contents of the virtual service offerings must also be backed up. This is discussed in more detail in the next lesson.

Host servers are the simplest kind of server because they only run one major role: virtualization. If you set up your infrastructure right, backing these machines up is relatively easy. The ideal infrastructure for host servers is that of a server connected to some form of shared storage. Ideally, each and every data drive on the server will be hosted within the shared storage infrastructure. This provides several levels of defense against data or system loss:

- Each partition can either rely on the Volume Shadow Copy Service (VSS) or the internal snapshot tool provided with the storage unit to provide a first level of defense.
- The second level of defense is provided by the volume shadow copies of the virtual machines located on the data drive. These copies are generated on a regular basis if the storage drive is also a shared folder.

- A third level of defense is provided through failover clustering.
- The last level of defense is provided through backups of the disks that make up each host system.

Most of these methods focus on the protection of virtual machines. In the case of virtual machines, you'll be using new disaster recovery techniques. However, because Hyper-V host servers use a parent partition that runs the Windows Server 2008 operating system, you can rely on standard Windows Server recovery techniques to get a non-working host server back into running shape. These include:

- **Driver rollback** If your system becomes unstable because of a faulty driver, you can roll the driver back to restore the previous version, as long as you can still log on to your system. This is done by viewing the device properties in the Device Manager, which is reached by launching Server Manager and then using the Diagnostics node to access Device Manager. Then right-click the faulty device, choose Properties, click the Driver tab, and select Roll Back Driver (see Figure 9-1).

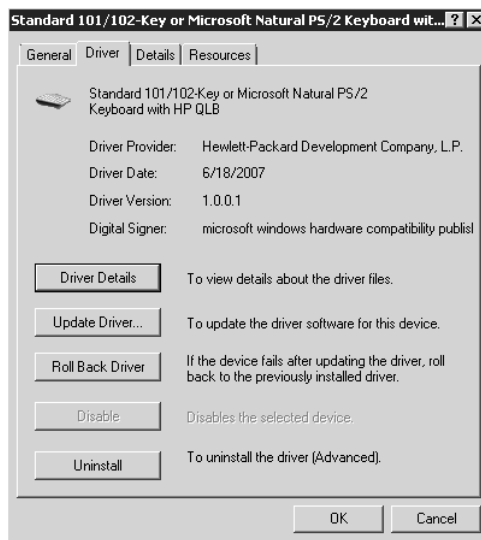


FIGURE 9-1 Rolling back a driver

- **Disabling devices** You can also use Device Manager to disable faulty devices. Do this by moving to Device Manager, locating the device, right-clicking it, and selecting Disable from the shortcut menu.
- **Last Known Good Configuration** Just like previous versions of Windows, Windows Server 2008 includes a Last Known Good Configuration startup choice. This reverts to the last configuration saved in the registry before you applied changes. You can access this option by pressing the F8 key during system startup. This also gives you access to a number of different startup modes: Safe Mode, Safe Mode With Networking, and so on. You can also use these various operational modes to try to repair non-working Windows Server 2008 installations.

- **Windows Recovery Environment (WinRE)** WinRE provides you with a special console that allows you to perform recovery operations, such as disabling services, copying device drivers or other files to the system, and otherwise repairing an installation. The console is available on the Windows Server 2008 installation media, but it can also be installed locally on host systems. You might consider installing this console on your host servers if you do not have ready access to an installation media DVD in the event of a mishap. This console includes a host of features that can repair a non-working system.

MORE INFO WinRE

For more information on WinRE, go to <http://technet.microsoft.com/en-us/library/cc766048.aspx>.

- **Windows PE** You can also use the Windows Preinstallation Environment (WindowsPE) to create a bootable device that will boot into a character-based Windows environment similar to Server Core. This is also an excellent recovery tool because Windows PE gives you access to both network drives and local NTFS drives during your repair process. Note that you can also use Windows PE to build a bootable device that includes WinRE.

MORE INFO WINDOWS PE

For more information on Windows PE, go to <http://technet.microsoft.com/en-us/library/cc749538.aspx>.

- **Windows Server Backup (WSB)** Using the default backup tool included within Windows Server 2008, you can back up and restore data to removable media or to spare disk drives. You can also back up entire systems to virtual hard drive images for complete system protection.
- **Third-party backup and restore tools** If you find that Windows Server Backup is not enough, you can choose from a number of different third-party tools. When selecting a third-party product, you must consider three key elements: integration with the Volume Shadow Copy Service APIs to take advantage of this feature, complete system recovery from bootable media, and integration with Windows Server 2008 roles such as Active Directory Domain Services.

As you can see, you should only resort to a backup to recover a server when nothing else works.

Understanding Virtual Machine Protection Strategies

When it comes to protecting virtual machines, your options are much more open than when you work with host servers. After all, most virtual machines are nothing but a set of files in a folder. Back up the files and you have a protected virtual machine. However, sometimes it isn't that easy. When a VM runs, it includes a lot of data in memory. If the machine is not in a saved state or is not shut down prior to the backup, you may lose data. In addition, when you back up only the files that make up VMs, the applications within the VMs will not be aware

that a backup has been performed. For example, when you back up database applications such as Exchange and Microsoft SQL Server, they do not truncate transaction logs because they do not know that a backup has been performed.

Because of their production nature, backing up virtual service offerings means backing up several types of information, including user data, corporate data, databases, documents, system state information for your servers, and Active Directory Domain Services data. You can use either the built-in backup tool or a third-party backup tool to perform these backups. But if you have multiple versions of operating systems in your VMs and you rely on the built-in tool, you need to rely on multiple, different tools. This is one more reason why you should be running enlightened guest operating systems. When you do, the backup tool you use at the Hyper-V host level will be able to rely on VSS to take a VSS snapshot of the VM while it is running and then create a data-consistent backup from this snapshot—as long as the Backup (Volume Snapshot) Integration Service is turned on for the child partition (see Figure 9-2).

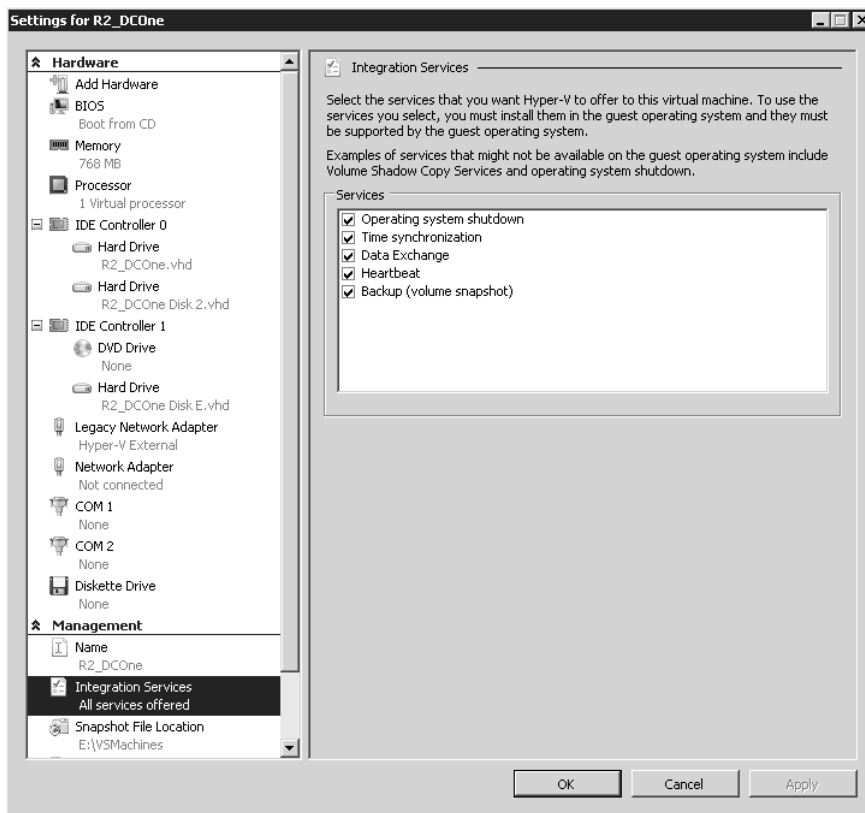


FIGURE 9-2 The Backup Integration service

If the machine is not enlightened, VSS cannot capture a snapshot of the VM's files, and the backup tool therefore saves the state of the VM and then takes a backup and restarts the VM when the backup is complete. Legacy VMs must be put into a saved state to create

data-consistent backups of the virtual hard disk contents. They are restored when the backup is complete. Obviously, this means that backups of legacy VMs must be done off-hours so that end users are not affected.

IMPORTANT VSS vs. HYPER-V SNAPSHOTS

Do not confuse Volume Shadow Copy Service snapshots with Hyper-V snapshots. When you take a Hyper-V snapshot, it automatically converts the VHD into a differencing disk and creates a parent-child relationship between the disks. Although this is a good way to retain a specific image of a VM, it is not a good way to perform VM backups. VSS snapshots, on the other hand, provide a disk image of the state of a VM and rely on this disk image to perform a backup. VSS snapshots are application-specific and maintain the consistency of a VM data during the backup operation.

You have some other ways to protect VMs, however. For example, you may already have been using Windows NTBackup to protect your physical machines before their conversion to Hyper-V VMs. These backups will not be compatible to Windows Server Backup if you upgrade the machines to Windows Server 2008. You can, however, download a version of NTBackup that works with Windows Server 2008. This ensures that your existing backups are still valid.

MORE INFO NT BACKUP

Download a Windows Server 2008-compatible version of NTBackup from Microsoft at <http://go.microsoft.com/fwlink/?LinkId=82917>.

Performing Internal VM Backups

You can also generate backups from within the VM itself. After all, VMs are nothing but a set of files, and to work with a backup, you only need to protect these files. However, you cannot protect the files if VM contents are in memory and not stored in the disk files. In this case, the best way to generate a backup is to use the following procedure:

1. Add a new dynamically expanding VHD to the VM. You use a dynamically expanding VHD to keep the file size as small as possible.
2. Format the new VHD in the VM.
3. Create a backup schedule inside the VM and use the new VHD as the backup target. Make sure your schedule is set to replace all backup contents on the target drive. This way each copy of the drive will contain only one backup set.
4. When the backup is complete, replicate the VHD containing the backup files to a new location in your network. If the location is offsite, you do not need to move the backups offsite manually. Use the RoboCopy.exe utility contained within the parent partition of Hyper-V hosts to perform this copy on a scheduled task. This creates a consistent backup of the VHD because the VHD is at rest as soon as

the backup is complete. Therefore, all contents are valid. The replication target can be a number of different locations:

- A local disk on the Hyper-V host server
 - A disk in a SAN
 - A local file share on your network
 - A remote file share on your network
 - A Windows SharePoint Services or Office SharePoint Server store
5. Use a schedule and target different folders for each day to maintain daily backups. For example, you could use the following schedule:
- Save the VHD once per day for an entire month. Retain for one month and then rotate the saved VHD copies.
 - Save one of the daily VHDs as a weekly backup for each week. Retain for six months and then rotate them.
 - Save one of the weekly VHDs as the monthly backup for each month. Retain for one year and then rotate them.
 - Save one of the monthly VHDs as the yearly backup for each year. Retain them for at least seven years or however long your compliance rules require it.
6. If restores are required, you can mount the backup VHDs using the VHDMount.exe utility, which can mount offline VHDs and let you view their contents. You can then use the original backup tool to restore contents from the backup within the VHD.

MORE INFO VHD MOUNT UTILITY

VHDMount.exe is part of the Microsoft Virtual Server 2005 R2 download and must be extracted from its content. Download Microsoft Virtual Server from <http://www.microsoft.com/windowsserversystem/virtualserver>. To install it, run the Virtual Server installation file and clear all of the components except for the VHD Mount tool.

Note that if the guest operating system is Windows Server 2008 and you use WSB to perform the backup, you do not need to use the VHD Mount utility. This also applies if you just want to restore contents from inside the VM using the original backup tool. Simply replace the VHD file that is attached to the VM with the appropriate copy of the replicated VHD and view the contents using the backup tool.

Using the Volume Shadow Copy Service on File Shares

Another way to protect VMs is through VSS itself. Each disk drive in Windows Server 2008 can protect the contents of shared folders through the use of VSS snapshots that are created on a schedule. Windows Server 2008 supports up to 512 snapshots before it needs to overwrite them. Another way to protect VMs is to rely on this shared folder snapshot process.

In Windows Server, each drive that is attached to a server is shared by default as Drive\$. This share is a hidden share—because of the attached \$ sign—but it is always generated automatically. This means that you do not need to create a share for the disks or folders that contain VM files because the share already exists. Then you can proceed as follows:

1. Ideally, you will be able to prepare the host server by adding an additional volume. This volume will be used to store all of its VSS snapshots. Because each snapshot is 300 MB in size and you want to store 512 of them, your volume should be about 180 GB in size. Double that if you need to protect two different data volumes.
2. Enable VSS for the data volume or the volume containing the VM files. VSC is a property of a disk volume in Windows Server. To enable it, open Windows Explorer, locate the data drive, right-click it, and select Configure Shadow Copies. Accept the User Account Control prompt if it appears.
3. Specify VSS settings. In the Shadow Copies dialog box, click the Settings button. In the Settings dialog box, use the drop-down list to select the new drive you added to store the snapshots (see Figure 9-3). Set the limit for the copy as appropriate. (The default should be fine.)

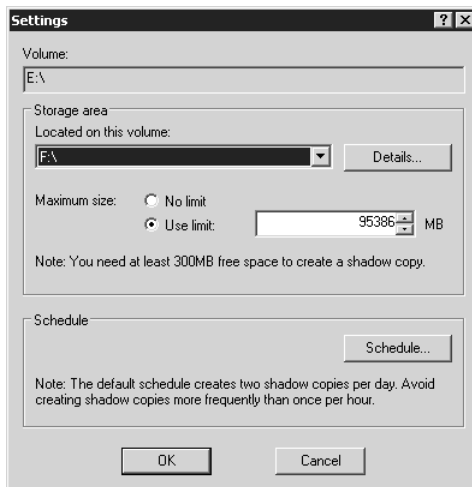


FIGURE 9-3 Configuring VSS settings for a drive

4. Change the schedule if required. Begin with the default schedule at first; you can always change it later. By default, snapshots are created at 7:00 A.M. and 12:00 P.M. every weekday. Click OK when done.
5. Make sure you select the data volume you want to protect and click Enable to turn on the VSS service for this volume. A warning will appear (see Figure 9-4). You can safely discard this warning because you just set the configuration for your snapshots. Click Yes.

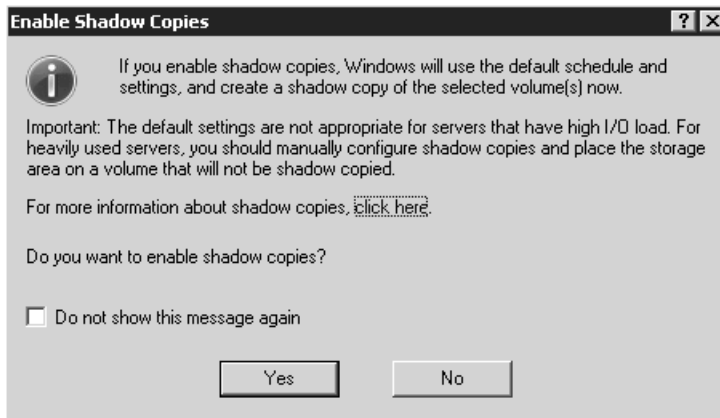


FIGURE 9-4 The VSS Enable Shadow Copies Warning

VSS will now automatically generate two snapshots per day for this volume. Repeat the operation for any other volume you want to protect.

In the event of a mishap, you can now rely on the Previous Versions client to restore lost files and folders or the files that make up a VM (see Figure 9-5). You can therefore rely on this tool to recover lost VMs on a Hyper-V host. The Previous Versions client is built in to Windows Vista and Windows Server 2008. It must be installed on older versions of Windows. It can be found in the %SystemRoot%\System32\Clients folder on Windows Server 2003 installations. The installation file is named TWCLI32.msi.

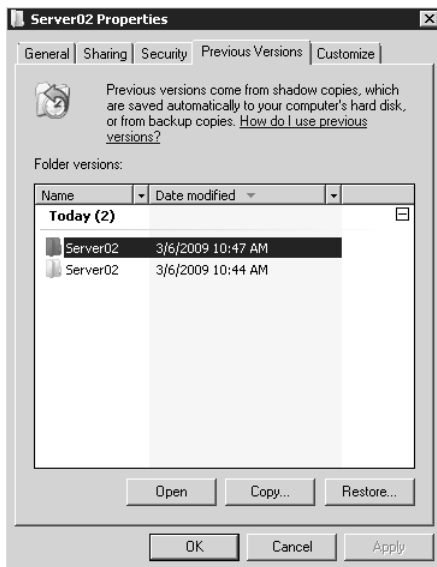


FIGURE 9-5 Restoring a previous version

Previous Versions is a feature of the properties of a file in Windows. Simply right-click the object (file or folder) and select Restore Previous Versions to recover the content you lost. This is a powerful feature of this operating system and one that Hyper-V simply inherits because it runs on top of the operating system.

You can open, copy, or restore the contents of a snapshot. This lets you restore any component of a virtual machine. In a way, this provides the same feature as the Hyper-V snapshot utility, but it provides you with 512 snapshots instead of 50 and it does not turn the VHD into a differencing disk.

IMPORTANT RESTORING VMs FROM PREVIOUS VERSIONS

Be very careful when you use Previous Versions to restore virtual machine files. Ideally, you will use this for data disks only. You can use it to restore an entire virtual machine, but do this with care. Production VMs and VMs running complex, time-based processes such as domain controllers are not good candidates for Previous Versions restores. Machines that contain all services in one VM, such as Windows Small Business Server, can be restored with this method because everything is contained in one computer. This method is very useful for test and development environments, but should be used with care on production VMs.

MORE INFO WORKING WITH SHADOW COPIES

You can manage shadow copies or VSS snapshots from the command line. To do so, you must use the DiskShadow.exe command. Find out more about this command at <http://technet.microsoft.com/en-us/library/cc772172.aspx>.

Working with Windows Server Backup

Windows Server Backup (WSB) is a feature included in Windows Server 2008. It provides a basic backup and recovery solution for computers running the Windows Server 2008 operating system. WSB replaces the previous version of Windows Backup (NTBackup.exe), which was found in all versions of Windows Server prior to 2008.

WSB is composed of a series of different components:

- A Microsoft Management Console (MMC) snap-in that is available as a standalone console (WBAdmin.msc), as a portion of Server Manager under the Storage node, or as a snap-in that you can add to a custom console. This console is only available on full installations.
- A command-line tool (WBAdmin.exe) that can be used on both the full and the Server Core installations.

MORE INFO WBAdmin.exe REFERENCE

For more information on WBAdmin.exe, go to <http://technet.microsoft.com/en-us/library/cc754015.aspx>.

- A series of Windows PowerShell cmdlets that are added by including the Windows PowerShell snap-in named Windows.ServerBackup. These cmdlets can run on the full installation or perform remote operations on Server Core installations. Remember, however, that you must enable the proper ports on Windows Firewall to support remote operations on Server Core installations.

With each method, you must be a member of the local administrators group or a member of the Backup Operators group to use any of these tools. Like all Windows Server 2008 features, WSB is not installed by default. It must be added as a feature. When you do so, you will be prompted to add two sub-features:

- Windows Server Backup, which adds the console and the WBAAdmin.exe command-line tool.
- Command-Line Tools, which add the Windows PowerShell cmdlets that support Windows Server Backup. This option also requires Windows PowerShell and the Microsoft .NET Framework.

WSB is designed to perform a variety of tasks. Those who have not seen WSB and are used to NT Backup will find that the WSB console is completely different, as is the WSB feature set. For example, you can use WSB to back up the following:

- A full server, including all of the volumes tied to the server. This supports the recovery of an entire server.
- Critical volumes or volumes that contain operating system files. This supports the recovery of the operating system itself or only the system state if required.
- Selected data volumes on the server. This supports the recovery of files, applications, or data from a given volume. For WSB, Hyper-V virtual machines are applications because Hyper-V uses a Volume Shadow Copy Service writer to perform the backup.

Note, however, that WSB does not support the backup of individual files or folders; it only backs up entire volumes—and only volumes that are formatted with NTFS. All other volumes are ignored.

It is also important to understand the backup targets you can use with WSB. Table 9-1 outlines the various targets you can use with WSB.

TABLE 9-1 Potential WSB Backup Targets

TARGET	COMMENT
Shared folder	You can back up to a shared folder, but each folder can only contain a single backup image. If you back up to the same folder each time, the previous backup will be overwritten. If the backup fails, you can be left without a backup. To avoid this issue, create a series of subfolders in the shared folder location and configure each backup to target a different subfolder. Subfolder names can reflect backup contents—for example, Monday, Tuesday, Wednesday, and so on. Note that you cannot schedule backups to shared folders.

TARGET	COMMENT
Optical media or removable media	You can back up to removable media, but if you do, you will only be able to recover entire volumes. Note that the backup will not work if the target media has less than 1 GB of free space. Note: You cannot schedule backups to optical or removable media.
Internal hard disk	You can back up to an internal hard disk. When you do so, you will be able to recover files, folders, applications, and volumes. If the backup includes critical volumes, you will also be able to recover the operating system or the system state. However, the volume must use separate spindles if you want to be able to back up the operating system. In addition, the backup volume will be reformatted by WSB, will be entirely dedicated to backup, and will not be visible in Windows Explorer. Note that you can schedule backups to internal disks.
External hard disk	You can back up to an external hard disk. When you do so, you will be able to recover files, folders, applications, and volumes. If the backup includes critical volumes, you will also be able to recover the operating system or the system state. Using an external hard disk will let you more easily move the backup offsite. Once again, the backup volume will be reformatted by WSB, will be entirely dedicated to backup, and will not be visible in Windows Explorer. Note that you can schedule backups to external disks.

Keep in mind that if the volume you are backing up is using BitLocker Full Drive Encryption, the backup will not be encrypted unless you also encrypt the target disk. In addition, WSB will not be able to back up volumes that are larger than 2,043 GB. However, after a volume is used as a backup target, you no longer need to worry about it running out of space because WSB automatically manages space on the volume from that point on.



EXAM TIP WSB BACKUP TARGETS

Remember that WSB no longer supports tape drives as a backup media. Don't get caught by this during the exam.

IMPORTANT EXTERNAL DISK TARGETS

If you used device control Group Policy Objects in your security strategy for the resource pool, you will not be able to use USB-based external hard disks as backup targets. If you want to use WSB for backup, you must enable the particular disk type in the device control GPO. Keep in mind that third-party backup tools do not have the same limitations as WSB.

MORE INFO WINDOWS SERVER BACKUP

For more information on Windows Server Backup, go to <http://technet.microsoft.com/en-us/library/cc770266.aspx>.

Understanding WSB PowerShell Cmdlets

Windows Server Backup includes two command-line tools for performing backups. The first is strictly a command-line tool: WBAdmin.exe. The second is a set of Windows PowerShell cmdlets that lets you control and script backup operations. Table 9-2 lists the different Windows PowerShell cmdlets available for WSB operations. You can view additional information about these cmdlets if you run the following two cmdlets in your Windows PowerShell command window:

```
Add-PSSnapin Windows.ServerBackup
Get-Command -PSSnapin Windows.ServerBackup | Get-Help -Full
```

The first cmdlet loads the Windows Server Backup PowerShell snap-in and the second cmdlet obtains help from the contents of the snap-in.

TABLE 9-2 WSB PowerShell Cmdlets

CMDLET	DESCRIPTION
<i>Add-WBBackupTarget</i>	Adds a backup target to the backup policy
<i>Add-WBVolume</i>	Adds a volume to the backup policy
<i>Get-WBBackupTarget</i>	Gets backup targets from a policy
<i>Get-WBDisk</i>	Gets all disks
<i>Get-WBPolicy</i>	Gets current backup policy
<i>Get-WBSchedule</i>	Gets backup schedule in policy
<i>Get-WBSummary</i>	Gets backup history and summary
<i>Get-WBVolume</i>	Gets all volumes
<i>New-WBBackupTarget</i>	Creates a new backup target
<i>New-WBPolicy</i>	Creates a new empty policy
<i>Remove-WBBackupTarget</i>	Removes a backup target from the policy
<i>Remove-WBPolicy</i>	Deletes the backup policy
<i>Remove-WBVolume</i>	Removes a volume from the policy
<i>Set-WBPolicy</i>	Saves the <i>WBPolicy</i> object to create a scheduled backup
<i>Set-WBSchedule</i>	Sets the schedule to the backup policy

You can use these cmdlets with the instructions in Chapter 7, “Automating VM Management with Windows PowerShell,” to create your own scripts for generating backups.

Protecting Hyper-V and VMs with Windows Server Backup

To back up host servers running Hyper-V parent partitions, you must begin by installing the Windows Server Backup tool. Perform the installation from Server Manager.

1. Open Server Manager, right-click Features in the Tree pane, and then click Add Features.
2. Scroll down and then expand Windows Server Backup Features. Select Windows Server Backup And Command-line Tools. Choose the Command-line Tools only if you intend to use Windows PowerShell to script backups. If you do, a dialog box will appear, asking you to install Windows PowerShell as a requirement if it is not already installed on the computer. This also happens for the .NET Framework if it is not already installed. Click Add Required Features and then click Next.

NOTE INSTALLING WINDOWS SERVER BACKUP

If you only select Windows Server Backup Features without expanding it, the installation only includes the WSB snap-in and the WBAdmin command-line tool—the Windows PowerShell cmdlets will not be installed.

3. Click Install to start the installation and click Close when complete.

Now that the installation is complete, you must add the Hyper-V Volume Shadow Copy Service snapshot writer to the registry. WSB can work with any number of VSS writers, but it cannot install them. Therefore, the Hyper-V VSS writer is not installed when you add WSB to a machine running Hyper-V.

1. Begin by identifying the globally unique identifier (GUID) for the Hyper-V VSS writer. Open an elevated command prompt. Right-click the Command Prompt shortcut on the Start menu and then click Run As Administrator. Accept all UAC prompts.

2. Type the following command to locate the GUID:

```
vssadmin list writers >writerslist.txt
```

3. This lists the available writers and stores the data into the writerslist.txt file. Open it in Notepad. Use the following command:

```
notepad writerslist.txt
```

4. Locate the GUID for the Hyper-V VSS writer in the writerslist.txt file (see Figure 9-6). Select the text, right-click it, and choose Copy. The copied data will be used in the next step.

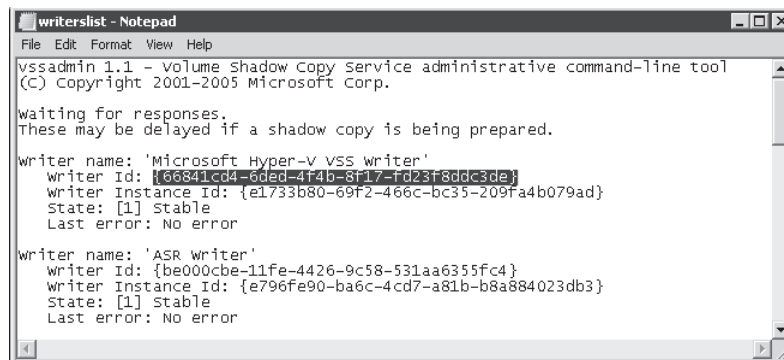


FIGURE 9-6 Locating the Hyper-V VSS writer GUID

5. Start the Registry Editor to add the Hyper-V writer to WSB:

```
regedit
```

IMPORTANT EDITING THE REGISTRY

Be very careful as you proceed through the next steps. Wrongly configuring the Windows Registry can result in a non-working server.

6. Navigate to HKey_Local_Machine\Software\Microsoft\Windows NT\CurrentVersion. If a sub-key named WindowsServerBackup exists, click it. If not, right-click CurrentVersion, select New, and then select Key. Type **WindowsServerBackup** and press Enter. This creates the Windows Server Backup branch.
7. Create a sub-key under WindowsServerBackup called Application Support. Right-click WindowsServerBackup, select New, and then select Key. Type **Application Support** and press Enter. This creates the sub-key.
8. Create a third sub-key with the Hyper-V GUID. Right-click Application Support, select New, and then select Key. Paste the GUID, including the brackets ({}).
9. Add a new string value to the Hyper-V GUID key. Right-click the key, choose New, and then choose String Value. Name the value **Application Identifier** and press Enter. Right-click the Application Identifier value and choose Modify. Type **Hyper-V VSS Writer** and click OK. The result should be a new entry for WSB (see Figure 9-7). WSB will read this key next time you perform a backup and will be able to use the Hyper-V VSS writer during the backup.

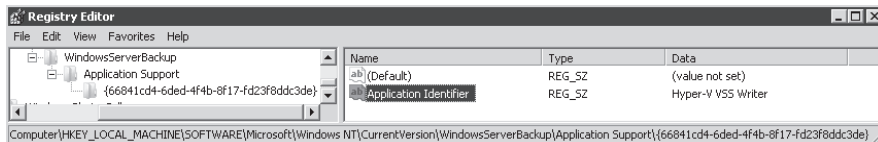


FIGURE 9-7 Adding the Hyper-V VSS Writer value to the registry

10. Now export this value so that you can update other servers to use the Hyper-V VSS writer. Right-click WindowsServerBackup in the Tree pane and choose Export. Name the file **Hyper-VWriter.reg** and click Save. This exports the branch you just created (see Figure 9-8). You can import it into any other computer simply by typing the following command in an elevated command prompt. It will prompt a warning. Click Yes to proceed and then click OK after the update has been added.

```
start hyper-vwriter.reg
```

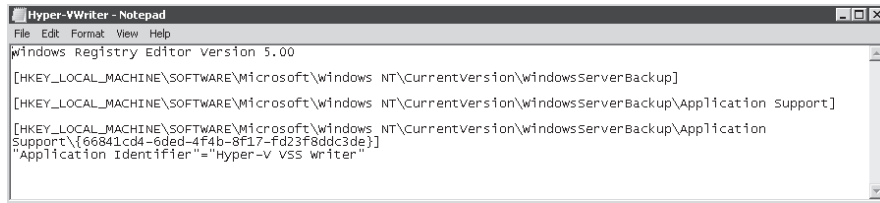


FIGURE 9-8 The contents of the Hyper-VWriter.reg file

Your server is now ready to run WSB backups. Make sure you import the registry file on all other servers to enable support for the Hyper-V VSS writer. As with all imported registry information, you will get a security warning when importing the .reg file. Click Yes to complete the import (see Figure 9-9).

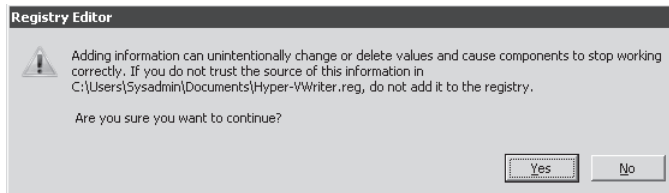


FIGURE 9-9 Adding the contents of the Hyper-VWriter.reg file to another computer

UPDATE ALERT POTENTIAL ISSUES WITH HYPER-V BACKUPS

You can run into potential issues when you use WSB to back up Hyper-V computers. For example, one known issue is that when you try to back up a machine whose configuration is missing—for example, it was located on a network share that is no longer available—WSB will fail to back up any VM on the server. Microsoft has issued an update to correct this. Find it at <http://support.microsoft.com/kb/956697>. A second update will help resolve issues regarding the number of volumes on a host and potential unstable states when performing backups. Get it from <http://support.microsoft.com/kb/959962>. A third update will deal with potential stop errors when performing Hyper-V VM backups. Find it at <http://support.microsoft.com/kb/960038>. The first update may already be on your servers; it is unlikely that the last two are. You can verify the updates through the server's update history. If you do not have them already, obtain them and install them on each host.

Now that your servers are ready, you can back them up using WSB. Make sure you have an additional external disk connected to your host server. Do not worry about cleaning the disk because WSB will reformat it and empty all contents. Proceed as follows:

1. Launch Windows Server Backup. In Server Manager, click the Storage node in the Tree pane and choose Windows Server Backup.

NOTE REMOTE BACKUPS

Windows Server Backup is included in the Remote Server Administration Tools (RSAT) and can be used on any Windows Server 2008 full installation or on a Windows Vista computer.

2. Because this is your first backup, use the Backup Once option. Click Backup Once in the Actions pane.
3. You must select Different Options because no other backup has been taken before. Click Next.
4. You can choose Full Server or Custom. The only difference between the two is the ability to select which volumes are included in the backup. Choose Custom to view the available volumes. Click Next.
5. Select the volumes to back up. Note that the system volume is already selected because the Enable System Recovery option is selected by default. Add the data disk or the disk storing VMs (see Figure 9-10). Click Next.

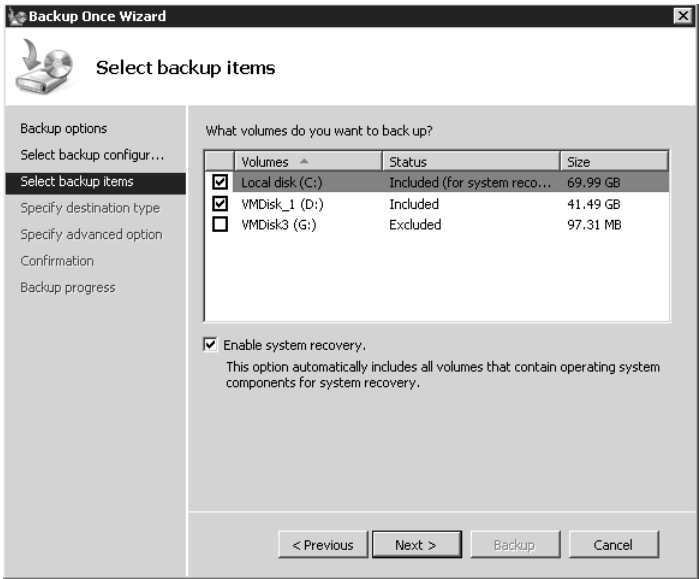


FIGURE 9-10 Selecting volumes to back up

6. Choose the location of your backup. Because you will be storing it on a local disk, leave the default and click Next. Note that when you perform a manual backup you can target a shared folder.
7. Select the backup destination by choosing your target disk from the drop-down list. Click Next.
8. Choose the mode to use for VSS. If you choose VSS Copy Backup, the backup will not truncate application log files during the backup. Use this mode if you run backups with another tool such as System Center Data Protection Manager (SCDPM) that requires these files along with WSB. Because your application is Hyper-V, choose VSS Full Backup. This will use the VSS writer you enabled earlier in the registry. Click Next.
9. Review the confirmation data and click Backup. The backup begins (see Figure 9-11).

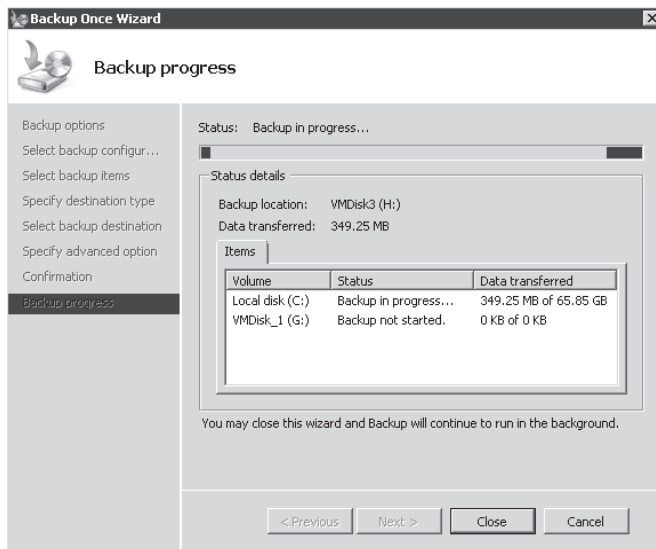


FIGURE 9-11 Running a WSB backup

- 10.** Click Close when the backup is complete. A new backup will be listed in the WSB Details pane.

You can also use the WSB console to schedule backups. Use the preceding procedure, but click Backup Schedule in the Actions pane. The major difference in the settings of this wizard is the ability to add a schedule to the backup (see Figure 9-12); you also have to label the target disk. When you do so, a new job is created in the Windows Task Scheduler. This job will run based on the schedule you created.

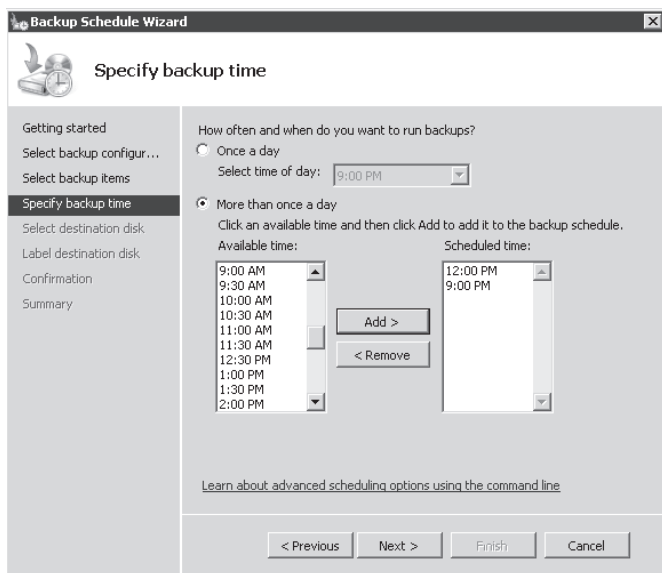


FIGURE 9-12 Scheduling a WSB backup

Note that while the backup is running, enlightened guest operating systems continue to run, but legacy VMs are put in a saved state for the duration of the backup.

You can also create a backup schedule with the command line. First identify the Disk ID for each disk, and then create the backup schedule. The following example performs a full system backup including critical disks and data disks (in this case the D: drive) twice a day at 9:00 A.M. and 6:00 P.M. to a disk partition:

```
wbadmin get disks
```

```
wbadmin enable backup -addtarget:DiskID -schedule:09:00,18:00 -allcritical -include:d:
```

IMPORTANT MANAGING BACKUP SCHEDULES

You must be a member of the local administrators group to create or modify backup schedules. Members of the Backup Operators group do not have this right.

Although you can't use WSB on Server Core installations, you can run it remotely to back up a Server Core installation. Simply choose Connect To Another Computer in the Actions pane. Note that you must use the WSB standalone console for this because this command is not available in the Server Manager WSB node.

Remember that you can also use Windows PowerShell to create these backup schedules.



EXAM TIP USING WSB

Make sure you spend time with WSB and Hyper-V hosts because they are an important part of the exam. Also make a point of noting the target disk types and the access rights required to work with WSB.

Restoring Systems with Windows Server Backup

When issues arise, you can rely on the WSB backups you performed to recover several different elements:

- **Full computer** If your host server is damaged and can no longer operate even if you have tried the other recovery methods mentioned at the beginning of this lesson, you can perform a recovery of a full computer. You rely on WinRE to perform this restore. WinRE is available from three potential sources:
 - **Installed locally** If you prepared your server with a WinRE partition, it will be available locally.
 - **On a custom disk** If you prepared a custom Windows PE disk with WinRE, you can rely on this disk to boot into WinRE to perform the restore.
 - **On the Windows Server Installation media** If all else fails, rely on the Windows Server 2008 installation media to boot into WinRE. Boot with the media and choose your language and keyboard. Then, instead of clicking Install Now, choose Repair Your Computer and then click Next. Choose the Windows Complete PC Restore to restore an entire server or choose Command Prompt to use WBAdmin.exe to restore only portions of the backup (see Figure 9-13).

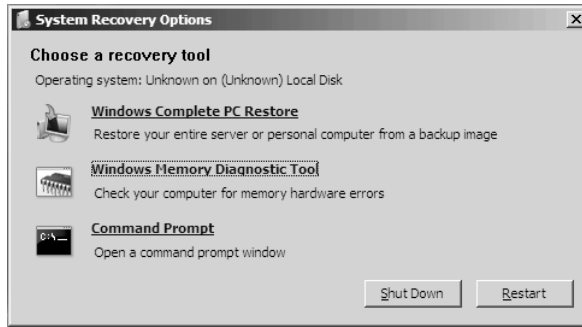


FIGURE 9-13 Using WinRE

- **Application** If you want to restore a single VM on Hyper-V, you must use an application restore. As far as WSB is concerned, virtual machines are Hyper-V applications.
- **Files and folders** If you want to restore single files or folders, you can choose a files and folders restore.
- **Volumes** If you want to restore an entire volume, you can choose a volume restore.

To restore either an application, data, or a volume, use the Recover command in the Actions pane of the WSB console and then follow these instructions:

1. Choose This Server and click Next.
2. Choose the date of the backup to restore (see Figure 9-14). Click Next.

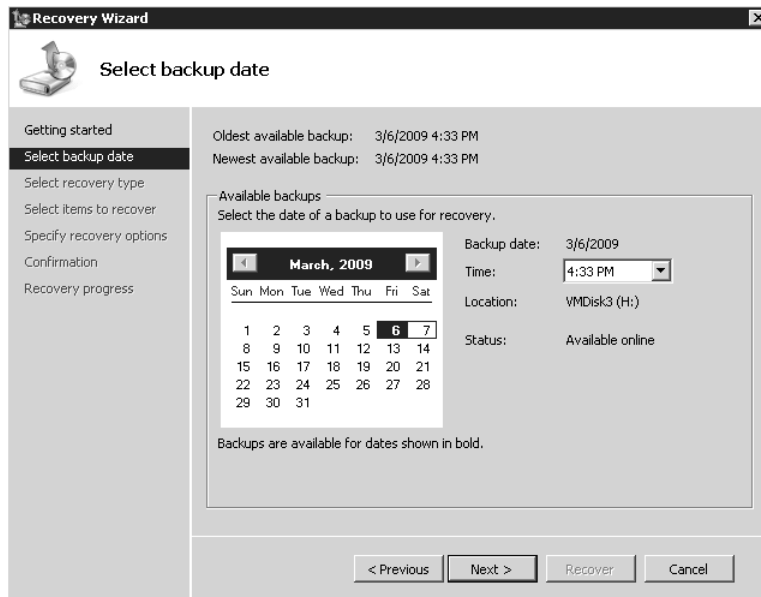


FIGURE 9-14 Choosing a recovery backup date

3. Choose the type of restore you need. For example, to recover a VM, choose Applications and then click Next.

4. WSB lists the available applications. This is a host server, so it lists Hyper-V VSS Writer (see Figure 9-15) because you made the registry changes earlier. You can click View Details to view the different applications the backup contains. Note that the VMs are listed by GUID and not by name (see Figure 9-16). Although you can click the VM GUIDs, you cannot choose the VM to recover. Also note that the backup includes the InitialStore.xml authorization store. Click OK and then Next.

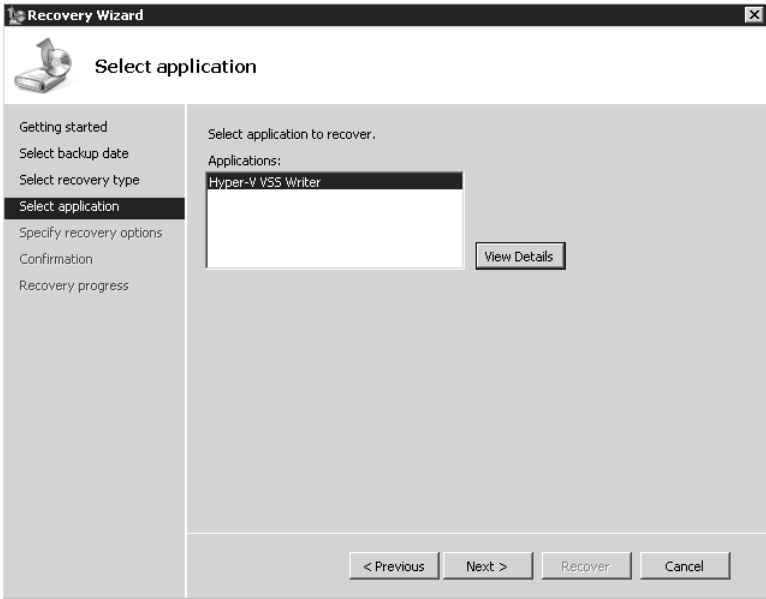


FIGURE 9-15 Choosing the application to recover from

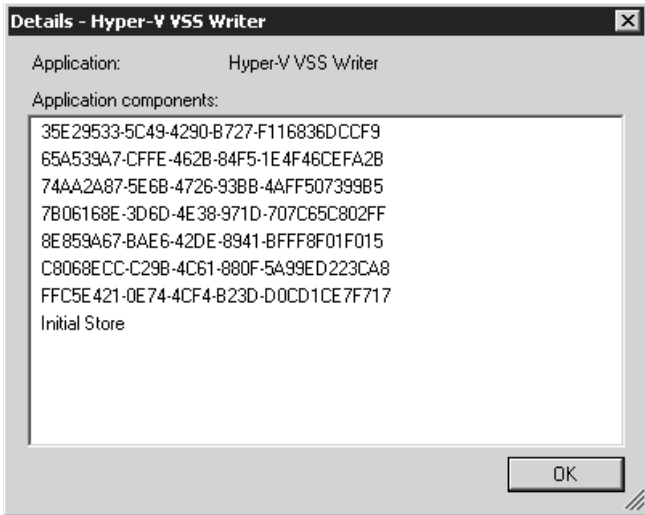


FIGURE 9-16 Viewing application contents

5. Choose where to recover the information. If you choose Recover To Original Location, both the application and the data will be recovered. If you choose Recover To Another Location, only the application data—in this case, the VM files—will be recovered. Make the selection based on your requirements and click Next. For example, if you want to restore all VMs to the state of a given date, choose the original location. If you want to recover files from within one of the VMs, choose another location, restore the VMs, and then mount the VM you want to recover data from on another server to recover the data.

IMPORTANT RECOVERY TO ORIGINAL LOCATION

Be very careful with the Recovery To Original Location option because it will replace all of the VMs on a server. This may break working VMs.

6. Confirm your options and click Recover.
7. Monitor the recovery operation and click Close when it is complete.

Alternatively, you can use a file-based restore. This option lets you choose which files to restore on a folder, then on a file basis (see Figure 9-17). In addition, you do not have to rely on the VM's GUID to identify which VM to restore because the VM's folder names are listed.

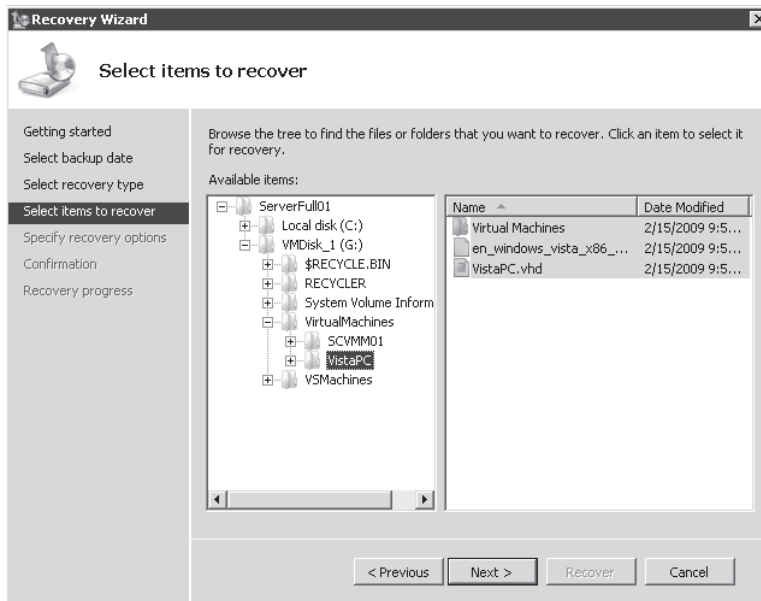


FIGURE 9-17 Choosing to restore an individual VM

Note, however, that when you choose to recover a VM as a set of files, this does not enable the VM in Hyper-V on the server you restore it to. To launch the VM, you have two options:

- **Create A New VM Configuration File** Create a new VM in Hyper-V using the New Virtual Machine command and link it to the VHDs you recovered. This is an excellent time to use the internal virtual network adapter because it isolates the VM from the public network—no conflicts with a running VM of the same name—and it lets you recover files because the host server can communicate with the VM.
- **Use The VHD Mount Utility** Recover only the VHDs you need and mount them as disk drives on a server to recover individual files from them.

As you can see, when you restore using the Application mode, the restore is all or nothing: You must restore all of the VMs as a whole as well as the initial authentication store. Be very careful how you use this option.

IMPORTANT APPLICATION RECOVERY

Be very careful with the Application Recovery To Original Location option because it not only replaces all of the VMs on a server, but it also restores the InitialStore.xml file on the host server. If you have made modifications to this file on the server after you have taken a backup and you restore a backup from an older date, you will lose all of your changes and may lock yourself out of the server.



EXAM TIP WSB RECOVERY

Remember the limitations in the recovery options of WSB. They will definitely be part of the exam.

Working with System Center Data Protection Manager

With System Center Data Protection Manager, Microsoft offers a streaming backup engine that captures remote VSS images and stores them centrally, allowing administrators to centrally manage all snapshots. The user's Previous Versions clients are automatically redirected to the central VSS repository instead of on each server. This makes it simpler to support users working with Previous Versions. DPM streams all backups to a central disk system and can then store them on tape for offline storage.

SCDPM provides backup services for several technologies:

- Active Directory Domain Services
- File servers
- SQL Server, including servers running mirrored databases
- Windows SharePoint Services and Office SharePoint Server
- Exchange Server, including servers running Standby Continuous Replication
- Microsoft Virtual Server virtual machines

- Hyper-V virtual machines
- Hyper-V host servers
- Virtual Server host servers

In addition, SCDPM lets you provide protection for several different types of information:

- File and folder data from volumes, network shares, or local storage
- Application-specific data
- Workstation-based data for Windows XP SP2 and Windows Vista
- Clustered servers
- System state data for both file and application servers

To protect Hyper-V, however, you must run SCDPM 2007 with Service Pack 1. The original version of SCDPM does not include support for Hyper-V.

SCDPM is a single-function product and must run on a dedicated server. In small organizations, you simply link the SCDPM server to a file-based store and, if required, to a tape library. Backups are stored on the file-based store and can then be moved to tape. In large organizations, you may need to include secondary SCDPM servers that will chain backups to a central repository managed by a main SCDPM server.

In resource pools, SCDPM should be hosted within the utility domain. In this case, SCDPM should be hosted on a dedicated virtual machine and can be linked to a storage pool on pass-through disks stored in a SAN, LUN, or on removable disks. If you run SCDPM on a VM, you limit yourself to disk-based backups. These disks can be duplicated offsite to provide further protection. This is the standard SCDPM configuration in the resource pool (see Figure 9-18).

If you want to include a tape library to protect the resource pool, you must install SCDPM on a dedicated physical server because Hyper-V does not support the integration of tape drives with virtual machines. In this case, the tape library will provide support for offsite data removal. Note, however, that it is entirely possible to use disk-only backups with SCDPM and Hyper-V resource pools.

MORE INFO SCDPM 2007 SP1

More information is available on SCDPM on the Microsoft Web site. General information on the product is available at <http://www.microsoft.com/systemcenter/dataprotectionmanager/en-us/default.aspx>. Technical information on the original release of SCDPM is available at <http://technet.microsoft.com/en-us/library/bb795539.aspx>. And information related to SCDPM 2007 SP1 is available at <http://technet.microsoft.com/en-us/library/dd363572.aspx>.

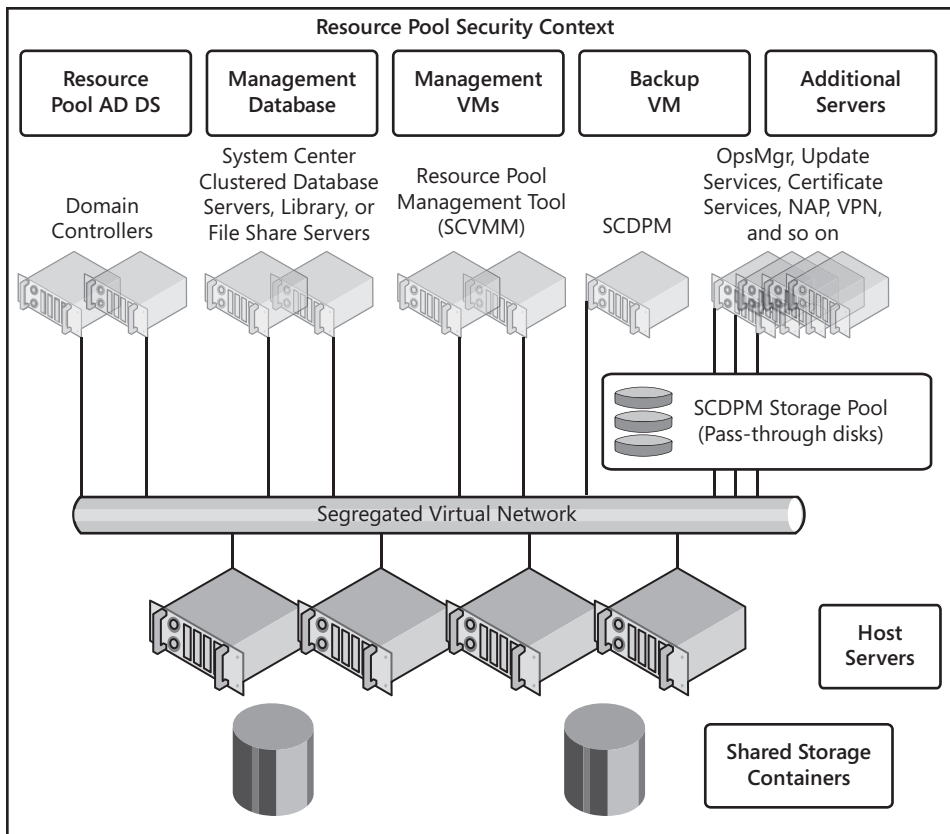


FIGURE 9-18 The SCDPM resource pool architecture

Requirements for SCDPM Protection

SCDPM requires several components to run properly. Table 9-3 outlines these requirements.

TABLE 9-3 Microsoft SCDPM Requirements

REQUIREMENT	DESCRIPTION
DPM Server	Cannot be the Management server for OpsMgr. Must be a dedicated server and cannot be a domain controller or application server. Cannot be a server with Failover Cluster services enabled. Only supports x86 and x64 operating systems; does not support for IA64. If you have more than 10 terabytes of data, DPM must run on an x64 operating system.

REQUIREMENT	DESCRIPTION
Operating system	Windows Server 2003 with SP2 or later. Windows Server 2003 R2 with SP2 Standard or Enterprise editions. Windows Server 2008 Standard or Enterprise editions. Windows Storage Server 2003 with SP2 or later Standard, Enterprise, or Express editions. Windows Storage Server 2003 R2 with SP2.
Software	■ Windows PowerShell 1.0 and the Microsoft .NET Framework 2.0 ■ Internet Information Services (IIS) 7.0: DPM needs all the components. ■ Microsoft SQL Server 2005 with SP2. Workstation components: can use an existing remote instance but must run a special preparation file on the SQL Server (SQLPrep.msi). In addition, the SQL Server service and SQL Server Agent service accounts need read and execute permissions to the SQL Server installation location. Microsoft SQL Server 2005 SP2 with Reporting Services if not installed on the remote instance. Note that DPM 2007 does not support using SQL Server 2008. In addition, the remote instance of SQL Server cannot be on a domain controller. The installation files include the SQL Server 2005 SP2 Standard edition setup files. ■ Windows Deployment Services ■ Single Instance Storage on Windows Server 2008, to install: start a command prompt and type start /wait ocsetup.exe SIS-Limited /quiet /norestart
Networking	The SCDPM server must have persistent network connections with all of the computers—servers and workstations—it protects. If you are protecting data over a WAN, you need a minimum of 512 Kbps of network bandwidth. SCDPM must be deployed within an AD DS domain. SCDPM will not protect computers across domains. If you are running multiple domains, even in a single forest, you must install an SCDPM server for each domain.
Protected computers	Volumes must be formatted with NTFS. Volume must be at least 1 GB in size. Servers running Windows Server 2003 must include the VSS update rollup package (see http://support.microsoft.com/kb/940349).

REQUIREMENT	DESCRIPTION
	Note: After installing the update, restart the machine and refresh the agent in the DPM Administration console. Note: If you install protection agents on Windows Vista or Windows Server 2008, you do not need the update.
Security	To install DPM you need to be a domain user in the local administrators group. To use the DPM Administrator Console, you need to be a domain user with local administrator access.
Disk	One dynamic disk is dedicated to the storage pool. Note: You cannot install DPM on this disk. One disk is dedicated to system files, DPM installation files, DPM prerequisite software, and DPM database files.
Memory	Minimum: 2 GB. Recommended: 4 GB.
Pagefile	0.2 percent the size of all recovery point volumes combined, plus 1.5 times the amount of RAM on the computer.
Disk space	Program files drive: minimum: 620 MB. Recommended: 2 to 3 GB. Database files drive: minimum: 900 MB. System drive: minimum: 2,650 MB. Note: DPM requires 300 MB of free space on each protected volume for the change journal, plus before archiving data to tape, DPM copies the file catalog to a DPM temporary installation location. You should have 2 to 3 GB of free space for this folder.
Disk space for storage pool	Minimum: 1.5 times the size of the protected data. Recommended: 2 to 3 times the size of the protected data.
Logical unit number (LUN)	Recommended: Maximum of 17 terabytes for GUID partition table dynamic disks. Recommended: 2 terabytes for master boot record disks which is the maximum for this disk type.

MORE INFO SCDPM REQUIREMENTS

For information on SCDPM requirements, go to <http://technet.microsoft.com/en-us/library/bb808894.aspx>.

In addition, Hyper-V host servers also require additional components to support SCDPM as a backup engine. Table 9-4 outlines these requirements.

TABLE 9-4 Hyper-V SCDPM Host Requirements

REQUIREMENT	DESCRIPTION
Update number KB951308	This update is required for clustered hosts. This update enhances the user experience in the Failover Clustering Management console. This update is recommended for host clusters and was described in Chapter 3. This update is required to have host clusters work with SCDPM. Find it at http://support.microsoft.com/kb/951308 .
Update number KB959962	This update is required for all Hyper-V hosts. This update fixes issues with the Hyper-V VSS writer and is necessary for SCDPM to work with Hyper-V. This update was mentioned earlier in the chapter, in the section “Working with Windows Server Backup.”
Update number KB960038	This update is required for all Hyper-V hosts. This update fixes potential stop errors with the Hyper-V VSS writer and is necessary for SCDPM to work with Hyper-V. This update was also mentioned earlier in the chapter, in the section “Working with Windows Server Backup.” Make sure you choose the Windows Vista x64 version of this update.
Updated Integration Services	To properly run SCDPM backups of virtual machines running enlightened guest operating systems, you must ensure that they are using the latest version of Integration Services. The appropriate version should be at least 6.0.6001.18016. You can verify this in Device Manager, under System Devices by viewing the Hyper-V Volume Shadow Copy device’s properties on the Driver tab (see Figure 9-19).

**FIGURE 9-19** Viewing the Integration Services version in a VM

MORE INFO HYPER-V REQUIREMENTS FOR SCDPM

For information on Hyper-V requirements for SCDPM, go to <http://technet.microsoft.com/en-us/library/dd347840.aspx>.

Preparing SQL Server for SCDPM

In the resource pool, you should be running a dedicated SQL Server installation for System Center products if you are running more than one System Center product. For example, if you are running SCVMM along with PRO, you will also be running System Center Operations Manager. In this case, you should be using a dedicated installation of SQL Server.

If this is the case, you should store the SCDPM database on this server as well. Some key requirements must be met by this installation to also support SCDPM:

- SQL Server cannot be installed on a domain controller. This should not be the case in the resource pool.
- SQL Server and SCDPM Server must be located in the same domain. This is the case in your utility forest.
- SCDPM Setup creates the `DPMDDBReaders$<SCDPM server name>` and `DPMDDBAdministrators$<SCDPM server name>` local groups on the remote instance of SQL Server. SCDPM administrators must be added to these groups to use the remote instance of SQL Server.
- The remote instance of SQL Server must be running IIS and SQL Server 2005 Standard or Enterprise edition with SP2, including the SQL Server Database Engine and Reporting services components. Add components if any are missing.
- In addition, you must prepare a new instance of SQL Server on the SQL Server computer to run SCDPM. Name the instance **SCDPM**.

IMPORTANT SQL SERVER 2008 AND SCDPM

SCDPM will not work with SQL Server 2008 installations. SQL Server installations must be running SQL Server 2005.

When you choose to use an existing instance of SQL Server instead of installing it from the SCDPM product DVD, the SQL Server Settings page appears during setup. You then need to identify the name of the new instance you created for SCDPM and enter appropriate administrator credentials to allow the SCDPM installation process to connect to this instance.

Installing SCDPM

Before installing SCDPM, prepare the machine that will host this service. You can use a virtual machine if you configure it properly. Ideally, because SCDPM operation is so disk-intensive, you would use pass-through disks for the storage pool. If you use a virtual machine, create a new VM based on Windows Server 2008, assign a minimum of 2 GB of RAM to the VM and

create a VHD for the operating system, and then assign a pass-through disk for the storage pool. Join the VM to the domain and make sure it includes all updates. This VM should not be running any other service.

When the VM is ready, proceed as follows:

1. Log on with a domain user account that is a member of the local administrators group.
2. Type the following command to enable basic single instance store (SIS) capabilities on the server. SIS will automatically deduplicate the contents you back up from multiple servers. For example, if you have multiple copies of cmd.exe backed up from multiple Windows Server 2008 computers, SIS will store only one copy with a reference to each machine. This can save enormous amounts of space during backups. Reboot the server after the command is enabled.

```
start /w ocsetup SIS-Limited /quiet /norestart
```

3. Log on again once the computer has been restarted and then insert the DPM product DVD in the DVD-ROM drive and start the installation. On a VM, you can link the VM's DVD drive to the SCDPM ISO file or insert the SCDPM DVD into the host server's physical DVD drive and link the VM to this drive. Launch the AutoPlay program.
4. On the Microsoft System Center Data Protection Manager 2007 screen, click Install Data Protection Manager.
5. Accept the license terms and then click OK.
6. Click Next on the Welcome page. DPM begins a prerequisites check for all required hardware and software. Everything should pass. Click Next. Repair anything the prerequisite check identifies as an issue if it comes up.
7. Enter your registration information and click Next.
8. Accept the default folder to install DPM. In the SQL Server settings section, specify whether you want to install the MS\$DPM2007\$ instance of Microsoft SQL Server. If you are running a small installation, you can have SCDPM install SQL Server Express 2005 on this computer. If you are running larger installations, select to run SCDPM from a separate SQL Server. For example, in your resource pool, you can have SCDPM share the SQL Server instance running in support of all System Center products. In this case, use the default SQL Server instance installation. Click Next.
9. SCDPM creates two local accounts during the installation. The MICROSOFT\$DPM\$Acct account is used to run SQL Server and the SQL Server Agent service. The DPMR\$<computer name> is used to securely generate reports. Both accounts are set to use the same password. This password is set not to expire by default. Use a strong password, confirm it, and then click Next.
10. Determine whether you want to opt in to the Microsoft Update service. Use the service if you do not have an internal update service installation and then click Next. Determine whether you want to opt in to the Customer Experience Improvement Program and then click Next. Review your installation summary and click Install. Click Close when the installation is complete. Restart the computer.

This restart is necessary to load the volume filter that SCDPM uses to track and transfer block-level changes between SCDPM and the computers it protects, or between the primary and secondary SCDPM servers.

Now update the installation to SCDPM Service Pack 1. Note that the Service Pack 1 installation cannot be removed. To remove it, you must remove SCDPM as a whole. However, this update is necessary to run SCDPM with Hyper-V.

MORE INFO SCDPM SERVICE PACK 1

For information on Service Pack 1 for SCDPM, go to <http://support.microsoft.com/kb/959605>.

Three separate components (with a possible fourth) must be updated with SCDPM Service Pack 1. The first is the update for SCDPM itself. There is a SQL Server update for SCDPM SP1. There is an update for the protection agents. If the agents have not yet been deployed as would be the case with an installation in the resource pool in support of Hyper-V, the update will be applied when the agents are deployed for the first time. And finally, if you have deployed the SCDPM Administrators Console on a separate computer, you need to apply the service pack to update the console.

IMPORTANT SCDPM SERVICE PACK 1

To install the SCDPM SP1 update, computers need to be running the Microsoft Visual C++ 2008 Redistributable Package for x64 systems. This package is required on each system that will run SP1 updates. You can download this package to install it prior to running SP1 from <http://go.microsoft.com/fwlink/?LinkID=120135> or you can let SCDPM SP1 install it for you.

Install the SP1 update on the SCDPM server first. To do so, run the DataProtectionManager2007-KB959605.exe file on the server. If the Visual C++ package is not present, it will be installed first. Reboot the computer after the service pack is installed.

If SQL Server is running on the same computer, the service pack will also update the SQL Server installation. If SQL Server is on another computer, you will need to install the Visual C++ package on that computer and then run the SQLPrep-KB959605.msp file on that computer.

Finally, you need to update the agents on the target computers. If the agents have already been deployed, use the SCDPM Administrator Console to update them and restart each of the clients to enable the new agent. If they have not been deployed, you need to run the agent installation on each computer to be protected. The installation file for the agent is located on the SCDPM server under the %ProgramFiles%\DPM\Agents\RA\2.0.5820.0 folder. Use the executable installation file in the AMD64 folder for your Hyper-V hosts. Note that once again, the Visual C++ package is required for each host and may be installed by the agent setup program. Reboot each host after the agent has been installed. When the system is rebooted, use the agent update file in the %ProgramFiles%\DPM\Agents\RA\2.0.8793.0 folder to install the Visual C++ package. Again, use the executable installation file. Reboot the server again. When the system is rebooted the second time, launch an elevated command prompt,

move to the %ProgramFiles%\Microsoft Data Protection Manager\DPM\Bin folder on the local computer, and run the following command, where *servername* is the name of your DPM server:

```
setdpmserver -dpmservername servername
```

This ties the agent installation to the DPM parent server.

MORE INFO AGENT INSTALLATION

You can also deploy the agent from the SCDPM server. When you do this, it automatically sets the parent server.

When SCDPM is installed and the agents are deployed, you need to configure the storage pool as well as a tape library if you intend to use one. Both configurations are performed from the Management tab. To add disks, use the Disks sub-tab. If you are using a virtual machine, use a pass-through disk and add it to the storage pool (see Figure 9-20). Disks that are not prepared properly will automatically be converted to dynamic volumes. Ideally, the disk will not be formatted because SCDPM formats disks when you add them. Tape Libraries are added under the Libraries sub-tab. After these items are configured, your SCDPM installation is ready to protect Hyper-V hosts and the VMs they run.

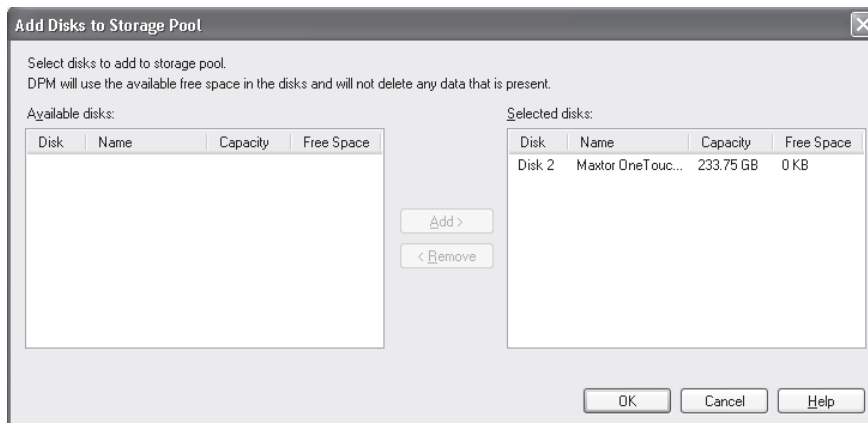


FIGURE 9-20 Adding a pass-through disk to the storage pool

Performing Host Server and Virtual Machine Backups

SCDPM uses shadow copy–based block-level protection for both host servers and virtual disks. Because it relies on VSS, SCDPM protects enlightened virtual machines without hibernation downtime by saving the state of the VM. The protection agent model used by SCDPM supports the protection of all virtual machines within a single host with only one agent on the host platform. Alternatively, you can deploy agents within each virtual instance. But because you are using SCDPM in the utility domain of the resource pool, you only need to install the agent on the host servers.

To protect hosts and VMs, run the backup from SCDPM. Begin by creating a Protection Group:

1. Launch the SCDPM Administrator Console and click the Protection Tab. Click Create Protection Group in the Actions pane. Click Next.
2. Select the entire host server folder structure by adding the server name to the protection group. Click the server name to add and select all of the values that are presented. To protect the operating system, you must also select the System State box. Do this for all machines and click Next when done.
3. Name the protection group—for example, **Hyper-V Hosts**—and select Short-Term Protection. Click Next.
4. Specify your short-term goals. Set appropriate values for your required protection schedule and click Next.
5. Review the allocations proposed by SCDPM and click Next.
6. Choose the method to use to create the replica. If you are doing this during off hours, choose Now. If not, set it to perform the operation automatically later or set it to Manual to perform it later on your own. Click Next.
7. Review your settings and click Create Group. SCDPM will create the group (see Figure 9-21). Click Close when done.

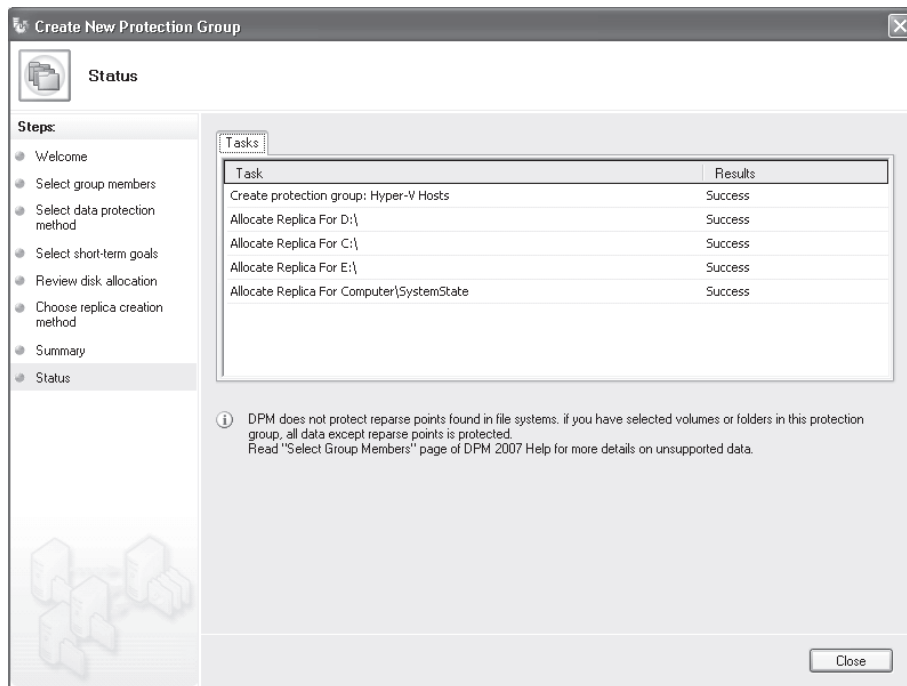


FIGURE 9-21 Creating a protection group

Your first Protection Group has been created. If you tell SCDPM to create the replica now, it will also perform the replica creation operation for each of the folders and applications you selected on the system.

After the replicas have been created, SCDPM performs backup operations on a scheduled basis based on the schedule you added to the Protection Group. Because you have created the first replica, further backups will be performed using block-level differentials based on the original replica. SCDPM also captures the shadow copies of each protected volume and stores them centrally. These shadow copies are then used to restore contents from specific time and dates. In this way, SCDPM offers a complete protection mechanism.

You can now use the SCDPM Administrator Console to monitor the protection of your host servers and the VMs they run.

Restoring VMs with SCDPM

Restoration of Hyper-V components in SCDPM is performed from the Recovery tab. SCDPM lets you recover individual virtual machine files (see Figure 9-22) unlike Windows Server Backup, where it is an all-or-nothing proposition. This makes it a much more practical tool for VM protection.

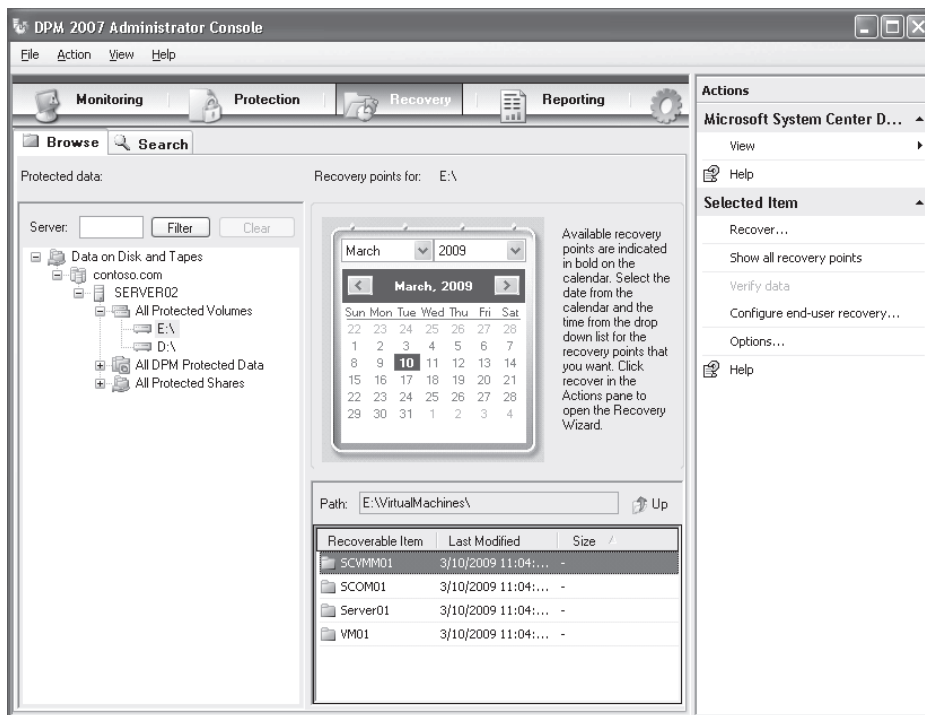


FIGURE 9-22 Viewing virtual machines to recover

NOTE SCDPM SYSTEM RECOVERY TOOL

SCDPM includes a special recovery tool that lets you recover failed computers. This tool can be installed on its own to rebuild failed systems or recover lost data. The tool is available on the SCDPM installation media.

Use the following procedure to recover a virtual machine:

1. Click the Recovery tab of the SCDPM Administrator Console. Click the server and drive that contain the VMs you want to recover in the Tree pane. This will list all available folders for this drive in the Details pane.
2. Click the calendar to choose the date from which you want to recover data and then double-click the VirtualMachines folder in the Details pane under the calendar.
3. Select the folder that contains the VM you want to recover. You can also select individual files within the VM folders. Click Recover in the Actions pane.
4. Verify that the proper item is selected and click Next.
5. Choose where to recover the data. If you choose Original Location, the restore will overwrite the existing files if they are still there. Select this option if the entire VM is lost. Choosing Alternate Location can let you recover the files without overwriting the existing VM. Select this option if you only need to recover files from within the VM disks. When you select Alternate Location, you must also identify where to recover the files. Click Next when done.
6. Select your recovery options (see Figure 9-23). Even if you selected the original destination, you can still choose to recover a copy. But if you need to fix a non-working VM, choose Overwrite The Existing Data. You can also control the security settings to recover. When recovering VMs, you should choose Apply The Security Settings Of The Recovery Point Version to make sure proper access rights are restored with the VM. If your storage pool is located on a SAN, you can recover using hardware-based snapshots, which will provide a faster recovery process. You can also set notifications if you have assigned a Simple Mail Transfer Protocol (SMTP) server in the optional settings of SCDPM. Click Next when done.
7. Review your settings and click Recover. SCDPM will begin the recovery process. Click Close when the VM has been restored.

As you can see, working with SCDPM to protect Hyper-V and the VMs it runs is a better option than working with Windows Server Backup and is an option to consider if you have medium to large resource pools.

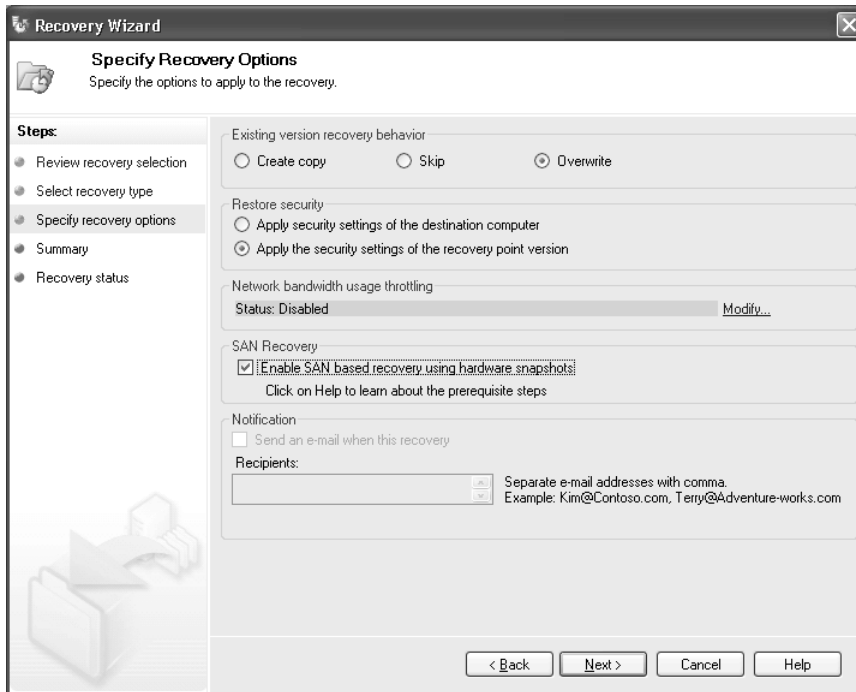


FIGURE 9-23 Selecting recovery options

PRACTICE Performing Internal VM Backups

One of the best ways to protect VM contents is to perform a backup from inside the VM itself to a VHD that is tied to the VM and then copy this VHD elsewhere. This is the object of this practice. This practice consists of three exercises. In the first exercise, you add a new VHD to an existing VM and configure it. In the second exercise, you create the backup schedule. In the third exercise, you use the Robocopy utility from the parent partition to create a scheduled copy task that copies the backup VHD to a network location.

EXERCISE 1 Preparing the VM for Backup

In this exercise you will add a new virtual hard disk to an existing VM running Windows Server 2008 and then you will configure the disk within the VM. You perform this operation on ServerFull01. Log on with domain administrator credentials.

1. Log on to ServerFull01 and move to the Hyper-V Manager console. Click ServerCore01 and make sure SCVMM01 is stopped. If not, right-click it and choose Shut Down to properly shut down the operating system.
2. When the VM is shut down, right-click SCVMM01 and choose Settings. Click IDE Controller 0, select Hard Drive, and then click Add.

3. Click New and then click Next. Choose Dynamically Expanding Disk—this will keep the disk as small as the data you back up—and click Next. Name the disk **SCVMM01_BUDisk** and store it in the SCVMM01 folder under VirtualMachines. Click Next. Make sure you size the disk appropriately for growth, click Next, and then click Finish. Click OK to close the VM's Settings dialog box.
4. Right-click SCVMM01 and click Start.
5. After the VM starts, double-click its thumbnail image to open a remote session to the VM. Log on to the VM with a domain administrator account.
6. After Server Manager opens, move to the Storage node, and then to the Disk Management node in the Tree pane. If the new disk is offline, right-click the disk number in the bottom of the Details pane and choose Online.
7. Right-click the disk, choose New Simple Volume, and then click Next. Use all of the available space and click Next. Assign the next available letter and click Next. Name the volume **Backup**, choose the NTFS file system, select Perform A Quick Format, and click Next. Click Finish. The disk is ready when the format completes.
8. Install Windows Server Backup by right-clicking Features in the Tree pane of Server Manager and choosing Add Feature. Scroll down to Windows Server Backup and select it. You do not need to add the command-line tools for this exercise. Click Next, click Install, and then click Close when the installation is complete.

Your server is ready for the next step.

EXERCISE 2 Creating the VM Backup

In this exercise you will create a backup schedule for SCVMM01 and use the newly added VHD as the target for the backup. Perform this exercise with domain administrator credentials.

1. Log on to SCVMM01 and move to the Storage node and then the Windows Server Backup node of the Tree pane in Server Manager.
2. Click Backup Schedule in the Actions pane.
3. Select Custom and then click Next. Choose Custom Backup because you want to exclude the backup disk you added from the backup so that you can use it as the backup target.
4. Clear the volume named Backup from the list and click Next. You will only back up drives C and D in this system.
5. Use the default daily backup schedule, which is 9:00 P.M., and click Next.
6. Click Show All Available Disks, select the disk you just added, and click OK. Select the disk as the destination and then click Next. The wizard warns you that the disk will be erased (see Figure 9-24). Click Yes.

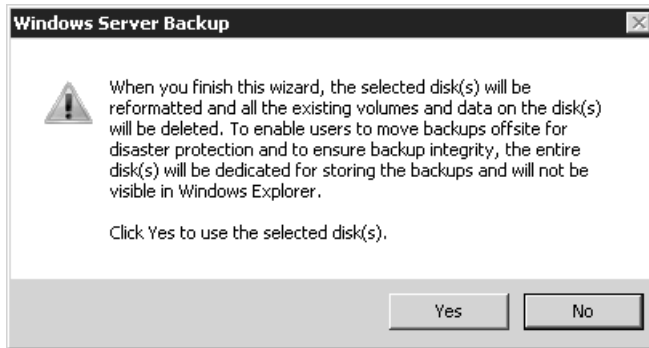


FIGURE 9-24 WSB takes ownership of disks used as targets for backups.

7. WSB labels the disk. Click Next and then click Finish. WSB formats the new disk. Click Close when done. You can wait until the scheduled backup is performed to move on to the next step, or you can perform a backup now.
8. Click Backup Once. Note that now that you have a scheduled backup, the wizard offers to use the same options as the scheduled backup (see Figure 9-25). This speeds up the Backup Once process. Select to use the same options and click Next.

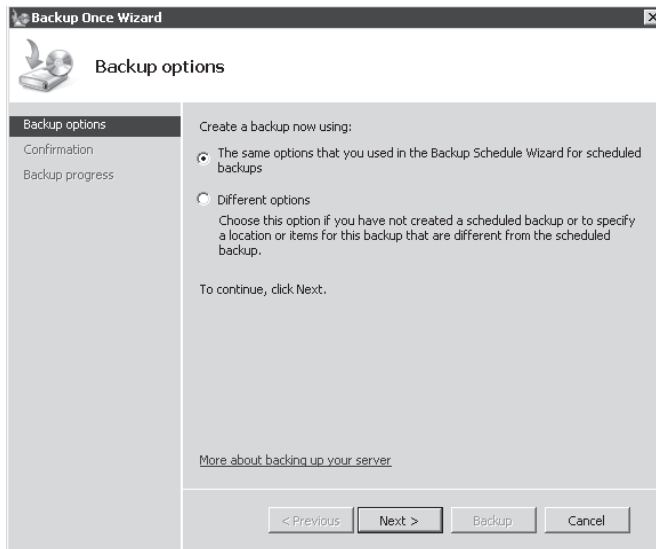


FIGURE 9-25 WSB will reuse a schedule for a one-time backup if it exists.

9. Click Backup to begin the process. This will take some time.
 10. Click Close when the backup is complete.
- Your first VM backup is complete. Proceed to the next step to protect the backup disk.

EXERCISE 3 Replicating the VM Backup

In this exercise you will use the Robocopy utility in Windows Server 2008 to protect the backup disk on SCVMM01. Perform this operation on ServerFull01. You must perform this

operation from a parent partition because you will be replicating a disk tied to a VM. Log on with a domain administrator account. To replicate the disk, you need two values: the location of the disk file itself and the target location that you want to replicate it to.

1. Log on to ServerFull01 and open Notepad by clicking Start, typing **notepad**, and pressing Enter.
2. In Notepad, type the following command:

```
robocopy \\servercore01\d$\VirtualMachines\SCVMM01\SCVMM01_BUDisk.vhd  
\\ServerFull01\Updates
```

This copies the backup VHD to the shared Updates folder on Server Full01. In your own resource pool, you should copy these disks to a more proper location. Updates is used for the purpose of simplifying this exercise.

3. Choose File and then choose Save. Choose All Files from the drop-down list and name the file **Replicate.cmd**. Place the file in the C:\Updates folder and click Save. Close Notepad. Do not place this file in your Documents folder because it will not run as a scheduled task when you are not logged on.
4. Move to Server Manager and choose Configuration and then Task Scheduler in the Tree pane.
5. Click Create Basic Task. Name the task **VHD Replication**, give it a short description, and click Next.
6. Choose Daily Trigger and click Next. Set the task to start at 4:00 A.M. and to recur every 1 days. Click Next.
7. Select Start A Program as the action and click Next. Click Browse to locate the program, navigate to C:\Updates and choose Replicate.cmd, and then click Open. Click Next.
8. Select Open The Properties Dialog For This Task When I Click Finish and then click Finish.
9. On the General tab of the tasks' Property page, select Run Whether The User Is Logged On Or Not to make sure the task runs at the appointed time. Note that the task is running using your domain administrator account. Because the task runs using network paths, you must let it store your password. Click OK, then type in your password and click OK.
10. Expand the Task Scheduler to view the Task Scheduler Library. Your new task should be listed. Right-click the task and choose Run. This will verify that the task works properly. Check the Updates folder when the task has completed to verify that the backup VHD has been copied.

MORE INFO ROBOCOPY UTILITY

For more information on Robocopy, go to <http://technet.microsoft.com/en-us/library/cc733145.aspx>. Microsoft also offers a graphical interface for Robocopy at <http://technet.microsoft.com/en-us/magazine/2006.11.utilityspotlight.aspx>.

Your system is ready to first back up the VM contents into the backup VHD and then replicate the VHD to a network folder. Ideally, you would create a proper directory structure in a custom shared folder to hold all of the replication copies. For example, you might create a shared folder called **Replicated_VHDs**, create a subfolder structure including the name of the source VM, and then create a folder for each day of the month. When you create the replication jobs, you need a command file for each day of the month to copy the backup VHD to the right folder each time. Of course, you can create a more complex script that will check the date and then copy the file to the appropriate folder based on the date.

This is a good method of protecting your VMs when you do not have access to other options.

Quick Check

1. What is the Last Known Good Configuration and how can you access it?
2. Which state should a legacy virtual machine be in to have a proper backup with Windows Server Backup?
3. Which Integration Service should be turned on for child partitions to rely on VSS to take a snapshot of an enlightened virtual machine?
4. Which command-line tool included in Windows Server Backup can be used on a full installation or a Server Core installation?
5. What are the potential backup targets for WSB? Name at least three targets.
6. What is the maximum size of a volume that WSB can back up?

Quick Check Answers

1. The Last Known Good Configuration can be used to revert to the last configuration saved in the registry before you applied changes. You can access this option by pressing the F8 key during system startup. The F8 key also gives you access to a number of different startup modes: Safe Mode, Safe Mode With Networking, and so on.
2. The legacy virtual machine can be in any state. If it is running, it will be put into a saved state and then restored after the backup.
3. To rely on the VSS to take a snapshot of an enlightened virtual machine, the Backup (Volume Snapshot) Integration Service should be turned on for the child partition.
4. Windows Server Backup's command-line tool is WBAdmin.exe.
5. The potential targets are: shared folder, optical media or removable media, and internal and external hard disk. Not all targets can be used in all backup modes.
6. Windows Server Backup can back up volumes that are no larger than 2,043 GB.

Case Scenario: Dealing with a Host Server Failure

In the following case scenario, you will apply what you have learned about protecting your Hyper-V host servers. You can find answers to these questions in the “Answers” section on the companion CD which accompanies this book.

As the resource pool administrator for Lucerne Publishing, you are responsible for managing both the host servers and the virtual machine objects they contain. Therefore, you have put in place a backup schedule based on Windows Server Backup for each of the host servers. You applied the appropriate updates on the host servers and created backup schedules for each host. In addition, each host server has a custom removable disk enclosure that allows you to easily swap disks each day. You rotate these disks and send them offsite each time a backup is taken.

On Monday morning when you come in to work, one of your colleagues tells you that a number of server failures occurred over the weekend in your test environment. The IT group tried to get everything working again over the weekend, but they have had a series of issues for each server. After further investigation, you discover that all of the failures are related to virtual machines. These virtual machines have been running on one of your host nodes: HostServer03, which is a standalone host. In fact, the failures are due to the fact that virtual machines have been restarting repeatedly because the host server is experiencing problems with its disk controller, causing it to reboot every time the failure occurs. This automatically reboots all of the VMs as well. In addition, the controller has corrupted the host server’s system drive.

Fortunately, you have an up-to-date backup of the server and you can restore it. You also have been performing backups inside each VM to a spare VHD and replicating the VHD to another location. You verify that the latest backup you have for the host is from Friday, but you have replicated backups from the virtual machines as recently as Sunday. To repair the server and the VMs, you need to answer the following questions:

1. What do you need to do to repair the host server?
2. What do you need to do to repair the virtual machines and bring them up to Sunday’s data?
3. What should you do to provide better protection for HostServer03?

Suggested Practices

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

Windows Server Backup

- **Practice 1** Take the time to perform backups with WSB on your host servers. Examine the Event Log to view the Volume Copy Snapshot events that are associated with the backups.
- **Practice 2** Take the time to perform restores of your host servers with WSB. Run through the restore process and try each of the different ways you can launch restorations on working and non-working host servers.

System Center Data Protection Manager

- **Practice 1** If you can, take the time to install and work with SCDPM for your Hyper-V hosts. At a minimum, seeing and working with the SCDPM interface will be useful for the exam.

Chapter Summary

- Windows Server Backup is composed of three elements: an MMC snap-in, a command-line tool, and a series of Windows PowerShell cmdlets.
- Windows Server Backup can restore several elements: full computer (installed locally, on a custom disk, on the Windows Server installation media), applications, files and folders, and volumes.
- Backups of host servers should be application-level backups that include the operating system, the data partitions, and the virtual machine contents.
- Windows Server recovery techniques include driver rollback, disabling devices, Last Known Good Configuration, WinRE, Windows PE, Windows Server Backup, and third-party backup and restore tools.
- Backups of virtual machines should include user data, corporate data, databases, documents, system state information for your servers, and Active Directory Domain Services data. In short, they should be specific to the application or data stored within the VM.
- The Volume Shadow Copy Service can take a VSS snapshot of an enlightened virtual machine while the machine is running and create a data-consistent backup from this snapshot. This is one more reason why you should run enlightened guest operating systems.
- When a backup of a legacy virtual machine is performed, it is put in a saved state for the duration of the backup.
- System Center Data Protection Manager can be used to capture remote VSS images and store them centrally. DPM streams all backups to a central disk system and can store them on tape for offline storage. To use DPM with Hyper-V you must run Service Pack 1.

Configuring Virtual Machine High Availability

Your resource pool is ready. So far, you've undertaken all of the tasks required to stage the resource pool (see Figure 10-1), including:

- Performing an assessment of your source environment, as outlined in Chapter 1, "Implementing Microsoft Hyper-V." Remember, three sources were possible:
 - You could start with a completely physical infrastructure and want to move to a virtual infrastructure running on a resource pool consisting of Hyper-V hosts.
 - You could have already begun the process of moving to a virtual infrastructure by relying on software-based virtualization engines such as Microsoft Virtual Server or VMware Server and want to move to a Hyper-V resource pool.
 - You could have already been running hardware-based virtualization using tools such as VMware ESX Server or Citrix XenServer and want to move to either a heterogeneous resource pool including Hyper-V and other hypervisors or a purely homogeneous resource pool running only Hyper-V.
- In any case, you needed to proceed with the construction of your Hyper-V Servers after the assessment was performed, as outlined in Chapter 2, "Configuring Hyper-V Hosts."
- Then, when your host servers were ready, you added further functionality in your resource pool by configuring the servers for remote administration, creating host clusters, and learning how to monitor host server and virtual machine performance as outlined in Chapter 3, "Completing Resource Pool Configurations."
- When the resource pool reached a reasonably functional level, you began learning how to work with virtual machines in Hyper-V as outlined in Chapter 4, "Creating Virtual Machines."
- In Chapter 5, "Automating Virtual Machine Creation," you learned how to generate VMs from pre-built templates and you saw how valuable resource pool infrastructures are given the time it takes to automatically generate a VM compared to working with physical machines.
- In Chapter 6, "Migrating to Hyper-V," you saw how machines—either physical or virtual—can be converted to Hyper-V and run in Hyper-V environments.
- In Chapter 7, "Automating Hyper-V with Windows PowerShell," you discovered just how easy it is to automate and script resource pool administration tasks with Microsoft's Windows PowerShell command language.

- Chapter 8, “Securing Hosts and Virtual Machines,” and Chapter 9, “Protecting Hyper-V Resource Pools,” helped you complete the resource pool configuration and bring it to a complete state of operational readiness by implementing security and disaster recovery strategies.

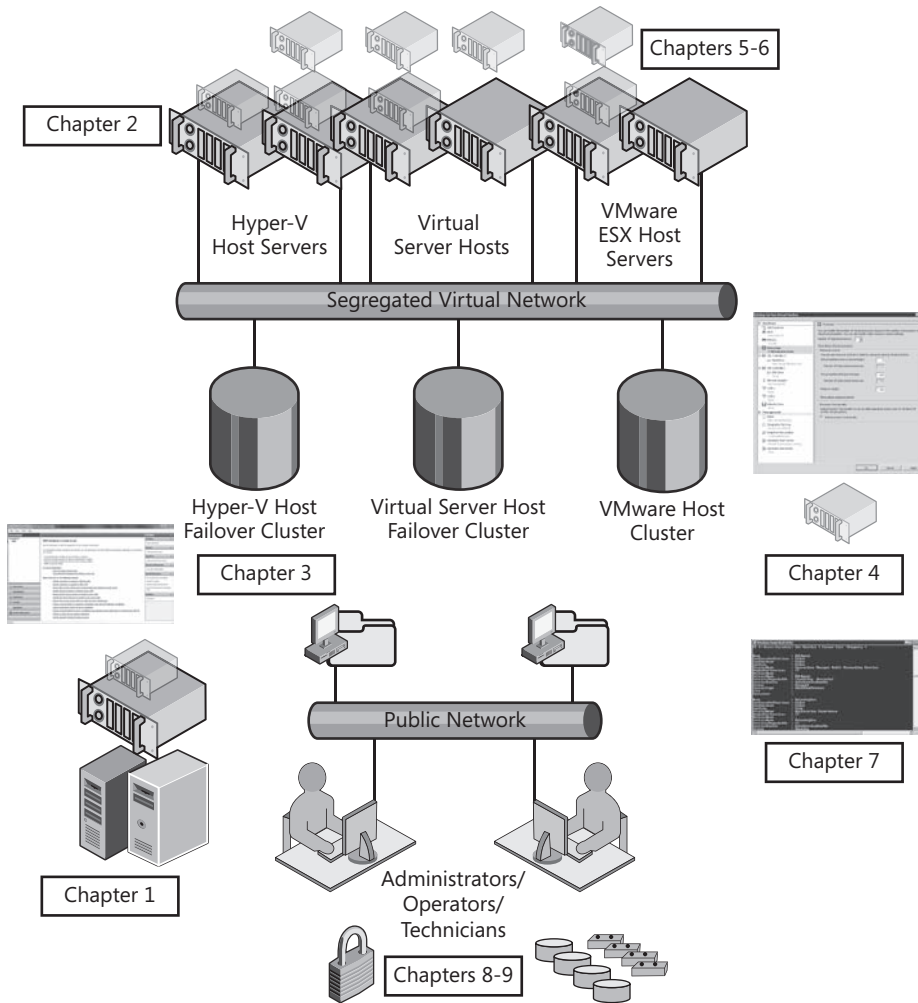


FIGURE 10-1 Building the resource pool for production

Now you're ready to bring the resource pool online and move it into production. Most of the virtual machines you've worked with to date have been designed to support resource pool operations—building domain controllers and management machines running anything from System Center Virtual Machine Manager to System Center Operations Manager and more. However, the machines you build now will be virtual machines supporting the virtual service offerings that make up your production network (see Figure 10-2).

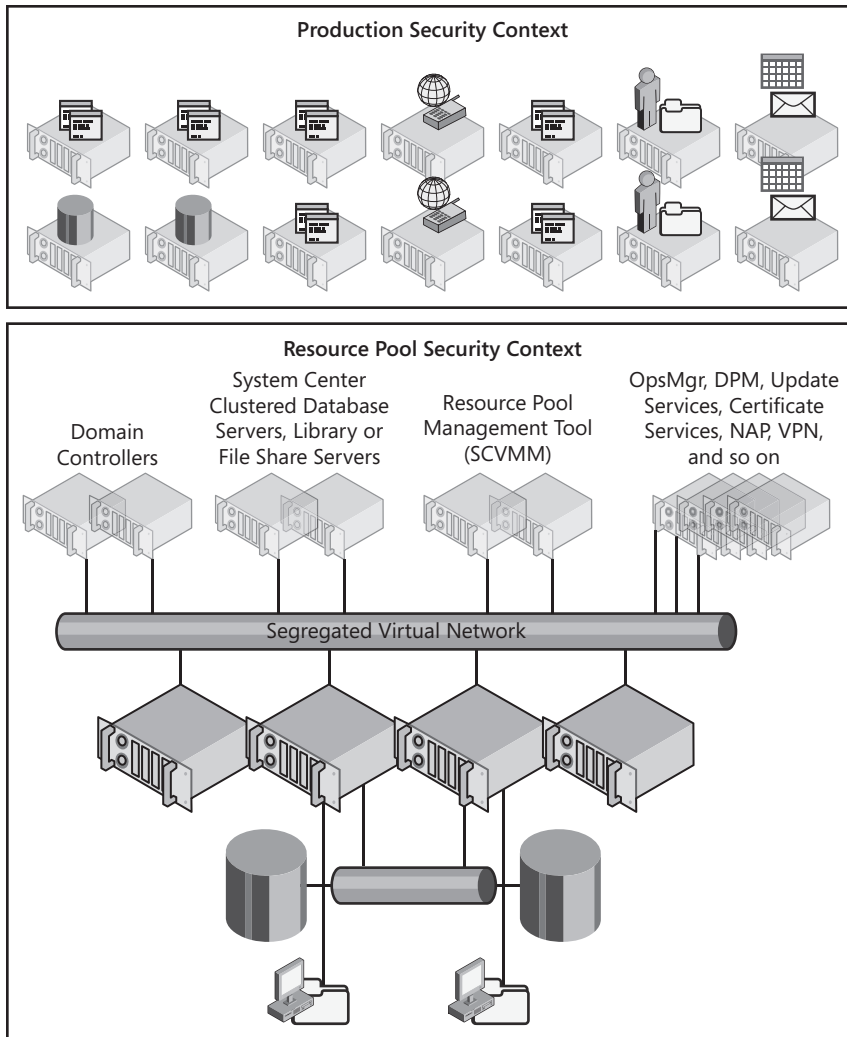


FIGURE 10-2 The production resource pool supports any number of VMs

Because these VMs will be running production services, you must consider how you will configure them. For example, essential services such as Microsoft Exchange Server or Microsoft Office SharePoint Server should be configured to provide their services through high-availability implementations. Other services will require different setups to ensure that their services are available when you need them. Microsoft publishes a series of articles on supported virtual configuration of specific services. The guidelines offered by these articles should be followed if you want to run the very best network.

In addition, now that your resource pool is ready, you will be able add additional virtualization layers such as virtual desktop infrastructures, application virtualization, and profile virtualization. Desktop virtualization in particular requires the implementation of

server virtualization before it can be used because desktops run as virtual machines on hypervisors much the same way as servers do.

But first, you must ensure that the configurations of the virtual machines you will use to run production network services are supported and highly available. This is the focus of this chapter.

Exam objectives in this chapter:

- Configure a virtual machine for high availability.
- Monitor and optimize virtual machines.

Before You Begin

To complete this chapter, you must have:

- Access to a setup as described in the Introduction. In this chapter, you will build further onto your production resource pool and begin adding virtual machines that can be used to support production services.

Lesson 1: Working with VM High Availability

The very best virtual machine is an available virtual machine. However, determining which method makes a VM highly available is not always easy because it often depends on the workload the VM is running. Helping you determine which is the best strategy for each VM is the focus of this chapter.

After this lesson, you will understand:

- How virtual machine high availability works.
- How quick migration works.
- How to configure redundant VM storage and network adapters.
- How to set up specific services in supported configurations.

Estimated lesson time: 60 minutes

Understanding Virtual Machine High Availability

In Chapter 3, you learned about creating failover clusters for host servers. Two cluster types are available for host servers: single-site clusters and multi-site clusters. Single-site clusters are based on shared storage in the form of either Fibre Channel storage area networks (SANs) or iSCSI targets. And, despite its name, the multi-site cluster does not need to span more than one site; instead, it can support the creation of clustered servers using direct-attached storage (DAS) along with a replication engine to keep the data between cluster nodes in synch.

When host servers are clustered, the virtual machines you create on them can be made highly available by placing them on clustered nodes. This does nothing for the applications contained within the virtual machine—the applications running in the VM are not aware of the high-availability feature, unlike applications that are installed directly into a cluster. However, it does ensure that the VM will always run in the event of a host failure (see Figure 10-3). This high-availability model works for most applications despite the fact that they are not aware of it when transfers occur from one node to another.

However, some applications that are state-sensitive—for example, Microsoft Exchange—do not behave properly under this model and may lose data when a transfer occurs. Transactional applications—especially applications that support very high-speed transactions—do not lend themselves well to this model because the application is designed to behave in a particular way when the failover occurs and cannot do so when a VM has been failed over.

Because of this, you should consider building highly available virtual machines—that is, creating clusters within the virtual machine layer—to create application-aware clusters to ensure the continuous availability and stability of the applications you move into the virtual layer of your resource pool. Depending on the application type, you can rely either on the single-site or the multi-site failover clustering model to create them. Remember, however,

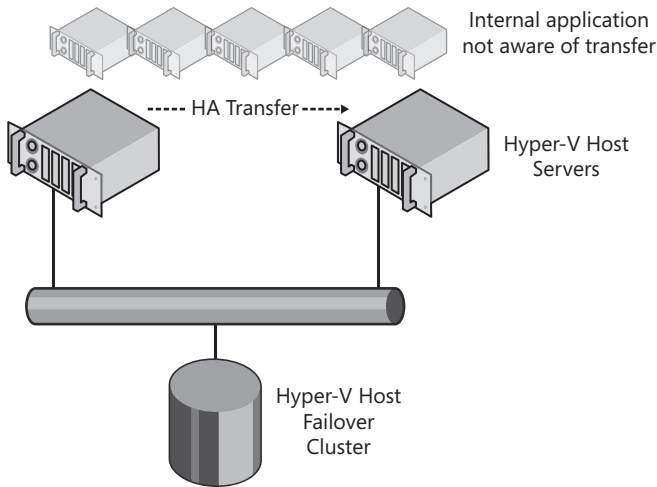


FIGURE 10-3 Internal applications are not aware of the status of a highly available VM.

that failover clusters only work for stateful workloads or workloads that persist data from user sessions. Stateless workloads or workloads that provide read-only services can rely on another high availability solution: Network Load Balancing (NLB). Like failover clustering, NLB is a high-availability solution that is fully supported in the virtual layer.

In the end, you have three options for making the workloads contained within virtual machines highly available:

- Creating host failover clusters
- Creating guest failover clusters
- Creating guest NLB clusters

Each option provides a given level of availability to your VMs and the applications they run.

Working with Host Failover Clusters

In Chapter 3, you learned how to create and implement host failover clusters. You also learned that any virtual machine can be made highly available by adding it as an application within the cluster. However, a VM is not like a traditional application. Even though the VM always remains available—or remains available as much as possible—when you run it on a host cluster, this model does not apply to every single workload in your production network.

You should, however, always endeavor to create host clusters wherever possible to provide two different levels of service continuity:

- Host clusters support the continuous operation of VMs. If a host fails or indicates that it is failing, all of the VMs running on the host will be automatically transferred to another node on the cluster.
- Host clusters support the operation of VMs during maintenance windows. If you need to work on one node of the cluster—for example, to install software updates—you

can move the VMs off of the node during the operation. Move them back to the node when the operation is complete. Repeat the process if the other nodes of the cluster require maintenance.

In either case, service will be interrupted for the VMs being moved. When the cluster detects that a node is failing, but the node has not failed yet, the cluster service will cause the VMs to fail over to another node. In this case, it will use the Quick Migration process to move the VM—saving the state of the VM on one node and restarting it on another. When a node actually fails, the cluster service moves the VM by simply restarting the VM on another node. The downtime for the VM is increased in this case because when the node fails, all of the VMs on that node will be turned off. When you need to perform maintenance on a node, you use Quick Migration to move a VM from one node to another.

Even when you use Quick Migration, the virtual machines must be put into a saved state and restored on the other node because the Failover Clustering feature in Windows Server 2008 uses a shared-nothing clustering model. In this model, only one node can own a shared disk volume at a time. To move a VM from one node to another, the cluster service must save the state of the VM and store that state on the shared volume, then pass the ownership of the volume to the other node, which can then restore the VM. Although this process does cause downtime for the VM, the downtime can be extremely minimal when you use very high-speed disk spindles in your shared volumes.

UPDATE ALERT LIVE MIGRATION IN WINDOWS SERVER 2008 R2

Microsoft has included the capability to perform live migrations in Windows Server 2008 R2. Live migrations move the in-memory contents for a VM from one node to another and then transfer the VM operation to the new node after the in-memory contents are copied. To do this, the VM is paused on one node and restarted on the other. This transfer is achieved through the new Cluster Shared Volume (CSV) model in the Failover Clustering feature. CSVs allow two or more cluster nodes to retain the ownership of a shared disk volume. Because the nodes already have ownership of the volume, there is no longer a delay in passing volume ownership from one node to another. Instead, it is performed through dynamic I/O redirection. Note that Hyper-V is responsible for moving the VM in-memory contents from one node to the other prior to the actual transfer. For more information on this feature, download the Hyper-V Live Migration Overview and Architecture document from <http://www.microsoft.com/DownLoads/details.aspx?familyid=FDD083C6-3FC7-470B-8569-7E6A19FB0FDF&displaylang=en>. You can also take a look at the Step-by-Step Guide to Using Live Migration at <http://go.microsoft.com/fwlink/?LinkId=139667>.

Microsoft recommends the use of SCVMM along with live migration. Together with OpsMgr, SCVMM can rely on the Performance and Resource Optimization (PRO) feature to move VMs from one host to another when VMs require additional resources to run—resources that are not available on the current host. In these scenarios, SCVMM supports dynamic live migration. Remember that to update a host server infrastructure to support live migration, you only need to update the host to Windows Server 2008 R2, and to update Hyper-V Server hosts to support live migration, you must update them to Hyper-V Server R2.

IMPORTANT PROCESSOR ARCHITECTURES AND VM MIGRATIONS

For both Quick Migrations and live migrations to work on a host cluster, the source and the target node must use the same processor architecture. For example, you cannot migrate a VM from a node running AMD processors to a node running Intel processes. This is because the migration process relies on the movement of in-memory contents. For a saved state to be restored on a node, the processor architecture must match the saved in-memory contents from the source node. For Hyper-V to move a VM through live migration, moving in-memory contents from one node to another, the processor architecture of the two nodes must match. This is one more reason that it is important to fully understand the processor characteristics of your host servers when you select them, as outlined in Lesson 3 of Chapter 1.

Working with Host Failures

Another very important aspect to keep in mind when working with host server failures of any type is the restart order of the VMs. When a host fails, all of the VMs on that host fail. Correspondingly, when the host restarts, all of the VMs start—and if you're not careful, all of the VMs will start at the same time. This slows down the restart process considerably because each VM is contending for host server resources—CPU, RAM, networking, and disks—at the same time.

This is why VM configuration settings allow you to set startup delays for your VMs (see Figure 10-4). This delay is set under the Automatic Start Action settings of the VM. Note that start actions are set to restart the VM if it was running when the host server was shut down by default. You can change them to Nothing—which leaves the VM stopped when the host restarts—or Always Start, which will always start the VM no matter what its state was before the shutdown of the host.

This means that you need to take several factors into consideration when you plan VM deployments on host servers. First, you need to consider how you will assign VMs to hosts. If a host server is going to run up to 20 VMs, the VMs cannot and should not contend for the same resources at the same time. In fact, you want to configure heterogeneous virtual workloads on host servers as much as possible and avoid configuring homogeneous workloads. To do this, you must look at the workloads and identify which processes and resources they need and when they require them.

For example, if you're running Windows services in your network, you can expect them to behave as follows (see Figure 10-5):

- Domain controllers require network and processor resources at peak times (early morning, after lunch) when users log on to the network.
- File and print servers require processor and network resources at off-peak times (mid-morning, mid-afternoon) when users perform their work.
- Web servers focus on network resources and, if properly constructed, will require a steady stream of resources, especially when they are configured to belong to NLB clusters.

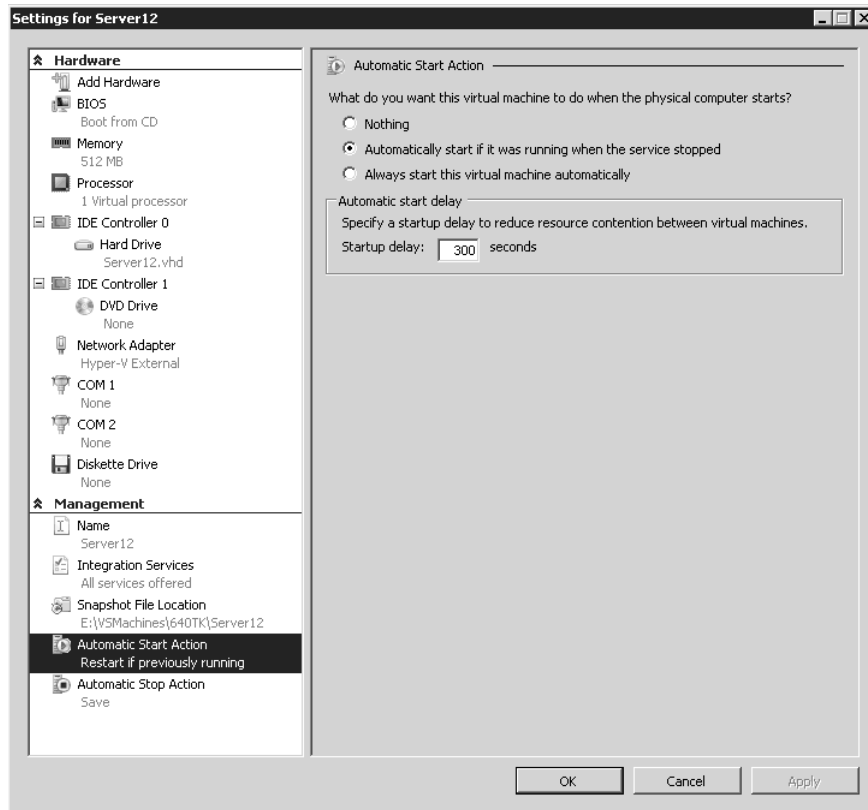


FIGURE 10-4 Setting startup delays for VMs

- Microsoft SQL Server and Exchange Server both require a steady amount of resources throughout the day and focus mostly on disk and processor resources.
- Test and development systems are often used during off hours or have variable loads during the day.
- Corporate applications often have scheduled resource requirements. For example, a payroll application can run on bimonthly or biweekly schedules.

Not all workloads are busy at all times. In fact, some workloads are “parked” and rarely run. If you find VMs that are in this state on an ongoing basis, perhaps you should simply remove them from your network.

Because server workloads require different resources at different times, you should configure your workloads in a heterogeneous manner (see Figure 10-6). This means one host server could run a DC, a network infrastructure server, a file server, one or more Web servers, test and development servers, and perhaps even a corporate application. The key is to focus on workloads that require different types of resources at different times.

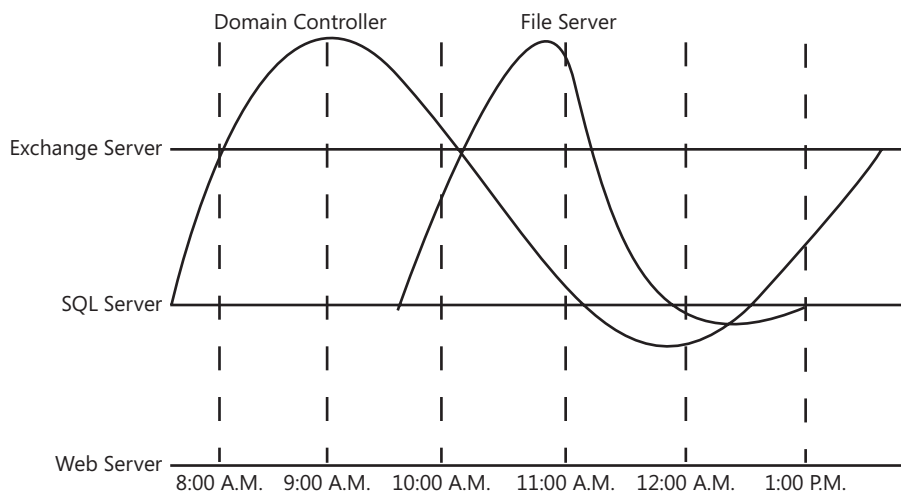


FIGURE 10-5 VM resource requirements over time

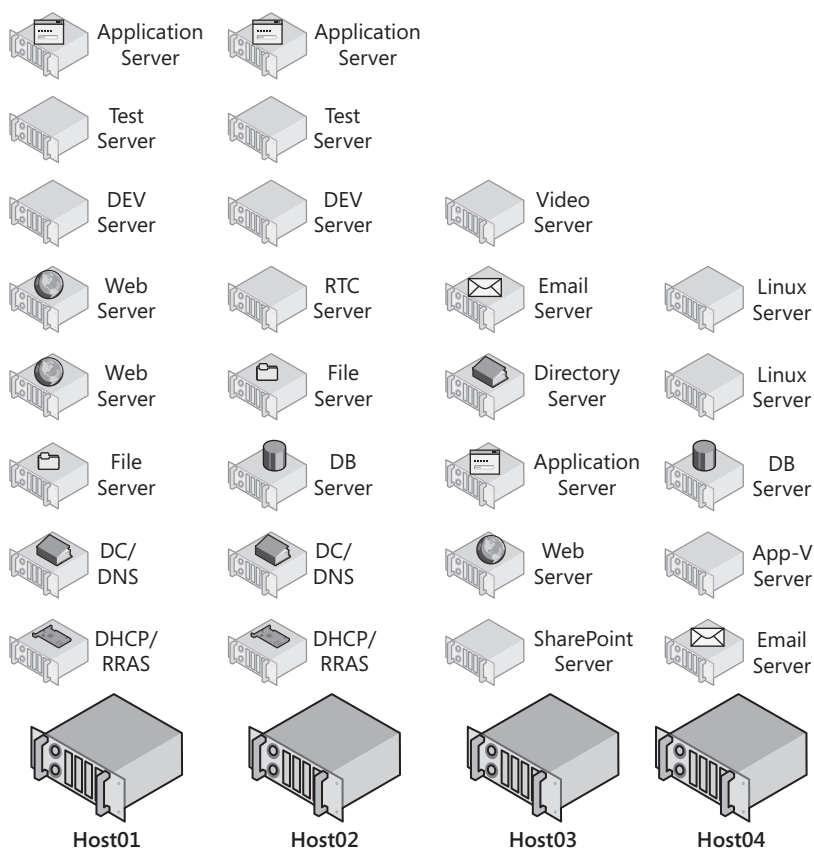


FIGURE 10-6 Assigning heterogeneous workloads to host servers

Some tools perform this operation automatically. This is the case for SCVMM when using the Performance and Resource Optimization (PRO) feature along with Intelligent Placement. PRO relies on historical performance data for a VM when it decides which host to place it on. If the VM is new, however, you won't have any historical data. In this case, you should make an educated guess as to where to place the VM and then closely monitor it for resource contentions.

In addition, you need to consider the startup delays you set for your VMs. If a host server is going to run a number of different VMs running different roles, you want to optimize the startup of these VMs to make sure the services they contain start up in the proper order. Table 10-1 outlines a sample startup order for VMs on a host.

TABLE 10-1 Sample Startup Order for VMs

VM ROLE	STARTUP DELAY	COMMENTS
Domain Controller/ Domain Name Service	0 seconds	Domain controllers should always start first since they provide logon services for all of the other VMs in a domain.
Dynamic Host Configuration Protocol (DHCP) servers	90 seconds	DHCP servers provide addressing services for any number of machines in a network and should therefore be started as soon as possible after the domain controllers.
Database servers	150 seconds	Database services often provide support for other applications and should be started as soon as possible.
Middleware servers	300 seconds	Middleware servers often depend on database services and must therefore start after the database services have booted.
Email servers	150 seconds	Users often turn to email services as soon as they are logged on. Therefore, email services should also start as soon as possible.
File and print servers	450 seconds	File and print servers do contend for critical resources while starting and can have a delayed start.
Web servers	600 seconds	Web servers often have back-end dependencies, such as when they are part of an n-tier application structure. Therefore, they must start only after databases and middleware servers are started.
Test and development servers	900 seconds	Test and development servers offer secondary services and therefore should only be started after other services have been launched properly.

The values presented in Table 10-1 provide an example of what you should consider when preparing VMs to run on host servers.

Understanding Guest Failover Clustering

When it comes to ensuring the high availability of the stateful applications within virtual workloads, most organizations opt to run single-site clusters because they are often easiest to create in the virtual infrastructure and they do not require a replication engine, which must often be procured from third-party sources. When you create single-site guest clusters, you therefore need to consider a few key points:

- **Use anti-affinity rules** If you create a two-node VM cluster to run on top of a host cluster, you must make sure the two nodes of the virtual machine cluster are not located on the same node of the host cluster. If both nodes of your VM cluster end up on the same node of the host cluster and that node fails, your entire VM cluster will fail and you will not gain any advantage from having created a VM cluster. You control VM location on host nodes through anti-affinity rules—or even better, by placing each node of the VM cluster on different host clusters. Anti-affinity rules are set using the Cluster.exe command. The actual attribute for the anti-affinity class can be any text value as long as it is absolutely unique in your network. For example, to set an anti-affinity rule using the Separate01 value for the VM01 group in the HostCluster cluster, use the following command:

```
cluster HostCluster group "VM01" /prop AntiAffinityClassNames="Separate01"
```

MORE INFO SETTING ANTI-AFFINITY RULES

Anti-affinity rules were introduced to Failover Clustering in Windows Server 2003 and continue to be available in Windows Server 2008. Find out more at <http://support.microsoft.com/kb/296799> and <http://support.microsoft.com/kb/299631> as well as [http://msdn.microsoft.com/en-us/library/aa369651\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa369651(VS.85).aspx).

- **Rely on virtual local area networks (VLANs)** Rely on the guest VLAN capabilities of Hyper-V to segregate the intra-cluster traffic required for the guest cluster from other traffic. Each virtual network adapter in a virtual machine can use a different VLAN (see Figure 10-7).
- **Rely on iSCSI storage** To target shared storage for your guest clusters, you should rely on iSCSI storage. iSCSI storage lets you create shared storage infrastructures that rely on network interfaces to access the storage. iSCSI shared storage can be consumed by VMs because they only need network adapters to access the storage.

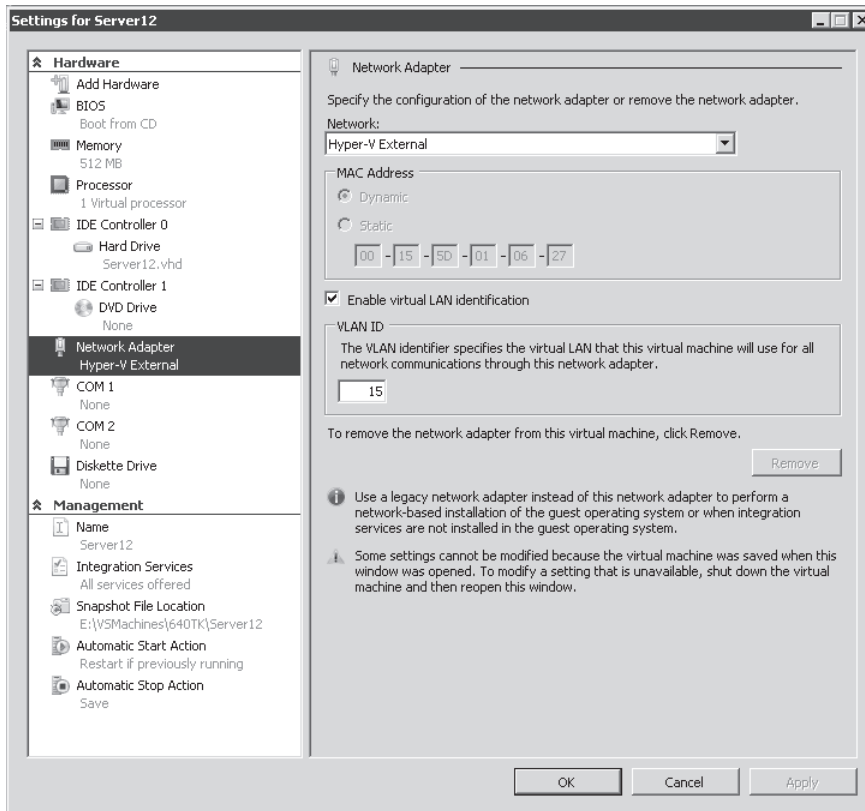


FIGURE 10-7 Assigning VLAN settings to a guest network adapter

Using these three approaches, you can configure single-site guest failover clusters and have them run in the virtual layer of the resource pool (see Figure 10-8). Note that because you need a network for private cluster traffic, you need a network for iSCSI storage and you need a network for public end-user traffic inside each VM in the cluster, you must configure several virtual network adapters in the VM and on the host servers.

IMPORTANT HYBRID CLUSTERS

Note that you can also run hybrid clusters or clusters that include one node as a physical machine and one node as a virtual machine. Hybrid clusters are useful for applications that you want to make highly available but may continue to require a physical footprint. Hybrid clusters are considerably less expensive than full, physical clusters.

When a failure occurs in a host server where one node of the guest cluster is running, the second node will discover the failure of the guest VM and automatically transfer the application within the VM to the other node in the guest cluster. End users will not experience downtime during this transfer (see Figure 10-9).

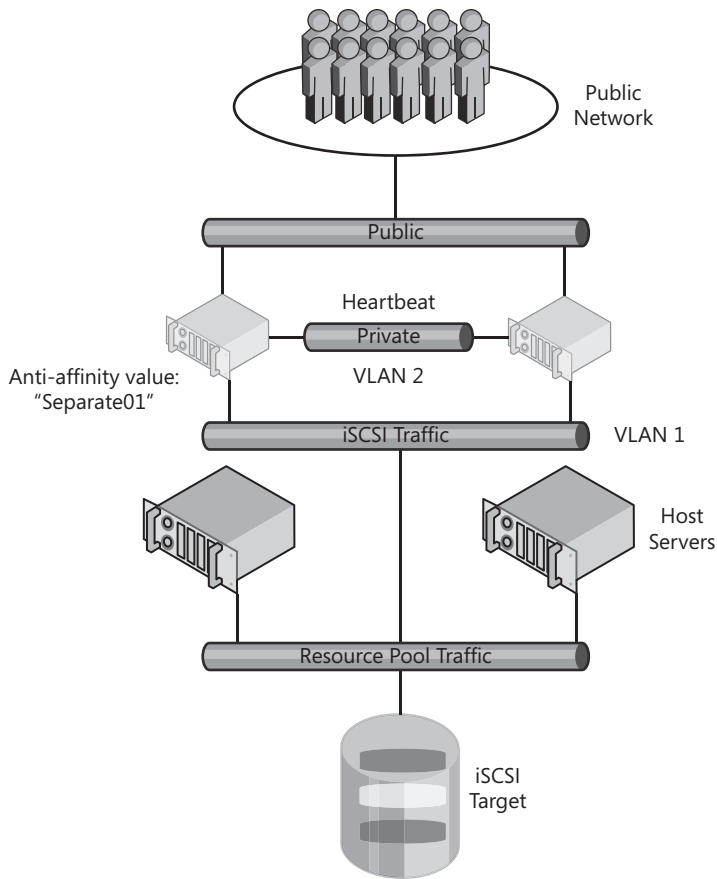


FIGURE 10-8 Creating single-site guest failover clusters

NOTE GUEST CLUSTER FAILOVERS

When an application running in a failover cluster is moved from one node to another, there may be a slight delay in response time for end users working with the application. However, this delay usually lasts only a few microseconds—depending on the application—and will often be imperceptible to end users.

Working with VLANs in Hyper-V

VLAN tagging allows you to segregate traffic within networks simply by assigning a special VLAN number or tag to each network adapter. When the network adapter transfers information to other network connections, the information only flows along the special VLAN channel you have set. In this way, the same network infrastructure can handle multiple streams of data, each along its own channel, protecting and segregating traffic within the infrastructure.

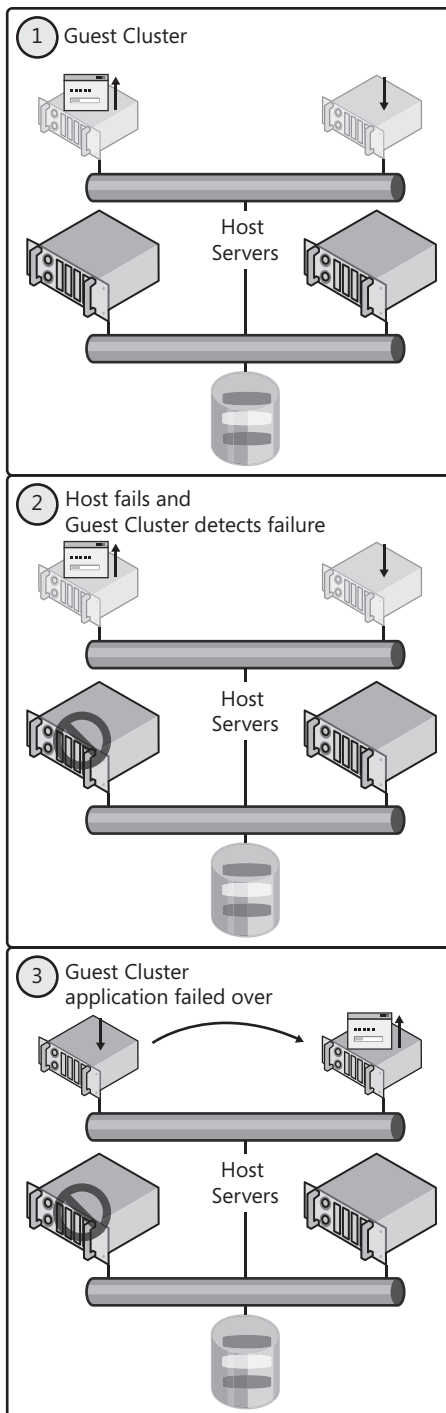


FIGURE 10-9 Guest application failover during a host failure

VLAN tagging is based on the Institute of Electrical and Electronics Engineers (IEEE) standard 802.1Q and is designed to control traffic flow by isolating traffic streams from one another. (See <http://standards.ieee.org> for more information.) Isolated streams cannot connect with each other unless a router is linked to each stream and the router includes a route that links both together. In this way, you can have a machine linked to VLAN_1 and another linked to VLAN_2, and if there is no route between the two, neither machine will be able to view the other's traffic.

VLANs can be set up in two ways:

- **Static VLANs** In a static VLAN, you assign static VLAN IDs to each port in a network switch. All traffic that flows through a specific port is then tagged with the VLAN attached to that port. This approach centralizes VLAN control; however, if you move a computer connection from one port to another, you must make sure the new port uses the same VLAN ID or the computer's traffic will no longer be on the same VLAN.
- **Dynamic VLANs** In a dynamic VLAN, you assign VLAN IDs at the device level. To do so, your devices must be 802.1Q aware; that is, they must support VLAN tagging at the device level.

Hyper-V supports dynamic VLAN tagging. This allows Hyper-V to support traffic isolation without requiring a multitude of physical adapters on the host server. Note, however, that the physical adapters on the host server must support 802.1Q even if you don't assign a VLAN to the adapter itself.

VLANs can be assigned at three different levels in Hyper-V:

- You can assign a VLAN ID to the physical adapter itself. If the adapter supports 802.1Q, you can assign a VLAN ID as part of the driver configuration for the adapter. You do this by clicking the Configure button in the driver's Properties dialog box and using the values available on the Advanced tab (see Figure 10-10). This isolates the traffic on the physical adapter.

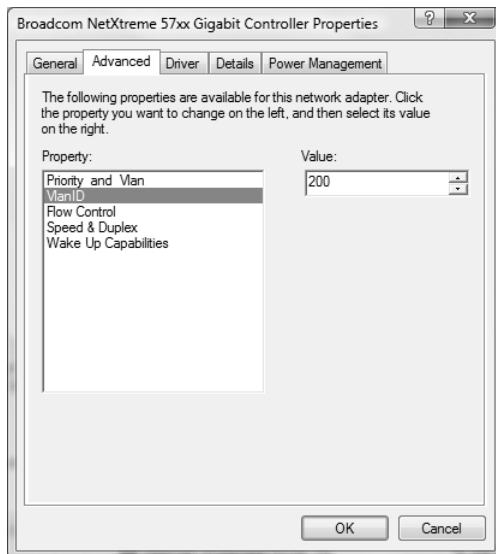


FIGURE 10-10 Configuring a VLAN ID on a physical adapter

- You can assign a VLAN ID to the parent partition when configuring either external or internal virtual network adapters (see Figure 10-11). You do this by setting the value as a property of the virtual adapter in the Virtual Network Manager. This isolates the traffic for the parent partition.

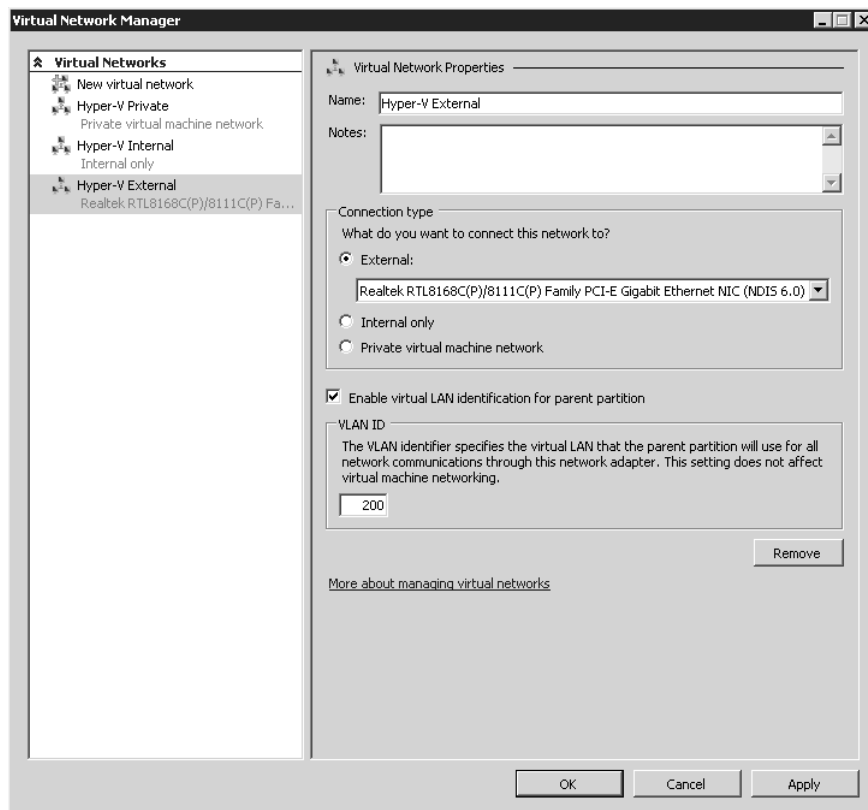


FIGURE 10-11 Configuring a VLAN ID for the parent partition on an external adapter

- You can assign a VLAN ID to child partitions by setting the value as part of the configuration of the virtual network adapter the VM is attached to (see Figure 10-7, shown earlier in the chapter). You do this by setting the VLAN ID as part of the virtual machine's attached network adapter settings. This isolates the traffic for the VM itself. Each virtual network adapter can be assigned to a different VLAN ID.

In all three cases, the switch ports that the physical adapters are attached to must support the VLAN ID you assigned; otherwise, the traffic will not route properly.

VLAN tagging is very useful in Hyper-V because it can be used to segregate traffic at multiple levels. If you want to segregate parent partition and utility domain traffic (as discussed in Chapter 8) and you do not have a separate physical adapter to assign to the process, you can use VLAN tagging for the parent partition and the virtual machines that are part of the resource pool. If you want to create a guest failover cluster and you want to isolate the traffic

for the private network, you can assign a VLAN ID to one of the virtual network adapters in the VM. Make sure, however, that your entire infrastructure can support the process.

Ideally, you will focus on only parent partition VLAN tagging and virtual machine VLAN tagging and omit using physical adapter VLAN tagging when you work with Hyper-V. This simplifies VLAN use and keeps all VLAN values within the Hyper-V configuration environment. In addition, all VLAN traffic is then managed by the Hyper-V virtual network switch.

MORE INFO VLAN TAGGING IN HYPER-V

For more information on VLAN tagging in Hyper-V, look up Microsoft Consulting Services Adam Fazio's blog at <http://blogs.msdn.com/adamfazio/archive/2008/11/14/understanding-hyper-v-vlans.aspx>.



EXAM TIP VLAN TAGGING IN HYPER-V

Remember that for a VLAN to work in Hyper-V, the physical adapter must support the 802.1Q standard; otherwise, the traffic will not flow even if you set all configurations properly at the VM level.

As a best practice, you should rely on the network address you assign to the adapters—physical or virtual—as the VLAN ID for the network. For example, if you assign IPv4 addresses in the 192.168.100.x range, use 100 as the VLAN ID; if you use addresses in the 192.168.192.x range, assign 192 as the VLAN ID, and so on. This will make it easier to manage addressing schemes in your virtual networks.

Configuring iSCSI Storage

When you work with iSCSI storage, you rely on standard network adapters to connect remote storage to a machine. All storage traffic moves through the network adapters. Storage is provisioned and offered for consumption to endpoint machines by an iSCSI target—a storage container running an iSCSI interpreter so that it can receive and understand iSCSI commands. An iSCSI target can be either the actual device offering and managing the storage, or it can be a bridge device that converts IP traffic to Fibre Channel and then relies on Fibre Channel Host Bus Adapters (HBAs) to communicate with the storage container. iSCSI target storage devices can be SANs that manage storage at the hardware level or they can be software engines that run on server platforms to expose storage resources as iSCSI targets.

MORE INFO iSCSI TARGET EVALUATION SOFTWARE

You can use several products to evaluate iSCSI targets as you prepare to work with highly available VMs. Microsoft offers two products that support iSCSI targets: Windows Storage Server 2003 R2 and Windows Unified Data Storage Server 2003. Both can be obtained as evaluations for use as iSCSI targets from <http://microsoft.download-ss.com/default.aspx?PromoCode=WSREG096&PromoName=elbacom&h=elbacom>. A registration process is required for each evaluation product you select.

You can also obtain an evaluation version of StarWind Server from Rocket Division Software to create iSCSI targets for testing virtual machine clustering. Obtain the free version from http://rocketdivision.com/download_starwind.html. The retail version of StarWind Server lets you create iSCSI targets from either physical or virtual machines running Windows Server software and including multiple disks. This greatly simplifies cluster constructions in small environments because you do not require expensive storage hardware to support failover clustering.

iSCSI clients run iSCSI Initiator software to initiate requests and receive responses from the iSCSI target (see Figure 10-12). If the iSCSI target is running Windows Server 2003, you must download and install the iSCSI Initiator software from Microsoft. If the client is running Windows Server 2008, the iSCSI Initiator software is included within the operating system. Because iSCSI storage traffic is transported over network adapters, you should try to install the fastest possible adapters in your host servers and reserve them for iSCSI traffic in VMs.

MORE INFO iSCSI INITIATOR SOFTWARE

You can also obtain the Windows Server 2003 iSCSI Initiator software from <http://www.microsoft.com/downloads/details.aspx?familyid=12cb3c1a-15d6-4585-b385-befd1319f825&displaylang=en>. Also, look up the iSCSI Initiator User's Guide at <http://download.microsoft.com/download/A/E/9/AE91DEA1-66D9-417C-ADE4-92D824B871AF/uGuide.doc>.

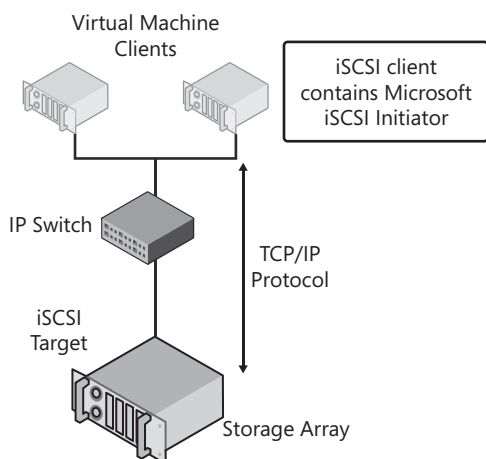


FIGURE 10-12 iSCSI Clients initiate requests that are consumed by iSCSI targets.

Installing and configuring the iSCSI Initiator is very simple. If you are using Windows Server 2003, you must begin by downloading and installing the Microsoft iSCSI Initiator, but if you are working with Windows Server 2008, the iSCSI Initiator is already installed and ready to run. You can find the iSCSI Initiator shortcuts in two locations on Windows Server 2008: in

Control Panel under Classic View or in Administrative Tools on the Start menu. To configure a machine to work with iSCSI storage devices, begin by configuring an iSCSI target on the storage device and then use the following procedure on the client. Note that you need local administrator access rights to perform this operation.

1. Launch the iSCSI Initiator on the client computer. If this is the first time you are running the Initiator on this computer, you will be prompted to start the iSCSI service. Click Yes. This starts the service and sets it to start automatically.
2. You are prompted to unblock the iSCSI service (see Figure 10-13). Click Yes. This opens TCP port 3260 on the client computer to allow it to communicate with the iSCSI target. This launches the iSCSI Initiator Properties dialog box and displays the General tab.



FIGURE 10-13 Unblocking the iSCSI Service on the client computer

3. Click the Discovery tab, click Add Portal, type in the IP address of the iSCSI target, make sure port 3260 is being used, and click OK.
4. Click the Targets tab. The iSCSI target you configured should be listed. Click Log On, select Automatically Restore This Connection When The Computer Starts, and then click OK. Note that you can also configure Multi-Path I/O (MPIO) in this dialog box (see Figure 10-14). MPIO is discussed later in the chapter. Leave it as is for now. Repeat the logon process for each disk you want to connect to. Each disk is now listed with a status of Connected.

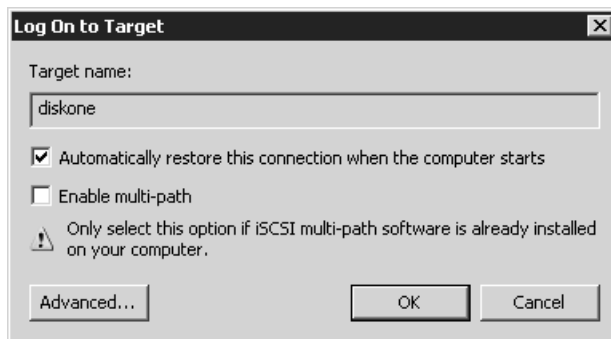


FIGURE 10-14 Logging on to the remote disk

5. Click the Volumes And Devices tab and then click Autoconfigure. All connected disks now appear as devices. Click OK to close the iSCSI Initiator Properties dialog box.

6. Reboot the cluster node to apply your changes. Repeat the procedure on the other node(s) of the cluster.
7. When the nodes are rebooted, expand the Storage node and then expand the Disk Management node of the Tree pane in Server Manager. The new disks appear offline. Right-click the volume names and click Online to bring the disks online.

You can now proceed to the creation of a cluster. Follow the steps outlined in Lesson 1 of Chapter 3.

MORE INFO CREATING iSCSI CLUSTERS IN HYPER-V

For a procedure outlining how to create an iSCSI cluster in Hyper-V, see the Ireland Premier Field Engineering blog at <http://blogs.technet.com/pfe-ireland/archive/2008/05/16/how-to-create-a-windows-server-2008-cluster-within-hyper-v-using-simulated-iscsi-storage.aspx>. For more information on iSCSI in general, see the Microsoft TechNet iSCSI landing page at <http://www.microsoft.com/windowsserver2003/technologies/storage/iscsi/default.mspx>. For a discussion on how to use the Windows Unified Data Storage Server evaluation as an iSCSI target for the creation of virtual machine clusters, see <http://blogs.technet.com/josebda/archive/2008/01/07/installing-the-evaluation-version-of-wudss-2003-refresh-and-the-microsoft-iscsi-software-target-version-3-1-on-a-vm.aspx>.



EXAM TIP THE iSCSI INITIATOR

Make sure you understand how to work with the iSCSI Initiator because it is an important part of the exam. If you do not have access to iSCSI target devices, you can always download the evaluation copy of StarWind Server from Rocket Division Software, as mentioned earlier.

MORE INFO USING THE INTERNET STORAGE NAME SERVICE (iSNS)

Windows Server also includes support for iSNS. This service is used to publish the names of iSCSI targets on a network. When you use an iSNS server, then the iSCSI Initiator will obtain target names from the list the iSNS server publishes instead of having them statically configured in each client once the address of the iSNS server has been added to the iSCSI Initiator configuration.

Understanding iSCSI Security

Transferring storage data over network interface cards (NICs) can be a risky proposition on some networks. This is one reason the iSCSI Initiator includes support for several security features that allow you to encrypt the data between the iSCSI client and the target. You can use three methods to secure client/target communications:

- **CHAP** The Challenge-Handshake Authentication Protocol (CHAP) is a protocol that authenticates peers during connections. Peers share a password or secret. The secret must be entered in each peer of the connection along with a user name that must

also be the same. Both the secret and the user name are shared when connections are initiated. Authentication can be one-way or mutual. CHAP is supported by all storage vendors supporting the Microsoft iSCSI implementation. If targets are made persistent, the shared secret is also made persistent and encrypted on client computers.

- **IPsec** The IP Security Protocol (IPsec) provides authentication and data encryption at the IP packet layer. Peers use the Internet Key Exchange (IKE) protocol to negotiate the encryption and authentication mechanisms used in the connection. Note that not all storage vendors that support the Microsoft iSCSI implementation provide support for IPsec.
- **RADIUS** The Remote Authentication Dial-In User Service (RADIUS) uses a server-based service to authenticate clients. Clients send user connection requests to the server during the iSCSI client/target connection. The server authenticates the connection and sends the client the information necessary to support the connection between the client and the target. Windows Server 2008 includes a RADIUS service and can provide this service in larger iSCSI configurations.

Because CHAP is supported by all vendors, it tends to be the security method of choice for several iSCSI implementations.

MORE INFO iSCSI SECURITY MODES

For more information on supported iSCSI security modes, go to <http://technet.microsoft.com/en-us/library/cc754658.aspx>.

In the case of CHAP and IPsec, however, the configuration of iSCSI security is performed on the General tab of the iSCSI Initiator Properties dialog box (see Figure 10-15). To enter the CHAP secret, click Secret. To configure IPsec settings, click Set Up. Make sure the same settings have been configured on the iSCSI target; otherwise, your iSCSI connections will fail. Note that the General page of the iSCSI Properties dialog box also lets you change the name of the Initiator. In most cases, the default name is fine because it is based on a generic name followed by the server name that differentiates it from other iSCSI Initiator names. Note, however, that the Internet Qualified Name (IQN) used by initiators and targets must be unique in all instances.

You can configure more advanced security settings on the Targets tab under the Log On button when you click Advanced (see Figure 10-16). Both CHAP and IPsec advanced settings are available in this dialog box. This is also where you can enable the use of RADIUS servers.

When you implement iSCSI storage for virtual machines, make sure you secure the traffic—these machines are running public end-user services and the storage traffic carries valuable information over the network. Also keep in mind that you can combine the security features of iSCSI for more complete protection. For example, you can use CHAP for authentication and IPsec for data encryption during transport.

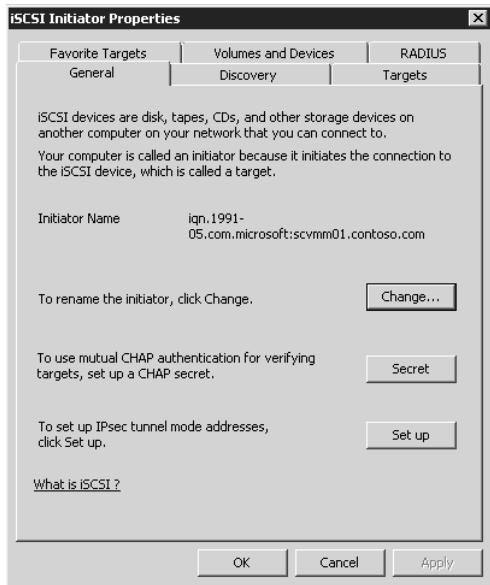


FIGURE 10-15 The General page of the iSCSI Initiator properties

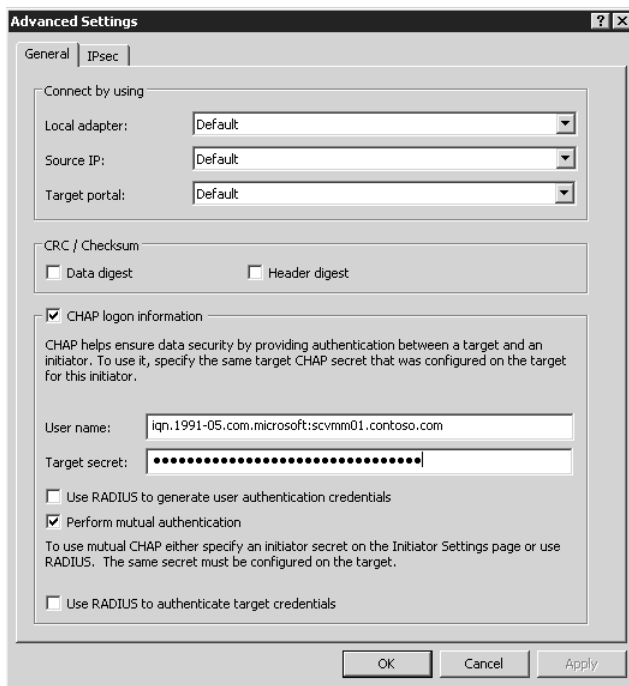


FIGURE 10-16 Using advanced CHAP or IPsec configurations

IMPORTANT ENABLING iSCSI ON SERVER CORE

When you work with Server Core, you do not have access to the graphical interface for iSCSI configuration. In this case, you must use the `iscsicli.exe` command to perform iSCSI configurations. You can type `iscsicli /?` at the command prompt to find out more about this command. In addition, you will need to enable iSCSI traffic through the Windows Firewall on client servers. Use the following command to do so:

```
netsh advfirewall firewall set rule "iSCSI Service (TCP-Out)" new enable=yes
```

Understanding Guest Network Load Balancing

Network Load Balancing is not a high-availability solution in the same way as failover clustering. In a failover cluster, only one node in the cluster runs a given service. When that node fails, the service is passed on to another node and at that time that node becomes the owner of the service. This is due to the shared-nothing cluster model that Windows Server Failover Clustering relies on. Because of this model, only one node can access a given storage volume at a time and therefore the clustered application can only run on a single node at a time.

UPDATE ALERT CLUSTER SHARED VOLUMES

It is precisely the shared-nothing model that is changed in Windows Server 2008 R2 to support live virtual machine migrations in Hyper-V. CSVs use a shared-everything model that allows all cluster nodes to “own” the shared storage volume. Note that this shared-everything model through CSVs is only available for clusters running Hyper-V. All other clustered applications will continue to use the shared-nothing model.

In NLB clusters, every single member of the cluster offers the same service. Users are directed to a single NLB IP address when connecting to a particular service. The NLB service then redirects users to the first available node in the cluster. Because each member in the cluster can provide the same services, services are usually in read-only mode and are considered stateless.

IMPORTANT CREATING GUEST NLB CLUSTERS

When you create a guest NLB cluster, you should apply a hotfix to the guest operating system otherwise the NLB.sys driver may stop working. Find out more on this issue at <http://support.microsoft.com/kb/953828>.

NLB clusters are fully supported in Hyper-V virtual machines because the Hyper-V network layer provides a full set of networking services, one of which is NLB redirection. This means that you can create multi-node NLB clusters (up to 32) to provide high availability for the services you make available in your production virtual machines. Note, however, that each computer participating in an NLB cluster should include at least two network adapters: one for management traffic and the other for public traffic. This is very simple to do in virtual machines—just add another virtual network adapter. Enlightened machines can

include up to 12 network adapters: 8 enlightened network adapters and 4 legacy network adapters. Keep in mind, however, that for performance reasons you should avoid mixing machines using legacy network adapters with machines using enlightened network adapters on the same host. Or at the very least, you should connect all of your legacy network adapters to a separate physical adapter to segregate legacy network traffic from enlightened network traffic.

Determining Which High Availability Strategy to Use for VMs

As you can see, you can use three different high-availability strategies for VMs. Each is a valid approach and each provides sound support for making your VMs highly available. However, it is not always evident which method you should use for which application. Table 10-2 outlines some considerations for choosing and implementing a high-availability solution for your production VMs.

TABLE 10-2 Choosing a High Availability Method for a VM

VIRTUAL MACHINE CHARACTERISTICS	HOST SERVER CLUSTERING	FAILOVER CLUSTERING	NLB
Windows Server 2008 edition	Web Standard Enterprise Datacenter	Enterprise Datacenter	Web Standard Enterprise Datacenter
Number of guest nodes	Single nodes only	Usually 2, but up to 16	Up to 32
Required resources	At least one virtual network adapter	iSCSI disk connectors Minimum of three virtual network adapters: Cluster Public, Cluster Private, and iSCSI	Minimum of two virtual network adapters
Potential server role	Any server role	Application servers (stateful) File and print servers Collaboration servers (storage) Network infrastructure servers	Application servers (stateless) Dedicated Web servers Collaboration servers (front end) Terminal servers (front end)
Internal VM application	Any application	SQL Server computers Exchange mailbox servers Message queuing servers	Web Farms Exchange Client Access Servers Internet Security and Acceleration Server (ISA)

VIRTUAL MACHINE CHARACTERISTICS	HOST SERVER	FAILOVER CLUSTERING	NLB
	CLUSTERING		
		Message queuing servers	Virtual Private Network (VPN) servers
		File servers	Streaming Media servers
		Print servers	Unified Communications servers
			App-V servers

The guidelines in Table 10-2 will assist you in your selection of a high-availability solution for your production virtual machines. However, keep in mind that you should always aim to create host failover clusters at the very least. This is because each host runs a vast number of production VMs and if that host fails and there is no high-availability solution, each and every one of the VMs on the host will fail. This is a different situation than when you run single workloads in individual physical machines. Nothing prevents you from running a host-level cluster and at the same time running a guest-level high-availability solution such as failover clustering or Network Load Balancing.

You can use the guidelines in Table 10-2 as well as your existing organization's service-level requirements to determine which level of high availability you want to configure for each VM. You also need to take into account the support policy for the application you intend to run in the VM. Support policies are discussed later in this chapter.

Configuring Additional High-Availability Components for VMs

Even though you create high-availability configurations for your VMs at both the host and the guest level, you should also consider which additional components you need to run a problem-free (or at least as problem-free as possible) virtual workload network. In this case, consider the following:

- Configure VM storage redundancy. Use the following best practices:
 - Make sure your storage array includes high-availability configurations such as random arrays of independent disks (RAID). Apply this at both the host and the VM level whenever a computer needs to connect to shared storage.
 - Try to use separate pools of spindles for each storage or iSCSI target to provide the best possible I/O speeds for your host servers.
 - If you are using iSCSI at the host or the guest level, you can also rely on MPIO to ensure high availability of data by using multiple different paths between the CPU on the iSCSI client and the iSCSI target where the data is physically located. This ensures data path redundancy and provides better availability for client virtual machines. When you select this option in the iSCSI Initiator, the MPIO files and the iSCSI Device Specific Module will be installed to support multi-pathing.
- Configure VM networking redundancy. Use the following best practices:

- Make sure your host servers include several network adapters. Dedicate at least one to host management traffic.
- Use the highest-speed adapters available on your host servers to provide the best level of performance to VMs.
- Create at least one of each type of virtual network adapter on your host servers.
- Use VLAN tagging to protect and segregate virtual networking traffic and to separate host-management traffic from virtual networking traffic. Make sure the VLANs you use on your host servers and VMs are also configured in your network switches; otherwise, traffic will not flow properly.
- Configure VM CPU redundancy. Use host servers that include multiple CPUs or CPU cores so that multiple cores will be shareable between your VMs.
- Configure VMs for RAM redundancy. Use host servers that include as much RAM as possible and assign appropriate amounts of RAM to each VM.
- Finally, monitor VM performance according to the guidelines provided in Lesson 3 of Chapter 3. Adjust VM resources as required as you discover the performance levels they provide.

If you can, rely on SCVMM and its PRO feature to continuously monitor VM performance and obtain PRO tips on VM reconfiguration. Remember that the virtual layer of your resource pool is now running your production network services and it must provide the same or better level of service as the original physical network; otherwise, the gains you make in reduced hardware footprints will be offset by the losses you get in performance.

Creating Supported VM Configurations

When you run production services in virtual machines, you want to make sure that the configuration you are using is a supported configuration; otherwise, if issues arise, you might need to convert the virtual machine into a physical machine before you can obtain support from the product's vendor. As a vendor of networking products and services, Microsoft publishes support articles on acceptable virtual machine configurations for its products. As a resource pool administrator, you should take these configurations into consideration when you prepare your virtual machines.

Table 10-3 outlines the different Microsoft products, applications, and server roles that are supported to run in virtual environments. Three environments are supported:

- **Windows Server with Hyper-V** Hyper-V supports 32-bit or 64-bit guest operating systems.
- **Microsoft Hyper-V Server** Also runs 32-bit or 64-bit guest operating systems. However, Hyper-V Server does not support failover clustering.
- **Server Virtualization Validation Program (SVVP) certified third-party products** Third-party hypervisors that have been certified through the SVVP can run either 32-bit or 64-bit VMs. This includes VMware and Citrix hypervisors, among others.

MORE INFO SVVP

For more information on the Server Virtualization Validation Program, go to <http://www.windowsservercatalog.com/svvp.aspx>.

In some cases, Microsoft also supports running the application in a Virtual Server 2005 R2 environment. Note, however, that only 32-bit applications can run on this platform. This is why Hyper-V is the preferred virtualization platform.

Specific articles outlining the details of the supported configuration are listed in Table 10-3 if they are available.

MORE INFO SUPPORTED MICROSOFT APPLICATIONS IN VMs

The information compiled in Table 10-3 originates from Microsoft Knowledge Base article 957006 as well as other sources. This article is updated on a regular basis as new products are added to the support list. Find this article at <http://support.microsoft.com/kb/957006>.

TABLE 10-3 Microsoft Applications Supported for Virtualization

PRODUCT	COMMENTS	KB ARTICLE
Active Directory	Domain Controllers can run in VMs.	See article number 888794: http://support.microsoft.com/kb/888794
Application Virtualization	Management Servers, Publishing Servers, Terminal Services Client, and Desktop Clients from version 4.5 and later can run in VMs.	
BizTalk Server	Versions 2006 R2, 2006, and 2004 are supported.	See article number 842301: http://support.microsoft.com/kb/842301
Commerce Server	Versions 2007 with SP2 and later are supported. Version 2002 can also run in a VM.	See article number 887216: http://support.microsoft.com/kb/887216
Dynamics AX	Versions 2009 and later server and client configurations are supported.	
Dynamics GP	Versions 10.0 and later are supported.	See article number 937629: http://support.microsoft.com/kb/937629
Dynamics CRM	Versions 4.0 and later are supported.	See article number 946600: http://support.microsoft.com/kb/946600

PRODUCT	COMMENTS	KB ARTICLE
Dynamics NAV	Versions 2009 and later are supported.	
Exchange Server	Versions 2003, 2007 with SP1, and later are supported.	See article number 320220: http://support.microsoft.com/kb/320220 or see the Microsoft TechNet Web page at http://technet.microsoft.com/en-us/library/cc794548.aspx
Forefront Client Security	Service pack 1 and higher are supported.	
Forefront Security for Exchange	Service Pack 1 or higher are supported.	
Forefront Security for SharePoint	Service Pack 2 or higher are supported.	
Host Integration Server	Versions 2006 and later are supported.	
Intelligent Application Gateway	2007 with SP2 and later are supported.	
Internet Security and Acceleration Server	Versions 2006 and later are supported.	See the Microsoft TechNet Web page at http://technet.microsoft.com/en-us/library/cc891502.aspx
Office Groove Server	Versions 2007 with SP1 and later are supported.	
Office PerformancePoint Server	Versions 2007 with SP2 and later are supported.	
Office Project Server	Versions 2007 with SP1 and later are supported.	See article number 916533: http://support.microsoft.com/kb/916533
Office SharePoint Server	Versions 2007 with SP1 and later are supported.	See article number 909840: http://support.microsoft.com/kb/909840
Operations Manager	Only the agents from version 2005 with SP1 are supported. See System Center OpsMgr for other supported versions.	See article number 957559: http://support.microsoft.com/kb/957559
Search Server	Versions 2008 and later are supported.	

PRODUCT	COMMENTS	KB ARTICLE
SQL Server	Versions 2005, 2008, and later are supported.	See article number 956893: http://support.microsoft.com/kb/956893
System Center Configuration Manager	All components from version 2007 with SP1 and later are supported.	See the Microsoft TechNet Web page at http://technet.microsoft.com/en-us/library/bb680717.aspx
System Center Data Protection Manager	Versions 2007 and later are supported, but for agent-side backup only.	
System Center Essentials	Versions 2007 with SP1 and later are supported.	
System Center Operations Manager	All components from version 2007 and later are supported.	See the Microsoft TechNet Web page at http://technet.microsoft.com/en-us/library/bb309428.aspx . Also see article number 957568: http://support.microsoft.com/kb/957568
Microsoft System Center Virtual Machine Manager	All components from version 2008 and later are supported.	
Systems Management Server	Only the agents from version 2003 with SP3 are supported. See System Center Configuration Manager for other supported versions.	See the Microsoft TechNet Web page at http://technet.microsoft.com/en-us/library/cc179620.aspx
Visual Studio Team System	Versions 2008 and later are supported.	
Windows 7	Windows 7 is supported.	
Windows Essentials Business Server	Versions 2008 and later are supported.	
Windows HPC Server	Versions 2008 and later are supported.	
Windows Small Business Server	Versions 2008 and later are supported.	
Windows Server Web edition	Versions 2003 with SP2, 2008, and later are supported.	
Windows Server, other editions	2000 Server with SP4, 2003 with SP2, and 2008 or later are supported.	

PRODUCT	COMMENTS	KB ARTICLE
Windows Server Update Services	Versions 3.1 and later are supported.	
Windows SharePoint Services	Versions 3.0 with SP1 and later are supported.	See article number 909840: http://support.microsoft.com/kb/909840
Windows Vista	Vista is supported.	
Windows XP	XP with SP2 (x86 and x64 editions) and XP with SP3 (x86 editions) are supported.	

As you can see, the list of products Microsoft supports for operation in the virtual layer is continually growing. Products that do not have specific configuration articles are supported in standard configurations as per the product documentation. This also applies to the vast majority of Windows Server roles—all roles are supported because Windows Server itself is supported. However, only Active Directory Domain Services rates its own support policy.

Supported configurations run from standalone implementations running on host failover clusters to high-availability configurations at the guest level. Remember, however, that you need to take a product's licensing requirements into account when creating virtual machine configurations for it. For example, both Small Business Server and Essential Business Server can run in virtual configurations, but they will not run on host failover clusters unless you acquire a different license for the host server because the license for these products is based on the Standard edition of Windows Server. The license for the Standard edition includes support for installation of Windows Server 2008 on one physical server and one virtual machine, but it does not include support for failover clustering. Read the support articles closely if you want to create the right configurations for your network. If a support article does not exist, read the product's configuration documentation to determine how best to deploy it in your network.

In addition, Microsoft has begun to use virtualization technologies at two levels for its own products:

- Virtual labs allow you to go to the Microsoft Web site and evaluate a given technology online.
- Evaluation VHDs include a preconfigured version of an application in a downloadable VHD file.

Table 10-4 outlines the evaluation VHDs that are available for Microsoft products. As you have seen throughout the exercises you performed in this guide, evaluation VHDs make it much simpler to deploy a networking product into your environment because you do not need to install the product. All you need to do is configure a VM to use the VHD and then configure the product within the VHD to run in your network. Then, if you choose to continue working with the product, all you need to do is acquire a license key for it and add it to the configuration to turn it into a production machine.

In addition, Table 10-4 points you to online virtual labs if they exist for the same product.

MORE INFO MICROSOFT APPLICATIONS AVAILABLE IN VHDs

Some of the information in Table 10-4 was compiled from the evaluation VHD landing page at <http://technet.microsoft.com/en-us/bb738372.aspx>. Watch this page to find more VHDs as they become available.

TABLE 10-4 Microsoft Evaluation VHDs

PRODUCT	EVALUATION VHD	VIRTUAL LAB
Exchange 2007 with SP1	http://www.microsoft.com/downloads/details.aspx?FamilyID=44C66AD6-F185-4A1D-A9AB-473C1188954C&displaylang=en	http://technet.microsoft.com/en-us/exchange/bb499043.aspx
Office SharePoint Server 2007	http://www.microsoft.com/downloads/details.aspx?FamilyID=67f93dcb-ada8-4db5-a47b-df17e14b2c74&displaylang=en	http://technet.microsoft.com/en-us/office/sharepointserver/bb512933.aspx
System Center Configuration Manager 2007 R2	http://www.microsoft.com/downloads/details.aspx?FamilyID=e0fadab7-0620-481d-a8b6-070001727c56&displaylang=en	http://msevents.microsoft.com/cui/webcasteventdetails.aspx?eventid=1032343963&eventcategory=3&culture=en-us&countrycode=us
System Center Essentials 2007 SP1	http://www.microsoft.com/downloads/details.aspx?familyid=e6fc3117-48c5-4fd1-a3d2-927eab397373&displaylang=en	
System Center Virtual Machine Manager 2008	http://www.microsoft.com/downloads/details.aspx?FamilyID=4a27e89c-2d73-4f57-a62c-83afb4c953f0&displaylang=en	http://www.microsoft.com/systemcenter/virtualmachinemanager/en/us/default.aspx
Windows 2003 R2 Enterprise edition	http://www.microsoft.com/downloads/details.aspx?FamilyID=77f24c9d-b4b8-4f73-99e3-c66f80e415b6&displaylang=en	http://technet.microsoft.com/en-us/virtuallabs/bb539981.aspx
Windows Server 2008 Enterprise Server Core	http://www.microsoft.com/windowsserver2008/en-us/virtual-hard-drive.aspx	http://technet.microsoft.com/en-us/virtuallabs/bb512925.aspx
Windows Vista	http://www.microsoft.com/downloads/details.aspx?FamilyID=c2c27337-d4d1-4b9b-926d-86493c7da1aa&displaylang=en	http://technet.microsoft.com/en-us/virtuallabs/bb539979.aspx

MORE INFO MICROSOFT APPLICATIONS AVAILABLE IN VIRTUAL LABS

For more information on Microsoft virtual labs, go to <http://technet.microsoft.com/en-us/virtuallabs/default.aspx>.

More and more products will be available in VHDs as time goes by. In fact, the VHD delivery mechanism is likely to become the delivery mechanism of choice for most products as Microsoft and others realize how powerful this model is.

You are now running a virtual infrastructure—production VMs on top of your resource pool—and this infrastructure is the way of the future. Eventually, you will integrate all new products using the VHD—or virtual appliance—model. This will save you and your organization a lot of time as you dynamically add and remove products from your infrastructure through the control of the VMs they run in.

MORE INFO VIRTUAL APPLIANCES

Virtual appliances have been around for some time. In fact, virtual appliances use the Open Virtualization Format (OVF), which packages an entire virtual machine—configuration files, virtual hard disks, and more—into a single file format. Hyper-V does not yet include an import tool for OVF files, but you can use Project Kensho from Citrix to convert OVF files to Hyper-V format. Find Kensho at <http://community.citrix.com/display/xs/Kensho>.

PRACTICE Assigning VLANs to VMs

In this practice, you will configure VMs to work with a VLAN to segregate the virtual machine traffic from your production network. This practice involves four computers: ServerFull01, ServerCore01, Server01, and SCVMM01. Each will be configured to use a VLAN ID of 200. This practice consists of three exercises. In the first exercise, you will configure the host servers to use new VLAN ID. In the second exercise, you will configure the virtual machines to use the VLAN ID. In the third exercise, you will make sure the machines continue to connect with each other.

EXERCISE 1 Configure a Host Server VLAN

In this exercise you will use ServerFull01 and ServerCore01 to configure a VLAN. Perform this activity with domain administrator credentials.

1. Begin by logging on to ServerFull01 and launching the Hyper-V Manager. You can use either the standalone console or the Hyper-V Manager section of Server Manager.
2. Click ServerFull01 in the Tree pane and then click Virtual Network Manager.
3. Select the External virtual network adapter and select the Enable Virtual LAN Identification For Parent Partition check box. Type **200** as the VLAN ID and click OK.

4. Repeat the operation for ServerCore01. Click ServerCore01 in the Tree pane and then click Virtual Network Manager.
5. Select the External virtual network adapter and select the Enable Virtual LAN Identification For Parent Partition. Type **200** as the VLAN ID and click OK.

Your two host servers are now using 200 as a VLAN ID. This means that you have configured the virtual network switch on both host servers to move traffic only on VLAN 200.

EXERCISE 2 Configure a Guest Server VLAN

In this exercise you will configure two virtual machines to use the 200 VLAN as well. Perform this exercise on ServerFull01 and log on with domain administrator credentials.

1. Begin by logging on to ServerFull01 and launching the Hyper-V Manager.
2. Click ServerFull01 in the Tree pane. Right-click Server01 and choose Settings.
3. Select the virtual network adapter for Server01 and select the Enable Virtual LAN Identification check box. Type **200** as the VLAN ID and click OK.
4. Repeat the operation for SCVMM01. Click ServerCore01 in the Tree pane, right-click SCVMM01, and choose Settings.
5. Select the virtual network adapter for SCVMM01 and select the Enable Virtual LAN Identification check box. Type **200** as the VLAN ID and click OK.

Your two virtual machines are now moving traffic only on VLAN 200.

EXERCISE 3 Test a VLAN

In this exercise you will verify that communications are still available between the host servers and the resource pool virtual machines. Perform this exercise from ServerFull01. Log on with domain administrator credentials.

1. Log on to ServerFull01 and launch a command prompt. Click Start and then choose Command Prompt.
2. Use the Command Prompt window to ping each of the machines you just moved to VLAN 200. Use the following commands:

```
ping Server01.contoso.com  
ping SCVMM01.contoso.com  
ping ServerCore01.contoso.com
```

3. You should get a response from each of the three machines. This means that all machines are now communicating on VLAN 200.

As you can see, it is relatively easy to segregate traffic from the resource pool using VLAN IDs. You can use a similar procedure to configure VLAN IDs for guest virtual machines when you configure them for high availability.

✓ Quick Check

1. What are the two types of cluster modes available for host servers?
2. What are the three different options to make workloads contained in virtual machines highly available?
3. What process does the Quick Migration feature use to move a virtual machine from one host cluster node to another?
4. Where can you set the startup delays for virtual machines, and what is the default setting?
5. What is the best tool to use for automatic VM placement on hosts?
6. What type of VLAN does Hyper-V support?
7. What are iSCSI target storage devices?
8. What is the most common protocol used to secure iSCSI implementations?
9. What is the major difference between failover clustering and Network Load Balancing?
10. How many network adapters (both enlightened and legacy network adapters) can be included in enlightened virtual machines?
11. Why is it important to create host failover clusters?

Quick Check Answers

1. The two types of cluster modes available for host servers are single-site clusters and multi-site clusters.
2. The three different options to make workloads contained in virtual machines highly available are:
 - **Create host failover clusters**
 - **Create guest failover clusters**
 - **Create guest NLB clusters**
3. The Quick Migration process moves a VM by saving the state of the VM on one node and restoring it on another node.
4. To set the startup delays for virtual machines, go to the VM configuration settings under the Automatic Start Action settings. By default the startup delay for VMs is set to zero.
5. The best tool to use for automated VM placement is the Performance and Resource Optimization (PRO) with Intelligent Placement feature in SCVMM.
6. Hyper-V supports dynamic VLAN tagging to support traffic isolation without requiring a multitude of physical adapters on the host server.

- 7.** iSCSI target storage devices can be SANs that manage storage at the hardware level or they can be software engines that run on server platforms to expose storage resources as iSCSI targets.
- 8.** CHAP is supported by all vendors; as such, it tends to be the security method of choice for several iSCSI implementations.
- 9.** In a failover cluster, only one node in the cluster runs a given service. In NLB every single member of the cluster offers the same service.
- 10.** Enlightened virtual machines can include up to 12 network adapters: 8 enlightened network adapters and 4 legacy adapters.
- 11.** You create host failover clusters because each host runs a vast number of production VMs and if the host fails and you have no high-availability solution, each VM on the host will also fail.

Case Scenario: Protecting Exchange 2007 VMs

In the following case scenario, you will apply what you have learned about creating supported VM configurations. 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. You have recently moved to a virtual platform running on Windows Server Hyper-V and you have converted several of your physical machines to virtual machines. You are now ready to place your Microsoft Exchange 2007 servers on virtual machines. You want to create a supported configuration for the product so you have read the information made available by Microsoft at <http://technet.microsoft.com/en-us/library/cc794548.aspx>. This article outlines the Microsoft support policy for Exchange Server 2007 in supported environments.

Basically, you have discovered that you need to be running Exchange Server 2007 with SP1 on Windows Server 2008 to virtualize the email service. Microsoft supports standalone Exchange machines in VMs as well as single-site cluster (Single-Site Cluster) and multi-site cluster (Cluster Continuous Replication) configurations. Exchange VMs must be running on Hyper-V or a supported hardware virtualization platform. Lucerne does not use the Unified Messaging role in Exchange; therefore, you don’t need to worry about the fact that you should not virtualize this role.

Exchange is supported on fixed-size virtual disks, pass-through disks, or disks connected through iSCSI. Other virtual disk formats are not supported and neither are Hyper-V snapshots. When you assign resources to the VMs, you must maintain no more than a 2-to-1 virtual-to-logical processor ratio. And most important, the Microsoft Exchange team does not support the Hyper-V Quick Migration feature. Therefore, you should not place an Exchange VM on a host cluster—or if you do, you should not make the VM highly available.

Given all of these requirements, your management has asked you to prepare a report on Exchange virtualization before you proceed to the implementation. Specifically, this report should answer the following three questions. How do you proceed?

1. How do you configure the disk targets for your Exchange VMs?
2. Which failover clustering model would you use for the Exchange VMs?
3. How do you manage Exchange high-availability operations after the VMs are configured?

Suggested Practices

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

Guest Failover Clusters

- **Practice 1** If you do not have access to iSCSI target hardware, take the time to download one of the evaluation software products that let you simulate iSCSI targets. Then use these targets to generate iSCSI storage within VMs.
- **Practice 2** Use the iSCSI targets you created to create a guest failover cluster. This will give you a better understanding of the way VMs behave when they are configured for high availability at the VM level.
- **Practice 3** Assign VLAN IDs to the network adapters you apply to VMs in your failover cluster to gain a better understanding of how VLAN tagging works in Hyper-V.

Guest NLB Clusters

- **Practice 1** Take the time to create guest NLB clusters. NLB is fully supported in Hyper-V and is a good method to use to provide high availability for applications you run inside virtual machines.

Supported VM Configurations

- **Practice 1** Take the time to look up the support policies listed in Table 10-3 before you move your own production computers into virtual machines. This will help you create a fully supported virtual infrastructure and ensure that you can acquire support from the vendor if something does go wrong.

Chapter Summary

- Clustered host servers make the virtual machines created on them highly available, but not the applications that run on the virtual machine.
- Host clusters support the continuous operation of virtual machines and the operation of virtual machines during maintenance windows. When a cluster detects that a node is failing, the cluster service will cause the VMs to fail over by using the Quick Migration process, but when a node fails the cluster service will move the VM by restarting it on the other node.
- When you create single-site guest cluster you should consider the following:
 - Use anti-affinity rules to protect the VMs from running on the same node.
 - Rely on VLANs to segregate VM cluster traffic.
 - Rely on iSCSI storage to create shared storage configurations.
- VLANs can be set in two different manners: static or dynamic. Hyper-V supports dynamic VLANs but the network adapters on the host server must support the 802.1Q standard. In Hyper-V VLANs can be assigned to the physical adapter itself, to the parent partition when configuring either external or internal virtual network adapters,

or to child partitions by setting the value as part of the configuration of the virtual network adapter the VM is attached to.

- An iSCSI target can be an actual device offering and managing the storage or it can be a bridge device that converts IP traffic to Fibre Channel and relies on HBA to communicate with the storage container.
- iSCSI clients run iSCSI Initiator software to initiate requests and receive responses for the target.
- iSCSI security includes three methods to secure client/target communications: CHAP, IPsec, and RADIUS.
- Network Load Balancing clusters are fully supported in Hyper-V and can support up to 32 NLB nodes in a cluster, but each computer participating in the NLB cluster should include at least two network adapters—one for management traffic and the other for public traffic.
- You can use three different high-availability strategies for VMs: host server clustering, guest failover clustering, and guest NLB. However, you should always aim to create host failover clusters at the very least.
- Several Microsoft products are supported to run in virtual environments like Windows Server with Hyper-V, Microsoft Hyper-V Server, and SVVP Certified Third-Party products. More will be supported as time goes on.

Glossary

.NET Object An instance of a .NET class that consists of data and the operations associated with that data.

A

Authorization Manager A tool used to manipulate special application-specific credential stores in Windows servers called authorization stores.

B

Backup Schedule A schedule that defines when backups should be performed. This schedule can be daily, weekly, monthly, custom, or a single time.

Basic virtual machine A machine as it is after it has been generated through the Hyper-V New Virtual Machine Wizard.

C

CHAP Challenge-Handshake Authentication Protocol, which authenticates peers during connections.

Child partition A partition that relies on separate memory spaces to host virtual machines.

Clean machine A machine that was cleanly installed and to which the workload has been newly applied.

D

Data collector set A collection of values collated from the local computer—including registry values, performance counters, hardware components, and more—that provides a diagnostic view into the behavior of a system.

Dynamic VLANs VLAN IDs that are assigned at the device level.

E

Enlightened guest operating system An operating system that uses the VMBus to communicate through the parent partition with machines outside the host.

F

Failover cluster A group of independent computers that work together to increase the availability of applications and services.

Fixed resources Settings that cannot be changed when the VM is running.

H

Heterogeneous resource pool Running multiple hypervisors in the resource pool and managing them through SCVMM.

Homogeneous resource pool Running Hyper-V host servers and SCVMM to control them and the VMs they operate in the same resource pool.

Hyper-V server settings These settings include the virtual hard disk and virtual machine location and they apply to the host server as a whole.

Hyper-V user settings These settings apply to each user session and can be different for each user.

Hypercall Adapter An adapter that sits underneath the Xen-enabled Linux kernel and translates all Xen-specific virtualization function calls to Microsoft Hyper-V calls.

Hypervisor An engine that is designed to expose hardware resources to virtualized guest operating systems.

I

Integration Services Special components that Hyper-V provides to enlightened guest operating systems.

IPsec IP Security Protocol, which provides authentication and data encryption at the IP packet layer.

iSCSI Initiator Software that runs on the iSCSI clients to initiate requests and receive responses from the target.

iSCSI Storage A storage container running an iSCSI interpreter so that it can receive and understand iSCSI commands.

L

Legacy machines An operating system that uses emulated device drivers that draw additional resources from the host server and impact performance.

Legacy virtual network adapters These adapter types have to use device emulation to communicate with the virtual networks in Hyper-V. One advantage of this adapter type is that it supports PXE booting because it does not need an installed device driver.

M

Method An action that can be performed on an object.

Multi-homing The inclusion of multiple network adapters in a VM with each adapter linked to a separate network.

Multi-Site cluster A cluster that supports the creation of clustered servers using DAS along with a replication engine to keep the data between cluster nodes in synch.

N

Network Load Balancing (NLB) Implementation of load balancing services to provide high availability and high reliability of stateless services.

O

Object A programming construct that provides a virtual representation of a resource of some type.

Operating system kernel The core part of the operating system that runs at ring 0.

OpsMgr Management Pack A set of monitoring and alerting rules design for a specific application, device, or operating system.

P

P2V Convert physical machines into virtual machines.

Pass-through disk A physical disk partition that is assigned to a virtual machine instead of a virtual hard disk.

Parent partition A system partition that hosts the virtualization stack in support of VM operation.

PDC Emulator Master of Operations A special domain controller role designed to manage time in AD DS networks, among other functions.

Performance and Resource Optimization (PRO) A feature that is available when SCVMM is linked with OpsMgr to perform an updated and ongoing assessment on the host and virtual machines.

Production Host Environment Hyper-V hosts are in production mode and can support the operation of any type of VM.

R

RADIUS The Remote Authentication Dial-In User Service, which authenticates clients by using a server-based service.

Resource pool administrators Resource pool administrators manage all of the hardware that is required to maintain and support virtual workloads or virtual service offerings as well as perform pre-virtualization assessments and migration activities.

S

SCVMM Library A special data store that includes the components needed to generate and build new virtual machines.

Self-Service Portal A Web page running an ASP.NET application in support of users creating and managing their own VMs.

Single-Site cluster A cluster based on shared storage in the form of either SAN or iSCSI targets.

Stateful Services Supports the modification of the information that it manages; however, only one machine node can change the information at a time.

Stateless Services The user cannot modify information and only views it in read-only mode.

Static VLANs VLAN IDs that are assigned to each port in a network switch and are independent of the network adapters in the computers.

Storage Pool The location where SCDPM stores all the data.

SysPrep Windows System Preparation Tool, which depersonalizes a copy of an operating system to support the deployment of a preconfigured operating system.

V

V2V Convert in a non-Hyper-V format into Hyper-V virtual machines.

VMBus The virtual machine bus allows virtual machine devices to communicate with the actual devices

through the parent partition. The VMBus is only used by enlightened guest operating systems.

Variable resources Settings that can be changed when the VM is running.

Verb-Noun A verb associated with a noun and separated with a hyphen.

Virtual Machine Simulated engines that provide support for x86-based operating systems (Windows or Linux) to run on shared hardware. In Hyper-V, virtual machines run in child partitions.

Virtual Service Offerings The networked services that were traditionally run on hardware but that are now virtualized.

Virtualization Service Clients (VSC) Synthetic devices that are installed within the child partition.

Volume Shadow Copy Service VSS is a service that can capture consistent information from running applications. This information can then be used as the source for a backup.

VSS Snapshot Provides a disk image of the state of a VM and relies on this disk image to perform a backup. VSS snapshots can also protect VMS through file server snapshots. VSS snapshots are not to be confused with Hyper-V snapshots.

W

Witness disk A disk in the cluster that is designated to hold a copy of the cluster configuration database.

Index

Symbols and Numbers

.NET Framework, 9, 17–18, 67, 443, 490

A

Access control

- host computer security, 443, 446
- Hyper-V features, 14
- resource pools, 435–436
- secure virtual service offerings, 490

Access-based enumeration, 440

Accounts

- Administrator, 61–63, 65
- attack surface, Hyper-V, 437
- auditing object access, 463–465
- failover clustering configuration, 131
- guest, 61
- host computer security, 445
- SCVMM Server account, 342
- two-node clusters, validating, 137–140

Acronis True Image Echo, 331, 368–371

Active Directory, 494, 576

Active Directory Certificate Services (ADCS), 440, 452

Active Directory Domain Controllers, 444

Active Directory Domain Services (ADDS)

- attack surface, Hyper-V, 437–439
- authorization store, 473
- backup, 529
- failover clustering requirements, 131
- host computer security, 442
- Hyper-V configuration, 80–81
- Microsoft Assessment and Planning (MAP) tool, 31
- practice, ADDS performance analysis, 201–205
- resource pool forests, 64
- secure virtual service offerings, 490
- System Center Virtual Machine Manager (SCVMM), 158

Active Directory Lightweight Directory Services, 473

Active Directory, Quest ActiveRoles Management Shell, 409

Active-active clusters, 125

Active-passive clusters, 125

Add Features Wizard, 149

Add Host Wizard, 277–280

Add Library Server wizard, 285–287

Add Roles Wizard, 74

Administration

- administrator description, 1–2
- assigning roles with SCVMM, 486–487
- AzMan, assigning roles, 481–486
- deploying Hyper-V Manager, 148–152
- Failover Cluster Management Console, 152–154
- failover clustering, 123–127
- firewall, 61
- Hyper-V features, 14
- Hyper-V host configuration, 59
- Microsoft Hyper-V Server 2008, 12–13
- overview, 121–122
- practice, delegating administrative roles in SCVMM, 496–500
- privileges, assigning, 435
- Remote Desktop, 64
- SCVMM Administration Console, 270
- securing Hyper-V resource pools, 435–436
- Server Core installation, 67
- System Center Virtual Machine Manager (SCVMM)
 - architecture, 164–165
 - communication ports, 166–167
 - distributed implementation recommendations, 173–174
 - implementation, preparing for, 168–176
 - overview, 154–163, 269–273
 - practice, installing, 176–185
 - SCVMM add-ons, 289–293

- SCVMM Library, 284–289
 - upgrading, 174–176
- workstations, security and, 450
- Administration, remote, 12–14
- AdministrativeAccount, Server Core installation, 69
- Administrator account, 61–63, 65
- Administrator Console, SCVMM, 162, 165
- Advanced Technology Attachment (ATA), 241–243
- Agent version, status of, 283
- Agents, adding, 184
- Aliases, PowerShell, 387, 389, 391–392
- AMD processors, 290, 556
- AMD Virtualization (AMD-V), 11, 40–41
- Answer files, 284–285, 288, 290
- Anti-affinity rules, 560
- Anti-malware, host computer security, 442, 489
- Anti-virus, host computer security, 442
- Appliances, virtual, 581
- Application context, Windows PowerShell, 411
- Application programming interfaces (APIs), 14, 19
- Applications
 - availability, 8
 - additional VM components, configuring, 574–575
 - case scenario, protecting Exchange 2007 VMs, 585
 - guest failover clustering, 560–562
 - guest network load balancing, 572
 - host failover clusters, 554–560
 - iSCSI security, 569–572
 - overview, 553–554
 - strategy selection, 573–574
 - supported VM configurations, 575–581
 - VLAN tagging, 562–566
 - change tracking, 191
 - data backups, 530
 - deployment, 7
 - external connections, 108
 - host computer security, 441, 448
 - recovery, 529
 - resource pool, securing, 451
 - restoring, 526
 - Snapshots and, 259
 - software stack, 6
 - Task Manager, 187–190
 - virtualizing, 3–7, 576
- App-V (Microsoft Application Virtualization), 6
- Architecture
 - enlightened vs. legacy guests, 20–23
 - hardware sharing, 14

- host computer security, 447
- Hyper-V, overview, 16–18
- parent vs. child partitions, 18–19
- System Center Virtual Machine Manager (SCVMM), 164–165
- Assessments, preparing, 29–30
- ATA (Advanced Technology Attachment), 241–243
- Attack surface, 12, 15, 436–439
- Audit Collection Database, 343
- Auditing, 440, 443, 453, 463–465, 490
- Authentication, 569–572
- Authorization Manager (AzMan)
 - assigning roles, 481–486
 - deploying Hyper-V, 26–27
 - host computer security, 440
 - Hyper-V features, 14
 - introducing, 472–475
 - SCVMM and, 471, 481
- Authorization stores, 472–475
- Automatic Start Action, 219–220, 228
- Automatic Stop Action, 219–220, 228
- Automatic updates, 61, 64, 70, 76.
 - See also* Update Alerts; Updates
- Automating virtual machine creation
 - creating a duplicate machine, 304–310
 - Hyper-V Manager vs. SCVMM, 280–284
 - overview, 267–268
 - practice, managing virtual machine templates, 318–324
 - SCVMM add-ons, 289–293
 - SCVMM Library, managing, 284–289
 - System Center Virtual Machine Manager (SCVMM),
 - overview, 269–273, 310–318
 - VMM Self-Service Portal, 315–318
- Automating virtual machine management,
 - PowerShell
 - case scenario, 429
 - commands for SCVMM, 412
 - managing Hyper-V operations, 402–409
 - overview, 383–384
 - practice, using Windows PowerShell, 424–428
 - running PowerShell scripts, 398–401
 - shortcut keys, 401
 - understanding PowerShell, 385–389
 - using PowerShell, 391–398
 - using PowerShell with SCVMM, 409–412, 422–423
 - Windows PowerShell constructs, 389–391
- Automation, 26, 48–49, 62

Availability. *See also* Failover clustering
 compatibility, hardware, software and drivers, 46
 file locations, virtual machines, 96
 host failovers, managing, 142–143
 host servers, 26, 49–52
 Hyper-V features, 14
 hypervisors, 8
 moving virtual machines, 314–315
 multi-site clustering requirements, 131–132
 practice, planning host failover clustering, 144–147
 resource pool, securing, 450
 SCVMM Library, 285
 two-node clusters, creating
 Hyper-V role installation, 133–137
 overview, 132
 server and operating system, 133
 validating, 137–140
 virtual machine creation, 141–142
 virtual network creation, 137
 virtual machines
 additional components, configuring, 574–575
 case scenario, protecting Exchange 2007
 VMs, 585
 guest failover clustering, 560–562
 guest network load balancing, 572
 host failover clusters, 554–560
 iSCSI security, 569–572
 iSCSI storage, configuring, 566–569
 overview, 553–554
 practice, assigning VLANs to VMs, 581–582
 strategy selection, 573–574
 supported VM configurations, 575–581
 VLAN tagging, 562–566
 Average Disk second/Read, 197
 Average Disk second/Write, 197
 AzMan (Authorization Manager)
 assigning roles, 481–486
 deploying Hyper-V, 26–27
 host computer security, 440
 Hyper-V features, 14
 introducing, 472–475
 SCVMM and, 471, 481

B

Background Intelligent Transfer Service (BITS), 335
 Backup Integration Service, 511

Backups
 Administrator account, 62
 Hyper-V protection strategies, 508–510
 migration and, 339
 planning for, 27
 practice, performing internal VM backups, 542–546
 resource pools, overview, 505–507
 resource pools, securing, 451
 snapshots, 15
 software stack, 6
 System Center Data Protection Manager (SCDPM)
 host server and VM backups, 538–540
 installing, 535–538
 overview, 529–530
 requirements, 531–535
 restoring VMs, 540–541
 SQL Server preparation, 535
 two-node clusters, 132
 virtual machines, 307, 510–516
 Volume Shadow Copy Service (VSS), 213
 Windows Server Backup
 overview, 516–518
 PowerShell cmdlets, 519
 protecting Hyper-V and virtual
 machines, 519–525
 restoring systems with, 525–529
 Best practices
 virtual networks, 111
 VLAN tagging, 566
 BIOS (Basic Input/Output System), 11, 74, 224
 BitLocker
 configuring, 61
 host computer security, 441, 446
 securing VM files, 461–462
 virtual hard disks, 239–240
 Windows Server Backup, 518
 BitLocker Drive Preparation Tool, 462
 BITS (Background Intelligent Transfer Service), 335
 BizTalk Server, 576
 Boot disks
 duplicate virtual machines, 305
 IDE or SCSI drives, 242
 migration, 332
 Preboot Execution Environment (PXE), 290–291
 Virtual Server migration, 365
 WindowsPE, 510
 Boot images, Windows PE, 292
 Boot start drivers, 46

Browsers, Microsoft Assessment and Planning (MAP) tool, 31

Buffers, overflow errors, 40–41

Bytes Total/second counter, 197

C

Caching, applications, 6

Case Scenarios

automating Hyper-V operations, 429

deploying SCVMM, 206

host server failure, dealing with, 547

moving from physical to virtual machines, 379–380

networking virtual machines, 117

protecting Exchange 2007 VMs, 585

provisioning virtual machines, 325

security, planning resource pool strategy, 502

server virtualization, preparing for, 55–56

virtual machine, moving, 263

CCR (Cluster Continuous Replication), 50–51

CD/DVD devices, 43, 159, 219–220, 225–226, 246

Central file share, securing, 450

Centralized management, 26

Centralized Resource Optimization (CRO), 158

Certificate revocation lists (CRLs), 440

Certificate Services, Active Directory, 452

Certificates, 354, 440, 452

Challenge-Handshake Authentication Protocol (CHAP), 569–572

Change System Properties, 65–66

Change tracking, 191

CHAP (Challenge-Handshake Authentication Protocol), 569–572

Check boxes, Hyper-V settings, 94

Child partitions, 211–212, 444, 446–447, 565.

See also Partitions

Chinese language, 76

Citrix, 10, 175–176, 436, 575

Citrix Project Kensho, 373

Citrix XenServer, 26, 331, 368, 372–373

Clean provisioning, 338–339

Client Access role, 339

Client Layer, SCVMM, 165

Clients, 31

Clipboard, 281

Clones, 305, 307, 319–320

Cluster Continuous Replication (CCR), 50–51

Cluster Shared Volume, 124

Clustered Share Volume (CSV), 555

Clusters. *See also* Failover clustering

additional components, configuring, 574–575

case scenario, protecting Exchange 2007 VMs, 585

file locations, virtual machines, 96

guest failover clustering, 560–562

guest network load balancing, 572

host failover clusters, 554–560

host server configuration, 49–52

iSCSI security, 569–572

manual conversions, 338–339

moving virtual machines, 314–315

overview, 553–554

parent partition overhead, 45

practice, assigning VLANs to VMs, 581–582

strategy selection, 573–574

supported VM configurations, 575–581

Virtual Server migration, 366

VLAN tagging, 562–566

Cmdlets

aliases, 387

default, 391–392

Hyper-V Windows PowerShell Library, 405

overview, 385–389

PowerShell commands for SCVMM, 412

syntax, 387

Windows Server Backup, 517, 519

Co-located setups, 158

Command line configuration, 67–72

Command-line tools, 290, 516. *See also* PowerShell

Commerce Server, 576

Communication ports, 43, 166–167, 219–220, 227

Communication protocols, 164–165, 215–216, 442, 489

Compaction, disk drives, 15, 251

Compatibility, hardware, software and drivers, 46–47

Computer Browser service, 31

Computer names, host server configuration, 64

Configuration Analyzer, SCVMM, 173

Configuration files, 96, 219–223, 288, 362, 365

Configuration management, 7, 49–52

Configuring Hyper-V hosts

active directory domain services, 80–81

full installation, 63–67

Hyper-V management tools, 91–93

initial server configuration, 61–72

installing Hyper-V role, 61, 72–78

installing Hyper-V updates, 79–80

- overview, 59
- practice, installing Hyper-V role, 85–90
- practice, Windows Server 2008 for Hyper-V, 97–102
- Server Core installation, 67–72
- Server Core, Hyper-V role, 76–78
- virtual networking
 - full vs. Server Core installations, 107–111
 - network types, 104–107
 - overview, 104
 - Virtual Network Manager Tool, 111–113
- Windows Hyper-V Server, installing, 81–84
- Configuring resource pools
 - basic virtual machines, settings, 219–220
 - case scenario, deploying SCVMM, 206
 - deploying Hyper-V Manager, 148–152
 - Failover Cluster Management Console, 152–154
 - failover clustering, 123–127
 - failover clustering, requirements, 127–132
 - host failovers, managing, 142–143
 - managing system resource, 186–198
 - multi-site clustering requirements, 131–132
 - optimizing Hyper-V hosts, 199–201
 - practice, ADDS performance analysis, 201–205
 - practice, planning host failover clustering, 144–147
- System Center Virtual Machine Manager (SCVMM)
 - architecture, 164–165
 - communication ports, 166–167
 - implementation, preparing for, 168–176
 - overview, 154–163
 - practice, installing, 176–185
 - upgrading, 174–176
- two-node clusters, creating
 - Hyper-V role installation, 133–137
 - overview, 132
 - server and operating system, 133
 - validating, 137–140
 - virtual machine creation, 141–142
 - virtual network creation, 137
- Windows Deployment Services (WDS), 292–293
- Windows PowerShell for SCVMM, 411–412
- Configuring, virtual machine availability
 - additional components, configuring, 574–575
 - case scenario, protecting Exchange 2007 VMs, 585
 - guest failover clustering, 560–562
 - guest network load balancing, 572
 - host failover clusters, 554–560
 - iSCSI Initiator, 567–569
 - iSCSI security, 569–572
 - iSCSI storage, configuring, 566–569
 - overview, 553–554
 - practice, assigning VLANs to VMs, 581–582
 - strategy selection, 573–574
 - supported VM configurations, 575–581
 - VLAN tagging, 562–566
- Connections
 - configuring virtual networks, 107
 - failover clustering requirements, 129
 - full vs. Server Core installations, 107–111
 - Hyper-V Manager vs. SCVMM, 280–284
 - pass-through disks, 240
 - SCVMM requirements, 171
 - status of, 283
 - virtual storage controllers, 43
 - VirtualMachineViewer.exe, 271
- Consolidation, 31, 158
- Control Panel, host server configuration, 65
- Controllers, virtual storage, 43
- Conversion Wizard, 371
- Conversions
 - case scenario, moving from physical to virtual machines, 379–380
 - caveats, 335–337
 - checklist, 337–338
 - clean provisioning, 338–339
 - integrating OpsMgr with SCVMM, 347–353
 - integrating SCVMM with VMware ESX, 353–354
 - migrating from
 - Citrix XenServer, 372–373
 - physical machines, 356–361
 - third-party disk image, 368–371
 - Virtual Server 2005 or Virtual PC, 362–366
 - VMware ESX formats, 371–372
 - optimizing virtual machines, 339–340
 - overview, 329, 355–356
 - Performance and Resource Optimization (PRO), 340–341
 - physical machines to virtual machines (P2V), 269
 - practice source-to-target conversions, 375–377
 - preparing for migration, 331–333
 - scenarios, 330–331
 - servers to virtual machines, 26
 - System Center Operations Manager, 341–347
 - System Center Virtual Machine Manager, 6
 - virtual machine provisioning approaches, 333–335
 - virtual machines, non-Hyper-V to Hyper-V, 269
 - VMC to Hyper-V Import tool, 367

- Convert Physical Server, 357
- Convert Virtual Machine, 371
- Counters, system, 192–193, 195–196
- CPU/BIOs requirements, 28, 278–280
- CPUs
 - performance baselines, 196–198
 - redundancy, 575
 - usage, Task Manager, 187–190
- CPU-Z.exe, 314
- Create Computer Objects permission, 131
- Creating
 - iSCSI clusters, 569
 - Library Servers, adding new, 285
 - networks, 112–113
 - performance baselines for Hyper-V, 196–198
 - practice
 - delegated user, 497
 - guest OS profile, 299–300
 - hardware profile, 300
 - management virtual network, 467–470
 - new Library share, Library Server, 293–294
 - role delegation in SCVMM, 497–498
 - unattended installation file, 294–299
 - virtual machines, 98–99
 - Protection groups, 538–540
 - Snapshots, virtual machines, 257–259
 - supported VM configurations, 575–581
 - two-node clusters
 - Hyper-V role installation, 133–137
 - overview, 132
 - server and operating system, 133
 - validating, 137–140
 - virtual machine creation, 141–142
 - virtual network creation, 137
 - virtual machines
 - advanced setting configurations, 223–231
 - basic virtual machines, 219–223
 - case scenario, moving a virtual machine, 263
 - child partitions, Hyper-V, 211
 - editing virtual hard disks, 249–251
 - examining virtual machine states, 232–233
 - Hyper-V Integration Services, 212–218
 - inspecting virtual hard disks, 254–255
 - legacy guests, installing, 230–231
 - overview, 218–219
 - practice, working with non-Windows VMs, 233–235
 - practice, working with VM disks, 259–262
 - Snapshots, working with, 255–259

- Virtual Hard Disk Wizard, 243–248
- virtual hard disks, 236–243
- virtual machines, automating
 - creating and managing VMs with SCVMM, 310–318
 - duplicate virtual machines, 304–310
 - Hyper-V Manager vs. SCVMM, 280–284
 - overview, 267–268
 - practice, managing virtual machine templates, 318–324
 - SCVMM add-ons, 289–293
 - SCVMM Library, managing, 284–289
 - SCVMM overview, 269–273
 - VMM Self-Service Portal, 315–318
- Credentials, 94, 437, 444
- CRLs (certificate revocation lists), 440
- CSV (Clustered Share Volume), 555
- Czech language, 75

D

- DAS (direct-attached storage), 42, 45, 49, 96, 128.
 - See also* Storage
- Data Collector Set templates, 193
- Data collector sets, 193, 196–198, 201–205
- Data control policies, software stack, 6
- Data Exchange, 213
- Data Execution Prevention, 74
- Data protection
 - case scenario, host server failure, 547
 - host computer security, 441
 - Hyper-V protection strategies, 508–510
 - overview, 505–507
 - practice, performing internal VM backups, 542–546
- System Center Data Protection Manager (SCDPM)
 - host server and VM backups, 538–540
 - installing, 535–538
 - overview, 529–530
 - requirements, 531–535
 - restoring VMs, 540–541
 - SQL Server preparation, 535
- virtual machine protection strategies, 510–516
- Windows Server Backup (WBS)
 - overview, 516–518
 - PowerShell cmdlets, 519
 - protecting Hyper-V and virtual machines, 519–525
 - restoring systems with, 525–529
- Database backup, 174. *See also* Data protection

- Database servers, startup delay, 559
- Datacenter operation, 155
- DataKeeper, 131
- DCOM (Distributed Component Object Model), 165
- Default recovery options, configuring, 63, 65
- DefaultGateway, 69
- Delegated Administrator role, 487
- Delete saved credentials, 94
- Deleting host groups, 277–280
- Delta certificate revocation list, 440
- Depersonalization, reference computers, 305
- Deploying. *See also* Hyper-V, configuring
 - applications, security and, 451
 - Hyper-V management tools, 91–93
 - Hyper-V, preparing for, 25–27
 - practice, SCVMM Agent, 184
 - SCVMM add-ons, 289–293
 - System Center Virtual Machine Manager (SCVMM), 158
 - virtual machines, 269
 - Windows Server 2008, 48–49
- Designed for Windows Server hardware program, 18
- Desired Configuration Management, 439
- Desktop virtualization, software stack, 4
- Desktop-based virtual machine operation, software stack, 6
- Desktops, software stack, 6
- Development servers, startup delay, 559
- Device drivers. *See also* Devices
 - compatibility, 46–47
 - Hyper-V architecture, 18–19
 - migration, 331–333
 - rollback, 509
 - selecting hardware, 40–47
 - synthetic devices, 215
- Device identification strings, 457
- Device Manager, 509
- Device setup classes, 458
- Devices. *See also* Device drivers
 - CD/DVD, 43, 159, 219–220, 225–226, 246
 - host computer security, 441
 - removable devices, 42, 441, 446, 457–461
- Differencing disks, 237, 245, 251, 365
- Digital Rights Management (DRM), 490
- Digital signatures, 46–47, 440
- Direct-attached storage (DAS), 42, 45, 49, 96, 128. *See also* Storage
- Directory service access, 463–465
- Disaster recovery
 - case scenario, host server failure, 547
 - Hyper-V protection strategies, 508–510
 - overview, 505–507
 - practice, performing internal VM backups, 542–546
 - System Center Data Protection Manager (SCDPM)
 - host server and VM backups, 538–540
 - installing, 535–538
 - overview, 529–530
 - requirements, 531–535
 - restoring VMs, 540–541
 - SQL Server preparation, 535
 - virtual machine protection strategies, 510–516
 - Windows Server Backup
 - overview, 516–518
 - PowerShell cmdlets, 519
 - protecting Hyper-V and virtual machines, 519–525
 - restoring systems with, 525–529
- Disk controllers, virtual machines, 242
- Disk latency, 197
- Disk resources, host optimization, 200
- Disk space, SCVMM requirements, 170–171
- Disk/Logical Unit Number (LUN), 29
- Diskette drives, virtual machine settings, 219–220, 227
- Disks, SCDPM requirements, 533
- DiskShadow.exe, 516
- Disk-to-disk backups, software stack, 6
- Display parameters, 339
- Display time, 62
- Distributed Component Object Model (DCOM), 165
- Distributed data center setups, 158
- Distributed management, 26
- DLL (dynamic-link library), 19, 270, 386, 439
- DNSIPAddress, 69
- Domain controller, 131, 338, 449, 559
- Domain Name System (DNS), 68, 131, 180, 338
- DomainName, Server Core installation, 69
- Domains, 64, 171, 173
- DOS, 216–218, 230–231
- Dot sourcing, 404
- DoubleTake Software, 131
- Downtime, planned, 127
- Downtime, unplanned, 127
- DPM Server, 531
- Drivers
 - compatibility, 46–47
 - Hyper-V Integration Services, 214
 - migration, 331–333

- rollback, 509
- selecting hardware, 40–47
- synthetic devices, 215

DRM (Digital Rights Management), 490

Duplicating virtual machines, 304–310

DVD devices, 43, 159, 219–220, 225–226, 246

Dynamic Host Configuration Protocol, 338, 559

Dynamic resource management, hypervisors, 8

Dynamic systems provisioning, 48–49

Dynamic VLANs, 564

Dynamically expanding virtual hard disk, 236, 244, 250, 259, 357

Dynamic-link library (DLL), 19, 270, 386, 439

Dynamics AX, 576

Dynamics CRM, 576

Dynamics GP, 576

Dynamics NAV, 576

E

EBS (Windows Essential Business Server 2008), 25

Edge Subscription, 339

Edge Transport, 339

Edit Disk command, 249–251

EFS (Encrypting File System), 239–240

E-mail services, 124, 339, 559

Embedded signatures, 46

Enable Virtual LAN Identification For the Parent Partition, 112

Encryption

- AD CS (Active Directory Certificate Services), 440

- BitLocker, 61, 441

- Encrypting File System (EFS), 239–240

- host computer security, 446

- iSCSI security, 569–572

- remote connections, 452

- storage, 448

- Windows Server Backup, 518

Encryption Key Wizard, 346

End-user desktops, software stack, 6

Enlightened guest operating system

- backups, 525

- child partitions, 211

- Hyper-V Integration Services, 214–215

- non-Windows guests, 215–216

- overview, 20–23

- pass-through disks, 241

Enlightened I/O, 20–23

Enlightened virtual machines (VMs), network adapters, 104–107

Environment

- deploying Hyper-V, 25–27

- inventorying, 27–29

- practice, perform assessment, 34–39

Error messages, 74, 189

Ethernet connections, 109, 129

Evaluation VHDs, 579–581

Event logs, 189, 463–465

Event messages, 341

Event Viewer, 186, 189–191

Exam Tip

- assessment tools, 33

- authorization stores and ADDS, 474

- BitLocker and VMs, 446

- conversion terms, 374

- digital signatures, 47

- DNS server name, 180

- duplication vs. export, 307

- filters, using, 284

- guest operating systems, 23

- host server chipsets, 366

- Hyper-V

 - characteristics, 43

 - default disk size, 99

 - features, 16

 - Integration Services drivers, 214

 - security, 431

 - settings defaults, 96

 - two-node clusters, 131

 - VM configuration files, 102

- Hyper-V Server, 13, 82

iSCSI Initiator, 569

legacy network adapters, 110

legacy VMS, Hyper-V and Terminal Services, 218

Linux Integration Components, 216, 242

local SCVMM database with SQL Server

- Express, 171

machine states, 233

managing virtual server hosts, 272

OC commands, 78

OCSETUP.exe, 78

offline conversions, 356

offline vs. online conversions, 335

pass-through disk size, 241

performance monitoring, Hyper-V, 189

- PowerShell, elevated rights, 411
- PRO inheritance, 353
- product keys and templates, 323
- resource monitoring, 191
- RSAT feature, 149
- SCSI vs. IDE, 229
- SCVMM Administrator Console, 284
- SCVMM and Authorization Manager, 472
- SCVMM architecture, 165
- SCVMM Configuration Analyzer, 173
- SCVMM vs. Authorization Manager, 471
- secure VMware communications, 354
- Server Manager, 92
- Server Performance Advisor, 196
- Snapshot location, 229
- Snapshots, creating, 255
- templates, creating, 310
- update 951308, 143, 145
- update verification, 76
- VHD, maximum size, 240
- virtual machines, high availability, 141
- virtual server configuration files, 221
- VLAN tagging, 566
- VM file placement, 98
- VMware versions, 354
- Windows 2000 Server, 215
- Windows NT Server 4, migrating, 357
- Windows PowerShell and Hyper-V, 385
- Windows Server Backup (WSB), 525
- wireless network adapters, 107
- WSB backup targets, 518
- WSB recovery, 529
- WUSA.exe command, 77
- Exchange 2007, 580
- Exchange Mailbox server, 124
- Exchange Server, 529, 576
- Exchange servers, manual conversion, 339
- Executables, 387, 450
- Expansion, disk drives, 15
- Export, Hyper-V to Hyper-V migration, 374
- Exporting, virtual machines, 15, 176–177, 288, 314–315
- Extended Markup Language (XML), 102, 440
- Extensibility, Hyper-V features, 14
- Exterior SATA, hardware selection, 42
- External connections, configuring, 108
- External hard disk, 177, 319, 518
- External virtual networks, 104–107

F

- Failover Cluster Configuration Program (FCCP), 46
- Failover Cluster Validation tool, 137–140
- Failover clustering
 - compatibility, 46
 - Failover Cluster Management Console, 142–143, 152–154
 - host server configuration, 49–52
 - Hyper-V features, 14
 - managing host failovers, 142–143
 - migration, 339
 - multi-site clustering requirements, 131–132
 - overview, 123–127, 553–554
 - parent partition overhead, 45
 - practice, planning host failover
 - clustering, 144–147
 - requirements, 127–131
 - resource pool, securing, 450
 - SCVMM Library, 285
 - System Center Virtual Machine Manager (SCVMM), 155, 159
 - two-node clusters, creating
 - Hyper-V role installation, 133–137
 - overview, 132
 - server and operating system, 133
 - validating, 137–140
 - virtual machine creation, 141–142
 - virtual network creation, 137
- virtual machine availability
 - additional components, configuring, 574–575
 - case scenario, protecting Exchange 2007 VMs, 585
 - guest failover clustering, 560–562
 - guest network load balancing, 572
 - host failover clusters, 554–560
 - iSCSI security, 569–572
 - iSCSI storage, configuring, 566–569
 - practice, assigning VLANs to VMs, 581–582
 - strategy selection, 573–574
 - supported VM configurations, 575–581
 - VLAN tagging, 562–566
- FalconStor, 131
- FAT, 251
- FAT32, 251
- Fault tolerance
 - Failover Cluster Management Console, 152–154
 - failover clustering, 123–127

- failover clustering, requirements, 127–132
- host failovers, managing, 142–143
- host remote administration, 148–152
- host servers, 46
- Hyper-V features, 14
- moving virtual machines, 314–315
- multi-site clustering requirements, 131–132
- optimizing Hyper-V hosts
 - managing system resources, 186–198
 - operations, 199–201
- overview, 121–122
- practice, ADDS performance analysis, 201–205
- practice, planning host failover clustering, 144–147
- System Center Virtual Machine Manager (SCVMM)
 - architecture, 164–165
 - communication ports, 166–167
 - distributed implementation recommendation, 173–174
 - implementation, preparing for, 168–176
 - overview, 154–163
 - practice, installing, 176–185
 - upgrading, 174–176
- two-node clusters, creating
 - Hyper-V role installation, 133–137
 - overview, 132
 - server and operating system, 133
 - validating, 137–140
 - virtual machine creation, 141–142
 - virtual network creation, 137
- FCCP (Failover Cluster Configuration Program), 46
- Fibre Channel, 42, 129
- File servers, 529, 559
- File system, host computer security, 442, 490
- Files, 95–96, 257–259, 526, 530
- Filters
 - management packs, 342
 - SCVMM Administrator Console, 283
 - Virtual Machine Manager, 274
- Firewalls
 - attack surface, Hyper-V, 438
 - configuring, 61
 - host server configuration, 64
 - SCVMM communication ports, 166–167
 - SCVMM requirements, 171
 - Server Core, 70–71
 - settings, 456
 - Windows Server Backup, 517
 - Windows Server Firewall, 439–440
- FireWire, hardware selection, 42
- Fixed resources, 223
- Fixed size disks, 237, 244, 251, 340
- Floppy drives, 43, 159, 288
- Folder Redirection, software stack, 6
- Folders, 526, 530
- Forefront Client Security, 576
- Forefront Security for Exchange, 577
- Forefront Security for SharePoint, 577
- Forest Trust relationships, 173
- Full installation
 - attack surface, 438
 - Authorization Manager (AzMan), 472
 - configuring for Hyper-V, 63–67
 - Failover Cluster Management Console, 152
 - Hyper-V role, 72–76
 - practice, create virtual network
 - interface, 113–114
 - two-node clusters, creating, 134
- Full Resource Pool Administrator, 486
- FULL SCREEN mode, 281

G

- Gateway Server, 343
- Gibson Research Corporation, 41
- Globally unique identifiers (GUID), 458
- Graphics, 20–23
- Group Policy Management Console, 458
- Group Policy Objects (GPOs), 454–455, 457–461, 463–465, 518
- Guest accounts, 61
- Guest failover clustering, 560–562
- Guest operating systems
 - installing, 269
 - performance monitoring, 197
 - practice, creating, 299–300
 - profiles, SCVMM Library, 288
 - SCVMM Library, 284–285
 - System Center Virtual Machine Manager (SCVMM), 160
- Guest OS Profile, 159–160
- Guest OS Support, 14, 16
- Guests, enlightened vs. legacy, 20–23
- GUID (globally unique identifiers), 458
- GUID partition table (GPT), 129

H

- HAL (hardware abstraction layer), 366
- Hard disks, 225, 259–260, 518. *See also* Virtual hard disks (VHDs)
- Hardware
 - compatibility, 46–47
 - device identification strings, 457
 - failover clustering requirements, 128
 - failures, change tracking, 191
 - Hyper-V and, 1–2
 - Hyper-V architecture, 16–18
 - inventory, 28
 - Microsoft Assessment and Planning (MAP) tool, 33
 - optimization, 8
 - Performance Monitor, 193
 - practice, create hardware profile, 300
 - profiles, 159–160
 - profiles, SCVMM Library, 288
 - SCVMM requirements, 170–171
 - selection, 40–47
 - sharing architecture, 14
 - software vs. hardware virtualization, 7–10
 - two-node clusters, creating, 132
 - virtual hard disks, settings, 94
 - virtual machines, default settings, 219–220
 - virtual machines, settings, 224
 - Windows Server 2008 Hyper-V, 10–12
- Hardware abstraction layer (HAL), 366
- Heartbeat, 213
- Heterogeneous resource pools, 437–439
- Heterogeneous system operation, 8
- Hibernation, 222
- Homogeneous resource pools, 437–439
- Host Bus Adapters (HBAs), 129–130
- Host groups, 277–280, 353, 487
- Host Integration Server, 577
- Host Reserves, 278
- Hosted virtualization platforms, 9
- Hosts, administration
 - backup, 506, 508
 - deploying Hyper-V Manager, 148–152
 - Failover Cluster Management Console, 152–154
 - Hyper-V management roles
 - assigning with SCVMM, 486–487
 - assigning with, AzMan, 481–486
 - Authorization Manager (AzMan), introducing, 472–475
 - overview, 471–472
 - Intelligent Placement, 311
 - memory, 42
 - overview, 269–273
 - resource usage, 44–46
 - SCDPM backups, 538–540
 - security
 - attack surface, Hyper-V, 436–439
 - auditing object access, 463–465
 - BitLocker, 461–462
 - case scenario, planning resource pool strategy, 502
 - features of host computers, 439–441
 - Hyper-V resource pools, securing, 435–436
 - Hyper-V virtual machines, 488–491
 - overview, 431–434, 441–449
 - populating VMs on host servers, 491–496
 - practice, creating the management virtual network, 467–470
 - practice, delegating administrative roles in SCVMM, 496–500
 - removable devices, 457–461
 - resource pool, securing, 449–452
 - Security Configuration Wizard (SCW), 453–457
 - updating host servers, 465–466
 - server limits, 172
 - status of, 283
- System Center Virtual Machine Manager (SCVMM), 159
 - architecture, 164–165
 - communication ports, 166–167
 - distributed implementation recommendations, 173–174
 - implementation, preparing for, 168–176
 - overview, 154–163
 - practice, installing, 176–185
 - upgrading, 174–176
 - updates, 127
- Hosts, configuring
 - configurations, required, 49–52
 - full installation, 63–67
 - full vs. Server Core installations, 107–111
 - Hyper-V role, installation, 72–76
 - managing system resources, 186–198
 - optimizing Hyper-V operations, 199–201
 - overview, 59, 61–72
 - prepare and deploy, 26
 - SCVMM Administration Console, 275

Hub Transport server role

- Virtual Network Manager tool, 111–113
- virtual networking
 - network types, 104–107
 - overview, 104
- Hub Transport server role, 339
- Hungarian language, 75
- Hybrid clusters, 561
- Hybrid pass-through disks, 241
- Hybrid virtual machines, 240
- Hypercall Adapter, 211, 215–216
- HyperText Transfer Protocol (HTTP), 164
 - Hyper-V Hypervisor Logical Processor, 198
- Hyper-V input release keys, 217
- Hyper-V Integration Services, 109, 199, 212–218, 494
- Hyper-V Manager
 - configuring, 91–93
 - deploying, 148–152
 - New Virtual Machine Wizard, 211
 - practice, working with, 97
 - resource pool configuration, 121–122
 - System Center Virtual Machine Manager (SCVMM), 155
 - vs. SCVMM, 280–284
- Hyper-V New Virtual Machine Wizard, 219–223
- Hyper-V Power Pack, 409, 428
- Hyper-V PowerShell Library, 403–405
- Hyper-V Release Key, 217
- Hyper-V Remote Management Update, 409
- Hyper-V Security Guide, 431
- Hyper-V Server 2008, 155, 159
- Hyper-V Snapshots. *See* Snapshots
- Hyper-V virtualization stack, 18–19
- Hyper-V, administration. *See also* Hyper-V Manager
 - assigning roles, AzMan, 481–486
 - Hyper-V Administrator role, 486
 - Hyper-V Microsoft Management Console (MMC), 14
 - management roles, overview, 471–472
 - role, installing, 61, 76–78, 133–137
 - SCVMM, 277–280
 - System Center Data Protection Manager (SCDPM), 530, 534
 - Windows PowerShell, 402–409
 - Windows Server Backup, 519–525
- Hyper-V, configuring
 - full installation, 63–67
 - full vs. Server Core installations, 107–111
- hosts
 - active directory domain services, 80–81
 - Hyper-V role, installation, 72–76
 - installing Hyper-V role, overview, 61
 - optimizing, 186–198
 - overview, 59
 - practice, installing Hyper-V role, 85–90
 - Server Core installation, 67–72
 - updates, 79–80
 - Windows Hyper-V Server, installing, 81–84
- Hyper-V Configuration Tool, 83–84
- optimizing operations, 199–201
- Server Core, Hyper-V role, 76–78
- virtual networking
 - full vs. Server Core installations, 107–111
 - network types, 104–107
 - overview, 104
 - Virtual Network Manager tool, 111–113
- Hyper-V, implementing
 - case scenario, preparing for server virtualization, 55–56
 - determining characteristics, 41–44
 - environment, evaluating, 25
 - deploying Hyper-V, 25–27
 - inventorying, 27–29
 - Microsoft Assessment and Planning Tool, 29–33
 - practice, perform assessment, 34–39
 - features, Hyper-V, 13–16
 - hardware selection, 40–47
 - installing Windows Server 2008, 47–52
 - Microsoft Assessment and Planning (MAP), 31–33
 - overview, 1–2
 - practice, prepare for deployment, 52–54
 - practice, understanding virtual machines, 23–24
 - Windows Server 2008 Hyper-V
 - datacenter, virtualizing, 3–7
 - exploring, 10–12
 - Microsoft Hyper-V Server 2008, 12–13
 - software vs. hardware virtualization, 7–10
- Hypervisors
 - attack surface, Hyper-V, 436–439
 - managing, 121–122
 - overview, 7–10
 - System Center Virtual Machine Manager (SCVMM), 164–165
 - third party, 165, 575
 - Windows Hypervisor Interface Library, 19

I

- I/O software, 130
- I/O storage, 18–19
- IA64 platforms, 531
- IBS (image-based setup), 47
- ICT (Initial Configuration Tasks), 62
- ID, Server Core installation, 69
- IDE (Integrated Drive Electronics)
 - booting from IDE drive, 219
 - hardware selection, 42–43
 - migration, 332
 - virtual machines, 219–220, 241–243
 - Virtual Server migration, 365
 - vs. SCSI, 229
- IDE Controllers, 225
- Identity, Hyper-V configuration, 80
- IIS (Internet Information Server), 443, 490
- IKE (Internet Key Exchange), 570–572
- Image files, 59, 290, 305, 368–371
- Image-based setup (IBS), 47
- ImgMgr.exe, 290
- Implementing Hyper-V
 - architecture
 - enlightened vs. legacy guests, 20–23
 - overview, 16–18
 - parent vs. child partitions, 18–19
 - case scenario, preparing for server
 - virtualization, 55–56
 - determining characteristics, 41–44
 - environment, evaluating
 - deploying Hyper-V, 25–27
 - inventorying, 27–29
 - Microsoft Assessment and Planning Tool, 29–33
 - overview, 25
 - practice, perform an assessment, 34–39
 - features, Hyper-V, 13–16
 - hardware selection, 40–47
 - installing Windows Server 2008, 47–52
 - Microsoft Assessment and Planning (MAP), 31–33
 - overview, 1–2
 - practice, prepare for deployment, 52–54
 - practice, understanding virtual machines, 23–24
 - Windows Server 2008 Hyper-V
 - datacenter, virtualizing, 3–7
 - exploring, 10–12
 - Microsoft Hyper-V Server 2008, 12–13
 - software vs. hardware virtualization, 7–10
- Importing
 - Hyper-V to Hyper-V migration, 374
 - practice, virtual machines, 100–101, 178
 - virtual machine settings, 15
 - virtual machines, 314–315
 - VMC to Hyper-V import tool, 367
- Information events, 189
- Infrastructure, preparing, 26
- Initial Configuration Tasks interface, 63
- Input release keys, 217
- Input subsystems, Hyper-V architecture, 20–23
- Input/Output software, 130
- Insertion of the Integration Services Setup Disk, 281
- Inspection, disk drives, 15
- Install Virtual Guest Services, 281
- Installing
 - Hyper-V role, overview, 61
 - installation scripts, SCVMM Library, 284–285
 - iSCSI Initiator, 567–569
 - practice
 - Microsoft Assessment and Planning (MAP)
 - tool, 34–35
 - PowerGUI, 424
 - practice, creating unattended installation file, 294–299
 - Remote Installation Services (RIS), 290–291
 - SCVMM Self-Service Portal, 316
 - System Center Data Protection Manager (SCDPM), 535–538
 - System Center Operations Manager, 341–347
 - Windows Deployment Services (WDS), 291–292
 - Windows PowerShell, 385–386
 - Windows Server 2008, 47–52
- Integrated Drive Electronics (IDE)
 - booting from IDE drive, 219
 - hardware selection, 42
 - migration, 332
 - virtual machines, 219–220, 241–243
 - Virtual Server migration, 365
 - vs. SCSI, 229
- Integration Components for Linux, 215–216
- Integration Components, Hyper-V
 - architecture, 20–23
- Integration Services, 73, 212–218, 227, 362–366, 534
- Intel 21140-based PCI Fast Ethernet Adapter, 109
- Intel Processor Validation Utility, 40
- Intel Processors, and Linux VMs, 234

- Intel Virtualization Technology (Intel VT), 11, 40–41
- Intelligent Application Gateway, 577
- Intelligent Placement, 160, 311, 332, 341, 356, 559
- Interfaces, network, 3–7
- Interfaces, user, 63
- Internal connections, 109
- Internal hard disk, 518
- Internal virtual machine backups, 512–513
- Internal virtual networks, 104–107
- Internet Explorer, 46–47
- Internet Information Server (IIS), 153, 443, 490
- Internet Key Exchange (IKE), 570–572
- Internet Qualified Name (IQN), 570
- Internet Security and Acceleration Server, 577
- Internet Storage Name Service (iSNS), 569
- Initial Configuration Tasks (ICT), 62
- Inventories, 7, 27–29
- IOPS (I/O per second), 278–280
- IP addresses, 64, 68, 131
- IP Security policies, 456, 569–572
- IPsec (IP-level security), 439–440, 569–572
- IPv4, 68
- IPv6, 68
- IQN (Internet Qualified Name), 570
- iSCSI
 - configuring virtual networks, 107
 - failover clustering requirements, 129–130
 - file locations, virtual machines, 96
 - guest failover clustering, 560
 - hardware selection, 42
 - Hyper-V architecture, 20–23
 - iSCSI security, 569–572
 - migration, 332
 - targets, software stack, 5
 - virtual machines, 242
- iSCSI Initiator software, 567
- iSNS (Internet Storage Name Service), 569
- ISO files
 - conversion, 369
 - host computer security, 446
 - image files, 246, 284–285, 288
 - resource pool, securing, 450
 - storing, 59
 - System Center Virtual Machine Manager (SCVMM), 160
- Isolation, private virtual networks, 105–107
- Itanium processors, 1, 10–11, 290

J

- Java, hypervisors, 9
- Jobs, 157, 276, 287

K

- Kerberos authentication, 494
- Kernel Mode Code Signing, 46
- Key Management Service (KMS), 71
- Keyboard, 94
- Korean language, 75

L

- LAN Diagnostics, 193
- Languages, updates, 75–76
- LANs
 - assigning, 112
 - diagnostics, 193
 - guest failover clustering, 560
 - hardware selection, VLAN, 42
 - practice, assigning VLANs to VMs, 581–582
 - virtual LAN identification, 226
 - VLAN tagging, 562–566
- Last Known Good Configuration, 509
- Legacy guest operating systems, 211, 216–218, 230–231, 241
- Legacy network adapters, 104–107, 109, 200, 231
- Legacy virtual machines, backups, 511–512, 525
- Libraries
 - administrator roles, 487
 - Hyper-V Windows PowerShell library, 403–405
 - placement of, 312
 - SCVMM Administration Console, 276
 - System Center Virtual Machine Manager (SCVMM), 157
 - virtual machines, 6
 - Windows Hypervisor Interface Library, 19
- Library Server
 - overview, 162, 284–285
 - practice, adding new, 293–294
 - resource pool, securing, 451
 - SCVMM, 170, 174
 - System Center Virtual Machine Manager (SCVMM), 160
- LIC (Linux Integration Components), 216, 242

- Life-cycle management, software stack, 6
- Limit Processor Functionality (LPF), 230
- Linux
 - attack surface, Hyper-V, 436
 - creating virtual machines, 211
 - guest operating systems, 21–22
 - hypervisor, 9–10
 - installing legacy guests, 231
 - integration components, 14, 215–216, 242
 - manual conversions, 338–339
 - practice, creating Linux VM, 233–235
- Local area networks (LAN)
 - diagnostics, 193
 - hardware selection, VLAN, 42
 - virtual LAN identification, 226
- Local storage, backup, 530. *See also* Backups
- Local System account, 173
- Locked-in virtual machines, 240–241
- Logical Disk, 197
- Logical processors, 41, 44
- Logical unit number (LUNs), 29, 96, 124–126, 133, 533
- Logon events, 463
- LPF (Limit Processor Functionality), 230

M

- MAC addresses, 229
- Machine conversions, software stack, 6
- Machine states, 232–233
- Machines. *See* Virtual machines (VMs)
- Macintosh operating systems, 9
- Mailbox server, 339
- Malicious scripts, software restriction policies, 439.
 - See also* Security
- Managed Computer layer, SCVMM, 164–165, 276
- Management
 - assigning roles with SCVMM, 486–487
 - backup schedules, 525
 - certificates, 440
 - distributed, 26
 - host computer security, 448
 - Hyper-V tools, 15, 91–93
 - Library contents, 287–289
 - life-cycle, 6
 - permissions, host computers, 440
 - practice, delegating administrative roles in SCVMM, 496–500
 - SCVMM add-ons, 289–293
 - SCVMM Library, 284–289
 - security, 64
 - Server Manager, 15
 - snapshots, 529
 - System Center Virtual Machine Manager (SCVMM), 6, 160, 269–273, 486–487
 - time synchronization, 494
 - virtual machines, default settings, 219–220
 - Virtual Network Manager tool, 111–113
 - virtualization infrastructure driver, 19
 - Windows PowerShell
 - case scenario, automating operations, 429
 - commands for SCVMM, 412
 - constructs, 389–391
 - managing Hyper-V operations, 402–409
 - overview, 383–384
 - practice, using PowerShell, 424–428
 - running scripts, 398–401
 - shortcut keys, 401
 - understanding PowerShell, 385–389
 - using PowerShell, 391–398
 - using PowerShell with SCVMM, 409–412, 422–423
- Management Reports, 31
- Management Server, 342
- Manual conversions, 338–339
- MAP (Microsoft Assessment and Planning) Tool, 31–33
- Master boot record (MBR), clustered volumes, 129
- MBCA (Microsoft Baseline Configuration Analyzer), 173
- MBSA (Microsoft Baseline Security Analyzer), 27–28
- Media, 226, 246, 281, 518
- MED-V (Microsoft Enterprise Desktop Virtualization), 6
- Memory
 - hosts, 42, 66, 200, 278–280
 - Hyper-V architecture, 18–19
 - Hyper-V features, 15
 - inventories, 28
 - management, 19
 - parent partition overhead, 45
 - performance monitoring, 197
 - redundancy, 575
 - SCDPM requirements, 533
 - System Center Virtual Machine Manager (SCVMM), 159
 - Task Manager, 187–190
 - virtual machine protection strategies, 510–516
 - virtual machine settings, 219–220, 224
- Memory Available Megabytes counters, 197

- Messages, event, 341
- Microsoft .NET Framework, 67, 385
- Microsoft Application Virtualization (App-V), 6, 31
- Microsoft Assessment and Planning Tool (MAP), 29–39
- Microsoft Baseline Configuration Analyzer (MBCA), 173
- Microsoft Baseline Security Analyzer (MBSA), 27–28, 70
- Microsoft Enterprise Desktop Virtualization (MED-V), 6
- Microsoft Exchange Server, 50–51
- Microsoft Hyper-V Server
 - exploring, 12–13
 - supported VM configurations, 575–581
- Microsoft Infrastructure Optimization, 30
- Microsoft Management Console (MMC), 14, 516
- Microsoft Office 2007, 31
- Microsoft Office Visio, 27
- Microsoft Open Specification Promise, 215
- Microsoft Operations Framework (MOF) Virtualization Process Companion Guide, 4
- Microsoft SQL Server, 162, 450
- Microsoft System Center, 17–18
- Microsoft System Center Virtual Machine Manager, 578
- Microsoft System Preparation Tool, 305
- Microsoft Virtual Network Switch Protocol, 106
- Microsoft Virtual PC, 9
- Microsoft Virtual Server, 6, 9, 529
- Microsoft Virtual Server 2005 Migration Toolkit (VSMT), 357
- Microsoft Windows Server 2008 Hyper-V.
 - See Windows Server 2008 Hyper-V
- Middleware servers, startup delay, 559
- Migration
 - case scenario, moving from physical to virtual machines, 379–380
 - clean provisioning, 338–339
 - conversion caveats, 335–337
 - conversion checklist, 337–338
 - from Citrix XenServer, 372–373
 - from Hyper-V to Hyper-V (Import/Export), 374
 - from physical machines, 356–361
 - from third-party disk image, 368–371
 - from Virtual Server 2005 or Virtual PC, 362–366
 - from VMware ESX format, 371–372
 - host failover clusters, 555
 - Hyper-V features, 14
 - integrating OpsMgr with SCVMM, 347–353
 - integrating SCVMM with VMware ESX, 353–354
 - live migration, 50
 - managing host failovers, 142–143
 - moving virtual machines, 314–315
 - optimizing virtual machines, 339–340
 - overview, 329
 - overview, source-to-target conversions, 355–356
 - Performance and Resource Optimization (PRO), 340–341
 - practice, source to target conversions, 375–377
 - preparing for, 331–333
 - scenarios, 330–331
 - server roles, 31
 - System Center Operations Manager, 341–347
 - to server virtualization infrastructure, 26
 - virtual machine provisioning approaches, 333–335
 - VMC to Hyper-V import tool, 367
- Mix-and-match clusters, 126
- MMC (Microsoft Management Console), 14, 516
- More Info
 - Acronis True Image, 368
 - Active Directory Certificate Services, 440
 - ADDS, 81
 - Advanced Firewall, Server Core, 71
 - anti-affinity rules, 560
 - applications available in VHDs, 580
 - Authorization Manager (AzMan), 474
 - automating virtual machine and host deployment, 289
 - BitLocker, 462
 - Citrix Essentials for Hyper-V Management, 175–176
 - clustering host servers and virtual machines, 52
 - collecting events centrally, 465
 - compacting non-NTFS disks, 251
 - configuring virtual machines, 220
 - database backup, 174
 - deploying virtual machines with SCVMM, 314
 - device control policies, 460
 - device ID strings and setup classes, 460
 - disk connections in VMs, 242
 - EBS 2008, virtualizing, 25
 - evaluation cluster, 144
 - Event Log, features, 190
 - Exchange Server, 51
 - failover clustering, 143

- Hyper-V component list, 439
- Hyper-V language pack, 76
- Hyper-V Manager, 93
- Hyper-V networking, 105–106
- Hyper-V PowerPack, working with, 428
- Hyper-V protection strategies, 506
- Hyper-V RAM calculator, 44
- Hyper-V Remote Management Configuration Utility, 486
- Hyper-V Server download, 81
- Hyper-V updates, 80
- Hyper-V Windows PowerShell Library, 403
- Hyper-V WMI Provider, 403
- Internet Storage Name Service (iSNS), 569
- iSCSI clusters, creating, 569
- iSCSI Initiator software, 567
- iSCSI Initiator configuration, 243
- iSCSI security, 570
- iSCSI target evaluation software, 566–567
- Linux Integration Components, 216
- MAP assessments for Hyper-V, 33
- MAP, download, 31
- Microsoft Open Specification Promise, 215
- Microsoft virtual labs, 581
- moving VMs from Virtual Server to Hyper-V, 366
- NTBackup, 512
- nWorks VMware management pack, 342
- offline VHD servicing, 307
- OpsMgr 2007, 343
- OpsMgr and SCVMM integration, 347
- OpsMgr and security, 451
- OpsMgr Management Packs, 347
- parent partition VLAN tagging, 112
- Performance Monitor scenarios, 198
- performance optimization, Hyper-V, 200
- performance, evaluating, 198
- PowerShell and SCVMM Administrator Console, 412
- Project Kensho and OVF, 373
- Quick Migration, 143
- Remote Desktops console, 152
- Resource Monitor, 188
- Robocopy utility, 545
- SC Operations Manager, Configuration Manager and Visio, 28
- SCDPM 2007 SP1, 530
- SCDPM agent installation, 538
- SCDPM requirements, 533, 535
- SCDPM Service Pack 1, 537
- screencast for Hyper-V configuration, Server Core, 67
- scripting in Windows PowerShell, 398
- scripts, elevating (PowerShell), 399
- SCVMM 2008, acquiring, 156
- securing Hyper-V, 449
- Security Configuration Wizard (SCW), 456
- security guides, Windows Server 2008, Vista and Hyper-V, 431
- Security in a Virtual World, 436
- self-signed certificates, 452
- Server Core and Windows PowerShell, 404
- shadow copies, 516
- snapshots, Hyper-V, 259
- SQL Server 2005, 343
- stepping in processors, 314
- supported Microsoft applications in VMs, 576
- SVVP, 575
- Type 1 hypervisors, 10
- Type 2 hypervisors, 9
- update 950050, 73
- upgrading RIS to WDS, 291
- USB storage devices, locking, 461
 - VHD Mount utility, 513
- virtual appliances, 581
- virtual hard disks, 238
- virtual machine failover clusters, 127
- virtualization layers, 4
- Vista Gadget, 201
- VLAN tagging, 436, 566
- VMC to Hyper-V Import tool, 367
- VMDK to VHD Converter, 371
- WBAdmin.exe, 516
- WDS Role installation, 292
- Windows Event IDs, 190
- Windows PowerShell and other platforms, 387
- Windows Server 2008 multi-site clusters, 132
- Windows Server Backup, 518
- Windows Server Deployment guidance, 291
- WinImage, 81, 247
- WinRE, 510
- working with MBSA and Visio, 28
- workloads, categorizing, 333
- Mouse release key, 94, 217
- MS-DOS, 216–218, 230–231
- Multi-homing, 492
- Multiprocessing support, 15
- Multi-site clusters, 49, 51, 124–126

N

Naming

- Administrator account, 62
- network adapters, 111–113
- virtual machine configuration files, 221
- virtual machine settings, 227
- virtual networks, 137
- NAS (network-attached storage), 5
- Native device drivers, 18–19
- netsh command, 68
- netsh firewall, 71
- Network access protection (NAP), 439, 443, 452
- Network adapters
 - configuring, 104, 111–113
 - failover clustering requirements, 128, 130
 - full vs. Server Core installations, 107–111
 - host optimization, 200
 - iSCSI storage, configuring, 566–569
 - network types, 104–107
 - number allowed, 248
 - parent partition overhead, 45
 - System Center Virtual Machine Manager (SCVMM), 159
 - virtual machine settings, 226
 - Virtual Network Manager tool, 111–113
 - VLAN tagging, 562–566
- Network bandwidth, 278–280
- Network cabling, 128
- Network component requirements, 130
- Network file transfers, 197
- Network interface cards (NIC)
 - inventories, 29
 - iSCSI security, 569–572
 - parent partition overhead, 45
 - Performance Monitor, 193
 - Task Manager, 187–190
- Network Interface counters, 197
- Network interfaces, virtualizing, 3–7
- Network Load Balancing (NLB)
 - fault tolerance, 123–127
 - guest network load balancing, 572
 - Hyper-V features, 14–15
 - manual conversions, 338–339
 - virtual machines, availability, 553–554
 - additional components, configuring, 574–575
 - case scenario, protecting Exchange 2007 VMs, 585
 - practice, assigning VLANs to VMs, 581–582
 - strategy selection, 573–574

- Network Power Pack, 409
- Network shares, backup, 530
- Network Storage System (Falcon Stor), 131
- Network-attached storage (NAS), software stack, 5
- Network-based SCSI (iSCSI), 129
- Networking. *See also* Network adapters
 - case scenario, virtual machines, 117
 - configuration, security and, 447
 - configuring, 64, 68
 - conversion, 336
 - hardware selection, 42
 - Hyper-V architecture, 20–23
 - Hyper-V features, 15
 - inventories, 29
 - performance monitoring, 197
 - redundancy, 574–575
 - resources, virtualizing, 3–7
 - SCDPM requirements, 532
 - SCVMM Administration Console, 276
 - SCVMM requirements, 171
 - segregating traffic, 436
 - Task Manager, 187–190
- New Virtual Machine Wizard, 98, 211, 243–248, 307, 310–314, 424
- FullName, 71
- NIC (Network Interface Card), 29, 45, 187–190, 193, 569–572
- NLB. *See* Network Load Balancing (NLB)
- Node and Disk Majority Quorum, 140
- NTBackup, 512
- NTFS access control entries (ACEs), 474–475
- nWorks, 342

O

- Objects, PowerShell cmdlets, 387–388
- OCLIST.exe, 77–78
- OCSETUP.exe, 77–78
- Office Groove Server, 577
- Office Performance Point Server, 577
- Office Project Server, 577
- Office SharePoint Server, 529, 577, 580
- Offline conversions, 334–335, 356–361
- Offline Virtual Machine Servicing Tool (OVMST), 495–496
- Online conversions, 334–335, 356–361
- Open Specification Promise, 215

Open Virtualization Format (OVF), 373, 581
 Operating System Shutdown, 212
 Operating systems. *See also* Guest operating systems
 backups, 508
 creating virtual machines, 211
 display time, 62, 65
 duplicating virtual machines, creating, 304–310
 elighted vs. legacy guests, 20–23
 guest operating systems, 16
 host optimization, 200
 legacy guests, 216–218, 230–231
 migration, preparing for, 331–332
 non-Windows guests, 215–216, 231
 practice, creating guest OS profile, 299–300
 practice, working with non-Windows VMs, 233–235
 SCDPM requirements, 532
 virtualizing, 3–7
 Windows Deployment Services (WDS), 289
 Windows Preinstallation Environment (WinPE), 290
 Operations Console, 342
 Operations Manager Database, 342, 577
 OpsMgr (Operations Manager), 17–18, 163, 347–353,
 356, 555
 OpsMgr Management Packs, 347–353
 Optical media, 518
 Optimization, Microsoft's Infrastructure
 Optimization, 30. *See also* Performance
 Output Queue Length counters, 197
 Overhead, resource usage, 44
 OVF (Open Virtualization Format) files, 373, 581
 OVMST (Offline Virtual Machine Servicing Tool),
 495–496

P

Page files, 63, 66, 72, 533
 Pages/second counters, 197
 Parallel Advanced Technology Attachment (PATA), 42
 Parallel SCSI, 130
 Parent partition. *See also* Partitions
 configuring virtual networks, 105–106, 110–111
 host computer security, 444, 446–447
 host optimization, 200
 Operating System Shutdown, 212
 virtual LANs, 112
 VLAN tagging, 565
 Parked virtual machines, securing, 488–489

Partitions
 backups, 508
 child partitions, Hyper-V, 211
 host computer security, 444, 446–447
 host server configuration, 65
 Hyper-V architecture, 18–19
 Hyper-V Integration Services, 212–213
 pass-through disks, 240–241
 planning, 29–30
 resource usage overhead, 44
 virtual hard disk storage, 239–240
 VLAN tagging, 565
 Pass-through disks, 240–241, 260–262, 267, 340,
 357, 535–536
 Passwords, 63, 69, 71, 440
 PATA (Parallel Advanced Technology Attachment), 42
 PATHPING.exe, 197
 PBX gateways, 339
 PDC Emulator Operations Master Role, 340, 494
 PEImg.exe, 290
 Percent Total Run Time counter, 198
 Performance
 BitLocker, 239–240
 hardware selection, 44
 host server configuration, 66
 Hyper-V architecture, 20–23
 Hyper-V features, 14
 legacy guests, 216
 Linux operating systems, 215
 Microsoft Assessment and Planning (MAP) tool, 31
 migrating from physical machines, 356
 multi-site clustering requirements, 131–132
 optimizing Hyper-V hosts
 managing system resources, 186–198
 operations, 199–201
 optimizing virtual machines, conversions, 339–340
 pass-through disks, 240
 practice, ADDS performance analysis, 201–205
 practice, assessing server performance, 35–37
 SCVMM host updates, 175
 Server Core installation, 67
 workload management, 559
 Performance and Resource Optimization (PRO)
 migrations, 332, 340–341, 555
 resource pool, securing, 451
 System Center Virtual Machine Manager
 (SCVMM), 160
 workload management, 559

- Performance Log and Alerts, 192
- Performance Log Users, 192
- Performance Monitor, 187, 192–196
- Permissions, host computers, 440
- Physical to Virtual (P2V) Conversion, 160.
 - See also* Migration
- Physical-to-virtual machine conversion, 6.
 - See also* Migration
- Ping test, 197
- PKI (Public Key Infrastructure), 46, 440, 443, 491
- Policies
 - auditing object access, 463
 - backups, 27
 - data control, 6
 - device control policies, 460
 - secure virtual service offerings, 490
 - Security Configuration Wizard (SCW), 454
 - Self-Service Portals, 317–318
 - usages, 6
- Polish language, 75
- Ports
 - port 2179, 271
 - port 443, 354
 - port 8100, 274
 - System Center Virtual Machine Manager (SCVMM), 166–167
 - TCP/IP, 167, 342
 - virtual machine settings, 219–220, 227
- Portuguese (Brazil) language, 75
- Portuguese (Portugal) language, 75
- Power consumption, 31
- Power Packs, 408–409, 428
- PowerGUI, 399, 408–409, 424
- PowerShell
 - case scenario, automating operations, 429
 - commands for SCVMM, 412
 - constructs, 389–391
 - managing Hyper-V operations, 402–409
 - overview, 383–384
 - practice using, 424–428
 - running scripts, 398–401
 - shortcut keys, 401
 - understanding PowerShell, 385–389
 - using, 391–398
 - using with SCVMM, 409–412, 422–423
 - Windows Server Backup, 519
- Practice
 - ADDs performance analysis, 201–205
 - assessments, environment, 34–39
 - assigning VLANs to VMs, 581–582
 - configuring Windows Server 2008 for Hyper-V, 97–102
 - conversions, source-to-target, 375–377
 - delegating administrative roles in SCVMM, 496–500
 - host failover clustering, planning, 144–147
 - Hyper-V deployment, preparing for, 52–54
 - Hyper-V role, installing, 85–90
 - performing internal VM backups, 542–546
 - SCVMM Library, working with, 293–303
 - security, creating the management virtual network, 467–470
 - System Center Virtual Machine Manager (SCVMM), installing, 176–185
 - understanding Hyper-V virtual machines, 23–24
 - virtual machine disks, working with, 259–263
 - virtual machine templates, managing, 318–324
 - virtual networks, working with, 113–116
 - Windows PowerShell, automating VM management, 424–428
- Preboot Execution Environment (PXE), 109, 290–292
- Presentation services, 3, 6
- Presentation virtualization, software stack, 4
- Previous Version client, 515–516, 529
- PrimalScript, 399
- Print servers, startup delay, 559
- Print system, host computer security, 443, 490
- Priority settings, 159
- Private virtual networks, 104–107, 109
- PRO (Performance and Resource Optimization)
 - live migration, 555
 - migration, 332, 340–341
 - resource pool, securing, 451
 - System Center Virtual Machine Manager (SCVMM), 160
 - workload management, 559
- PRO inheritance, 353
- Processes
 - performance monitoring, 198
 - SCDPM requirements, 531
 - Task Manager, 187–190
- Processors. *See also* x32 platforms; x64 platforms; x86 platforms
 - AMD processor validation utilities, 40
 - Hardware Profile, 159
 - hardware selection, Hyper-V, 40–47
 - Hyper-V architecture, 16, 18–19
 - Itanium, 1
 - management, 19

- migrations and, 556
- multiprocessing support, 15
- redundancy, 575
- SCVMM requirements, 170–171
- stepping, 314
- virtual machine settings, 219–220, 224
- Windows Server 2008 Hyper-V, 10–12
- Product key, 47, 323
- Profile virtualization
 - software stack, 6
- Profile virtualization, software stack, 4
- Project Kensho, 373
- Properties, viewing, 282
- Protection Groups, 538–540
- Protocols, Hyper-V architecture, 20–23
- Provisioning, 6, 338–339
- PSDrives, 389
- Public Key Infrastructure (PKI), 46, 440, 443, 491
- Public user profile, 96
- PXE (Preboot Execution Environment), 109, 290–292

Q

- Quest ActiveRoles Management Shell for Active Directory, 409
- Quick Migrate Virtual Machines, 142–143, 374, 555
- Quorum disk, 139–140

R

- RADIUS (Remote Authentication Dial-In User Service), 570–572
- RAID (redundant arrays of independent disks), 30, 128
- RAM
 - hosts, 42, 66, 278–280
 - Hyper-V features, 15
 - parent partition overhead, 45
 - redundancy, 575
 - SCDPM requirements, 535–536
 - SCVMM requirements, 170–171
 - virtual machine settings, 219–220, 224
- RAST (Remote Server Administration Tools)
 - Failover Cluster Management Console, 152
 - host server configuration, 63
 - Hyper-V Manager, 121–122, 149
 - updates, 66
 - Windows Server 2008, 12
 - Windows Server Backup, 522
- RBAC (role-based access control), 14, 440, 443, 490
- Reboot process, 65, 465–466
- Recovery
 - case scenario, host server failure, 547
 - default options, host servers, 63
 - host server configuration, 65–66
 - Hyper-V protection strategies, 508–510
 - overview, 505–507
 - practice, performing internal VM
 - backups, 542–546
 - resource pool, securing, 451
 - settings, Server Core installation, 72
- System Center Data Protection Manager (SCDPM)
 - host server and VM backups, 538–540
 - installing, 535–538
 - overview, 529–530
 - requirements, 531–535
 - restoring VMs, 540–541
 - SQL Server preparation, 535
- two-node clusters, 132
- virtual machine protection strategies, 510–516
- Windows Server Backup
 - overview, 516–518
 - PowerShell cmdlets, 519
 - protecting Hyper-V and virtual machines, 519–525
 - restoring systems with, 525–529
- Recovery to Original Location, 528
- Redundancy. *See also* Failover clustering
 - configuring virtual networks, 107
 - failover clustering requirements, 128, 130
 - host servers, 26
 - Microsoft Hyper-V Server 2008, 12–13
 - Network Load Balancing (NLB), 123–127
 - planning, 30
 - virtual machine storage and networking, 574–575
- Redundant arrays of independent disks (RAID), 30, 128
- Reference computers
 - copying, 307
 - creating, 304
- Registry Editor, 521
- Registry keys, 193
- Release to manufacturing (RTM) version, 59
- Reliability Monitor, 187, 191

Remote administration

- administrator description, 1–2
 - assigning roles with SCVMM, 486–487
 - AzMan, assigning roles, 481–486
 - deploying Hyper-V Manager, 148–152
 - Failover Cluster Management
 - Console, 152–154
 - failover clustering, 123–127
 - firewall, 61
 - Hyper-V features, 14
 - Hyper-V host configuration, 59
 - Microsoft Hyper-V Server 2008, 12–13
 - overview, 121–122
 - practice, delegating administrative roles in
 - SCVMM, 496–500
 - privileges, assigning, 435
 - Remote Desktop, 64
 - resource pool configuration, 121–122
 - SCVMM Administration Console, 270
 - securing Hyper-V resource pools, 435–436
 - Server Core installation, 67
 - System Center Virtual Machine Manager (SCVMM)
 - architecture, 164–165
 - communication ports, 166–167
 - distributed implementation
 - recommendations, 173–174
 - implementation, preparing for, 168–176
 - overview, 154–163, 269–273
 - practice, installing, 176–185
 - SCVMM add-ons, 289–293
 - SCVMM Library, 284–289
 - upgrading, 174–176
 - workstations, security and, 450
- Remote Authentication Dial-In User Service (RADIUS), 570–572
- Remote connections
 - Hyper-V Manager vs. SCVMM, 280–284
 - VirtualMachineViewer.exe, 271
- Remote Desktop, 61, 64, 70
- Remote Desktop Connections, 450
- Remote installation, 48, 290–291
- Remote Installation Services (RIS), 290–291
- Remote Registry Service, 31
- Remote Server Administration Tools (RAST)
 - Failover Cluster Management Console, 152
 - host server configuration, 63
 - Hyper-V Manager, 121–122, 149
 - updates, 66
 - Windows Server 2008 Hyper-V, 12
 - Windows Server Backups, 522
- Remote Server Share, 77
- Remote storage, 107
- Remote-site backups, 6
- Removable devices, 42, 441, 446, 457–461
- Replication, 49
- Replication engine, 131–132
- Report Metrics, 31
- Reporting Data Warehouse, 342
- Reporting Server, 343
- Reports
 - Microsoft Assessment and Planning (MAP)
 - tool, 31
 - performance, 198
 - SCVMM Administration Console, 276
 - SCVMM and OpsMgr, 163
 - System Center Virtual Machine Manager (SCVMM), 157
- Requests, Hyper-V architecture, 18–19
- Reset, Hyper-V features, 15
- Resource Monitor, 187
- Resource pool administration.
 - See also* Remote administration
 - administrator description, 1–2
 - failover clustering, 123–127
 - overview, 121–122
 - resource pool forests, 64
 - SCVMM Administration Console, 270
 - securing Hyper-V resource pools, 435–436
- Resource pool configuration
 - case scenario, deploying SCVMM, 206
 - Failover Cluster Management Console, 152–154
 - failover clustering, 123–127
 - failover clustering, requirements, 127–132
 - hardware selection, 43
 - host failovers, managing, 142–143
 - host remote administration, 148–152
 - Hyper-V protection strategies, 508–510
 - multi-site clustering requirements, 131–132
 - optimizing Hyper-V hosts
 - managing system resources, 186–198
 - operations, 199–201
 - overview, 49–52
 - planning, 91–93
 - practice, ADDS performance analysis, 201–205
 - practice, planning host failover
 - clustering, 144–147

System Center Virtual Machine Manager (SCVMM)
 architecture, 164–165
 communication ports, 166–167
 distributed implementation recommendations,
 173–174
 implementation, preparing for, 168–176
 overview, 154–163
 practice, installing, 176–185
 upgrading, 174–176
 two-node clusters, creating
 Hyper-V role installation, 133–137
 overview, 132
 server and operating system, 133
 validating, 137–140
 virtual machine creation, 141–142
 virtual network creation, 137

Resource pools, backup and recovery
 case scenario, host server failure, 547
 overview, 505–507
 practice, performing internal VM backups, 542–546

System Center Data Protection Manager (SCDPM)
 host server and VM backups, 538–540
 installing, 535–538
 overview, 529–530
 requirements, 531–535
 restoring VMs, 540–541
 SQL Server preparation, 535

virtual machine protection strategies, 510–516

Windows Server Backup
 overview, 516–518
 PowerShell cmdlets, 519
 protecting Hyper-V and virtual machines, 519–525
 restoring systems with, 525–529

Resources
 allocation, 199
 fixed and variable, virtual machines, 223
 host computer security, 443
 host groups, 278
 host server usage, 44–46
 Hyper-V architecture, 18–19
 managing system resources, 186–198
 optimization, 8
 SCVMM Library, 284–285
 secure virtual service offerings, 490
 storage, security, 448
 virtualizing, 3–7

Restart, 556

Restore, 156, 339, 525–529. *See also* Recovery

Roaming Profile, software stack, 6
 Robocopy utility, 545
 Rocket Division Software, 144
 Role-based access control (RBAC), 14, 440, 443, 490
 Role-based administration, 64, 160
 Root partitioning, Hyper-V architecture, 16
 RootkitRevealer, 439
 Routing and remote access (RRAS), 443, 452, 491
 RTM (release to manufacturing), 59
 Russian language, 75

S

SANs (storage area networks). *See also* Storage
 backup, 506
 file locations, virtual machines, 96
 hardware selection, 42
 integration, 160
 Library Server, 285
 software stack, 5
 using SCVMM, 310
 Windows Server 2008 installation, 48–49

Sapien Technologies, 399

SAS (serial attached SCSI), 42, 129

SATA (Serial Advanced Technology Attachment), 42

Save states, virtual machines, 222

Saved state files (.vsv), 288, 365

SCDPM. *See* System Center Data Protection Manager (SCDPM)

Scripts
 adding Library Server, 285–287
 installation, 284–285
 SCVMM Library, 288
 Windows PowerShell
 case scenario, automating operations, 429
 commands for SCVMM, 412
 constructs, 389–391
 managing Hyper-V operations, 402–409
 overview, 383–384
 practice using, 424–428
 running scripts, 398–401
 shortcut keys, 401
 understanding PowerShell, 385–389
 using with SCVMM, 409–412, 422–423

SCSI (Small Computer System Interface)
 add or remove connectors, 247
 hardware selection, 42

- Hyper-V architecture, 20–23
- migration, 332, 365
- virtual machines, 241–243
- vs. IDE, 229
- SCSI Primary Commands-3 (SPC-3), 130
- SCSI virtual adapters, conversions, 340
- SCVMM. *See* System Center Virtual Machine Manager (SCVMM)
- SCVMM Administrator Console
 - creating virtual machines, 310
 - host server management, 269–273
 - PowerShell scripting, 422
 - practice, installing, 183–184
 - user interface, 273–277
- SCVMM Agent, 162, 184
- SCVMM Library Server, 293–303, 451
- SCVMM P2V Wizard, 357–361
- SCVMM Server, 162
- SCW (Security Configuration Wizard), 441, 453–457, 463, 491
- Search Server, 577
- SecurAble, 41
- Secure HTTP (HTTPS), 165
- Secure Sockets Layer (SSL), 165, 354, 443, 452
- Secure Sockets Tunneling Protocol (SSTP), 443, 452, 491
- Security
 - access control features, 14
 - attack surface, 12, 15, 436–439
 - auditing object access, 463–465
 - BitLocker, 461–462
 - buffer overflow errors, 40–41
 - case scenario, planning resource pool strategy, 502
 - clients, 31
 - host and virtual machines, overview, 431–434
 - host computers, features, 439–441
 - Hyper-V configuration, 80
 - Hyper-V hosts, 441–449
 - Hyper-V management roles
 - assigning with SCVMM, 486–487
 - assigning with, AzMan, 481–486
 - Authorization Manager (AzMan), introducing, 471–475
 - Hyper-V resource pools, 435–436
 - Hyper-V virtual machines, 488–491
 - iSCSI security, 569–572
 - management, 64
 - populating VMs on host servers, 491–496
 - practice

- creating the management virtual network, 467–470
- delegating administrative roles in SCVMM, 496–500
- removable devices, 457–461
- resource pool, 449–452
- SCDPM requirements, 533
- SCVMM PowerShell, 411
- Security Configuration Wizard (SCW), 441, 453–457, 463, 491
- System Center Virtual Machine Manager (SCVMM), 174
 - updating host servers, 465–466
 - virtual hard disks, 239–240
- Security Configuration Wizard (SCW), 441, 453–457, 463, 491
- Security Event Log, 465
- Security guides, 431
- Security in a Virtual World, 436
- Self-Service Portal, 161–162, 165
- Self-Service User Roles, 317–318
- Serial (COM) ports, 43, 219–220, 227
- Serial Advanced Technology Attachment (SATA), 42
- Serial attached SCSI (SAS), 42, 129
- Server Core
 - attack surface, 438
 - Authorization Manager (AzMan), 472
 - configuring, 67–72
 - host optimization, 200
 - Hyper-V features, 15
 - Hyper-V role, 76–78
 - installation, automating, 62
 - iSCSI, enabling, 572
 - managing from Windows Vista, 151
 - Microsoft Hyper-V Server 2008, 12–13
 - practice, create virtual switch, 114–116
 - practice, installing, 53–54
 - SCVMM Library, 284
 - two-node clusters, creating, 133
 - updates, 70
 - Windows PowerShell, 386, 403–404, 408
 - Windows Server 2008 Hyper-V, 12
- Server Management Suite Enterprise (SMSE), 156
- Server Manager
 - Event Viewer, 189
 - host server configuration, 64–67
 - Hyper-V features, 15
 - Hyper-V management tools, 91–93
 - memory, insufficient, 187
 - Windows Server Backup, 516

- Server message block (SMB) protocol, 42
- Server Performance Advisor (SPA), 192, 196
- Server roles, 31
- Server Virtualization Validation Program (SVVP), 575–581
- Server-based virtual machine operation, software stack, 6
- ServerName, 71
- Servers. *See also* Server Manager
 - activation, 62, 65
 - backup, 506
 - case scenario, preparing for server virtualization, 55–56
 - host configuration, 61–72
 - inventory, 28
 - populating VMs on host servers, security, 491–496
 - power consumption, 31
 - practice, performance assessment, 35–37
 - SCVMM Administrator Console user interface, 273–277
 - System Center Virtual Machine Manager (SCVMM), 159
 - transforming to virtual machines, 26
 - virtualization layer, 25
 - virtualization, software stack, 4
- ServerShare, 77
- Service flexibility, hypervisor, 8
- Service volume, failover clustering requirements, 129
- Services, Task Manager, 187–190
- Settings
 - advanced virtual machine configurations, 223–231
 - host computer security, 445
 - network adapters, 107
 - overview, 93–95
 - practice, configuring, 97–98
 - Security Configuration Wizard (SCW), 441, 453
 - virtual machines, 15, 211, 219–220, 281
- Shadow copies, 516
- Shared folder, Windows Server Backup, 517
- Shared storage connectivity, 129
- Shared storage containers, 129, 139–140
- Shared volumes, update alert, 572
- Shared-nothing clustering, 124
- Shortcut keys, PowerShell, 401
- Sigcheck, 439
- Signatures, digital, 46–47
- Signing requirements, 46
- Simple Network Management Protocol (SNMP), 31
- Simple Object Access Protocol (SOAP), 164
- Single-site clusters, 49, 51, 124–126
- Small Computer System Interface (SCSI). *See* SCSI (Small Computer System Interface)
- SMP (symmetric multiprocessing), 9–10
- Snapshots
 - backup strategies, 508
 - hardware selection, 43
 - host optimization, 200
 - Hyper-V features, 15
 - Hyper-V Manager, 93
 - location of, 229
 - migration, 365
 - System Center Data Protection Manager (SCDPM), 529–530
 - virtual machines, 219–220, 222, 228, 510–516
 - vs. Volume Shadow Copy Service (VSS), 512
 - VSS, using on file shares, 513–516
 - working with Hyper-V Snapshots, 255–259
- SNMP (Simple Network Management Protocol), 31
- SOAP (Simple Object Access Protocol), 164
- Software. *See also* Update Alerts; Updates
 - change tracking, 191
 - compatibility, 46–47
 - restriction policies, 439
 - SCDPM requirements, 532
 - SCVMM requirements, 170
 - software vs. hardware virtualization, 7–10
 - System Center Operations Manager requirements, 342
 - updates, 11
- Software stack, 4–7
- Solaris operating system, 9
- SPA (Server Performance Advisor), 192, 196
- SQL Server, 338, 535, 577
- SQL Server 2008, 31, 173, 450, 529
- SQL Server authorization store, 473
- SQL Server Express, 171
- SQL Server Management Studio, 174
- SSCM (System Center Configuration Manager), 28
- SSL (secure sockets layer), 354, 443, 452
- SSTP (Secure Sockets Tunneling Protocol), 443, 452, 491
- Stand-alone hosts, 51
- Startup, 65, 224, 556, 559
- StarWind Server, 144
- Stateful services, 123
- Stateful workloads, 553–554
- Stateless services, 123
- Stateless workloads, 553–554

- Static VLANs, 564
- staticIPAddress, 69
- Status values, 283
- SteelEye, 131
- Storage. *See also* Backups; Recovery
 - conversions, 336
 - event messages, 341
 - failover clustering requirements, 129–130
 - file locations, virtual machines, 95–96
 - hardware selection, 42
 - host computer security, 445, 448
 - Hyper-V architecture, 18–23
 - iSCSI, 560
 - ISO Store, 285
 - Library Server, 285
 - local, backup, 530
 - multi-site clustering requirements, 131–132
 - parent partition overhead, 45
 - planning, 30
 - quorum disk, 139–140
 - remote, 107
 - SCDPM requirements, 533
 - Server Core installation, 72
 - shared, planning, 30
 - Snapshots, virtual machines, 257–259
 - system calls, 18–19
 - USB devices, 42, 446, 457–461
 - virtual hard disks, understanding, 236–243
 - virtualizing, 3–7
- Storage area networks (SANs)
 - backup, 506
 - file locations, virtual machines, 96
 - hardware selection, 42
 - integrator, 160
 - Library Server, 285
 - software stack, 5
 - using SCVMM, 310
- Storage virtualization, software stack, 4
- Stored virtual machines, 160–161
- SubnetMask, 69
- Sun Microsystems, hypervisors, 9–10
- Surveillance, host computer security, 442
- SVVP (Server Virtualization Validation Program), 575–581
- Swedish language, 76
- Switches, 42, 107–111, 114–116
- Symantec Ghost, 331
- Symmetric multiprocessing (SMP), 9–10
- SysPrep, 160, 308–309
- System calls, Hyper-V architecture, 18–19
- System Center Configuration Manager (SCCM)
 - acquiring, 156
 - creating and managing VMs, 310–318
 - environment inventory, 28
 - evaluation VHDs, 580
 - resource pool, securing, 451
 - software stack, 7
 - support for virtualization, 577
- System Center Data Protection Manager (SCDPM)
 - host server and virtual machine backups, 538–540
 - installing, 535–538
 - overview, 529–530
 - requirements, 531–535
 - resource pool, securing, 451
 - restoring VMs, 540–541
 - software stack, 6
 - SQL Server preparation, 535
 - support for virtualization, 578
- System Center Database Server, 450
- System Center Essentials, 451, 578, 580
- System Center GUI, 161
- System Center Operations Manager
 - acquiring, 156
 - installing, 341–347
 - resource pool, securing, 451
 - SCVMM architecture, 165
 - software stack, 7
 - support for virtualization, 578
- System Center Virtual Machine Manager (SCVMM)
 - add-ons, 289–293
 - architecture, 164–165
 - assigning management roles, 486–487
 - Authorization Manager and, 481
 - automation of virtual machine creation, 269–273
 - case scenario, deploying SCVMM, 206
 - communication ports, 166–167
 - decision flow, 172
 - deploying Hyper-V, 26
 - distributed implementation recommendations, 173–174
 - evaluation VHDs, 580
 - failover clustering, 127
 - host server configuration, 64
 - Hyper-V architecture, 17–18
 - implementation, preparing for, 168–176
 - integrating SCVMM with VMware ESX, 353–354

- integrating with OpsMgr, 347–353
- on SANS, 310
- overview, 154–163
- planning resource placement, 30
- PowerShell commands, 412
- practice
 - installing, 176–185
 - managing virtual machine templates, 318–324
 - working with SCVMM Library, 293–303
- resource pool configuration, 121–122
- resource pool, securing, 450
- SCVMM Library, 284–289, 451
- SCVMM templates, 288
- software stack, 6
- upgrading, 174–176
- using PowerShell, 409–412, 422–423
- versions covered, 148
- VMM Self-Service Portal, 315–318
- vs. Authorization Manager, 471
- vs. Hyper-V Manager, 280–284
- workload management, 559
- System consolidation, hypervisors, 8
- System counters, 192–193, 195–196
- System Diagnostics, 193
- System images, 290, 292
- System Monitor, 192
- System operation, hypervisor, 8
- System Performance, 193
- System Preparation Tool (SysPrep.exe), 48, 290
- System Properties, host server configuration, 65
- System state data, 530
- Systems Management Server, 28, 578

T

- Tape backups, 530
- Task Manager, 186–190
- Tasks, 269, 484
- TCP Chimney Offload, 106
- TCP/IP ports, 167, 342
- Templates
 - Data Collector Set, 193
 - practice, managing virtual machine templates, 318–324
 - product keys and, 323
 - SCVMM Library, 284–285
 - SCVMM templates, 288

- System Center Virtual Machine Manager (SCVMM), 161
 - virtual machines, creating, 218–219, 309–310
 - virtual machines, managing, 269, 309–310
 - VMware templates, 288
- Terminal Services, 218, 339
- Terminal Services ActiveX Control (MSTSCAX.dll), 271
- Terminal Services RemoteApp, 91–93
- Test servers, startup delay, 559
- Testing, system, 8
- Third-party backup and restore tools, 510
- Third-party device drivers, 18–19
- Third-party disk images, 368–371
- Third-party hypervisors, 575
- Third-party tool development, 14
- TIB images, 368
- Time
 - host server configuration, 62, 65
 - Server Core installation, 68
 - setting, 64
 - synchronization, 212, 340, 494
 - zones, configuring, 61
- Toolbars, 281
- TPM module, 461
- Transactional applications, availability, 553
- TripWire, 439
- Trusts, 46, 173, 437–439
- Turkish language, 76
- Type 1 hypervisor, 7–10
- Type 2 hypervisor, 7–10

U

- UAC (User Account Control), 450
- Unattend.xml, 48
- Unattended installation answer files, 284–285, 294–299
- UNC (Universal Naming Convention), 77
- Undo Disks, 365
- Unified Messaging role, 339
- Universal Naming Convention (UNC), 77
- Universal Serial Bus (USB), 42, 441, 446, 457–461
- Update Alerts. *See also* Updates
 - cluster shared volumes, 572
 - Hyper-V backups, issues with, 522
 - Hyper-V characteristics, 43
 - Hyper-V Manager, running from Windows 7, 151
 - Hyper-V security guide, 431

Updates

- Hyper-V shared-everything clusters, 124
- live migrations in Windows Server 2008, 555
- MAC Address Management in Windows Server 2008 R2, 229
- Microsoft Cluster Update for Hyper-V, 137
- network adapter teaming and TCP Chimney Offload, 106
- Service Pack 2, 59
- VM Settings UI in Windows Server 2008 R2, 229
- Windows PowerShell and Server Core, 386
- Updates. *See also* Update Alerts
 - 950050, 148
 - 951308, 143
 - automatic, configuring, 61, 64, 76
 - configuring, 70
 - host computer security, 446
 - Hyper-V hosts, 79–80
 - Hyper-V role installation, 72–76
 - Integration Services, 534
 - KB951308, 534
 - KB959962, 534
 - KB960038, 534
 - language, 75–76
 - network access protection (NAP), 439
 - offline/parked virtual machines, 489, 495–496
 - resource pool, securing, 450–451
 - SCDPM Service Pack 1, 537–538
 - SCVMM host updates, 175
 - updating host servers, 465–466
 - Windows Server 2008 Hyper-V, 11
- Usage policies, software stack, 6
- USB (Universal Serial Bus), 42, 441, 446, 457–461
- User Account Control (UAC), 450
- User interface, 63, 66
- User mode, 18–19
- UserName, 71
- Users
 - credentials, Hyper-V settings, 94
 - identification, 443, 490
 - profiles, 3, 63, 66, 96
 - roles, 276
 - settings, 96
 - Task Manager, 187–190
- Utilities. *See also* PowerShell
 - cmdlets, PowerShell, 387
 - Desired Configuration Management, 439
 - hardware validation, 40
 - Hyper-V Remote Management Configuration, 486

- Robocopy, 545
- RootkitRevealer, 439
- Sigcheck, 439
- TripWire, 439
- Utility development, 14
- Utility forest, 444

V

- Validate A Configuration Wizard, 137
- Validation, 40–41, 137–140
- Variable resources, 223
- Variables, PowerShell constructs, 389
- VDI (Virtual Desktop Infrastructure), software stack, 6
- VDS (virtual disk service), 72
- VECD (Vista Enterprise Centralized Desktop), 6
- VHD (Virtual Hard Disk) tools, 15
- VHDs (virtual hard disks). *See* Virtual hard disks (VHDs)
- Video, 14, 18–19
- Virtual appliances, 581
- Virtual Desktop Infrastructure (VDI), 6
- Virtual devices, Hyper-V architecture, 18–19
- Virtual disk service (VDS), 72
- Virtual engine access, 435
- Virtual floppy disks, 288, 446, 450
- Virtual Hard Disk (VHD) tools, 15
- Virtual hard disk file (.vhd), 245
- Virtual Hard Disk Wizard, 243–248
- Virtual hard disks (VHDs). *See also* Migration disk files, 221
 - duplicate virtual machine, creating, 304–310
 - editing, 249–251
 - evaluation VHDs, 579–581
 - file locations, 96
 - hardware selection, 43
 - Hyper-V settings, 94
 - inspecting, 254–255
 - practice, obtaining images, 23–24
 - practice, working with, 259–262
 - SCDPM installation, 535–536
 - SCVMM Library, 284–285, 288
 - software stacks, 5
 - storing, 59
 - System Center Virtual Machine Manager (SCVMM), 160
 - understanding, 236–243
 - VHD Mount utility, 513
 - virtual machine settings, 219–220, 225

- Virtual local area network (VLAN)
 - assigning, 112
 - guest failover clustering, 560
 - practice, assigning VLANs to VMs, 581–582
 - VLAN tagging, 562–566
- Virtual local area network (VLAN) channel, 42
- Virtual Machine Additions, 365–366
- Virtual Machine Bus (VMBus), 16, 18–19, 215–216
- Virtual machine configuration (VMC) files, 362, 367
- Virtual Machine Connection tool, 73, 217, 280–284
- Virtual Machine Management Service, 19
- Virtual Machine Manager (VMM), 121–122, 174, 275
- Virtual Machine Manager (VMM) Service, 162
- Virtual Machine Manager Administrator, 174
- Virtual Machine Remote Control, 174, 272
- Virtual Machine Remote Control ActiveX Control, 270
- Virtual Machine Service (VM Service), 18–19
- Virtual machine templates, 160, 284–285
- Virtual Machine User role, 487
- Virtual Machine Viewer, 271, 281–284
- Virtual Machine Worker (VM Worker), 18–19
- Virtual machines (VMs)
 - backups, 508
 - practice, performing internal VM backups, 542–546
 - case scenario, networking, 117
 - case scenario, provisioning, 325
 - deploying, 27
 - file makeup, 220–223
 - hardware selection, 42
 - hybrid, 240
 - Hyper-V management role
 - assigning roles, AzMan, 481–486
 - assigning with SCVMM, 486–487
 - Authorization Manager (AzMan), introducing, 472–475
 - Hyper-V Manager, 93
 - overview, 471–472
 - Hyper-V settings, 94
 - libraries, 6
 - locked in, 240–241
 - moving with SCVMM, 314–315
 - placement, planning, 30
 - practice
 - exporting, 176–177
 - importing, 178
 - working with non-Windows VMs, 233–235
 - settings, 211, 245
 - snapshots, 15
 - software stack, 6
 - status of, 269
 - templates, 309–310
 - time synchronization, 494
 - transforming servers, 26
 - two-node clusters, creating, 141–142
 - updating offline machines, 495–496
 - Windows Server 2008 Hyper-V, 3
 - Windows Server Backup, 519–525
- Virtual machines (VMs), availability
 - additional components, configuring, 574–575
 - case scenario, protecting Exchange 2007 VMs, 585
 - guest failover clustering, 560–562
 - guest network load balancing, 572
 - host failover clusters, 554–560
 - iSCSI security, 569–572
 - iSCSI storage, configuring, 566–569
 - overview, 553–554
 - practice, assigning VLANs to VMs, 581–582
 - strategy selection, 573–574
 - supported VM configurations, 575–581
 - VLAN tagging, 562–566
- Virtual machines (VMs), creating
 - advanced setting configurations, 223–231
 - basic virtual machines, 219–223
 - case scenario, moving a virtual machine, 263
 - child partition, Hyper-V, 211
 - creating and managing VMs with SCVMM, 310–318
 - duplicate virtual machines, 304–310
 - editing virtual hard disks, 249–251
 - examining virtual machine states, 232–233
 - Hyper-V Integration Services, 212–218
 - Hyper-V Manager vs. SCVMM, 280–284
 - inspecting virtual hard disks, 254–255
 - legacy guests, installing, 230–231
 - overview, 218–219, 267–268
 - practice, creating, 98–99
 - practice, managing virtual machine templates, 318–324
 - practice, working with VM disks, 259–262
 - SCVMM add-ons, 289–293
 - SCVMM Administration Console, 276
 - SCVMM Library, 284–289
 - SCVMM, overview, 269–273
 - Snapshots, working with, 255–259
 - Virtual Hard Disk Wizard, 243–248
 - virtual hard disks, 236–243
 - VMM Self-Service Portal, 315–318

Virtual machines (VMs), security

- attack surface, Hyper-V, 436–439
 - auditing object access, 463–465
 - BitLocker, 461–462
 - case scenario, planning resource pool strategy, 502
 - delegating administrative roles in SCVMM, 496–500
 - host computer security, 441–449
 - host computers, features of, 439–441
 - Hyper-V resource pools, securing, 435–436
 - Hyper-V virtual machines, 488–491
 - overview, 431–434
 - populating VMs on host servers, 491–496
 - practice, creating the management virtual network, 467–470
 - protection strategies, 510–516
 - removable devices, 457–461
 - resource pool, securing, 449–452
 - Security Configuration Wizard (SCW), 453–457
 - System Center Data Protection Manager (SCDPM), 530
 - performing backups, 538–540
 - restoring VMs, 540–541
 - updating host servers, 465–466
- Virtual network adaptors. *See* Network adapters
- Virtual Network Computing (VNC) protocol, 271
- Virtual Network Switch creation, 74
- Virtual networks
- configuring
 - full vs. Server Core installations, 107–111
 - network types, 104–107
 - overview, 104
 - Virtual Network Manager tool, 111–113
 - Hyper-V features, 15
 - practice, working with, 113–116
 - security, populating VMs on host servers, 491–496
 - two-node clusters, creating, 137
- Virtual PC, 6, 362–366, 368
- Virtual private networks (VPNs), 443, 452, 491
- Virtual SCSI support, 15
- Virtual Server, 365, 368, 530
- Virtual Server 2005
- migrating from, 362–366
 - R2 SP1 Update, 175
 - System Center Virtual Machine Manager (SCVMM), 155, 159, 163, 174
 - VMRC.exe, 271
- Virtual Service Client (VSC), 14, 18–19, 214–216
- Virtual Service Provider (VSP), 14, 18–19, 214–216
- Virtual switch, 107–111, 114–116
- Virtual to physical conversions. *See* Migration
- Virtual to virtual conversions. *See* Migration
- Virtualization
- Microsoft Assessment and Planning (MAP) tool, 31
 - practice, recommendation assessment, 37–39
- Virtualization drivers, 369
- Virtualization Infrastructure Driver, 19
- Virtualization Managers, 276
- Virtualization Service Client (VSC), 214–215
- Virtualization Service Providers (VSP), 18–19, 214–215
- Virtualization Service Version, status, 283
- Virtualization Service, status of, 283
- Virtualizing resources, datacenter, 3–7
- Visio, 28
- Visio Connector for System Center Operations Manager, 28
- Vista Enterprise Centralized Desktop (VECD), 6
- Visual Studio Team System, 578
- Virtual floppy disks, 160
- VLAN (virtual local area network)
- assigning, 112
 - guest failover clustering, 560
 - hardware selection, 42
 - practice, assigning VLANs to VMs, 581–582
 - VLAN tagging, 562–566
- VM heartbeat, 199
- VM Service (Virtual Machine Service), 18–19
- VM Worker (Virtual Machine Worker), 18–19
- VMAdmin.exe, 270
- VMareESX, 26
- VMbus (Virtual Machine Bus), 16, 18–19, 215–216
- VMC (virtual machine configuration) files, 362, 367
- VMM Self-Service Portal, 315–318
- VMRC.exe, 271
- VMware
- attack surface, Hyper-V, 436
 - management packs, 342
 - migration, 331, 371–372
 - SCVMM Library, 288
 - SVVP certified, 575
 - TIB files, 368
- VMware ESX, 155, 159, 163, 165, 272, 353–354, 371–372
- VMware ESXi Server, 155, 159, 163, 165, 272, 354
- VMware Server, 9–10
- VMware templates, 288
- VMware Virtual Center, 354
- VMware virtual hard disk formats (.vmdk), 288

VMware Virtual Infrastructure 3, 155, 159
 VMware Virtual Infrastructure Application
 Programming Interface, 165
 VMware Workstation, 9
 VMwareViewer.exe, 272
 VNC (Virtual Network Computing) protocol, 271
 Voice over IP (VOIP), 339
 Volume Shadow Copy Service (VSS)
 backups, 508
 creating virtual machines, 213
 Hyper-V features, 15
 using on file shares, 513–516
 virtual machines, 222
 vs. Hyper-V Snapshots, 512
 Volumes
 backup, 530
 restoring, 526
 VPNs (virtual private networks), 443, 452, 491
 VSC (virtual service client), 14, 18–19, 214–216
 VSP (virtual service provider), 14, 18–19, 214–216
 VSS (Volume Shadow Copy Service)
 creating virtual machines, 213
 Hyper-V features, 15
 using on file shares, 513–516
 virtual machines, 222
 vs. Hyper-V Snapshots, 512

W

WAIK (Windows Automated Installation Kit), 48,
 289–290
 Warning events, 189
 WBAdmin.exe, 519
 WDS (Windows Deployment Services), 48, 289–293
 Web Console, 343
 Web servers, 123, 559
 Web Service Management Protocol
 (Ws-Management), 164
 Web Sites. *See* More Info
 Web-based components, 162
 WIM (Windows Imaging Format), 292
 Windows 2000, 371–372
 Windows 2003, 580
 Windows 3.x, legacy guests, 216–218
 Windows 7, 151, 290, 578
 Windows Authorization Manager (AzMan), 14, 26–27,
 471–475, 481–486

Windows Automated Installation Kit
 (WAIK), 48, 289–290
 Windows Backup (NTBackup.exe), 516
 Windows Defender, 442
 Windows Deployment Services (WDS), 48, 289–293
 Windows Deployment Services Configuration
 Wizard, 292–293
 Windows Essentials Business Server, 25, 578
 Windows Event Log, 189–191
 Windows Explorer, 287
 Windows failures, change tracking, 191
 Windows Firewall, 456, 517. *See also* Firewalls
 Windows Firewall, 166–167
 Windows HPC Server, 21–22, 214–215, 578
 Windows Hyper-V Server, software stack, 6
 Windows Hypervisor Interface Library, 19
 Windows Imaging Format (WIM), 292
 Windows Installer, 440
 Windows Management Instrumentation (WMI), 14,
 18–19, 31, 105–106, 165, 402
 Windows NT, 216–218, 230–231
 Windows NTBackup, 512
 Windows Package Manager (PKGmgr.exe), 153
 Windows PE (Preinstallation Environment), 291, 335, 510
 Windows PE (Preinstallation Environment) engine, 47,
 290, 510
 Windows Performance Monitor, 192–195
 Windows PowerShell, 67
 adding Library Server, 285–287
 case scenario, automating operations, 429
 commands for SCVMM, 412
 constructs, 389–391
 conversions, 361
 managing Hyper-V operations, 402–409
 overview, 383–384
 practice using, 424–428
 running scripts, 398–401
 shortcut keys, 401
 System Center Virtual Machine Manager
 (SCVMM), 162
 understanding PowerShell, 385–389
 using PowerShell, 391–398
 using with SCVMM, 409–412, 422–423
 Windows Server Backup, 517
 Windows PowerShell Integration, 161
 Windows Recovery Environment (WinRE), 63, 66, 510
 Windows Reliability and Performance, 198
 Windows Reliability Monitor, 191

Windows Remote Management (WinRM)

Windows Remote Management (WinRM), 164

Windows Remote Shell (WinRS), 72

Windows Server 2000, 21–22, 73, 214–215

Windows Server 2003

- guest operating systems, 21

- Hyper-V Integration Services, 214–215

- Hyper-V role installation, 73

- migrating VMware formats to Hyper-V, 371–372

- online conversions, 356

- SCDPM requirements, 532

- SCVMM Console, 273

- SCVMM Library, 284

- SCVMM Self-Service Portal, 316

- System Center Virtual Machine Manager (SCVMM), 155–156

- Windows Deployment Services, 290

- x64 platforms, 21

- x86 platforms, 21

Windows Server 2008

- 32-bit editions, 10

- Datacenter edition, 7, 10

- Enterprise edition, 7, 10

- Enterprise Server Core, 580

- Hyper-V Integration Services, 214–215

- Hyper-V role installation, 73

- installing, 47–52

- MAC address management, 229

- memory requirements, RAM, 45

- Microsoft Assessment and Planning (MAP) tool, 31

- migrating from VMware formats, 371–372

- on-line conversions, 356

- practice

 - configuring for Hyper-V, 97–102

 - downloading ISO file, 294

 - installing, 52

- Remote Server Administration Tools (RAST), 12

- SCDPM requirements, 532

- SCVMM Console, 273

- SCVMM Library, 284

- SCVMM Self-Service Portal, 316

- secure virtual service offerings, 489–491

- server roles, 31

- Service Pack 2, 59

- software stack, 5

- Standard edition, 7, 10

- system images, 292

- System Preparation Tool, 290

- update alert, live migrations, 555

VM settings UI, 229

Windows Deployment Services, 290

Windows Preinstallation Environment (WinPE), 290

Windows Server Backup (WSB), 516–518, 522

- x64 editions, 10, 21

- x86 editions, 10, 21

Windows Server 2008 Hyper-V.

- See also* Windows Server 2008

- architecture

 - enlightened vs. legacy guests, 20–23

 - overview, 16–18

 - parent vs. child partitions, 18–19

- datacenter, virtualizing, 3–7

- exploring, 10–12

- features, Hyper-V, 13–16

- overview, 12–13

- practice, understanding virtual machines, 23–24

- software vs. hardware virtualization, 7–10

- System Center Virtual Machine Manager

 - (SCVMM), 155, 159

Windows Server 2008 Interface, 195–196

Windows Server 2008 Security Guide, 431

Windows Server 2008 Server Core, 53–54

Windows Server 2008 Terminal Services, 6

Windows Server 2008 with Active Directory, 6

Windows Server Backup (WSB), 510, 516–518

Windows Server Failover Clustering, 572

Windows Server Firewall with Advanced

- Security, 439–440

Windows Server Hardware Catalog, 46

Windows Server Update Services (WSUS), 70, 451, 578

Windows Server Web edition, 578

Windows Server, Hyper-V, 575–581

Windows SharePoint Services, 529, 579

Windows Small Business Server, 578

Windows Storage Server, 5, 532, 566–567

Windows System Image Manager, 48, 290

Windows Unified Data Storage Server, 5, 566–567

Windows Updater Standalone Installer

- (WUSA.exe), 150, 153

Windows Vista

- administrator workstations, 450

- backup, 530

- evaluation VHDs, 580

- Failover Cluster Management Console, 152

- failover clustering, 136

- guest operating systems, 21

- Hyper-V Integration Services, 214–215

- Hyper-V Manager, 92, 149–150
- Hyper-V role installation, 73
- installing Windows Server 2008, 47
- Microsoft Assessment and Planning (MAP) tool, 31
- migrating VMware formats to Hyper-V, 371–372
- on-line conversions, 356
- removable devices, security, 457–461
- SCVMM Console, 273
- Server Core, managing, 151
- Service Pack 1, 66
- support for virtualization, 579
- system images, 292
- System Preparation Tool, 290
- Windows Preinstallation Environment (WinPE), 290
- Windows Server Backup, 522
- Windows Vista Security Guide, 431
- Windows XP
 - backups, 530
 - guest operating systems, 21
 - Hyper-V Integration Services, 214–215
 - Hyper-V role installation, 73
 - migrating VMware formats to Hyper-V, 371–372
 - on-line conversion, 356
 - SCVMM Console, 273
 - support for virtualization, 579
 - system images, 292
- WinImage, 81, 246–247, 368–371
- WinRE (Windows Recovery Environment), 63, 66, 510, 525–529
- WinRM, 164
- WinRS (Windows Remote Shell), 72
- Wireless network adapters, 107
- Witness disk, 129
- Wizards
 - Add Features Wizard, 149
 - Add Library Server, 285–287
 - Add Roles Wizard, 74
 - Conversion Wizard, 371
 - Encryption Key Wizard, 346
 - Hyper-V New Virtual Machine Wizard, 219–223
 - New Virtual Machine Wizard, 98, 211, 307, 310–314, 424
 - SCVMM P2V Wizard, 357–361
 - Security Configuration Wizard (SCW), 441, 453–457, 463, 491
 - Server Virtualization and Consolidation Wizard, 37
 - Validate a Configuration Wizard, 137
 - Virtual Hard Disk Wizard, 243–248
 - Windows Deployment Services Configuration, 292–293
 - Windows PowerShell, 383
- WMI (Windows Management Instrumentation), 14, 18–19
- WMI Provider, 19, 402
- Workgroups, 158
- Workloads
 - assessing, 29–30
 - guest failover clustering, 560–562
 - inventory, 28
 - manual conversions, 338–339
 - Microsoft Assessment and Planning (MAP) tool, 33
 - migrating, 332–333, 356
 - virtual machine availability
 - additional components, configuring, 574–575
 - case scenario, protecting Exchange 2007 VMs, 585
 - guest network load balancing, 572
 - iSCSI security, 569–572
 - overview, 553–554
 - practice, assigning VLANs to VMs, 581–582
 - strategy selection, 573–574
 - supported VM configurations, 575–581
 - VLAN tagging, 562–566
 - virtualizing, overview, 1–2
- Workstation-based data, backup, 530
- WSB (Windows Server Backup), 510, 516–518
- WSUS (Windows Server Update Services), 70, 451, 578

X

- x32 platforms, 10
 - Hyper-V features, 14
 - migrating VMware formats to Hyper-V, 371–372
 - on-line conversions, 356
 - System Center Virtual Machine Manager (SCVMM), 163
 - Windows PowerShell, 386–387
- x64 platforms
 - failover clustering, 136
 - hardware selection, 42
 - hardware validation, 40–41
 - host optimization, 200
 - Hyper-V features, 14
 - Hyper-V Manager updates, 148
 - Hyper-V Manager, deploying, 149

x86 platforms

- Hyper-V updates, 79–80
- hypervisor, 9–10
- ImageX, 290
- managing virtual server hosts, 272
- migrating VMware formats to Hyper-V, 371–372
- on-line conversions, 356
- SCDPM requirements, 531
- SCDPM Service Pack 1, 537
- SCVMM Console, 273
- SCVMM Library, 284
- SCVMM Self-Service Portal, 316
- System Center Virtual Machine Manager (SCVMM), 155–156, 163
- updates, 73
- Windows PowerShell, 386–387
- Windows Preinstallation Environment (WinPE), 290
- Windows Server 2008, 10
- x86 platforms
 - failover clustering, 136
 - hardware selection, 42
 - Hyper-V Manager updates, 148
 - Hyper-V Manager, deploying, 149
 - Hyper-V role installation, 73
 - Hyper-V updates, 79–80
 - hypervisor, 9–10
 - ImageX, 290
 - managing virtual server hosts, 272
 - SCDPM requirements, 531
 - SCVMM Console, 273
 - SCVMM Library, 284
 - SCVMM Self-Service Portal, 316
 - System Center Virtual Machine Manager (SCVMM), 155–156
 - Windows PowerShell, 386–387
 - Windows Preinstallation Environment (WinPE), 290
 - Windows Server 2008, 10
- Xen-enabled SUSE Linux Enterprise Server, 21
- XenServer, 26, 368
- XML (Extended Markup Language), 102, 440
- XML store, 473
- XML Stores, 474–475
- xVM VirtualBox, 9

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>.