

Understanding Microsoft®

Virtualization Solutions

From the Desktop to the Datacenter

Mitch Tulloch
with the Microsoft
Virtualization Team

PUBLISHED BY

Microsoft Press

A Division of Microsoft Corporation

One Microsoft Way

Redmond, Washington 98052-6399

Copyright © 2009 by Microsoft Corporation

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

Library of Congress Control Number: 2008940458

Visit our Web site at www.microsoft.com/mspress. Send comments to mspinput@microsoft.com.

Microsoft, Microsoft Press, Active Directory, ActiveX, Authenticode, BitLocker, ClearType, Excel, Hyper-V, Internet Explorer, MS, MSDN, MS-DOS, Outlook, PowerPoint, SharePoint, SQL Server, Visual Basic, Visual C++, Win32, Windows, Windows Media, Windows Mobile, Windows NT, Windows PowerShell, Windows Server, Windows Vista, and WinFX are either registered trademarks or trademarks of the Microsoft group of companies. 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.

Author: Mitch Tulloch

Acquisitions Editor: Martin DelRe

Developmental Editor: Karen Szall

Project Editor: Kathleen Atkins

Editorial Production: Waypoint Press

Technical Reviewer: Bob Hogan; Technical Review services provided by Content Master, a member of CM Group, Ltd.

Cover: Tom Draper Design

Table of Contents

Acknowledgments	xi
Introduction	x
1 Microsoft's Virtualization Solution.....	1
Why Virtualization?	1
Virtualization Isn't Anything New	2
Virtualization Changes Everything	2
Types of Virtualization.....	4
Server Virtualization	4
Application Virtualization.....	5
Desktop Virtualization	5
Presentation Virtualization.....	6
Profile Virtualization	6
Benefits and Uses of Virtualization	7
Microsoft's Infrastructure Optimization Model	7
Virtualization's Business Benefits.....	9
Virtualization and Dynamic IT	11
Before and After Virtualization	12
Summary of IT Pro Benefits	13
Common Virtualization Scenarios.....	13
Understanding Microsoft Virtualization 360.....	16
Why Use Microsoft's Virtualization Solutions?	18
Microsoft's Commitment to Virtualization	18
Additional Resources.....	20
General	20
Microsoft Virtual PC	20
Microsoft Virtual Server	20
Microsoft's IT Infrastructure Optimization Model	20

 **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

Microsoft's Dynamic IT	21
Microsoft Virtualization Technologies and Solutions	21
Windows Optimized Desktop Scenarios	22
Microsoft's Vision and Strategy for Virtualization	22
2 Server Virtualization—Hyper-V	23
Understanding Server Virtualization	23
Understanding Virtual Machines	23
Understanding Hypervisors	25
Understanding the Hyper-V Architecture	29
Understanding the Parent Partition	30
Understanding Child Partitions	35
Working with Hyper-V	37
System Requirements for Using Hyper-V	37
Supported Guest Operating Systems	39
Functionality Provided by Integration Services	41
Installing Hyper-V	42
Using the Hyper-V Management Snap-in	45
Using the Virtual Machine Connection Tool	56
Creating a Virtual Machine	61
Working with Virtual Machines	65
Tools for Managing Hyper-V and Virtual Machines	74
Key Features of Hyper-V	79
Comparing Hyper-V and Virtual Server 2005 R2	80
Comparing Hyper-V and VMware ESX Server	80
Key Benefits of Using Hyper-V	81
Hyper-V Usage Scenarios	82
Server Consolidation	82
Business Continuity and Disaster Recovery	82
Testing and Development	83
The Dynamic Data Center	83
Additional Resources	83
General	83
Deploying Hyper-V	84
Managing and Maintaining Hyper-V	84
Hyper-V on Server Core	85
Resources for Hyper-V Developers	85

Hyper-V Bloggers at Microsoft	85
Other Hyper-V Bloggers.....	87
Hyper-V Forum on TechNet.....	87
3 Managing Virtualization—VMM 2008.....	89
Understanding Virtual Machine Manager 2008.....	89
Terminology	89
VMM 2008 Components	91
VMM 2008 Architecture.....	92
Working with VMM 2008	106
System and Infrastructure Requirements.....	106
Installing VMM 2008.....	110
Using the VMM Administrator Console.....	114
Working with Managed Hosts.....	117
Working with the Library	133
Working with Virtual Machines.....	139
Performing P2V Conversions.....	158
Performing V2V Conversions.....	160
Configuring User Roles	161
Using the Self-Service Portal	170
Key Features of VMM 2008	173
Windows Server 2008 Hyper-V Management	173
VMware (VI3) Management.....	174
Windows Server 2008 Failover Clustering Integration	174
Delegated Administration Based on Role-Based Authorization	175
Performance and Resource Optimization (PRO)	175
Key Benefits of VMM 2008.....	176
Usage Scenarios for VMM 2008	178
Server Consolidation.....	178
Provisioning of Virtualized Resources	178
Business Continuity	179
Performance and Resource Optimization	179
Additional Resources.....	180
General	180
Deploying and Using VMM	180
System Center Blog	180
VMM Forums on TechNet	180

4	Application Virtualization—App-V	181
	Understanding App-V	181
	App-V Terminology	181
	How App-V Works	183
	App-V Components	190
	App-V Architecture	199
	Working with App-V	202
	App-V Deployment Scenarios	202
	Obtaining App-V	211
	Using the Management Console	211
	Using the Sequencer	222
	Working with App-V Clients	234
	Key Features of App-V	239
	Dynamic Suite Composition	240
	Enhanced Scalability	240
	Globalization	241
	Enhanced Security	242
	Key Benefits of App-V	242
	Usage Scenarios for App-V	243
	Additional Resources	243
	General	243
	Deployment App-V	244
	Managing and Maintaining App-V	244
	App-V Team Blog	244
	App-V Forums on TechNet	244
5	Presentation Virtualization—Terminal Services	245
	Understanding Presentation Virtualization	245
	New Features of Terminal Services in Windows Server 2008	246
	Enhancements to Terminal Services Core Functionality	246
	Terminal Services RemoteApp	251
	Terminal Services Web Access	251
	Terminal Services Gateway	251
	Terminal Services Session Broker	252
	Terminal Services Licensing	252
	Other Enhancements	252

Understanding Terminal Services	259
Installing the Terminal Services Role	259
Terminal Services System Services	261
Remote Desktop	262
Terminal Services Licensing	263
Terminal Server Security	265
Installing Applications on Terminal Servers	269
Managing Terminal Servers	271
Understanding TS RemoteApp	281
How TS RemoteApp Works	281
Managing TS RemoteApp	283
Deploying and Using RemoteApp Programs	284
Understanding TS Web Access	290
How TS Web Access Works	291
Using TS Web Access to Deploy RemoteApp Programs	292
Using Remote Desktop Web Connection	295
Understanding TS Gateway	298
How TS Gateway Works	299
Implementing TS Gateway	300
Understanding TS Session Broker	302
Key Benefits of Terminal Services	306
Terminal Services Usage Scenarios	307
Branch Office	307
Controlled Partner Access or Outsourcing	308
Easing the Burden of Regulatory Compliance	308
Merger Integration	308
Mobile Workers	308
Task Workers	309
Additional Resources	309
General	309
Deploying Terminal Services	309
Maintaining and Managing Terminal Services	310
Terminal Services Client Software	310
Microsoft IT Showcase	311
Terminal Services Team Blog	311
Terminal Services Webcasts	311
Terminal Services Forum on TechNet	312

6	Desktop Virtualization—MED-V and VDI	313
	Understanding Desktop Virtualization Technologies	313
	Understanding Microsoft Enterprise Desktop Virtualization	314
	The Foundation—Microsoft Virtual PC	314
	Introducing Microsoft Enterprise Desktop Virtualization	315
	How MED-V Works	317
	Key Benefits of MED-V	325
	MED-V Usage Scenarios	326
	MED-V Availability	327
	Understanding Microsoft Virtual Desktop Infrastructure	328
	How Microsoft VDI Works	328
	Implementing Microsoft VDI	330
	Managing Microsoft VDI	332
	Key Benefits of Microsoft VDI	335
	Microsoft VDI Usage Scenarios	335
	Microsoft VDI Availability	335
	Additional Resources	337
	General	337
	Microsoft Virtual PC 2007	337
	Microsoft Optimized Desktop Pack	337
	Software Assurance	337
	Windows Vista Enterprise Edition	337
	Windows Vista Enterprise Centralized Desktop	338
	Microsoft Enterprise Desktop Virtualization	338
	Microsoft Virtual Desktop Infrastructure	338
7	User State Virtualization	339
	Understanding User State Virtualization	339
	Understanding User Profiles	339
	Where User Profiles Are Found	340
	Structure of a User Profile	341
	Limitations of Local User Profiles	347
	The Solution: User State Virtualization	348
	Understanding Roaming User Profiles	349
	How RUP Works	349
	Implementing RUP	350
	Limitations of RUP	356

Understanding Folder Redirection	358
How Folder Redirection Works	358
Implementing FR in a Workgroup	360
Implementing FR with RUP	361
Limitations of FR/RUP	366
Understanding Offline Files	366
How Offline Files Works	367
Implementing Offline Files	375
Key Benefits of RUP, FR, and Offline Files	380
Benefits of RUP	380
Benefits of FR with RUP	381
Benefits of Offline Files with FR and RUP	381
Usage Scenarios for RUP, FR, and Offline Files	381
Additional Resources	382
General	382
User Profiles	383
FR and RUP	383
Offline Files	383
Microsoft Bloggers	383
TechNet Webcasts	384
TechNet Forums	384

8 Building a Virtualization Infrastructure 385

Microsoft Virtualization Solution Accelerators	385
Infrastructure Planning and Design Guides for Virtualization	386
Microsoft Assessment and Planning Toolkit 3.1	391
Offline Virtual Machine Servicing Tool	403
Other Solution Accelerators	403
Microsoft System Center Solutions	404
System Center Management Suite Enterprise	405
System Center Essentials	405
Other System Center Products	406
Benefits of System Center for Virtualization	406
Virtualization Licensing	409
The Evolution of Microsoft Virtualization Licensing	410
Licensing Terminology	411
License Pricing	412
Volume Licensing Briefs	412

Conclusion..... 413

Resources..... 414

 General 414

 Microsoft Solution Accelerators 414

 Microsoft Infrastructure Planning and Design Guides 414

 Microsoft Assessment and Planning Toolkit..... 414

 Offline Virtual Machine Servicing Tool 415

 Microsoft System Center Solutions..... 415

 Virtualization Licensing..... 415

Index..... 417



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

Acknowledgements

This book would not have been possible without the gracious assistance of many people both inside and outside of Microsoft. First, special thanks to Edwin Yuen, Senior Product Manager for Integrated Virtualization Strategy at Microsoft, who helped drive this project forward and provided liaison for me with other members of the virtualization team at Microsoft. Also my special thanks to David Greschler, Director for Integrated Virtualization Strategy at Microsoft, whose support was essential for the success of this project.

Many thanks to following experts at Microsoft who provided key technical insights, peer-reviewed chapter content, wrote *Direct from the Source* sidebars, and assisted me in many other ways:

- Alex Balcanquall
- Anshul Rawat
- Baldwin Ng
- Fei Lu
- James O'Neill
- Jason Leznek
- Jeff Woolsey
- Karri Alexion-Tiernan
- Kyle Beck
- Michelle Foley
- Ming Zhu
- Peter Ballantyne
- Peter Larsen
- Ran Oelgiesser
- Sean Donahue

Big thanks especially to Bill Noonan, Mark Kitris, Dan Bond, and the rest of the CSS Global Technical Readiness (GTR) team at Microsoft without whose generous help this book would not have been possible.

Thanks also to the following Microsoft Most Valuable Professionals (MVPs) who wrote *Direct from the Field* sidebars for the chapter on App-V:

- Falko Gräfe
- Kalle Saunamäki
- Tim Mangan

Thanks also to Brett Polen of Xtreme Consulting Group Inc. who helped with the chapter on MED-V, and to Beth Harvey of Muse Marketing Group LLC for her help on the final chapter.

Special thanks to Karen Szall, my development editor at Microsoft Press, and Kathleen Atkins, project editor at Microsoft Press, both of whom I've enjoyed working with on this project and hope to do so again in the near future. Thanks also to Steve Sagman, who managed the editing and production of this book. And thanks of course to Martin DelRe, who first approached me about being involved in this project.

As always, thanks to my friend and agent, Neil Salkind of Salkind Literary Agency, which is part of Studio B Productions, Inc.

And last but never least, thanks to my wife, Ingrid, for her encouragement and support during this project.

Introduction

Welcome to *Understanding Microsoft Virtualization Solutions: From the Desktop to the Datacenter*. This is the book for IT professionals who want to learn more about the latest Microsoft virtualization technologies, including Windows Server 2008 Hyper-V, System Center Virtual Machine Manager 2008, Microsoft Application Virtualization 4.5, Microsoft Enterprise Desktop Virtualization, and Microsoft Virtual Desktop Infrastructure. The book also examines other virtualization-enabling technologies from Microsoft including Windows Server 2008 Terminal Services, Roaming User Profiles, Folder Redirection, and Offline Files.

Who Is This Book For?

The primary target audience for this book is IT administrators, implementers, and decision makers of large and mid-sized organizations who want to learn about the benefits of the latest virtualization technologies and how to plan, implement, and manage virtual infrastructure solutions based on these technologies. The book assumes that you are familiar with core Windows Server technologies and how to implement an Active Directory Domain Services infrastructure. The book also assumes you have experience working with the latest client and server versions of Windows, namely Windows Vista and Windows Server 2008. Finally, the book assumes you are already familiar with Microsoft Virtual Server 2005 and Microsoft Virtual PC 2007.

How This Book Is Organized

The book is intended to be read from cover to cover and will give you a good understanding of the capabilities, features, and operation of Microsoft virtualization technologies. You can also read individual chapters to gain an understanding of a particular product or technology.

The topics covered by the various chapters are as follows:

- **Chapter 1: Microsoft's Virtualization Solution** This chapter lays the framework of what virtualization is and why IT pros get excited about it. The chapter also examines the different types of virtualization and the benefits of virtualization. Finally, the chapter provides an overview of Microsoft's integrated virtualization solution known as Virtualization 360 and how it fits within Dynamic IT, Microsoft's strategy for enabling agile business.
- **Chapter 2: Server Virtualization—Hyper-V** Microsoft Hyper-V is the new hardware-assisted virtualization technology that is included as part of Windows Server 2008 x64 editions. Hyper-V is a hypervisor-based virtualization platform that enables you to

create and manage virtual machines. This chapter provides a detailed overview of how Hyper-V works, examines its key features and benefits, and describes some scenarios where businesses can benefit from deploying it.

- **Chapter 3: Managing Virtualization—VMM 2008** While Hyper-V alone might be sufficient for some organizations, others might have virtualized workloads running on the earlier Microsoft Virtual Server 2005 R2 platform or on VMware ESX Server computers within a VMware VI3 environment. These organizations can benefit from implementing the latest version of System Center Virtual Machine Manager, which now has the capability of managing virtualized workloads running on all three host platforms—Hyper-V, Virtual Server, and VMware ESX Server—from a single, centralized platform. This chapter delves into the workings of Virtual Machine Manager 2008 and explains how it works, how to use it, its key features and benefits, and key usage scenarios.
- **Chapter 4: Application Virtualization—App-V** This chapter deals with Microsoft Application Virtualization (App-V) 4.5, which is Microsoft's platform for delivering application virtualization solutions. Formerly known as SoftGrid Application Virtualization, App-V is part of the Microsoft Desktop Optimization Pack (MDOP) for Software Assurance (SA) version R2. This chapter examines how App-V works and how it can be used to deliver applications to users who need them. The chapter also summarizes the key features of App-V, the benefits App-V can provide organizations, and different usage scenarios for App-V.
- **Chapter 5: Presentation Virtualization—Terminal Services** This chapter examines Windows Server 2008 Terminal Services, which is Microsoft's presentation virtualization solution. Terminal Services can help your business simplify application deployment, increase security, and make remote workers more efficient. This chapter examines the new and enhanced features and components of Terminal Services in Windows Server 2008, explains how each Terminal Services component works, summarizes their benefits, and looks at different usage scenarios whereby businesses can benefit from deploying them.
- **Chapter 6: Desktop Virtualization—MED-V and VDI** This chapter is about two emerging desktop virtualization technologies from Microsoft, namely Microsoft Enterprise Desktop Virtualization (MED-V) and Microsoft Virtual Desktop Infrastructure (Microsoft VDI). Desktop virtualization refers to any technology that creates an additional isolated operating system environment on a standard desktop computer. Microsoft's desktop virtualization technologies are rapidly evolving, and some of the products and solutions described in this chapter are still under development, which means that some of this chapter is based on prerelease product information and is therefore subject to change. Nevertheless, because these new technologies are powerful and exciting, it's important that you know about them now.

- **Chapter 7: User State Virtualization** This chapter deals with user state virtualization, which is based on three core technologies available in Windows Vista and Windows Server 2008, namely Roaming User Profiles, Folder Redirection, and Offline Files. The chapter explains how these three technologies can be used together along with Group Policy to implement an efficient and reliable user state virtualization solution for your enterprise.
- **Chapter 8: Building a Virtualization Infrastructure** The final chapter of this book covers some of the other tools and features you'll need to build and manage an integrated virtualization solution that can meet the needs of your business. Specifically, this chapter describes Microsoft Virtualization Solution Accelerators, Microsoft System Center solutions, and Virtualization licensing.

Conventions Used in This Book

The following elements have been used in this book to help keep the text clear and easy to follow:

- **Note** Provides additional detail or a sidelight on the topic under discussion
- **Tip** Gives you some cool pointers that you'll probably want to know because it will make your job easier
- **Caution** Informs you of things to be aware of so that you can avoid potential pitfalls

An important feature of the book is sidebars written by Microsoft product groups and experts in the field. Sidebars written by individuals or teams inside Microsoft are titled *Direct from the Source*; sidebars written by other experts such as Microsoft Most Valuable Professionals (MVPs) are titled *Direct from the Field*.

Other Virtualization Resources

While this book is intended as a broad introduction to the technical aspects and benefits of Microsoft virtualization technologies, Microsoft provides many other useful resources from which you can learn more about these technologies. These resources include Microsoft TechNet, Microsoft bloggers, and other online resources. To help you find the most relevant resources, each chapter concludes with an "Additional Resources" section that provides descriptions and URLs for these resources.

Contact the Author

Feel free to contact me if you have comments, questions, or suggestions regarding anything in this book. Although I respond to all queries from readers and will do my best to answer your question to your satisfaction, I cannot provide readers with technical support. Please send your questions to the alias virtual@mtit.com, where they will be queued for my attention; expect a reply within one or two days. You can also check my Web site <http://www.mtit.com> for links to numerous articles and tips I've written. Please check these out because the answer to your question or problem might already be published in one of these.

Support

Every effort has been made to ensure the accuracy of this book. Microsoft Press provides corrections for books through the World Wide Web at the following address: <http://www.microsoft.com/mspress/support>.

If you have comments, questions, or ideas about this book, please send them to Microsoft Press using either of the following methods:

Postal mail:

Microsoft Press
Attn: Editor for *Understanding Microsoft Virtualization Solutions: From the Desktop to the Datacenter*
One Microsoft Way
Redmond, WA 98052-6399

E-mail:

msspinput@microsoft.com

Please note that product support isn't offered through the mail addresses. For support information, visit Microsoft's Web site at <http://support.microsoft.com/>.

Chapter 1

Microsoft's Virtualization Solution

Virtualization is a broad topic, and Microsoft's offerings in this area are also broad. This chapter sets up the framework for discussing what virtualization is and why IT pros get excited about it. The chapter also examines the different types of virtualization and the benefits of virtualization. Finally, the chapter provides an overview of Microsoft's integrated virtualization solution known as Virtualization 360 and describes how it fits within the larger framework of Microsoft's strategic vision known as Dynamic IT.

Why Virtualization?

Bob Muglia, Senior Vice President for the Server and Tools Business at Microsoft Corporation, has provided a good definition of the concept of *virtualization* as follows (from "Harnessing the Power of Virtualization for Dynamic IT," a Microsoft executive e-mail on January 21, 2008):

"Virtualization is an approach to deploying computing resources that isolates different layers—hardware, software, data, networks, storage—from each other."

Think about this for a moment. What does separating the different resources of a computing environment actually do for the IT professional? It makes them easier to manage. It also makes them easier to provision and maintain. Bob goes on to say the following:

"Typically today, an operating system is installed directly onto a computer's hardware. Applications are installed directly onto the operating system. The interface is presented through a display connected directly to the local machine. Altering one layer often affects the others, making changes difficult to implement."

"By using software to isolate these layers from each other, virtualization makes it easier to implement changes. The result is simplified management, more efficient use of IT resources, and the flexibility to provide the right computing resources, when and where they are needed."

We'll examine these benefits of virtualization in more detail shortly, but for now it's important to understand two things:

- Virtualization isn't anything new, and
- Virtualization changes everything.

Virtualization Isn't Anything New

The whole idea of virtualizing computing resources really isn't anything new. Back in the late 1960s, IBM first introduced the idea of virtual machines with its mainframe computers. In its essence, a *virtual machine* is simply software that runs on a physical computer and that behaves so similarly to the physical computer that any programs running in the virtual machine think they are running directly on the physical computer. In other words, the virtual machine emulates the environment of a physical computer, and when you run multiple virtual machines on one physical box the result is "virtually" the same as if you have multiple boxes to work with.

In 2004, Microsoft brought virtual machine technology to desktop computing with Microsoft Virtual PC. Virtual PC virtualizes the hardware of a standard personal computer (PC), allowing users to run multiple copies of Microsoft Windows, each with their own suite of applications, on a single physical computer. Microsoft also released a similar product called Microsoft Virtual Server, which could be used to virtualize server workloads by allowing multiple copies of Windows Server operating systems to run on a single physical server. Both of these products have been hugely popular in enterprise environments and are available today as Virtual PC 2007 Service Pack 1 and Virtual Server 2005 R2 Service Pack 1. This book assumes you have some familiarity with using these popular products and are interested in learning about Microsoft's latest virtualization offerings.

Citrix, VMware, and many other vendors also produce and sell virtualization products as well. CIO Magazine even has an article on up-and-coming virtualization vendors to keep your eye on (see "10 Virtualization Vendors to Watch in 2008," found at <http://www.cio.com/article/print/160951>). Why the sudden explosion of virtualization products and solutions? And why the intense interest from customers both large and small? If virtualization has been around for so many years, why get so excited about it?

Virtualization Changes Everything

With the rapid growth of the Internet since the late 1990s, enterprise computing has rapidly grown in size and complexity, and away from the mainframe model and toward a distributed computing model. Instead of relying on computing services provided by a single large mainframe, a few heavy-duty UNIX servers, or an outsourced data services provider, businesses have built their own computing services using low-cost Intel or AMD hardware running Microsoft Windows Server or Linux operating systems. The shift from centralized to in-house computing has given businesses greater control over the processing and storage of their business information, increased flexibility in responding to technological and marketplace changes, and greater efficiency in the allocation of budgetary resources.

But there have been some downsides to this revolutionary change in business computing. Pressured by rapid technological change and evolving customer demand, many businesses responded by throwing more physical servers at the problem, leading to poorly planned growth in their computing infrastructure—otherwise known as *server sprawl*. As a result, what promised to be easy to manage has in some cases become a nightmare for over-stretched IT departments.

Rapid technological change has also led to a second problem: platform and application incompatibility. Businesses that strived to stay on the leading edge of Web-enabled technologies often added new operating systems and applications to their infrastructures without proper migration planning, resulting in a mix of platforms and applications that failed to deliver on their promised efficiencies. Older versions of applications wouldn't run properly or at all on the latest desktop and server operating systems. And newer applications couldn't fulfill their potential when deployed on older operating systems.

For businesses conscious of their bottom line, a third issue has been the inefficiencies resulting from poorly thought-out purchases of hardware and software driven by the need to compete in a rapidly evolving Web-driven economy. As a result, most enterprises have at least some percentage (often significant) of their servers running well below their capacity, and finding some way to consolidate computing resources to reduce these inefficiencies and reduce cost has become a priority for IT departments living under the constant threat of the budgetary axe.

So instead of the promised flexibility and scalability that distributed computing could provide, many of today's enterprise networks are rigid and inflexible. They scale poorly and are difficult to grow without causing even more management headaches. Automation is hindered by having to integrate multiple different operating systems, operating system versions, and application versions.

Something is needed to bring server sprawl under control and to simplify management, facilitate automation, enhance scalability, and resolve incompatibility issues. Something is needed to enable businesses to extract maximum value from the latest and greatest computing technologies becoming available in the marketplace. Something is needed to turn things around and enable distributed network computing to realize its potential. Something is needed to bring your IT infrastructure under control and optimize the use of your computing resources—and to do this with less money and fewer dedicated IT staff in today's competitive business environment.

That something you need is virtualization.

Types of Virtualization

Virtualization is really a whole family of technologies and not just one thing. That's because computing environments are more than just computers. For example, a typical IT infrastructure involves provisioning, managing, and maintaining all or most of the following:

- Servers that perform various network roles
- Various clients, including desktop computers, laptops, smart phones, and personal digital assistants (PDAs)
- Operating systems, including Windows, Linux/UNIX, and Macintosh
- Applications (both server and client)
- Storage devices, such as storage area networks (SANs)
- Network devices, such as switches, routers, and various appliances
- Users' desktops and profiles (data and settings)

That's a lot to manage, and much of it is interrelated. Using different types of virtualization technologies, however, these relationships can be rationalized by separating their physical aspect (specific hardware and location) from their logical side.

Almost every aspect of IT infrastructure can be virtualized today to some degree. Although the specific names for these technologies might vary, a simple way of classifying the different approaches to virtualizing computing resources is the following:

- Server virtualization
- Application virtualization
- Desktop virtualization
- Presentation virtualization
- Profile virtualization

For now, let's briefly define each of these different types of virtualization. We'll go much deeper into each technology in later chapters of this book.

Server Virtualization

The primary goal of *server virtualization* is to allow you to decouple your server workloads from your physical server computers so that you can consolidate these workloads and provision your resources more efficiently. The Hyper-V role of Microsoft Windows Server 2008 is a hypervisor-based technology that enables you to run multiple guest operating systems, called *partitions*, on a single "Designed for Windows" server hardware system. In addition to

enabling you to consolidate server workloads, Hyper-V can also provide greater uptime for your servers, improve availability and scalability, simplify backup and recovery, and reduce your operating costs.

Hyper-V is Microsoft's successor to its earlier Microsoft Virtual Server product and is the foundation of Microsoft's virtualization solutions. You'll learn more about how Hyper-V works and its benefits in Chapter 2, "Server Virtualization—Hyper-V."

Application Virtualization

Application virtualization is another virtualization technology and lets you decouple applications from desktop operating systems to dynamically deliver applications on demand to your users. By running applications centrally instead of installing them on each user's computer, software update management is simplified, application-to-application conflicts are reduced, and application compatibility regression testing is made easier.

Microsoft Application Virtualization (App-V), which was formerly known as Microsoft SoftGrid Application Virtualization, is an enterprise-level application virtualization solution designed for today's marketplace. App-V is part of the Microsoft Desktop Optimization Pack (MDOP). It transforms application management from a tedious series of manual tasks into an automated, streamlined process. And because applications are never actually installed on client computers, there is minimal impact on client operating systems and other applications running on the client. This means improved stability, greater reliability, and an overall enhanced user experience.

You'll learn more about how App-V works and its benefits in Chapter 4, "Implementing Application Virtualization Using App-V."

Desktop Virtualization

Desktop virtualization refers to any type of technology that creates an additional isolated operating system environment on a standard desktop. Implementing desktop virtualization can help you support older applications running on current operating systems and can help reduce application compatibility issues. In addition, desktop virtualization can help prevent desktop refresh cycles from being blocked because of such application issues. This allows businesses to move forward with the latest operating system versions and gain benefits from all the new and enhanced features available in these new versions.

Microsoft's first foray into desktop virtualization was Microsoft Virtual PC, a still-popular product used mostly for development and testing. Microsoft has other new and emerging desktop virtualization solutions, however. They include Microsoft Enterprise Desktop

Virtualization (MED-V), which is part of MDOP, for enterprise customers, as well as technology recently acquired from Kidaro and Microsoft Virtual Desktop Infrastructure (VDI), a complete, end-to-end Microsoft virtualization solution that enables Windows Vista Enterprise and other desktop environments to run and be managed in virtual machines on a centralized server.

You'll learn more about how MED-V and VDI work and their benefits in Chapter 6, "Desktop Virtualization—MED-V and VDI."

Presentation Virtualization

Presentation virtualization involves separating processing and data storage from the user's computer. The key to enabling this is Terminal Services, one of the core virtualization technologies available in Windows Server 2008. Using Terminal Services makes it possible to run an application in one location while having it controlled in another. Instead of installing applications locally on each user's computer, you install and manage them on centralized servers in your server room or data center. Terminal Services presents each user with screen images that can be individual applications or entire desktops, while the user's computer sends keystrokes and mouse movements back to the server.

You'll learn more about how Terminal Services in Windows Server 2008 works and its benefits in Chapter 5, "Presentation Virtualization—Terminal Services."

Profile Virtualization

Profile virtualization involves separating user profiles, with their data and application settings, from the user's computer. Profile virtualization involves several familiar technologies—Folder Redirection, Roaming User Profiles, and Offline Files—that have each been significantly enhanced in Windows Vista. Folder Redirection is a client-side technology that provides the ability to transparently change the target location of predetermined folders located within the user profile. Roaming User Profiles are user profiles stored on a central server location that follow users as they log on to and log off from different computers. And Offline Files allows users to access files available on a network share and continue working with these files when the user's computer is not connected to the network.

We'll collectively label these technologies Vista Roaming Desktop, and you'll learn more about how they work and their benefits in Chapter 7, "User State Virtualization."

Benefits and Uses of Virtualization

Each of the different types of virtualization technologies described in the previous section can bring its own unique benefits, depending on the needs of your business. It's useful, however, to step back and look at the big picture of virtualization's benefits, as these benefits are to some degree provided by all virtualization technologies. A clear understanding of the benefits of virtualization also helps you understand the different scenarios in which virtualization can be used to enhance your business. But before we list the possible benefits of implementing virtualization solutions, we need to briefly examine the concept of the optimized IT infrastructure.

Microsoft's Infrastructure Optimization Model

Without an IT environment that is efficient, reliable, and easily managed—at the lowest possible cost—businesses today won't survive. This observation is true particularly in the mid-market sector, where the pressure to grow your business is greatest, where competition for IT talent is most intense, and where budgetary constraints are often felt the hardest.

As a response to the needs of this segment, Microsoft has developed its IT Infrastructure Optimization Model, a framework that helps organizations understand and improve their IT infrastructure using specific, concrete actionable items. This framework outlines the steps a business can take to determine where it is today with their IT infrastructure, where it needs to go, and exactly how to get there. The application of this framework can help a business create an IT environment that is easy to manage and makes the most efficient use of IT resources—including people, hardware, and software—as may be possible.

Microsoft's Infrastructure Optimization Model is particularly helpful for midsized businesses because they generally don't have the luxury of having a large IT staff. Yet they do have a critical need for an IT infrastructure that provides the level of service your workers need when operating in today's business environments. Workers today need quick access to the electronic resources, an ability to easily communicate and collaborate online, and the most up-to-date business tools in order to perform their jobs. Microsoft's Infrastructure Optimization Model—together with virtualization as a key enabler of this framework—can help make this happen for your company.

As shown in Figure 1-1, Microsoft's Infrastructure Optimization Model defines your existing IT infrastructure as being in one of four possible categories: Basic, Standardized, Rationalized, and Dynamic. These categories range from least optimized (Basic) to most optimized (Dynamic).

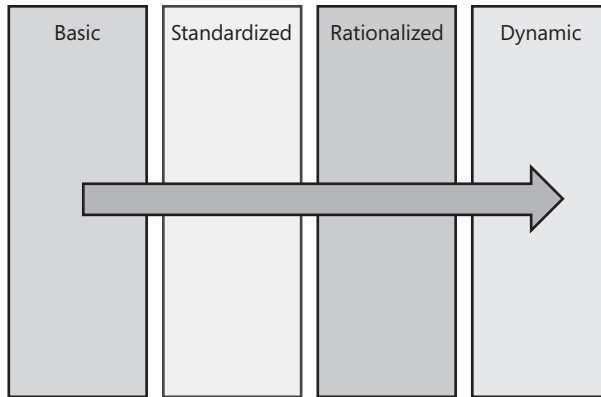


FIGURE 1-1 Microsoft's Infrastructure Optimization Model

Basic IT Infrastructure

A typical Basic IT infrastructure is one characterized by manual, localized business processes, minimal central control of resources, and nonexistent or unenforced IT policies and standards for security, backup, deployment, compliance, and other common IT practices. In a Basic IT infrastructure, the health of your applications and services is generally unknown because of a lack of suitable tools and resources for gauging this. In addition, patch management, software deployment, and desktop services are provisioned and maintained manually.

Standardized IT Infrastructure

A typical Standardized infrastructure builds on the Basic one by introducing controls through implementing standards and policies for managing desktops and servers, controlling provisioning and deployment of computers onto the network, and using Active Directory directory service to centralize management of network resources, security policies, and access control. Patch management, software deployments, and desktop services have been partially automated using light-touch technologies. Efforts are made for inventorying hardware and software and for managing licenses. Security at the perimeter of the network has been enhanced by the use of a firewall and malware filtering, but security inside the network is not yet a primary focus.

Rationalized IT Infrastructure

A typical Rationalized infrastructure is one in which the costs involved in managing desktops and servers has been significantly lowered and the processes and policies that support your business have been optimized. The approach to security is now proactive both at the perimeter and within the network, and threat response is methodical in its approach. Zero-touch deployment technologies simplify software deployment and minimize cost. Hardware and software are carefully inventoried, and the business purchases only the licenses it needs.

Dynamic IT Infrastructure

A typical Dynamic infrastructure is one in which the business is fully aware of the strategic value of its IT infrastructure, and this awareness enables it to run its business efficiently and remain ahead of competitors. IT costs are now fully controlled, and there is tight integration between users, data, desktops, and servers. Collaboration between users is pervasive, and mobile users have nearly the same level of access as desktop users. IT processes have been fully automated, which facilitates managing IT according to the needs of the business. Any additional technology investments made by your IT department tend to yield specific, measurable benefits for the operation of the business. Both manageability and security have been greatly enhanced by the use of self-provisioning software and quarantine-like systems, and these systems help ensure compliance with established security policies to improve reliability, lower costs, and increase service levels.

Virtualization's Business Benefits

Where does your IT infrastructure fit in the Infrastructure Optimization Model? Are you at the Basic or Standardized stage, or are you moving toward having a Rationalized or Dynamic infrastructure? And how can implementing virtualization technologies help move your infrastructure further along toward the goal of an efficient, reliable Dynamic IT infrastructure? Figure 1-2 summarizes some of the many benefits of virtualization technologies and how these benefits align with the Infrastructure Optimization Model.

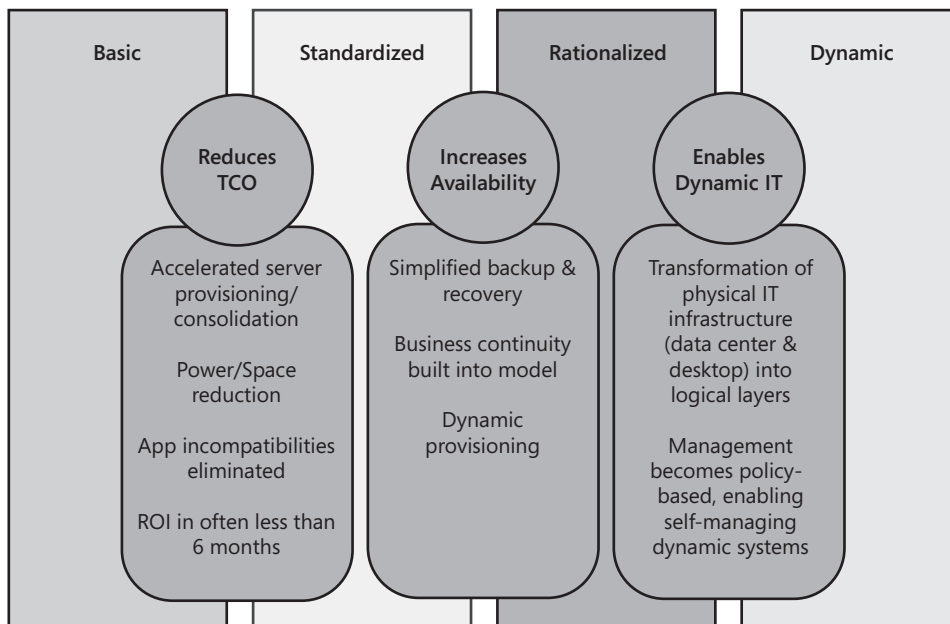


FIGURE 1-2 How the business benefits of virtualization align with Microsoft's IT Infrastructure Optimization Model

From Basic to Standardized

As the figure illustrates, from a business perspective, virtualization can help move your IT infrastructure from the Basic stage to the Standardized stage by reducing your total cost of ownership (TCO). Virtualization does this in the following ways:

- **Reducing power and space requirements** By reducing the number of physical computers you need on your network to host your services and applications, virtualization can help you reduce your power requirements and thus the cost of supplying power for your IT infrastructure. And reducing the number of physical computers you need also means less space is required in your server room or hosting area. The cost savings involved can be especially significant in large data centers, where the amount of electricity needed to run thousands of computers, the amount of floor space you need to lease to locate them, and the expensive cooling equipment needed to maintain them can cause costs to reach six figures or higher each year.
- **Accelerating server provisioning and consolidation** By enabling you to consolidate multiple servers onto fewer physical computers, virtualization makes the utilization of your IT assets more efficient and can help future-proof them against obsolescence. And by providing you with tools for quickly and easily provisioning servers, your infrastructure becomes more flexible and adaptive to change.
- **Eliminating application incompatibility issues** By allowing you to run older applications in their own virtual environments while running on the latest physical hardware, application compatibility issues are minimized or even eliminated. In addition, you can retire the inefficient, old hardware your older applications used to run on.
- **Rapid return on investment** All of the above benefits of using virtualization to move your IT infrastructure toward the Standardized stage can mean a significant ROI for your business, even in as short a time frame as six months.

From Standardized to Rationalized

From a business perspective, virtualization can also help move your infrastructure from the Standardized stage to the Rationalized stage by increasing the availability of business-critical applications and services. Virtualization does this in the following ways:

- **Simplifying backup and recovery** By enabling you to back up and recover entire virtual machines easily, virtualization helps rationalize your backup and restore processes, making them simpler to use and more reliable. Recovering from backup becomes a rapid process that minimizes service interruptions for workers and customers, thus increasing availability of business-critical network services.
- **Enhancing business continuity** By allowing you to capture point-in-time snapshots of running virtual machines, you can save an image of the machine that you can then return to at any later stage if needed. From a business-continuity perspective, this means

you can recover your business more quickly after a disaster. For example, snapshots of virtual machines can quickly be restored onto hardware located at a standby location, allowing the business to resume operations with minimal interruption. This enhanced capability for business continuity is built right into the virtualization business model.

- **Enabling dynamic provisioning** By enabling physical storage to be shared between different virtual machines, virtualization enables *dynamic provisioning*—the addition or removal of virtualized storage resources as needed. The flexibility provided by dynamic provisioning not only reduces costs by preventing underutilization of storage resources, it also prevents storage capacity from running out and causing application crashes. For example, virtual machines can be automatically unmapped from a lower priority use, reconfigured as might be needed, and quickly brought up for some new use to meet evolving demand.

From Rationalized to Dynamic

From a business perspective, virtualization can also help move your infrastructure from the Rationalized stage to the Dynamic stage by increasing the agility (flexibility and responsiveness to change) of your infrastructure. Virtualization does this in the following ways:

- **Providing a logical IT infrastructure** By enabling you to view and manage your IT infrastructure as a series of logical layers instead of a collection of physical hardware, virtualization simplifies the provisioning, management, and troubleshooting of systems and applications. These benefits can be felt throughout your infrastructure—from the data center to the desktop.
- **Facilitating self-managing dynamic systems** The holy grail of business computing is an agile IT infrastructure that enhances the dynamic capabilities of people, processes, and technology. Microsoft's Dynamic IT, formerly known as Dynamic Systems Initiative (DSI), is designed to provide technology and solutions that enable businesses to be as agile as possible, and agility is key to success in the fast-moving world of the Internet economy. And as described next, virtualization is one of the key enablers of Dynamic IT.

Virtualization and Dynamic IT

Survival in business today means responding dynamically to change, and Dynamic IT is Microsoft's technology strategy to help businesses become more dynamic. While the IT Infrastructure Optimization Model maps out the execution path for becoming dynamic, Microsoft's Dynamic IT provides the products and solutions that make such execution possible. Microsoft's Dynamic IT comprises the following three architectural elements:

- **Virtualized infrastructure** The goal here is to use virtualization technologies to mobilize the resources of your infrastructure. Virtualizing your infrastructure allows your business to achieve greater agility while leveraging your existing infrastructure. For

example, by consolidating system resources into a virtual service pool, a virtualized infrastructure makes it easier for a system to rapidly add, subtract, or move the resources it draws on to perform its work.

- **Knowledge-driven management** The goal here is to enable you to rapidly and effectively put your IT resources to work to meet the dynamic demands of your business. Key to making this possible is systems management software that can embrace your entire infrastructure, provide at a moment's notice key information on health and operations, and automate provisioning and reallocation of resources based on such gathered information.
- **Design for operations** The goal here is to ensure that your IT systems are built with operational requirements for excellence. To accomplish this, you must capture and integrate the diverse knowledge of business architects, managers, application developers, IT professionals, and industry partners, and embed this knowledge within your IT infrastructure using system models. Microsoft is committed to building such capabilities into its software so that the IT infrastructure of a business can "just work."

Before and After Virtualization

Before you implement virtualization in your computing environment, your situation looks something like this:

- Your operating systems are tied to specific physical hardware.
- Your applications are tied to specific operating systems and hardware.
- The processing of information is tied to the graphical and input/output subsystems of the physical system where the information is processed.
- Users' profiles and settings are tied to a specific operating system and hardware.
- Data storage is tied to specific physical hardware in specific locations within your infrastructure.
- Network resources are tied to specific locations within your infrastructure.

When you begin implementing virtualization technologies in your environment, however, these restrictive ties begin to disappear and your infrastructure becomes more agile. Specifically, the following benefits are gained:

- Using virtual machines means that operating systems are no longer bound to specific hardware but can be assigned to any desktop or server computer as needed (virtual machines).
- Using virtual applications means that applications are no longer tied to a specific system running a certain operating system and can instead be supplied to any computer on demand.

- Using virtual presentation means that information processing no longer needs to take place on the same system where presentation (accepting user input and displaying results) is performed.
- Using virtual profiles means that users' profiles and settings are no longer bound to users' own computers and instead can reside anywhere on the network.
- Using virtual storage means that data is no longer tied to specific locations on your network but instead are presented to users in virtualized form.
- Using virtual networking means that network resources are no longer tied to specific locations; instead, dispersed resources can be localized using virtualization.

Summary of IT Pro Benefits

Although business decision-makers will clearly be able to see the benefits of implementing virtualization, it's the IT pros who often get most excited about it. And whether you're an architect, an implementer, a developer, or a support engineer, virtualization can make your job easier in the following ways:

- Easier to provision and centrally manage servers, desktops, and applications
- Easier to maintain multiple versions of applications, including older applications
- Easier to test different infrastructure scenarios
- Easier to develop and test applications
- Easier to back up and recover systems and applications
- Greater security and reliability through isolating different computing layers
- Greater flexibility through on-demand dynamic provisioning of desktops and applications

And perhaps most important of all: easier to live within the constraints of shrinking IT budgets.

Common Virtualization Scenarios

Broadly speaking, we can divide virtualization scenarios into two areas: the data center and the desktop. We've already looked at the many benefits virtualization brings to the data center, including server consolidation, improved business continuity, accelerated provisioning, and facilitating development and test programs. The result of all this is the dynamic data center, something that is only beginning to emerge today but holds great promise for the future.

Users of desktop computers can also benefit in many ways from virtualization technologies, however, and in the upcoming sections we'll examine five client computing scenarios and how virtualization can bring benefits to the user's experience in these scenarios:

- The mobile worker
- The office worker
- The task worker
- The contract or offshore worker
- The worker needing access to her applications or data from anywhere

As we examine each of these different client computing scenarios, also known as *Windows Optimized Desktop Scenarios*, we can see how both your users and your IT department can benefit from the implementation of Microsoft's virtualization technologies.

Mobile Worker Scenario

Businesses are increasingly relying on a mobile workforce to meet the demands of the evolving marketplace, and two Microsoft virtualization technologies (App-V and Vista Roaming Desktop technologies) can bring big benefits to both the mobile users themselves and the IT departments that manage them. Specifically, App-V and Vista Roaming Desktop technologies provide the following end-user benefits for mobile workers:

- A rich user experience that enables users to run multiple applications simultaneously and that, from the user's perspective, feels the same as having these applications installed locally and having data accessible locally on his computer.
- Flexible configurations for managing the roaming user data and settings in different ways.
- The ability to access applications and data when not connected to the company network.

And adding BitLocker Drive Encryption to the formula ensures that the mobile workforce is a secure, reliable, and efficient option for enterprises to move toward.

From the IT side, implementing App-V and Vista Roaming Desktop technologies provides the following benefits when managing mobile workers and their computers:

- Safeguarding user data through centralized profile storage, redirection of folders to network file servers, or both
- The ability to migrate user data and settings from previous versions of Windows to Windows Vista by using the User State Migration Tool (USMT)
- The ability to share user data between v1 and v2 user profiles by using Folder Redirection

Office Worker Scenario

In a traditional office worker environment where users have desktop computers, three virtualization technologies (App-V, Terminal Services, and Vista Roaming Desktop) can provide significant benefits for both users and the IT department.

From the perspective of the office worker, the benefits are similar to two of those for mobile users described in the previous section—namely, a rich user experience and flexible configurations for managing roaming user data and settings. The ability to access applications and data when not connected to the network is not an issue, however, because uninterrupted network connectivity is a defining aspect of this scenario.

From the IT department perspective, implementing these virtualization technologies provides the following direct benefits:

- Simplifies the task of moving users to different desktop computers when they are transferred between departments or locations
- Helps to ensure compliance by enabling sensitive applications to be executed centrally on servers instead of on less-secure desktop computers

Task Worker Scenario

Task workers generally need access to only a few task-specific applications to be able to perform their job. Examples of such workers include bank tellers, customer service personnel, and shipping/receiving personnel. Terminal Services, Microsoft's presentation virtualization technology, is ideal in this scenario because it can provide users with the specific remote applications they need by using Terminal Services RemoteApps or it can provide them with an entire remote desktop if this is required. Combining Terminal Services with Group Policy in an Active Directory environment allows administrators to lock down functionality presented to users and provide them with a limited, task-oriented user interface that enables them to do their job and nothing else.

IT departments also benefit significantly in this scenario because Terminal Services enables centralized management and enhanced security at a lower cost than other client-computing scenarios. In addition, businesses that want to leverage older hardware can also use Windows Fundamentals for Legacy PCs (WinFLP), which gives organizations the opportunity to extend the life of their older PCs and provides task workers with a cost-efficient, no-frills client device that, when used together with Terminal Services, supplies them with all the business application functionality they require.

Contract/Offshore Worker Scenario

Businesses that need to hire outside contractors or offshore developers often cope with having unmanaged, non-corporate PCs connected to their network. Connecting unmanaged

PCs to your corporate network can expose your network to possible threats from malware-infected computers. And if access is not carefully controlled, your sensitive business information might also be exposed. Microsoft's recommended virtualization solution in this case is to use Windows Vista Enterprise Centralized Desktop (VECD). VECD is a unique licensing option of Microsoft's Virtualized Desktop Infrastructure that—when implemented with Hyper-V, App-V, WinFLP, and Vista Roaming Desktop technologies—can provide access to the right applications and data, and nothing else.

IT departments also benefit in this scenario by having centralized management of applications and data. Security and compliance are also facilitated by these technologies. And although this scenario might be a little more complex to implement than, say, setting up a terminal server or two, the benefit of having your business secrets safe while allowing lower-cost contract or offshore workers to access your network are clear and compelling for most organizations.

Anywhere-Access Scenario

Sometimes a user needs to access her applications or data but cannot get into the office—for example, during a snowstorm, while away on vacation, or simply when at home during the evening. If your users need “anywhere access” like this from computers not owned by the company, you can provide it for them by using Terminal Services Gateway, which allows users to access their individual applications or their entire desktop through Terminal Services over the Internet from any computer running Windows Vista with Service Pack 1 or Windows XP with Service Pack 3 or by using Microsoft Internet Explorer. And if your users require a more flexible remote desktop that includes the complete Windows Vista experience, you can use VECD virtual machines hosted on Hyper-V through the Terminal Services Gateway.

The benefits for users in this scenario are clear: secure access to their desktop, applications, and data from anywhere, at anytime. The benefits for IT departments that implement these solutions are also compelling and include centralized management, security, and compliance.

Understanding Microsoft Virtualization 360

What distinguishes Microsoft's vision and strategy for virtualization from that of its competitors is this: instead of providing products that implement only one or two types of virtualization technologies, Microsoft offers businesses a comprehensive set of virtualization products that range from the data center to the desktop and allows assets—both physical and virtual—to be easily managed from a single platform.

Figure 1-3 shows how Microsoft's various virtualization products and technologies provide a comprehensive, integrated solution to organizations seeking to implement the benefits of virtualization in their IT infrastructures.

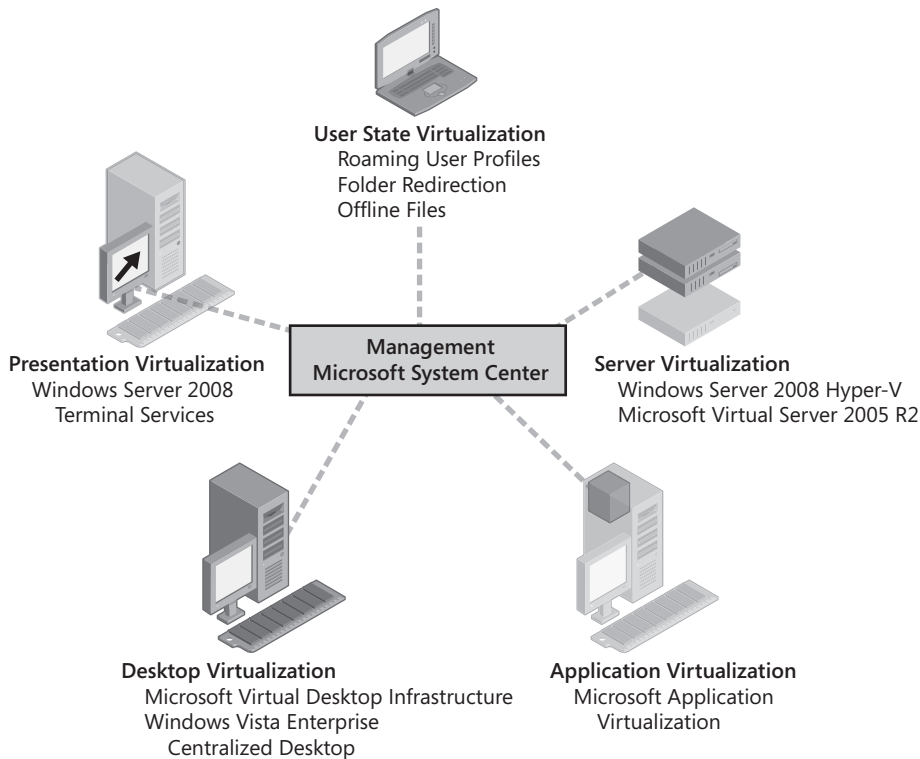


FIGURE 1-3 Microsoft's integrated virtualization solution known as Virtualization 360

As you can see from the figure, what ties Hyper-V, App-V, Terminal Services, MED-V/VDI, and Vista Roaming Desktop technologies together is Microsoft System Center, Microsoft's suite of systems management products that allow IT departments to manage their physical and virtual IT infrastructure across data centers, desktops, and devices. By using System Center Virtual Machine Manager, System Center Configuration Manager, System Center Operations Manager, and System Center Data Protection Manager, IT departments can provision, configure, monitor, and back up infrastructure software applications on both physical and virtualized servers and desktops.

In particular, System Center Virtual Machine Manager (SCVMM) lets you seamlessly manage both physical and virtual resources from the same "pane of glass" and enables you to integrate virtualization technologies, including VMware ESX environments, into existing environments and processes. You'll read more about how SCVMM works and about its benefits in Chapter 3, "Managing Virtualization Using System Center Virtual Machine Manager." And in Chapter 8, "Building and Maintaining a Virtualization Infrastructure," you'll learn some of the benefits of using other System Center products to manage your IT infrastructure.

Why Use Microsoft's Virtualization Solutions?

Before finishing this chapter, it's worth pausing a moment to ask why you should implement Microsoft virtualization products and technologies instead of those of competing virtualization vendors. Four answers to this question immediately come to mind.

First, Microsoft is the platform you know, the tools you are familiar with. Windows Server 2008 is the latest version of Microsoft's Windows Server operating system, and in addition to new features such as Hyper-V, it also includes enhanced versions of features present in previous Windows Server operating systems, such as Terminal Services, Roaming User Profiles, Folder Redirection, and other technologies. And even new features such as Hyper-V are managed using familiar Microsoft Management Console (MMC) tools. And because Microsoft virtualization technologies can all leverage existing product features, such as Active Directory Domain Services (AD DS), the path to learning is clear and training costs are reduced for both IT personnel and end users.

Second, Microsoft doesn't just offer one type of virtualization technology; it offers an entire suite of products that enable you to virtualize your infrastructure from the data center to the desktop. A full range of virtualization products and solutions and a large and thriving partner ecosystem give you another compelling reason to implement Microsoft virtualization solutions instead of those from competing vendors.

Third, Microsoft not only provides you with the technologies to virtualize your servers, desktops, and applications, it also provides you with the tools to manage these technologies regardless of which components of your infrastructure are physical and which are logical or virtual. Microsoft's management solutions also support interoperability with third-party virtualization solutions from vendors such as VMware, allowing you to manage a cross-hypervisor virtual environment.

Finally, Microsoft virtualization solutions can provide a better TCO than any vendor's virtualization solution and the fastest return on investment (ROI) to recoup your investment. With both lower up-front cost and lower ongoing cost in many scenarios, with a comprehensive and integrated set of virtualization products, and with tools that let you manage both virtual and physical computing resources from a single management platform, Microsoft virtualization products and technologies can clearly help you solve the critical technological and business issues facing your business.

Microsoft's Commitment to Virtualization

In conclusion, let's hear what Steve Ballmer, CEO of Microsoft, said at the Microsoft Management Summit back in 2005 (from "Microsoft CEO Steve Ballmer Affirms Commitment to Dynamic Systems Initiative" on Microsoft PressPass, April 5, 2005).

"We've heard from our enterprise IT customers loud and clear that they need their systems to be more automated and flexible. That's why we're investing in the Dynamic Systems Initiative and areas like virtualization, more secure network access and interoperability—we're committed to helping IT deliver greater efficiency and value."

And with the September 2008 release of System Center Virtual Machine Manager 2008 and Microsoft Application Virtualization 4.5, the release earlier this year of the Hyper-V role for Windows Server 2008, and the ongoing development of Microsoft Enterprise Desktop Virtualization and the Microsoft Virtual Desktop Infrastructure, Microsoft is fulfilling its commitment to providing a virtualization strategy that reaches from the data center to the desktop.

Direct from the Source: The Compelling Argument for Virtualization

There's no doubt that virtualization is one of the most compelling technologies, and for good reason. From server consolidation to business continuity to accelerated desktop deployments to Green IT, virtualization is a key enabler for making IT more dynamic, efficient, and agile. However, today there are a number of barriers blocking wide-scale adoption of virtualization, including deployment complexities, training, and high costs.

To overcome those barriers, Microsoft is offering virtualization products that cover everything from the data center to the desktop, including comprehensive management solutions. The Microsoft approach is to make it as seamless as possible to integrate virtualization into your existing IT environment. On the server, Microsoft's Hyper-V hypervisor and Terminal Services are key features of Windows Server 2008. So, if you know Microsoft Windows Server, you'll know virtualization. On the desktop, Microsoft Application Virtualization integrates with Active Directory, making it easy to add to your existing desktop environments while accelerating migrations to Windows Vista. And *all* Microsoft virtualization products can be managed with System Center, so you can manage your virtual infrastructure the same way you manage your physical infrastructure.

But it doesn't end here. Microsoft sees virtualization as a strategic investment that will provide a foundation for the next generation of IT innovation, so it's continuing to develop its virtualization products and work closely with its partners so that Microsoft customers have all they need to make virtualization ubiquitous across their entire IT infrastructure. Virtualization is just the beginning of something much bigger.

—David Greschler, Director, Integrated Virtualization Strategy

Additional Resources

The resources listed in this section were either referred to in the chapter or provide additional information concerning concepts and products discussed in this chapter.

General

For a brief history of IBM virtual machines, see <http://www.cap-lore.com/Software/CP.html>.

Bob Muglia's executive e-mail on virtualization technologies can be found at <http://www.microsoft.com/mscorp/execmail/2008/01-21virtualization.mspix>.

Steve Ballmer's commitment to Microsoft's Dynamic Systems Initiative (now called Dynamic IT), which includes virtualization, can be found at <http://www.microsoft.com/presspass/press/2005/Apr05/04-20VirtualizationInvestmentsPR.mspix>.

Microsoft Virtual PC

For more information about Microsoft Virtual PC 2007, see <http://www.microsoft.com/windows/products/winfamily/virtualpc/default.mspix>.

Another good resource for Virtual PC aficionados is Ben Armstrong's blog titled "The Virtual PC Guy's Weblog" at http://blogs.msdn.com/virtual_pc_guy/default.aspx. See especially the older posts about running old games on Virtual PC.

Microsoft Virtual Server

For more information about Microsoft Virtual Server 2005 R2, see <http://www.microsoft.com/windowsserversystem/virtualserver>.

Learn about Virtual Server deployment and operations and download the latest version of Virtual Server at the Microsoft Virtual Server TechCenter on Microsoft TechNet at <http://technet.microsoft.com/en-us/virtualserver/default.aspx>.

Another good resource for users of Virtual Server is Keith Combs' blog titled "Keith Combs' Blahg" at <http://blogs.technet.com/keithcombs/default.aspx>. Click the Virtualization Team tag on the left side of the home page to display relevant articles.

Microsoft's IT Infrastructure Optimization Model

You can find a description of Microsoft's IT Infrastructure Optimization Model, together with specific recommendations on moving your Infrastructure from the Basic stage towards the

Dynamic stage, at the Infrastructure Optimization TechCenter on Microsoft TechNet at <http://technet.microsoft.com/en-ca/infrastructure/default.aspx>.

Another good source of information is the Infrastructure Optimization blog on TechNet at <http://blogs.technet.com/io/default.aspx>.

Microsoft's Dynamic IT

Bob Muglia, senior vice president of the Server and Tools Business at Microsoft, outlined Microsoft's strategic vision for Dynamic IT at TechEd 2007. You can read about it on Microsoft PressPass at <http://www.microsoft.com/presspass/press/2007/jun07/06-04TechED07PR.msp>.

You can also watch videos of Bob Muglia and other senior leaders at Microsoft explaining the benefits of Dynamic IT at <http://www.microsoft.com/presspass/press/2007/jun07/06-04DynamicITVideos.msp>.

Learn more about how virtualization technologies provide one of the architectural underpinnings of dynamic systems by downloading the virtualization white paper found at <http://www.microsoft.com/business/dsi/virtualization.msp>.

You can download a white paper in PDF format titled "Optimize and Secure Your Core Infrastructure" from the Microsoft Download Center at <http://download.microsoft.com/download/8/d/8/8d8fd1f8-9af5-4ae9-898d-ffbe130d1ca9/Whitepaper-OSCI-all-up-CoreIO-FY08.pdf>.

Microsoft Virtualization Technologies and Solutions

Get the big picture concerning Microsoft's integrated virtualization vision and learn about Microsoft's various virtualization products and technologies at <http://www.microsoft.com/virtualization/default.msp>.

Find out more about virtualization and consolidation using Windows Server 2008 Hyper-V at <http://www.microsoft.com/windowsserver2008/en/us/virtualization-consolidation.aspx>.

Read technical details concerning virtualization and partitioning on the Windows Hardware Developer Central Web site at <http://www.microsoft.com/whdc/system/platform/virtual/default.msp>.

Stay up to date on the latest virtualization developments from Microsoft by subscribing to the newsfeed of the Microsoft Windows Virtualization Product Group Team Blog at <http://blogs.technet.com/virtualization/default.aspx>.

Windows Optimized Desktop Scenarios

For more information about how Microsoft virtualization technologies can benefit users in different client computing scenarios, see <http://www.microsoft.com/windows/products/windowsvista/enterprise/scenarios.mspix>.

For additional examples of virtualization in action for different types of workers, see <http://www.microsoft.com/virtualization/action.mspix>.

Microsoft's Vision and Strategy for Virtualization

You can download a white paper in PDF format titled "Virtualization From the Datacenter to the Desktop" from <http://www.microsoft.com/virtualization/datacenter.mspix> or from the Microsoft Download Center at <http://download.microsoft.com/download/0/A/C/0AC57003-473C-4F9A-84B0-8ADEF6ACE753/VirtualizationWhitepaper.pdf>.

Chapter 2

Server Virtualization—Hyper-V

At the center of Microsoft's vision and strategy for virtualization is Microsoft Hyper-V, the new hardware-assisted virtualization technology that is included as part of Microsoft Windows Server 2008 x64 editions. Hyper-V is a hypervisor-based virtualization platform that enables you to create and manage virtual machines (VMs). Hyper-V is both a robust and highly scalable technology, and it enables virtualized workloads that previously needed to be run on physical hardware to achieve the level of performance needed by businesses. This chapter provides a detailed overview of how Hyper-V works, examines its key features and benefits, and describes some scenarios where businesses can benefit from deploying it.

Understanding Server Virtualization

Hyper-V is an example of server (or machine) virtualization technology. What this means is that Hyper-V allows you to virtualize entire computers by running multiple operating systems (usually server operating systems) on a single physical computer (typically server-class hardware). Each guest operating system thinks (if operating systems could think) that it owns the computer and has exclusive use of the computer's hardware resources. Each operating system is therefore said to be running in a separate virtual machine, with these multiple virtual machines running on the same physical computer. In a typical nonvirtualized environment, only one operating system can run on a computer—it's Hyper-V that makes running multiple virtual machines possible. Clearly, we need to dig deeper into the concept of virtual machines before we can understand how Hyper-V works.

Understanding Virtual Machines

A *virtual machine* is a computing environment that is implemented in software and that abstracts the hardware resources of the physical computer so that multiple operating systems can run simultaneously on a single computer. Each operating system runs in its own virtual machine and is allocated logical instances of the computer's processors, hard disks, network cards, and other hardware resources. An operating system that is running in a virtual machine is unaware that it is executing in a virtual environment and behaves as if it exclusively controls the underlying physical computer's hardware.

Realizing virtual machines as described in the preceding paragraph means that server virtualization must be implemented in a way that meets the following requirements:

- **Management interfaces** Server virtualization requires management interfaces so that administrators can create, configure, and monitor virtual machines running on the computer. These interfaces should also support programmatic administration, and they must be able to work over the network so that virtual machines can be managed remotely.
- **Memory management** Server virtualization requires a memory manager, which ensures that each virtual machine receives its allocation of memory resources and that those memory resources are isolated between each virtual machine.
- **Scheduler** Server virtualization requires a scheduler to manage access to physical resources by different virtual machines. The scheduler must be configurable by the administrator so that different virtual machines can be given different priority to hardware as might be needed.
- **State machine** Server virtualization requires a state machine that can track information concerning the current state of all virtual machines on the computer. State information for a virtual machine includes its CPU, memory, devices, and whether the virtual machine is running or stopped. The state machine must also be designed to manage transitions between different states.
- **Storage and networking** Server virtualization requires functionality that can abstract storage and networking resources on the computer so that each virtual machine is presented with the view that it owns its own exclusive hard disks and network interfaces. In addition, machine virtualization must be able to multiplex access to physical devices in a way that is consistent, isolated, and secure.
- **Virtualized devices** Server virtualization requires virtualized devices that can provide operating systems running in virtual machines with logical representations of devices that behave in a similar manner as their physical counterparts. In other words, when an operating system running in a virtual machine needs to access a physical device on the computer, it does so by accessing a corresponding virtualized device, and this virtualized device is accessed in the same manner as a physical device would be accessed.
- **Virtual device drivers** Server virtualization requires that virtual device drivers be installed on operating systems running in virtual machines. These virtual device drivers enable applications to access the virtual representations of hardware and I/O connections in the same manner that they would access hardware and I/O connections on the underlying physical hardware.

As we'll see in a moment, Microsoft designed Hyper-V, its server virtualization solution, to meet all the above requirements. But first let's examine the key software component that makes server virtualization possible: the hypervisor.

Understanding Hypervisors

A *hypervisor* is a virtualization platform that enables you to run multiple operating systems on a single physical computer called the *host computer*. The main function of the hypervisor is to provide isolated execution environments for each virtual machine and to manage access between the *guest operating systems* running in virtual machines and the underlying hardware resources on the physical computer.

The term “hypervisor” goes way back to 1972 when IBM updated the control program of its System/370 mainframe computing platform to support virtualization. The creation of the hypervisor was a milestone in the evolution of computing because it provided a way to overcome the architectural limitations and high cost of using mainframe computers.

Hypervisors come in several different flavors. They can be categorized, for example, by type—that is, by whether they run directly on the physical hardware or within (hosted by) an operating system environment. Hypervisors can also be categorized by design—that is, whether they are monolithic or microkernel.

Type 1 Hypervisor

Type 1 hypervisors run directly on the underlying physical hardware of the host computers and function as a control program. In other words, they run on bare-metal systems. Guest operating systems then run within multiple virtual machines positioned above the hypervisor layer as shown in Figure 2-1.

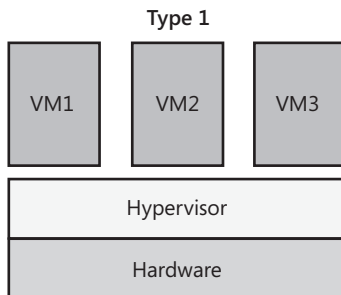


FIGURE 2-1 Type 1 hypervisors run directly on bare metal.

Because Type 1 hypervisors run directly on bare metal instead of within an operating system environment, they can generally provide the best performance, availability, and security of any form of hypervisor. Some examples of server virtualization products that implement Type 1 hypervisors include these:

- Microsoft Hyper-V
- Citrix XenServer
- VMware ESX Server

Type 2 Hypervisor

Type 2 hypervisors run within an operating system environment running on the host computer. Guest operating systems then run within virtual machines above the hypervisor as shown in Figure 2-2. This type of virtualization is typically referred to as *hosted virtualization*.

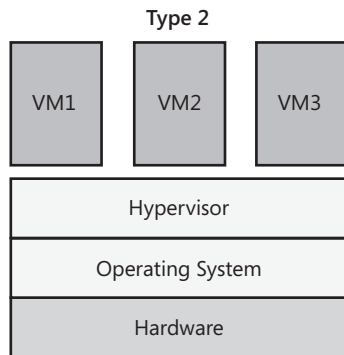


FIGURE 2-2 Type 2 hypervisors run within an operating system environment.

As you can see by comparing Figure 2-2 with Figure 2-1, guest operating systems running in virtual machines on Type 2 hypervisor platforms are one level further separated from underlying physical hardware than guest operating systems on Type 1 hypervisor platforms. This extra level of separation between the virtual machines and the hardware results in a performance hit being incurred on Type 2 hypervisor platforms, and the effect of this added overhead limits the number of virtual machines you can realistically run on Type 2 platforms.

Examples of server virtualization products that use Type 2 hypervisors include these:

- Microsoft Virtual Server
- VMware Server

The desktop machine virtualization product Microsoft Virtual PC also uses a Type 2 hypervisor architecture.

Monolithic Hypervisor

Monolithic hypervisor design involves using hypervisor-aware device drivers that are hosted within and managed by the hypervisor as shown in Figure 2-3.

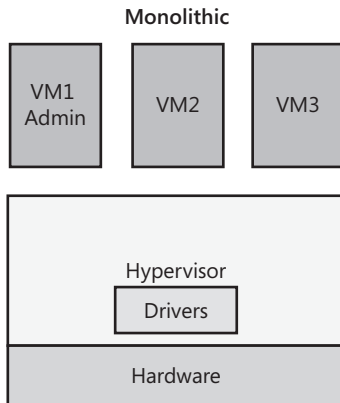


FIGURE 2-3 Monolithic hypervisor platforms require hypervisor-aware device drivers.

The monolithic design choice results in some benefits but also some drawbacks. For example, monolithic hypervisors do not need a controlling, or parent, operating system because all guest operating systems interact directly with the underlying physical hardware of the host computer by using hypervisor-aware device drivers. This is an example of the benefit of the monolithic design.

On the other hand, the fact that device drivers must be specifically developed for the hypervisor creates significant challenges because there are so many different types of motherboards, storage controllers, network adapters, and other types of hardware devices on the market. The result is that vendors of monolithic hypervisor platforms have to work closely with manufacturers of hardware devices to ensure these manufacturers develop hypervisor-aware versions of device drivers for their hardware. It also means that vendors of monolithic hypervisor platforms are dependent on manufacturers of hardware devices to supply such drivers for their products. The result is that the number of devices that can be used in virtualized operating system environments running on monolithic hypervisor platforms can be more limited than when those same operating system environments are run directly on physical computers.

One important point is that in this design you're ignoring one of the most important security tenets: defense in depth. With defense in depth, you provide multiple layers of defense to prevent against attacks. In this model, there is no defense in depth because everything is running in the most privileged part of the system.

An example of a server virtualization product that uses a monolithic hypervisor design is VMware ESX Server.

Microkernel Hypervisors

Microkernel hypervisors do not require hypervisor-aware device drivers because they have an operating system acting as the root, or parent, partition. This parent partition then provides the execution environment needed for device drivers to access the underlying physical hardware of the host computer. We'll talk more about partitions in a moment, but for now, simply think of the term "partition" as being equivalent to the previously introduced concept of a virtual machine.

On microkernel hypervisor platforms, you need to install device drivers only for physical devices in the operating system running in the parent partition. You do not need to install these drivers in guest operating systems running in child partitions because when these guest operating systems need to access physical hardware on the host computer, they simply do so by communicating with the parent partition. In other words, in the microkernel design, the guest operating systems do not have direct access to the underlying hardware. They can access physical devices only by communicating with the parent partition. Figure 2-4 shows the microkernel hypervisor design.

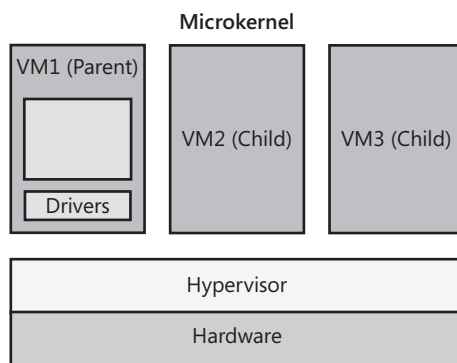


FIGURE 2-4 Microkernel hypervisor platforms require that guest operating systems that want to access hardware must do so via the parent partition.

The microkernel hypervisor design has several advantages over the monolithic design. First, because microkernel hypervisors do not need hypervisor-aware drivers, they can immediately use the wide range of existing drivers that are available from device manufacturers. Second, because device drivers are not part of the hypervisor, the hypervisor has less overhead, which means it's smaller and might therefore be more reliable. Third and perhaps more importantly, the attack surface is minimized because foreign code is not loaded in the hypervisor. (Device drivers are manufactured by third-parties and are therefore considered to be foreign code from the standpoint of the hypervisor vendor.) After all, the last thing you want to have happen is for malware to infect your hypervisor and thus take control of all the virtual operating systems running on your computer!

The only downside of the microkernel design is that a special partition, the parent partition, is required. This adds measurable (but usually minimal) overhead to your system because of the communication between parent and child partitions that is required to allow the child partitions to access the hardware through the parent.

One great benefit to Hyper-V microkernelized architecture is the use of the defense in depth. Hyper-V has been architected to run as little as possible in its hypervisor and push more functionality up into the stack, such as its state machine and management interfaces, which reside up the stack in user mode.

So what's an example of a server virtualization platform that implements the microkernel design? You guessed it—it's Microsoft Hyper-V, and it requires running Windows Server 2008 x64 in the parent partition.

Understanding the Hyper-V Architecture

Figure 2-5 shows the big picture concerning the Hyper-V architecture.

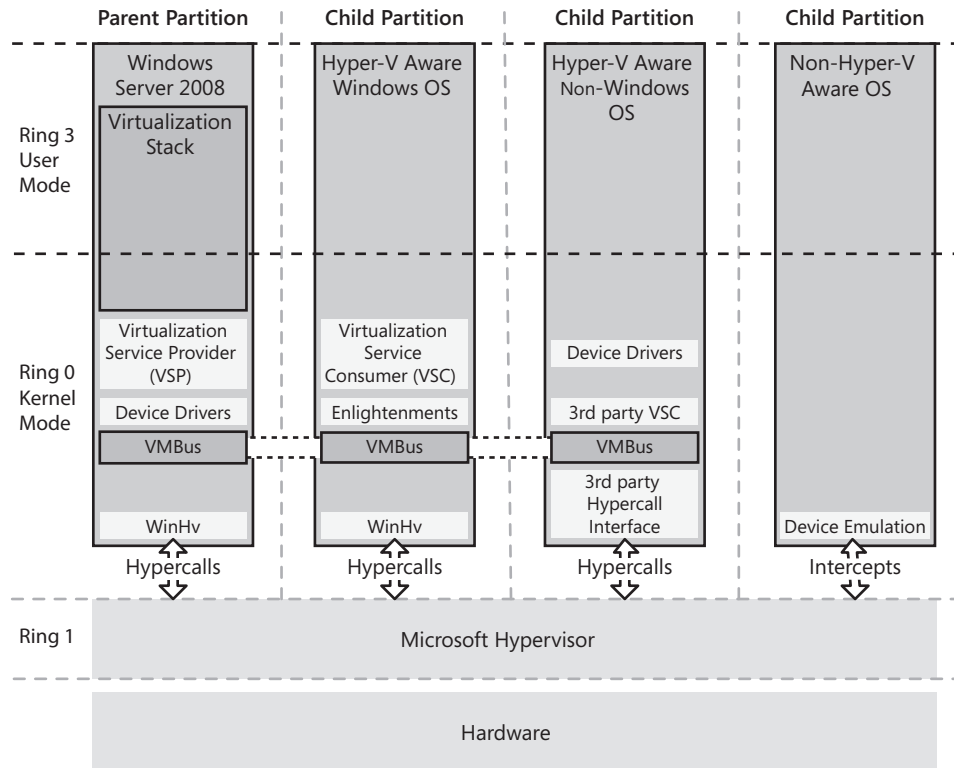


FIGURE 2-5 Overview of Hyper-V architecture

As you can see from Figure 2-5, Hyper-V consists of the Microsoft Hypervisor component running on top of bare metal, which demonstrates that Hyper-V is a Type 1 hypervisor platform. Running on top of the hypervisor are one parent partition and one or more child partitions. In virtualization terminology, a *partition* is simply a unit of isolation within the hypervisor that is allocated physical memory address space and virtual processors. There are two types of partitions:

- The *parent partition* is the controlling partition in which the virtualization stack runs. The parent partition is also the partition that owns the hardware devices and manages resources for the child partitions
- A *child partition* is any partition that has been created by the parent partition. Guest operating systems and their applications run in child partitions.

In the Microsoft implementation of the Type 1 hypervisor model—that is, in Hyper-V—the parent partition must be running either a Full or Server Core installation of Windows Server 2008 x64 Standard, Enterprise, or Datacenter edition as its operating system. For more information on what kind of computer you need for running Hyper-V, see the section titled “System Requirements for Using Hyper-V” later in this chapter.

Partitions communicate with the hypervisor layer by using *hypercalls*, which are application programming interfaces (APIs) that partitioned operating systems can use to leverage the optimizations that the hypervisor provides. Developers who are interested in learning how to develop applications that use hypercalls can learn more about them in the MSDN Library at <http://msdn.microsoft.com/en-us/library/bb969694.aspx>.

Understanding the Parent Partition

In the Hyper-V implementation of server virtualization, the parent partition includes a number of special components not present in child partitions. Figure 2-6 shows the various components of the parent partition in more detail, including both user-mode (ring 3) and kernel-mode (ring 0) processes.

The parent partition is the first partition created on the system when the hypervisor is started. The parent partition is created for the Windows Server 2008 operating system instance that hosts the Hyper-V server role. The parent partition in Hyper-V serves the following purposes:

- The parent partition is used for creating and managing other (child) partitions on the system and includes the WMI provider, which provides an interface for remote administration.
- The parent partition manages and assigns hardware devices, except for processor scheduling and physical memory allocation, which are handled by the hypervisor.

- The hardware resources of the parent partition are shared or allocated for use by child partitions.
- The parent partition handles power management, plug and play operations, and logging of any hardware failure events when they occur.

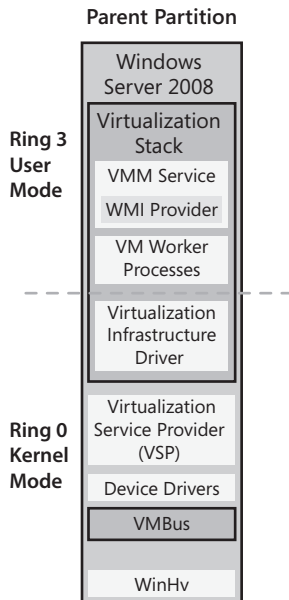


FIGURE 2-6 Detailed view of components of parent partition in Hyper-V.

The Virtualization Stack

The virtualization components hosted in the parent partition are referred to collectively as the *virtualization stack*. The virtualization stack runs in the parent partition and has direct access to the hardware of the underlying host computer through mechanisms described later. In Microsoft's Hyper-V implementation of the Type 1 hypervisor model, the virtualization stack consists of the following components:

- Virtual Machine Management Service
- Virtual Machine Worker Process
- Virtual Devices
- Virtualization Infrastructure Driver
- Windows Hypervisor Interface Library

Other components of the parent partition include the following:

- Virtualization Service Providers
- Virtual Machine Bus

The sections that follow examine each of the remaining components of the parent partition in detail.

Virtual Machine Management Service

The Virtual Machine Management Service (VMM Service or VMMS) is responsible for managing the state of all virtual machines in child partitions. This includes managing stopped or offline virtual machines, handling the creation of snapshots, and managing the addition or removal of devices. When a virtual machine in a child partition is started, the VMMS spawns a new Virtual Machine worker process, which is used to perform the management tasks for that virtual machine.

The VMMS also controls which operations can be performed on a virtual machine in a given state. For example, when you are deleting a snapshot of a virtual machine, the VMMS prevents you from applying the snapshot. (See the section titled “Working with Snapshots” later in this chapter for more information concerning snapshots.) Specifically, the VMMS manages the following virtual machine states:

- Starting
- Active
- Not Active
- Taking Snapshot
- Applying Snapshot
- Deleting Snapshot
- Merging Disk

Online virtual machine operations—such as Pause, Save, and Power Off—are not managed by the VMMS. Instead, they are managed by the Virtual Machine worker process that the VMMS spins up for the virtual machine being managed.

The VMMS is implemented in both user mode and kernel mode as a system service (VMMS.exe) and has dependencies on the Remote Procedure Call (RPC) and Windows Management Instrumentation (WMI) services. The VMMS comprises a number of components, one of which is a WMI Provider that exposes a set of WMI-based APIs for managing and controlling virtual machines. These Hyper-V WMI APIs can be used together with Visual Basic Scripting Edition (VBScript) or Windows PowerShell to manage most aspects of a Hyper-V environment either from the command line or by using scripts. The Hyper-V WMI APIs also allow Microsoft System Center products to manage Hyper-V servers. We’ll talk more about how System Center leverages Hyper-V in Chapter 3, “Managing Virtualization—SCVMM,” and Chapter 8, “Building a Virtualization Infrastructure,” later in this book.

Virtual Machine Worker Processes

A Virtual Machine worker process (vmwp.exe) is a user-mode process that provides virtual machine management services from the Windows Server 2008 instance in the parent partition to the guest operating systems in the child partitions. The VMMS spawns a separate VM worker process for each running virtual machine to isolate one virtual machine from another. That way, if one VM worker process fails, only the virtual machine associated with that VM worker process is affected. For enhanced security, VM worker processes run under the Network Service built-in identity.

The VM worker process manages the following aspects of its associated virtual machine:

- Creation, configuration, and running of the virtual machine
- Pausing and resuming the virtual machine
- Saving and restoring the virtual machine
- Taking snapshots of the virtual machine

In addition, the VM worker processes contains the Virtual Motherboard (VMB). The VMB exposes guest memory, IRQ generation, and memory-mapped and port-mapped I/O to the virtual machine as separate devices. The VMB is also responsible for the management of virtual devices, which are described next.



Tip You can view the globally unique identifier (GUID) for the virtual machine associated with a particular VM worker process by opening Task Manager, selecting the Processes tab, and adding the Command Line column to the Processes view. This displays each running instance of vmwp.exe on the computer along with its GUID.

Virtual Devices

Virtual Devices (VDevs) are software modules that provide device configuration and control for child partitions. The VMB includes a basic set of VDevs, including a PCI bus and the chip-set-level devices found on the Intel 440BX motherboard. VDevs come in two types:

- **Core VDevs** These virtual devices model existing hardware devices and are available to each virtual machine. They are typically used in situations where compatibility is important so that existing software such as the BIOS or device drivers can work properly without needing modifications. Core VDevs can be either of the following:
 - **Emulated devices** These virtual devices emulate a specific hardware device, such as a VESA video card. Most Core VDevs are emulated devices like this, and examples include BIOS, DMA, APIC, ISA Bus, PCI Bus, PIC Device, PIT Device, Power Mgmt device, RTC device, Serial Controller, Speaker device, 8042 PS/2 keyboard/mouse controller, Emulated Ethernet (DEC/Intel 21140), Floppy controller, IDE Controller, and VGA/VESA video.

- ❑ **Synthetic devices** These virtual devices do not model specific hardware devices. Examples of synthetic devices include a synthetic video controller, synthetic Human Interface Device (HID) controller, a synthetic network interface card (synthetic NIC), a synthetic storage devices, synthetic interrupt controller, and memory service routines. These synthetic devices are available only to guest operating systems that support Integration Services, which are discussed later in this section.
- **Plug-in VDevs** These virtual devices do not model existing hardware devices and are used to instantiate, configure, and manage Virtualization Service Providers running in the parent partition, which is the partition that controls the hardware. Plug-in VDevs enable direct communication between the parent and child partitions through the VMBus.

Virtualization Infrastructure Driver

The Virtualization Infrastructure Driver (Vid.sys) is the kernel-mode component of the virtualization stack and provides partition management services, virtual processor management services, and memory management services for all child partitions. The Vid.sys also enables user-mode components of the virtualization stack to communicate with the hypervisor.

Windows Hypervisor Interface Library

The Windows Hypervisor Interface Library (WinHv.sys) is a kernel-mode dynamic-link library (DLL) that loads within the Windows Server 2008 instance running in the parent partition, and within the guest operating system in any child partition where the guest is Hyper-V-aware. WinHv.sys abstracts the hypercall implementation details and enables the operating system's drivers to call the hypervisor by using standard Windows calling conventions.

Virtual Service Providers

Virtual Service Providers (VSPs) are hosted in the parent partition and provide a way of publishing device services to child partitions by providing I/O-related resources to Virtualization Service Clients (VSCs) running in child partitions. VSPs are the server endpoint and VSCs are the client endpoint for client/server communications for device functionality. All communications between VSPs and VSCs take place over the VMBus.

Virtual Machine Bus

The Virtual Machine Bus (VMBus) is a logical, channel-based, inter-partition communication mechanism between the parent partition and child partitions. The purpose of the VMBus is to provide a high-speed, highly optimized communications mechanism between virtualized partitions rather than other techniques that are slower because of the higher overhead that emulation imposes.

Guest operating systems that do not support Integration Services are not hypervisor-aware and must use emulation. That means that the hypervisor must intervene to intercept calls to the physical hardware from these guests and route them to the emulated device, which runs in the VM worker process in the parent partition. Emulation requires much more overhead for processing than communication using the VMBus, which is why it is recommended that users install the Hyper-V Integration Services after the guest operating system is installed.

The way it works is that the parent partition hosts VSPs, which communicate over the VMBus to handle device access requests from child partitions. Child partitions host VSCs, which redirect device requests to VSPs in the parent partition via the VMBus. The communication process between parent and child partitions over the VMBus is transparent to the guest operating system.

Understanding Child Partitions

As shown in Figure 2-7, the Hyper-V implementation of the Type 1 hypervisor model supports three types of child partitions:

- Child partitions hosting Hyper-V-aware Windows operating systems
- Child partitions hosting Hyper-V-aware non-Windows operating systems
- Child partitions hosting non-Hyper-V-aware operating systems, either Windows or other types

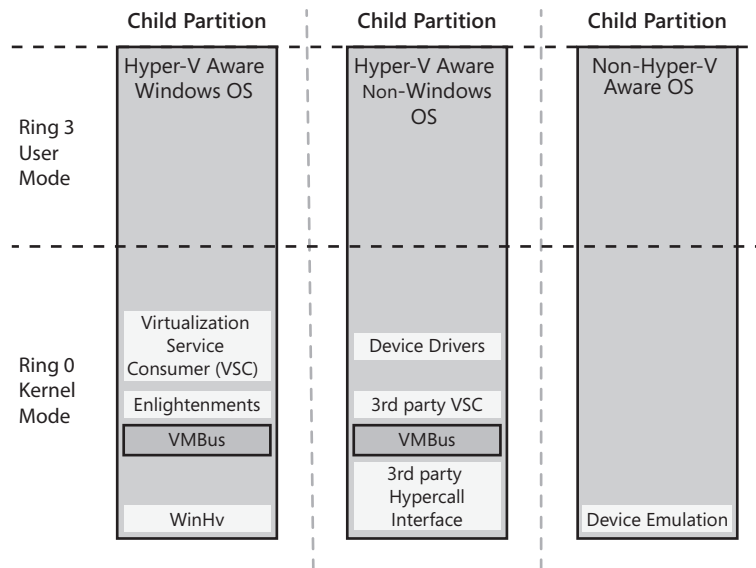


FIGURE 2-7 Different types of child partitions supported by Hyper-V.

Child Partitions Hosting a Hyper-V-Aware Windows Operating System

As shown on the left side of Figure 2-7, child partitions running Windows operating systems that are Hyper-V aware include the following kernel-mode virtualization components:

- **Virtualization Service Clients** VSCs are synthetic devices residing in the child partition that use hardware resources provided by the VSPs in the parent partition by communicating over the VMBus. VSCs are automatically made available for installation when Integration Services are installed in the child partition, which enables the child partition to use synthetic devices. Without Integration Services installed, a child partition can only use emulated devices as shown on the right side of Figure 2-7.
- **Enlightenments** This term refers to modifications made to operating system code to make the operating system hypervisor aware so that it runs more efficiently when it detects that it is running as a guest within a hypervisor environment. Hyper-V supports enlightenment of the following resources: storage, networking, graphics, and input subsystems. An *enlightened guest* is an operating system whose kernel can detect whether or not it is running in a virtualized environment. Windows Server 2008 is an enlightened guest and is therefore a fully enlightened operating system. Windows Vista is an operating system that can reach a degree of enlightenment by installing Integration Services onto it.



Note The VMBus and WinHv.sys components were discussed previously in the section titled “Understanding the Parent Partition” earlier in this chapter.

Child Partitions Hosting a Hyper-V-Aware Non-Windows Operating System

As shown in the middle portion of Figure 2-7, child partitions running non-Windows operating systems that are Hyper-V aware use third-party VSCs to communicate over the VMBus with VSPs in the parent partition in order to access hardware. These VSCs are provided to the child partition by installing Integration Services in the partition.

Integration Services are primarily used to address usability issues that occur because of the isolated environment that is inherent to virtual machines. Integration services also provide the components that allow child partitions to communicate with other partitions and the hypervisor. In previous Microsoft virtualization platforms, such as Microsoft Virtual Server and Microsoft Virtual PC, integration services were referred to as Virtual Machine Additions.

Integration Services also provides the following functionality to the child partition:

- **Heartbeat** Used to verify that the child partition is responding to requests from the parent partition.

- **Key\Value Pair Exchange** Registry key pairs exchanged between child and parent partitions (used in management tools).
- **Time Synchronization** Synchronizes the child partition time with the parent partition.
- **Shutdown** Allows the child partition to respond to shutdown requests from the parent partition.
- **Volume Shadow Copy Service** Works with the VSS component in the parent partition to facilitate data-consistent backups.

Hyper-V includes Integration Services for both x86 and x64 versions of the following Windows operating systems:

- Windows XP with Service Pack 3 (SP3)
- Windows Vista with Service Pack 1 (SP1)
- Windows Server 2003 SP2
- Windows Server 2008

Microsoft has also developed Integration Services for Novell SUSE Linux Enterprise Server 10 called Linux Integration Components For Hyper-V. These Integration Components are freely available from Microsoft at <http://connect.microsoft.com>.

Child Partitions Hosting a Non-Hyper-V-Aware Operating System

As shown on the left side of Figure 2-7, child partitions running non-Hyper-V-aware operating systems (whether versions of Microsoft Windows or some third-party operating system) cannot have Integration Services installed on them. This means that these guest operating systems must use emulated devices instead of synthetic devices and suffer the performance hit that is incurred by the use of such emulated devices.

Working with Hyper-V

This section provides a brief overview of how you can deploy, configure, manage, and use Microsoft's Hyper-V platform. Topics are treated in different levels of detail and are intended as an overview only rather than as a comprehensive Hyper-V operations guide. For detailed technical information on implementing and maintaining Hyper-V, see the Hyper-V product and feature information available from the Virtualization TechCenter on Microsoft Technet at <http://technet.microsoft.com/en-us/virtualization/default.aspx>.

System Requirements for Using Hyper-V

As was discussed earlier in this chapter, to run Hyper-V on a computer, the computer must be running either a Full or Server Core installation of Windows Server 2008 x64 Standard,

Enterprise, or Datacenter edition as its operating system. In addition to needing the correct version of Windows Server 2008, the host computer on which Hyper-V is installed must have hardware that supports the following features:

- Support for *hardware-assisted virtualization*, which is included in the Intel VT and AMD-V line of processors. Processors that support hardware-assisted virtualization include extensions to provide the ability to load a hypervisor virtualization platform in between the computer hardware and the main, or host, operating system.
- Support for *hardware-based Data Execution Prevention (DEP)*, a security feature that prevents a process from executing code from a nonexecutable memory region. Although an implementation of DEP can be hardware based, software based, or a combination of the two, support for hardware-based DEP is required in order to use Hyper-V. Hardware-based DEP requires processors that can mark memory pages as nonexecutable. Examples of processors that support hardware-based DEP include the Intel XD (Execute Disable) and AMD NX (No-Execute) lines of processors.
- Sufficient physical memory (RAM) to allow you to run the virtualized workloads you plan to run on the system. Windows Server 2008 Standard Edition x64 with the Hyper-V role installed supports up to 32 GB of RAM. Windows Server 2008 Enterprise Edition x64 with the Hyper-V role installed supports up to 1 TB of RAM, and each virtual machine can address up to 64 GB. In both cases, the sum of the memory assigned to virtual machines cannot exceed the system's physical RAM minus 1 GB allocated for the parent partition.

The following are some additional notes concerning the system requirements for Hyper-V:

- Hyper-V is not supported on any 32-bit version of Windows Server 2008, nor is it supported on Windows Server 2008 Web edition. In addition, there are versions of Windows Server 2008 (both x86 and x64) that do not include Hyper-V, and these versions are identified using product names such as "Windows Server 2008 Standard Edition without Hyper-V" and so on. Finally, Hyper-V is not supported on Itanium versions of Windows Server 2008.
- Although x64 editions of Windows Server 2008 support up to 64 processor cores, with the Hyper-V role installed, a maximum of 16 logical processors are supported. A logical processor is a unit that executes computing tasks. For example, a server that has two dual-core processors that feature hyperthreading technology will appear to the operating system as having eight logical processors.
- The Quick Migration feature of Hyper-V, which depends on the Failover Clustering feature of Windows Server 2008, is available only in the Enterprise and Datacenter editions of Windows Server 2008 x64. Quick Migration is described further in Chapter 8.

Direct from the Source: Hardware Assisted Virtualization

Since the introduction of the 80286 CPU, operating system architectures have supported four modes of execution called *rings* (for example, ring 0 – 3). Ring 0 is the most privileged mode, and components running in ring 0 have direct access to the underlying hardware. Ring 3 is the least-privileged mode, and operations to modify the hardware are generally not allowed in this ring. Windows historically has used only ring 0 (for kernel-mode components) and ring 3 (for user-mode components).

Virtual Server uses ring compression, or ring depriving, so the Virtual Machine Manager (VMM) can control the execution of a guest operating system in a virtual machine. With this design, kernel-mode operations in a virtual machine are performed in ring 1. Most privileged operations issued by the kernel in a guest operating system result in a transition to the VMM to interact with the underlying hardware. Because it is unlikely that the guest operating system running in a virtual machine is aware of the VMM, virtual machine additions are implemented to facilitate the VMM transitions for these operating systems.

These VMM transitions are expensive in terms of CPU cycles, and therefore, they affect system performance. To overcome this limitation, Intel and AMD have implemented extensions to the classical four-ring architecture to provide an additional level, often called ring –1, for a VMM to execute. This allows virtual guest operating systems' kernels to run at ring 0 and invoke the VMM in ring –1 for critical operations with much less overhead. The hypervisor is synonymous with the VMM in this context. The basic concept is that components running in the new ring –1 can control components running in ring 0. These extensions also implement extended page tables and tagged Translation Lookaside Buffers (TLBs) to support the isolation of virtual machines.

The Microsoft implementation of a hypervisor requires these processor virtualization extensions. The extensions are currently implemented in the Intel VT and AMD-V lines of processors.

—CSS Global Technical Readiness (GTR) team

Supported Guest Operating Systems

Following is a list of operating systems that are supported at the time of this writing for use as guest operating systems running in virtual machines on Hyper-V.

The following 32-bit and 64-bit editions of Windows Server 2008 can be used as a supported guest operating system on a virtual machine configured with either one, two, or four virtual processors:

- Windows Server 2008 Standard and Windows Server 2008 Standard without Hyper-V
- Windows Server 2008 Enterprise and Windows Server 2008 Enterprise without Hyper-V
- Windows Server 2008 Datacenter and Windows Server 2008 Datacenter without Hyper-V
- Windows Web Server 2008
- Windows High Performance Computing (HPC) Server 2008 Edition

The following editions of Windows Server 2003 can be used as a supported guest operating system on a virtual machine configured with either one or two virtual processors:

- Windows Server 2003 R2 Standard Edition with Service Pack 2
- Windows Server 2003 R2 Enterprise Edition with Service Pack 2
- Windows Server 2003 R2 Datacenter Edition with Service Pack 2
- Windows Server 2003 Standard Edition with Service Pack 2
- Windows Server 2003 Enterprise Edition with Service Pack 2
- Windows Server 2003 Datacenter Edition with Service Pack 2
- Windows Server 2003 Web Edition with Service Pack 2
- Windows Server 2003 R2 Standard x64 Edition with Service Pack 2
- Windows Server 2003 R2 Enterprise x64 Edition with Service Pack 2
- Windows Server 2003 R2 Datacenter x64 Edition with Service Pack 2
- Windows Server 2003 Standard x64 Edition with Service Pack 2
- Windows Server 2003 Enterprise x64 Edition with Service Pack 2
- Windows Server 2003 Datacenter x64 Edition with Service Pack 2

The following versions of Windows 2000 can be run on a virtual machine configured with one virtual processor:

- Windows 2000 Server with Service Pack 4
- Windows 2000 Advanced Server with Service Pack 4

The following 32-bit and 64-bit versions of Windows Vista can be used on a virtual machine configured with either one or two virtual processors:

- Windows Vista Business with Service Pack 1
- Windows Vista Enterprise with Service Pack 1
- Windows Vista Ultimate with Service Pack 1

The following versions of Windows XP can be run on a virtual machine as specified:

- Windows XP Professional with Service Pack 3 (configured with one or two virtual processors)
- Windows XP Professional with Service Pack 2 (configured with one virtual processor)
- Windows XP Professional x64 Edition with Service Pack 2 (configured with one or two virtual processors)

The following Linux distributions can be run on a virtual machine configured with one virtual processor:

- Suse Linux Enterprise Server 10 with Service Pack 2 (x86 edition)
- Suse Linux Enterprise Server 10 with Service Pack 2 (x64 edition)
- Suse Linux Enterprise Server 10 with Service Pack 1 (x86 edition)
- Suse Linux Enterprise Server 10 with Service Pack 1 (x64 edition)



Note You can run both 32-bit and 64-bit guest operating systems at the same time on a single server running Hyper-V.

Functionality Provided by Integration Services

Although Hyper-V comes with Integration Services for all supported guest operating systems (with the exception of Linux Integration Components For Hyper-V, which is provided out-of-band as a download), not all guests receive the same usability and performance enhancements from these Integration Services. Table 2-1 describes the enhancements provided by Integration Services for each supported guest.

TABLE 2-1 Usability and Performance Enhancements Provided by Integration Services for Different Guest Operating Systems

Guest Operating System	Device and Service Support
Windows Server 2008 (x64 editions)	Drivers: IDE, SCSI, networking, video, and mouse Services: Operating system shutdown, time synchronization, data exchange, heartbeat, and online backup
Windows Server 2008 (x86 editions)	Drivers: IDE, SCSI, networking, video, and mouse Services: Operating system shutdown, time synchronization, data exchange, heartbeat, and online backup
Windows Server 2003 (x64 editions) with Service Pack 2	Drivers: IDE, SCSI, networking, video, and mouse Services: Operating system shutdown, time synchronization, data exchange, heartbeat, and online backup
Windows Server 2003 (x86 editions) with Service Pack 2	Drivers: IDE, SCSI, networking, video, and mouse Services: Operating system shutdown, time synchronization, data exchange, heartbeat, and online backup

Guest Operating System	Device and Service Support
Windows 2000 Server with Service Pack 4	Drivers: IDE, networking, video, and mouse Services: Operating system shutdown, time synchronization, data exchange, heartbeat, and online backup
Windows 2000 Advanced Server with Service Pack 4	Drivers: IDE, networking, video, and mouse Services: Operating system shutdown, time synchronization, data exchange, heartbeat, and online backup
Windows Vista (x64 editions) with Service Pack 1	Drivers: IDE, SCSI, networking, video, and mouse Services: Operating system shutdown, time synchronization, data exchange, heartbeat, and online backup
Windows Vista (x86 editions) with Service Pack 1	Drivers: IDE, SCSI, networking, video, and mouse Services: Operating system shutdown, time synchronization, data exchange, heartbeat, and online backup
Windows XP Professional (x86 editions) with Service Pack 2 or 3	Drivers: IDE, SCSI, networking, video, and mouse Services: Operating system shutdown, time synchronization, data exchange, and heartbeat
Windows XP Professional x64 Edition with Service Pack 2	Drivers: IDE, SCSI, networking, video, and mouse Services: Operating system shutdown, time synchronization, data exchange, and heartbeat
Suse Linux Enterprise Server 10 (x64 edition) with Service Pack 1 or 2	Drivers only: IDE, SCSI, networking, and mouse
Suse Linux Enterprise Server 10 (x86 edition) with Service Pack 1 or 2	Drivers only: IDE, SCSI, networking, and mouse

Installing Hyper-V

Hyper-V is implemented as a server role on both Full and Server Core installations of Windows Server 2008 x64 Standard, Enterprise, and Datacenter editions. You can install Hyper-V on a Full installation of Windows Server 2008 using the following methods:

- By launching the Add Roles Wizard from the Initial Configuration Tasks (ICT) interface
- By launching the Add Roles Wizard from the Server Manager MMC snap-in
- By using the ServerManagerCmd.exe command-line tool

To install Hyper-V on a Server Core installation of Windows Server 2008, you must use the Ocsetup.exe utility by typing **start /w ocsetup Microsoft-Hyper-V** at the command prompt.

However, because the release version of Windows Server 2008 does not include the final Hyper-V bits, you must download and install the Hyper-V RTM Update Package (.msu file) before you install the Hyper-V role using any of the methods just described. The release

version of the Hyper-V technology for Windows Server 2008 is described in Microsoft Knowledge Base (KB) article KB950050 at <http://support.microsoft.com/kb/950050> and is available on Windows Update.

After you install Hyper-V, you must restart your computer before the role can take effect. If you discover that Hyper-V does not start properly after performing one of the listed procedures, try shutting down your computer completely and performing another cold boot of the system. If Hyper-V still fails to start, follow these steps to troubleshoot the problem:

- Verify with the manufacturer that the processors in your system support both hardware-assisted virtualization and hardware Data Execution Prevention.
- Make sure that hardware-assisted virtualization is enabled in the BIOS. If it isn't, enable it and then shut down your computer before rebooting it so that the BIOS change can take effect.
- Check the manufacturer's Web site to see whether an updated version of the BIOS is available for your computer; install the update if one is available.
- Verify that the BCD store is configured properly by typing **bcdedit /enum** and verifying that `HypervisorLaunchType` is set to `AUTO`.

For more information about deploying Hyper-V, see the "Hyper-V Planning and Deployment Guide," which is available from the Microsoft Download Center at <http://www.microsoft.com/downloadS/details.aspx?FamilyID=5da4058e-72cc-4b8d-bbb1-5e16a136ef42&displaylang=en>.

Direct from the Source: Considerations for Physical Servers Hosting the Hyper-V Role

Before setting up a physical server to host the Hyper-V role, download, read, and understand information included in the white paper "Performance Tuning Guidelines for Windows Server 2008" available at http://www.microsoft.com/whdc/system/sysperf/Perf_tun_srv.msp. Three sections in this white paper that can have a significant impact on the performance of the physical server discuss tuning the server hardware and setting up the networking and storage subsystems. These are especially critical for Hyper-V because the hypervisor itself sits on top of the hardware layer as described earlier and controls all hardware in Windows Server 2008. The operating system itself essentially runs in a virtual machine, better known as the Parent Partition.

Best practices for physical servers hosting the Hyper-V role are described in the following sections of this sidebar.

Avoid Overloading the Server

Determining the number of virtual machines that will be hosted on the Hyper-V server and the workloads they will be handling is critical. The version of the operating system that will be installed on the physical server can help in this regard, so the first "best

practice” is to consider using Windows Server 2008 Datacenter x64 with Hyper-V. The Datacenter x64 edition supports up to 64 processors, 2 terabytes of physical memory, and 16 failover cluster nodes for Quick Migration scenarios and allows unlimited virtual machines to be run in Hyper-V. Selecting a Server Core installation provides added benefits, including enhanced security and lower maintenance.

Ensure High-Speed Access to Storage

For storage, consider using a storage area network (SAN) that is configured with high-speed (10,000 rpms or greater) drives (SATA or SAS) that support queued I/O and Raid 0 +1 configurations. You can use either Fibre Channel or iSCSI SAN hardware.

Install Multiple Network Interface Cards

For networking, be sure to have more than one network card installed on the physical server and dedicate one network interface to Hyper-V server administration. This means no virtual networks in Hyper-V will be configured to use this NIC. For high-workload virtual machines, you might want to dedicate a physical network adapter on the server to the virtual network the virtual machine is using. Ensure virtual machines that share a physical adapter do not oversubscribe to the physical network. Use the Reliability And Performance Monitor to establish a performance baseline for the load and then adjust NIC configurations and loads accordingly.

If you have only a single NIC in the machine that you are configuring the Hyper-V role on and you are doing the configuration remotely—say, in an RDP session—if you choose to bind the Virtual Switch Protocol to the single NIC in the machine, you will be disconnected from your session and a reconnection might not be possible until the newly created virtual network adapter has been properly configured.

Avoid Mixing Virtual Machines That Can Use Integration Services with Those That Cannot

Do not mix on the same physical server virtual machines that can take advantage of Hyper-V Integration Services with those that cannot. Virtual machines that cannot use Integration Services must use legacy network adapters to gain access to the physical network. To accommodate legacy network adapters, you might need to disable some high-end features on the network interface, which can unnecessarily limit the functionality of the synthetic devices. Additionally, using emulated devices places an extra workload on the Hyper-V server.

Configure Antivirus Software to Bypass Hyper-V Processes and Directories

If you are running antivirus software on the physical server, you might want to consider excluding the Vmms.exe and Vmswp.exe processes. Also, exclude the directories that contain the virtual machine configuration files and virtual hard disks from active scanning. An added benefit of using passthrough disks in your virtual machines is that you

can use the antivirus software running on the physical server to protect that virtual machine.

Avoid Storing System Files on Drives Used for Hyper-V Storage

Do not store any system files (Pagefile.sys) on drives dedicated to storing virtual machine data.

Monitor Performance to Optimize and Manage Server Loading

When running multiple high-workload virtual machines on a Hyper-V server, ensure a proper aggregate performance baseline is obtained over a specified period of time—say, five days during normal working hours—to ensure the hardware configuration for the physical server is optimal to support the load being placed on it by the virtual machines. If adding more memory, processors, or higher performing storage is not possible, you might need to migrate the virtual machines to other Hyper-V servers.

—CSS Global Technical Readiness (GTR) team

Using the Hyper-V Management Snap-in

When you install the Hyper-V role on a Full installation of Windows Server 2008, the Hyper-V Manager snap-in is also installed and is available from both the Administrative Tools menu as a separate MMC console (Virtmgmt.msc) and from within the Server Manager console. You can also install the Hyper-V Manager console on the following systems:

- A computer running a Full installation of Windows Server 2008 that does not have the Hyper-V role installed. Install Hyper-V Tools from the Remote Administration Tools section of the Remote Server Administration Tools (RSAT) feature by using the Add Features Wizard.
- A computer running Windows Vista with Service Pack 1 (x86 or x64) Business, Enterprise, or Ultimate edition on which you have downloaded and installed the Windows Vista Service Pack 1 Management Tools update for the release version of Hyper-V. This update package installs both the Hyper-V Manager snap-in and the Virtual Machine Connection tool on a computer that is running Windows Vista SP1. You can find more information about this update and where to obtain it from Microsoft Knowledge Base article KB952627 at <http://support.microsoft.com/kb/952627>.



Tip If you plan on using a Server Core installation of Windows Server 2008 as your Hyper-V platform, you must manage the Hyper-V role remotely because the Hyper-V Manager snap-in is not available on Server Core.

Figure 2-8 shows the Hyper-V Manager snap-in remotely connected to a Hyper-V server named SEA-SCV running Server Core, which can be used to manage both the Hyper-V server (parent partition) itself as well as the virtual machines that are running in child partitions on the server. Note that no virtual machines (child partitions) have been created yet on this server. You can connect to additional Hyper-V servers by right-clicking on the root node in the left pane to bring up the Select Computer dialog box. This enables you to use the Hyper-V Manager snap-in running on one computer that is running either Windows Server 2008 or Windows Vista SP1 and to use it to manage multiple Hyper-V servers remotely.



FIGURE 2-8 The Hyper-V Manager snap-in.

Configuring Server Settings

As shown in Figure 2-8, when a Hyper-V server is selected in the left pane, a series of configuration actions is displayed in the Actions pane on the right side. These configuration actions can also be selected from a context menu by right-clicking on the server node in the left pane. Some of these server-level management actions are self-explanatory (such as Stop Service or Remove Server). Others require some degree of explanation as follows:

- **New Virtual Machine** Selecting this action starts the New Virtual Machine Wizard, which steps you through creating a new virtual machine (child partition) on the host computer. The steps for creating a new virtual machine are as follows:
 1. Name the virtual machine.
 2. Select a location to store the virtual machine configuration file.

3. Assign memory.
 4. Configure networking.
 5. Configure storage.
 6. Install an operating system.
 7. Start the virtual machine (optional).
- **New Hard Disk** Selecting this action starts the New Virtual Hard Disk Wizard, which steps you through creating a new virtual hard disk. The steps involved are as follows:
 1. Choose the type of disk (Dynamically Expanding, Fixed Size, Differencing).
 2. Name and choose a storage location for the disk.
 3. Configure the disk (including specifying the size of disk or copying the contents of an existing disk).
 - **New Floppy Disk** Selecting this action creates a 1.4-MB virtual floppy disk (.vfd) file in the location specified.
 - **Import Virtual Machine** Selecting this action enables you to import previously exported virtual machines by pointing to the appropriate virtual hard disk (.vhd) file. Selecting this option allows you to move virtual machines between different Hyper-V servers.



Note The Import Virtual Machine action does *not* let you import virtual machines created in Virtual Server 2005.

- **Hyper-V Settings** Selecting this action allows you to configure both Server and User settings as shown in Figure 2-9.

There are two Server settings you can configure:

- ☐ **Default Location for Virtual Hard Disks** Selecting this option enables you to specify the default location for virtual hard disk (.vhd) files to be used by the virtual machines running on the server. The default location is the C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks directory.
- ☐ **Default Location for Virtual Machine Configuration Files** Selecting this option enables you to specify the default location for the virtual machine configuration (.vmc) files on the server. The default location is the C:\ProgramData\Microsoft\Windows\Hyper-V directory.

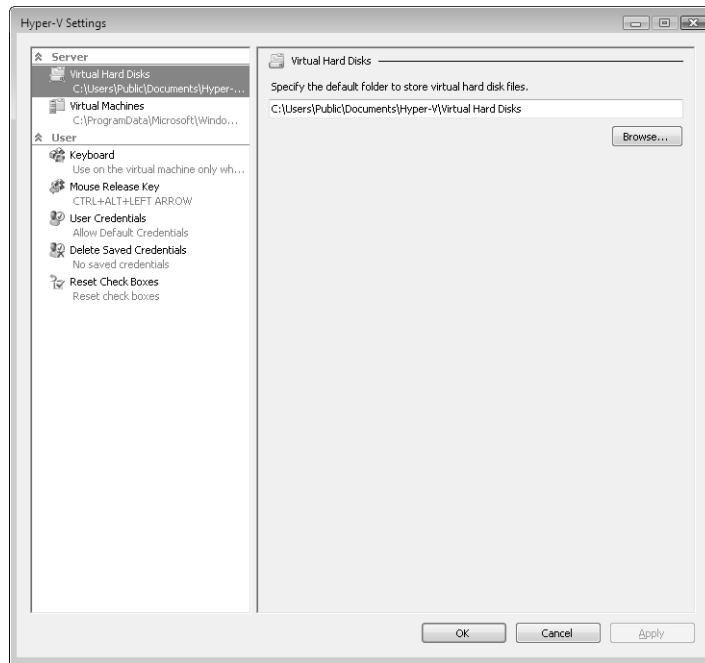


FIGURE 2-9 Configuring Server and User settings for a Hyper-V server.



Tip For the best performance, move the location for virtual hard disks to a non-system drive and move the configuration files to the same location.

There are five User settings that apply to users managing the Hyper-V server, the virtual machines running on the server, or both. These settings are as follows:

- ☐ **Keyboard** This option allows you to specify the default setting for how keyboard combinations such as Alt+Tab will be used.
- ☐ **Mouse Release Key** This option allows you to specify the setting for the key-stroke sequence used to release the mouse from inside a virtual machine. The default is Ctrl+Alt+Left Arrow, and you can change this to Ctrl+Alt+Right Arrow, Ctrl+Alt+Space, or Ctrl+Alt+Shift as desired. Note that this configuration option does not apply to guests that have had Integration Services installed on them.
- ☐ **User Credentials** This option allows you to specify the credentials that will be used to connect to a virtual machine. The default is to use the same credentials you used to run the Hyper-V Manager snap-in; otherwise, you will be prompted when connecting.
- ☐ **Delete Saved Credentials** This option allows you to delete any saved user credentials on the Hyper-V server for enhanced security.

- ☐ **Reset Check Boxes** This option allows you to reset all Hyper-V confirmation messages and wizard pages to their defaults when the Hyper-V role was installed.
- **Virtual Network Manager** Selecting this action enables you to configure virtual networking settings for the virtual machines running on the server. As illustrated by Figure 2-10, there are three types of virtual networks you can configure:
 - ☐ **External virtual networks** This type of virtual network binds to a physical network adapter on the host computer. An external network is required in order to access the Internet or to connect to organizational resources that do not reside in the parent partition. You can bind only one external network per physical adapter or port, so if multiple external networks are needed, additional physical adapters or ports will have to be installed in the Hyper-V server. VLAN access is also supported on external virtual networks if the physical network the parent partition is connected to is properly configured. You should use the external type of virtual network when you want to allow communication between different virtual machines running on the same host computer, between virtual machines and the parent partition, and between virtual machines and externally located (physical or virtual) servers.



Note Microsoft recommends that you have at least two physical network adapters on the host computer running Hyper-V: one network adapter dedicated to the physical machine and used for remote management, and one or more network adapters dedicated to the virtual machines.

- ☐ **Internal virtual networks** This type of virtual network is an external virtual network that is not bound to a physical network adapter. You should use this type of virtual network when you want to allow communication between different virtual machines running on the same host computer and between virtual machines and the parent partition, but not between virtual machines and externally located servers. You can also isolate virtual machines on an internal virtual network by selecting the Enable Virtual LAN Identification For Parent Partition check box for a particular adapter or port. A common use for internal virtual networks is to build test environments where you need to connect to the virtual machines from the parent partition.
- ☐ **Private virtual networks** This type of virtual network is an internal virtual network without a virtual network adapter in the parent partition. You should use this type of virtual network when you want to allow communication only between different virtual machines running on the same host computer. A typical use for private virtual networks is when you want to isolate virtual machines from network traffic in the parent partition and in the external networks.

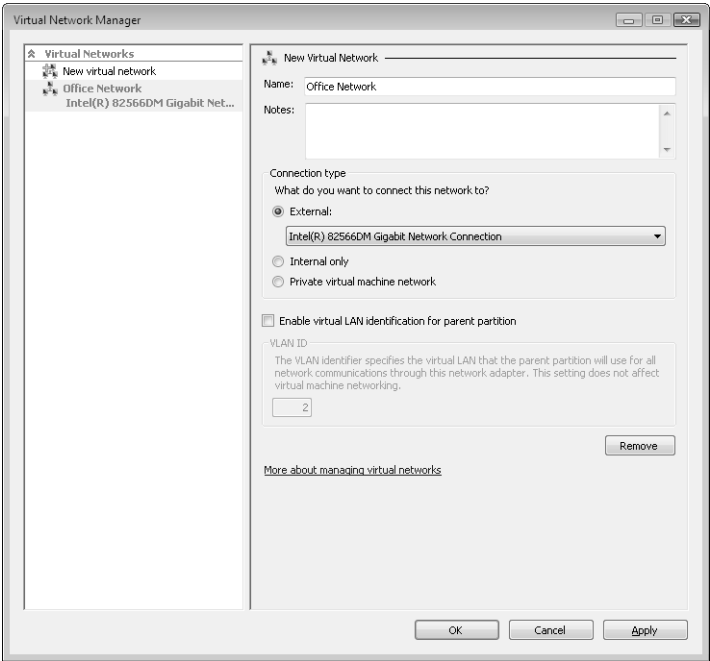


FIGURE 2-10 Configuring a virtual network.

Table 2-2 summarizes the different types of virtual networks you can configure and the connectivity allowed by each type. For more information about how networking works in Hyper-V, see the sidebar titled “Direct from the Source: The Hyper-V Networking Model” later in this section.

TABLE 2-2 Connectivity Allowed by Different Types of Virtual Networks

Type of Virtual Network	Between VMs on the Host Computer	Between VMs and the Parent Partition	Between VMs and External Servers
External	✓	✓	✓
Internal	✓	✓	
Private	✓		

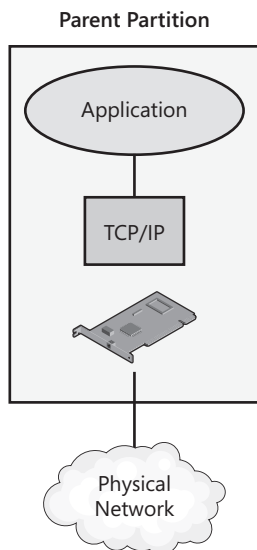
- **Edit Disk** Selecting this action starts the Edit Virtual Hard Disk Wizard, which enables you to make changes to existing virtual hard disks. The actions you can perform include the following:
 - ❑ **Compact** This option allows you to shrink a disk by removing blank space that remains when data is deleted from the disk.

- ❑ **Convert** This option allows you to convert a dynamic virtual hard disk to a fixed hard disk by creating a new fixed-size virtual disk having a different name and then copying the contents of the dynamic disk to the new fixed disk. The new fixed disk can then be associated with the virtual machine, and the virtual machine can be started, after which the old dynamic disk can be deleted.
- ❑ **Expand** This option allows you to expand the capacity of a virtual hard disk.
- **Inspect Disk** Selecting this option displays information about a virtual hard disk.

Direct from the Source: The Hyper-V Networking Model

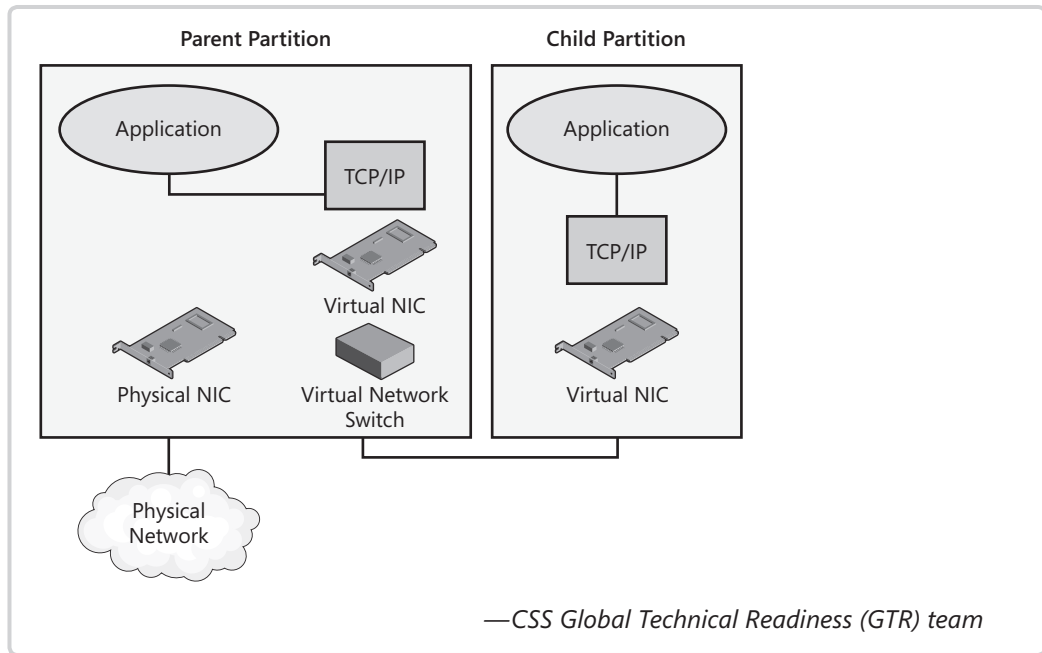
One of the more challenging concepts to grasp in Hyper-V is how networking is implemented both from the perspective of the Hyper-V server, which is essentially a virtual machine itself called the *parent partition*, and also from the perspective of the child partitions created and supported by the parent partition.

In general, when the Hyper-V role is installed and prior to creating any virtual networks, the parent partition is functioning as seen in this diagram:



In the configuration just shown, all protocols are bound to the physical network card, which provides direct connectivity for the Hyper-V server to the physical network.

After a virtual network is created and configured to be used by virtual machines (child partitions) running on the Hyper-V server, the networking model shifts as seen the diagram that follows.



Managing Virtual Machines

In addition to using the Hyper-V Manager snap-in to manage the Hyper-V server, you can also use this snap-in to manage various aspects of virtual machines running on the server. Figure 2-11 shows a Hyper-V server with a new virtual machine that has just been created on it. This virtual machine has not been started and has no operating system installed on it.

As you can see from Figure 2-11, the Actions pane now has two sections: an upper section named after the Hyper-V server (SEA-SCV) that displays the server-level settings that we have already described, and a lower section named after the new virtual machine (SEA-SRV1-V), which provides options you can select for managing various aspects of the virtual machine. If your Hyper-V Manager console is connected to additional Hyper-V servers and/or the servers have additional virtual machines, more sections are displayed in the Actions pane accordingly. Some of these VM-level management actions are self-explanatory (such as Start or Delete). Others require more explanation, as follows:

- **Connect** Let's you connect to and manage an individual virtual machine using the Virtual Machine Connection interface. There are two ways to connect to a virtual machine whether it is running or not:
 - ❑ By selecting the virtual machine in the center pane and then selecting the Connect action.
 - ❑ By double-clicking on the virtual machine in the center pane.

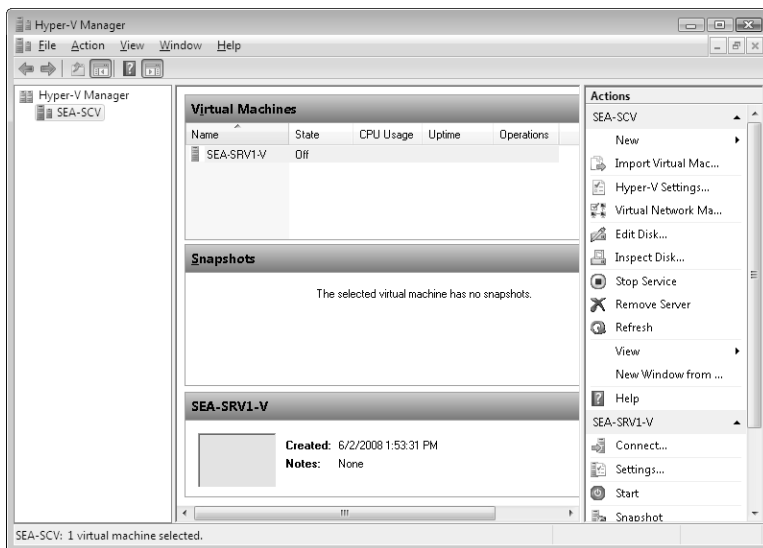


FIGURE 2-11 Hyper-V server with a new virtual machine created.



More Info For more information about connecting to virtual machines, see the section titled “Using the Virtual Machine Connection Tool” later in this chapter.

- **Settings** Selecting this action allows you to configure or modify different settings that apply to the selected virtual machine. These virtual machine settings fall into two categories: Hardware and Management settings.

The hardware settings you can configure for each virtual machine include the following:

- ❑ **Add Hardware** Allows SCSI, network adapters, and legacy network adapters to be added to a virtual machine. Each virtual machine can be configured with up to 12 virtual network adapters where eight of these can be of the “network adapter” type and four can be of the “legacy network adapter” type. The “network adapter” type provides better performance it’s a synthetic device that takes advantage of the new high-speed Hyper-V I/O architecture. For more information about network adapters and legacy network adapters, see the sidebar titled “Direct from the Source: Network Adapters in Hyper-V” later in this section.
- ❑ **BIOS** Allows changes to be made to the virtual machine’s BIOS, such as changing the Numlock status or the boot order.
- ❑ **Memory** Allows changes to be made to the amount of physical RAM allocated to the virtual machine.
- ❑ **Processor** Allows changes to be made to the number of virtual processors allocated to the virtual machine and the host physical processor resources allocated to virtual machines. (See Figure 2-12.)

- ❑ **IDE Controller** Allows you to add hard drives and DVD drives to the virtual machine. There are two IDE controllers, and two drive types can be supported per controller. Note that Hyper-V virtual machines can boot only from IDE drives, not from SCSI drives.
- ❑ **SCSI Controller** Allows you to add up to four SCSI controllers with up to 64 disks each, for a total of 256 drives, per virtual machine.
- ❑ **Network Adapter** Displays the configuration for the virtual network the virtual machine is connected to. You can also configure network adapter MAC addresses and enable VLAN IDs.
- ❑ **COM 1\2** Allows for communication with the parent partition via a named pipe connection. This can be useful for debugging a virtual machine.
- ❑ **Diskette Drive** Provides a connection to a 1.4-MB floppy disk created as a .vfd file.

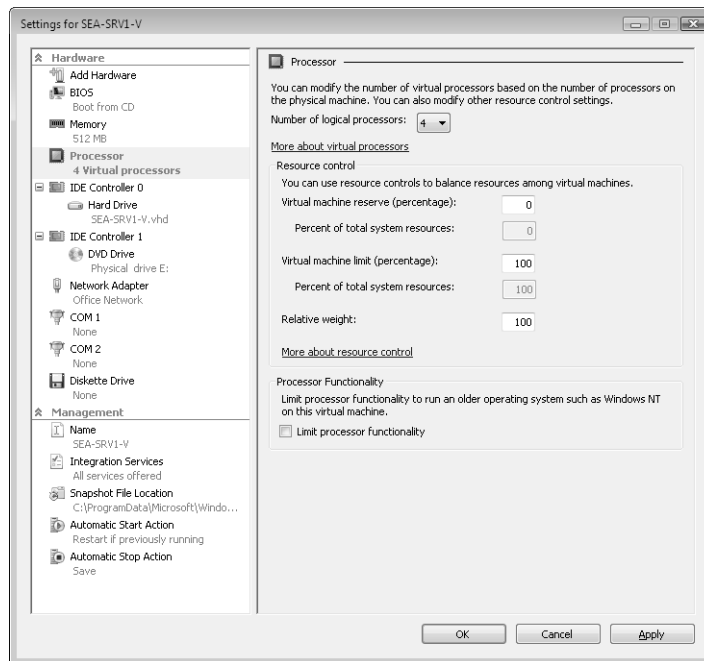


FIGURE 2-12 Configuring Processor settings for a virtual machine.

In addition to configuring the hardware settings just described, you can also use the Hyper-V Manager snap-in to configure different management settings for each virtual machine as follows:

- ❑ **Name** Allows the name of the virtual machine to be changed and for descriptive notes to be added.

- ❑ **Integration Services** Displays what Integration Services have been installed and are currently in effect. There are five services available: Operating System Shutdown, Time Synchronization, Data Exchange, Heartbeat, and Backup (volume snapshot).
- ❑ **Snapshot File Location** Displays the location of snapshots that have been taken of the selected virtual machine. Note that if there is an active snapshot of the virtual machine, the file location cannot be changed.
- ❑ **Automatic Start Action** Specifies the action the virtual machine executes when the parent partition starts. The default action is Automatically Start If It Was Running When The Service Stopped. A start delay can also be configured so that virtual machines starting up do not contend with the parent partition for resources on the host computer.
- ❑ **Automatic Stop Action** Specifies the action the virtual machine executes when the parent partition or the Virtual Machine Management Service stops. The default action is to save the state of the virtual machine.
- **Snapshot** Selecting this action takes a point-in-time snapshot of a virtual machine. The virtual machine can be running, saved, or stopped when the snapshot is taken. As shown in Figure 2-13, taking consecutive snapshots of a virtual machine builds a snapshot tree in the Snapshots pane with a green arrow followed by Now, indicating which snapshot is active in the virtual machine. Snapshots can also be annotated by adding descriptive notes to them. For more information about snapshots, see the section titled “Working with Snapshots” later in this chapter.

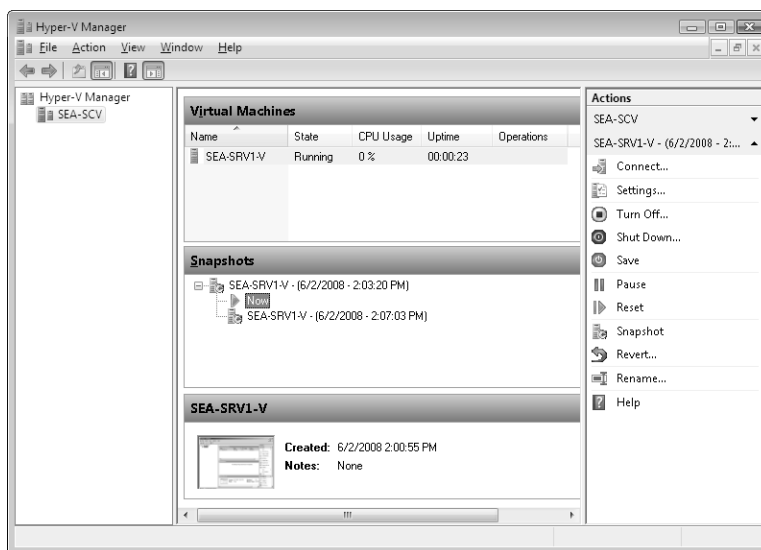


FIGURE 2-13 Snapshots of a virtual machine

- **Rename** Selecting this action allows you to rename a virtual machine. This change is reflected only in the Hyper-V Manager interface—the names of the virtual machine files or the machine name (as known to the guest operating system) are not changed.

Direct from the Source: Network Adapters in Hyper-V

Hyper-V contains two types of network adapters that can be used by guests: a legacy network adapter and a network adapter.

The *legacy network adapter* is an emulated adapter (Intel 21140 PCI) that is available to guests who either cannot take advantage of Integration Services or must have connectivity to the physical network to download and install prerequisites before they can take advantage of Integration Services (for example, Windows XP Professional x86 must download and install Service Pack 3).

A *network adapter* is a synthetic device that can be used only after Integration Services are installed in nonenlightened guests. Enlightened guests already have the necessary components installed in the operating system to begin taking advantage of this type of network adapter.

The default is to configure a network adapter when creating a new virtual machine. If a legacy network adapter needs to be added, it must be done after the virtual machine is created. This is accomplished by selecting the virtual machine in the Hyper-V Manager console and modifying the settings by using the Add Hardware process. If this is not done, there will be no virtual NIC present in the guest after it boots.

After Integration Services are installed on a guest, the legacy network adapter can be removed and replaced with a network adapter (synthetic NIC).



Note If a guest operating system is going to be installed using PXE boot to download an image, a legacy network adapter must be used and the boot order must be modified in the virtual machine settings.

—CSS Global Technical Readiness (GTR) team

Using the Virtual Machine Connection Tool

You can use the Virtual Machine Connection tool to connect to and manage an individual virtual machine running on a Hyper-V server. The Virtual Machine Connection tool uses the same Remote Desktop Protocol (RDP) technology used for remotely connecting to Windows desktops.

VMConnect links RDP to a simulated virtualized display of the VM. It's sometimes easier to think of it as a virtual keyboard video mouse (KVM) device in the parent partition—on one side, it's RDP; on the other, it's the keyboard and screen of the VMs.

Figure 2-14 shows the Virtual Machine Connection tool connected to a virtual machine named SEA-SRV1-V running on a Hyper-V server named SEA-SCV. The Virtual Machine Connection tool is currently running in windowed mode and shows that a guest operating system—a Full installation of Windows Server 2008 x64 Standard Edition—is in the process of being installed in the virtual machine.

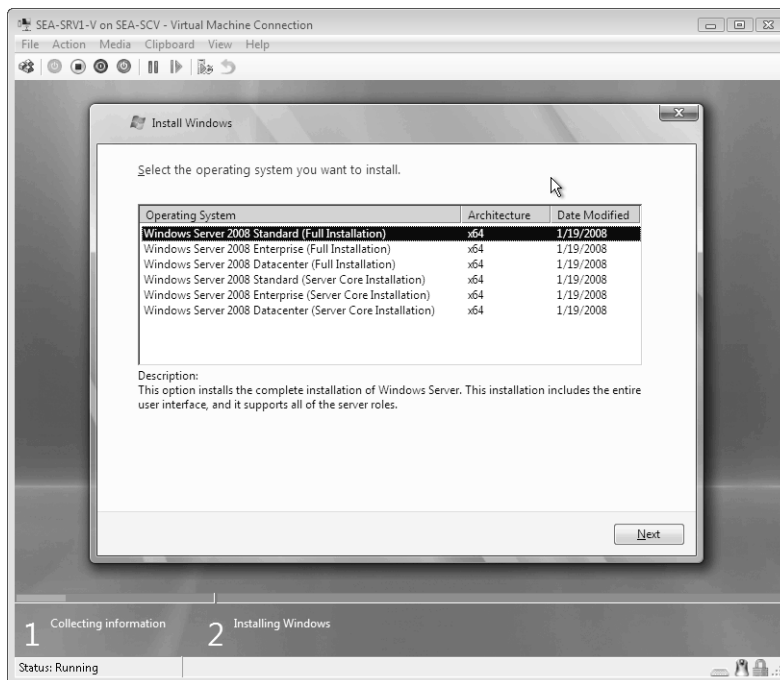


FIGURE 2-14 The Virtual Machine Connection tool.

The Virtual Machine Connection tool's menu bar provides the following options to select from:

- **File** This menu option allows you to access the Settings dialog box for the virtual machine (as shown earlier in Figure 2-12) or to exit from (close) the Virtual Machine Connection tool.

- **Action** This menu option allows you to perform any of the following actions for the virtual machine:
 - ❑ Display the Windows Logon screen (the screen that would result if you pressed Ctrl+Alt+Del in the virtual machine).
 - ❑ Turn Off, Shut Down, or Save the state of the virtual machine.
 - ❑ Pause or Reset the virtual machine.
 - ❑ Take a Snapshot of the virtual machine or Revert to a previous snapshot.
 - ❑ Choose the Insert Integration Services Setup Disk option, which launches the process of installing Integration Services on the virtual machine.
- **Media** This menu option includes a DVD Drive option that allows you to insert a DVD/CD/ISO file into the virtual machine's DVD drive or eject a disk from it, or to capture the physical DVD/CD drive on the host computer. It also provides a Diskette Drive option that allows you to insert or eject a virtual floppy disk drive (.vfd file).
- **Clipboard** This menu option includes a Type Clipboard Text option that allows you to transfer text from the parent partition into the child partition, and a Capture Screen option that allows you to capture a screen shot in the child partition so that you can paste it into an imaging program, such as Microsoft Paint, that is running in the parent partition.
- **View** This menu option includes a Full Screen Mode option that allows you to expand the Virtual Machine Connection interface so that it fills the screen, and a Toolbar option that allows you to return the Virtual Machine Connection tool to windowed mode.



Tip The Virtual Machine Connection tool also displays a toolbar when running in windowed mode. This toolbar is shown in Figure 2-14 immediately below the menu bar. You can use it to send Ctrl+Alt+Del to the virtual machine, start or stop the virtual machine, pause the machine, take a snapshot of the virtual machine's state, and perform other actions.

Installing the Virtual Machine Connection Tool

The Virtual Machine Connection tool is installed by default when you add the Hyper-V role to a Full installation of Windows Server 2008. When you use the Virtual Machine Connection tool to connect to and manage virtual machines running on your local Hyper-V server, the title bar of each Virtual Machine Connection tool displays *localhost* as the name of the Hyper-V server on which each virtual machine runs. If you use the Virtual Machine Connection tool to connect to and manage virtual machines running on a different Hyper-V server, the title bar of each Virtual Machine Connection tool displays the name of the Hyper-V server on which the virtual machines are running.

You can also install the Virtual Machine Connection tool onto a Windows Server 2008 computer that is not running the Hyper-V role, and then use the Virtual Machine Connection tool on this computer to manage virtual machines running on your Hyper-V servers. To do this, install Hyper-V Tools from the Remote Administration Tools section of the Remote Server Administration Tools (RSAT) feature using the Add Features Wizard.

You can also install the Virtual Machine Connection tool onto a computer running Windows Vista with Service Pack 1 (x86 or x64) Business, Enterprise, or Ultimate edition and use this computer to manage virtual machines running on your Hyper-V servers. To do this, download and install the Windows Vista Service Pack 1 Management Tools update for the release version of Hyper-V from <http://support.microsoft.com/kb/952627>.



Note If your Hyper-V server is running Server Core, you will not be able to install either the Hyper-V Manager snap-in or the Virtual Machine Connection tool directly on your server. Instead, you must use these tools remotely from a different computer running either Windows Vista SP1 or a Full installation of Windows Server 2008.

Connecting to a Virtual Machine

To use the Hyper-V Manager console to connect to and manage a virtual machine by using the Virtual Machine Connection tool, do one of the following:

- Right-click on a virtual machine listed in the top center Virtual Machines pane of the Hyper-V Manager console and select Connect.
- Click on a virtual machine listed in the top center Virtual Machines pane of the Hyper-V Manager console to select the virtual machine, and then click Connect in the Actions pane or select Connect from the Action menu.
- Double-click on a virtual machine listed either in the top center Virtual Machines pane or on a thumbnail of a virtual machine displayed in the lower center pane.

You can also launch the Virtual Machine Connection tool from the command prompt. For example, to connect to a virtual machine named SEA-SRV1-V running on the local Hyper-V server, type **"C:\Program Files\Hyper-V\vmconnect.exe" localhost SEA-SRV1-V** at the command prompt. If you have two or more virtual machines with the same display name, you can connect to the desired virtual machine by specifying the GUID of the virtual machine instead of its display name as shown in the preceding command example. To specify a GUID, you must use the **-G** switch like this: **"C:\Program Files\Hyper-V\vmconnect.exe" localhost -G <GUID>**.



Note Although the Hyper-V Manager snap-in always runs in an elevated state, the Virtual Machine Connection tool does not. To avoid authentication issues when running the Virtual Machine Connection tool on a computer running Windows Vista SP1, you must either run the tool As Administrator or add your user account to the Hyper-V Administrators role by using the Authorization Management tool.

Using Windows Keyboard Accelerators

Standard Windows keyboard accelerators must be replaced by their equivalents when managing a virtual machine using the Virtual Machine Connection tool. These differences are summarized in Table 2-3.

TABLE 2-3 Changes to Standard Keyboard Accelerators When Managing a Virtual Machine Using the Virtual Machine Connection Tool

Standard Windows Keyboard Accelerator	Virtual Machine Connection Equivalent	Description
CTRL+ALT+DEL	CTRL+ALT+END	Displays the Windows Security dialog box
ALT+TAB	ALT+PAGE UP	Switches between programs from left to right
ALT+SHIFT+TAB	ALT+PAGE DOWN	Switches between programs from right to left
ALT+ESC	ALT+INSERT	Cycles through the programs in the order they were launched
CTRL+ESC	ALT+HOME	Displays the Windows Start menu
N/A	CTRL+ALT+PAUSE	Changes the Virtual Machine Connection window to or from full-screen mode
N/A	CTRL+ALT+LEFT ARROW	Releases the mouse and keyboard focus from the Virtual Machine Connection window when Integration Services is not installed



Note By default, standard Windows keyboard accelerators are not sent to the virtual machine unless you are working in full-screen mode. You can modify this, however, so that standard Windows keyboard accelerators are always sent to the virtual machine when the Virtual Machine Connection tool has the focus. You do this by opening the Hyper-V Manager console, selecting Hyper-V Settings, choosing Keyboard, and selecting the Use On The Virtual Machine option. Note, however, that Ctrl+Alt+Del will always go to the host (physical) computer, so you must use Ctrl+Alt+End regardless of the setting you have selected here.

Creating a Virtual Machine

Once your Hyper-V server has been deployed and configured and you are familiar with how to use the Hyper-V Manager console and the Virtual Machine Connection tool, you can create new virtual machines (child partitions) on your server and install a guest operating system onto each virtual machine.

Based on how you configure disk storage, there are two types of virtual machines you can create:

- Virtual machines that have their guest operating system installed on a virtual hard disk, which is implemented as a file on the hard drive of the host computer
- Virtual machines that have their guest operating system installed on a separate hard drive on the host computer, a configuration that is known as a *passthrough disk*

The following sections outline the general procedures for creating virtual machines using each of these storage configurations. For additional information concerning how Hyper-V storage works and how it can be configured, see the sidebar titled “Direct from the Source: Understanding Hyper-V Storage” later in this section.



Tip Before you create a new virtual machine, make sure you have sufficient disk storage space on your host computer for the operating system and applications you will be installing in the virtual machine. Also make sure that you have configured a virtual network so that guests will be able to access the physical network if needed.

Direct from the Source: Understanding Hyper-V Storage

Hyper-V supports several different storage options, including Direct Attached Storage (DAS)—for example, SATA or SAS—and SAN Storage—for example, FC or iSCSI. After the Hyper-V server has been connected to storage, it can be made available to guests in many different ways.

After storage has been exposed to the Hyper-V server, there are two choices available for hosting the guest operating system.

- Creating a virtual hard disk (VHD) on one of the volumes on the Hyper-V server. The virtual hard disk is simply a file that is stored on one of the storage volumes on the Hyper-V server. There are two types of virtual hard disks: dynamic and fixed. The maximum size of a VHD file is 2040 gigabytes (just short of 2 terabytes).
- Using a passthrough disk, which allows the virtual machine to access the disk directly. The raw disk (no size limit) can be a disk local to the Hyper-V server or a logical disk (logical unit number [LUN]) on a SAN. Before configuring a guest

with a passthrough disk, the disk must be placed in an offline state so that there is no contention between the virtual machine and the Hyper-V server. This is accomplished in the Windows Disk Management snap-in or by using the Diskpart.exe command-line interface (CLI).

Connecting Storage to the Guest

There are three methods available to connect storage to a virtual machine:

- **IDE** The Hyper-V IDE controller allows for disks up to 2048 gigabytes. Additionally, the new filter driver used for IDE in Hyper-V essentially bypasses the emulation path for IDE, providing much higher performance that is almost on par with SCSI. The IDE controller can support either virtual hard disks or passthrough disks. There can be up to four IDE disks configured on a guest (2 controllers with 2 disks each). One important note is that Hyper-V virtual machines can boot only from IDE. Booting from virtual SCSI is not supported. This is mainly because a SCSI controller is a synthetic device and must be added only after Integrated Services have been installed on the guest.
- **SCSI** The Hyper-V SCSI controller is a synthetic device and therefore cannot be added to a guest configuration until after Integrated Services have been installed. There can be up to four SCSI controllers configured per guest. Each controller can support 64 disks each, for a total of 256 disks per virtual machine. SCSI disks backed with VHD are limited to 2040 GB. A guest cannot be configured to boot from a SCSI controller.
- **iSCSI** Guests connected to a physical network can take advantage of iSCSI storage. Guests can connect directly to iSCSI storage over an iSCSI network, completely bypassing the Hyper-V server itself. All that is required is the proper configuration of an iSCSI client in the guest and an iSCSI target running somewhere on the network that is accessible by the guest. There is no limit to the number of iSCSI disks that can be supported on the guest. A guest cannot boot from an iSCSI disk.

—CSS Global Technical Readiness (GTR) team



Tip You can bypass the 2048-GB size limitation for IDE and SCSI virtual disks by using passthrough disks.

Creating a Virtual Machine Using a Virtual Hard Disk

The general procedures for creating a new virtual machine that uses a virtual hard disk (.vhd file) and installing a guest operating system are as follows:

1. Launch the New Virtual Machine Wizard from the Hyper-V Manager console. Follow the steps of the wizard to assign memory, configure a network, and perform other required steps. If the operating system you plan on installing in your virtual machine is an unenlightened guest, do not configure a network at this point because you need to either install Integration Services first or configure a legacy network adapter for connectivity.



Note If your virtual machine will be running a 64-bit version of either Windows XP or Windows Server 2003, there is no driver for the legacy network adapter included in Hyper-V. This means the synthetic network adapter must be used, which requires Integration Services to be installed first.

2. When you get to the Connect Virtual Hard Disk page of the wizard, choose the Create A Virtual Hard Disk option and verify the location for the disk.
3. When you finish the wizard, the virtual machine will start and you can install the guest operating system from CD or DVD media. Connect to the virtual machine using the Virtual Machine Connection tool so that you can respond to any prompts displayed during the install process.
4. After you install any guest operating system, the next thing you should do is install the Integration Services components on your virtual machine.
5. At this point, shut down your virtual machine to configure additional storage controllers, additional hard disks, and additional processors as needed. Then boot your virtual machine and install roles and features, install applications, join the domain, and perform other initial configuration tasks as needed.

Creating a Virtual Machine Using a Passthrough Disk

The general procedures for creating a new virtual machine that uses a passthrough disk and installing a guest operating system are as follows:

1. Ensure that you have at least one dedicated disk volume of sufficient size on your host computer to use as the system/boot volume for your new virtual machine.
2. Ensure that you have a separate location available for storing the virtual machine configuration (.xml) files for your new virtual machine. This is required because a virtual machine configured with a passthrough disk uses the entire passthrough disk volume

for its operating system. The .xml files for the virtual machine must be stored on a different volume. The location you choose for storing the .xml files can be a different hard disk volume on your Hyper-V server, or it can even be a shared folder on a network file server. For more information, see the sidebar titled “Direct from The Source: Relocating Virtual Machine Configuration Files” later in this section.

3. Launch the New Virtual Machine Wizard from the Hyper-V Manager console. Follow the steps of the wizard to assign memory, configure a network, and perform other required steps. If the operating system you plan on installing in your virtual machine is an unenlightened guest, do not configure a network at this point because you need to either install Integration Services first or configure a legacy network adapter for connectivity.
4. When you get to the Connect Virtual Hard Disk page of the wizard, choose the Attach A Virtual Hard Disk Later option and continue through the wizard.
5. This time, when you finish the wizard, the virtual machine will not start because no storage has been configured for it to use.
6. Select your virtual machine in the Hyper-V Manager console, and click Settings in the Actions pane.
7. Select IDE Controller 0, click Add, select the Physical Hard Disk option, and then choose the correct physical disk volume from the drop-down list.
8. Select IDE Controller 1, and select the physical CD/DVD drive, or mount an .iso image file that has your operating system files.
9. Apply the settings you have configured, start your virtual machine, and install the guest operating system. Connect to the virtual machine by using the Virtual Machine Connection tool so that you can respond to any prompts displayed during the install process. Continue as described in the previous section.

Direct from the Source: Relocating Virtual Machine Configuration Files

The typical configuration of a virtual machine (guest) includes storing the virtual machine configuration files in the default location on the system drive under \ProgramData\Microsoft\Windows\Hyper-V in a folder corresponding to the name given to the virtual machine in the New Virtual Machine Wizard. This location can be changed by manipulating the settings for the Hyper-V server using Hyper-V Settings in the Actions pane in the Hyper-V Manager console.

There are scenarios where storing virtual machine configuration files on a remote server that is not running Hyper-V is a very real possibility. Storing Hyper-V configuration files in an alternate location is required when using passthrough disks. This is because the entire disk is used for the operating system files and there is no room for

the configuration files. This is true whether this configuration is used in a standalone Hyper-V server or when making a virtual machine highly available in a failover cluster.

As an example, follow these steps to store configuration files in a remote location (for example, File Server):

1. First, configure a folder on a remote machine that will be shared and used to store the virtual machine configuration files. In this example, the shared folder VMCONFIG is created on a remote server that can be accessed from the Hyper-V server.
2. When configuring the virtual machine, use the network share for the location of the virtual machine configuration files (UNC path).
3. If the default permissions on the share are not modified, an error will be encountered when you are trying to complete the New Virtual Machine Wizard.
4. Permissions need to be modified on the share such that the user running the New Virtual Machine Wizard and the Hyper-V server computer account both have Write permissions to the share. After that has been accomplished, the wizard will complete and the configuration files will be placed on the file share.

—CSS Global Technical Readiness (GTR) team

Working with Virtual Machines

You can use the Hyper-V Manager console to perform a number of management tasks involving virtual machines. This section briefly examines two of these tasks:

- Exporting and importing virtual machines
- Working with snapshots

Exporting and Importing Virtual Machines

You can use the Hyper-V Manager console to export a virtual machine from one Hyper-V server so that you can import it onto a different Hyper-V server. This import/export functionality thus allows you to migrate a virtual machine from one host computer to another.

The procedure for migrating a virtual machine from one Hyper-V server involves two steps:

1. Export the virtual machine from the first Hyper-V server as a collection of exported files and folders.
2. Import the exported files and folders onto your destination Hyper-V server.

The following is an outline of the steps involved for exporting a virtual machine:

1. Begin by shutting down the virtual machine you want to move. To shut down a virtual machine, select the virtual machine in the Hyper-V Manager console and click Shut Down in the Actions pane.
2. Decide on the location to which you will export your virtual machine. Your export location could be any one of the following:
 - ❑ A temporary folder on an external hard drive to transport the exported virtual machine files from the first Hyper-V server to the destination server.
 - ❑ A shared folder on a network file server used to temporarily store the virtual machine files until they are moved to the destination server.
 - ❑ A shared folder on your destination server that represents the final location to which your virtual machine is being migrated.
3. Select the virtual machine you want to export, and click Export in the Actions pane. When the Export Virtual Machine dialog box is displayed, type or browse to the path of the export location. If the destination folder is a shared folder on the network, specify the path to the folder as a UNC path.
4. Click the Export button to initiate the export process.

When the export process is finished, the following files and folders will be present in the export location:

- **Config.xml** An XML file that contains information about the original locations of all virtual hard disks configured for the exported virtual machine.
- **Virtual Machines** A folder that contains an export file whose name is of the form <GUID>.exp. This export file contains configuration information for the exported virtual machine and is converted during the import process into an XML configuration file.
- **Virtual Hard Disks** A folder that contains the virtual hard disks (.vhd files) for the exported virtual machine.
- **Snapshots** A folder that contains information about any snapshots taken of the virtual machine, including the snapshot differencing disks (.avhd files) and state information files (.vsv and .bin files) for those snapshots.

After you have exported your virtual machine and copied the export files and folders to their final locations on your destination server, you are ready to import these files and folders so that you can re-create your virtual machine on the destination server.

But there are two things you need to know about first concerning this import process. First, you can import only virtual machines that were exported from another Hyper-V server. You cannot import virtual machines that were imported from either Virtual Server 2005 or Virtual PC. This is because even though all three server virtualization products (Hyper-V, Virtual

Server, and Virtual PC) use the same virtual hard drive (.vhd) file format, they store virtual machine configuration information differently and also have additional incompatibilities in terms of the features they each support.

Second, you can perform the import process only once per exported virtual machine. This is because, during the import process, the export (.exp) files are converted into XML configuration (xml) files. What this also means is that if the import process fails or is performed incorrectly—for example, if you import the exported files and folder into the wrong location—the only way to recover is to delete the virtual machine, relocate the .vhd files to the correct location, and then re-create the virtual machine by recalling the settings that were used.

The following is an outline of the steps involved for importing your exported virtual machine files and folders:

1. Make sure your exported files and folders are in their correct locations on your destination server.
2. Connect to your destination server using the Hyper-V Manager console, and click Import Virtual Machine in the Actions pane.
3. In the Import Virtual Machine dialog box, type or browse to the location of the exported files and folders.
4. Click the Import button to initiate the import process.

After the virtual machine has been imported, try starting it and make sure it is functioning properly.



Tip An easier way of moving virtual machines from one Hyper-V server to another is to use System Center Virtual Machine Manager 2008. For more information about this product, see Chapter 3.

Working with Snapshots

A *snapshot* is a point-in-time picture of the state and settings of a virtual machine. Hyper-V allows you to capture snapshots of virtual machines and revert back to those snapshots. For example, you could install a guest operating system on a virtual machine, take a snapshot, make some configuration changes to the guest, and then revert back to your snapshot to undo your configuration changes.

Snapshots can be taken when a virtual machine is running, saved, or shut down. Snapshots cannot be taken, however, when a virtual machine is paused. You can take multiple snapshots of a virtual machine to create a snapshot tree, which is a sequence of snapshots taken at different times. You can manage this tree of snapshots by deleting individual snapshots or an entire subtree of snapshots. And you can revert to any particular snapshots in a tree by applying that snapshot to your virtual machine.

Snapshots can be particularly useful during the test and development stages of a product development cycle. For example, you can install an application you are developing on a virtual machine, take a snapshot, and then try working with the application. If the application crashes, you can revert back to your snapshot and try to reproduce the steps that led to the crash, which can help you troubleshoot the cause of the crash.



Note Snapshots should generally not be used in production environments because they are not intended as replacements for proper backup and recovery processes. For example, although running domain controllers in virtual machines is supported on Hyper-V, taking snapshots of domain controllers and then reverting to them later can cause replication problems and should therefore not be done in a production environment.

You can use the Hyper-V Manager console to take a snapshot of a virtual machine. To do this, select the virtual machine in the Virtual Machines pane and click Snapshot in the Actions pane for the selected virtual machine. As Figure 2-15 shows, when a new snapshot is created, an icon for the snapshot is displayed in the Snapshots pane in the center of the console. The new snapshot is given a descriptive name that includes the name of the virtual machine from which the snapshot was made and the date and time when the snapshot occurred.

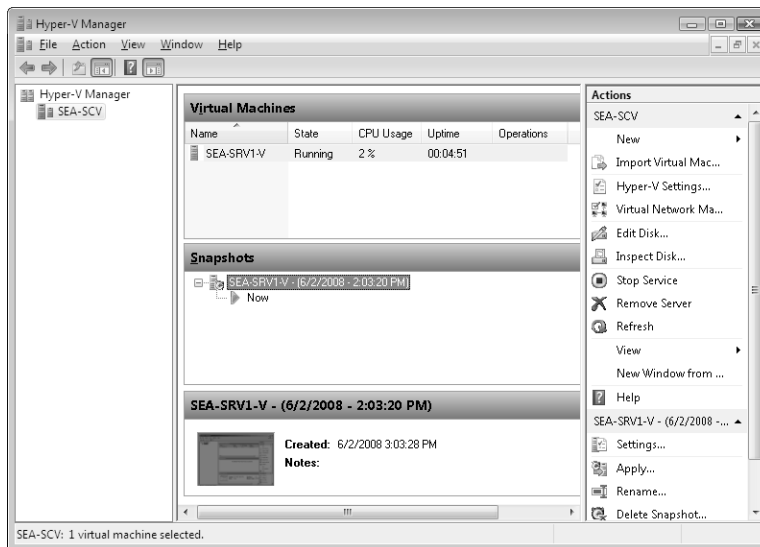


FIGURE 2-15 Snapshot of a virtual machine.

As shown in Figure 2-15, when you take a snapshot of a virtual machine, a green arrow labeled Now is also displayed in the Snapshots pane. This Now arrow represents the current running configuration of the virtual machine.

You can also take snapshots of a virtual machine using the Virtual Machine Connection tool. You can do this in two ways:

- By selecting Snapshot from the Action menu bar item.
- By clicking the Snapshot icon on the toolbar.

When you take a snapshot using the Virtual Machine Connection tool, a Snapshot Name dialog box is displayed, prompting you to provide a descriptive name for the new snapshot.

By default, all snapshot files are stored in the following folder on your Hyper-V server:

`%SystemRoot%\ProgramData\Microsoft\Windows\HyperV\Snapshots`

You can change this location on a per-VM basis by configuring the settings for each VM.

Taking a snapshot of a virtual machine creates the following types of snapshot files:

- Virtual machine configuration (.xml) file
- Virtual machine saved state (.vsv) files
- Virtual machine memory contents (.bin) files
- Snapshot differencing disk (.avhd) files

As shown in Figure 2-15, when you select a snapshot in the Snapshots pane, the Actions pane displays various actions you can perform with that snapshot. These include the following:

- **Apply** Selecting this action allows you to copy the complete virtual machine state from the selected snapshot to the active virtual machine. This allows you to revert your virtual machine to the state contained in the selected snapshot. When you select this action, any unsaved data in your currently active virtual machine will be lost. Because of this, you are prompted to choose whether you want to create a new snapshot of your current virtual machine state before the state contained in the selected snapshot is applied.
- **Rename** Selecting this action allows you to modify the descriptive name of the selected snapshot.
- **Delete Snapshot** Selecting this action allows you to remove only the files associated with the selected snapshot. (Files for other snapshots will not be affected.) After you delete a snapshot, you will be unable to revert to the state contained in that snapshot. The current state of the active virtual machine is not affected by this action.
- **Delete Snapshot Tree** Selecting this action allows you to delete the selected snapshot and any snapshots hierarchically beneath it. The current state of the active virtual machine is not affected by this action.



Note Snapshots are read-only. The only settings you can configure for a snapshot are its name and any attached descriptive notes.

If you select the virtual machine in the Virtual Machines pane, the tasks displayed in the Actions pane change to the following:

- **Snapshot** Selecting this action allows you to take another snapshot of your virtual machine.
- **Revert** Selecting this action allows you to apply the previous snapshot (the snapshot directly above the green Now arrow in the Snapshots pane).



Tip When you delete an entire snapshot tree, the result will be the last snapshot applied to the running virtual machine. If your intention, instead, is to have the result be the pristine installation of your virtual machine, your first snapshot should be taken after your virtual machine is configured and before you make any alterations for testing your configuration. That way, you can apply your first snapshot (the root snapshot) before deleting the snapshot tree, and the result is that your virtual machine's configuration will return to where you started before you made your alterations.

Direct from the Source: Best Practices for Configuring Virtual Machines

Virtual machine performance is affected not only by how the physical server is configured but also by the selections made when configuring the virtual machine itself. The following sections discuss best practices that should be considered when configuring virtual machines in Hyper-V.

Change Default Locations for Virtual Hard Disk and Machine Configuration Files

Change the default locations for storing the virtual hard disks and the virtual machine configuration files. By default, they are stored on the drive where the operating system is installed. For better performance, move the location to another disk on a SAN, if possible. If no SAN storage is configured, use another internal, fault-tolerant drive or drives that can be dedicated to storing virtual machine data and are not supporting the operating system.

Install Integration Services

The first, and probably most important, best practice for virtual machines is to install Integration Services, which comes with Hyper-V, as soon as possible if the operating system running in the virtual machine is supported. Then update Integration Services as needed.

Uninstall VM Additions and Compact VHDs

When migrating virtual machines from Virtual PC or Virtual Server 2005 R2, uninstall the VM Additions and compact the virtual hard disk before moving the disk to the Hyper-V server.

Set Display for Best Performance

For the best display in a virtual machine, ensure the display interface is set for Best Performance. This ensures the hardware acceleration is set to Full.

Configure Fixed-Size VHDs

Choose to configure fixed-size virtual hard disks rather than dynamically expanding disks. Performance is faster, the file system is less likely to fragment, and managing space on the physical disk is easier. Always defragment a physical disk before creating a virtual hard disk.

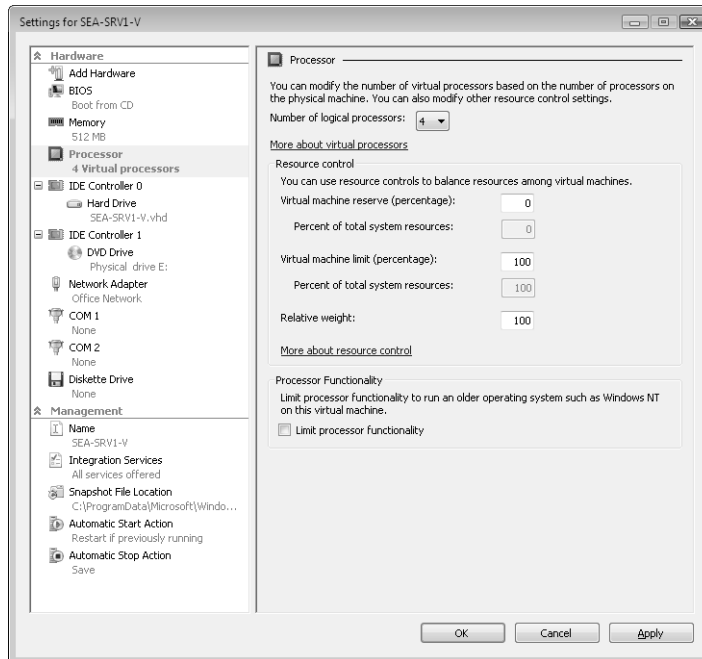
Use SCSI Virtual Adapters for Data Drives

Hyper-V requires the virtual machine to boot from a virtual IDE controller; however, SCSI virtual adapters can be used after that for mounting additional virtual hard disks. Although performance differences between a virtual IDE controller and a virtual SCSI controller in Hyper-V is negligible (with Integration Services installed), more and larger capacity virtual hard disks can be attached to a virtual SCSI controller (4 controllers with 64 virtual disks each, for a total of 256). So, if you need more than four virtual hard disks attached to a virtual machine, use a virtual SCSI controller.

Allocate CPU Resources Based on Anticipated Usage

It is also important to determine virtual machine performance to ensure CPU resource allocation on the physical server is adequate to support the workload inside the virtual machine. The default in Hyper-V server is to treat all virtual machines equally. In reality, this might not be a practical or wise business decision. When allocating physical machine CPU resources to a virtual machine, it is important not to over-subscribe—that is, trying to allocate more physical machine resources than are really available. The next version of System Center Virtual Machine Manager (SCVMM 2008) will play a key role in monitoring virtual machine performance.

To help with this process, the following figure shows the Processor configuration setting for a virtual machine:



The interpretation of the Processor configuration settings shown in the preceding figure are as follows:

- ❑ **Virtual Machine Reserve** Percent of the logical CPU that is set aside for the running virtual machine. As each VM is started, the available capacity on the Hyper-V server itself is reduced.
- ❑ **Virtual Machine Limit** Percentage of logical CPU that a running virtual machine is not allowed to exceed.
- ❑ **Relative Weight** Determines how CPU is distributed when there is contention among all running virtual machines. The higher the number, the more processing power allocated to the VM. Relative weight can range from 1 to 10,000.
- ❑ **Limit Processor Functionality** Reduces vulnerability of some operating systems to high central processing unit identification (CPUID) values. Unexpected, high CPUID values could cause a crash.

Consider Using Passthrough Disks

When creating a virtual machine, it is a best practice to use virtual hard disks; however, circumstances might dictate using passthrough disks. Performance using passthrough disks is slightly better than performance achieved using a virtual hard disk (VHD), you can conserve drive letters, and you can configure disks larger than two terabytes (if the external storage supports that). However, when using passthrough disks, the virtual machine configuration files need to be relocated to either another hard disk or a file share. Additionally, you lose snapshot functionality when using passthrough disks, and they are not portable like a file (VHD).

Ensure File Share High Availability

If a file share is being used to store virtual machine configuration data, it is a best practice to ensure the file share is highly available (for example, a file share being hosted in a failover cluster). You also need to modify the security on the file share to allow the Hyper-V server (all nodes of it if it's in a failover cluster) write access to the share.

Configure Domain Controllers to Optimize Performance

Domain controllers are supported in Hyper-V. The following best practices are recommended for these configurations:

- Never save state in a domain controller because this might cause synchronization issues in the domain.
- Never pause a domain controller virtual machine for long periods of time because this might adversely affect replication.
- Always shut down a domain controller.
- Do not take snapshots of a domain controller.
- Make a determination regarding time synchronization. The decision is either to use the Hyper-V Integration Service For Time Synchronization or not. If the decision is to treat the virtualized domain controllers like hardware-based domain controllers, disable the Time Synchronization capability in the settings for each virtual machine and point the PDC Emulator to an external time source and allow all the other domain controllers to synchronize with the PDC Emulator. If the decision is to synchronize with the parent partition, enable only the Time Synchronization capability for the domain controller holding the PDC Emulator FSMO role.

—CSS Global Technical Readiness (GTR) team

Tools for Managing Hyper-V and Virtual Machines

We've already described in detail two tools you can use for managing Hyper-V servers and virtual machines: the Hyper-V Manager snap-in and the Virtual Machine Connection tool, which can be installed on any Windows Server 2008 or Windows Vista SP1 computer. There are several other ways, however, that you can remotely manage Hyper-V servers and virtual machines running on them, including the following:

- Remote Desktop Connection
- Terminal Services RemoteApp
- Windows Management Instrumentation (WMI)
- Windows PowerShell
- System Center Virtual Machine Manager 2008

System Center Virtual Machine Manager 2008 is covered in detail in Chapter 3, so the sections that follow deal with the remaining management tools.

Managing Hyper-V Using Remote Desktop Connection

Instead of connecting to a remote Hyper-V server using the Hyper-V Manager snap-in, you can use Remote Desktop Connection (Mstsc.exe) to connect to the desktop of the remote server and then run the Hyper-V Manager console locally on that server. To do this, you simply have to enable Remote Desktop on the remote Hyper-V server.

There are some downsides to this approach for managing Hyper-V, however:

- If your Hyper-V server is running on a Server Core installation of Windows Server 2008, the Hyper-V Manager snap-in and Virtual Machine Connection tools are not available locally on the server, so this management approach won't work in this case.
- If you are connected to the remote desktop of a Hyper-V server and you open the Virtual Machine Connection tool on the server, you might have to contend with the following issues:
 - You will not have any mouse control inside the virtual machine unless Integration Services has been installed. The workaround is of course to make sure Integration Services is installed on your virtual machines.
 - Certain keyboard accelerators such as Ctrl+Alt+Del might have unexpected results when the Virtual Machine Connection tool is running within a Remote Desktop session. This is because Remote Desktop Connection intercepts these keyboard accelerators before the Virtual Machine Connection can see them. To resolve this, you have to modify your Hyper-V Server settings to allow Windows keyboard

accelerators to go to the virtual machine—for example, by changing the release key combination to something other than Ctrl+Alt+Left Arrow and by using the toolbar button or Action menu of Virtual Machine Connection to send a Ctrl+Alt+Del signal to the virtual machine.

Managing Hyper-V Using Terminal Services RemoteApp

If you want to manage Hyper-V servers from a computer running an earlier version of Microsoft Windows, such as Windows XP Professional, you can do so by using Terminal Services RemoteApp to publish the Hyper-V Manager application on the Hyper-V server using Terminal Services. In brief, the procedure for doing this is as follows:

1. Install the Terminal Services role on a server running a Full installation of Windows Server 2008. Be sure to include the Terminal Services Web Access role service in your Terminal Services role installation.
2. Install the Hyper-V role or Hyper-V role management tools on the terminal server.
3. Configure user/group membership as needed for the Remote Desktop Users and Terminal Services Web Access Computers security groups. Also, configure RDP and security settings as needed.
4. Launch the RemoteApp Wizard from Terminal Services RemoteApp Manager, and add the Hyper-V Manager console (Virtmgmt.msc) to the list of published applications on the terminal server.

Now, from the computer running the earlier Windows operating system, connect to the terminal server using Terminal Services Web Access, select the remotely published application (Hyper-V Manager) to launch the connection screen, and authenticate with the terminal server. At this point, the Hyper-V Manager console will be running on your computer—it will look and work just as if the console was installed locally on your computer, with the exception of the word *Remote* in the title bar indicating that it is a RemoteApp and not a local program.

Managing Hyper-V Using Windows Management Instrumentation

Hyper-V also includes a Windows Management Instrumentation (WMI) provider that enables developers and scripters to build custom tools, utilities, and scripts for most aspects of a Hyper-V platform. This WMI provider exposes WMI classes for the following types of functionality:

- BIOS
- Input
- Integration components
- Memory

- Networking
- Processor
- Profile registration
- Resource management
- Serial devices
- Storage
- Video
- Virtual system
- Virtual system management

For example, the BIOS classes include the *Msvm_BIOSElement* class, which represents virtual BIOS software that is loaded into memory to configure and start the system, and the *Msvm_SystemBIOS* class used to associate a virtual system with its BIOS. The *Msvm_BIOSElement* class exposes properties such as *BaseBoardSerialNumber*, *BIOSGUID*, *BIOSNumLock*, *BootOrder*, and so on. Some of these properties are read-only, while others are read/write.

You can find more information concerning the Hyper-V WMI provider in the MSDN Library at [http://msdn.microsoft.com/en-us/library/cc136992\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/cc136992(VS.85).aspx).

Managing Hyper-V Using Windows PowerShell

You can also use Windows PowerShell to manage most aspects of a Hyper-V platform. Windows PowerShell is a new command-line shell and task-based scripting technology that helps administrators control and automate system administration tasks. Windows PowerShell includes numerous system administration utilities, has consistent syntax and naming conventions, and enables improved navigation of common management data, such as the Windows registry, the certificate store, and WMI namespaces. Windows PowerShell also includes an intuitive scripting language specifically designed for Windows administration. For more information about Windows PowerShell, see the Windows PowerShell FAQ at <http://www.microsoft.com/windowsserver2008/en/us/powershell-faq.aspx>. A collection of useful resources for learning Windows PowerShell can be found on the Script Center on Microsoft TechNet at <http://www.microsoft.com/technet/scriptcenter/hubs/msh.msp>.

A growing Windows PowerShell management library for Hyper-V can be found on the CodePlex Project at <http://www.codeplex.com/PSHyperv>. CodePlex is Microsoft's open-source project-hosting Web site that allows you to start a new project, join an existing one, or download software created by the CodePlex community. Note that the CodePlex site is provided by Microsoft to the developer community solely as a Web storage site and service—Microsoft does not control, review, revise, endorse, or distribute any third-party

projects hosted on this site. For more information about CodePlex, see its Terms Of Use at <http://www.codeplex.com/Legal/Terms.aspx>.

At the time of this writing, the CodePlex Windows PowerShell management library for Hyper-V includes 66 Windows PowerShell functions that can be used to perform Hyper-V management tasks, such as finding a VM, connecting to a VM, discovering and manipulating the state of a VM, backing up a VM, exporting a VM, taking a snapshot of a VM, and many other common administrative tasks.



Note You can use Windows PowerShell to manage virtual machines running on Hyper-V servers running Server Core, but you must run your scripts remotely from a computer that has Windows PowerShell installed on it. In addition, your Windows PowerShell scripts can be used only to access the WMI interface on the targeted Server Core installation. This means that the primary Windows PowerShell cmdlet you will use to manage virtual machines running on Server Core is the *Get-WmiObject* cmdlet, which also has the associated *gwmi* alias in Windows PowerShell.

Direct from the Source: Managing Hyper-V with Windows PowerShell

Hyper-V provides an MMC snap-in that can be used to manage it remotely, but no command-line tools. Fortunately, the MMC invokes a set of WMI interfaces that are all documented on MSDN, which allows for development of tools using any language capable of supporting WMI.

Windows PowerShell has built-in support for WMI with a *Get-WmiObject* cmdlet. After the cmdlet retrieves the object, its properties and methods are available to a Windows PowerShell script. Because you need to script Hyper-V operations, and because Windows PowerShell is positioned as Microsoft's scripting tool for the future, I set about developing a library of Windows PowerShell functions that are available from Microsoft's CodePlex Open Source repository <http://www.codePlex.com/PSHyperV>. These functions range in complexity from a simple *Get-VM*—which takes a name and returns the matching *MSVM_VirtualMachine* WMI object (in its raw state)—to complex tools for modifying the configuration of VMs and their virtual hard disks. The same handful of Windows PowerShell techniques are used again and again. For example, here is the basic form of *GET-VM*:

```
Function Get-VM
{
    Param ($machineName, $Server=".")

    $WQL="Select * From MSVM_ComputerSystem Where ElementName Like '$machineName' AND
Caption Like 'Virtual%' "

    Get-WmiObject -computername $Server -Namespace "root\virtualization" -Query $WQL
}
```

As you can see, the function has two parameters. The *Server* parameter defaults to ".", the local machine. Later, I decided to default the machine name to a wildcard, which is the % sign in the WMI query language. Because I kept using *Name**, I added code to replace * with % in the name, and I added switches that modify the WMI Query Language (WQL) to return only running machines. So now I use the command like this:

```
Get-VM -Server "HV-Core"-Running | suspend-VM
```

The *MSVM_ComputerSystem* object has a method called Request State Change, so *suspend-VM* calls this asking for a change in state to Suspended. Changing the settings for a VM is a task that needs a bit more work. This involves calling the Modify Virtual System Resources method of the *MSVM_VirtualSystemManagementService* WMI object. This is given a machine name, a block of XML, and a *Null* variable to contain the result. Building the XML usually means getting a WMI object, which describes the object being changed, and then calling its *getText* method and asking for XML text, like this:

Function Set-VMemory

```
{Param ($VM , $memory, $server=".")
  if ($VM -is [String]) {$VM=(Get-VM -MachineName $VM -Server $Server) }
  $memSettingData=Get-WmiObject -computerName $vm.__server Namespace
    "root\virtualization" Query "select * from Msvm_MemorySettingData
    where instanceId Like 'Microsoft:$( $vm.name)%' "
  $memSettingData.Limit          = $Memory / 1MB
  $memSettingData.Reservation    = $Memory / 1MB
  $memSettingData.VirtualQuantity = $Memory / 1MB
  $arguments=@($VM.__Path, @($memSettingData.psbase.GetText([System.Management.
  TextFormat]::WmiDtd20)) , $null)
  $VSMgtSvc = (Get-WmiObject -computerName $vm.__server -Namespace
    "root\virtualization" -Class "MsVM_VirtualSystemManagementService")
  $result=$VSMgtSvc.psbase.invokeMethod("ModifyVirtualSystemResources",$arguments)
  if ($result -eq 0) {"Set memory for '$($vm.elementName)' to $memory."} else
    {"Failed to set memory for '$($vm.elementName)', result code: $result."} }
}
```

With these two techniques under your belt and documentation of the WMI provider from MSDN (not forgetting the examples from CodePlex), you can put together your own scripts to do pretty much anything.

—James O'Neill, IT Pro Evangelist, Microsoft UK

Key Features of Hyper-V

The overview of Hyper-V technologies provided by the previous section has already introduced you to some of the capabilities and features of Hyper-V. However, for purposes of summarization, the following are some of the key features of Microsoft's Hyper-V platform:

- **Broad OS Support** Hyper-V includes broad support for simultaneously running different types of operating systems, including both 32-bit and 64-bit operating systems across different server platforms, such as Windows, Linux, and others.
- **Extensibility** Hyper-V has standards-based WMI interfaces and APIs to enable independent software vendors (ISVs) and developers to quickly build custom tools, utilities, and enhancements for the virtualization platform.
- **Network Load Balancing** Hyper-V includes new virtual switch capabilities that provide the ability to use the Windows Network Load Balancing (NLB) service to load-balance across virtual machines running on different servers.
- **New and Improved Architecture** Hyper-V has a new 64-bit microkernelized hypervisor architecture that enables the platform to provide a broad array of device support methods and improved performance and security.
- **New Hardware Sharing Architecture** Hyper-V includes a new Virtual Service Provider (VSP) and Virtualization Service Client (VSC) architecture, which provides improved access and utilization of hardware resources, such as disk, networking, and video.
- **Quick Migration** Hyper-V provides the ability to rapidly migrate a running virtual machine from one physical host computer to another with minimal downtime, leveraging the high-availability capabilities of Windows Server 2008 and System Center management tools.
- **Scalability** Hyper-V includes support for multiple processors and cores at the host level and improved memory access within virtual machines to enable virtualization environments to be scaled to support a large number of virtual machines on a given host while continuing to leverage quick migration for scalability across multiple hosts.
- **Symmetric Multiprocessors (SMP) Support** Hyper-V includes support for up to four processors in a virtual machine environment in order to take advantage of multithreaded applications running in a virtual machine.
- **Virtual Machine Snapshots** Hyper-V provides the ability to take snapshots of a running virtual machine to enable you to easily revert to a previous state, thus improving backup and recoverability solutions.

An additional discussion of the features of the release to manufacturing (RTM) version of Hyper-V can be found at <http://www.microsoft.com/windowsserver2008/en/us/hyperv-features.aspx>.

Comparing Hyper-V and Virtual Server 2005 R2

Because of its new and advanced capabilities, Hyper-V can probably be expected to quickly supplant Microsoft Virtual Server in enterprises that have been using Virtual Server for server consolidation, business continuity, and testing/development reasons. To show the difference between these two platforms, Table 2-4 compares some of their features and specifications.

TABLE 2-4 Comparison of Features and Specifications of Virtual Server 2005 R2 and Hyper-V

Feature or Specification	Virtual Server 2005 R2	Hyper-V
Architecture		
Type of virtualization	Hosted	Hypervisor-based
Performance / Scalability		
32-bit VMs	Yes	Yes
64-bit VMs	No	Yes
Multiprocessor VMs	No	Yes
Maximum Guest RAM	3.6 GB	64 GB
Maximum Guest CPUs	1	4
Maximum Host RAM	256 GB	1 TB
Maximum Number of Running VMs	64	128
Resource Management	Yes	Yes
Availability		
Guest to Guest Failover	Yes	Yes
Host to Host Failover	Yes	Yes
Host Migration	Yes	Yes
VM Snapshots	No	Yes
Management		
Scriptable/Extensible	Yes, COM	Yes, WMI
User interface	Web Interface	MMC 3.0 Interface
SCVMM Integration	SCVMM 2007	SCVMM 2008

Comparing Hyper-V and VMware ESX Server

Hyper-V also compares favorably with competing products from other virtualization vendors. As an example of this, Table 4-5 compares the features and specifications of Hyper-V with those of VMware ESX Server 3.5.

TABLE 4-5 Comparison of Features and Specifications of Hyper-V and VMware ESX Server 3.5

Feature or Specification	Hyper-V	VMware ESX Server 3.5
Hypervisor	Microkernel	Monolithic
x64 Hosts and Guests	Yes	Yes
Guest SMP	Yes (up to 4-way)	Yes
Maximum Guest RAM	64 GB	64 GB
Maximum Host RAM	1 TB	128 GB
Maximum Guest CPUs	4	4
Quick Migration	Free	Requires VMotion
Management	Integrated (Physical + Virtual)	Virtual Management Only

Key Benefits of Using Hyper-V

The benefits of using Hyper-V in business environments of all sizes can be numerous. The following is a quick summary of three key benefits:

- Hyper-V allows you to easily consolidate systems, workloads, and operating environments. For example:
 - You can use Hyper-V to combine multiple workloads and operating systems onto one physical server, thus reducing the costs of hardware and operations.
 - You can use Hyper-V to test versions of software on the hardware that they will later use in production mode without affecting your production workloads.
 - You can use Hyper-V virtual systems as low-cost test systems without jeopardizing your production workloads.
 - You can run multiple operating system types and releases on a single physical computer, with each virtual system running the operating system that best matches its application and user requirements.
- Hyper-V allows you to optimize use of your computing resources. For example:
 - Using Hyper-V can allow you to achieve high resource usage by assigning virtual resources such as processors and memory to physical resources through mechanisms such as dispatching and paging. The virtual resources that can be provided in this manner can exceed the physical system resources in both quantity and functionality.
 - Using Hyper-V can allow you to dynamically share physical resources and resource pools. The result is higher resource usage, particularly for variable

workloads where the average needs are much less than might be supplied by using an entire dedicated resource.

- ❑ Because different workloads tend to show peak resource usage at different times of the day and week, implementing multiple workloads in the same physical server using Hyper-V can help you improve system use, cost, and performance.
- Hyper-V can improve the flexibility and responsiveness of your IT infrastructure and thus bring the same kinds of benefits to your business. For example:
 - ❑ Hyper-V can allow service providers to create one virtual system or clone many virtual systems on demand, thus facilitating dynamic resource provisioning.
 - ❑ Hyper-V allows you to implement virtual systems with variable resources to enable the manual or automated management of workload resources.

Hyper-V Usage Scenarios

Finally, I'll conclude this chapter by briefly describing four common usage scenarios involving Hyper-V. These are the four usage scenarios:

- Server Consolidation
- Business Continuity and Disaster Recovery
- Testing and Development
- The Dynamic Data Center

Server Consolidation

A key use of server or machine virtualization is to help consolidate many servers onto a single system while maintaining isolation between the servers. One of the main benefits of using Hyper-V for this purpose is the lower total cost of ownership (TCO), which is achieved not only by lowering hardware requirements but also by lowering the costs of power, cooling, physical hosting space, and hardware maintenance fees. Another benefit of using Hyper-V for this purpose is its ability to integrate 32-bit and 64-bit workloads in the same environment.

Business Continuity and Disaster Recovery

Business continuity is the ability to minimize both scheduled and unscheduled downtime. Hyper-V includes powerful business continuity features, such as live backup and quick migration, that allow businesses to meet stringent uptime and response metrics. Disaster recovery is also a key component of business continuity, and by leveraging the Failover Clustering feature of Windows Server 2008, Hyper-V provides support for disaster recovery within IT environments and across data centers, even for geographically dispersed clusters.

Testing and Development

Testing and development are important business functions that can leverage the use of virtualization technologies such as Hyper-V. By using virtual machines in place of physical systems, developers can create and test a wide variety of scenarios in an isolated, self-contained environment that closely resembles the behavior of physical systems. With its extensive guest operating system support and checkpoint features, Hyper-V also helps maximize the use of test hardware, which can help reduce development costs, improve software life-cycle management, and improve test coverage.

The Dynamic Data Center

When integrated with Microsoft System Center, Hyper-V can help you realize the promise of the dynamic data center—the vision of self-managing dynamic systems and operational agility. Because Hyper-V includes features such as automated virtual machine reconfiguration, flexible resource control, and quick migration, data center administrators can create a dynamic IT environment that employs virtualization not only for responding to problems but also to anticipate increased demands. For more information about Microsoft System Center products and how they can be used with Hyper-V to provide an integrated virtualization solution, see Chapters 3 and 8.

Additional Resources

The resources listed in this section were either referred to in the chapter or provide additional information concerning concepts and products discussed in this chapter.

General

A general overview of the features and benefits of Hyper-V can be found on the Windows Server 2008 product information page at <http://www.microsoft.com/windowsserver2008/en/us/default.aspx>. The following pages in particular are useful resources concerning Hyper-V:

- The “Virtualization and Consolidation with Hyper-V” page at <http://www.microsoft.com/windowsserver2008/en/us/virtualization-consolidation.aspx> summarizes the core usage scenarios for Hyper-V.
- The “Windows Server 2008 Hyper-V FAQ” page at <http://www.microsoft.com/windowsserver2008/en/us/hyperv-faq.aspx> provides useful information concerning Hyper-V support, licensing, requirements, and features.
- The “Windows Server 2008 Hyper-V Key Features” page at <http://www.microsoft.com/windowsserver2008/en/us/hyperv-features.aspx> summarizes the key enhancements found in the RTM version of Hyper-V.

- The “Supported Guest OS on Windows Server 2008 Hyper-V” page at <http://www.microsoft.com/windowsserver2008/en/us/hyperv-supported-guest-os.aspx> details the latest information concerning guest operating system support in Hyper-V.

Another useful overview of Hyper-V usage scenarios and benefits can be found in the white paper “Windows Server 2008 Hyper-V Product Overview” available from the Microsoft Download Center at <http://www.microsoft.com/downloads/details.aspx?FamilyID=0fe4e411-8c88-48c2-8903-3fd9cbb10d05&DisplayLang=en>.

For detailed technical information concerning implementing and maintaining Hyper-V, the best place to start is the Virtualization TechCenter on Microsoft Technet at <http://technet.microsoft.com/en-us/virtualization/default.aspx>. On this page in the “Products and Technologies” section, you will find a Hyper-V link that takes you to another page that displays a growing list of technical resources for IT administrators who want to learn more about deploying and managing Hyper-V in their organizations. Some of these resources are specifically called out in the sections that follow to help you find them more easily.

Deploying Hyper-V

For a quick introduction on installing and using Hyper-V, see the “Step-by-Step Guide to Getting Started with Hyper-V” white paper available from the Microsoft Download Center at <http://www.microsoft.com/downloads/details.aspx?FamilyID=bcaa9707-0228-4860-b088-dd261ca0c80d&DisplayLang=en>.

A quick summary of how to install the RTM version of Hyper-V can also be found at <http://www.microsoft.com/windowsserver2008/en/us/hyperv-install.aspx>.

Installing the release version of the Hyper-V technology for Windows Server 2008 is also described in Microsoft Knowledge Base (KB) article KB950050 at <http://support.microsoft.com/kb/950050>.

The Hyper-V Release Notes, containing last-minute information about the RTM version of Hyper-V, can be obtained from the Microsoft Download Center at <http://www.microsoft.com/downloads/details.aspx?FamilyID=3ed582f0-f844-40ba-b692-230845af1149&DisplayLang=en>.

For more detailed information about deploying Hyper-V, see the “Hyper-V Planning and Deployment Guide,” which is available from the Microsoft Download Center at <http://www.microsoft.com/downloadS/details.aspx?FamilyID=5da4058e-72cc-4b8d-bbb1-5e16a136ef42&displaylang=en>.

Managing and Maintaining Hyper-V

The Windows Vista Service Pack 1 Management Tools update for the release version of Hyper-V is an update package (.msu file) that can be used to install both the Hyper-V

Manager snap-in and the Virtual Machine Connection tool on a computer that is running Windows Vista Service Pack 1 (SP1). You can find more information about this update and where to obtain it from Microsoft Knowledge Base article KB952627 at <http://support.microsoft.com/kb/952627>.

Detailed information concerning the Hyper-V WMI provider can be found in the MSDN Library at [http://msdn.microsoft.com/en-us/library/cc136992\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/cc136992(VS.85).aspx).

A growing Windows PowerShell management library for Hyper-V can be found on the CodePlex Project at <http://www.codeplex.com/PSHyperv>.

The “Step-by-Step Guide for Testing Hyper-V and Failover Clustering,” available from the Microsoft Download Center at <http://www.microsoft.com/downloads/details.aspx?FamilyID=cd828712-8d1e-45d1-a290-7edadf1e4e9c&DisplayLang=en>, demonstrates how to make a virtual machine highly available by creating a simple two-node cluster.

The white paper “Windows Server 2008 Hyper-V and BitLocker Drive Encryption,” available from the Microsoft Download Center at <http://www.microsoft.com/downloads/details.aspx?FamilyID=2c3c0615-baf4-4a9c-b613-3fda14e84545&DisplayLang=en>, explains how to use Hyper-V and BitLocker Drive Encryption together for enhanced security.

The white paper “Performance Tuning Guidelines for Windows Server 2008” contains a section on tuning performance for the Hyper-V role and can be downloaded from Windows Hardware Developer Central (WHDC) at http://www.microsoft.com/whdc/system/sysperf/Perf_tun_srv.mspx.

Hyper-V on Server Core

For helpful information about how to deploy and manage Hyper-V on the Server Core installation option of Windows Server 2008, see the book *Windows Server 2008 Server Core Administrator's Pocket Consultant* by Mitch Tulloch (Microsoft Press, 2008). See <http://www.microsoft.com/mspress/books/12977.aspx> for more information.

Resources for Hyper-V Developers

Developers who are interested in learning how to develop applications that use hypercalls can learn more about them in the MSDN Library at <http://msdn.microsoft.com/en-us/library/bb969694.aspx>.

Hyper-V Bloggers at Microsoft

A good place to begin traversing the blogosphere in search of the latest Hyper-V information is the Microsoft Virtualization Team Blog found at <http://blogs.technet.com/virtualization>.

John Howard, Senior Program Manager, Hyper-V team, Windows Core Operating System Division, has many helpful posts concerning Hyper-V on his blog at <http://blogs.technet.com/jhoward/archive/tags/Hyper-V/default.aspx>. See especially his five-part series of posts about remote management of Hyper-V, which begins with <http://blogs.technet.com/jhoward/archive/2008/03/28/part-1-hyper-v-remote-management-you-do-not-have-the-requested-permission-to-complete-this-task-contact-the-administrator-of-the-authorization-policy-for-the-computer-computername.aspx>.

Mike Kolitz, Software Design Engineer in Test on the Virtualization Technologies team at Microsoft, has lots of helpful “how-to” posts concerning Hyper-V on his blog at <http://blogs.msdn.com/mikekol/archive/tags/Microsoft+Hyper-V/default.aspx>.

James O'Neill, a Windows Server Evangelist at Microsoft UK, has tons of helpful information about managing Hyper-V using Windows PowerShell on his blog at <http://blogs.technet.com/jamesone/archive/tags/Virtualization/default.aspx>.

Another Microsoft blogger who often posts about managing Hyper-V using Windows PowerShell is the Virtual PC Guy, Ben Armstrong, Program Manager on the core virtualization team at Microsoft. You can find the Hyper-V posts on Ben's blog at http://blogs.msdn.com/virtual_pc_guy/archive/tags/Developing+on+Virtual+Server+_2F00_+Hyper-V/default.aspx.

Matthijs ten Seldam, a Principal Consultant with Microsoft Consulting Services who focuses on virtualization, has been developing a “Virtual Server to Hyper-V import tool” that can simplify the task of taking virtual machines created on Virtual Server/Virtual PC and using them on Hyper-V. You can read more about this tool in his blog at <http://blogs.technet.com/matthts/default.aspx>.

Jose Barreto, a member of the Storage Solutions Division at Microsoft, has a helpful post titled “Failover Clustering for Windows Server 2008 Hyper-V with File Server Storage” on his blog at <http://blogs.technet.com/josebda/archive/2008/07/16/failover-clustering-for-hyper-v-with-file-server-storage.aspx>. Another useful post on his blog is “Storing Windows Server 2008 Hyper-V files on a CIFS/SMB file share,” which can be found at <http://blogs.technet.com/josebda/archive/2008/06/24/storing-windows-server-2008-hyper-v-files-on-an-cifs-smb-file-share.aspx>. Still other useful posts about Hyper-V on Jose's blog can be found at <http://blogs.technet.com/josebda/archive/tags/Hyper-V/default.aspx>.

Taylor Brown, Test Lead for Windows Core OS Division on the Hyper-V Team, has a helpful post titled “Hyper-V WMI: Creating/Applying/Deleting Virtual Machine Snapshots” on his blog at <http://blogs.msdn.com/taylorb/archive/2008/06/16/hyper-v-wmi-creating-applying-deleting-virtual-machine-snapshots.aspx>. Other useful posts about Hyper-V on Taylor's blog can be found at <http://blogs.msdn.com/taylorb/archive/tags/Hyper-V/default.aspx>.

Tony Voellm, the lead of the Hyper-V Performance Team, has a blog called All Topics Performance that has many useful posts about Hyper-V performance monitoring at <http://blogs.msdn.com/tvoellm/archive/tags/Hyper-V+Performance+Counters/default.aspx>.

Clive Watson, Virtualization Architectural Product Technical Specialist at Microsoft UK, often posts about Hyper-V on his blog at http://blogs.technet.com/clive_watson.

The Microsoft Enterprise Support Windows Server Core Team has some helpful posts about Hyper-V on their blog ASKCORE found at <http://blogs.technet.com/askcore/archive/tags/Hyper-V/default.aspx>. One especially useful post is “Publishing the Hyper-V Management Interface using Terminal Services” found at <http://blogs.technet.com/askcore/archive/2008/07/22/publishing-the-hyper-v-management-interface-using-terminal-services.aspx>, which explains how to use Terminal Services RemoteApp to publish the Hyper-V Manager snap-in so that you can run it on a pre-Vista version of Windows.

Other Hyper-V Bloggers

Mark Wilson, a Senior Customer Solution Architect for a leading IT services company, has compiled a useful list of videos from the Hyper-V product team on his blog at <http://www.markwilson.co.uk/blog/2008/07/how-hyper-v-works-product-team-videos.htm>.

Hyper-V Forum on TechNet

To obtain help with your questions and problems concerning Hyper-V, and to help others, use the Hyper-V forum on Microsoft TechNet at <http://forums.technet.microsoft.com/en-US/winserverhyperv/threads>.

Chapter 3

Managing Virtualization— VMM 2008

In the previous chapter, we saw how to provision and manage virtual machines running on Windows Server 2008 Hyper-V hosts. Although Hyper-V alone might be sufficient for some organizations, others might have virtualized workloads running on the earlier Microsoft Virtual Server 2005 R2 SP1 platform or on VMware ESX 3.x Server computers within a VMware VI3 environment. These organizations can benefit from implementing the latest version of Microsoft System Center Virtual Machine Manager (VMM), which now has the capability of managing virtualized workloads running on all three host platforms—Hyper-V, Virtual Server, and VMware ESX Server—from a single, centralized platform. This chapter delves into the workings of Virtual Machine Manager 2008 and explains how it works, how to use it, its key features and benefits, and key usage scenarios.

Understanding Virtual Machine Manager 2008

System Center Virtual Machine Manager 2008 consists of a number of components that work together at different layers to facilitate the provisioning and management of virtualized workloads across an enterprise. This section describes the terminology, different components, and underlying architecture of VMM 2008 to explain how the product works.

Terminology

The following are some of the key concepts and terms you need to understand when working with VMM 2008:

- **Guest operating system profile** A saved collection of settings that provide customization of the guest operating system. This profile is analogous to a setup answer file and contains information about the system settings, administrator account, and domain. Specific guest operating system profiles can be saved in the library and then used to quickly apply the settings to new virtual machines that are created from templates.
- **Hardware profile** A saved collection of settings that define the hardware characteristics of a virtual machine. These settings include items such as processors, memory, network, and DVD drives. Specific hardware profiles can be saved in the library and then used to quickly apply the settings to new virtual machines and templates.
- **Host** Also known as a virtual machine host, a physical computer that can host one or more virtual machines. Examples of hosts that can be managed using VMM 2008

include servers running Microsoft Windows Server 2008 with the Hyper-V role installed, servers running Microsoft Virtual Server 2005 R2, and servers running VMware ESX. Hosts are added by using the Add Hosts Wizard in the VMM Administrator Console, and until you add a host you cannot use VMM to create virtual machines.

- **Library server** The component of VMM 2008 that holds stored virtual machines, virtual hard disks, .iso files (CD/DVD software images), post-deployment customizations scripts, hardware configurations, and templates. The library provides a single interface for all of these virtualization building blocks.
- **Managed host** A host that has been added to a VMM library. VMM 2008 allows for controlling multiple hosts by adding them to a central library and managing these hosts from one centralized location. After being added to the library, a host then becomes a managed host that can be managed by only one VMM server at a time. Although multiple VMM servers can exist on a network, a host can be managed by only one of these at a time. Should a different VMM server want to add a host to its library and manage that host, it would have to take the host away from whatever other VMM server had it.
- **Performance and Resource Optimization (PRO)** A new feature in VMM 2008 that leverages the monitoring and alerting capabilities of Microsoft System Center Operations Manager (OpsMgr) 2007 to surface tips or recommendations within VMM 2008 that help administrators ensure high performance and an efficient virtualized environment.
- **Physical-to-Virtual (P2V)** A process in VMM 2008 that converts a physical machine into a virtual machine.
- **Stored virtual machine** A managed virtual machine whose .vhd files and other properties are stored in the VMM library. A new .vmc file is created for a new virtual machine created from a stored virtual machine.
- **Template** A combination of a guest operating system profile, hardware profile, and one or more .vhd files. The .vhd file containing the operating system files has computer identity information removed using Sysprep. Templates are used to create new virtual machines.
- **Virtual machine host** Also known simply as a host, a virtual machine host is a physical computer that can host one or more virtual machines. Examples of hosts that can be managed using VMM 2008 include servers running Windows Server 2008 with the Hyper-V role installed, servers running Microsoft Virtual Server 2005 R2 SP1, and servers running VMware ESX 3.x.
- **Virtual-to-Virtual (V2V)** A process in VMM 2008 that converts a virtual machine running in a VMware environment (specifically, ESX virtual machines using the .vmdk format) into a virtual machine running in a Windows Hyper-V environment.

VMM 2008 Components

VMM consist of several core components, as described in the following sections. These components can be either installed together on a single server or distributed across multiple servers (or even workstations in some instances).



More Info For more information on installing VMM 2008 components, see the section titled “Installing VMM 2008” later in this chapter.

Virtual Machine Manager Server

The VMM Server is the core component of a VMM 2008 infrastructure—all other VMM components interact and communicate through the VMM Server. The Virtual Machine Management Service runs on the VMM Server and enables the running of commands and transferring of files throughout your VMM infrastructure. The VMM Server also controls all communications with other VMM components and with virtual machine hosts and VMM Library Servers via VMM Agents installed on these other computers. The VMM Server also connects to the Microsoft SQL Server 2005 or 2008 database used to store all VMM configuration information. By default, the VMM Server is also the default VMM Library Server. You configure and manage the VMM Server using the VMM Administrator Console.

Virtual Machine Manager Library Server

The VMM Library Server maintains the VMM library, a catalog of resources that can be used to create and configure virtual machines within a VMM infrastructure. The library contains files stored on library shares and can contain file-based resources, including .iso images, scripts, virtual hard disks, virtual floppy disks, virtual machine templates, guest operating system profiles, and hardware profiles. The library can also contain stored virtual machines that are not in use.

Virtual Machine Manager Agent

The VMM Agent manages virtual machines on virtual machine hosts and enables both and Library Servers to communicate with the VMM Server. Using the VMM Administrator Console to add a host or a Library Server belonging to a trusted domain automatically installs the VMM Agent on that managed computer. If the host is not joined to a domain, belongs to an untrusted domain, or resides on the perimeter network, the VMM Agent must be installed locally on the host before you can add the host using the VMM Administrator Console.

Virtual Machine Manager Administrator Console

The VMM Administrator Console is an MMC console you can use to manage global configuration settings; manage and monitor hosts and Library Servers; and create, deploy, and manage virtual machines. You can install the VMM Administrator Console on the same computer as the VMM Server or on a different computer. Installing the VMM Administrator Console also installs the Windows PowerShell console, which provides Virtual Machine Manager cmdlets you can use to perform all tasks that you can do using the VMM Administrator Console from the command line.

Virtual Machine Manager Self-Service Portal

The VMM Self-Service Portal is an optional, Web-based component you can use to allow end users to create and manage their own virtual machines. You do this by configuring self-service policies that control which templates self-service users can use to create their virtual machines, how many virtual machines they can create, which hosts their virtual machines can run on, and which actions the users can perform on their virtual machines.



Tip You must install the VMM Administrator Console on the same computer as your OpsMgr server if you plan on using the Reporting feature of VMM. This is because the Windows PowerShell console, used by Virtual Machine Manager, is needed by the System Center Operations Manager 2007 administrator in order to perform tasks from within the Virtualization Management Pack.

VMM 2008 Architecture

VMM 2008 was designed using a modular architecture to provide the greatest flexibility for managing the entire virtualization infrastructure of an enterprise. Using VMM 2008, you can manage virtualized workloads on hosts running Microsoft's Hyper-V or Virtual Server 2005 R2 platforms, or on VMware's ESX Server platform.

As shown in Figure 3-1, the modular architecture of VMM 2008 consists of three layers that communicate with one another using well-known documented interfaces:

- Client Layer
- Engine Layer
- Managed Computer Layer

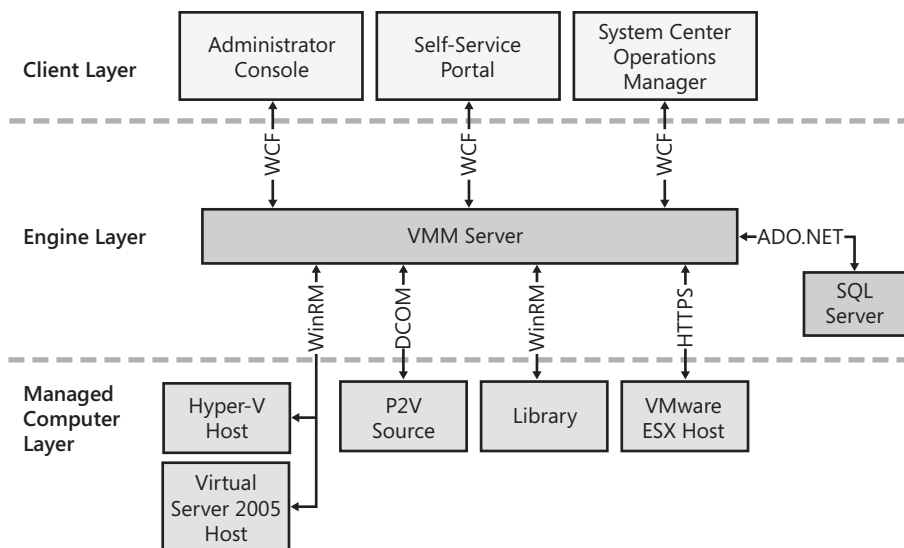


FIGURE 3-1 Modular architecture of VMM 2008.

Interlayer Communications

Communications between the different layers of the VMM 2008 architecture involve the following transport mechanisms:

- **Windows Communication Foundation** WCF is a Microsoft messaging platform for building service-oriented applications that is part of the .NET Framework 3.0. In VMM 2008, WCF is used for all communication between the Client Layer applications and the Engine Layer.
- **Windows Remote Management** WinRM is the Microsoft implementation of the WS-Management Protocol, a standard Simple Object Access Protocol (SOAP)-based, firewall-friendly protocol that enables hardware and operating systems from different vendors to interoperate. WinRM uses a client/server architecture that includes a HyperText Transfer Protocol (HTTP) listener on the WinRM server that awaits calls from WinRM clients. In VMM 2008, WinRM is used for communication between the Engine Layer and Hyper-V hosts, Virtual Server hosts, and Library Servers.
- **Distributed Component Object Model** DCOM is the Microsoft Component Object Model (COM) specification that defines how components communicate over Windows-based networks. In VMM 2008, the Engine Layer communicates with Physical-to-Virtual (P2V) source servers in the Managed Computer Layer using Windows Management Instrumentation (WMI) via DCOM.
- **Hypertext Transfer Protocol over Secure Sockets Layer** HTTPS is a combination of HyperText Transfer Protocol (HTTP) over Transport Layer Security (TLS). In VMM 2008, HTTPS is used by the Engine Layer for calling virtual infrastructure (VI) Web Services application programming interfaces (APIs) on VMware ESX hosts in the Managed Computer Layer.

In addition to the preceding transport mechanisms, VMM 2008 also uses ADO.NET for communications between the VMM Server and the Microsoft SQL Server database within the Engine Layer. ADO.NET is a suite of data access technologies included in the .NET Framework class libraries that provide access to relational data and XML.

Communications Ports

Communication between Client Layer applications, the Engine Layer, and managed hosts and Library Servers in the Managed Computer Layer of VMM 2008 take place using specific well-known TCP ports. This means that if the components of VMM 2008 are distributed across multiple computers, the host firewalls on these computers must be configured to enable communications over these ports. If Windows Firewall is enabled on these computers when VMM 2008 components are installed on them, the necessary exceptions are automatically opened in Windows Firewall.

Table 3-1 summarizes the transport mechanisms and ports used for communications by VMM 2008.

TABLE 3-1 Transport Mechanisms and Ports Used for Communications Between VMM 2008 Architectural Components

Communications Endpoints	Transport	Port
VMM Server to VMM Agent (control)	WinRM	80
VMM Server to VMM Agent (data)	BITS	443
VMM Server to remote database	HTTP	1433
VMM Server to P2V source	WinRM	135
VMM Administrator Console to VMM Server	WCF	8100
VMM Administrator Console to VMM Self-Service Portal	WCF	80
VMM Library to virtual machine hosts	BITS	80
Virtual machine host to virtual machine host	BITS	80
VMM Self-Service Portal user Internet Explorer session to Virtual Server host	VMRC	5900
VMM Self-Service Portal user Internet Explorer session to Hyper-V host	RDP	3389
VMM Administrator Console reporting view to System Center Operations Manager (OpsMgr) reporting server	HTTP	80
VMConnect on Hyper-V hosts for single-class console view	—	2179

Table 3-2 summarizes the ports used by each component of VMM 2008.

TABLE 3-2 Ports Used by Each Component of VMM 2008

Component	Ports Needed
VMM Server	80 (HTTP, WS-MAN) 443 (HTTPS, BITS) 8100 (WCF connections to Windows PowerShell or Administrator Console)
VMM Library Server	80 (HTTP, WS-MAN) 443 (HTTPS, BITS) 3389 (RDP) 2179 (VMConnect on Hyper-V hosts for single-class console view) 5900 (VMRC on Virtual Server hosts)
Virtual machine hosts	80 (HTTP, WS-MAN) 443 (HTTPS, BITS) 3389 (RDP) 2179 (VMConnect on Hyper-V hosts for single-class console view) 5900 (VMRC on Virtual Server hosts)
SQL Server	1433 (Remote SQL instance connection) 1434 (SQL browser service—only needed for initial setup)
VMware Virtual Center server	443 (HTTPS for calling VI Web Services APIs)
VMware ESX hosts	443 (HTTPS for calling VI Web Services APIs) 22 (SSH for sFTP files to/from ESX hosts—not needed for ESX version 3.5i)

Client Layer

The Client Layer of the VMM 2008 architecture represents the applications and interfaces you use to interact with VMM 2008. These applications include

- VMM Administrator Console
- VMM Self-Service Portal
- System Center Operations Manager
- Windows PowerShell Command-Line Interface

Using the applications in the Client Layer, you can perform actions such as creating and deploying a new virtual machine, starting or stopping virtual machines, monitoring virtual machines, and other tasks.

When you perform an action using one of the applications in the Client Layer, these actions are transformed into a Windows PowerShell script, which is run by the Engine Layer of VMM 2008 to perform the specified action.



More Info For more information concerning Windows PowerShell integration with VMM 2008, see the sidebar titled “Direct from the Source: Windows PowerShell Integration in VMM 2008” in this chapter.

Direct from the Source: Windows PowerShell Integration in VMM 2008

Most user actions performed using the Client Layer applications result in the creation of a Windows PowerShell script that specifies the tasks that will be performed by the Engine Layer of VMM 2008. Windows PowerShell is not included with VMM 2008, but it is an integral component and is installed by default when VMM 2008 is installed, as a Windows Server 2008 feature.

Windows PowerShell is a Windows command-line shell that provides an interactive command prompt and scripting environment built on the .NET Framework. Windows PowerShell introduces the concept of a cmdlet (pronounced “command-let”), a simple, single-function command-line tool built into the shell. Windows PowerShell includes more than 100 core cmdlets that can be used alone or in conjunction with one another to perform complex tasks.

Windows PowerShell is also extensible in that additional cmdlets can be created and loaded as a snap-in dynamic-link library (DLL). Windows PowerShell is extended to include VMM 2008 cmdlets using the Microsoft.SystemCenter.VirtualMachineManager.dll snap-in DLL, located in the following folder:

%ProgramFiles%\System Center Virtual Machine Manager 2008\Bin

Launching the Windows PowerShell Virtual Machine Manager Command-Line Interface

The VMM 2008 Windows PowerShell snap-in DLL is loaded when you start Windows PowerShell using the Windows PowerShell Virtual Machine Manager shortcut on the Start menu or when clicking the Windows PowerShell button in the VMM Administrator Console. The Start menu shortcut uses the following command to start Windows PowerShell and load the snap-in DLL:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  
-PSConsoleFile "C:\Program Files\Microsoft System Center Virtual Machine  
Manager 2008\bin\cli.psc1" -NoExit
```

The command starts Windows PowerShell and specifies the console file cli.psc1. The cli.psc1 Windows PowerShell console file is an XML file containing the following elements, including the reference to Microsoft.SystemCenter.VirtualMachineManager.dll:

```
<?xml version="1.0" encoding="utf-8"?>
<PSConsoleFile ConsoleSchemaVersion="1.0">
  <PSVersion>1.0</PSVersion>
  <PSSnapIns>
    <PSSnapIn Name="Microsoft.SystemCenter.VirtualMachineManager" />
  </PSSnapIns>
</PSConsoleFile>
```

Note that the Microsoft.SystemCenter.VirtualMachineManager.dll snap-in is *not* loaded in Windows PowerShell if Windows PowerShell is started using its default Start menu shortcut launched by Start\Programs\Windows PowerShell 1.0\Windows PowerShell.

Configuring Windows PowerShell for Use with VMM 2008

The following four items are needed to configure Windows PowerShell for use with VMM 2008:

- An application-specific profile
- An application-specific snap-in
- A security context with sufficient permissions to run custom scripts
- An application context

The application-specific profile and application-specific snap-in are configured when the cli.psc1 Windows PowerShell console file is loaded. The security context must be set by the user.

Windows PowerShell operates using one of the following security contexts:

- **Restricted** This is the default PowerShell execution policy. When this policy is in effect, script execution is disabled; however, Windows PowerShell can still be used as an interactive command interpreter.
- **AllSigned** Specifies that only Authenticode-signed scripts can be executed. When running a signed script, users are asked if they want to trust the signer of the script.
- **RemoteSigned** Specifies that all scripts that are downloaded from a remote location must be Authenticode-signed before they can be executed.
- **Unrestricted** Windows PowerShell will execute any script. It will still prompt the user when it encounters a script that has been downloaded from a remote location. This is the least-secure setting.

Two Windows PowerShell cmdlets, Get-ExecutionPolicy and Set-ExecutionPolicy, can be used to view and change the current execution policy. To set the execution policy,

open a Windows PowerShell console with administrative rights and type the following command:

set-executionpolicy <executionpolicy>

where <executionpolicy> is either Restricted, AllSigned, RemoteSigned, or Unrestricted.

The current execution policy can also be viewed by typing the following command:

get-executionpolicy

The application context sets the specific VMM Server to which all subsequent commands apply. By default, no application (server) context, even the local machine that is running Windows PowerShell, is assumed. Before executing VMM Windows PowerShell commands, the application context must be set. *Application context* refers to the specific instance of the VMM Server against which the requested script is to be run. To set the application context, type the following command:

get-VMMServer –ComputerName <FQDN computer name>

Note that configuring these Windows PowerShell settings is not needed when tasks are executed using the VMM Administrative Console user interface. This is because these tasks are executed internally within the VMM engine without using Powershell.exe.

—CSS Global Technical Readiness (GTR) team

VMM Administrator Console The VMM Administrator Console provides a central location for administering virtual machines and virtual machine hosts throughout an enterprise. The Administrator Console does this by creating and executing jobs, which are collections of tasks that perform virtual machine-related tasks, such as

- Creating and deploying virtual machines
- Converting physical machines to virtual machines (P2V)
- Converting from one type of virtual machine to another type, such as converting a VMware virtual machine to a Hyper-V virtual machine (V2V)
- Managing virtual machines running on local or remote virtual machine hosts
- Refreshing the VMM Administrator Console display
- Creating and managing virtual machine templates
- Managing the library resources needed to build virtual machines
- Delegating management tasks through Role-Based Authorization profiles and the Self-Service Portal user roles

The main executable for the Administrator Console is Vmmadmin.exe, which is found in the following directory:

%ProgramFiles%\System Center Virtual Machine Manager 2008\Bin

Vmmadmin.exe loads the Virtual Machine Remote Control ActiveX Control (Vmractivexclient.dll), which provides functionality for viewing (but not interacting with) virtual machines within the Administrator Console.

The Administrator Console also includes the Virtual Machine Viewer process (Virtualmachineviewer.exe), which provides remote access to virtual machines running on Hyper-V-based managed hosts. Virtualmachineviewer.exe is located in the following directory:

%ProgramFiles%\Microsoft System Center Virtual Machine Manager 2008\Bin

Virtualmachineviewer.exe is automatically started by Vmmadmin.exe when a connection is made from the Administrator Console to a Hyper-V-based virtual machine. Virtualmachineviewer.exe uses the Terminal Services ActiveX control, Mstscax.dll, to make a Remote Desktop Protocol (RDP) connection to the remote connection port specified when the host was added to the Administrator Console as a managed host. By default, TCP port 2179 is used for the RDP communication to Hyper-V-based hosts because this is the default port that the Hyper-V Virtual Machine Management Service (VMMS) listens on for incoming management connections.

Virtualmachineviewer.exe can also be launched separately from outside the Administrator Console interface by using a command prompt as follows:

virtualmachineviewer.exe /host *host* /computername *compname* [/port *portnumber*] [/vmid *vmid*] [/vmname *name*] [/vgsinstalled *true* | *false*]

Table 3-3 lists the various Virtualmachineviewer.exe command-line options.

TABLE 3-3 Command-Line Options for Virtualmachineviewer.exe

Option	Description
/host	The name of the host to connect to. When a host is provided, the connection feed is routed through the host so that the virtual machine is visible even when rebooting or disconnected from the network. This option cannot be used with the <i>computername</i> parameter.
/computername	The machine name of the the virtual machine to connect directly to through remote desktop. This option cannot be used with the <i>host</i> parameter.
/port	Sets the port on which to communicate with the host. This option is ignored unless used with the <i>host</i> parameter. By default, this is set to 2179.

Option	Description
/vmid	The ID of the virtual machine to connect to. This must be provided to connect to the virtual machine when the <i>host</i> parameter is specified.
/vmname	A display name for the virtual machine used in the title bar of the viewer. This is required when the <i>host</i> parameter is specified.
/vgsinstalled	A Boolean value of true or false that indicates whether the Virtual Guest Services are installed on the virtual machine. By default, this is set to false.

Vmmadmin.exe also starts the Virtual Machine Remote Control process (Vmrc.exe) when a connection is made from the Administrator Console to a Virtual Server 2005 SP1–based virtual machine. Vmrc.exe provides remote access to virtual machines running on Virtual Server 2005 SP1–based managed hosts and is found in the following folder:

%ProgramFiles%\Microsoft System Center Virtual Machine Manager 2008\Bin

Vmrc.exe uses a modified Virtual Network Computing (VNC) protocol to communicate with Virtual Server 2005 SP1–based virtual machines using the remote connection port that was specified when the host was added to SCVMM as a managed host. Vmrc.exe can also be launched directly from outside the Administrator Console by using a command prompt as follows:

vmrc.exe [-fullscreen] [-viewonly] [-reducecolors] [vmrc server URL]

Table 3-4 lists the various Vmrc.exe command-line options.

TABLE 3-4 Command-Line Options for VMRC.exe

Option	Description
-fullscreen	Opens the VMRC console in full-screen mode
-viewonly	Disables mouse and keyboard input
-reducecolors	Enables reduced colors mode to increase performance
vmrc server URL	URL to a virtual server

Vmmadmin.exe also starts the VMware viewer process (Vmwareviewer.exe) when a VMware-based virtual machine is selected in the Administrator Console. Vmwareviewer.exe provides the initial connection to virtual machines running on VMware ESX Server–based managed hosts and loads the VMware WebCenter Remote MKS Plug-in control to enable communication with the VMware VirtualCenter Server console.

VMM Self-Service Portal The VMM Self-Service Portal is a Web-based ASP.NET application that provides an interface to allow designated users to perform specific virtual machine management tasks on managed hosts. The options that are available to Self-Service Portal users depend on the rights assigned to them by an administrator when their specific user role is created.

The Self-Service Portal can be installed on Internet Information Services (IIS) 6.0 on Windows Server 2003 or on IIS 7.0 on Windows Server 2008. During installation, you specify which port will be used for the Self-Service Portal. By default, port 80 is used unless another Web site, such as the Default Web Site, is already using port 80.

The Self-Service Portal is accessed by using Internet Explorer and requires the installation of ActiveX controls to provide remote access to virtual machines on managed hosts. When a user uses the Self-Service Portal to view or connect to any of her virtual machines, she is prompted to install the appropriate ActiveX control in Internet Explorer on her local machine.

Direct from the Source: System Center Operations Manager and VMM 2008

System Center Operations Manager (OpsMgr), formerly Microsoft Operations Manager (MOM), is a performance-monitoring and event-monitoring application that can be used to monitor the health of an enterprise's IT infrastructure, including devices, operating systems, and applications. An OpsMgr agent is installed on monitored computers to monitor objects based on a predefined health model. The agents monitor several sources for events or other alerts and forward the information to a central OpsMgr server that maintains a database that includes a history of alerts. The OpsMgr server applies filtering rules to alerts as they arrive and takes appropriate action if needed. A filtering rule can trigger a notification, such as an e-mail or a pager message; generate a network support ticket; or trigger some other workflow intended to correct the cause of the alert.

OpsMgr uses the term *management pack* to refer to a set of filtering rules that are specific to a monitored application. Management packs are available for VMM 2008 as well as several other Microsoft products, such as SQL Server and Exchange Server. OpsMgr also provides facilities for authoring custom management packs. Although an administrator role is needed to install agents, configure monitored computers, and create or install management packs, rights to monitor alerts can be given to any valid user account.

OpsMgr agents can be installed on the VMM Server, Windows-based virtualization hosts, and Windows-based virtual machines, including Windows-based virtual machines running on VMware ESX Server. OpsMgr communicates with the agents using the WCF over TCP port 5723.

OpsMgr integration with VMware is agentless and is accomplished using third-party management packs, such as nWorks, communicating directly with the VMware Web service using public VMware APIs. Users also get limited OpsMgr integration from VMM itself.

OpsMgr Integration with VMM 2008

VMM 2008 increases integration with System Center Operations Manager 2007 by introducing support for Performance and Resource Optimization (PRO). PRO relies on OpsMgr to monitor and collect performance data from hosts and virtual machines within an environment. It is designed to make recommendations or take actions that take advantage of the capabilities provided by a virtualized environment. PRO collects performance and configuration data, which is used to generate tips to help users place, migrate, or reconfigure virtual machines to ensure workload uptime. PRO tips can be managed from the VMM Windows PowerShell console or from the VMM Administrator Console.

PRO leverages Intelligent Placement to help determine the best location for any VMs that are migrated as a result of tips that are generated. PRO provides workload-aware and application-aware resource optimization within host clusters that are managed jointly by VMM 2008 and OpsMgr. PRO is designed to help you evaluate whether physical resources provided by clustered host servers to the virtual machines deployed on those hosts are used efficiently.

PRO tips suggest how to remedy the issues raised in the alerts generated by OpsMgr. For example, a PRO tip might recommend increasing performance for a virtual machine by moving it to a new host with more resources or by adding an additional CPU to the virtual machine itself.

Capabilities of PRO

PRO in VMM 2008 has the following capabilities:

- **Intelligent Placement** Provides intelligent placement of multemachine configurations across multiple hosts.
- **Clustering** PRO works in a clustered environment.
- **Health-based decisions** PRO uses health to determine when remediation is necessary.
- **In-Guest aware** PRO uses data collected from within the guest to suggest remediation.
- **Virtual machine right-sizing** PRO can make recommendations to alter the configuration of VMs to improve performance.
- **Host-level load balancing** PRO can provide a solution that ensures that the host load is balanced.
- **Automatic Remediation** PRO can be set up to automatically implement suggested remediation.

As noted in the preceding text, you can configure VMM 2008 to take corrective action automatically based on PRO tips or you can choose to respond to PRO tips manually.

The following paragraphs describe what happens if you specify that VMM 2008 will implement PRO tips automatically.

For Hyper-V hosts configured in a host cluster, VMM 2008 can monitor and report at both the guest and host level and can use the Hyper-V Quick Migration feature to move virtual machines transparently between nodes in the cluster.

For VMware hosts configured in a host cluster, VMM 2008 can also monitor and report at both the guest and host level and can use the VMware Live Migration feature (VMotion) to move virtual machines transparently between nodes in the cluster.

PRO Windows PowerShell Cmdlets

The following new or updated Windows PowerShell cmdlets are provided for PRO in VMM 2008:

- Get-PROTip
- Dismiss-PROTip
- Set-PROTip
- Invoke-PROTip
- Set-VMHostCluster

The Set-VMMServer SCVMM cmdlet now also supports parameters to enable PRO support in VMM 2008.

—CSS Global Technical Readiness (GTR) team

Engine Layer

The VMM 2008 Engine Layer performs the tasks communicated to it by the Client Layer applications. The Engine Layer also controls the resources used by the Managed Computer Layer components. The 2008 Engine Layer is comprised of the following:

- Virtual Machine Management Service
- Microsoft SQL Server
- Other components

Virtual Machine Management Service The Virtual Machine Management Service (VmmService) is a system service implemented in VmmService.exe that provides the WinRM, WMI, HTTP, and WCF interfaces used for communication with the Client Layer applications and the Managed Computer Layer components. The Virtual Machine Management Service is also responsible for executing the individual tasks that make up a job. The Virtual Machine Management Service is dependent on the SQL Server (Microsoft\$VMM\$) system service.

SQL Server VMM 2008 employs a Microsoft SQL Server database to maintain the database used to store library resource objects and certain configuration options, such as the VMware port number to use for communication with a VMware VirtualCenter Server. The version of SQL Server that you use with VMM depends on the needs of your environment. For example, if there is no previously installed version of SQL Server in your environment, installing VMM 2008 will install Microsoft SQL Server Express edition. If you don't plan on using the PRO functionality of VMM 2008, SQL Server Express can provide the database functionality needed by VMM. Using the PRO feature of VMM 2008, however, requires using OpsMgr, which requires the full 64-bit version of SQL Server.



Note The structure of the database and the manner in which VMM 2008 interacts with the database is the same regardless of which version of SQL Server you are using.

VMM 2008 employs ADO.NET to communicate with SQL Server. ADO.NET is a .NET Framework-based data-access technology that enables applications to connect to data stores and manipulate the data contained in them. ADO.NET implements a disconnected database access model whereby a connection to the database is opened to serve an application request and is then closed after the request has been completed. This mechanism conserves system resources, has less impact on system performance, and enhances the security of databases. ADO.NET employs XML when interacting with a database and converts all of the data into XML format for database-related operations.



Note If a remote SQL Server database is used, TCP port 1433 must be open for the communication.

Other Engine Layer Components Some of the additional components within the Engine Layer of VMM 2008 include

- Authorization Manager
- A backup and restore engine
- Virtual Disk Service Providers

Managed Computer Layer

The Managed Computer Layer consists of the various types of virtualization hosts that VMM 2008 manages, including the Library Server and P2V Source servers. The Library Server maintains two kinds of resources:

- Resources not currently in use, such as library resources and P2V Source servers

- In-use resources, such as Hyper-V hosts, Virtual Server 2005 R2 SP1 hosts, VMware ESX hosts, and V2V Source hosts

VMM Agents With the exception of VMware-based hosts, communication between VMM 2008 and the hosts it manages is accomplished using an agent service installed on the hosts. There are two types of VMM Agents:

- Host agent
- P2V agent

A host agent is automatically installed on a managed host when the host is added to VMM as a managed entity. The host agent is implemented as the VMMAgent service (Vmmagent.exe) and is used for managing Hyper-V and Virtual Server hosts. In addition to installing the VMMAgent service on remote managed hosts, the VMMAgent service is also installed by default on the VMM Server because it is needed for managing the library that is created on the server. The VMMAgent service depends on the Background Intelligent Transfer Service (BITS), Windows Management Instrumentation (WMI), and Windows Remote Management (WinRM) services.

A P2V agent is installed during a P2V conversion and is implemented using Vmmp2vagent.exe.

Library Servers and Resources The VMM library is a collection of resources that can be used to create and configure virtual machines. Library resources include the following:

- Virtual Hard Drive (.vhd) and Virtual Machine Configuration (.vmc) files
- Virtual machine templates and guest operating system profiles
- Scripts and Sysprep answer files
- ISO image files
- Virtual floppy disks

The VMM Library Server is a file server that has one or more shares. A VMM Agent runs on the Library Server to enable communication with a VMM Server and to identify the Library Server to the VMM Server as a Library Server. Only one VMM Agent can run on each Library Server, which means that a Library Server can connect only to one VMM Server. A VMM Server can connect to more than one Library Server, however.

Library Servers basically have two functions:

- To store the objects that can be used to create and configure virtual machines
- To transfer these objects to the hosts where they will be instantiated as running virtual machines



Tip Because the images that are stored in the library can be very large, a significant amount of network traffic can occur when these images are transferred to a virtual machine host during the virtual machine creation process. You should therefore locate your Library Servers on the same subnet as the hosts that they will be servicing.

The VMM library is more than just a collection of files in a share folder. Instead, library resources are organized into groups of objects that exist physically in the library share along with other objects that exist only within the SQL database. An example of a type of library object that does not exist physically in the library share but is still tracked as a library object is virtual machines, which run on managed hosts while being catalogued in the SQL database as part of the library infrastructure.

Working with VMM 2008

System Center Virtual Machine Manager 2008 is a powerful and flexible platform for managing different virtualized resources, including Hyper-V, Virtual Server, and VMware ESX Server virtual machines. This section examines how to install and use VMM 2008 and covers the following topics:

- System and Infrastructure Requirements
- Installing VMM 2008
- Using the VMM Administrator Console
- Working with Managed Hosts
- Working with the Library
- Working with Virtual Machines
- Performing P2V Conversions
- Performing V2V Conversions
- Configuring User Roles
- Using the Self-Service Portal

System and Infrastructure Requirements

Before you deploy VMM 2008 in your production environment, you need to ensure that all prerequisites have been met. The prerequisites for installing VMM 2008 include

- Hardware requirements
- Software requirements
- Infrastructure requirements

Hardware Requirements

The hardware requirements for installing VMM 2008 depend on the number of hosts with virtualized workloads that you plan on managing with your VMM server. If you plan on managing fewer than 150 hosts with your VMM server, you can deploy VMM 2008 in a configuration where your VMM server is also your Library Server. In this scenario, the recommended hardware for your VMM server is as follows:

- A dual-processor or dual-core x64 system running at 3.2 GHz or higher
- At least 4 GB of RAM
- At least 160 GB of hard disk space with 120 GB allocated for the library server

In an environment where your VMM server will be managing more than 150 hosts, it's a good idea to not use the default library share on your VMM server but instead add one or more additional Library Servers. In this scenario, the recommended hardware for your VMM server is as follows:

- A dual-processor or dual-core x64 system running at 3.6 GHz or higher
- At least 8 GB of RAM
- At least 40 GB of hard disk space

Software Requirements

You must install VMM 2008 on an x64 edition of Windows Server 2008. Before you install the VMM server or any other VMM 2008 components, you must do the following to prepare your server:

- Install the Web Server (IIS) role (including the IIS 6 Metabase Compatibility and IIS 6 WMI Compatibility components) using the Add Roles Wizard.
- Add the .NET Framework 3.0 Features feature using the Add Features Wizard.
- Add the Windows PowerShell feature using the Add Features Wizard.

If you plan on using the same server for both your VMM Server and database server, you must also install either of the following:

- Microsoft SQL Server 2005 Express Edition (for scenarios where your VMM server will be managing fewer than 150 hosts)
- A full edition of Microsoft SQL Server 2005 (for scenarios where your VMM server will be managing more than 150 hosts)



Tip For the best performance, especially when your VMM server will be managing a large number of hosts, you should use a separate server for your VMM database.

Some VMM 2008 components can be installed on other servers running operating systems other than Windows Server 2008 (x64). In addition, running all VMM 2008 components on a single server, although not highly recommended, is supported only on Windows Server 2008 with Hyper-V 64-bit, Standard, Enterprise, and Datacenter Editions.

Table 3-5 lists the supported operating systems for installing the VMM Server components and Windows-based virtual machine hosts.

TABLE 3-5 Supported Operating Systems for Installing the VMM Server Components and Windows-Based Virtual Machine Hosts

Operating System	VMM Server	Hyper-V Hosts	Virtual Server Hosts
Windows Server 2008 with Hyper-V 64-bit, Standard, Enterprise, and Datacenter Editions	Yes	Yes	Yes
Windows Server 2008 without Hyper-V 64-bit, Standard, Enterprise, and Datacenter Editions	Yes	No	Yes
Windows Server 2008 without Hyper-V 32-bit, Standard, Enterprise, and Datacenter Editions	No	No	Yes
Windows Server 2008 — Server Core installation, Standard, Enterprise, and Datacenter Editions	No	Yes	No
Windows Server 2003 with Service Pack 2, Standard, Enterprise, and Datacenter Editions	No	No	Yes
Windows Server 2003 R2 with Service Pack 2	No	No	Yes
Windows Server 2003 x64 with Service Pack 2	No	No	Yes
Windows Server 2003 R2 x64 with Service Pack 2	No	No	Yes

Table 3-6 lists the supported operating systems for the VMM Administrator Console, Self-Service Portal, and Library Server components.

TABLE 3-6 Supported Operating Systems for the VMM Administrator Console, Self-Service Portal, and Library Server Components

Operating System	VMM Administrator Console	VMM Self-Service Portal	VMM Library Server
Windows Server 2008 with Hyper-V 64-bit, Standard, Enterprise, and Datacenter Editions	Yes	Yes	Yes

Operating System	VMM Administrator Console	VMM Self-Service Portal	VMM Library Server
Windows Server 2008 without Hyper-V 64-bit, Standard, Enterprise, and Datacenter Editions	Yes	Yes	Yes
Windows Server 2008 without Hyper-V 32-bit, Standard, Enterprise, and Datacenter Editions	Yes	Yes	Yes
Windows Server 2008 - Server Core installation, Standard, Enterprise, and Datacenter Editions	No	Yes	Yes
Windows Web Server 2008	No	Yes	No
Windows Server 2003 with Service Pack 2, Standard, Enterprise, and Datacenter Editions	Yes	Yes	Yes
Windows Server 2003 R2 with Service Pack 2	Yes	Yes	Yes
Windows Server 2003 x64 with Service Pack 2	Yes	Yes	Yes
Windows Server 2003 R2 x64 with Service Pack 2	Yes	Yes	Yes
Windows Vista with Service Pack 1	Yes	No	No
Windows XP Professional with Service Pack 2 or Service Pack 3	Yes	No	No
Windows XP Professional x64 with Service Pack 2	Yes	No	No

Infrastructure Requirements

VMM 2008 must be deployed within an Active Directory Domain Services environment. Specifically, the server or servers on which you will be installing the VMM 2008 components must be joined to a domain. In addition, any hosts that your VMM server will manage must also be a domain member, either of the same domain where your VMM server resides or in a trusted domain.

Although a Fast Ethernet (100 Mbps) network infrastructure is usually sufficient connectivity for the servers in your VMM 2008 deployment, using Gigabit Ethernet (1000 Mbps) can lead to improved performance.

Installing VMM 2008

After you've verified that your environment meets the system and infrastructure requirements for deploying VMM 2008, you can begin the installation process.

Using the Virtual Machine Manager Configuration Analyzer

The first step of the installation process involves running the Virtual Machine Manager Configuration Analyzer (VMMCA), a diagnostic tool that verifies the configuration settings for computers to verify that they can run VMM 2008. Using the VMMCA, you can scan your computers to verify whether they are suitable to function as a VMM Server, run the Administrator Console, function as a Self-Service Portal, or be a managed virtual machine host.

After you've run the VMMCA and verified that your computers will support running VMM 2008, you're ready to begin installing the various components of the product. As mentioned earlier, these different components can be installed either on a single server or on multiple servers on your network.

Installing the VMM Server

The first component you should install should be the VMM Server. When you install this component, the domain account you are currently logged in with is automatically added to the VMM Administrator user role. You can add other user accounts to the VMM Administrator user role afterwards—see the “Managing User Roles” topic in VMM Help for information on how to do this.

When you install the VMM Server component, you are prompted to configure SQL Server settings. You can do this either by installing SQL Server 2005 Express Edition SP2 locally on your VMM Server or by specifying an existing remote instance of SQL Server 2005.

During installation of the VMM Server, you are also prompted to create a new library share on your server or specify a preconfigured share on another server. The VMM library serves as a central, secure store for the resources used to create virtual machines in your VMM 2008 environment and helps enable the re-use of approved images and configurations. The library share is created as part of the VMM Server Setup process. The default is to create a share on the VMM Server on the system drive at %SystemRoot%\ProgramData\Virtual Machine Manager Library Files using a share name of MSSCVMMLibrary. Additional Library Servers and shares can then be added afterwards by using the VMM Administration console.

A best practice is to make the Library Server by using a highly available file server running on a Windows Server 2008 Failover cluster. If a Failover cluster is not available, locate the share on a nonsystem, high-speed (minimum 10,000 rpm) hard disk drive for best performance.

Make your selection carefully because you cannot remove or relocate the default Library Server or its library share after installing your VMM Server.

Installing the VMM Administrator Console

After you finish installing your VMM Server, install the VMM Administrator Console on the local server. Installing the Administrator Console also installs the Windows PowerShell Virtual Machine Manager console on the computer.


You might also want to install the Administrator Console on additional computers later to remotely access and manage your VMM Server, but it's helpful to install this console locally on your VMM Server in case you need it for troubleshooting purposes. In addition, if you plan on using the reporting feature of VMM 2008, you must install the Administrator Console on the same computer as the VMM Server component. This is because the reporting feature of VMM 2008 relies on System Center Operations Manager 2007 (OpsMgr), and it relies on OpsMgr administrators to perform tasks on hosts and virtual machines from within the Server Virtualization Management Pack, which requires that the Windows PowerShell Virtual Machine Manager console be installed on the VMM Server.

Installing the VMM Self-Service Portal

An optional deployment step is to install the VMM Self-Service Portal, a Web-based component that lets users create and manage their own virtual machines within a controlled environment. If you choose to install the Self-Service Portal, you should install it on a separate computer from your VMM server for best performance. Note that installation of the Self-Service Portal on a domain controller is not supported.

Direct from the Source: Upgrading from VMM 2007 to VMM 2008

The following steps document the process for upgrading from an VMM 2007 environment to VMM 2008.



Caution To avoid any loss of important data, before you upgrade VMM, it is highly recommended that you perform a full backup on your VMM database. Do not use the VMM database backup function to perform this backup, because you will not be able to restore this backup by using the new version of VMM. Use SQL Server Management Studio to back up your VMM database. For more information about backing up your SQL Server database, see SQL Server Management Studio at <http://msdn.microsoft.com/en-us/library/ms187510.aspx>.

When you update VMM, you lose the passwords and product keys for the following objects:

- Standalone templates
- Operating system profiles
- Hardware profiles
- Jobs table

When you update VMM, you maintain the following data and objects:

- Self-Service information
- Custom fields for virtual machines and hosts

To Upgrade from VMM 2007

1. Use SQL Server Management Studio to create a copy of the VMM 2007 database, and then, on the computer that will host the VMM 2008 database, restore the copy of the VMM 2007 database.
2. Identify a computer that is separate from your current VMM installation and that meets the minimum system requirements for installing the VMM server for VMM 2008.
3. Install the VMM server for VMM 2008 and, on the SQL Server Settings page of the wizard, specify the restored copy of the VMM 2007 database. Note that specifying the restored copy of the VMM 2007 database automatically upgrades it to a VMM 2008 database. In addition, if you are using a remote instance of SQL Server for the VMM database, for important configuration information, you must also configure a remote instance of SQL Server for VMM.
4. Follow the instructions for installing the VMM Administrator Console, and then connect it to the new VMM server.
5. In the VMM Administrator Console, in Administration view, click Managed Computers. All hosts that are being managed by VMM 2007 will appear in the results pane with an agent communication status of Access Denied.
6. In the results pane, do one of the following:
 - ❑ Select one or more hosts with an agent communication status of Access Denied, and then click Reassociate. The hosts will have an agent version status of Unsupported.



- ❑ Select one or more hosts with an agent version status of Unsupported, and then click Update Agent. The hosts will have an agent communication status of Responding and an agent version status of Up-to-date. This indicates that the upgrade for the agents on the hosts is complete.
- ❑ Repeat the preceding steps until all hosts have been updated.

Note So that performance is not adversely affected, it is recommended that you update hosts in batches of 10 to 25, first associating the hosts with the VMM 2008 server and then updating the agents on the hosts, until all the hosts have been updated to VMM 2008.

7. In the results pane, do the following:

- ❑ Select one or more computers that have a role of Library and an agent communication status of Access Denied, and then, in the Actions pane, click Reassociate. The Library Servers will have an agent version status of Unsupported.
- ❑ Select one or more computers that have a role of Library and an agent version status of Unsupported, and then click Update Agent. The Library Servers will have an agent communication status of Responding and an agent version status of Up-to-date. This indicates that the upgrade for the agents on the Library Servers is complete.

8. In the VMM Administrator Console, in the Hosts view, select hosts with a status of Needs Attention and then click Refresh. Hosts that have the Virtual Server 2005 R2 SP1 update (KB948515) installed have a host status of OK. This indicates that the upgrade for the hosts is complete. Download the Virtual Server 2005 R2 SP1 update at <http://go.microsoft.com/fwlink/?LinkID=120488>. Hosts that do not have the Virtual Server 2005 R2 SP1 (KB948515) update installed will still have a host status of Needs Attention and the Update Virtual Server action will now be enabled.

9. Select one or more hosts with a status of Needs Attention, and then in the Actions pane, click Update Virtual Server. The host will have a host status of OK. This indicates the upgrade for the hosts is complete.

—CSS Global Technical Readiness (GTR) team

Using the VMM Administrator Console

The VMM Administrator Console can be used to manage all aspects of a virtualized environment including virtual machines on managed hosts running Microsoft Hyper-V, Microsoft Virtual Server 2005 R2, and VMware ESX Server within a VMware Infrastructure 3 (VI3) or newer environment. As mentioned previously, the Administrator Console can be installed both locally on your VMM Server and also on additional computers in your environment for remote management purposes. By default, any user account that has local administrator privileges on your VMM Server can use the Administrator Console.

Figure 3-2 shows the basic layout of the Administrator Console with its various panes, task-bar, filters, and view buttons. Each view in the Administrator Console has its own navigation pane, results pane, details pane, filters, and actions for performing various tasks.

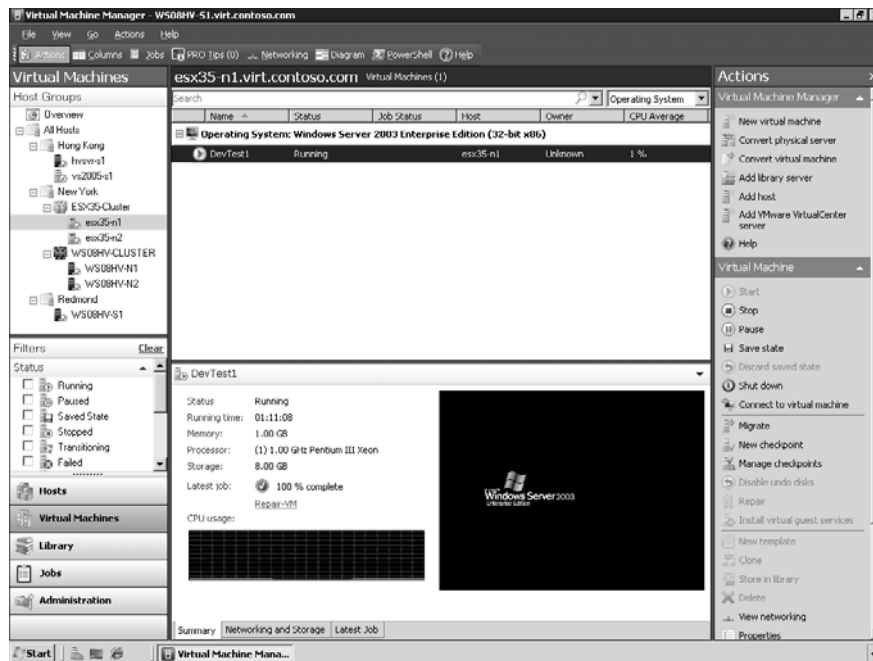


FIGURE 3-2 The layout of the VMM Administrator Console.

When you launch the Administrator Console on the local VMM Server, it connects to the local server and displays different information depending on the view selected. You can use the Administrator Console to connect to other VMM Servers within your organization by selecting Open New Connection from the File menu. The default port for connecting to remote VMM Servers is port 8100.

Understanding Views

Depending on how you have deployed VMM 2008, the Administrator Console can show up to seven possible views: Hosts, Virtual Machines, Library, Jobs, Administration, Reporting, and Diagram. It is possible that not all views are available for your installation. For example, the Reporting and Diagram views are not available unless VMM 2008 has been configured to work with System Center Operations Manager 2007.

The sections that follow list the seven views available in the Administrator Console and describe the different administrative tasks you can perform using each view. Additional information about using some of these views can be found in the sections that follow.

■ 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.

■ Library view:

- ❑ Add file-based resources to the Virtual Machine Manager library 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 every 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.

- Administration view:
 - ❑ Overview—View graphical summary information of the environment (hosts, virtual machines, recent jobs, and library resources).
 - ❑ General—Configure global VMM settings, such as 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, such as Virtual Machine Manager and VMware VirtualCenter Server.
- Reporting view:
 - ❑ View and open reports. Reporting view is available only if you have configured Operations Manager.
- Diagram view:
 - ❑ Displays the health of the Virtual Machine Manager Server, database server, Library Servers, hosts, virtual machines, and VMware VirtualCenter Server servers. Diagram view is available only if you have configured Operations Manager.



Note In addition to the seven views just described, there is also a special Networking view that can be used to display a graphical representation of the current network configuration. The Networking view does not have a view button and is invoked differently than the other views. See the section titled “Using Networking View” later in this chapter for more information.

Using Filters

The information displayed in each view can be filtered by using the Filters section of the Administrator Console. The type of filtering you can perform depends on which view is currently selected. For example, Figure 3-3 shows the Virtual Machines view selected, and the Filters section of the console can be used to filter virtual machines based on whether they are running, stopped, paused, saved, or in some other state.

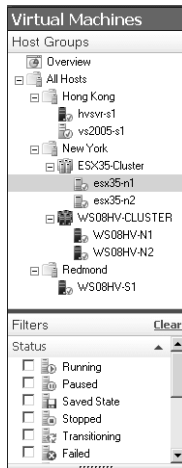


FIGURE 3-3 The filters available in the Virtual Machines view.

Working with Managed Hosts

You can use the Administrator Console to manage virtual machine hosts across a virtualization infrastructure. For example, you can create host groups to organize your hosts, add hosts to a host group, and configure and manage different kinds of hosts, including Hyper-V, Virtual Server, and VMware ESX hosts. The following sections provide further details concerning some of the tasks you can perform for managing hosts.

Creating and Using Host Groups

A *host group* is a logical container for organizing managed hosts within the Administrator Console. Creating host groups and adding hosts to them is a simple way of making it easier for you to manage hosts across your virtualization infrastructure.

You create and work with host groups within the Hosts view of the Administrator Console. By default, all managed hosts belong to the All Hosts group. When you create a new host group, the new group is added beneath the All Hosts group. You can also nest host groups to create three, four, or more levels of host groups if desired.

After you've created your hierarchical structure of host groups with the All Hosts group at the top, you can then add managed hosts and host clusters to each group as desired.

Figure 3-4 shows an example of how to use host groups to organize managed hosts according to geographical location. In this figure, three host groups—New York, Hong Kong, and Redmond—were created within the All Hosts group. Managed hosts and host clusters were then added to each host group as shown.

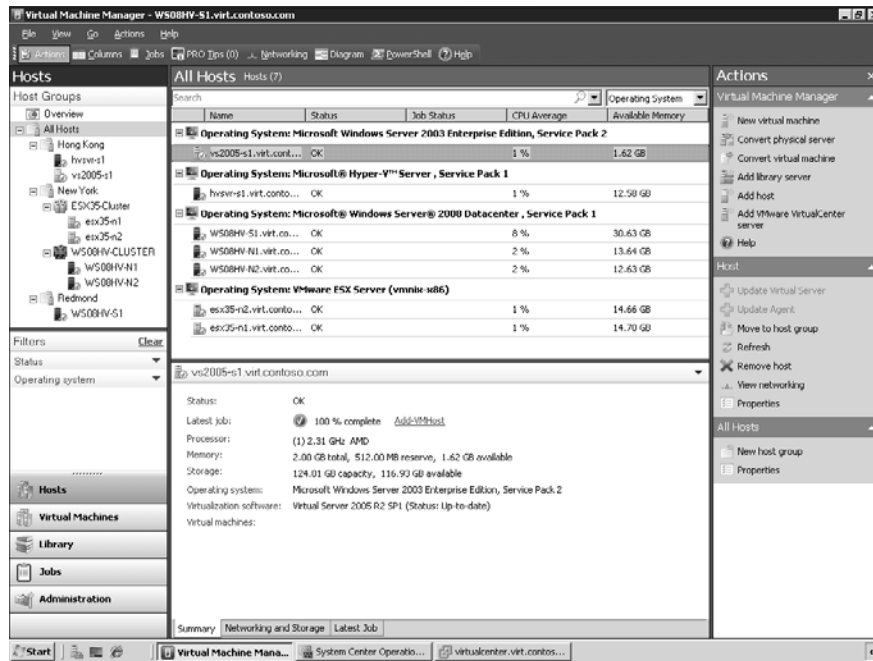


FIGURE 3-4 Working with host groups.

The Actions pane on the right side in Figure 3-4 has three sections: Virtual Machine Manager, Host, and All Hosts.

The Virtual Machine Manager section allows you to perform actions on the selected managed host in the top middle Results pane. In this figure, a managed host named vs2005-s1.virt.contoso.com is currently selected in the Results pane, and the status and other information concerning this virtual machine is displayed on the Summary tab in the bottom middle Details pane. The actions you can perform on this managed host include creating a new virtual machine, converting a physical server, converting a virtual machine, and other tasks. You can perform these actions either by clicking the appropriate link in the Actions pane or by right-clicking on a managed host in the Results pane and using the shortcut menu options.

The Hosts section of the Actions pane allows you to perform other actions on managed hosts, including moving the selected host to a different host group, removing a host from the console, displaying and configuring the properties of the host, and so on.

The All Hosts section of the Actions pane lets you create new host groups for organizing your managed hosts for easier administration. You can also use this section of the Actions pane to view and configure the properties of a host group. For example, you can configure the properties of a host group to specify how much reserved computing resources (percentage of CPU usage, MBs of memory, MBs of disk space, and so on) you want to allocate to the host.

You would do this to ensure that the host does not become starved for resources by running too many virtual machines on it.

Adding a Managed Host You add managed hosts to a host group by using the Add Hosts Wizard. This wizard can be used to add hosts belonging to an Active Directory domain or residing on a perimeter network. You can also add VMware ESX Servers to host groups as managed hosts provided these servers are managed by VMware VirtualCenter Server. You can also add managed hosts that are part of a managed host cluster. If you try and add a host that belongs to a cluster, all the nodes in the cluster are added as hosts.

Removing a Managed Host If you no longer want to manage a host with VMM 2008, you can remove the host using the Administrator Console. After you remove a host, it is no longer managed by VMM and the VMM Agent is automatically removed from the host. When you remove a host from VMM, the host and all of its associated virtual machines are removed from the VMM database and from the Administrator Console views. However, both the host and its virtual machines remain available and can be added as a host again to VMM if desired, or you can manage the host and its virtual machines outside of VMM using standard Hyper-V, Virtual Server, or VMware administrative tools.

To remove a managed host when the VMM Server can no longer communicate with that host or when you do not have the credentials for that host, use the Remove-VMHost Windows PowerShell cmdlet together with the *Force* parameter. When you specify the *Force* parameter, VMM does not prompt for or check credentials, and VMM does not attempt to connect to the host and uninstall the VMM agent. Using the *Force* parameter is recommended only when you need to remove stale host records from the VMM database.



Note If a single computer is serving as both a host and a library server and you remove the host role from the computer, the VMM Agent remains on the computer until the Library Server role is also removed.

Direct from the Source: Managed Host Agent Management

This sidebar deals with installing, reassociating, and updating managed host agents on managed hosts.

Installing the Agent Automatically

When you add a virtual machine host or Library Server, VMM 2008 remotely installs a VMM Agent on the managed computer. The VMM Agent deployment process uses both the Server Message Block (SMB) ports and the Remote Procedure Call (RPC) port (TCP 135) and the DCOM port range. You can use either SMB packet signing or IPSec to help secure the agent deployment process. You can also install VMM Agents locally on hosts, discover them in the VMM Administrator Console, and then control the host using only the WinRM port (default port 80) and BITS port (default port 443).

Installing the Agent Manually

To install the VMM Agent manually, log on to the intended host computer and run Setup.exe from your VMM 2008 product media. When the Setup splash screen is displayed, select Local Agent from under the Setup options.

Installing the Agent on Server Core

To manually install the VMM Agent on a Server Core installation of Windows Server 2008, navigate to the ..\Prerequisites\VCRedist\amd64 directory on your VMM 2008 product media and install the Visual C++ 2005 Redistributable Package by running Vcredist_x64.exe. After this finishes, navigate to the ..\amd64\msi\Agent directory and execute the following Msiexec.exe command line to install the VMM Agent:

msiexec /I vmmagent.msi

After the agent has been installed, the Add Host Wizard can be initiated on the VMM Server to add the host to a host group or to the library.

Reassociating an Agent

Occasionally, you might want to move one or more hosts from one VMM Server to another. For example, you might want to consolidate hosts that are being managed by two or more VMM Servers onto a single VMM Server.

Alternatively, you might want to move one or more hosts back to a VMM Server on which they had been previously managed but from which they have not yet been removed. In this situation, the hosts still appear in the Managed Computers pane of Administration view on the original VMM Server. However, because the agents on the hosts have been associated with a different VMM Server, the host status on the original VMM server is reported as Needs Attention in Hosts view and Access Denied in the Managed Computers pane in Administration view. Before you can manage the hosts again on the original VMM server, you must reassociate the hosts with the original VMM Server.

To associate a host with a VMM Server, select the Reassociate Host With This Virtual Machine Manager Server check box in the Add Hosts Wizard or choose the host from the Hosts view and select Reassociate from the Actions pane. Note that the Reassociate command is enabled only when the status of an agent is reported as Access Denied because it is no longer associated with the current VMM Server.

Updating an Agent

After upgrading VMM 2008 from its previous version, you must update the agents on all your managed hosts. For the agent update to work properly, the version of the agents on managed computers must match the version of the VMM Server. To update

a VMM Agent on a managed host, select either the Hosts view or the Administration view in Managed Computers, and select the managed hosts on which you want to update the agent. In the Actions pane, click Update Agent.

—CSS Global Technical Readiness (GTR) team

Managing Hosts

When you select a managed host in the Administrator Console and click Properties in the Actions pane, the properties dialog box for the managed host is displayed. You can use the different tabs to configure various aspects of the host. The sections that follow describe the different configuration options available for managed hosts.

Summary tab This tab provides descriptive information about the host, including some limited system information such as CPUs, memory, storage capacity, operating system, and other information. (See Figure 3-5.) The version of the installed VMM Agent is also displayed on this tab.

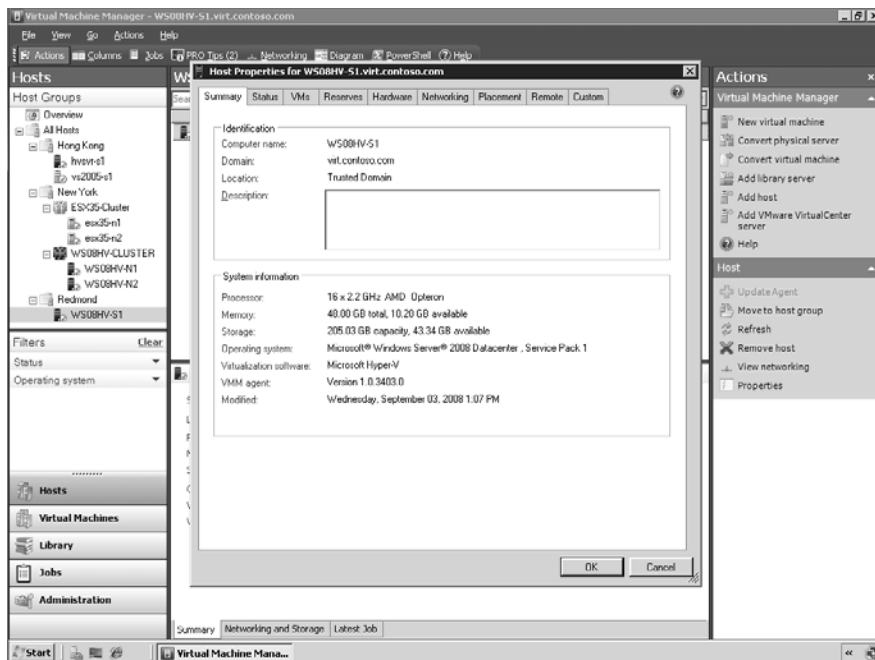


FIGURE 3-5 The Summary tab of the properties of a managed host.

Status tab This tab provides overall status information for the host, as well as specific information about certain configuration settings on the host. (See Figure 3-6.)

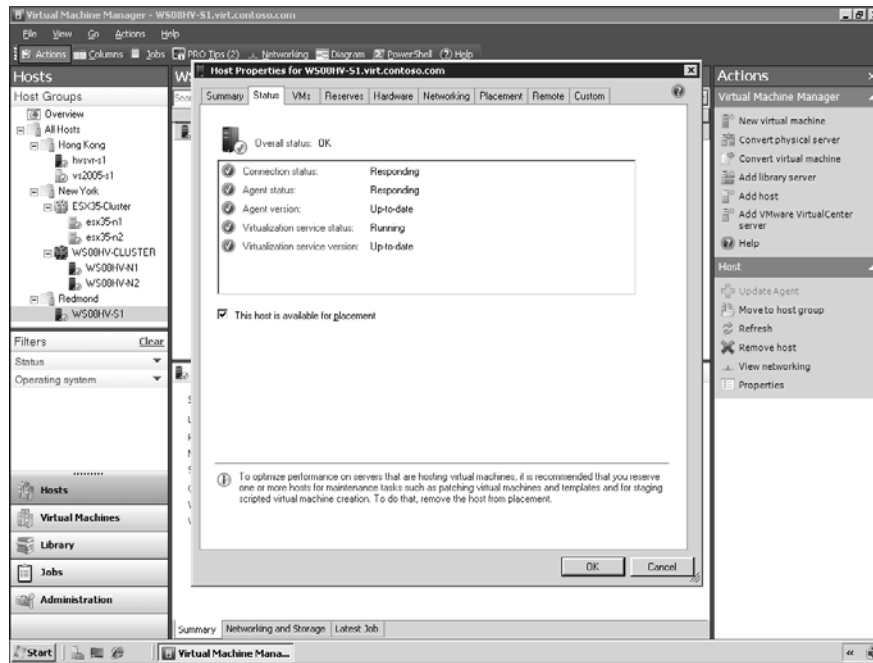


FIGURE 3-6 The Status tab of the properties of a managed host.

The types of status information and their possible values that the Status tab can display include the following:

- Overall status

- ❑ OK—No issues exist with any host status.
- ❑ OK (Limited)—The VMware ESX Server host requires credentials and other security configurations before it can be fully managed by VMM.
- ❑ Needs Attention—A problem exists with the status of one or more hosts.

- Connection status

- ❑ Responding—The VMM Server is able to communicate with the agent on the host.
- ❑ Not Responding—The VMM Server is unable to communicate with the agent on the host.
- ❑ Access Denied—The VMM Agent is no longer associated with the VMM Server.

- Agent version

- ❑ Up-to-date—The version of the VMM Agent is up to date.
- ❑ Upgrade Available—The version of the VMM Agent must be upgraded to match the version of VMM Server.

- ❑ Unsupported—The version of the VMM Agent is not supported for any VMM functions.
- Virtualization service status
 - ❑ Running—The virtualization service is started.
 - ❑ Stopped—The virtualization service is stopped.
- Virtualization service version
 - ❑ Up-to-date—The version of the virtualization software is up to date.
 - ❑ Upgrade Available—The version of the virtualization software must be upgraded to a version supported by VMM.
 - ❑ Unsupported—The version of the virtualization software is not supported for any VMM functions.

Additional status information will be displayed if the host belongs to a cluster. The host status values do not change in the Administrator Console until the VMM Server performs a host refresh, which by default runs automatically every 30 minutes. You can also perform a refresh on demand by right-clicking the host and clicking Refresh.

VMs This tab provides basic information concerning the virtual machines that are hosted on the selected managed host. In Figure 3-7, for example, there are five virtual machines on the host, and the selected virtual machine displays its status, up time, and virtual hardware resources on the tab.

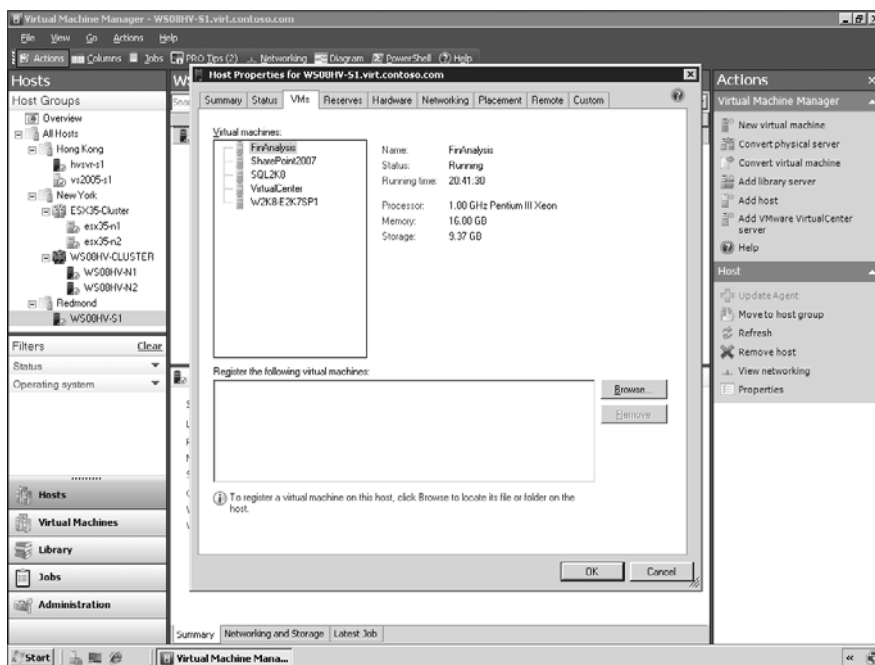


FIGURE 3-7 The VMs tab of the properties of a managed host.

There is also an additional setting on this tab, Register The Following Virtual Machines, that enables you to register virtual machines that have files located on the host but have not been added as a virtual machine. Registering a virtual machine is done automatically when you create, deploy, or migrate a virtual machine to a host. However, you might have files for a virtual machine that have not been added on a host or in VMM as a managed virtual machine. Registering these virtual machines adds them to the host and allows for management using VMM.

Reserves This tab lets you to configure resource parameters (CPU percentage, memory, disk space, maximum disk I/O, and network capacity) that will be used to determine whether a virtual machine can be hosted on the host. (See Figure 3-8.) If the host does not meet all these requirements, virtual machines cannot be placed on that host.

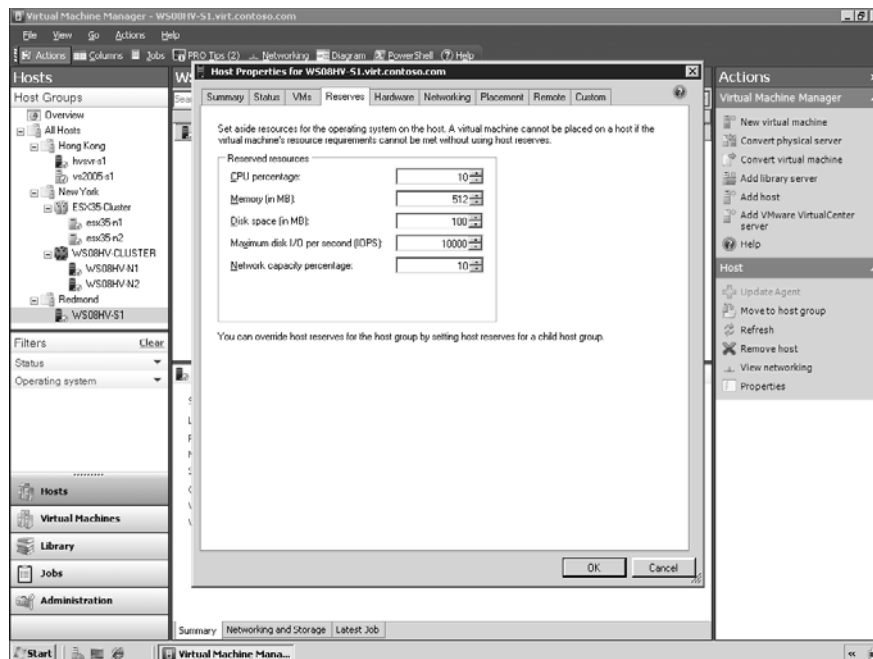


FIGURE 3-8 The Reserves tab of the properties of a managed host.

Hardware This tab displays information concerning the hardware configuration of the host. (See Figure 3-9.) You can use this tab to specify whether or not a specific volume is available for placement, to override the discovered network location for a specific network adapter, and for other purposes.

Networking This tab displays information concerning the virtual networks that are configured on the host to support virtual machines running on the host. Virtual Networks can be added, modified, or removed by using this tab. The type of virtual networks displayed here depends on the type of virtualization running on the host. For example, Figure 3-10 shows the virtual networks configured on a Hyper-V host.

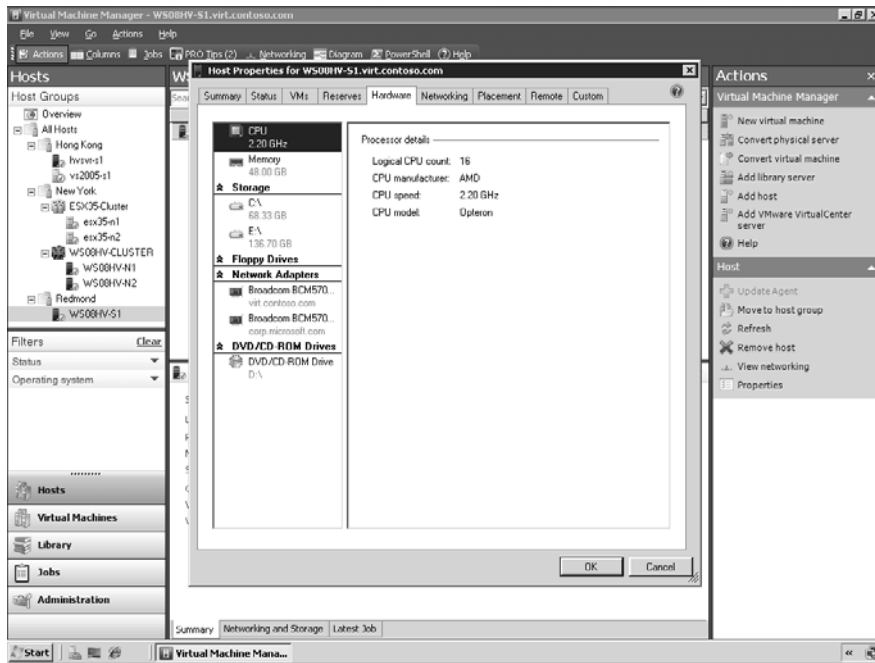


FIGURE 3-9 The Hardware tab of the properties of a managed host.

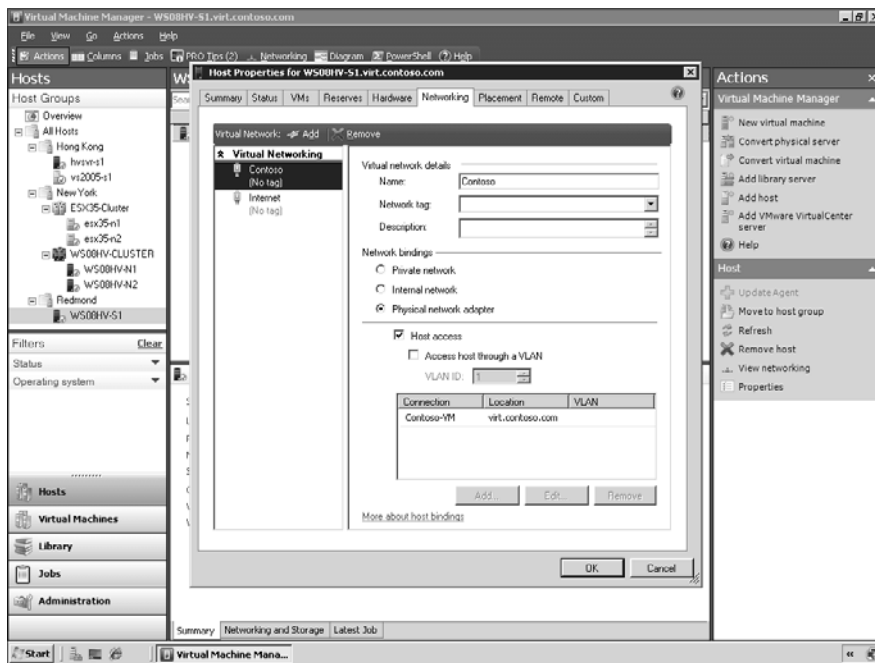


FIGURE 3-10 The Networking tab of the properties of a managed host.



More Info For more information concerning virtual networks, see Chapter 2, “Server Virtualization—Hyper-V” in this book.

Placement This tab displays information concerning the default paths available on the host for placement of virtual machines. (See Figure 3-11.) If a path was not specified when the host was added to VMM, all known paths will be displayed.

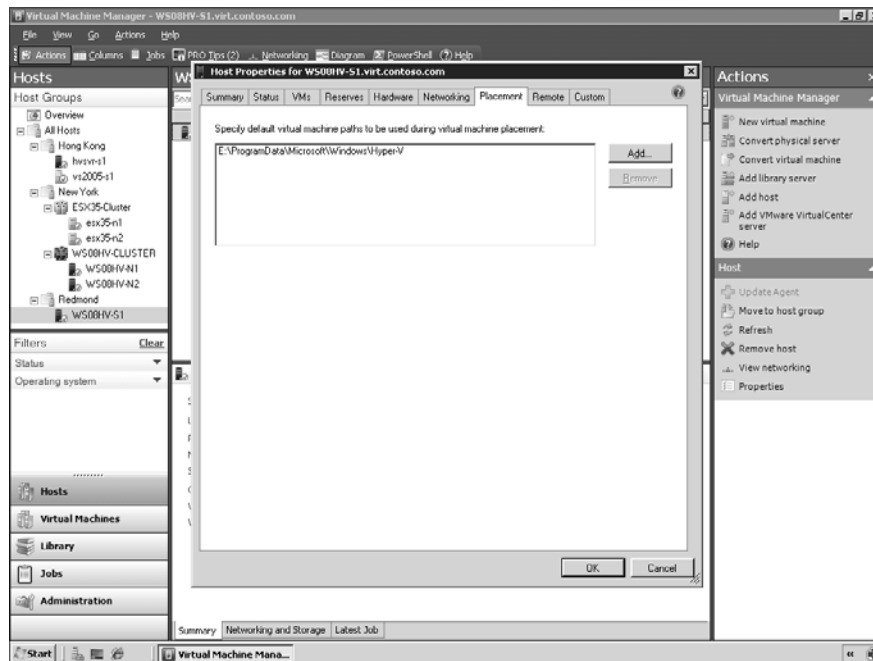


FIGURE 3-11 The Placement tab of the properties of a managed host.

Remote This tab displays the port used by VMRC for remote connection. (See Figure 3-12.) The default port for VMRC in Hyper-V is port 2179, while in Virtual Server 2005 R2 SP1 it is port 5900.

Custom This tab lets you add custom properties to the host for informational purposes. (See Figure 3-13.) To add more columns, including custom properties, to the Results pane of the Hosts view, select Columns from the toolbar to open the Select Columns dialog box. You can also right-click on the column header to add or remove columns.

Other settings for managed hosts In addition to the settings available on the Properties page of a managed host, more information concerning the host is displayed in the Details pane at the bottom middle of the Administrator Console. To view this information, choose the Host view to display a list of hosts in the Results pane and then select one of these hosts.

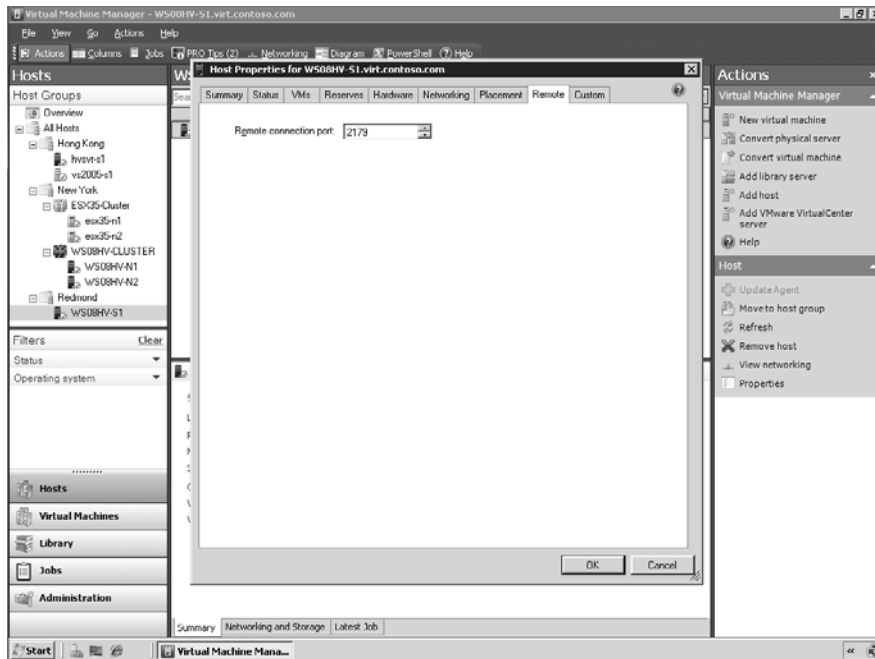


FIGURE 3-12 The Remote tab of the properties of a managed host.

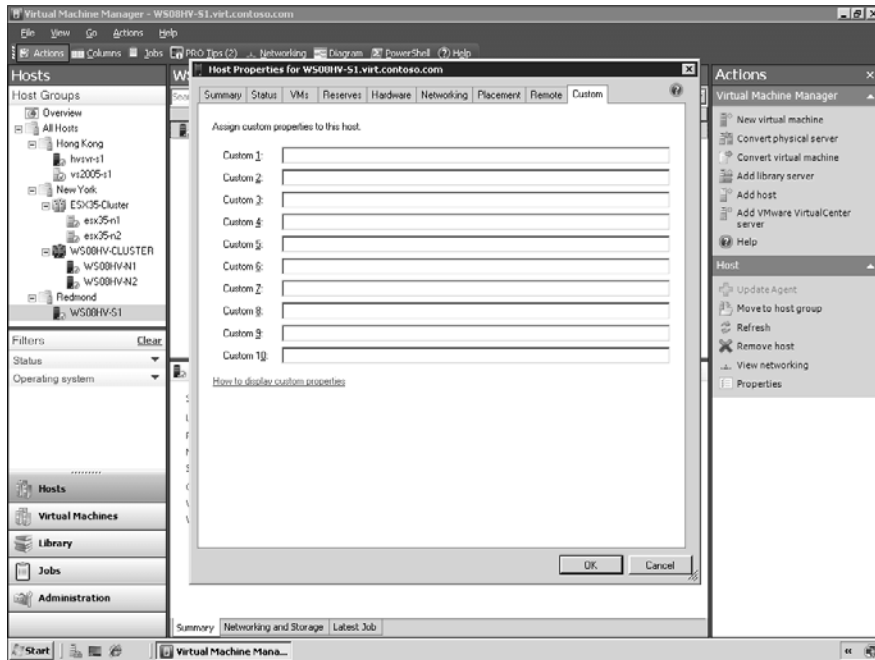


FIGURE 3-13 The Custom tab of the properties of a managed host.

The Details pane displays three tabs of information: Summary, Networking and Storage, and Latest Job. (See Figure 3-14.) The Summary tab provides general information concerning the host including which virtual machines are currently being hosted. The Networking and Storage tab shows which networks are connected and what storage is available, plus some usage statistics. The Latest Job tab displays information concerning the last job that was run against the host.

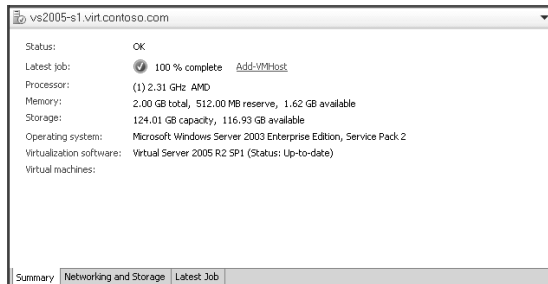


FIGURE 3-14 Additional information concerning managed hosts is displayed in the Details pane.

Using Networking View

There is also a Networking view that is available for managed hosts. The Networking view shows what networks the host is connected to and what networks its hosted virtual machines are connected to. Figure 3-15 shows how you can specify the scope of the Networking view by selecting the host groups you want to display using this view.

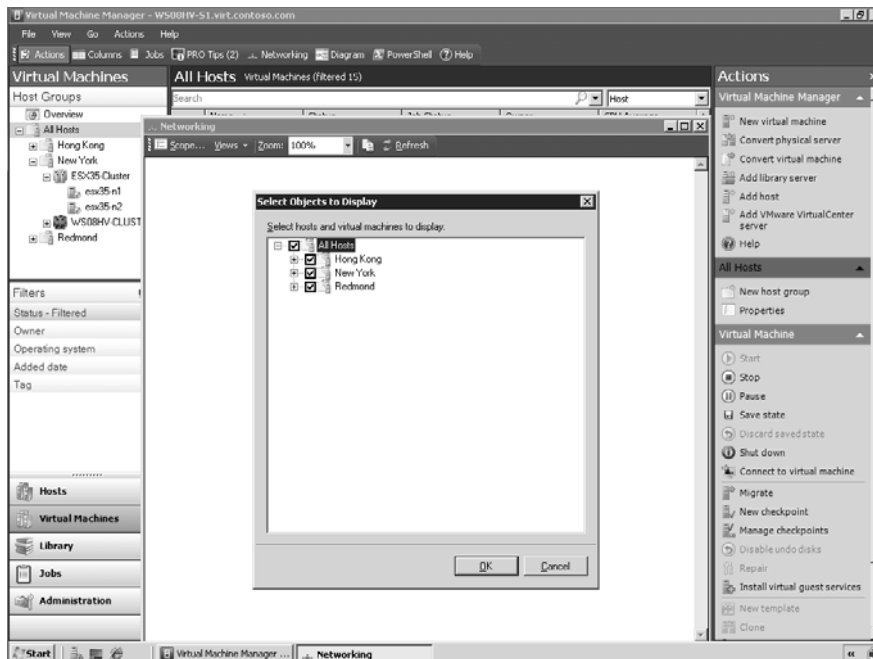


FIGURE 3-15 Specifying the scope to be used for the Networking view.

After you've specified the scope you want to use, the Networking view is displayed as a separate window as shown in Figure 3-16.

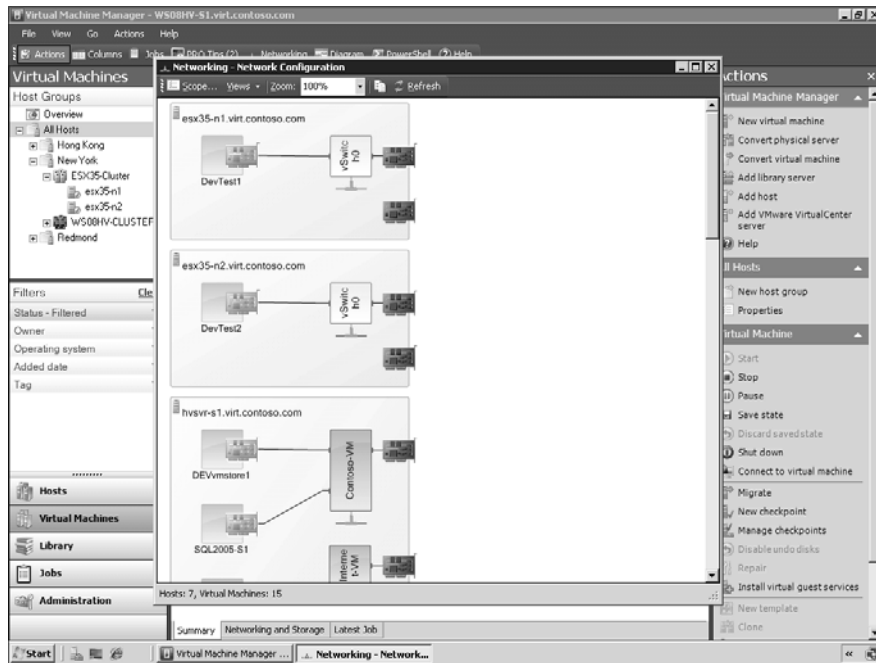


FIGURE 3-16 Displaying the Networking view window.

Managing Host Clusters

You can manage host clusters in a similar way to how you manage individual hosts as previously described. The main difference is that in a host cluster the hosts are grouped together. Plus there is some additional management functionality available. A benefit of using host clusters in VMM 2008 is that you can take advantage of the integration between VMM 2008 and OpsMgr 2007 using the new Performance and Resource Optimization (PRO) feature in VMM 2008. PRO provides workload-aware and application-aware resource optimization within host clusters and host groups. PRO is implemented through PRO tips, which can recommend or automatically implement actions such as virtual machine migration or virtual machine right-sizing based on policies implemented using OpsMgr 2007. For example, if you configure a host cluster for automatic implementation of PRO tips, VMM 2008 can migrate virtual machines automatically between nodes in a host cluster.

Direct from the Source: Managing a VMware Infrastructure 3 Environment

VMM 2008 manages VMware through the VMware Infrastructure API, so to start managing VMware, you must add a VMware VirtualCenter Server to VMM. When you add a VMware VirtualCenter Server to Virtual Machine Manager, all existing ESX Server hosts managed by the VirtualCenter Server are also added to VMM.

Requirements for Managing VMware

Virtual Machine Manager supports the following VMware releases:

- Virtualization managers:
 - ❑ VMware VirtualCenter 2.5
 - ❑ VMware VirtualCenter 2.0.1
- Virtual machine hosts:
 - ❑ VMware ESX Server 3.5
 - ❑ VMware ESX Server 3.0.2
 - ❑ VMware ESX Server 3i

Adding ESX Server Hosts

Your first step in configuring VMM to manage a VI3 environment is to add the VirtualCenter Server so that VMM can use the VMware Infrastructure API to manage the ESX Server hosts and virtual machines. When you add the VirtualCenter Server, you specify whether or not to communicate with the ESX Server hosts in Secure Mode. If you choose Secure Mode, you must provide a certificate and a public key in addition to credentials for each ESX Server host.

To Add a VMware VirtualCenter Server

1. In any view of the VMM Administrator Console, click Add VMware VirtualCenter Server.
2. Supply the computer name, port (default of 443) and administrative credentials of the VMware VirtualCenter Server to add.
3. Under Security, specify whether or not to communicate with the ESX Server hosts in secure mode.

In secure mode, a certificate and public key are required for each ESX Server host. Clear this option if you want to trust communications and require only credentials for the hosts.

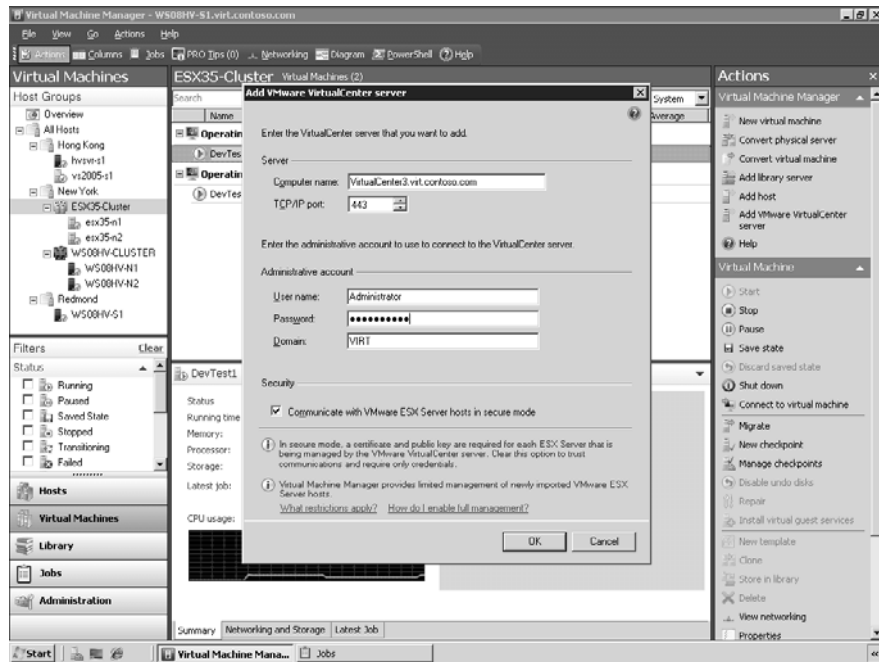


FIGURE 3-17 Adding a VMware VirtualCenter Server

4. If the VirtualCenter Server has a self-signed certificate, to verify the server's identity, you must import the server's security certificate to the local machine certificate store.

After the server is added to VMM, the ESX Server hosts are added to VMM in their own host group hierarchy. This operation might take several minutes although VMM adds the ESX Server hosts and then refreshes virtual machine data on the new hosts.

Configuring Security for Individual VMware ESX Server Hosts

Newly discovered ESX Server hosts initially have OK (Limited) status in VMM. To fully manage the virtual machines on the hosts, you must enter credentials in the host properties. If you are managing the VirtualCenter Server in Secure Mode, you also must provide a certificate and public key. For information about the restrictions that apply to virtual machines on a host that has OK (Limited) status, see Table 3-7.

TABLE 3-7 Supported Virtual Machine Actions for VMware ESX Server Hosts by Host Status

Virtual Machine Action	OK(Limited)	OK
Start	Yes	Yes
Stop	Yes	Yes
Pause	Yes	Yes
Modify properties	Yes	Yes
Create a new checkpoint	Yes	Yes
Manage checkpoints	Yes	Yes
Remove	Yes	Yes
Migrate with VMotion	Yes	Yes
Migrate across VirtualCenter Server	No	Yes
Save state	No	Yes
Discard a saved state	No	Yes
Store in the VMM library	No	Yes
Clone within the same VirtualCenter	No	Yes
Clone on the same ESX Server host	No	Yes
Perform (V2V conversion	No	Yes
Create from a VMM template	No	Yes
Create from a blank disk	No	Yes

To change the status of the ESX Server host to OK so that you can fully manage virtual machines, you must provide credentials and, if security mode is enabled on the host, upload a certificate and public key from the host to VMM.

Setting Credentials for Host Communication

To communicate with a virtual machine host that is on a perimeter network in a domain that does not have a two-way trust with the VMM Server’s domain, VMM uses credentials for an account that has administrative privileges on the host. To communicate with a VMware ESX Server host, VMM uses credentials for an account that has administrative privileges on the host and, if the host is in secure mode, a certificate and public key.

To update the credentials for communicating with a host, follow these steps:

- 1. In the Hosts view, select the host on which you want to update the credentials.
- 2. In the Host area of the Actions pane, click Properties.

3. Click the Security tab and then do one of the following:

- For a host on a perimeter network, type the credentials for the local agent service account and then click OK.
- For a host on a nontrusted domain, type the credentials for account on the host that has administrative privileges and then click OK.
- For a VMware ESX Server host, in the Credentials For This Host area, type the user name and password for an account that has administrative privileges on the host, and then type the password again to confirm it. If the host is in secure mode, in the Certificate And Public Key area, click Retrieve to upload the certificate and public key from the host select the Accept Both The Certificate And Public Key For This Host check box, and then click OK. Note that after adding a VirtualCenter Server to VMM, you can use the Add Hosts Wizard to manually add any new ESX Server hosts to VMM. VMM does not discover the new hosts automatically. Note also that removing an ESX Server host removes it immediately from VMM and also from the VirtualCenter Server.

—CSS Global Technical Readiness (GTR) team

Working with the Library

The VMM library is basically a catalog that provides access to file-based resources such as ISO images, virtual hard disks, scripts, and other types of files that are stored on VMM Library Servers. The library also provides access to virtual machine templates, guest operating system profiles, and hardware profiles you create and that reside in the VMM database. You can also store virtual machines in the library when they are not in use.

When you install your VMM Server, a Library Server is automatically installed on the server. The default location for the Library Server share on a VMM Server is `%SystemRoot%\ProgramData\Virtual Machine Manager Library Files`, and the share name is `MSSCVMMLibrary`. By default, when you install a Library Server, the only directory that is created is the one that holds two built-in .vhd files: Blank Disk Small and Blank Disk Large. You can then expand the folder structure under the library share to include folders for storing operating system installation images (ISO files), Windows PowerShell scripts, stored virtual machines, and other kinds of resources.

Library Server Requirements

Library Servers must meet the following requirements:

- Must be running either Windows Server 2008 or Windows Server 2003 SP1 or later. For highly available file servers, Windows Server 2008 Failover Clustering must be configured.

- Must be in an Active Directory domain that has a two-way trust relationship with the VMM Server's domain.



Note VMM 2008 does not support file servers configured with the case-sensitive option for Windows Services for UNIX. (The NFS Case Control is set to Ignore.)

Adding Library Servers

In a distributed environment with branch offices, it's a good idea to have additional Library Servers available to support remote locations, especially when users are using a Self-Service Portal to create virtual machines for their own use. This is because having all the necessary files available locally to support a virtualized environment can enhance performance and reduce network traffic. To accomplish this, you can add more Library Servers to VMM and then arrange for the replication of the necessary files to these new servers.

To add a Library Server, open the Administrator Console and select any view. In the Actions pane on the right side, select Add Library Server to launch the Add Library Server Wizard and then follow the prompts. If you have multiple Library Servers, you can organize them into Library Server groups in a similar way to how managed hosts can be organized into host groups. Figure 3-18 shows the Library view in the Administrator Console with a single Library Server and its resources visible. After you've deployed a Library Server, you can create additional library shares on it and add files to your library.

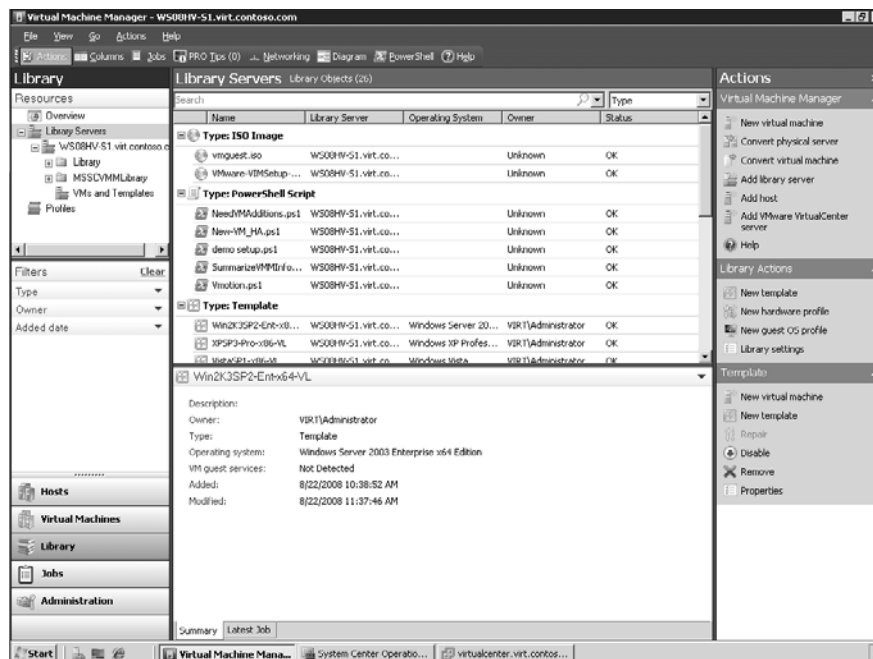


FIGURE 3-18 Library view in the Administrator Console.

Adding Virtual Machine Templates

Virtual machine templates can be used to create new virtual machines repeatedly using standardized hardware and software settings. Self-service users must use assigned templates to create their own virtual machines.

A virtual machine template is a library resource consisting of the following components:

- **Virtual hard disk** You can use a generalized virtual hard disk from the library, or you can create a virtual hard disk from an existing virtual machine. If the source virtual machine for your template has multiple virtual hard disks, select the disk that contains the operating system. To simplify the generalization process, include Virtualization Guest Services (such as Virtual Machine Additions or Integration Services) in your template.
- **Hardware profile** To define a standard set of hardware settings, you can create a hardware profile and associate it with a template. When you create a new template or create a virtual machine from a template, you can specify the virtual hardware settings or reuse an existing hardware profile from the library. For more information about hardware profiles, see the section titled “Adding Hardware Profiles” that follows.
- **Guest operating system profile** To maintain guest operating system standardization in deployed VMs using templates, you can attach a guest operating system profile from the library to the template. When you create a new template or create a virtual machine from a template, you can specify the settings manually or use an operating system profile associated with your answer files. For more information about guest operating system profiles, see the section “Adding Guest Operating System Profiles” that follows.

Virtual machine templates can be created in the Library view in the Administrator Console. In the Actions pane on the right side, select New Template to launch the New Template Wizard and then follow the prompts.

Adding Hardware Profiles

Hardware profiles are library resources that contain hardware specifications that can be applied to a new virtual machine or to a virtual machine template. For example, hardware profiles can contain specifications for CPU, memory, network adapters, a DVD drive, a floppy drive, COM ports, and the priority given to a virtual machine when allocating resources on the virtual machine’s host.

You can create hardware profiles that import a standard hardware configuration into a template or into a virtual machine. The options are the same whether you update the hardware configuration of a virtual machine, hardware profile, or virtual machine template. After specifying a hardware profile for a virtual machine, you can change the settings that were imported. The changes do not affect the hardware profile. No association is maintained with the hardware profile after the virtual machine is created.

Hardware profiles are managed in the Library view of the Administrator Console. To create a hardware profile, click the New Hardware Profile action in the Library view. You can also save a new hardware profile based on the hardware configuration of an existing virtual machine or virtual machine template.

Adding Guest Operating System Profiles

A *guest operating system* is the operating system that runs on a virtual machine. By contrast, a *host operating system* is the operating system that runs on the physical computer (the virtual machine host) on which one or more virtual machines are deployed. In VMM 2008, a guest operating system profile is a collection of operating system settings that can be imported into a virtual machine template to provide a consistent operating system configuration for virtual machines that are created from that template.

You create guest operating system profiles to provide standard settings for the operating systems on your virtual machines. Guest operating system profiles are database objects that do not have any physical files associated with them. Guest operating system profiles are configured in the Library view, where they are displayed in a special VMs And Templates folder as shown in Figure 3-19.

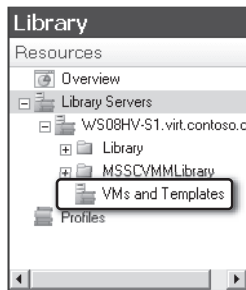


FIGURE 3-19 The VMs And Templates folder, which contains guest operating system profiles.

To create a guest operating system, use the New Guest OS Wizard in the Library view. Alternatively, you can save a guest operating system based on your current settings while you are creating a template. After the template is created, no association is maintained between the template and the guest operating system profile that was used with it. Any changes that are made to a guest operating system profile affect only new templates that are created after the changes are made.

Removing Library Resources

Library resources can be removed as well as added. In addition, specific files stored in the library can be disabled, library shares can be removed, and Library Servers can be removed from VMM.

When you no longer need a file in the VMM library, you can remove the file using the Administrator Console. If you remove the file from a library share outside of VMM, any template, guest operating system profile, hardware profile, or virtual machine that uses the file must be repaired to remove the reference to the deleted file. If you use the Remove action in the Library view to remove the file, VMM lists any virtual machines, templates, or guest operating system profiles that reference the file, and, if you choose to proceed, VMM removes references to the deleted file from the dependent resources.

Table 3-8 summarizes the resource dependencies that exist for different resource types. These dependencies involve only physical files. When a guest operating system profile, hardware profile, or template is used to create a virtual machine or a template, the settings are imported without maintaining any link to the source configuration.

TABLE 3-8 Resource Dependencies for Different Resource Types

Resource Type	Dependent Resources
Templates	ISO images, scripts, answer files, virtual hard disks, and virtual floppy disks.
Guest Operating System Profiles	Scripts and answer files.
Hardware Profiles	ISO images, virtual floppy disks.
Virtual Machines	The virtual hard disks and virtual floppy disks attached to a virtual machine are indexed in Virtual Machine Manager, but they are not displayed in the library because the files are not available for use with other resources.

Direct from the Source: Backing Up and Restoring the VMM 2008 Database

The VMM 2008 library comprises both flat files in the library share and the VMM database. The VMM database is a Microsoft SQL Server database that contains not only Library information but all VMM configuration information, including managed hosts, host configuration settings, VM settings, and other information. It is therefore important to back up the VMM database regularly as part of a comprehensive backup plan for protecting all VMM data, including data on hosts, virtual machines, and Library Servers. In addition to using the tools provided in VMM, you can also use SQL Server Management Studio to back up and restore the VMM database.

To Back Up the VMM Database

1. In the Administration view, click General, and in the Actions pane, click Back Up Virtual Machine Manager.
2. In the Virtual Machine Manager Backup dialog box, type the path for a destination folder for the backup file.



Note The folder must not be a root directory and must be accessible to the SQL Server.

To Restore the VMM Database on the Same Computer

1. To restore the VMM database, run the Scvmmrecover.exe tool from the command line. The Scvmmrecover.exe tool is located on the product CD at the following path: %cddrive%\i386\bin for a 32-bit computer, or %cddrive%\amd64\bin for a 64-bit computer.
2. On the VMM database computer, open a command-prompt window with elevated privileges, and then run the Scvmmrecover.exe tool using the following syntax:

SCVMMRecover [-Path <location>] [-Confirm]

where <location> is the Location of the Virtual Machine Manager database backup.

3. If any hosts has been added or removed since the database backup and the physical computer that you are restoring the VMM database on has the same System Identification (SID) number as the computer it was on before, then in the VMM Administrator Console, in the Hosts view, you must remove any hosts that might have been removed from VMM since the last backup was created. If a host has been removed from VMM after the last backup was created, it will have a status of Needs Attention in the Hosts view, and any virtual machines on that host will have a status of Host Not Responding in the Virtual Machines view. Then you must add any hosts that might have been added since the last backup.

To Restore the VMM Database on a Different Computer

1. To restore the VMM database, run the Scvmmrecover.exe tool from the command line. The Scvmmrecover.exe tool is located in %ProgramFiles%\Microsoft System Center Virtual Machine Manager 2008\bin.
2. On the VMM database computer, open a command-prompt window with elevated privileges, and then run the Scvmmrecover.exe tool using the following syntax:

SCVMMRecover [-Path <location>] [-Confirm]

where <location> is the location of the Virtual Machine Manager database backup.

3. Because the VMM Server is a different computer and the existing hosts are now not associated with this new VMM Server computer, you must perform the following steps to reassociate the hosts with the VMM Server:
 - a. In the VMM Administrator Console, in the Administration view, click Managed Computers, and in the Results pane, identify any managed computers with a status of Access Denied. Then click a managed computer with a status of Access Denied, and in the Actions pane, click Reassociate.
 - b. If any hosts have been added or removed since the database backup, in the VMM Administrator Console, in the Hosts view, remove any hosts that might have been removed from VMM since the last backup was created. If a host has been removed from VMM after the last backup was created, it will have a status of Needs Attention in the Hosts view and any virtual machines on that host will have a status of Host Not Responding in the Virtual Machines view. Then add any hosts that might have been added since the last backup.
 - c. If any VMs have been removed since the database backup, in the VMM Administrator Console, in the Virtual Machines view, remove any of those virtual machines. If a host is present but has a virtual machine that was removed since the last backup, the virtual machine will have a status of Missing in the Virtual Machines view.

—CSS Global Technical Readiness (GTR) team

Working with Virtual Machines

You can use VMM 2008 to create and manage virtual machines hosted on Hyper-V, Virtual Server, or VMware ESX Server managed hosts. You can also use VMM to perform P2V and V2V conversions and perform other tasks relating to virtual machines.

Creating New Virtual Machines

You can use VMM 2008 to create a new virtual machine from a template, from an existing virtual machine, or using a blank virtual hard disk. You can also use VMM to clone a virtual machine. The following walk-through illustrates how to create a new virtual machine from a template and place the virtual machine on a highly available managed host cluster.

Figure 3-20 shows a host cluster named WS08HV-CLUSTER. This host cluster has two hosts, named WS08HV-N1 and WS08HV-N2, and both of these hosts are running Windows Server 2008 with Hyper-V. The Results pane shows that the cluster currently has three virtual machines running on it: PRODExch4, WMVserver1 and SQL2005-S2.

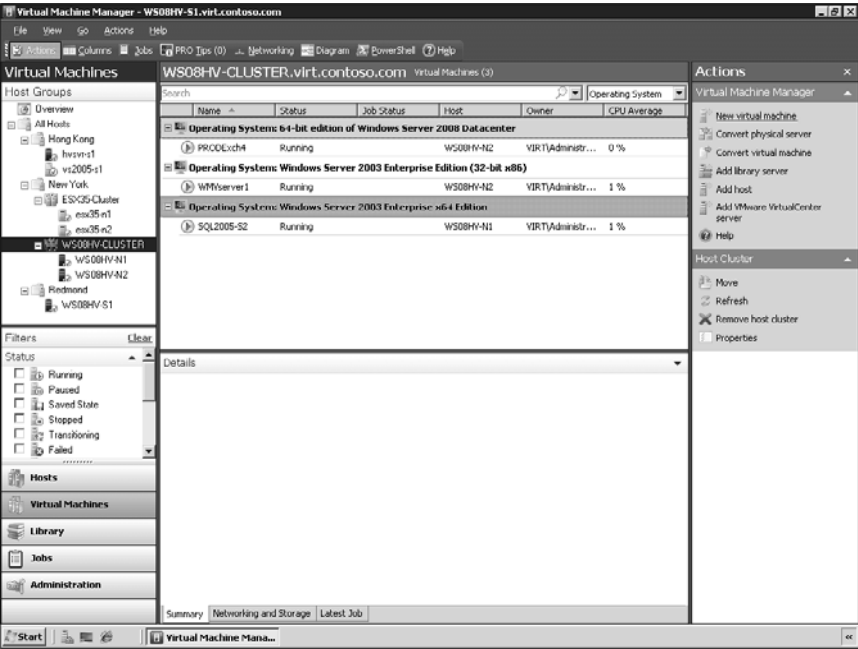


FIGURE 3-20 A managed host cluster with two nodes running three virtual machines.

Let's create a new virtual machine and place it on the cluster. To do this, click New Virtual Machine in the Actions pane. This launches the New Virtual Machine Wizard. (See Figure 3-21.)

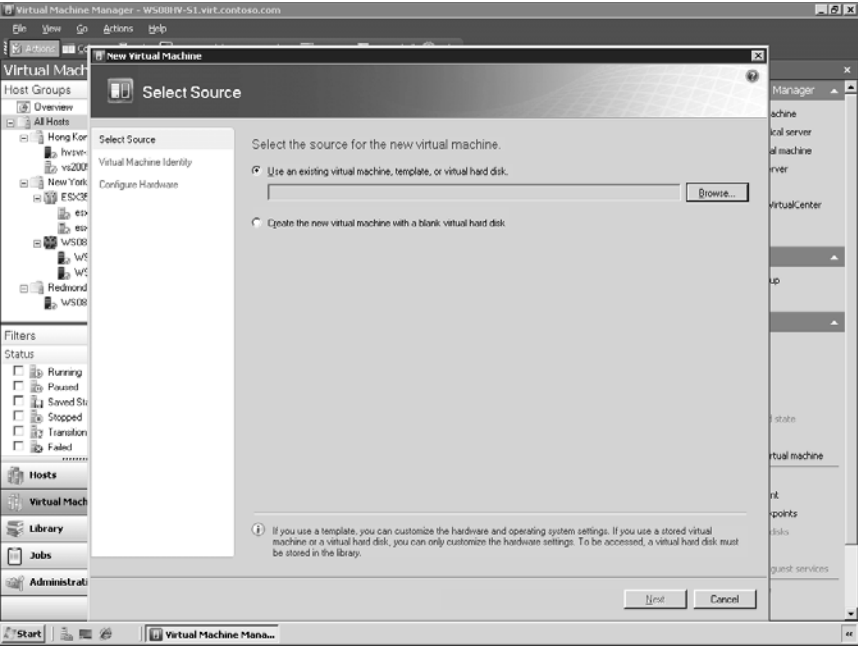


FIGURE 3-21 New Virtual Machine Wizard.

The New Virtual Machine Wizard gives you two options:

- You can create a new virtual machine from a template, an existing virtual machine, or an existing virtual hard disk.
- You can create a new virtual machine using a blank virtual hard disk. When you install your VMM Server, two blank virtual hard disks are added by default to the Library Server. These blank VHDs are named Blank Disk – Small and Blank Disk – Large. Both of these disks are dynamically expanding virtual hard disks (VHDs) that differ only in how large they can expand to. Specifically, the small VHD can expand to a size of 16 GB while the large VHD can expand to 60 GB.

To create a new virtual machine from a template, select the first option and click Browse. This opens the Select Virtual Machine Source dialog box, which displays a list of virtual machine templates and available virtual hard disks to choose from. We'll select the template named Win2K3SP2-Ent-x64-VL, which is configured to use Windows Server 2003 Enterprise x64 Edition as the guest operating system for the new virtual machine. (See Figure 3-22.)

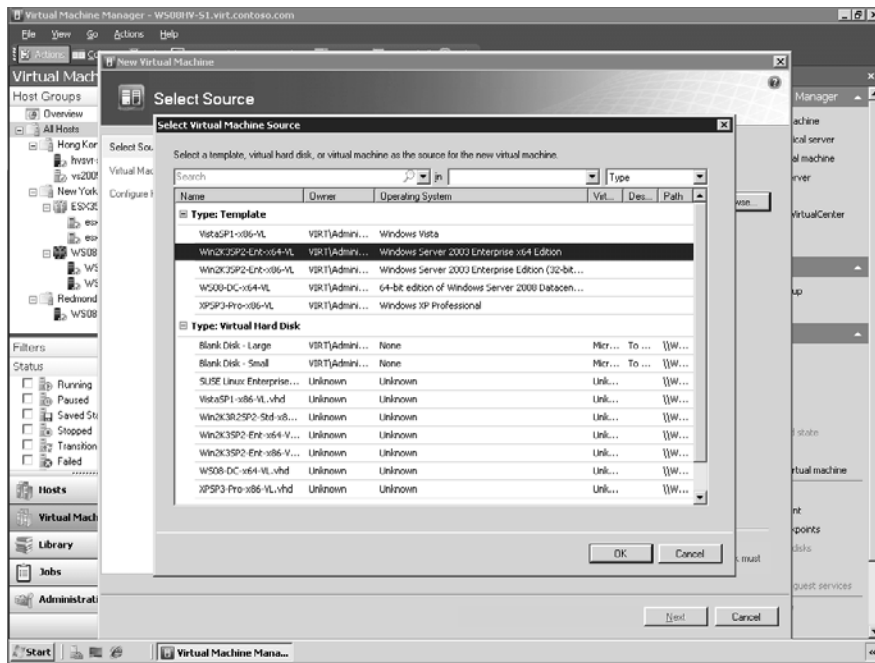


FIGURE 3-22 Selecting a virtual machine template.

Selecting the desired template and clicking OK returns you to the New Virtual Machine Wizard. (See Figure 3-23.)

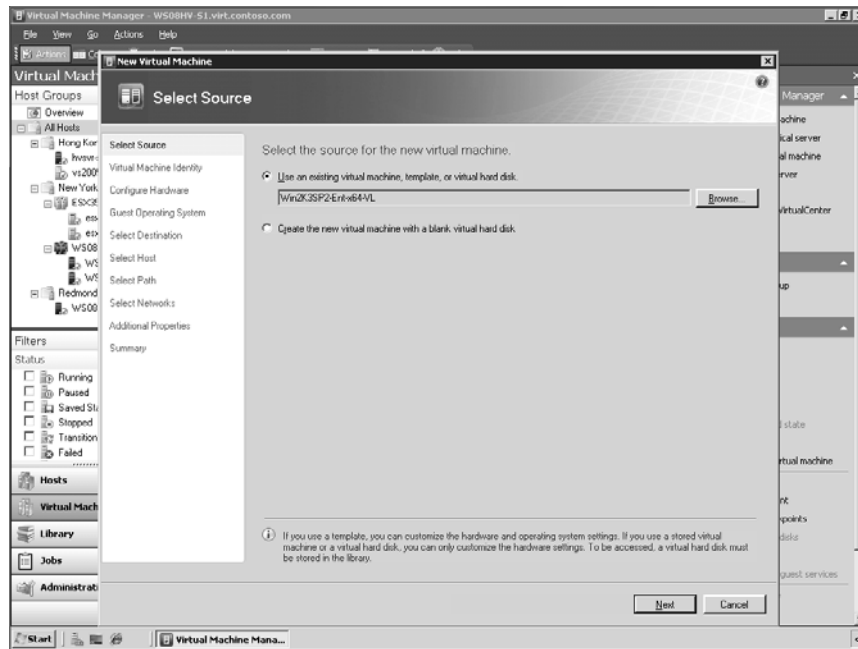


FIGURE 3-23 Creating a new virtual machine from a template.

Continuing through the wizard, the next thing you must do is give your new virtual machine a name. (See Figure 3-24.)

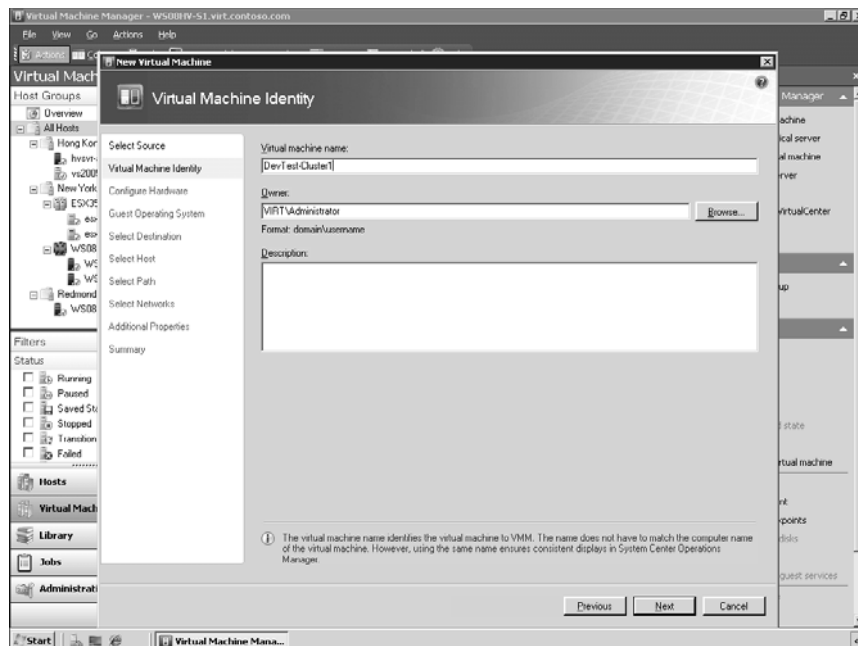


FIGURE 3-24 Naming the new virtual machine.

On the next page of the wizard, you configure the virtual hardware settings for your new virtual machine. Virtual hardware settings include BIOS, processor, memory, IDE controllers, network adapters, and other virtual devices that collectively represent the hardware profile of the virtual machine. Figure 3-25 shows the virtual machine's memory being configured as 1024 MB of RAM.

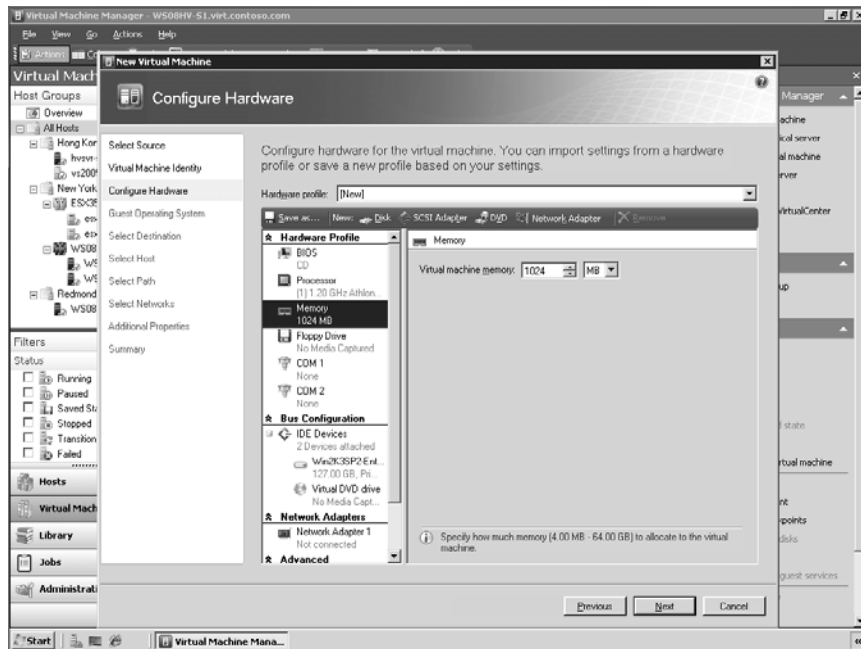


FIGURE 3-25 Configuring virtual hardware settings for the virtual machine.

On the next page of the wizard, we've selected the option to make the new virtual machine highly available by placing the virtual machine on a Microsoft Hyper-V server that is part of a cluster. (See Figure 3-26.)

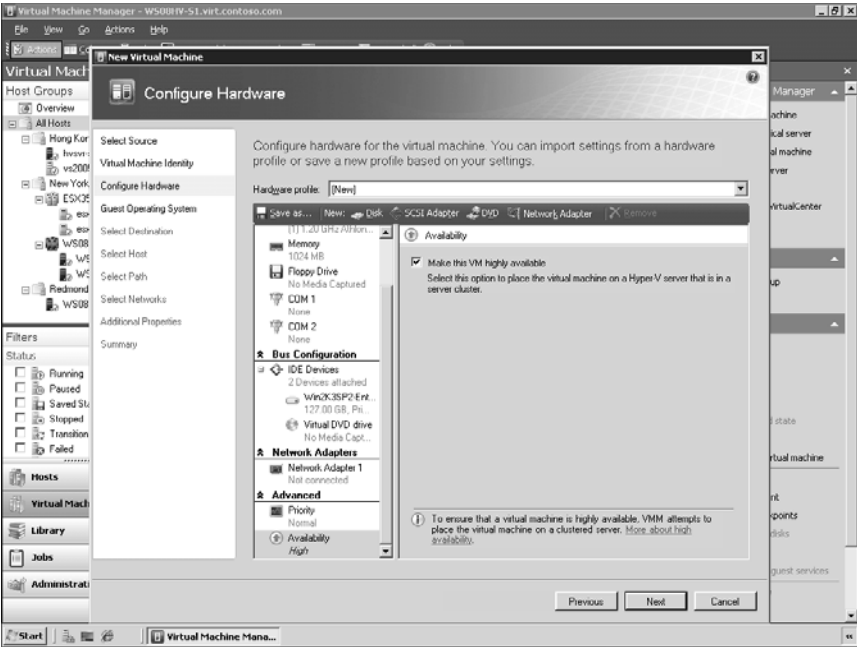


FIGURE 3-26 Configuring the new virtual machine for placement on a cluster.

On the next wizard page, you specify a password for the local Administrator account of the guest operating system for the virtual machine. (See Figure 3-27.)

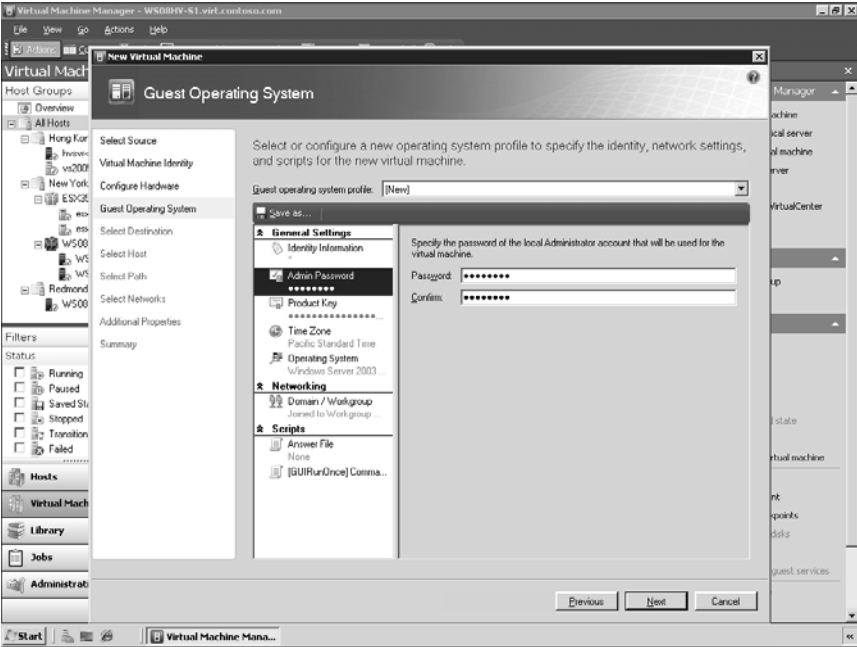


FIGURE 3-27 Specifying a password for the Administrator account.

The next page lets you choose whether to place your new virtual machine on a host or store it in the library. (See Figure 3-28.)

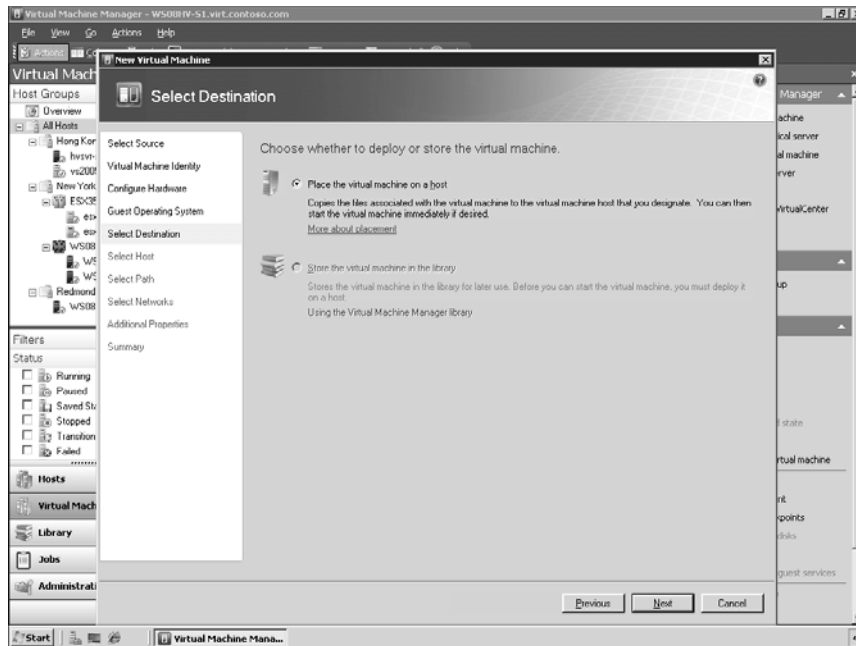


FIGURE 3-28 Choosing whether to deploy or store the virtual machine.

Selecting the option to deploy the virtual machine on a host brings up a list of possible hosts you can deploy the machine on. Figure 3-29 shows that we have chosen to deploy the new virtual machine onto one of the nodes of our host cluster. The node we will place our virtual machine on is named WS08HV-N2.virt.contoso.com and uses a storage area network (SAN) for storage. The Details portion of this wizard page shows that this cluster node currently has two other virtual machines running on it, named PRODExch4 and WMVserver1.

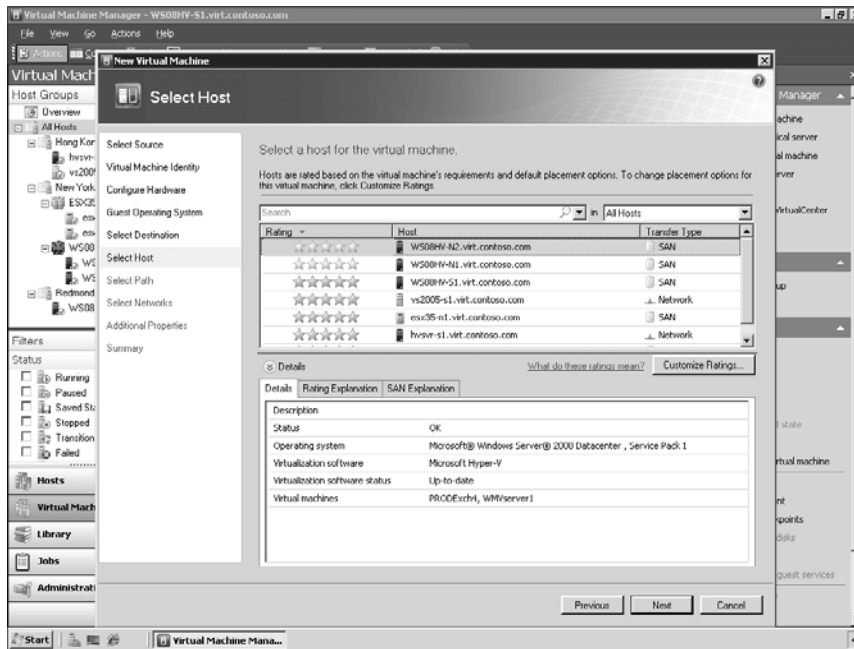


FIGURE 3-29 Choosing to place the new virtual machine on a node in a host cluster.

The next wizard page lets us specify the path on the host to where we will save the file associated with the virtual machine. (See Figure 3-30.)

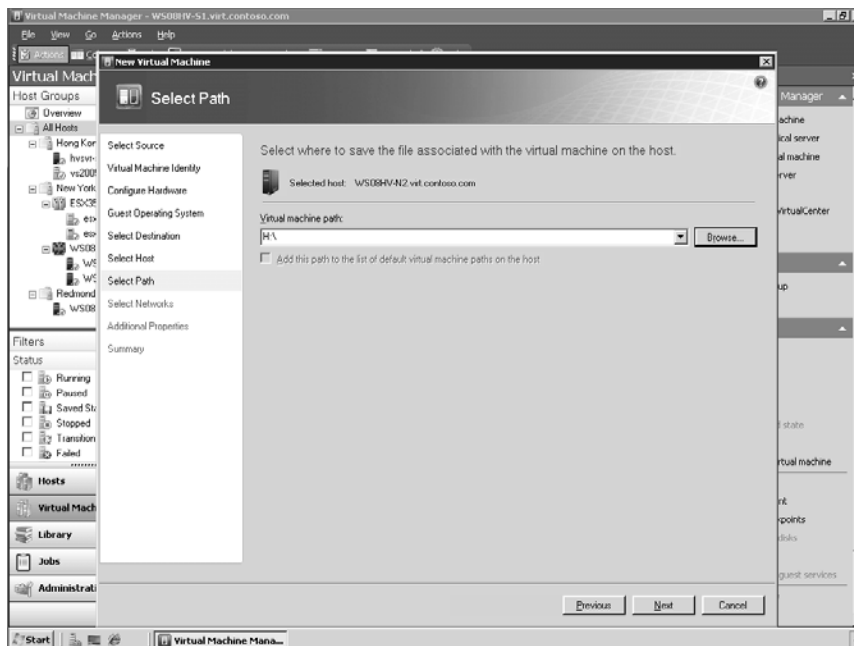


FIGURE 3-30 Specifying the path for storing the virtual machine files.

Clicking Browse opens the Select Destination Folder dialog box, which displays the various cluster disks we can choose from for storing the files for our new virtual machine. (See Figure 3-31.)

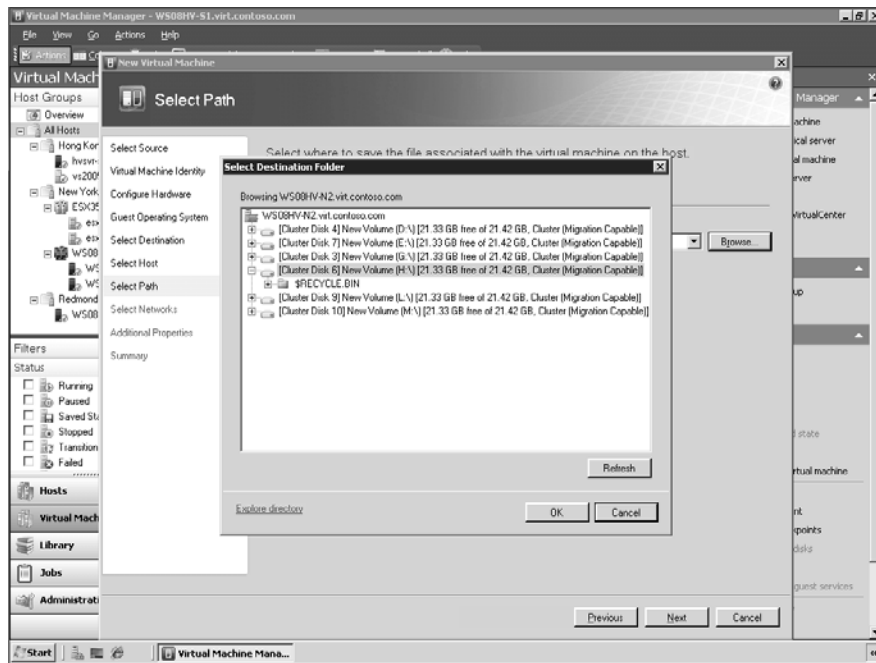


FIGURE 3-31 Browsing the available storage resources for the host cluster.

In the next page of the wizard, you select the virtual network that the new virtual machine will use. (See Figure 3-32.)

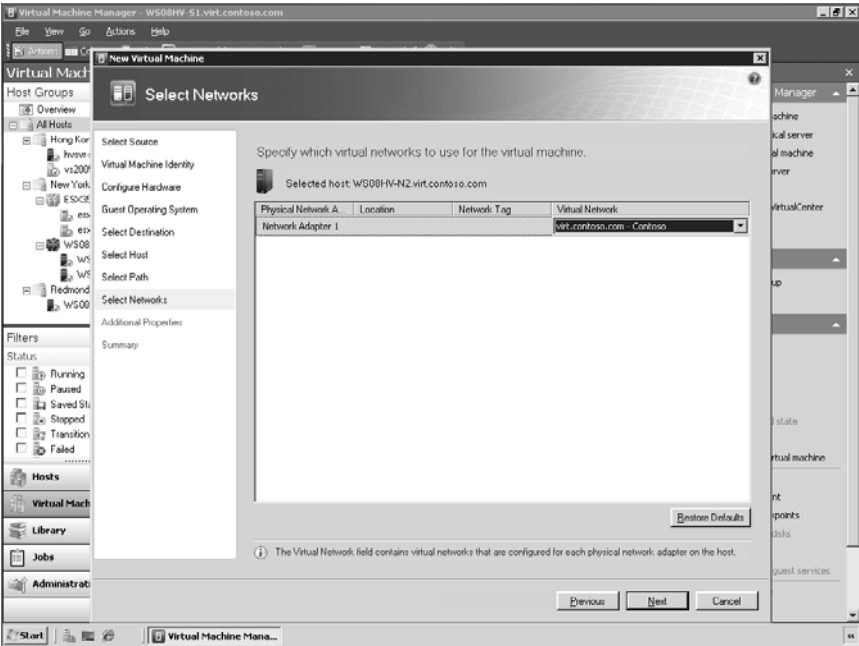


FIGURE 3-32 Selecting a virtual network for the new virtual machine.

The Additional Properties page of the wizard lets you specify what action should be performed on the virtual machine when the physical server stops or starts. (See Figure 3-33.)

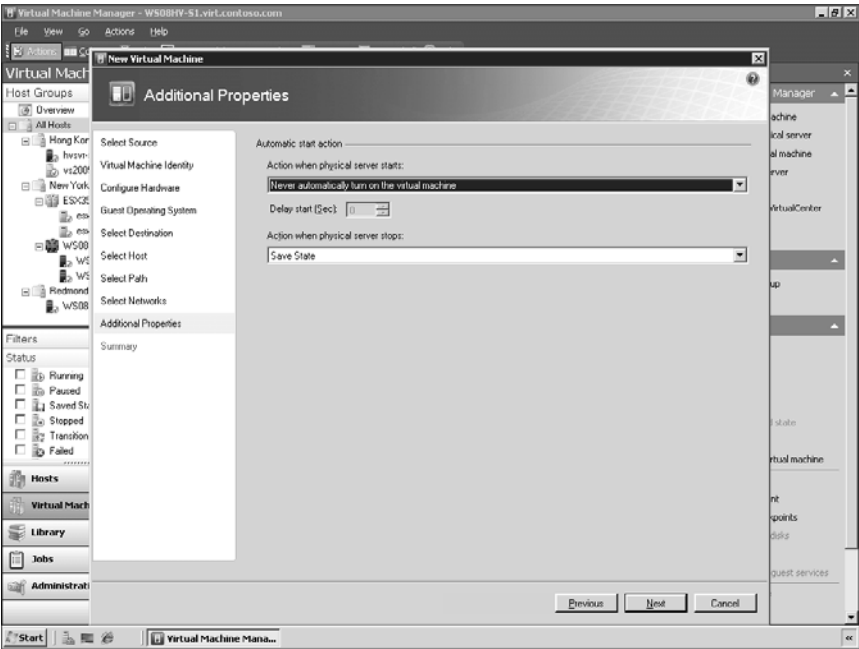


FIGURE 3-33 Specifying what happens to the virtual machine when the host stops or starts.

The final page of the wizard lets you review the settings you have chosen for your new virtual machine. (See Figure 3-34.) After you complete the wizard, the new virtual machine is created and deployed to the host cluster you specified.

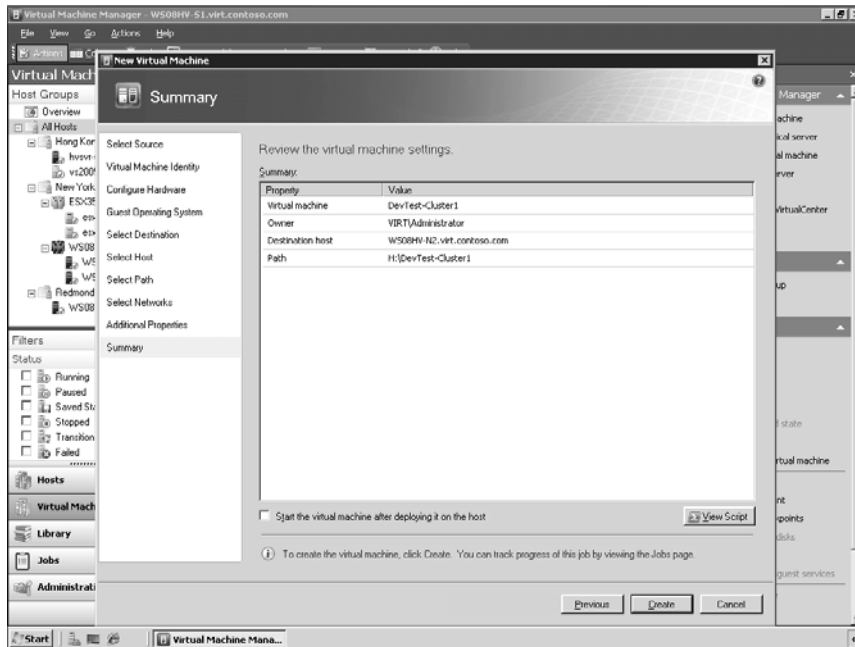


FIGURE 3-34 Summary page of New Virtual Machine Wizard.

Managing Virtual Machines

You can use the Administrator Console to manage virtual machines. (See Figure 3-35.) The following are some of the management actions that can be performed on virtual machines:

- **Start** Starts a virtual machine that is stopped, paused, or in a saved state.
- **Stop** Stops a virtual machine and does not save any state information. This action has the same effect on the virtual machine as does pulling the plug on a physical computer.
- **Pause** Suspends execution of a virtual machine, and keeps all virtual machine state in memory.
- **Save State** Suspends execution of a virtual machine, and saves the current virtual machine state to disk to release memory and CPU resources for other virtual machines. When the virtual machine is restored from the saved state, it returns to the condition that it was in when its state was saved.
- **Discard Saved State** Discards the state that was saved for a virtual machine that is in a saved state, and turns off the virtual machine.
- **Shut Down** Shuts down the guest operating system on the virtual machine.

- **Connect To Virtual Machine** Connects to a virtual machine by using Remote Desktop Protocol (RDP). VMM attempts to connect to a running virtual machine that you select in the Results pane and adds a thumbnail of the connection—the desktop of the virtual machine—to the virtual machine details. To open a larger connection window so that you can log on to the virtual machine, you can either double-click the thumbnail or click Connect To Virtual Machine in the Actions pane.
- **Repair** Repairs a failed virtual machine by retrying the action that caused the failure, restoring the virtual machine to its state before the action caused it to fail, or refreshing the data for the virtual machine in VMM after mitigating the issue outside VMM.
- **Install Virtual Guest Services** Installs Virtual Guest Services, such as Integration Services (Hyper-V) or Virtual Machine Additions (Virtual Server) on the virtual machine.
- **Disable** Disables a virtual machine that is stored in the library to temporarily prevent use of the virtual machine. A disabled virtual machine remains in the library but cannot be deployed or repaired. (This option is available in Library view only.)
- **Properties** Modifies the properties of a virtual machine.

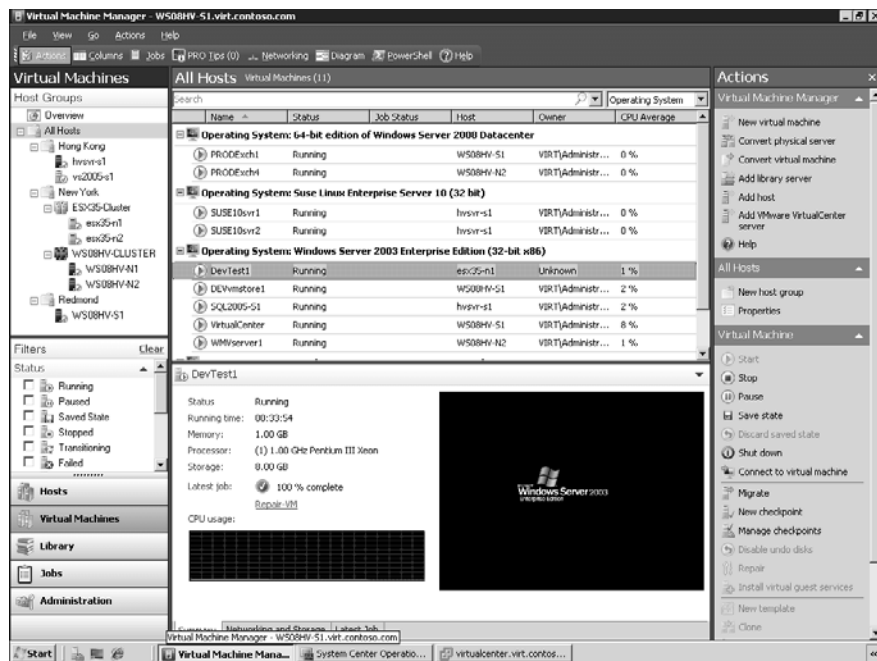


FIGURE 3-35 Managing virtual machines using the Administrator Console.

You can also use the Administrator Console to view and configure the settings for virtual machines. The settings for a virtual machine can be accessed either in the Virtual Machines view or the Library view, depending on whether or not the virtual machine is deployed to a host or is stored in the library. The settings that can be modified also depend on the current state of the virtual machine.

Virtual machine settings can be accessed by double-clicking on the virtual machine, by right-clicking on the virtual machine and selecting Properties, or by clicking Properties in the Actions pane when in the Virtual Machine view. The properties dialog box for a virtual machine has six tabs with configurable settings as follows:

- **General** This tab is used to view general information concerning the virtual machine. The only setting that is not available for modification if the virtual machine is running, saved, or paused is the name of the virtual machine. Significant entries here are Owner and Tag. For example, if the virtual machine will be used as part of the Self-Service Portal, the Self-Service Portal user or users should be designated as the owner or owners of the virtual machine or they will be denied access. Additionally, tag entries can be used as part of the deployment or placement process, where virtual machines can be deployed only to managed hosts that meet specific requirements based on tags that are set on templates in the library that Self-Service Portal users have access to.
- **Hardware Configuration** This tab documents the hardware configuration of the virtual machine. The settings here can be changed only if the virtual machine is not running and its status shows as Stopped.
- **Checkpoints** This tab shows the checkpoints (snapshots in Hyper-V terminology) that have been taken for the virtual machine. You can also create a new checkpoint, remove a checkpoint, or restore a configuration to a virtual machine.
- **Custom Properties** This tab allows for configuration of up to 10 custom fields for the virtual machine. You can use custom fields to identify, track, and sort virtual machines by any property, including department, geographic area, or function.
- **Settings** This tab allows for the configuration of Self-Service Quota Points and Physical Resource Optimization (PRO) settings. By default, all virtual machines are allocated 1 quota point.
- **Actions** This contains settings that determine what happens when the physical host server starts and stops.

The settings available for when the physical server starts are

- Never Automatically Turn On The Virtual Machine
- Always Automatically Turn On The Virtual Machine
- Automatically Turn On The Virtual Machine If It Was Running When Virtual Server Stopped

The settings available for when the physical server stops are

- Save State
- Turn Off Virtual Machine
- Shut Down Virtual Machine

Direct from the Source: Connecting to Virtual Machines

Remote connections to virtual machines running on managed hosts can be made in the VMM Administrator Console. VMM uses Virtual Machine Remote Control (VMRC), which is a feature of Virtual Server 2005 that lets you enable, disable, and configure virtual machines from within Virtual Machine Manager. Remote control options and the connection ports for virtual machines on virtual machine hosts vary depending on the virtualization software running on the host and the operating system running on the computer on which the VMM Administrator Console is installed. The settings for the VMRC are configured under the General settings in the Administration view.

To connect to a virtual machine, the following requirements must be met:

- Credentials must be provided to log on to the virtual machine. Local administrator credentials can be configured during virtual machine creation (if using a template).
- For Microsoft Virtual Server, you must have specified the port on the VMM Server to use for remote control. RDP must be enabled on the virtual machine host.

You can also use remote control to access the guest operating system of a virtual machine much like you can access Windows by using Remote Desktop. However, unlike Remote Desktop, which allows you to connect only if the operating system is running, remote control in VMM allows you to access a virtual machine prior to the guest operating system startup.

Controlling Hyper-V Hosts

To control virtual machines on a Hyper-V host by remote control, VMM uses either VMConnect or RDP, depending on the operating system that is running on the computer that the VMM Administrator Console is installed on.

For all supported versions of Windows Server 2008 and for Windows Vista with SP1, VMM uses VMConnect with the default port of 2179. You can change the default port that is used for connecting to virtual machines on new Hyper-V hosts. For all other supported operating systems, VMM uses RDP with the default port of 3389.

Controlling Virtual Server Hosts

To control virtual machines on a Virtual Server host by remote control, VMM uses VMRC.

The VMRC client connects to an instance of Virtual Server on a host and allows you to access its virtual machines. Through VMRC, you can use a virtual machine as if you were using it through the Virtual Server Administration Web site. However, VMRC does not provide the administrative capabilities available in the Administration Web site,

such as creating a new virtual machine or changing a virtual machine configuration. You can perform those functions in VMM.

You can enable and configure VMRC settings when you add a host or after you have added the host.

You can set up VMRC access accounts to give administrators access to all virtual machines on all managed hosts. To gain access to a virtual machine through VMRC, an administrator must be logged on under an account that has administrative credentials on the local host computer.

By default, when you add a host to VMM, VMRC is enabled and uses the following settings:

- The connection port is set to the global default port setting for Virtual Server hosts as specified in General settings in the Administration view.
- No connection time-out is enabled.
- Only one user at a time is allowed to connect to a virtual machine.
- The VMRC connection is not encrypted. (You can modify this setting only after a host has been added.)



Note It is recommended that you implement Secure Sockets Layer (SSL) security for VMRC connections, particularly if you use Basic authentication, which transmits passwords in plain text.

If you change the VMRC port, the port setting you assign for the hosts must identically match the port settings that are assigned in Virtual Server.

You can allow multiple users to connect to the same virtual machine. However, each user can access the guest operating system without the knowledge of the other users. This is by design for training and lab scenarios, where one user wants to demonstrate a task to other users and have them connect to and view the same remote session. Because VMRC connections do not use sessions, allowing more than one user to connect can result in collisions.

You can use SSL to encrypt communications over the VMRC connection by uploading a certificate from an appropriate internal or third-party certification authority.

Controlling ESX Server Hosts

To control virtual machines on VMware ESX Server hosts by remote control, VMM uses the VMware mouse keyboard and screen (MKS) Client with default port 902. You cannot change the remote control settings or default port for an ESX Server host in VMM.

Before connecting to a VM on an ESX Host, you must install the VMware ActiveX control. To install the ActiveX control, in the Virtual Machines view, from the Results pane, select an ESX host. In the Summary tab of the details pane, the expected thumbnail view of the VM will have the following message: "VMware ActiveX control not installed. To view a thumbnail for this virtual machine, you must install the VMware ActiveX component." Select Install ActiveX Control, and follow the instructions. Note that thumbnails are not visible for 64-bit VMware clients.

Connecting to a Virtual Machine

To connect to a virtual machine, locate the host it is running on and either double-click the thumbnail view in the middle pane or select the Connect To Virtual Machine action. This will open the Virtual Machine Viewer (Hyper-V), the VMRC Viewer (Virtual Server 2005), or the VMware Viewer (VMware ESX), accordingly.

—CSS Global Technical Readiness (GTR) team

Deploying Virtual Machines

You can use VMM 2008 to deploy virtual machines stored in the library to managed hosts. Deploying a virtual machine stored in the library removes the virtual machine from the library and places it on the target host. Alternatively, you can use the New Virtual Machine Wizard by selecting to use an existing virtual machine or VHD in the library if you want to keep the original virtual machine in the library as a source for additional future deployments.

To deploy a virtual machine, select the virtual machine from the appropriate Library Server and click Deploy. This launches the Deploy Virtual Machine Wizard. Then you follow the prompts.

Migrating Virtual Machines

You can use VMM 2008 to migrate virtual machines between hosts that are running the same virtualization platform (Hyper-V, Virtual Server, or VMware ESX Server). You can also migrate virtual machines from Virtual Server to Hyper-V.

The following methods are available to migrate a deployed virtual machine to a different host when in the Virtual Machines view:

- Click the Migrate action to launch the Migrate Virtual Machine Wizard, which enables you to select a suitable host, specify the path that will store the virtual machine, and select the type of transfer to be performed.
- Drag and drop the virtual machine onto a host.
- Drag and drop the virtual machine onto a host group. Through automatic placement, the virtual machine is placed on the most suitable host that is available in the host group based on the virtual machine's requirements and the group or individual host rating metrics.

The transfer methods available to migrate Hyper-V and Virtual Server virtual machine include SAN transfers (when a properly configured SAN is available) and Network (LAN) transfers. Note that if you migrate a virtual machine that is connected to SAN storage, the virtual machine will not be able to reconnect to the SAN unless the destination host also has access to that SAN. VMM is not able to detect whether a virtual machine is connected to a SAN or whether the destination host is connected to the same SAN, and therefore it cannot provide a warning. You must ensure that the new host is configured to allow the virtual machine to reconnect to the SAN before you migrate the virtual machine.

As an example of using the Migrate Virtual Machine Wizard, we'll migrate a virtual machine named DevTest1 running on a VMware ESX Server named esx35-n1 to a VMware ESX Server named esx35-n2, both of which are nodes in a highly available cluster named ESX35-Cluster. Figure 3-36 shows the shortcut menu that is displayed when you right-click on the DevTest1 virtual machine.

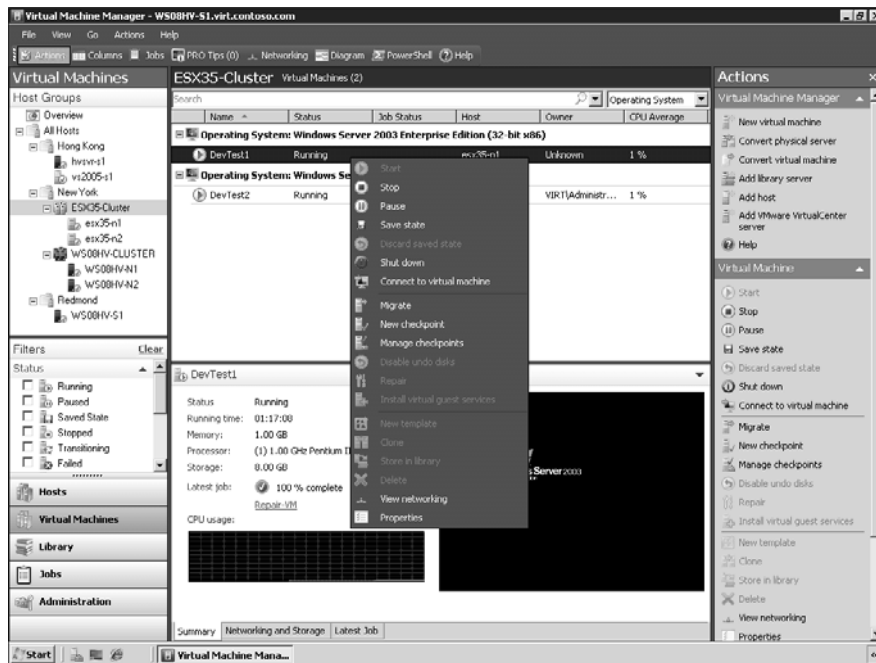


FIGURE 3-36 Preparing to migrate a virtual machine running on a VMware ESX Server.

You then select the Migrate option from the shortcut menu to launch the Migrate Virtual Machine Wizard. The Select Host page of the wizard displays the hosts available to which you can migrate the virtual machine. As shown in Figure 3-37, the first available host is the desired one, a VMware ESX Server named esx35-n2, and the transfer method used for migrating this host is VMware's VMotion, which enables live migration of virtual machines without service interruption.

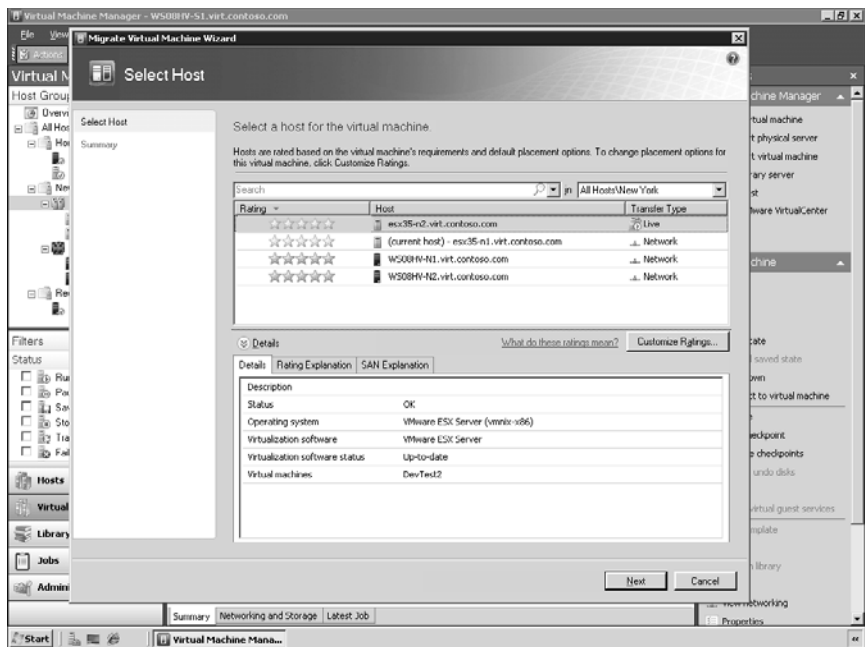


FIGURE 3-37 Selecting the destination host to which the virtual machine will be migrated.

The Summary page of the wizard shows the migration action that will be performed. (See Figure 3-38.)

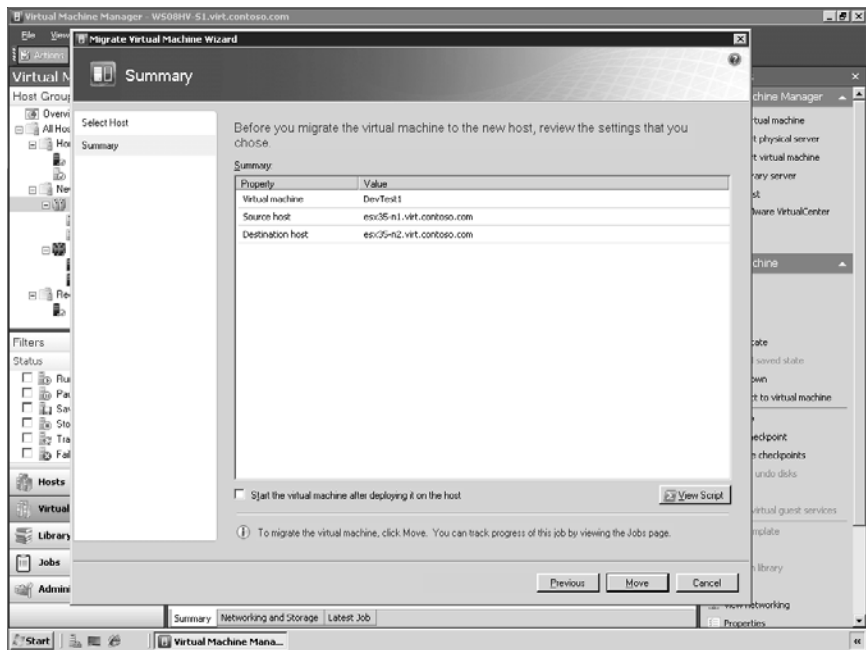


FIGURE 3-38 Summary page of Migrate Virtual Machine Wizard.

Figure 3-39 shows the migration currently underway.

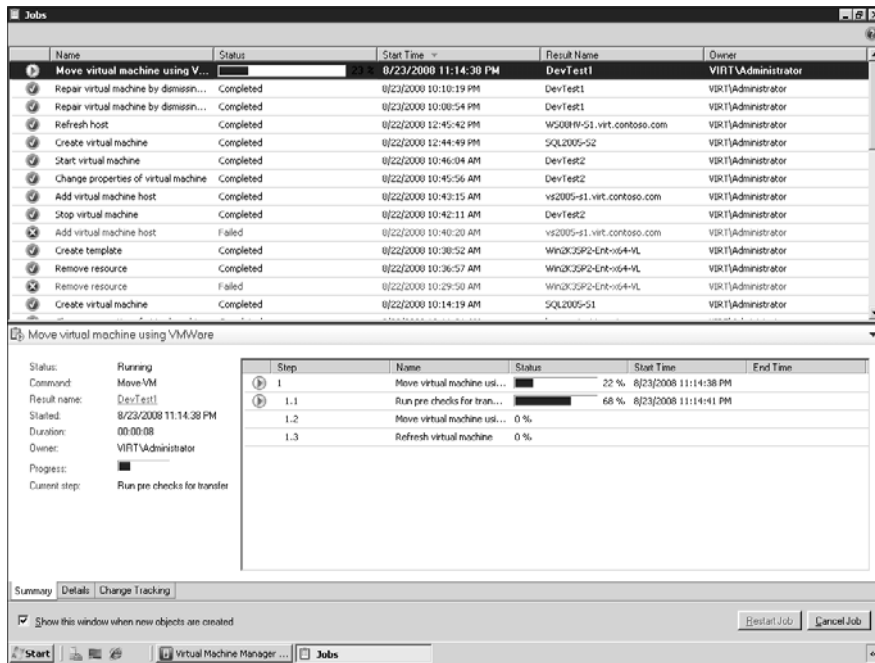


FIGURE 3-39 The migration is underway.

Cloning Virtual Machines

You can use VMM 2008 to “clone” (make an exact copy) of a virtual machine. The virtual machine you want to clone can be one that already exists in the library or one that is already deployed to a host (in which case, it must be turned off). The cloning process can also be used to back up virtual machines.



Note A cloned virtual machine has the same security identifier (SID) as the original, so they cannot be running simultaneously on the same network.

When you clone a virtual machine, you cannot make changes to the operating system settings, but you can make changes to the hardware profile.

To begin the cloning process, first make sure that the virtual machine is shut down on the host. Then select the virtual machine in the Administrator Console and click the Clone action to launch the New Virtual Machine Wizard and then follow the prompts.

Performing P2V Conversions

You can use VMM 2008 to convert a physical computer to a virtual machine. The process of doing this is known as Physical-to-Virtual (P2V) conversion. You might typically use the P2V conversion process as part of a server consolidation project where underutilized physical servers are converted into virtual machines so that these physical servers can be repurposed or decommissioned.



Tip You can use System Center Operations Manager to generate a Virtualization Candidates report that can help identify underutilized physical servers that could be good candidates for the P2V conversion process.

When identifying your best candidates for P2V conversion, consider converting the following types of servers, which are listed in order of preference:

- Non-business-critical underutilized servers. By starting with the least utilized servers that are not business critical, you can learn how the P2V process works with relatively low risk. Web servers can often make good candidates here.
- Servers with low utilization that are hosting less critical in-house applications.
- Servers with higher utilization that are hosting less critical applications.
- Other underutilized servers.

The requirements for a physical source computer depend on whether you are going to perform an online or offline P2V conversion:

- **Online P2V conversion** In this scenario, VMM uses BITS to copy data while the source computer continues to service user requests. The source computer is not restarted during the conversion, and the Volume Shadow Copy Service (VSS) is used to ensure data consistency. To perform an online P2V conversion, the source computer must have at least 512 MB of RAM.
- **Offline P2V conversion** In this scenario, the physical source computer restarts into the Windows Preinstallation Environment (Windows PE) before VMM converts the physical disks to VHDs. The Windows PE environment is used by the conversion process to capture the disk and therefore requires network and storage controller drivers for Windows PE. By default, VMM scans for these devices during the P2V conversion process and injects the required drivers into the Windows PE environment automatically. If third-party network interface card (NIC) or storage controller drivers are needed, however, these drivers must be provided by the administrator.

In either case, VMM temporarily installs the VMM Agent on the physical source computer that you want to convert.

The following operating systems are supported for P2V conversions:

- Windows Server 2008 (32-bit)
- Windows Server 2008 (64-bit)
- Windows 2000 Server SP4 or later (Offline P2V only)
- Windows 2000 Advanced Server SP4 or later (Offline P2V only)
- 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)

Although P2V conversion of source computers running Windows NT Server 4.0 is not supported by VMM 2008, you can use the Microsoft Virtual Server 2005 Migration Toolkit (VSMT) or third-party solutions for converting computers running Windows NT Server 4.0 into virtual machines.



Note When performing a P2V conversion of Windows 2000 Server or Advanced Server, the following components must be installed on the source computer:

- Service Pack 4
- Windows Installer 3.1 Redistributable (v2)
- Microsoft Visual C++ 2005 Redistributable Package
- .NET Framework 2.0
- BITS 2.0 Update KB842773

To perform a P2V conversion, you use the Convert Physical Server (P2V) Wizard. (See Figure 3-40.)

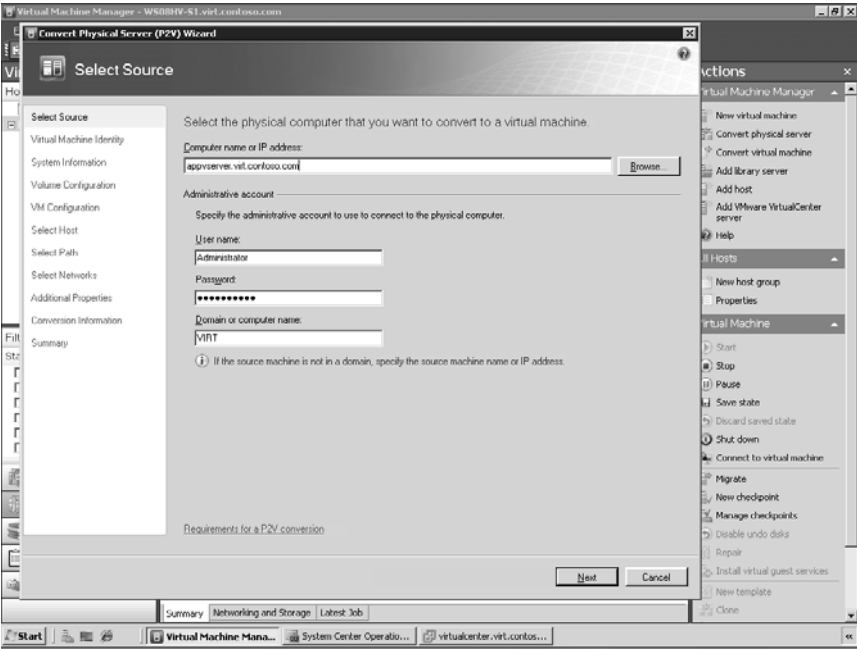


FIGURE 3-40 Using the Convert Physical Server (P2V) Wizard.

Performing V2V Conversions

You can use VMM 2008 to convert a VMware ESX Server–based virtual machine to a Hyper-V or Virtual Server–based virtual machine. This process is called virtual-to-virtual (V2V) conversion and is different from migration, which is the process of moving a virtual machine from one host to another and was discussed earlier in this chapter. Table 3-9 summarizes the difference between virtual machine migration and V2V conversion.

TABLE 3-9 Options for Virtual Machine Migration and V2V Conversion

From	To	Method
Hyper-V	Hyper-V	Migration
Virtual Server	Virtual Server	Migration
Virtual Server	Hyper-V	Migration
VMWare ESX Server	VMWare ESX Server	Migration
VMWare ESX Server	Hyper-V	V2V
VMWare ESX Server	Virtual Server	V2V

The following guest operating systems are supported for virtual-to-virtual (V2V) conversion:

- Windows Server 2008 (32-bit)
- Windows Server 2008 (64-bit)

- Windows 2000 Server SP4 or later
- Windows 2000 Advanced Server SP4 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)

V2V conversion can be performed by using the Convert Virtual Machine Wizard, which converts the .vmdk files to .vhd files and makes the guest operating system on the virtual machine compatible with Microsoft virtualization technologies. The virtual machine created by the wizard matches the VMware virtual machine properties, including its name, description, memory, disk-to-bus assignment, CD and DVD settings, network adapter settings, and other parameters.

Direct from the Source: Using P2V to Convert a Running VM from Another Hypervisor

One task that administrators ask for is the ability to do a Virtual-to-Virtual (V2V) conversion of a running VMware virtual machine to a Hyper-V server. The current V2V process in VMM is an offline process, but you can do an easy online conversion of a VMware VM. We have to remember that virtual machines are machines first and virtual second, and that VMs present themselves to users and administrators just like physical machines. Thus, administrators can do a Physical-to-Virtual conversion of the VMware VM. Even though it is a virtual machine, the VM can look like a physical machine to VMM, and if the operating system is a supported P2V operating system, VMM can do a live migration of that VMware VM to a Hyper-V VM.

—Edwin Yuen, Senior Product Manager, Integrated Virtualization Strategy

Configuring User Roles

VMM 2008 employs user roles to determine the level of access users and groups can have to different kinds of resources. You can create three types of user roles using the Administrator Console:

- **Administrator role** Able to perform all actions using the Administrator Console, including creating new Delegated Administrator and Self-Service User roles and adding members to these roles. The default membership in the Administrator role includes members of the local Administrator group on the VMM Server, the domain account of the user who installed the VMM Server, and the computer account of the VMM Server.

- **Delegated Administrator role** Able to perform most actions using the Administrator Console as restricted by the scope defined for the role. The scope defines which host groups and Library Servers the Delegated Administrator is permitted to manage. Members of this role can also create new Delegated Administrator and Self-Service User roles and add members to these roles.
- **Self-Service User role** Able to use the Self-Service Portal to perform tasks on virtual machines as defined by the scope and permissions for the role. Members of this role cannot create any new user roles.

You can create user roles by using the New User Role Wizard as demonstrated in the following sections.

Creating a Delegated Administrator Role

If you belong to either the Administrator or Delegated Administrator role, you can use the New User Role Wizard to create a new Delegated Administrator role. To do this, begin by selecting User Roles under Administration in the Administration pane. (See Figure 3-41.)

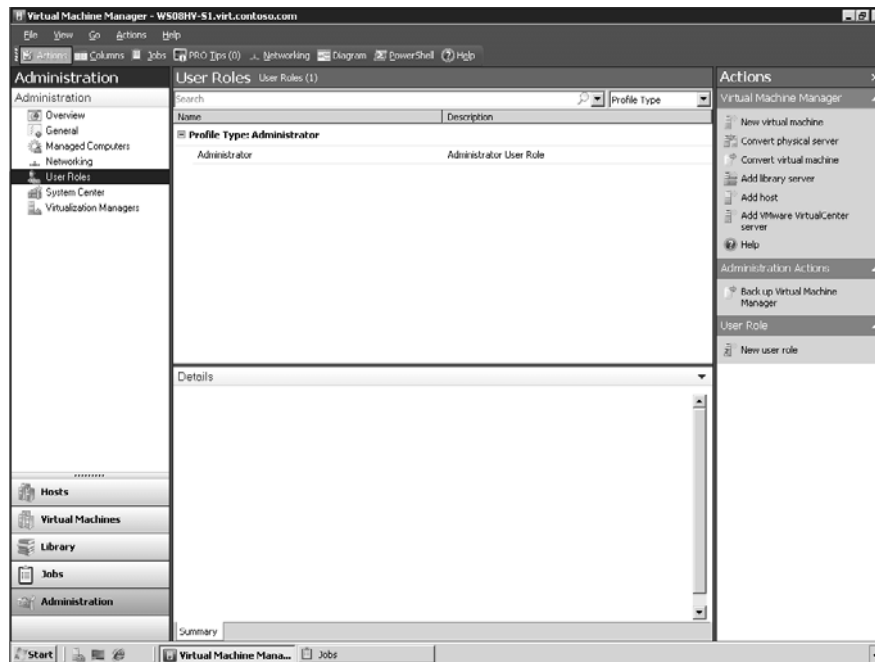


FIGURE 3-41 Managing user roles.

Now click New User Role under User Role in the Actions pane. This launches the New User Role Wizard. Type a name for the new role you will create and an optional description. Then select Delegated Administrator as the kind of role you will create. (See Figure 3-42.)

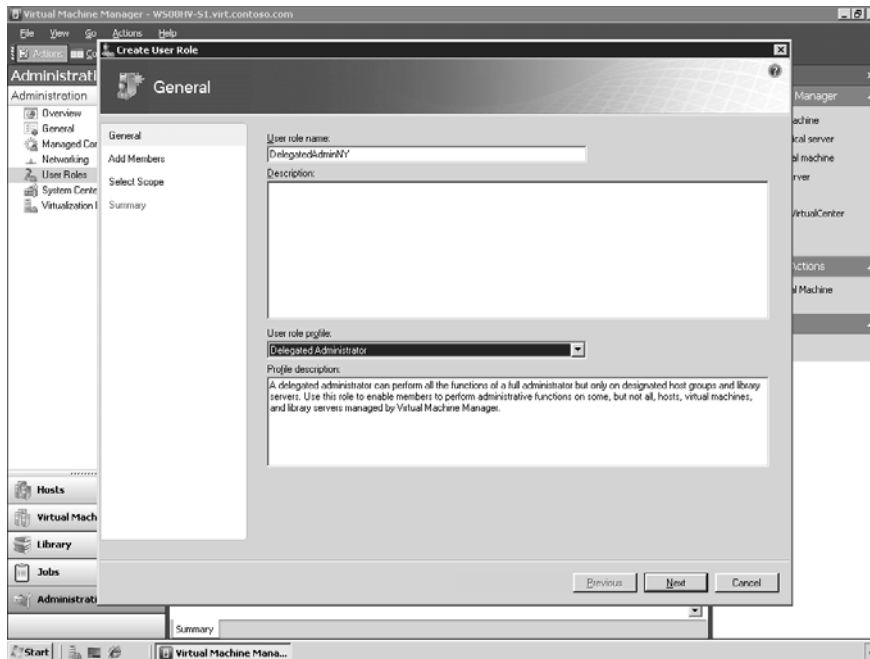


FIGURE 3-42 Creating a new Delegated Administrator role.

On the next page of the wizard, browse Active Directory to select the user accounts you want to add as members of your new role. (See Figure 3-43.)

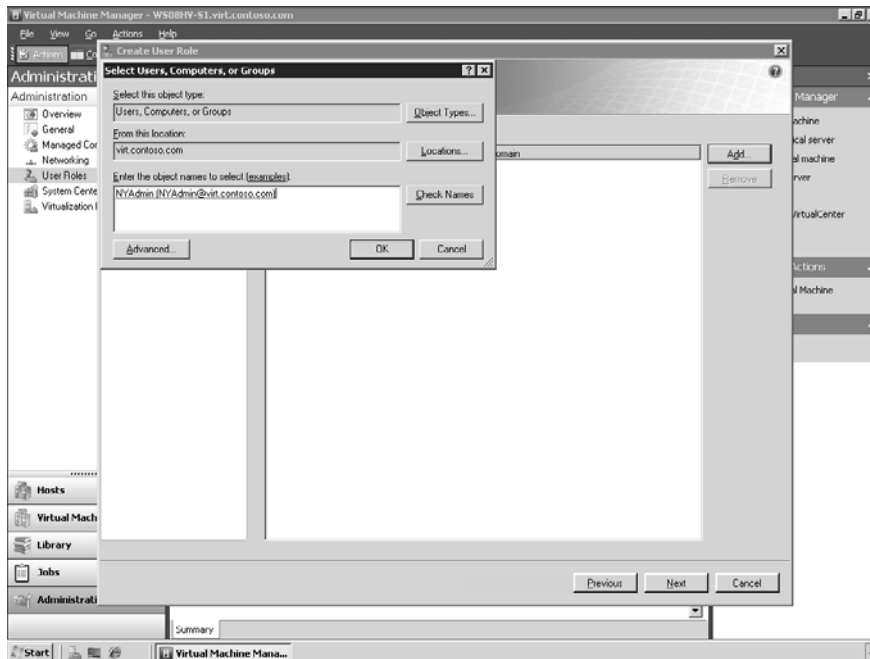


FIGURE 3-43 Adding members to the role.

On the next wizard page, specify the scope of your new role. (See Figure 3-44.)

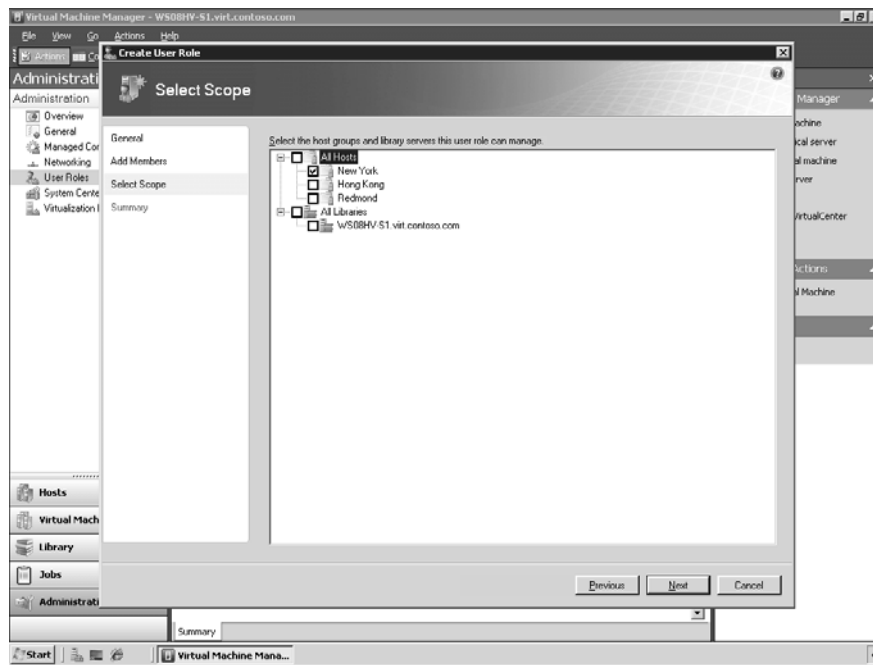


FIGURE 3-44 Specify the scope for the Delegated Administrator role.

The final page of the wizard presents a summary of the selections you have made on the previous pages. After you're satisfied you are configuring the new role appropriately, click Create to create the new Delegated Administrator role. (See Figure 3-45.)



Tip You can click View Script on the final wizard page to view the Windows PowerShell script that will be used to perform the actions you specified in the wizard. This can be useful for automation purposes. For example, you could copy the script from this role and modify it to create multiple roles in one batch operation.

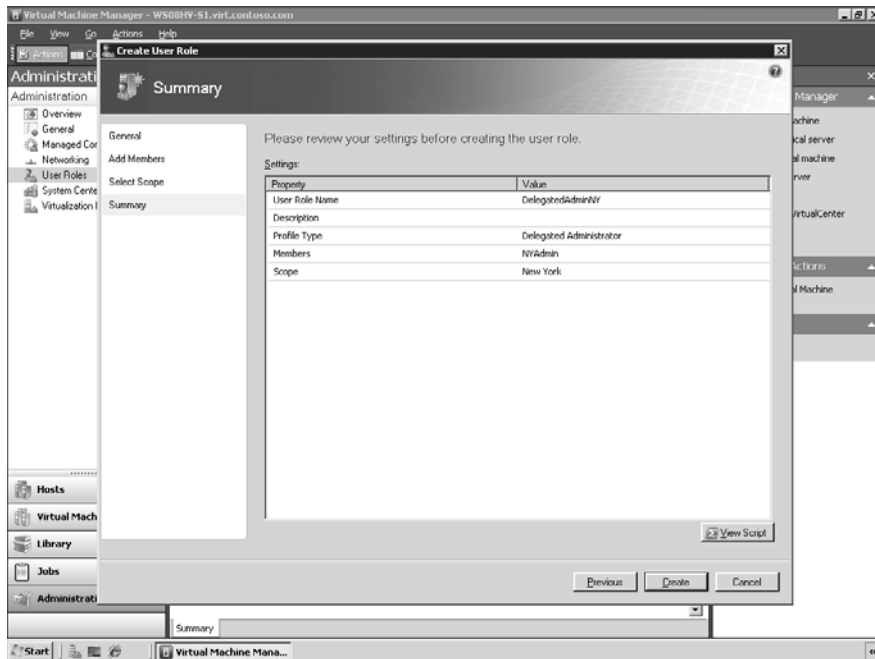


FIGURE 3-45 Summary page of Create User Role Wizard.

Creating a Self-Service User Role

If you belong to either the Administrator or Delegated Administrator role, you can also use the New User Role Wizard to create a new Self-Service User role. To do this, begin again by selecting User Roles under Administration in the Administration pane as shown in Figure 3-41 previously. Click New User Role under User Role in the Actions pane to launch the New User Role Wizard. Type a name for the new role you will create and an optional description. Now select Self-Service User as the kind of role you will create. (See Figure 3-46.)

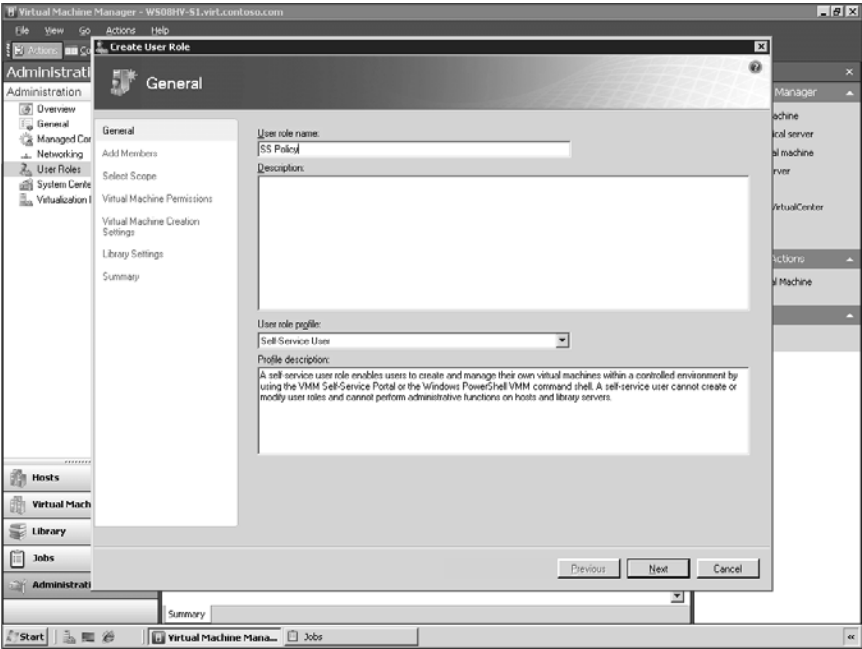


FIGURE 3-46 Creating a new Self-Service User role.

Browse Active Directory to select the user accounts you want to add as members of your new role. (See Figure 3-47.)

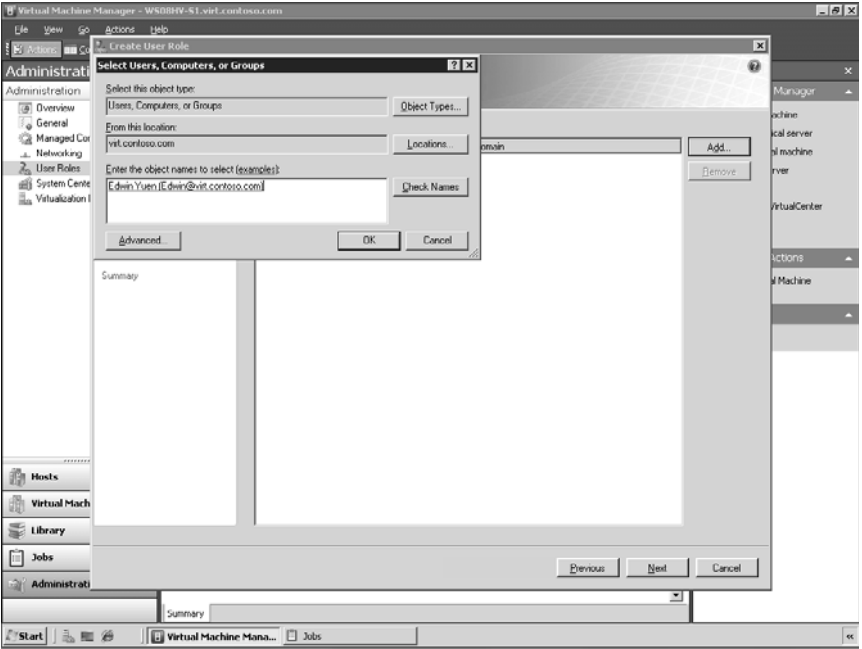


FIGURE 3-47 Adding members to the role.

Next, specify the scope of your new role. (See Figure 3-48.)

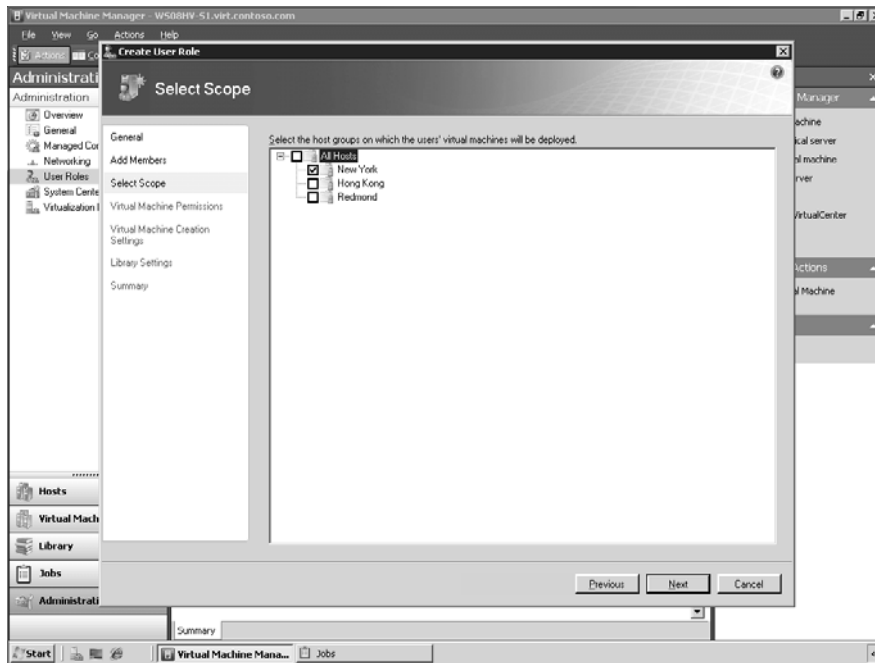


FIGURE 3-48 Specify the scope for the Self-Service User role.

Next you specify the permissions that members of this role will have for managing virtual machines running on hosts that belong to host groups that are within the scope of the role. You can either specify that role members can perform any action on the virtual machines, or you can select specific actions to allow them to perform. (See Figure 3-49.)

On the next page of the wizard, you specify whether members of this role are allowed to create new virtual machines on hosts that belong to host groups that are within the scope of the role. You can also specify which virtual machine templates the role members can use when creating their new virtual machines. (See Figure 3-50.)

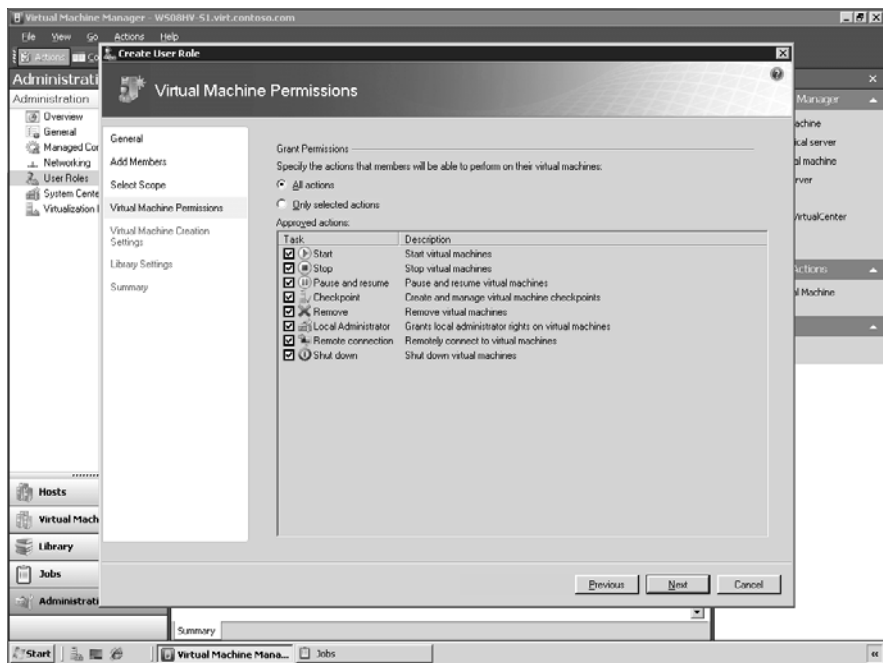


FIGURE 3-49 Specify the virtual machine permissions for the Self-Service User role.

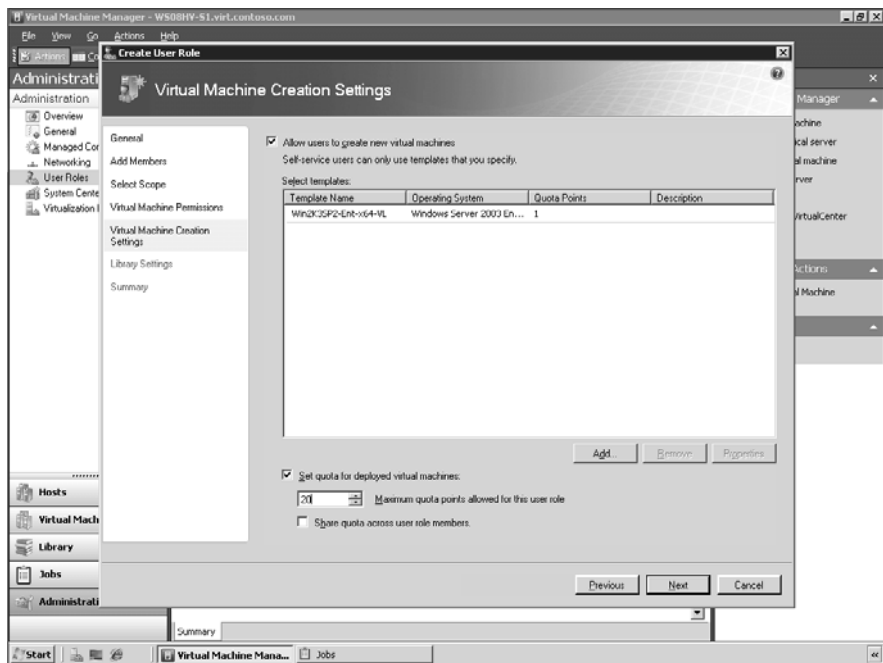


FIGURE 3-50 Specify the templates that role members can use for creating new virtual machines.

On this wizard page, you can also set a quota for deployed virtual machines for members of the Self-Service User role. A virtual machine quota in a Self-Service User role is a limit to the number of virtual machines that members of the role can deploy. Quota points are assigned to the templates that self-service users use to create their virtual machines, and they apply only to virtual machines on a virtual machine host. If a self-service user is allowed to store virtual machines, the quota does not apply to virtual machines stored in the library. When the self-service user's quota is reached, the user cannot create any new virtual machines until an existing virtual machine is removed or stored in the library.

On the next page of the wizard, you can specify whether the user is allowed to store her virtual machines in the library. (See Figure 3-51.)

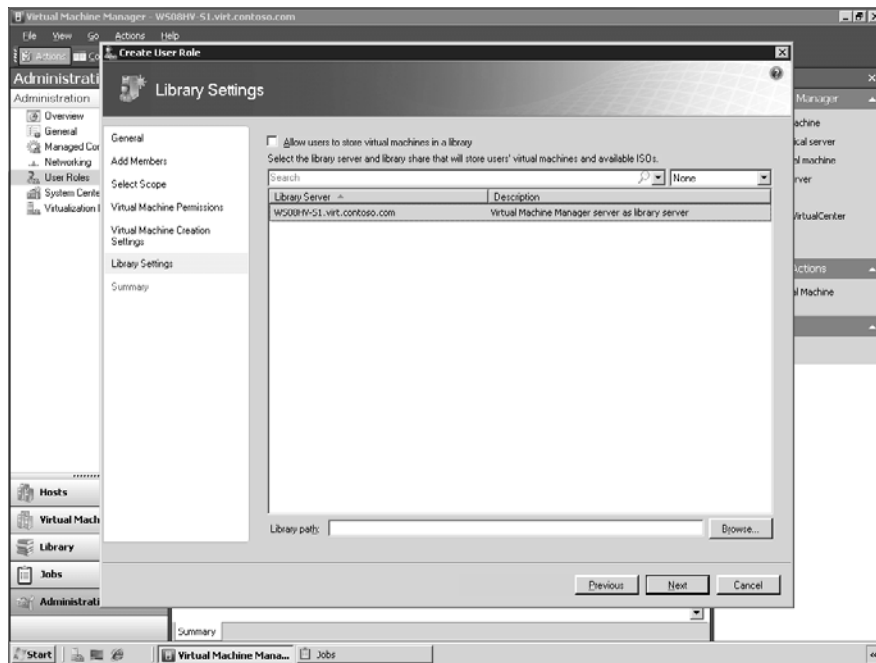


FIGURE 3-51 Specify whether role members can store their virtual machines in the library.

The final page of the New User Role Wizard displays a summary of the selections you have made. (See Figure 3-52.)

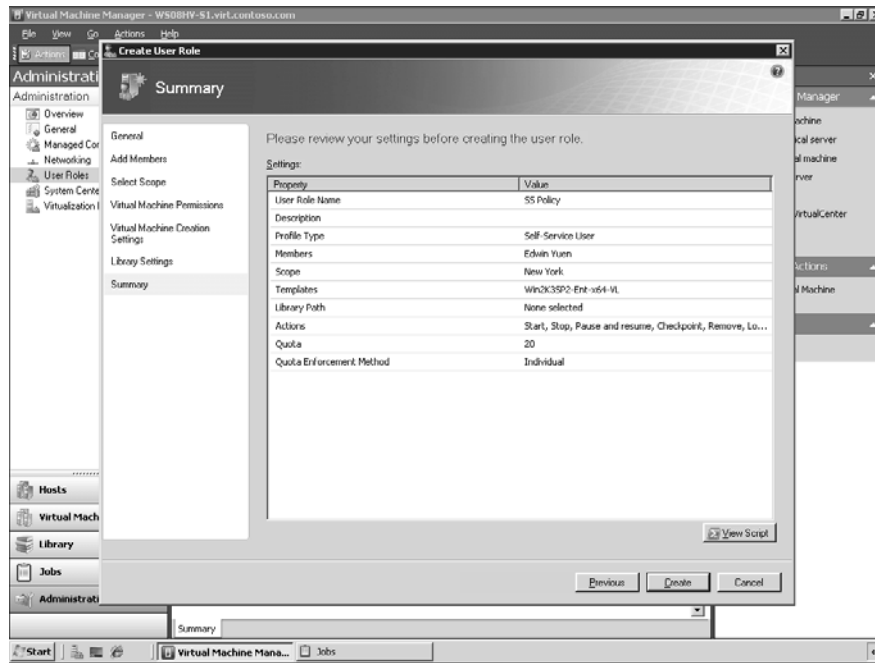


FIGURE 3-52 Summary page of the Create User Role Wizard.

Using the Self-Service Portal

The VMM Self-Service Portal provides Web-based functionality that allows users to create, manage, and operate their own virtual machines independently within a controlled environment. Setting up the Self-Service Portal involves the following steps:

1. Installing the VMM Self-Service Portal on a Web server running IIS. You can configure the Self-Service Portal on your VMM Server or on a dedicated Web server in your domain.
2. Creating a host group to use for virtual machine self-service, and moving hosts into the host group. This configuration is useful for limiting self-service users to a specific group of managed hosts.
3. Creating virtual machine templates that your self-service users can use to create their own virtual machines.
4. Creating Self-Service User roles to grant users permissions to administer their virtual machines and to allow them to create their virtual machines from templates.
5. Specifying the e-mail address of the administrator who will support the self-service users.



Tip If self-service users will use virtual machines that you have created, create the virtual machines, configure them for virtual machine self-service, and deploy the virtual machines on a host in the host group that you use for self-service.

After the Self-Service Portal has been configured, users who are members of a Self-Service User role can use a Web browser such as Internet Explorer to open the home page of the portal and log on using their domain credentials. (See Figure 3-53.)

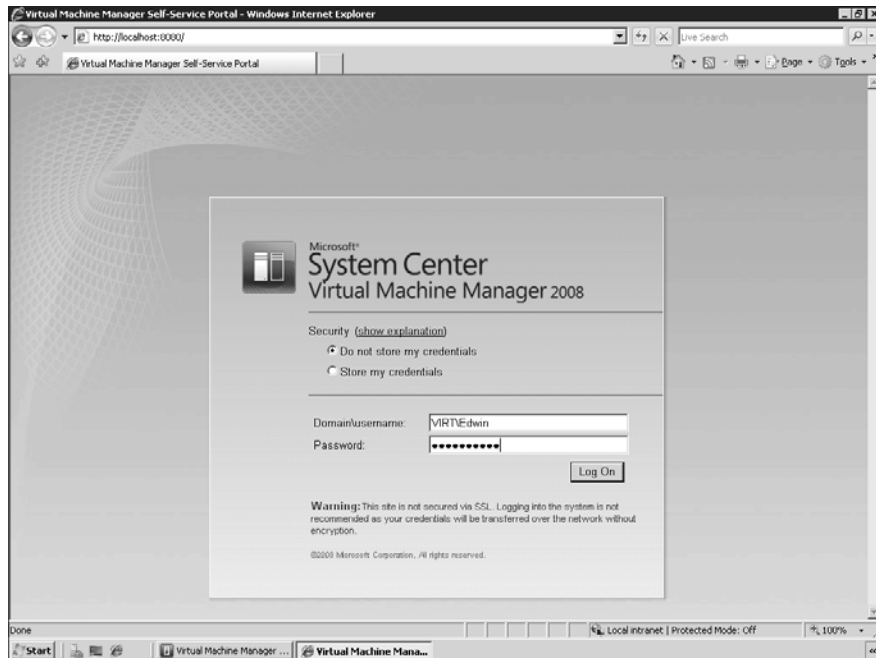


FIGURE 3-53 Logging on to the Self-Service Portal.

After members of the Self-Service User role log on, they can manage their virtual machines using the portal by clicking the Computers tab on the Portal.aspx page. By clicking List View, they can view the name, status, owner, assigned memory, disk space used, date deployed, and quota points for each virtual machine they have access to. (See Figure 3-54.) And by selecting a virtual machine, they can perform the actions they have permissions to perform as determined by the Self-Service Portal role to which they belong.

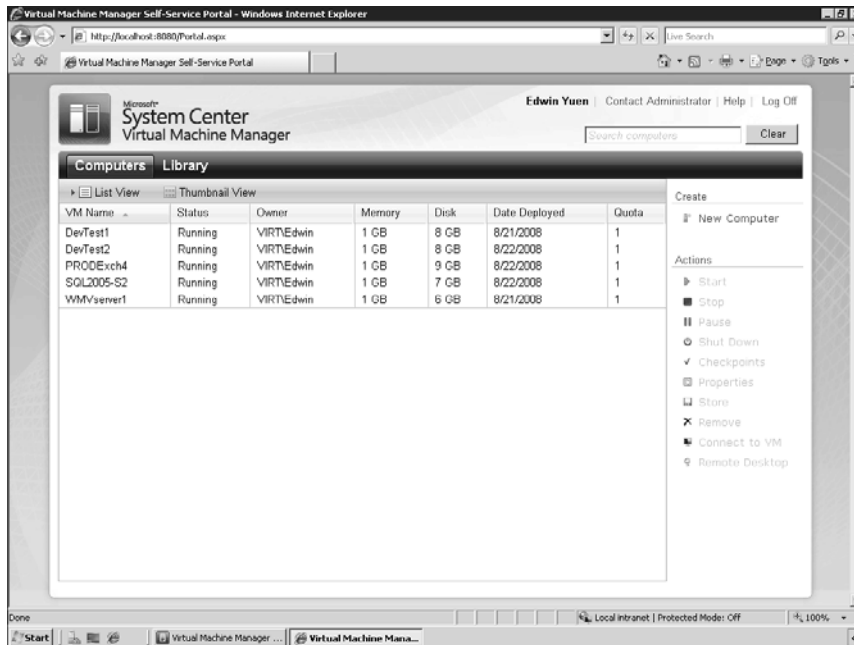


FIGURE 3-54 Viewing a list of the user's virtual machines.

By clicking Thumbnail View, they can view a thumbnail image of their running virtual machines. (See Figure 3-55.) And by selecting one of the thumbnails, they can perform the actions they have permissions to perform as determined by the role.

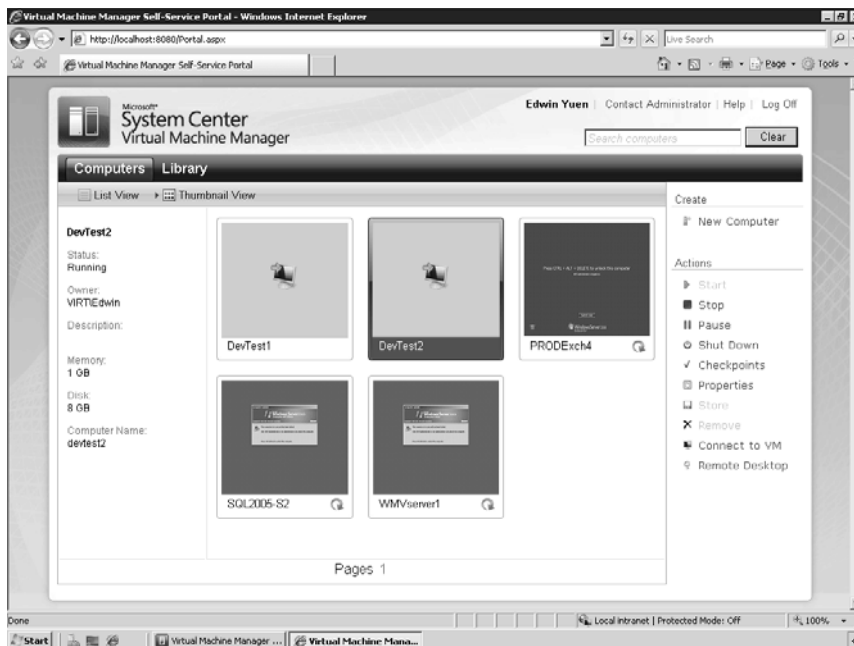


FIGURE 3-55 Viewing thumbnails of the user's virtual machines.

Finally, by clicking New Computer under Create on the right side of their portal page, the user can create a new virtual machine. (See Figure 3-56.)

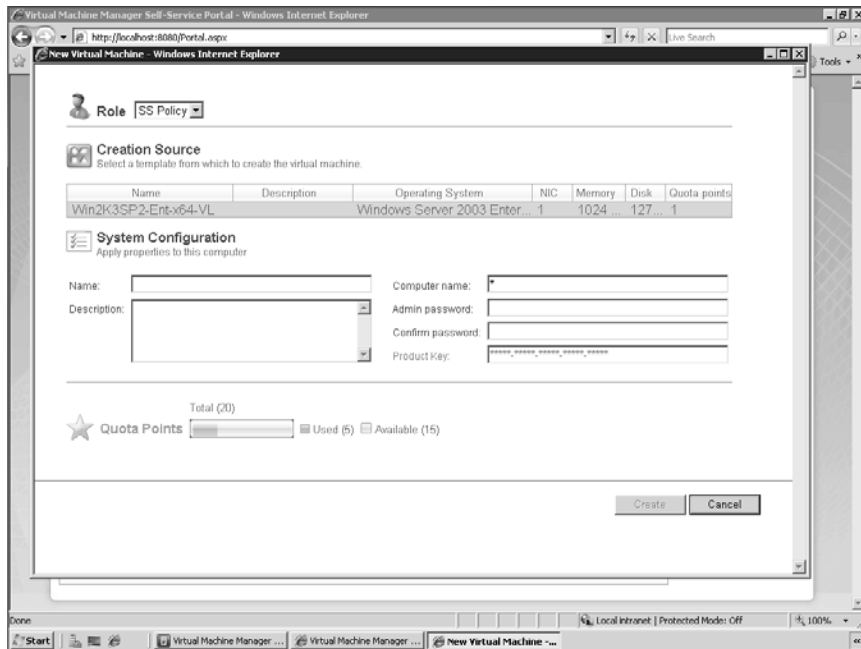


FIGURE 3-56 Creating a new virtual machine.

Key Features of VMM 2008

The overview of System Center Virtual Machine Manager 2008 provided by the previous section has already introduced you to some of the capabilities and features of VMM 2008. However, for purposes of summarization, the following are key features of VMM 2008 compared to the earlier version, VMM 2007:

Windows Server 2008 Hyper-V Management

New in this version of VMM is support for managing hosts running Microsoft Hyper-V, specifically:

- VMM 2008 has been designed to fully use the foundational features and services of Windows Server 2008 Hyper-V, including Hyper-V's 64-bit architecture and attack-hardened security model.
- VMM 2008 supports installing the Hyper-V role remotely from the VMM 2008 console.

- VMM 2008 integrates with the new Failover Clustering feature in Windows Server 2008 to allow you to create fault-tolerant and cluster-aware virtual machines.
- VMM 2008 supports all Hyper-V functionality while providing VMM-specific functions such as Intelligent Placement, the VMM Self-Service Portal, and the integrated VMM library.

VMware (VI3) Management

New in this version of VMM is support for managing VMware ESX Server hosts running within a VMware VI3 environment, specifically:

- VMM 2008 integrates multihypervisor management into one tool with its support for virtual machines running on VMware ESX infrastructure.
- VMM 2008 provides comprehensive support for VMware VI3, including moving virtual machines among virtual hosts with no downtime by using VMotion through integration with VMware's VirtualCenter.
- VMM 2008-specific features—such as Intelligent Placement, consolidation candidate recommendations, and others—can be run against virtualized infrastructure on any supported platform, including VMware VI3.
- Windows PowerShell scripts for customization or automation are also supported across Hyper-V, VMware ESX, and Virtual Server implementations.

Windows Server 2008 Failover Clustering Integration

With greatly expanded support for failover clusters, this new version of VMM has enhanced high-availability capabilities for managing mission-critical virtual machines. Specifically, these capabilities include the following:

- VMM 2008 is now fully cluster aware and can detect and manage Hyper-V host clusters as a single unit.
- VMM 2008 now has automatic detection of virtual hosts that are added or removed from the cluster, which eases the burden on the administrator to manage this function.
- VMM 2008 creates a highly available virtual machine in a one-step process: the administrator selects a check box that designates a virtual machine as highly available. Behind the scenes, VMM 2008 orchestrates the creation of that highly available virtual machine by instructing the Intelligent Placement feature of VMM 2008 to recommend only hosts that are part of a host cluster.
- VMM 2008 includes improved highly available virtual machine management features, such as the Failover Cluster Management console for performing cluster-related tasks

such as designation and management of cluster reserves, letter-less disk drives, and guest clusters, and so on.

- VMM 2008 also now supports VMware host clusters in which the nodes of the cluster are VMware ESX Servers.

Delegated Administration Based on Role-Based Authorization

This new version of VMM now includes the following support for delegated administration based on role-based authorization:

- VMM 2008 allows administrators to create new user roles of the following types:
 - Administrator role
 - Delegated Administrator role
 - Self-Service User role
- VMM 2008 lets you define a scope for the Delegated Administrator or Self-Service User role to define which objects (such as host groups and Library Servers) the user can take actions on.
- VMM 2008 also lets you define permissions for a Self-Service User role to define what actions a user can perform on his virtual machines.

Performance and Resource Optimization (PRO)

VMM 2008 includes a new feature called Performance and Resource Optimization (PRO) that can dynamically respond to failure scenarios or poorly configured components that are identified in hardware, operating systems, or applications. Specifically, PRO provides these capabilities:

- Working via PRO-enabled management packs and using System Center Operations Manager 2007's monitoring capabilities, PRO can either alert an administrator of an unhealthy system or application state and recommend corrective action, or it can respond automatically on its recommendations to provide a self-healing virtualization infrastructure.
- Because of the highly granular level of monitoring available to PRO, a wide range of hardware, operating system, or application variables can trigger PRO to take corrective action.
- PRO's capabilities are also available to VMware ESX or Virtual Server hosts, allowing administrators to manage their entire virtualized environment regardless of the virtualization platform they are using.

Key Benefits of VMM 2008

The key benefits of using System Center Virtual Machine Manager 2008 to manage your entire virtualized environment include the following:

- **Designed for virtual machines running on Windows Server 2008 Hyper-V** Hyper-V is the next-generation, hypervisor-based virtualization platform from Microsoft that is designed to offer high performance, enhanced security, high availability, scalability, and many other improvements. VMM 2008 is designed to take full advantage of these foundational benefits through a powerful yet easy-to-use console that streamlines many of the tasks necessary to manage virtualized infrastructure. Administrators can also manage their traditional physical servers right alongside their virtual resources through one unified console.
- **Support for Microsoft Virtual Server and VMware ESX Server** VMM 2008 can now manage a VMware ESX virtualized infrastructure in conjunction with VMware VirtualCenter Server. This means that administrators running multiple virtualization platforms can now rely upon a single tool to manage virtually everything within their infrastructure. With its compatibility with VMware VI3 through VirtualCenter Server, VMM 2008 now supports features such as VMware's VMotion and can even provide VMM-specific features such as Intelligent Placement to VMware ESX Servers.
- **Performance and Resource Optimization (PRO)** The PRO feature of VMM 2008 enables dynamic management of virtual resources through PRO-enabled management packs for System Center Operations Manager 2007. PRO lets administrators establish remedial actions for VMM to execute if poor performance or pending hardware failures are identified. As an open and extensible platform, PRO also encourages partners to design custom management packs that promote compatibility of their products and solutions with PRO's powerful management capabilities.
- **Maximizing datacenter resources through consolidation** A typical physical server in the datacenter operates at only 5 to 15 percent CPU capacity. VMM 2008 can assess and then consolidate suitable server workloads onto a virtual machine host infrastructure, thus freeing up physical resources for repurposing or retirement. Through physical server consolidation, continued datacenter growth is less constrained by space, electrical, and cooling requirements.
- **Easier machine conversions** Converting a physical machine to a virtual one used to be a daunting undertaking that was slow, problematic, and typically required you to halt the physical server. Thanks to the enhanced Physical-to-Virtual (P2V) conversion in VMM, however, P2V conversions can now become routine. In addition, VMM 2008 also provides a straightforward wizard for converting VMware virtual machines to VHDs via a quick and easy Virtual-to-Virtual (V2V) transfer process.

- **Fast provisioning of new machines** In response to new server requests, an agile IT department can now use VMM 2008 to deliver new servers to its business clients anywhere in the network infrastructure with a very quick turnaround. VMM 2008 enables this agility by providing IT administrators with the ability to deploy virtual machines in a fraction of the time it would take to deploy a physical server. Through one console, VMM 2008 allows administrators to manage and monitor virtual machines and hosts across an organization to ensure they are meeting the needs of business groups within that organization.
- **Minimizing virtual machine guesswork in deployment via Intelligent Placement** VMM 2008 does extensive data analysis of a number of factors before recommending which physical server should host a given virtual workload. This is especially critical when administrators are determining how to place several virtual workloads on the same host machine. And with access to historical data provided by System Center Operations Manager 2007, the Intelligent Placement process is able to factor in past performance characteristics to ensure the best possible match between the virtual machine and its host hardware.
- **Delegated virtual machine management** Virtual infrastructures are commonly used in test and development environments, where there is constant provisioning and tear down of virtual machines for testing purposes. This new version of VMM has a thoroughly reworked and improved Web-based Self-Service Portal through which administrators can delegate this provisioning role to authorized users while maintaining precise control over the management of virtual machines.
- **Organizing virtual machine components** To keep a datacenter's virtual house in order, VMM 2008 provides a centralized library to store various virtual machine building blocks, such as offline machines, templates, virtual hard disks, and other virtualization components. With the library's easy-to-use, structured format, IT administrators can quickly find and reuse specific components and thus remain highly productive and responsive to new server requests and modifications. Additionally, multiple Library Servers can be deployed throughout the organization if needed for increased scalability.
- **A rich management and scripting environment that uses Windows PowerShell** The entire VMM 2008 application is built on the command line and scripting environment provided by Windows PowerShell. This version of VMM adds more Windows PowerShell cmdlets and View Script controls that allow administrators to explore customizing or automating operations at an unprecedented level.

Usage Scenarios for VMM 2008

Finally, we'll conclude this chapter by briefly describing four common usage scenarios involving System Center Virtual Machine Manager 2008:

- Server consolidation
- Provisioning of virtualized resources
- Business continuity
- Performance and resource optimization

Server Consolidation

One of the key scenarios that can take maximum advantage of the features found in VMM 2008 is server consolidation. By consolidating physical servers, organizations can realize significant business benefits, including power savings and increased asset utilization. Organizations can take one of two approaches to server consolidation using VMM 2008:

- A conservative, incremental approach whereby new applications are added to the virtual infrastructure while old applications remain on dedicated physical assets until retired.
- A more aggressive approach that takes the form of a server consolidation project where the IT group identifies candidate applications for virtualization and then migrates the identified workloads to appropriate physical resources.

VMM 2008 facilitates an aggressive approach to server consolidation by providing the following capabilities:

- Integration with System Center Operations Manager (OpsMgr) 2007 to enable VMM 2008 to identify potential consolidation candidates within the OpsMgr database.
- A straightforward P2V conversion process that uses BITS to move data to the virtual machine and that can be automated using Windows PowerShell scripts.
- A straightforward V2V conversion process that allows migration of a virtual machine running on VMware ESX Server to either Virtual Server 2005 R2 or Hyper-V.
- An Intelligent Placement feature that helps identify the best host for running a virtualized workload.

Provisioning of Virtualized Resources

Another key scenario for VMM 2008 is facilitating the provisioning of virtualized resources to users and business groups who need them. By using virtualization, IT administrators no longer have to procure and configure physical servers for new applications, a task that sometimes takes weeks or months. Instead, IT administrators can provision new virtual ma-

chines in a matter of minutes using VMM 2008. And administrators can also delegate this provisioning role to authorized users by creating delegated administrators for groups and departments while maintaining precise control over the management of virtual machines. Authorized users can also access a Web page that enables them to provision their own virtual machines within predefined restraints laid down by administrators.

VMM 2008 enables such provisioning of virtualized resources by providing the following capabilities:

- Support for creating Administrator, Delegated Administrator, and Self-Service User roles and defining scope of management action and virtual machine permissions for members of these roles.
- A Web-based Self-Service Portal that an administrator can use to provide ordinary users with the capability to easily create and manage their own virtualized resources.

Business Continuity

Business Continuity Planning refers to the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption. VMM 2008 can help ensure an organization's business continuity by enabling the management virtualized resources running on Windows Server 2008 to be integrated with the following:

- An enterprise-level backup and recovery platform such as System Center Data Protection Manager 2007
- Quick migration of virtualized workloads between nodes of a Windows Server 2008 failover clustering to ensure high availability of business-critical resources

Performance and Resource Optimization

Performance and Resource Optimization (PRO) is a feature of VMM 2008 that helps administrators ensure that virtual machine hosts and their virtual machine guests are operating in the most efficient possible manner. PRO leverages OpsMgr 2007 to monitor a complete end-to-end IT infrastructure, including hardware, host and guest operating systems, and applications. PRO also enables an administrator to create operational policies and automatically take actions based on those policies. For instance, when an event occurs that triggers a policy, PRO can be configured to present the issues to the administrator along with recommended resolutions. PRO can also be configured to automatically implement the preconfigured corrective actions for lights-out operations.

Additional Resources

The resources listed in this section were either referred to in the chapter or provide additional information concerning concepts and products discussed in this chapter.

General

A general overview of the features and benefits of VMM 2008 can be found on the VMM product information page at <http://www.microsoft.com/systemcenter/virtualmachinemanager/en/us/default.aspx>. Be sure also to look at the other Microsoft System Center products at <http://www.microsoft.com/systemcenter/en/us/products.aspx>.

Deploying and Using VMM

At the time of this writing, the System Center Virtual Machine Manager TechCenter on Microsoft TechNet has only planning and operations manuals for the 2007 version of VMM. See <http://technet.microsoft.com/en-us/scvmm/default.aspx>. Much of this information should still be relevant for the new 2008 version of VMM, however, and you should stay tuned to this site for updated information soon for VMM 2008.

System Center Blog

Find all the latest information concerning VMM and other Microsoft System Center products via Nexus SC—the System Center Team Blog at <http://blogs.technet.com/systemcenter>.

VMM Forums on TechNet

To obtain help with your questions and problems concerning VMM, and to help others, use the VMM forums on Microsoft TechNet at <http://forums.microsoft.com/TechNet/default.aspx?ForumGroupID=489&SiteID=17>.

Chapter 4

Application Virtualization—App-V

Another important component of Microsoft's Virtualization 360 vision is application virtualization, which refers to any technology that lets you decouple applications from desktop operating systems to dynamically deliver applications on demand to your users. When you run applications centrally instead of installing them on each user's computer, software update management is simplified, application-to-application conflicts are reduced, and application compatibility regression testing is made easier.

Microsoft's primary platform for delivering application virtualization solutions is Microsoft Application Virtualization (App-V) 4.5, formerly known as SoftGrid Application Virtualization. App-V is part of the Microsoft Desktop Optimization Pack (MDOP) for Software Assurance (SA) version R2. This chapter examines how App-V works and how it can be used to deliver applications to users who need them. The chapter also summarizes the key features of App-V, the benefits App-V can provide organizations, and different usage scenarios for App-V.

Understanding App-V

Microsoft Application Virtualization provides the ability to deliver applications to end users without actually installing the applications on their client computers. This section is designed to help you understand App-V and covers the following topics:

- App-V terminology
- How App-V works
- App-V components
- App-V architecture

App-V Terminology

The following are some of the key concepts and terms you need to understand when working with App-V:

- **Active Upgrade** A feature of App-V that provides for automatically upgrading an application on all end-user computers at their next publishing refresh cycle. To gain the benefit of this feature, you must have either an App-V Management Server or an App-V Streaming Server in your environment.
- **Content Folder** A directory, named Content by default, where the virtual application package contents (.sft files) are stored and streamed from. This directory can be in a

shared folder on your App-V Management Server, in a highly available Distributed File System (DFS) share, or on a storage area network (SAN) or network-attached storage (NAS) device.

- **Desktop Client** An application that resides on a Microsoft Windows-based computer desktop and that communicates and authenticates with the Microsoft System Center Virtual Application Server to receive the application code and allow a sequenced application to be run locally.
- **Dynamic Suite Composition** A feature that enables a virtual application package to allow dependent plug-ins or middleware packages to use the primary package's registry settings so that the packages behave and interact with one another in the same way as if they were installed locally on a computer. This feature allows applications to be sequenced in separate virtual environments yet selectively communicate with each other.
- **Installation directory** The directory where the installer for the application virtualization sequencer places its files.
- **Management Console** A Microsoft Management Console (MMC) snap-in that is used to administer a specific deployment of the App-V platform that includes all of the components that are managed by a single data store.
- **Management Server** One of two App-V server types (the other being Streaming Server) from which a sequenced application package can be streamed. The Management Server also offers other services, such as publishing, management, reporting, and so on.
- **Microsoft Application Virtualization for Terminal Services** Refers to the client component of App-V running in a Terminal Services environment.
- **Publishing an application** This makes an application available to authorized users whose computers have the App-V Client installed. Publishing delivers the icons (.ico file), package definition information, and content source location (.osd file) to each computer where the App-V Client has been installed.
- **Q: drive** The default virtual application client drive from which sequenced applications are "run". For more information, see the sidebar titled "Direct from the Source: The Q: Drive" later in this chapter.
- **Sequenced application** An application that has been monitored by the Sequencer, broken up into primary and secondary feature blocks, streamed to a computer running the App-V Terminal Services Client or the App-V Desktop Client, and that can run inside of its own virtual environment. A sequenced application is an application that has been transformed from a traditional installed application to one that runs inside an App-V virtual environment.

- **Sequenced application package** The files that make up a virtual application and allow the virtual application to run. These files are created after sequencing and include .osd, .sft, .sprj, and .ico files.
- **Sequencer** A utility that monitors and records the installation and setup process for applications so that an application can be sequenced and run in the virtual environment. This type of server is best suited for a branch location.
- **Sequencing** The process of creating an application package by using the Application Virtualization Sequencer. In this process, an application is monitored, its shortcuts are configured, and a sequenced application package is created containing the .osd, .sft, .sprj, and .ico files. Sequencing is performed by using the Sequencing Wizard, which walks you through sequencing an application, including configuring a package, installing the application or applications to be sequenced, and sequencing the application package for streaming.
- **Sequencing computer** The computer used to perform sequencing and create a sequenced application package.
- **Streaming** The process of obtaining content from a sequenced application package (.sft file) starting with feature block 1 and then obtaining additional blocks as needed.
- **Streaming Server** One of two App-V server types (the other being Management Server) from which a sequenced application package can be streamed. The Streaming Server only streams applications to the client machines and does not offer other services, such as publishing, management, reporting, and so on.
- **Terminal Services Client** An application that resides on a terminal server and that communicates and authenticates with the App-V Server to receive the application code and allow a sequenced application to be run locally.
- **Virtual application** An application packaged by the Sequencer to run in a self-contained, virtual environment that contains the information necessary to run the application on the client without installing the application locally.

How App-V Works

App-V lets you create virtual applications, which are applications that have been packaged so that they can run within a self-contained virtual environment or “sandbox” on client computers. This virtual environment contains all the information needed to be able to run the virtual application on the client computer and runs within the App-V Client software on the client computer. After you have packaged applications and deployed the App-V Client software to client computers, you can deliver these applications to the client computers in various ways that resolve many of the issues associated with the traditional application deployment life cycle. The sections that follow examine these processes in more detail.

App-V Virtual Environment

The App-V virtual environment is a run-time container that defines the resources available to application processes launched from a sequenced application package. The resources that are defined by the virtual environment include

- **Virtual COM** A subsystem that manages COM objects created by application processes running in the virtual environment and prevents conflict with the same objects created outside the virtual environment.
- **Virtual directory** An opaque directory where only files and subdirectories defined in the virtual application package or created through interaction with an application in a virtual environment are visible. Any files that are in an identically named local directory are not visible to the virtual application.
- **Virtual file** A file name within the virtual environment that is mapped to an alternate target location. A virtual file appears alongside other files in the containing directory, regardless of whether that directory is virtual or local.
- **Virtual file system** A subsystem that intercepts and redirects file system requests from application processes running in a virtual environment. These requests are processed based on the virtual files and directories defined in the application package and created or modified through interaction with a virtual application.
- **Virtual registry** A subsystem that intercepts and redirects registry requests for keys and values from application processes running in a virtual environment. The redirection is based on the registry information defined in the application package and created or modified through interaction with a virtual application.
- **Virtual services** A subsystem that acts as the Service Control Manager for services running in a virtual environment

This virtual environment is created by the App-V Client software, which runs on the client computer and enables the end user to interact with virtualized applications after they have been delivered to the client computer. For more information concerning App-V Client software, see the section titled “App-V Clients” later in this chapter.

Sequencing Applications

Before you can use App-V to deliver applications to users on client computers, you first need to package the applications for delivery. The process of packaging an application to enable it to run within its own self-contained virtual environment on a client computer is called *sequencing the application*. Sequenced applications are virtualized and are completely isolated from one another, which eliminates any application conflicts that might occur between two applications.

A sequenced application package contains four types of files that make up a virtual application and allow the virtual application to run. These files are created after sequencing and include the following types of files:

- **.ico file** This is the type of file for the icon on the client's desktop used to launch a sequenced application.
- **.osd file** This is an XML-based Open Software Descriptor file that instructs the client on how to retrieve the sequenced application from the App-V Management Server or Streaming Server and how to run the sequenced application in its virtual environment.
- **.sft file** This type of file contains one or more sequenced applications that the Sequencer has packaged into streaming blocks, as well as the associated delivery information. An .sft file is stored on each server that must stream the packaged applications to a client.
- **.sprj file** This is an XML-based Sequencer Project file in which the Sequencer stores its Exclusion Items and Parse Items information. An .sprj file is used in the creation of application records and when upgrading a package.

In addition, a sequenced application package can also contain a Microsoft Windows Installer (.msi) file that can be used for standalone distribution of virtual applications, for publishing application packages using an electronic software distribution (ESD) system such as Microsoft System Center Configuration Manager 2007, or for both purposes.

For more information concerning sequencing applications, see the sections titled "App-V Sequencer" and "Using the Sequencer" later in this chapter.

Publishing Applications

After an application has been sequenced to create a virtual application package consisting of the aforementioned files, the application must be published on the App-V Management Server. Publishing an application delivers the icons, package definition information, and content source location to each client that has the App-V Client installed. There are three publishing delivery methods supported by App-V:

- Using the App-V Management Server
- Using an ESD system such as System Center Configuration Manager 2007
- Standalone delivery

For organizations that already have an existing ESD system in place, using this publishing delivery mechanism provides the benefits of reducing the cost of acquiring and deploying additional hardware, operating systems, and database licenses. Leveraging your existing ESD infrastructure can also help your organization avoid the support issues associated with needing to maintain two infrastructures.

If you use ESD as your publishing delivery mechanism, you can choose from the following three approaches for publishing the application to the clients:

- **MSI files** Uses Microsoft Windows Installer (.msi) files
- **MSI Manifest** Uses the MSI Manifest contained in the .msi file.
- **SFTMIME commands** Uses a command-line window and SFTMIME commands for adding the applications and loading the .sft file.

Streaming Packages

After an application has been published and its .ico and .ocd files have been streamed to the client, the virtual application package or .sft file must be delivered to the client. App-V supports various ways of doing this, including using the App-V Management Server, an Internet Information Services (IIS) Web server, a file server, standalone delivery, or a distribution point running IIS within a System Center Configuration Manager 2007 environment.

The first time a user double-clicks on an application icon that has been placed on a computer via the publishing process, the App-V Client first performs authorization and license checking. The client then begins streaming the virtual application package content (.sft file) from the configured streaming source location. The way this works is that the .sft file is mounted in RAM on the streaming server, which then delivers the application in blocks of 32 KB size by default over the wire to the client. The streaming source location is typically a server that is accessible by the user's computer, but some electronic distribution systems such as System Center Configuration Manager 2007 can distribute .sft files to a folder on the user's computer and then stream the package from that local folder. A streaming source location for virtual application packages can even be set up on a computer that is not a server—that is, on a workstation. This type of solution can be especially useful in a small branch office location that has no server.

Virtual Application Management

App-V greatly simplifies application deployment by helping you resolve several key issues that often arise during the traditional application management life cycle:

- App-V can help resolve the kind of problems that can arise when you install two applications that are incompatible with one another onto the same computer. Because each virtual application deployed using App-V runs within its own isolated virtual environment, registry and file conflicts are significantly reduced between different virtual applications running on the same client computer.

- App-V can help reduce or eliminate the time-consuming regression testing that is needed before deploying applications onto client computers to ensure that application-compatibility issues are detected before the applications are installed.
- App-V can help reduce the headache of maintaining applications installed on client computers by applying service packs, security fixes, and other types of software updates.
- App-V helps prevent the mess that can result when applications that are no longer needed by users are uninstalled from their computers but leave remnant files and registry settings that can create conflicts later on when other applications are installed.

For more information on how App-V helps resolve these problems and other kinds of issues associated with the traditional application management life cycle, see the sidebar titled "Direct from the Source: App-V and the Application Management Life Cycle" in this chapter.

Direct from the Source: App-V and the Application Management Life Cycle

Every organization faces the challenges of deploying, updating (that is, installing patches, service packs, and upgrades), supporting (such as troubleshooting, license compliance, and training), and terminating all the applications in the enterprise in an ongoing cycle. There are many diverse solutions to this problem, but most of these solutions target only one or two areas of this life cycle.

Deployment is the initial process that organizations take to install their applications onto the client machines. This can be done using any of several traditional methods, ranging from having a support engineer touch every client PC with the install media to remotely using an electronic software distribution method to having the client access a terminal server (or Citrix XenApp server) remotely.

Updates are a natural and necessary process in the application management life cycle. As applications gain maturity in the market place, they will undoubtedly be revised and updated through service packs or hot fixes. It is the burden of the support engineer in an enterprise to update every client PC that has a particular revised application installed on it.

Providing support for the entire library of applications in an enterprise environment can be a daunting task. Issues from the most basic elements of application conflict to users inadvertently damaging their own application installations by deleting critical files can result in considerable overhead to an organization's support team.

Termination of installed applications is the last phase of the application management life cycle. Applications are eventually replaced or retired and, as such, need to be removed from the client environment. In a traditional management model, this might necessitate the support engineer visiting those clients PCs and uninstalling that application. In doing so, it is not 100 percent guaranteed that the process will remove all of the files and registry entries, meaning some are left to be orphaned and possibly to cause an issue later on.

One of the most basic challenges that enterprises encounter with the standard application management life cycle is the possibility that two or more applications will conflict with each other. When an application is allowed to install onto a host or client computer, its programmed behavior is to add or modify files and registry settings on that client's operating system. If that application did not add or modify settings in the registry and was contained exclusively in its own directory on the file system, conflicts would never occur. However, because thousands of applications have been made available since 1995, the application will almost always place its own files (.dll, .vxd, .sys, and so on) in numerous directories throughout the file system. It will also populate the registry of that client with its own values or modify existing values. One of the advantages of deploying applications this way is that they will take advantage of the local resources on the device onto which they were installed.

Having incompatible applications on a system would not be so frequent an occurrence if enterprises ran only one or a very select group of applications. Because most enterprises need to run countless applications, ending up with applications that conflict with one another is almost guaranteed. Until App-V Application Virtualization, the solution for many organizations was to separate these applications by placing them on different computers. In essence, a user would have two or more computers on her desk, one to run Application A and another separate computer to run Application B, although one of these computers could be a virtual machine running on the user's physical computer. Although this is a possible solution, it is very impractical from an expense and support perspective.

Applications that are App-V enabled are never allowed to install or modify the local file system or local registry. When an application is App-V enabled, it is made to run inside its own virtual environment. (See Figure 4-1.) Contained inside of this virtual environment are all the files, registry information, fonts, COM, embedded services, and environment variables that the application normally would have installed and been expected to use on the client PC. Instead, with all of these assets residing inside the virtual environment, the application leverages them from this virtual environment and remains isolated from other applications, which are also running inside of their own separate virtual environment. The process of creating the virtual environment is known as sequencing.

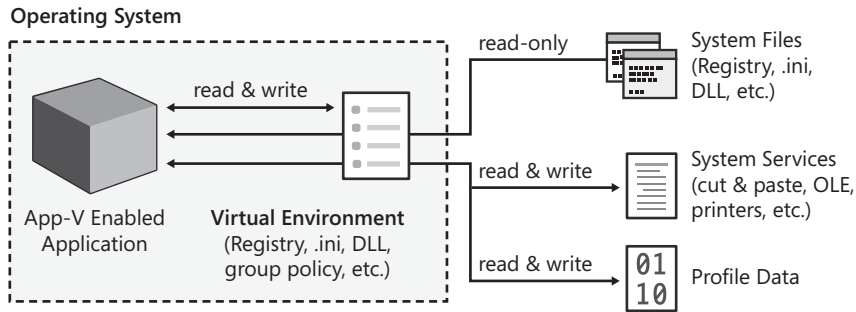


FIGURE 4-1 The App-V virtual environment.

The Sequencer is the component in the App-V system that is vital in creating the SystemGuard for an application or suite of applications. App-V-enabled applications will be able to use local and network drives, CPU, RAM, the local Windows Installer Service, and other local resources on the App-V Client to which they are streamed to, cached, and run.

Regression testing has always been a top priority inside enterprises when the enterprise is deploying any new or updated application. In enterprises with formalized processes for doing this, every application is tested against every known configuration that could exist within that organization. This could, and often does, exceed 40 hours of effort for a single application. With an App-V-enabled application, however, this is reduced to only the time required to sequence that application. When the application is deployed, it is isolated from any other applications that were sequenced or that are still locally installed on the client, guaranteeing a conflict-free environment.

Updates

It is a natural part of an application's life cycle to have updates in the form of service packs or hot fixes become available. These updates need to be applied to that application, and this is often done by having the support engineer visit every client PC or terminal server machine and manually apply the update in question. This process can be very time consuming, and it can also increase the likelihood of causing an application conflict because the update modifies files and registry settings on the client. With an App-V-enabled application, updates are performed centrally and occur at only one time. The sequence engineer takes the original App-V-enabled application's package back to a clean sequencer workstation and performs a package upgrade, appending the original package with the updates. This updated package is then used to replace the original package on the App-V Server, and the App-V Client receives the updated files seamlessly.

Support

In addition to eliminating application conflicts, the App-V platform can solve many other support-related issues. When you run each application inside of its own protected SystemGuard environment, App-V-enabled applications remain immune to users inadvertently or intentionally deleting critical files needed by that application to run. Because the App-V-enabled applications are running inside of their own SystemGuard environment, users and local system administrators never see any of the application's files or registry entries if they look at those local resources. This can effectively reduce the number of help desk calls an organization requires. Another issue facing support personnel inside an enterprise is the concern surrounding licensing. App-V enables organizations to control the number of users who can gain access to App-V-enabled applications concurrently. This licensing feature is administered centrally from the sole administrative utility for Microsoft App-V Application Virtualization, the App-V Management Console.

Termination

At the end of an application's life cycle, it is time to retire or terminate that application. In a traditional method, someone is required to visit every client PC or terminal server machine and uninstall that application. This approach has the potential to leave some files and registry settings orphaned and create conflicts later on. With App-V-enabled applications, the organization simply needs to deactivate or remove that retired application centrally from the App-V Management Console. By doing so, the users subsequently have the application removed from their desktop, and all previously cached data blocks of the application are removed as needed. Because applications are no longer truly installed when App-V is used, there is never a need to remove the application from the client's computer.

—Sean Donahue, Senior Program Manager,
System Center Alliance, Microsoft Corporation

App-V Components

The App-V environment consists of the following components:

- App-V Management Server
- App-V Management Web Service
- App-V Data Store
- App-V Streaming Server
- App-V Management Console

- App-V Sequencer
- App-V Client

In addition, you can publish your virtual application packages using your existing electronic software distribution system such as Microsoft System Center Configuration Manager 2007 instead of using the App-V Management Server. You might also need one or more file servers, Web servers, or both, depending on how you want to use App-V.



Note Not all of these components need to be installed in your environment; the components that need to be installed depend on how you plan on using App-V to deploy virtual applications to users. For more information on different App-V deployment scenarios, see the section titled “App-V Deployment Scenarios” later in this chapter.

The sections that follow provide more information concerning each component of the App-V environment.

App-V Management Server

The App-V Management Server is used for streaming the virtual application package content and for publishing virtual application shortcuts and file type associations to the App-V Client. Because the Management Server streams virtual applications to end users on demand, these servers are ideally suited for environments that have reliable, high-bandwidth local area networks (LANs), such as head office environments. The Management Server also supports Active Upgrade; the Desktop Configuration Service, which is used by the client to retrieve the applications that the logged-in user has access to; and licensing and metering capabilities.

The Management Server should be installed on a dedicated server computer and needs access to a Microsoft SQL Server database that can either be installed on the same server or on a different server on your network. Microsoft SQL Server is used to manage the database and data store for the App-V environment. You can deploy a single Management Server or use many of them. In a typical App-V environment, multiple Management Servers share a common data store for configuration and package information. For more information concerning the App-V Data Store, see the section titled “App-V Data Store” later in the chapter.

The Management Server also needs access to the Content folder, which is a repository for the virtual application packages you want to publish and stream to the client computers on your network. The Content folder is where the SFT files are loaded and stored, and it can be located on either the Management Server itself, on a separate file server on your network, on a Distributed File System (DFS) share, or on a SAN. For more information concerning the Content folder, see the sidebar titled “Direct from the Source: Using the Content Folder” in this chapter.

The Management Server handles user requests for application data and then streams this data on demand to authorized users. This streaming of application data takes place using one of the following protocols:

- Real-Time Streaming Protocol (RTSP)
- Real-Time Streaming Protocol Secure (RSTPS), which is RTSP over Transport Layer Security (TLS)
- Hyper-Text Transfer Protocol (HTTP)
- Hyper-Text Transfer Protocol Secure (HTTPS), which is HTTP over Transport Layer Security (TLS)

You configure and manage the Management Server by using the Application Virtualization Management Console, which is described in the section titled “App-V Management Console” later in the chapter.

Direct from the Source: Using the Content Folder

Depending on the implementation scenario, the Content folder is accessed during several deployment steps. First, it can be used as the source for OSD and ICO files when using the Application Virtualization Management Server (Native Mode). And second, it is used as the source for SFT files as follows:

- Online when using Management Server (Native Mode), Streaming Server (Lightweight Server), or perhaps an ESD deployment.
- Offline when using System Center Configuration Manager 2007 R2 Integration or Standalone Mode.

OSD and ICO File Delivery

To deliver OSD and ICO files, two technical implementations are commonly used. In a (virtual) LAN environment, where all users and computers are members of the same Active Directory Domain (or Active Directory structure), the Content folder often is accessed as a Windows file share (SMB/CIFS) by specifying a UNC name in the App-V Management Console, either in the System Options settings, in each application’s OSD and ICO paths, or both. Here, each user has to have read access permissions (Windows Share and NTFS) to the Content Folder.

The other implementation grants access to the OSD and ICO files by means of a Web server. (Therefore, IIS is often used.) Here, on the IIS server a new virtual directory has to be created that points to the Content folder (and OSD has to be registered as a MIME type). App-V clients then access the files via HTTP or HTTPS. The advantage of using a Web server virtual directory is easier access management, because not every user (only the Web server service account) needs NTFS permissions. OSD and ICO

access based on HTTP or HTTPS also is configured within the App-V Management Console (using the System Options settings for each application).

SFT File Delivery

There is an offline way and online way to load the SFT file into the client's Virtual Application Cache.

Offline in this context means that the App-V Client does not load the SFT file directly from the Content folder and is used in SCCM Mode and Native Mode. In SCCM Mode, the SFT files are copied to an SCCM distribution point and then transferred to the client using SCCM defaults, such as Background Intelligent Transfer Service (BITS).

In Offline Mode, the App-V Client is instructed (by registry settings or during setup) not to contact any central server and to fall back to local load. In this scenario, the App-V Client attempts to load the SFT from the same location where the MSI is located (which enables the new virtual application on the client).

Online loading used to be called *streaming*, but with App-V 4.5, Microsoft introduced additional methods to load the SFT files from a central location beyond strictly *streaming*.

The protocol and server to be used are specified with the sequencer (in the OSD file) and can be changed afterward (with some caution).

Originally, RTSP (or RTSPs) was the only protocol you could use to transfer SFT files to the client. In App-V, the Application Virtualization Management Server (Native Mode) and the Lightweight Server (Streaming Server) can be used as a loading source.

Microsoft then added the ability to load SFT files from a (Windows) file server. Therefore, the user must have read permissions to the content file share.

This SMB/CIFS loading can be used with ESD tools, which simply push (and launch) the virtual application MSI file. It also can be used in conjunction with an Application Virtualization Management Server—for instance, if the client resides in a branch office and the SFT files should be loaded from a decentralized file server.

Quite new to App-V 4.5 is the ability to load SFT files from a Web server using HTTP or HTTPS. Usage scenarios and configuration are quite similar to Server Message Block (SMB) loading; however, it is easier to secure this communication and to traverse firewalls. Also, users don't need to have NTFS access permissions to the Content folder.

All online loading concepts support the usage of a system variable to specify the server name. The variable defaults to %SFT_SOFTGRIDSERVER% for RTSP or RTSPS. This default value can (best) be changed (in the Sequencer's Deployment tab) after the Sequencing Wizard has ended. Both App-V Management Server and Streaming Server

use the file system's Content folder as an entry point; therefore, in URLs using RTSP or RTSPS, "content" does not appear. This is different for the other protocols, as the following examples show:

```
RTSP://<server name or variable>:<Port>/defaultapp.sft
```

Here "server name" can be the IP address, the hostname, or the fully qualified domain name (FQDN) of an App-V Management Server or Streaming Server—for example:

```
RTSP://MyStreamingServer:554/DefaultApp.sft
```

Alternatively, the server name can be represented by a variable (%SFT_SOFTGRIDSERVER% by default) that has to be resolvable on the client. Using RTSPS requires using an FQDN for the server name (or as the value for the variable).

If you are using IIS, use the following format:

```
HTTP://<web server name or variable>:<Port>/<Virtual Web Directory>/defaultapp.sft
```

Here is an example:

```
HTTP://MyWebServer:80/webcontent/DefaultApp.sft
```

Here "web server name" can be specified as an IP address, hostname, or FQDN and "Virtual Web Directory" is an IIS pointer to the Content folder. Using HTTPS requires using an FQDN. Usually, "webcontent" is named "content" as well.

For a file server, use this format:

```
FILE:\\<file server name or variable>\<share name>\defaultapp.sft
```

Here is an example:

```
FILE://\MyFileServer\contentshare\defaultapp.sft
```

Here "file server name" can be an IP address, hostname, or FQDN. Users must have file share and NTFS read permissions. Usually, "contentshare" is called "content" as well.

Outsourcing the Content Folder

In most descriptions, the Content Folder resides on the same machine as the App-V Management Server or the App-V Streaming Server. Both implementations can be configured to use a remote folder to access the SFT files. Therefore, the services have to be configured to start under a certain service account. The Microsoft App-V Team Blog describes how to accomplish this:

<http://blogs.technet.com/softgrid/archive/2008/08/21/how-to-configure-the-app-v-management-server-service-to-run-as-a-service-account.aspx>

For deployment scenarios that do not use RTSP or RTSPS for SFT loading, the Content folder can be placed on (literally) any location.

—Falko Gräfe, MVP

App-V Management Web Service

The App-V Management Web Service is the component responsible for communicating read/write requests to the App-V Data Store. The App-V Web Service functions as an intermediary between the Management Console and the Data Store.

Note that even though the administrator makes his changes in the GUI of the App-V Management Console, those changes do not get written to the Data Store by this MMC console. Instead, the Management Console makes a .NET Remoting connection to the Management Web Service. This service then makes an OLE DB connection to the SQL Data Store and performs the actual read/write operations. Although these actions are unsupported by Microsoft, an administrator can perform them manually by using the SQL Admin Console. However, doing it this way is not recommended.

The App-V Management Web Service can be installed either on the Management Server itself or on a separate server that has IIS 6.0 or higher installed. In addition, Microsoft Data Access Components (MDAC) 2.7 or higher and the .NET Framework 2.0 must be installed on the server running the App-V Management Web Service in order to allow connectivity with the data store.

App-V Data Store

The App-V Data Store is a required component when you deploy an App-V Management Server. The data store is responsible for storing all information related to the App-V infrastructure, including the following:

- App-V Management Server configuration information
- App-V Management Server reporting information
- Application records
- Application assignments
- Application licensing information
- Logging information

The Data Store consists of a SQL Server database that can be installed on either Microsoft SQL Server 2005 or Microsoft SQL Server 2008.

When a user tries to launch an application that has been virtualized using App-V, the Management Server that receives the user's request contacts Active Directory Domain Services for authorization and the data store for application licensing information.

App-V Streaming Server

The App-V Streaming Server is responsible for hosting and streaming virtual application packages to App-V clients. You can think of the Streaming Server as a lightweight version of the Management Server that includes only streaming functionality, doesn't include the App-V Management Web Service or the Management Console, and doesn't require using a Microsoft SQL Server database. Instead, the Streaming Server uses access control lists (ACLs) for granting user access to the package files. The Streaming Server also supports Active Upgrade, but it doesn't have a Desktop Configuration Service, licensing or metering capabilities.

Like the Management Server, the Streaming Server also needs access to the Content folder, which is the repository for your virtual application packages. The Content folder can be located either on the Streaming Server itself, on a separate file server on your network, or on a SAN.

The Streaming Server can be used in environments that have an existing ESD, such as System Center Configuration Manager 2007. The Streaming Server can be used together with the Management Server. For example, the Streaming Server can be used at a branch office while the Management Server is deployed at the head office, with a slow wide area network (WAN) link between the two locations. Alternatively, the Streaming Server can be used alone without the Management Server in environments that don't have the infrastructure to support the Management Server. For more information on different App-V deployment scenarios, see the section titled "App-V Deployment Scenarios" later in this chapter.

App-V Management Console

The App-V Management Console is an MMC snap-in you can use to manage your App-V environment. Using the Management Console, an administrator can do the following:

- Import applications
- Manage file type associations for applications
- Manage application licenses
- Create and manage server groups
- View and configure server settings
- Create provider policies
- Generate reports

The Management Console can be installed locally on the Management Server, and it can also be installed on any workstation that has MMC 3.0 and .NET Framework 2.0 installed to allow remote management of the App-V environment.

Figure 4-2 shows the layout of the Management Console and displays a list of the applications that have been sequenced on the local Management Server.

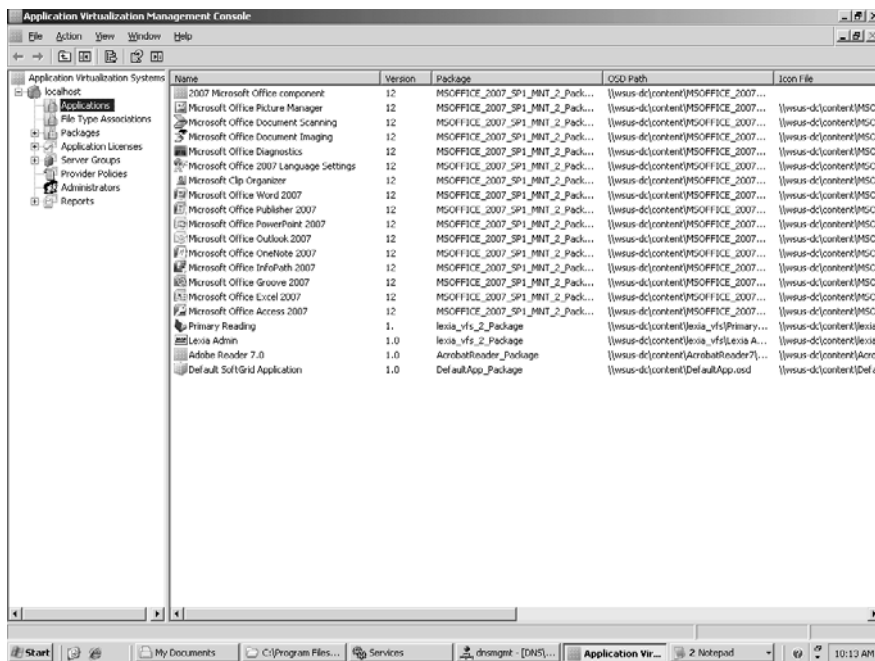


FIGURE 4-2 The App-V Management Console showing a list of virtual application packages on the local App-V Management Server.

App-V Sequencer

The App-V Sequencer is a wizard-based tool that can be used to monitor and capture the installation of an application to create a virtual application package you can publish and stream to client computers. After an application has been sequenced, the resulting App-V-enabled application package can be delivered to users on demand to run within an isolated virtual environment on the user's computer.

The output of the sequencing process includes an application's icon (.ico) files, an .osd file containing the package definition information, a package manifest file (manifest.xml), and the .sft file that contains the application program's content assets. The sequencing process is performed once for each application or suite of applications you want to virtualize, and the process protects the application's integrity by not making any modifications to the source code of the application. After an application has been sequenced, its files must be copied to the Content folder before they can be streamed or published to the App-V Client. Alternatively, the .ico and .osd files can be hosted on a Web server and delivered to the App-V Client using HTTP or HTTPS.

The Sequencer component typically must be installed on a separate computer from the other App-V components. This separate computer is called the *sequencing computer*. This sequencing computer needs to be a clean image that can be restored back to its virgin state at the end of every successful sequencing operation.

During the sequencing process, the Sequencer is first placed in monitor mode. The application to be sequenced is then installed on the sequencing computer. The sequenced application is then started, and common tasks are performed with the application so that the monitoring process can configure the primary feature block, which contains the minimum application package content that is needed for the virtualized application to run properly. When all of these steps are finished, monitoring mode is stopped and the sequenced application is saved. The sequenced application should then be thoroughly tested to ensure that it works properly when virtualized.



Tip Some applications cannot be sequenced, including Internet Explorer, device drivers, applications that start services at boot time, and some other parts of the Windows operating system.

For more information about sequencing applications, see the section titled “Using the Sequencer” later in this chapter.

App-V Client

The App-V Client is the software component that resides on the client computer and provides the virtual environment for running virtual applications. The App-V Client also handles the streaming of the application content from a Streaming Server if one has been deployed. The streaming process structures the application content so that the initial user interaction is streamed to the client computer first. This is done so that the user can launch the application immediately without needing to wait for the entire application content to be streamed to the client. Users can launch virtual applications by clicking on icons on their desktop or Start menu, or by double-clicking on file types associated with the application.

There are two kinds of App-V Client software:

- **App-V Desktop Client** This client is used on standard desktop computing environments. The App-V Desktop Client is included in the Microsoft Desktop Optimization Pack (MDOP) for Software Assurance (SA). The App-V Desktop Client is installed on end-user workstations to C:\Program Files\Microsoft Application Virtualization Client and is responsible for caching and launching virtualized applications. The App-V Desktop Client turns desktop applications into services to be deployed on demand without installation and without administrators having to be concerned about conflicts with any existing applications. The App-V Desktop Client also allows applications to be centrally managed with real-time license compliance.

- **App-V Terminal Services Client** This client is used in Terminal Services environments. The App-V Terminal Services Client behaves much like the App-V Desktop Client except that it provides for installation on a terminal server, which hosts the virtualized application instead of having the virtualized application run directly on the client computer. The App-V Terminal Services Client allows administrators to deliver any application to any Terminal Services or Citrix XenApp server without having to perform the installation, without being concerned about conflicts or testing, and without disruption of service.

The App-V Client must be configured at installation time using the Client Management Console to specify the name or IP Address of the Desktop Configuration Server that it contacts at login to retrieve application icons and .osd files that the user has access to. If you are going to use the App-V Desktop Client, you must also deploy this software to your client computers. This is typically done using ESD system such as Microsoft System Center Configuration Manager 2007, but it can also be done using other methods, such as Group Policy Software Installation, scripting, or even manual installation.

App-V Architecture

Figure 4-3 illustrates the App-V architecture, showing the different components of the App-V platform and the protocols and other transport mechanisms used for communications between these components.

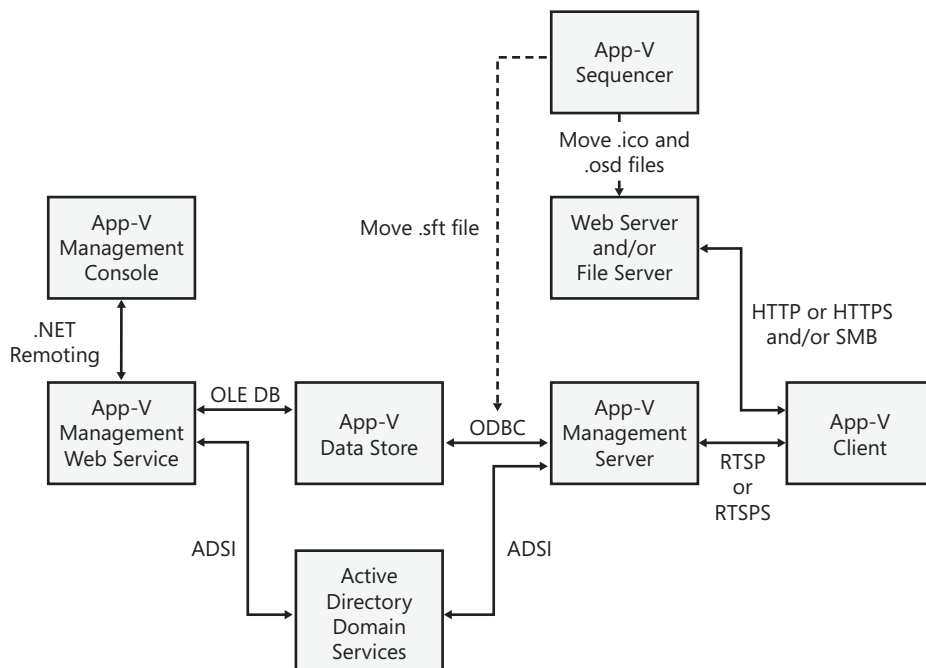


FIGURE 4-3 The App-V architecture.

The section titled “App-V Components” that preceded this section summarized the function of each of the different App-V components. The following is a summary of the protocols and other transport mechanisms used for communications between these components:

- **.NET Remoting** A component of the .NET Framework that enables client applications to use objects in other processes on the same computer or on any other computer available on its network. This used by the Management Web Service to connect to the SQL Data Store.
- **ADSI** Active Directory Service Interfaces, a set of COM interfaces used to access the features of directory services from different network providers. ADSI is used in a distributed computing environment to present a single set of directory service interfaces for managing network resources. This is used by the Management Server to retrieve user group associations from Active Directory.
- **HTTP** Hypertext Transfer Protocol, an application-level protocol for distributed, collaborative, hypermedia information systems, such as text, graphic images, sound, video, and other multimedia files on the World Wide Web. This can be used to stream the SFT file to the App-V clients.
- **HTTPS** Hypertext Transfer Protocol over Secure Sockets Layer, an extension of HTTP that securely encrypts and decrypts Web page requests using Secure Sockets Layer (SSL). SSL is a security protocol that supports confidentiality and integrity of messages in client and server applications communicating over open networks. This can be used to stream the SFT file to the App-V clients with added security.
- **OLE DB** A set of COM-based interfaces that expose data from a variety of sources. OLE DB interfaces provide applications with uniform access to data stored in diverse information sources or data stores. This is used by the Management Web Service to connect to the SQL Data Store.
- **ODBC** Open Database Connectivity, a universal data access interface that enables applications to concurrently access, view, and modify data from multiple, diverse databases. This is also used by the Management Web Service to connect to the SQL Data Store.
- **RTSP** Real-Time Streaming Protocol, an application-level protocol that controls the transport of multimedia content, session announcements, and tear-downs. When the App-V client communicates with the App-V Management Server, the client uses RTSP over port 554 to establish the initial connection with the server. After the initial connection has been made, however, the client continues to send and receive blocks of the streamed application package content using two other protocols, the Real-Time Transport Protocol (RTP) and the Real-Time Control Protocol (RTCP). These two protocols open connections with the clients, starting with ports 49152 up to 65535, concurrently for send/receive.
- **RTSPS** Real-Time Streaming Protocol Secure, which is RTSP over Transport Layer Security (TLS). When the App-V client communicates with an App-V Management

Server that has a certificate assigned to it, the client uses RTSPS over port 322 to establish the initial connection with the server and then uses RTP and RTCP for streaming of blocks of application package content. If there is no certificate assigned to the server, the communication uses RTSP over port 554 if the option to allow nonsecure connections is selected.

- **SMB** Server Message Block, a protocol used to request file and print services from server systems over a network. Standard ports are used when App-V is deployed in a trusted environment, such as a corporate LAN, while restricted ports are used when App-V is delivering virtual applications to untrusted clients—for example, over the Web. Restricted reports require that a server certificate be installed on the Management Server during installation of the server, and also on any file, Web servers, or both that are used to stream application package content to clients.

Table 4-1 lists the various ports that must be open for App-V components to communicate with one other.

TABLE 4-1 App-V Communications Ports

Communications Function	Standard Port	Protocol	Restricted Port	Secure Protocol
Between the Management Console and the Management Web Service	80	HTTP	443	HTTPS
Between the Data Store and the Management Web Service	1433	ODBC	1433 (IPsec)	ODBC
Between the Data Store and the Management Server	1433	ODBC	1433 (IPsec)	ODBC
Between App-V clients and the Management Server	554	RTSP	322	RTSPS
Used by RTSP and RTSPS to manage communications after initial communication has been established between App-V clients and the Management Server	49152-65535	RTP RTCP		



Note For more information on the protocols and other transport mechanisms used by App-V, see article KB 932017 in the Microsoft Knowledge Base on Microsoft TechNet at <http://support.microsoft.com/kb/932017>.

Working with App-V

Microsoft App-V provides organizations with powerful and flexible solutions for delivering virtualized applications to end users. This section covers some of the basics of working with App-V and includes the following topics:

- App-V deployment scenarios
- Obtaining App-V
- Using the Management Console
- Using the Sequencer
- Working with App-V clients



Note A full treatment of how to deploy, configure, use, and maintain an App-V environment is beyond the scope of this chapter. For detailed information on these topics, see the "Planning and Deployment Guide for the Application Virtualization System" and "Operations Guide for the Application Virtualization System" on Microsoft TechNet at <http://technet.microsoft.com/en-us/library/cc843848.aspx>.

App-V Deployment Scenarios

Microsoft App-V has a great deal of flexibility in how it can be deployed within an organization. For example, you can choose from the following three publishing delivery methods for transferring the .osd and .ico files from their designated location (typically, \Content) to the App-V Client software running on client computers:

- Using the App-V Management Server alone as the core of your virtual application deployment platform to transfer the .osd and .ico files from the Content folder on your Management Server. You can also use an App-V Streaming Server, such as an IIS Web server or file server, to host your Content folder if you already have such infrastructure in place and want to use it.
- Using an electronic software distribution (ESD) system, such as System Center Configuration Manager 2007, to move .osd and .ico files to clients via standalone Microsoft Windows Installer (.msi) files, the MSI manifest contained within .msi files, or SFTMIME commands.
- By standalone (locally-installed) delivery of .msi files to users via network shares, removable media, or some other method.

You also have several choices as to which package delivery method you use to stream the virtual application packages or .sft files from your Management Server to the App-V Client software running on client computers:

- An IIS Web server, which streams package content using HTTP or HTTPS
- A file server, which streams package content using SMB

- An App-V Streaming Server, which streams package content using RTSP, RTSPS, or HTTP/S (if IIS is installed)

You can also deliver package content via standalone delivery or by using an ESD system, but the most typical ways of streaming packages are by using a Streaming Server, IIS server, or file server. Table 4-2 lists some of the advantages and disadvantages of each of these package delivery methods.

TABLE 4-2 Advantages and Disadvantages of Different Package Delivery Methods

Package Delivery Method	Advantages	Disadvantages
App-V Streaming Server	Supports Active Upgrade and RTSPS for enhanced security; needs only one firewall port open	Requires supporting a dual infrastructure; requires additional server administration
IIS server	Supports streaming to remote clients via the Internet and HTTPS for enhanced security; highly scalable; needs only one firewall port open	Adds the overhead of managing IIS servers
File server	Supports using existing file servers to provide a simple low-cost solution	Does not support Active Upgrade

For more information on the power and flexibility of the various ways you can deploy App-V in your organization, see the sidebar titled “Direct from the Source: App-V—A Scalable Solution for Application Virtualization” in this chapter.

Direct from the Source: App-V—A Scalable Solution for Application Virtualization

One of the features in the new version of App-V that I am most excited about is the number and variety of deployment methods for the virtual application packages. In SoftGrid versions 4.2 and earlier, you were limited to deploying your virtual applications with a full SoftGrid back-end infrastructure only. This could prove to be quit limiting for a branch office environment. In short, you had to deploy a SQL data store at each of your branch offices along with a SoftGrid Streaming Server. App-V, however, is much like choosing from a cafeteria line of selections for how you deploy your virtual applications. You pick and choose the options you want—and those you don’t want, you leave under the warming lights for later.

The way I look at App-V, today is by looking at the virtual application package first. Because this package can be deployed to multiple clients in various ways, the package is the constant. For example, I can take the same package and deploy it to a collection of Windows Vista clients at Corporate HQ using what is considered to be a traditional method. That is, I use the App-V Management Console to publish the application to a group of Active Directory users. This is written in the SQL data store, and the package files (.SFT, .ICO, .OSD, .SPRJ) are stored in the Content folder of the Streaming Server. The client logs in and contacts his Desktop Configuration Refresh Server, which is most often the same server as the App-V Streaming Server, and gets a list of his applications from the SQL data store. The icons and OSD files are transferred to the client, and upon initial launch of the icon the SFT file starts streaming, using RTSPS, to the client. Nothing new here.

However, if I'm in a branch office instead, I could use what is referred to internally as the Lightweight Streaming Server. This is an App-V server whose only purpose and function is to stream App-V SFT files using RTSPS (by default). As an administrator, I publish the App-V applications to my user groups in Active Directory as I did in the traditional model. I then copy the SFT file to a server in the local branch office that had the lightweight streaming server (LWS) installed on it. The user logs on to his computer, authenticates, and then contacts the Desktop Configuration Refresh Server to receive a list of applications he has permissions to. The icons and OSD files transfer to the client as they do with the method used at Corporate HQ. However, when the user launches the application shortcut, the application streams from the local LWS instead of over the WAN from Corporate HQ. This happens because as the administrator, I have set the Application Source Root in the client's registry that told the clients in the branch to override whatever the HREF line in the OSD file said and use the local branch server instead. Additionally, I can set the Icon Source Root and the OSD Source Root in the same way and have all traffic, except the refresh, occur from the local LWS. But wait! There's More!

What if I told you that in addition to this you could now deploy your App-V packages to remote users who did not have regular access to an office connection? During the sequencing process you could select the check box that generates an MSI file in addition to the standard App-V package's files. You could then deploy the MSI and SFT files to a location accessible to this remote user—for example, to a DVD or local share. The user double-clicks the MSI file, and it uses the Windows Installer Service to "install" the virtual application. Rest assured that nothing is actually installed. Instead, what really happens is the installer service calls one of the App-V client executables called Sftmime.exe. If you open the MSI in Orca or another MSI edit utility, you see a bunch of SFTMime commands that basically add the application to the client, publish the shortcuts, add the OSD, and load the SFT file into the local file system cache, sftfs.fsd. This is combined with a registry setting that sets the Require Authentication Even If Cached option to 0. I use this all the time when testing applications from independent software

vendors (ISVs) that I've sequenced. I simply copy the MSI and SFT to a client and launch it. No back-end whatsoever is needed.

As if that weren't enough, you also have the ability to use an ESD, such as System Center Configuration Manager R2. With this option, the administrator advertises the package in System Center Configuration Manager as he would with a physically installed application. However it is really a Virtual Application instead. By using System Center Configuration Manager, you would still need the App-V client on the desktop in addition to the System Center Configuration Manager Advanced Client. System Center Configuration Manager uses a new file added to the App-V packages called the manifest file (`_manifest.xml`) which stores information about all of the applications in the package. This file is used to populate several of the fields in the new applications added to the System Center Configuration Manager console. System Center Configuration Manager also allows distribution points, which are most likely already established in the organization, to act as the streaming points for the App-V packages. When the System Center Configuration Manager Advanced Client does its policy refresh it will pick up the App-V applications just like it does the physically installed Apps. The beauty here is that this requires no special App-V infrastructure, it uses all of the existing System Center Configuration Manager configuration. It also allows the publishing of App-V packages to physical collections and not just users.

Sometimes I feel like a proud Papa bragging on and on about how great their prodigy child is. But this last feature on scalability that I will call out here in this sidebar is the introduction of HTTPS streaming instead of RTSPS. Now to some this might seem an anticlimactic way of ending. "Isn't this an obvious evolution?" One might say. As obvious as it might seem it introduces a whole new world to App-V. Imagine being able to stream virtual applications that never change or alter the foot print on a client devices, over the Internet. Yes Virginia, there is a Santa Claus. This means that a company, or an ISV, could host their applications on a Web server and deliver those virtual applications to their clients anywhere in the world. The client would still need the App-V client and a Web server would need to be configured with a content location under the root. But the question is, "Who doesn't have a Web server?"

Back in my day we didn't have these fancy delivery methods. We had to have a Streaming Server and SQL data store in every branch office. And we liked it! Nowadays you kids have it easy. You take your App-V package and pick and choose your delivery method. "I think I'll stream this to these clients with RTSPS. But deliver it to these clients with an LWS, and then burn to DVD and mail it to these remote users. Oh but for this segment of machines I'll use System Center Configuration Manager to advertise to a collection and then stream it over the Web using HTTPS to these customers." What's next? A better network topology than ARCNet?

*—Sean Donahue, Senior Program Manager,
System Center Alliance, Microsoft Corporation*

Deploying App-V at a Single Site

If your organization is located at a single site and has a fast, reliable LAN throughout, you can deploy App-V using the traditional or classic approach familiar to earlier SoftGrid 4.2 administrators. (See Figure 4-4.) Here are the App-V components you need to deploy for this scenario:

- App-V Management Server
- App-V Management Web Service
- App-V Data Store
- Content Folder location
- App-V Management Console
- App-V Client software

For smaller sites, all of the components just listed can be installed on a single server with the Content folder located on any of the following:

- A share on the server itself
- A highly available DFS share
- A highly available SAN/NAS device

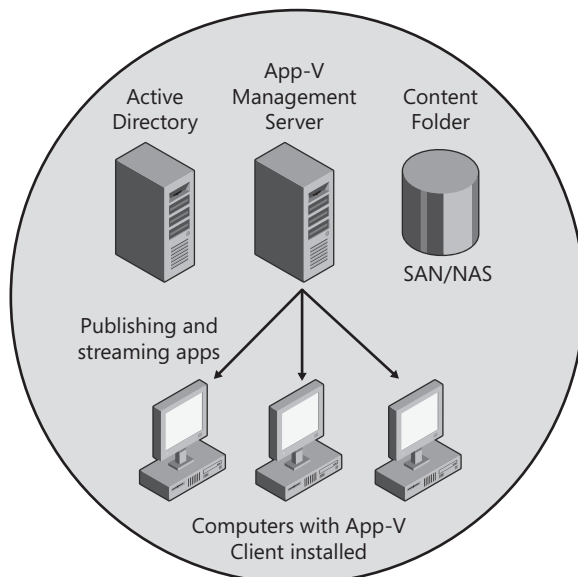


FIGURE 4-4 Deploying App-V at a single site.

After you've deployed the App-V components needed for this scenario, you can use the Sequencer to create virtual application packages and copy the package files to the Content

Folder. Then the administrator can publish each application to groups of users in Active Directory Domain Services so that when the user logs on to his computer he sees shortcuts on his Start menu and desktop to launch these applications. When the user double-clicks on a shortcut, the App-V Client on the user's computer streams the .sft file for the application package from the Management Server and then launches the application for the user to use. The application package is also cached locally on the user's computer so that the application can be launched more quickly next time the user needs to run the application.

Deploying App-V at Branch Offices

Larger organizations that include branch offices at remote sites can add another App-V component, the App-V Streaming Server, to enable users to efficiently use virtual applications that are provisioned from the head office site over slower WAN links. For this scenario, you can deploy a Streaming Server at each branch office and your remaining App-V components at the central head office location. (See Figure 4-5.) In this scenario, virtual applications are published to client computers at the branch office over the WAN link while application package content is streamed to these clients over the branch office LAN. In this branch office scenario, it is possible to either have the .ico and .osd files delivered to the client over the WAN link or to modify the client's registry so that these files are also delivered from the local branch office's server.

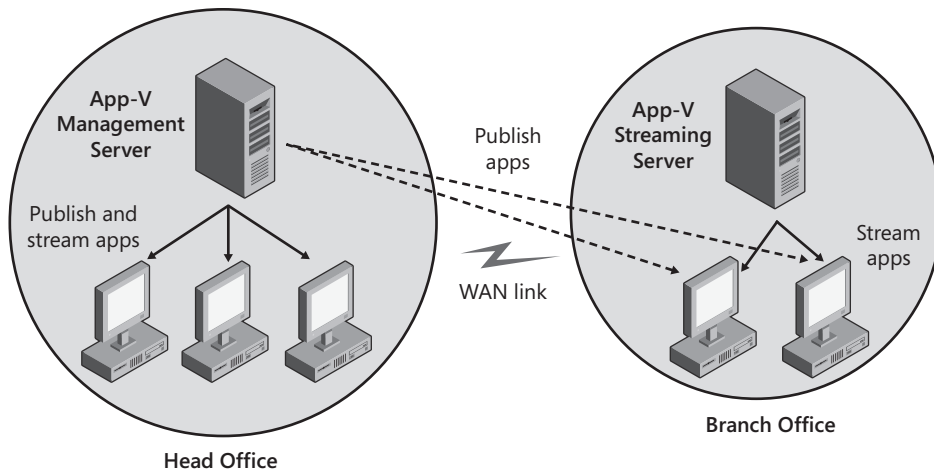


FIGURE 4-5 Deploying App-V for branch offices.

Deploying App-V Using an Existing ESD System

Large enterprises that already have an electronic software distribution (ESD) system in place can leverage their existing infrastructure to provide application virtualization to users in a number of different ways. For example, Figure 4-6 shows an enterprise that has two sites

(head and branch offices) plus external users who need to access virtual applications over the Internet. In this particular implementation, client computers at the head office stream virtual application package content from an App-V Streaming Server. This gives these clients the benefits of Active Upgrade, a feature of App-V that requires App-V servers to be deployed and that enables automatic upgrading of virtual applications on end-user computers at their next publishing refresh cycle. By contrast, client computers at the branch office stream their virtual application package content directly from the ESD distribution point running on a file server on their local network. This scenario is a simple, low-cost solution that uses SMB to stream the package content from an existing file server that hosts the Content Folder for the clients, but it doesn't support Active Upgrade. Finally, an IIS server on the perimeter network at the head office is used to stream virtual application package content over the Internet using HTTPS to external client computers such as mobile users with laptops, which is another scenario that is simple to implement but doesn't support Active Upgrade.

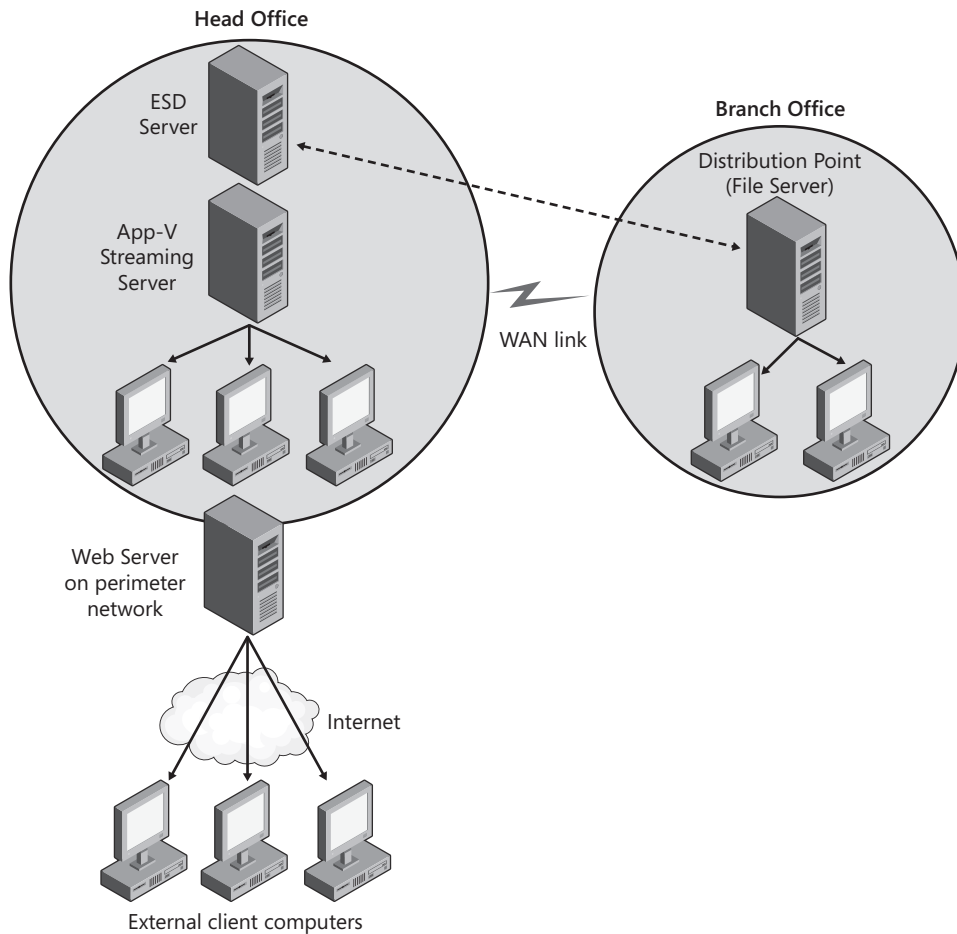


FIGURE 4-6 Sample App-V deployment leveraging an existing ESD system.

Standalone Deployment of Virtual Applications

The App-V Sequencer also has an option to create an .msi file that automates the “installation” of a virtual application. This .msi file contains additional metadata that enables an ESD system to recognize and control virtualized applications. Standalone mode requires the App-V Client to be configured for standalone mode, which allows only .msi-based updates of virtual applications. (Streaming is not allowed while in standalone mode.) This mode is meant to be used by rarely connected users that need the power of virtualized applications but do not have access to a server. So, in this scenario, you need to provide the .msi file to the user directly—for example, on CD or DVD media.

It is important to note that the package’s content file (.sft) is not included inside of the .msi file. The .sft file must be available in tandem with the .msi. The .ico and .osd files, however, are in the .msi file. When the user double-clicks the .msi file for a virtual application, a series of commands using the App-V client’s built in SFTMIME command are used to add the application and load the .sft file into the local cache. In this standalone deployment scenario, third-party products such as FullArmor’s GPAnywhere can be used to apply Group Policy settings to the virtual applications.

Deploying App-V with Terminal Services

You can also deploy App-V with Terminal Services so that users can run virtual applications on a terminal server instead of on their local computers. In this scenario, the user employs the App-V Terminal Services Client instead of the App-V Desktop Client. For more information on the benefits of deploying App-V together with Terminal Services, see the blog post titled “SoftGrid and Terminal Services: Better Together” on the Microsoft Application Virtualization team blog at <http://blogs.technet.com/softgrid/archive/2008/04/10/softgrid-and-terminal-services-better-together.aspx>.

Direct from the Source: Application Publishing with Streaming Server

If you use the Streaming Server at a branch site, you need to consider how to publish the application shortcuts, icons, and file type associations to the client systems at the branch site. Streaming Server only provides for delivery of the virtual application (the SFT file) on demand when the user requests to launch the application. There are several options available to perform this publishing.

The most straightforward option is to configure branch-site App-V clients to use the main-site full server for the purpose of application publishing only. Using this option, you retain the ability to publish on a per-user basis. This option does create a dependency on the main site for new and updated publishing; however, this is usually an acceptable situation both from a risk and bandwidth perspective. When the main site is

not accessible, all applications previously published will work at the branch site, even if the user has never run the application before. Traffic to the main site is limited to publishing at user logon, which is the equivalent of a Web-page query.

To use this option, configure the branch-site clients with the main-site publishing server just as you would main site clients. When configuring the publication server using either RTSP or RTSPS the Path field is not used. Create a branch-site equivalent of the main-site content share, and ensure that the complete contents of the share remain in sync with the main site. This can be done using DFS or a script (using xcopy or robocopy). Then configure the branch-site clients for overrides for ApplicationSourceRoot, IconSourceRoot, and OsdSourceRoot in the Windows registry under HKLM\Software\Microsoft\SoftGrid\4.5\Client\Configuration. The value for ApplicationSourceRoot would be in the form of "rtsp:\\branchserver:554". The value for the IconSourceRoot and OsdSourceRoot would be in the form \\branchcontentserver\contentsharename.

By adding the OSR/ISR overrides, these files will be pulled by the client from the local repository during publishing. The Application Source Root setting will direct the client to stream from the local streaming server.

The great thing about using these overrides is that it eliminates the need to manually edit OSD settings, which can be an error-prone task.

The second option is to add IIS to the Streaming Server (or other computer at the branch site) and post an XML file with the publishing information. This option minimizes both risk and WAN traffic, but it requires creation of an XML file with the publishing information.

To use this option, you still create the branch-site equivalent of the main-site content share and ensure that the complete contents of the share remain in sync with the main site. Configure the App-V clients to publish using HTTP from the local IIS server. You will set the path field to point to the XML file or dynamic Web page reference to be served up by the Web server. Application Source Root, ISR, and OSR overrides are also configured on the clients, just as in the first option.

The XML file has the following format:

```
<DESKTOPCONFIGURATION>
<APPLIST>
<APP NAME="..." >... </APP>
<APP NAME="..." >... </APP>
</APPLIST>
<DESKTOPCONFIGURATION>
```

The XML file can be created manually or using a dynamic Web page method. This latter method requires some programming skills.

To create the Applist.xml file manually, start with a base file from the format just shown with an empty APPLIST. Next, for each package you want to publish, copy everything from within the <APPLIST> element from the _manifest.xml file of the package into your new Applist.xml file, placing the content within the <APPLIST> element. Place this file at the configured Web page. This method will publish all applications to all branch users with the App-V client at the site.

The second method of creating the Applist.xml information is to use a dynamic Web page, which is an ASPX page that creates and publishes the equivalent information. A dynamic page allows for per-user publishing; however, you will need someone to code both the dynamic XML creation and ADSI lookups to determine which packages to publish to the user.

—Tim Mangan, MVP

Obtaining App-V

Microsoft Application Virtualization is available as part of the Microsoft Desktop Optimization Pack (MDOP) for Software Assurance, an add-on subscription license available to Software Assurance (SA) customers. App-V is also available as part of a separate product called Microsoft Application Virtualization for Terminal Services.



More Info For more information on obtaining MDOP, see <http://www.microsoft.com/windows/products/windowsvista/enterprise/default.aspx>. For information on obtaining Microsoft Application Virtualization for Terminal Services, see <http://www.microsoft.com/systemcenter/softgrid/evaluation/softgrid-ts.aspx>.

Using the Management Console

The App-V Management Console is your central location for performing all App-V-related management tasks. The following sections describe common administrative tasks you can perform when using this console.

Managing Applications

The Applications node of the Management Console lets you perform the following tasks:

- **Import an application** This action makes an application available for streaming from an App-V server. To import an application, you need to have either its .osd or .sprj file

available on the server. Importing an application automatically creates a package for the application during the import process.

- **Manually add an application** This action requires that you manually specify all the information that is normally determined automatically by the Import Applications Wizard. Adding an application manually also requires that you manually add a package for the application. For information about adding packages, see the next section.
- **Grant or deny access to an application** These actions let you specify which groups of users will be allowed to access the application.

Other actions you can perform using this node include renaming, deleting, and moving an application and changing an application icon.

As an example of how you can manage applications using this console, the following procedure demonstrates how you can import an application. Figure 4-7 shows the Application node before any applications have been imported.

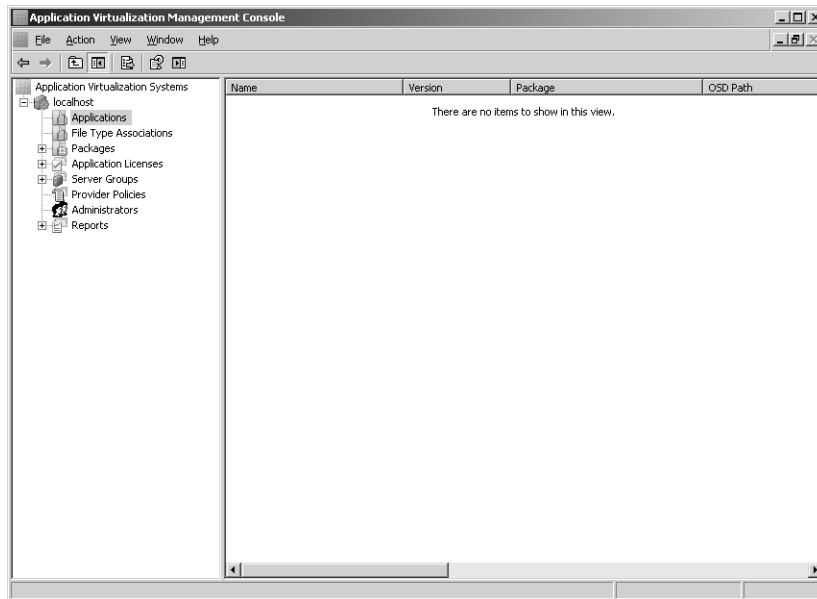


FIGURE 4-7 No applications have been imported yet.

Right-clicking on the Applications node brings up a shortcut menu. From this menu, select Import Applications. In the Open dialog box that appears, browse to locate the .osd or .sprj file for the application. (See Figure 4-8.) By using the .osd file, the administrator would need to add each application in a suite individually. By importing from the .sprj file, however, all the applications in the suite will be imported at one time.

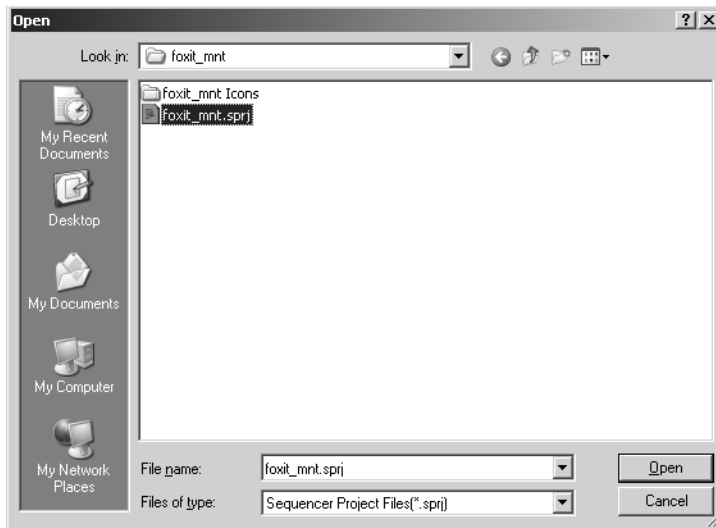


FIGURE 4-8 Selecting an application to import.

After you've selected the application you want to import, click Open. This launches the New Application Wizard. The first page of this wizard is automatically populated with the name, version, OSD path, icon path, application license group, and server group of the application. (See Figure 4-9.) If you want to stream the application to clients, make sure that the Enabled check box is selected as shown. You can also add a description for the application if desired. Verify that the remaining information displayed is correct before proceeding with the wizard. The OSD path and Icon path should reference either a UNC path or a URL because this will tell the user where those files can be copied from during the client's refresh.

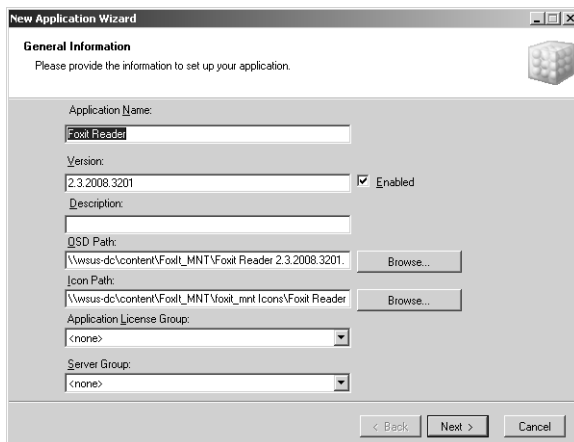


FIGURE 4-9 The New Application Wizard.

The next page of the wizard lets you specify the locations where you would like application shortcuts to appear on client computers. (See Figure 4-10.) By default, these will mimic what the application's installation would have populated as captured during sequencing.

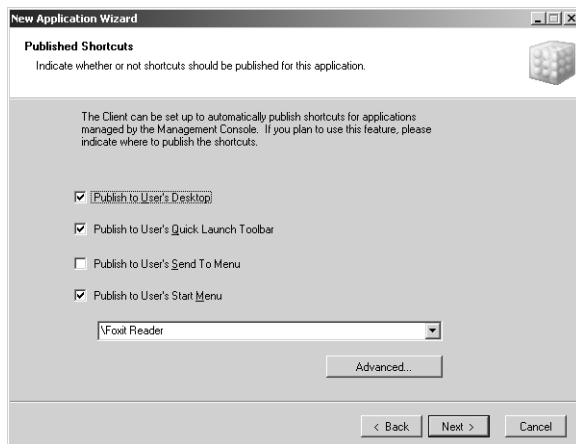


FIGURE 4-10 Specifying the application shortcuts that should appear on client computers.

The next page of the wizard displays the file associations that are currently configured for the application. (See Figure 4-11.) This screen also allows you to add new file associations for the application by clicking the Add button and to edit or remove existing file associations by clicking the corresponding buttons for these actions. By default, these will mimic what the application's installation would have populated as captured during sequencing.

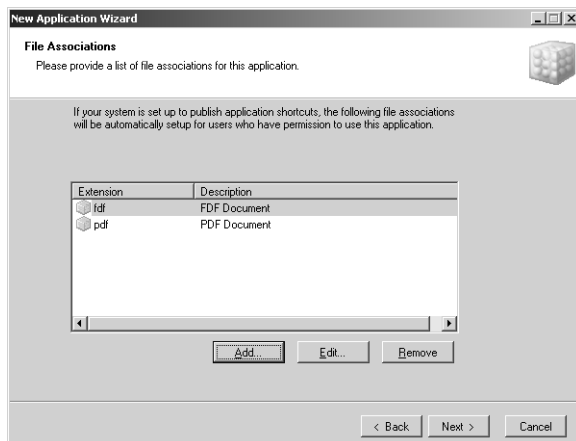


FIGURE 4-11 Viewing and modifying file associations for the application.

The next wizard page lets you assign which groups of users will be granted permission to use the application. (See Figure 4-12.)

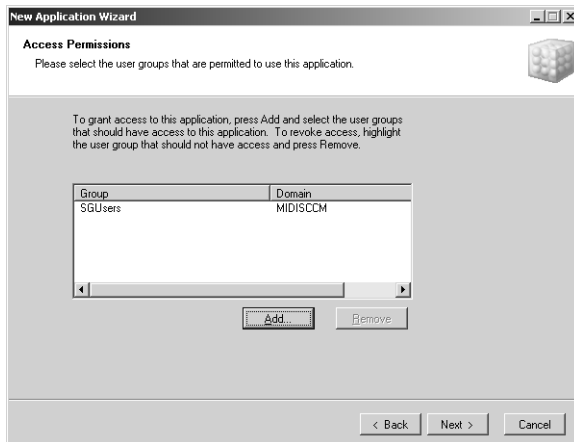


FIGURE 4-12 Granting access to the application.

The final page of wizard ask you to confirm the selections you have made. (See Figure 4-13.) If any conflicts were detected (such as File Type association) with an already existing application, you will receive a warning in this dialog box.

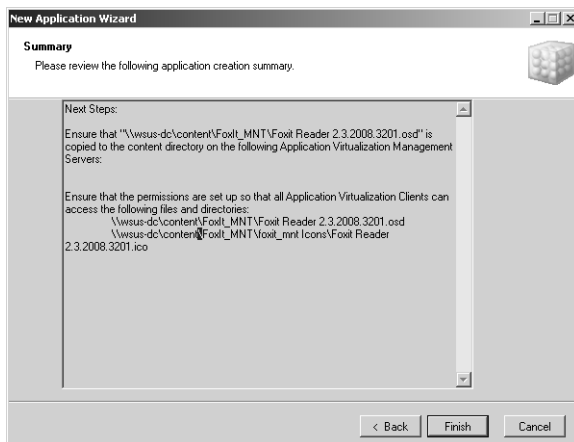


FIGURE 4-13 Summary page of the wizard.

Clicking Finish imports the application you have selected. The result of the import process is shown in Figure 4-14.

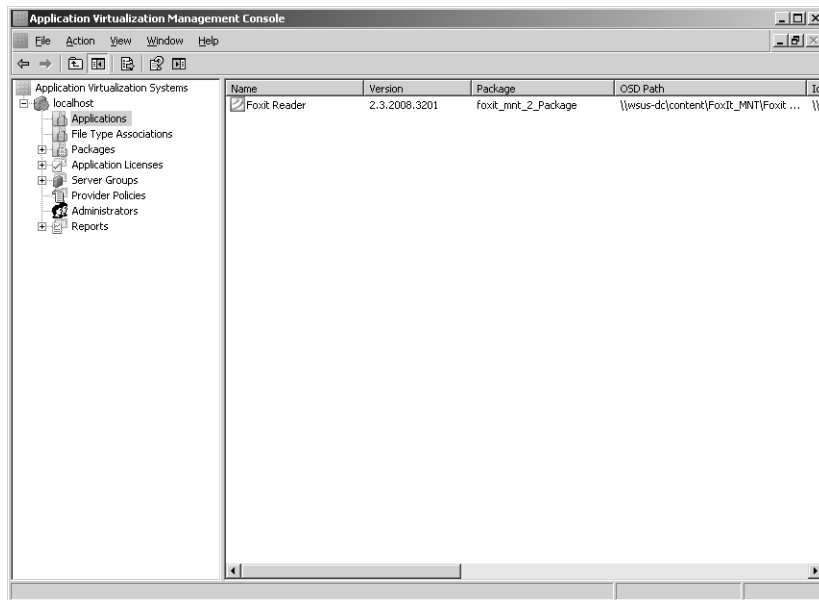


FIGURE 4-14 The application has been imported.

After the application has been imported, it is ready to be streamed to clients.

You can also use the Applications node to organize your applications into groups for easier management. For example, you might create application groups for specific departments, divisions, or sites in your organization. You can also create application groups for specific types of applications such as enterprise resource planning (ERP) applications, customer resource management (CRM) applications, and so on. Using application groups also makes it easier to grant permissions to applications and manage application licenses.

Direct from the Source: Using Application Groups in Active Directory Domain Services

When using the App-V Management Console to assign Active Directory Domain Services (ADDS) users and groups to imported applications, we have found in working with companies deploying virtual applications that they tend to use one of two approaches: organizational or functional. Both approaches work well, and the selection choice does not affect the functionality provided. Quite often, the selected approach depends on if the company already has experience and practices in place using other application-management products based on ADDS, such as electronic software distribution systems for traditionally installed applications.

The first approach is to assign organizational groups to applications or packages. Often, ADDS organizational units already exist in ADDS and application usage tends to fall into these predefined groups. Using this approach (other than the initial setup of the two App-V administrator and user groups), changes need not be made to ADDS to modify application assignment. Control over all the assignments are performed directly using the App-V Management Console and are stored in the App-V database. Multiple organizational groups and even the odd individual user can be assigned to allow use of the application. When changes to application assignments are needed, the App-V Management Console is again used to make the changes.

The second approach is to create a unique group in ADDS for each application package. Before importing the package using the App-V Management Console, create the application group in ADDS. When importing the package, assign this group to the package. When changes to application assignments are needed, the ADDS console is again used to make the changes.

Larger companies tend to prefer this second approach because of their existing practices. In particular, the personnel responsible for implementing change requests for new employees and those changing positions within the company will be more familiar with making changes in ADDS than the App-V Management Console.

—Tim Mangan, MVP

Managing Packages

Virtual application packages can be managed using the Packages node in the Management Console. (See Figure 4-15.) Packages let you control virtual application versions on your App-V Management Servers. Using the Packages node, you can

- Manually add a package by specifying the package name and the path to the application's .sft file.
- Add a new version of a package. (You can leave the previous version in place for compatibility reasons if needed.)
- Delete all versions of a package or only the specified version.
- Upgrade a package. (An automatic upgrade occurs when you perform an Open For Package Upgrade action of an existing package in the Sequencer.)

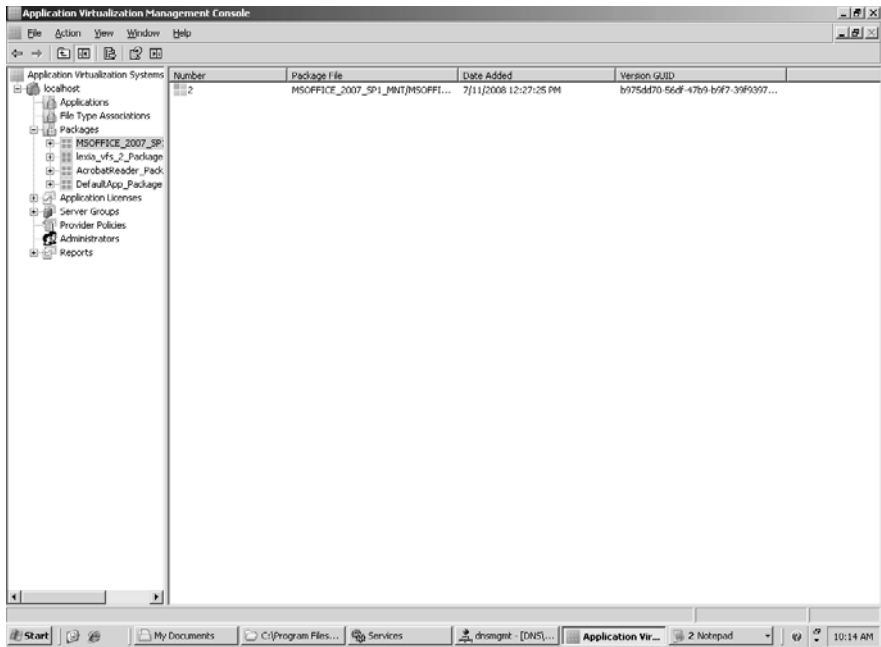


FIGURE 4-15 Managing packages.

Managing Application Licenses

You can use the Application Licenses node to add, remove, configure, and control application license groups. Depending on the type of license group you create, you will be able to control which users have access to your applications and how many users will be allowed to access applications at a given time. App-V helps administrators ensure license compliance: if there is a license available when a user tries to launch an application, the user is allowed to launch the application; if there is no available license, the client’s system tray will report Launch Failed and an error message will be displayed indicating that there is no available license.



Note License Groups are not application specific. This means that one license group can be applied to multiple applications, although license groups are typically created with specific applications in mind.

Three types of licenses can be created using the Management Console:

- **Concurrent License** This type of license allows a limited number of users to have simultaneous access to the applications that have the license groups assigned to them. Concurrent License groups are the most common type of licensing used for virtual applications and can reduce licensing costs by limiting the number of copies of an application that can be run concurrently.
- **Unlimited License** This type of license allows any number of users to have simultaneous access to the applications that have the license groups assigned to them. Unlimited License groups are useful for evaluating the number of licenses that will be required for an application, and when used in conjunction with Reporting they can assist in your purchasing decisions for applications.
- **Named License** This type of license allows only the specified users to have access to the application associated with the license. Named License groups are typically used for applications whose use must be restricted to certain groups of users, such as administrators, members of the management team, and specially trained users.

Managing Servers

You can use the Server Groups node of the Management Console to manage the App-V servers in your environment, including your Management Servers and Streaming Servers. Specifically, you can

- Create or remove server groups to organize your servers for easier management.
- Add a server to a server group or remove it from a group.
- Adjust the maximum memory allocation for the server cache of a server, specify the maximum block size to be used when streaming content from the server, or modify the port number used for RTSP or RTSPS streaming from the server.

By right-clicking on a server group and selecting Properties, you can manipulate the settings of all App-V servers in the selected server group.

The Default Server Group is created when you set up your App-V environment. (See Figure 4-16.) Small and mid-sized organizations might be able to get by with using only the Default Server Group.

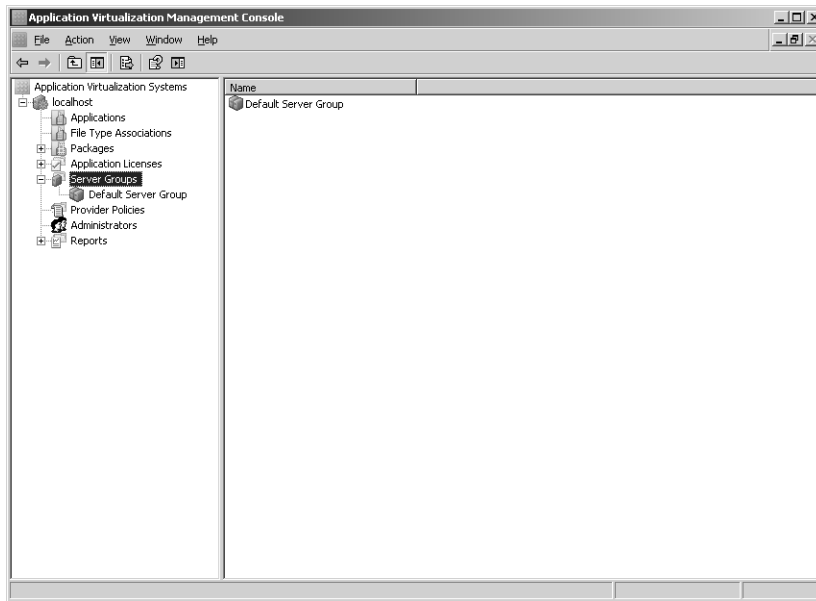


FIGURE 4-16 The Default Server Group.

Managing Reports

The Reports node of the Management Console can be used to generate different kinds of reports that contain information about your App-V system. These reports are created using a SQL Reports run-time agent, which is installed by default with the Management Console. Reports can be viewed, printed, or exported to PDF format to gather information about how your App-V system has been used over the course of daily, weekly, or monthly periods. Before running a report, metering and logging to a database must be enabled in your App-V system.

The following types of reports can be generated using this node:

- **Application Utilization** This report graphs the total daily and concurrent sessions over time during the reporting period for the specified application. The report uses a simple line graph with an independent y-axis for each metric. The report also lists all users who used the application, as well as the number of sessions, total session duration, average session duration for each user, and a summary of total usage for all users.
- **Software Audit** This report lists usage information during the reporting period for all applications defined in the database. For each application, this report lists the top N users who used the application together with the number of sessions, total session duration, average session duration for each user, and a summary of total usage for all users.
- **System Utilization** This report graphs the total daily and concurrent usage over time during the reporting period for the specified server, server group, or entire enterprise.

This report uses a simple line graph with an independent y-axis for each metric. The report also graphs usage by day of week and by hour of day.

- **System Error** This report graphs the number of fatal errors, errors, and warnings logged by the specified server, server group, or entire enterprise during the reporting period. This report uses a simple stacked bar graph with an independent y-axis for each metric. The report also lists each of the fatal errors, errors, and warnings logged in ascending order by time.

File Type Associations

The File Type Associations node lets you display and manage all the file type associations for all the applications you have imported. (See Figure 4-17.)

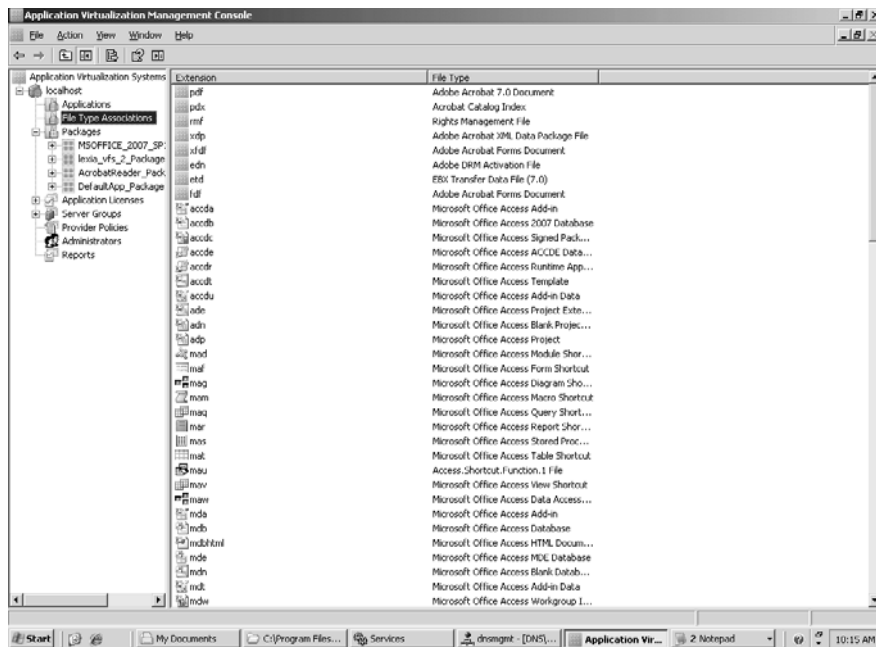


FIGURE 4-17 Displaying file type associations for all imported applications.

Provider Policies

The Provider Policies node lets you specify a set of rules that are applied to users making connections to virtual applications. As connections come into the server group (provider), the server appends several rules (provider policy) to the connection. If the user does not specify a custom provider policy, the rules of the Default Provider are applied. (See Figure 4-18.)

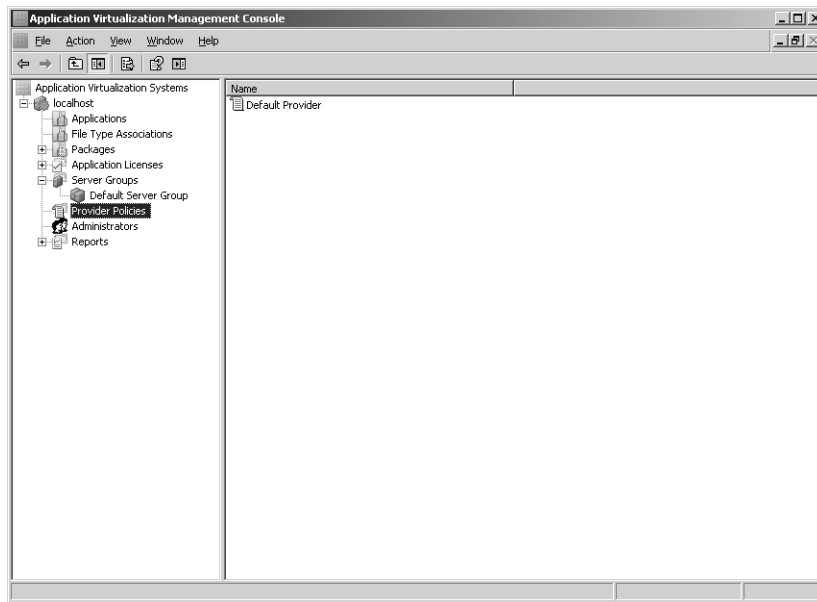


FIGURE 4-18 The Provider Policies node.

Administrators

The Administrators node lets you view the group specified during installation as responsible for the administration of your App-V system. You can also add new groups to this node or remove groups you no longer need.

For more information on using the App-V Management Console to manage an App-V system, see the "Operations Guide for the Application Virtualization System" in the TechCenter Library on Microsoft TechNet at <http://technet.microsoft.com/en-us/library/cc843770.aspx>.

Using the Sequencer

The Sequencer is used to create a virtual application package for an application. The sequencer does this by monitoring and recording the installation and setup processes for an application. The result of sequencing an application is a set of files (.ico, .osd, .sft, .sprj, _manifest.xml, and optionally .msi) that contain all the necessary information for running the application within a virtual environment on the client.

To sequence an application, log on to your sequencing computer and select Microsoft Application Virtualization Sequencer from under Microsoft Application Virtualization in the Programs section of your Start menu. This launches the App-V Sequencer Console as shown in Figure 4-19.

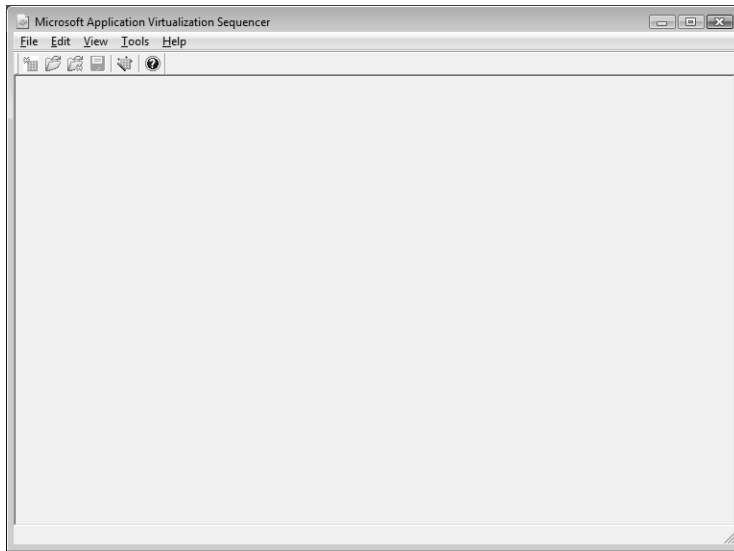


FIGURE 4-19 The App-V Sequencer Console.

From the File menu of your Sequencer Console, select New Package. This launches the Sequencing Wizard and displays the first page of the wizard, which lets you specify a name and add an optional comment for your new package. (See Figure 4-20.)

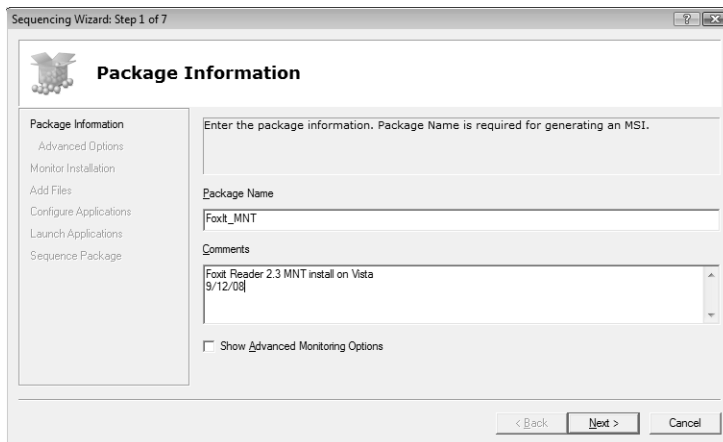


FIGURE 4-20 Specifying a package name, and adding an optional comment.

Select the Show Advanced Monitoring Options check box if you want to display the Advanced Options page of the wizard. The Advanced Options page can be used to specify the block size for your virtual application, which determines how the .sft file will be divided up when the package is streamed to client computers.

The third page of the wizard is called Monitor Installation. (See Figure 4-21.) Click the Begin Monitoring button to start monitoring the installation of your application.



FIGURE 4-21 Monitoring the installation of an application.

After the virtual environment has been loaded, begin installing your application. (See Figure 4-22.)



FIGURE 4-22 Launch setup for your application.

Choose the Custom installation option for your application. (See Figure 4-23.)

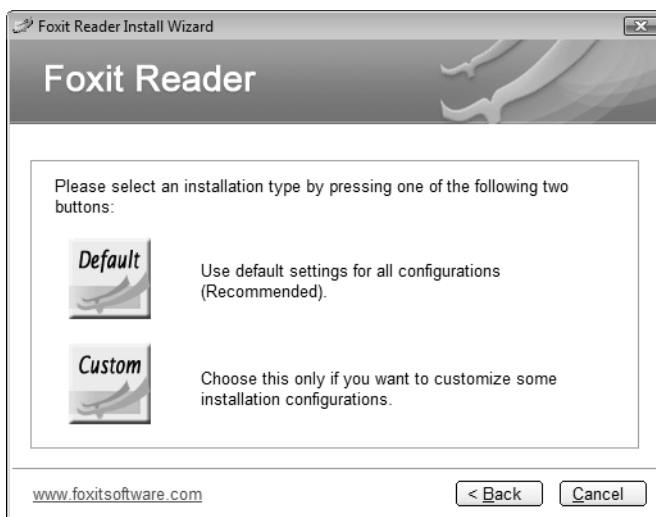


FIGURE 4-23 Select the Custom installation option.

Specify a location on your App-V virtual drive (Q: drive) where the application will be installed. For more information about the Q: drive, see the sidebar titled “Direct from the Source: The Q: Drive” later in the chapter.



FIGURE 4-24 Install the application in a folder on the Q: drive.

After your application has been installed, click the Stop Monitoring button on the Sequencing Wizard.

The next page of the wizard lets you specify additional files to be added to the virtual file system. (See Figure 4-25.) You can also click the Reset button to clear any existing files from the virtual file system.

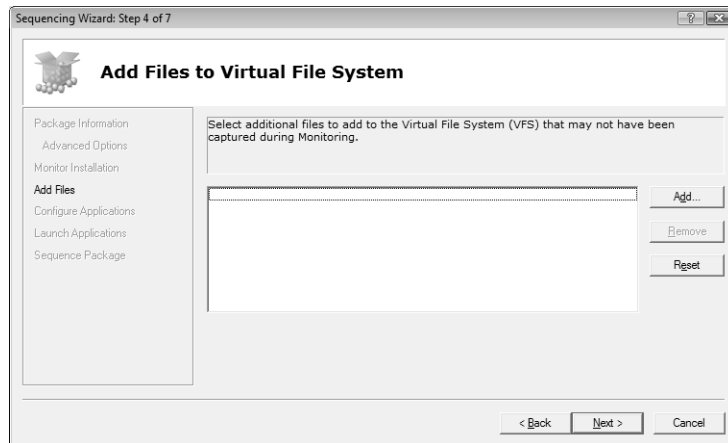


FIGURE 4-25 Adding files to the virtual file system.

On the next page of the Sequencing Wizard, you can configure shortcuts and file associations for the virtual application if needed. (See Figure 4-26.)

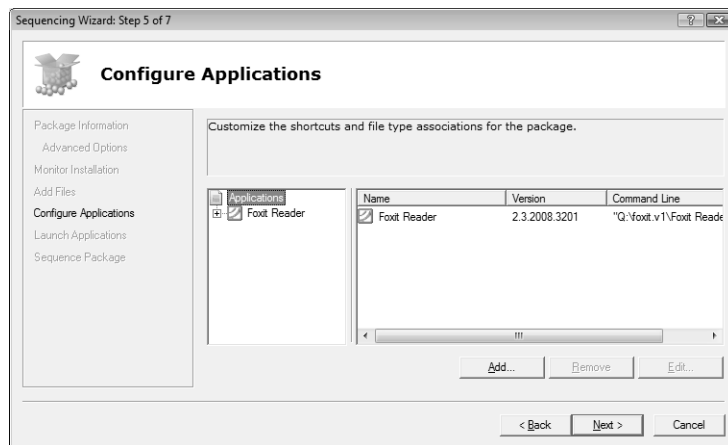


FIGURE 4-26 Configuring shortcuts and file associations for the package.

The next page of the wizard is named Launch Applications. (See Figure 4-27.) Select your application, and click the Launch All button to start the application to ensure that the virtual application package is properly optimized for streaming. Doing this is useful for several reasons:

- It allows you to configure how the application initially runs on client computers.
- It allows you to accept any license agreement for the application prior to making the application available to users.

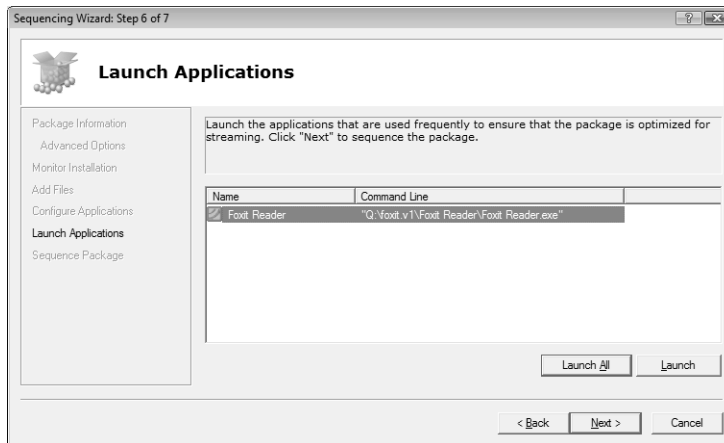


FIGURE 4-27 The Launch Applications page of the wizard.

When you have finished with this step, click Next to sequence the application. The final page of the wizard, named Sequence Package, appears and displays the progress of the sequencing process. (See Figure 4-28.)

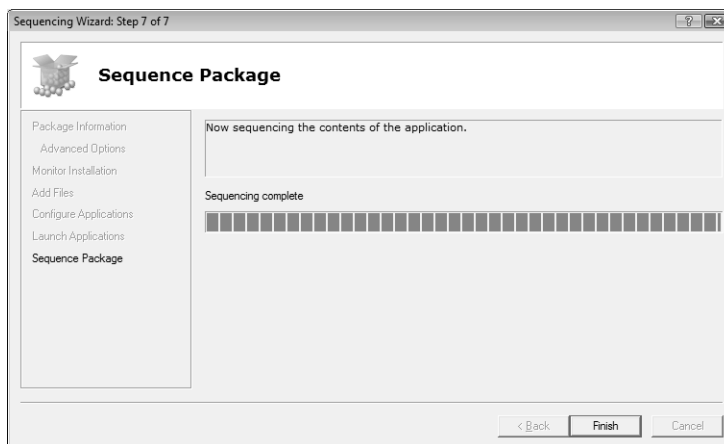


FIGURE 4-28 Sequencing progress.

When the sequencing process is complete, click Finish to close the wizard and return to the App-V Sequencer Console. The console now displays the results of the sequencing operation. The Properties tab shows basic information for the package, such as creation date, maximum block size, launch size, compression algorithm, and block size. (See Figure 4-29.)

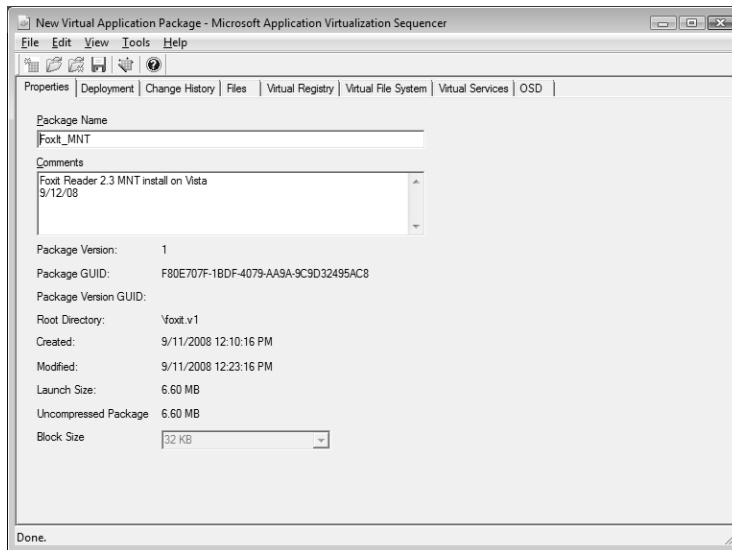


FIGURE 4-29 Properties tab of the new package.

The Deployment tab lets you configure the streaming protocol, Streaming Server, port, application path, supported operating systems, and other options. (See Figure 4-30.) You can also select the Generate Microsoft Windows Installer (MSI) Package check box on this tab to generate an .msi file for the package.

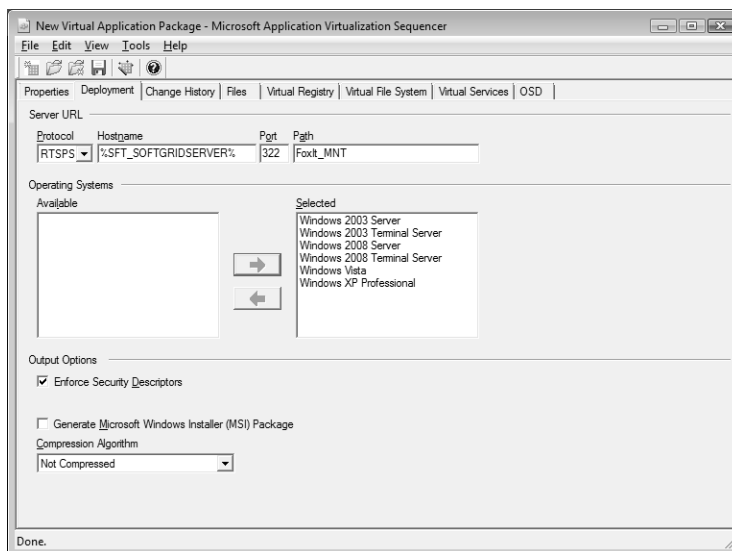


FIGURE 4-30 Deployment tab of the package.

The Change History tab displays the version history of the virtual application package.

The Files tab displays the files the application copied, modified, or created and where those files reside. (See Figure 4-31.)

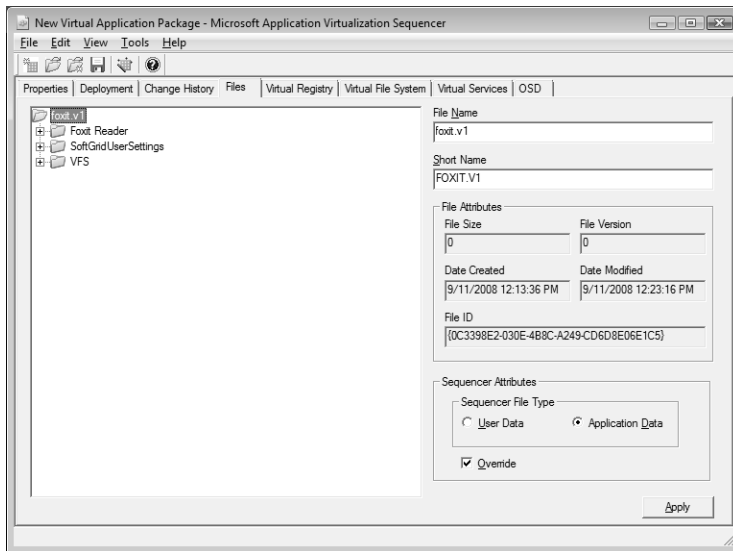


FIGURE 4-31 Files tab of the package.

The Virtual Registry tab displays every registry setting that was created or modified and lets you view or change the settings and manually create or delete keys and values. (See Figure 4-32.)

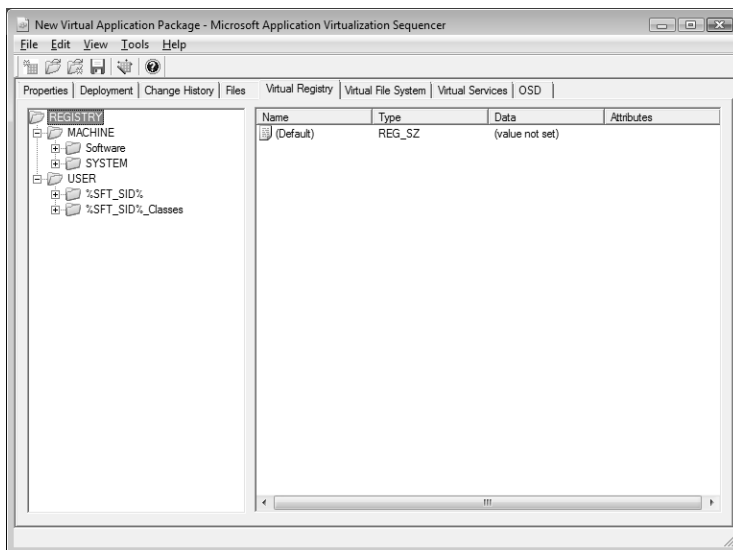


FIGURE 4-32 Virtual Registry tab of the package.

The Virtual File System tab displays the hierarchical directory of the files that comprise the package in common system folders.

The Virtual Services tab displays information about any Windows services that were detected and that are included as part of the sequence. (See Figure 4-33.)

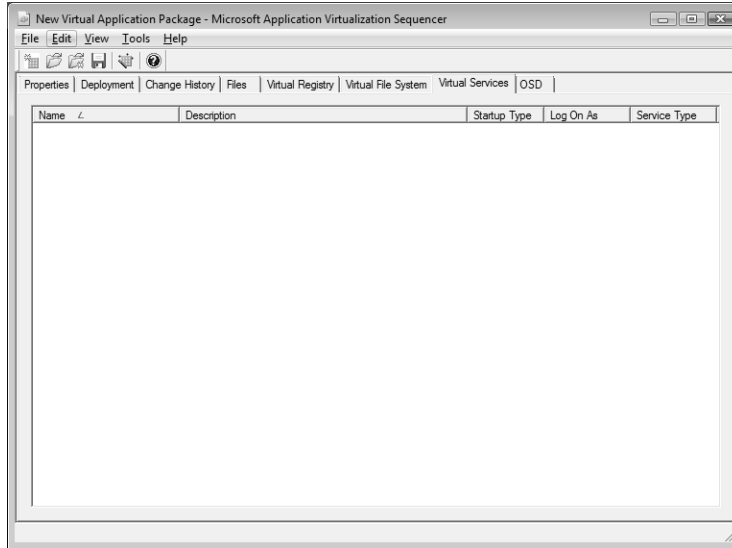


FIGURE 4-33 Virtual Services tab of the package.

Finally, the OSD tab displays a hierarchical representation of the .xml descriptor file contents and lets you modify these values if needed to suit the application.

After you've reviewed your package settings and modified them as needed, select Save from the File menu and specify the name and location where your package should be saved. (See Figure 4-34.)

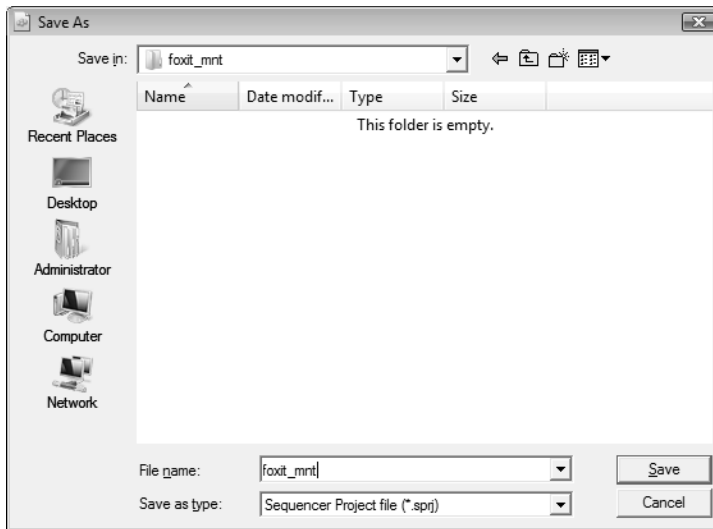


FIGURE 4-34 Saving the package.

Direct from the Source: The Q: Drive

As you may well be aware, one of the best practices for sequencing an application is to have the application install itself during the monitoring phase to an 8.3 directory on the Q: drive. What came up during launch of App-V is the need for deeper clarification on the reasons and even an extension to this particular best practice.

During sequencing, you enter the information in the package configuration phase that is common for all .osd files in the suite, and then you enter what is called the “installation phase.” It is during this phase that you Install, Test, and Configure the application or applications being virtualized. Also during this phase, the Sequencer monitors the actual installation of the application so that it can capture all of the files, registry settings, COM settings, embedded services, fonts, and so on that the application would normally lay down on a client during its native install.

The best practice states, “You should install the application to an 8.3 root directory on the Q: drive of the Sequencer. Each installer in the package should then have its own subdirectory under this 8.3 root. For example, if sequencing Microsoft Office 2007, during the installation phase the installer of Office will ask you where it should install into:

- Default: C:\Program Files\Microsoft Office\
- Best Practice: Q:\Off2k7.v1\Microsoft Office\

In the preceding example, we followed the best practice with an 8.3 root and each piece of the suite having its own subdirectory. If we were to add Microsoft

Communicator to this SoftGrid suite, we would put it during the monitoring phase into the Q:\Off2k7.v1\Microsoft Office Communicator\ folder.

But why?

Good question. Let's break this into pieces, shall we?

Question: "Why do I need to install it to Q:\?"

Answer: The App-V System has been built to try to remove any restrictions on where you install applications to during sequencing and which drive is used for the App-V File System on your deployed clients. This is done by searching for paths in the sequenced application that point to the installed path and replacing them with the variable *%SFT_MNT%*. However, some applications might have paths hard-coded in nonstandard configuration files that are not found by App-V. When that happens, the application will stream to the client, launch into the virtual environment and look to Q:\, yet the Mount Point of the client might actually be B:\ and the application will not work properly.

Essentially, the application is looking for what it was always told to look for, yet when it gets there its ideal does not exist.

Question: "Why do I need to install it to an 8.3?"

Answer: Most, if not all, applications will generate a backward-compatible 8.3 directory name even when they install into a long folder name. If you do not even remember the days when we were limited by our directory and file names to an 8.3 convention please, do me a favor, and just skip ahead. You're too young. Now an application such as Microsoft Office 2000 will install into a long folder of "Microsoft Office." When it auto-generates the 8.3, it follows the algorithm of first 6 characters, a tilde (~) and a number (1). So Office 2000 would be Micros~1.

Following proper sequencing practices, you would revert the Sequencer back to its clean state at the end of every successful sequence and start over fresh. If you were then to sequence Office 2003, it would install to a long folder of "Microsoft Office" again. And again, because the Sequencer is clean, it would autocreate its 8.3 as Micros~1.

So if you stream these two packages to a single client, there is a short name collision. By specifying an 8.3 name, you avoid the autogenerated short name and generate packages that won't have the short name collision.

Question: "Why should I put each component of the suite in its own subdirectory of the 8.3 root?"

Answer: Even if it is its own single application and no other applications will coexist in the suite, it should get its subdirectory under the 8.3 root. In the path of the

application, it might have been “told” to always look under the relative path to that directory for its components. For example, Microsoft Office Help is coded to always look to a path relative to “Microsoft Office.” In the preceding example, the Q:\Off2k7 takes the place of the C:\Program Files and the \Microsoft Office is still in its expected relative path.

Question: “When I click Stop Monitoring, the sequencer prompts me to select the directory that the application was installed to. Why do I have to choose the 8.3 root as the directory the application was installed to? Why wouldn’t I select the actual subdirectory of the 8.3 root?”

Answer: Primarily because you did install the application to the 8.3 root, albeit you put it into a subdirectory of that root. What if you had installed both Office and Communicator to the same 8.3 root during the same sequence? By selecting the 8.3 root, you avoid the short path generation we mentioned previously.

Also, by selecting the 8.3 root here you are essentially saying, “OK. I installed the bulk of the assets under this root. But as with almost all applications, some files went to common folders such as C:\Windows\System32.”

The Sequencer caught those common file locations. And it is at this point, as a result of you selecting the 8.3 root as the install folder, that the Sequencer will then create the Virtual File System (VFS) structure. As you may well know, the VFS folder structure and the Virtual Environment file get placed in whatever directory is selected at the end of monitoring. These are two components that are shared by all applications in this suite.

What you will end up with is the following:

Q:\Off2k7

 \Microsoft Office

 \Microsoft Office Communicator

 \VFS

 \Osguard.cp

When teaching the App-V class, I used to use this analogy:

- Q:\ is the town in which you live.
- The 8.3 root is your house.
- The First Subdirectory (Microsoft Office) is the boys’ bedroom.
- The second subdirectory (Microsoft Office Communicator) is the girls’ bedroom.

- The VFS directory is the common dining room.
- The Osguard.cp file is the common rumpus room.
- Each child (application) gets his or her own bedroom where the bulk of that child's assets live, but they all share the common areas of the dining room and the rumpus room.

I hope this better clarifies the what and the why behind the 8.3 root.

*—Sean Donahue, Senior Program Manager,
System Center Alliance. Microsoft Corporation*



More Info For more information on using the App-V Sequencer to sequence applications, see "Operations Guide for the Application Virtualization System" in the Virtualization TechCenter Library on Microsoft TechNet at <http://technet.microsoft.com/en-us/library/cc843770.aspx>.

Working with App-V Clients

App-V Clients are small programs residing on desktop computers or terminal servers that communicate and authenticate with the App-V Server, receive the streamed application code, and enable the application to be executed for the user to use it. Administrators can configure the App-V Desktop Client and App-V Terminal Services Client and manage applications by using the Application Virtualization Client console.

Applications

The Applications node in this console can be used to manually manage virtual applications. (See Figure 4-35.) By selecting this node and then right-clicking on an virtual application, you can perform various tasks, such as the following:

- Load or unload an application from the cache.
- Clear an application from the console, which also removes the application's settings, shortcuts, and file type associations.
- Repair an application to remove any customizations and restore the application's default settings.
- Import an application into the cache.
- Lock or unlock an application. (A locked application cannot be removed from the cache to make room for new applications.)
- Delete an application, which means that the application will no longer be available to any users on that client. This operation also removes any shortcuts and file type

associations for the application. The operation also removes the application from the cache unless another application refers to the selected application's file system cache data.

- Change the icon associated with an application.
- Manually add an application to the client by selecting New Application from the shortcut menu.
- Publish shortcuts to an application on the desktop, Quick Launch toolbar, Send To menu, Programs section of the Start menu, or some other location.

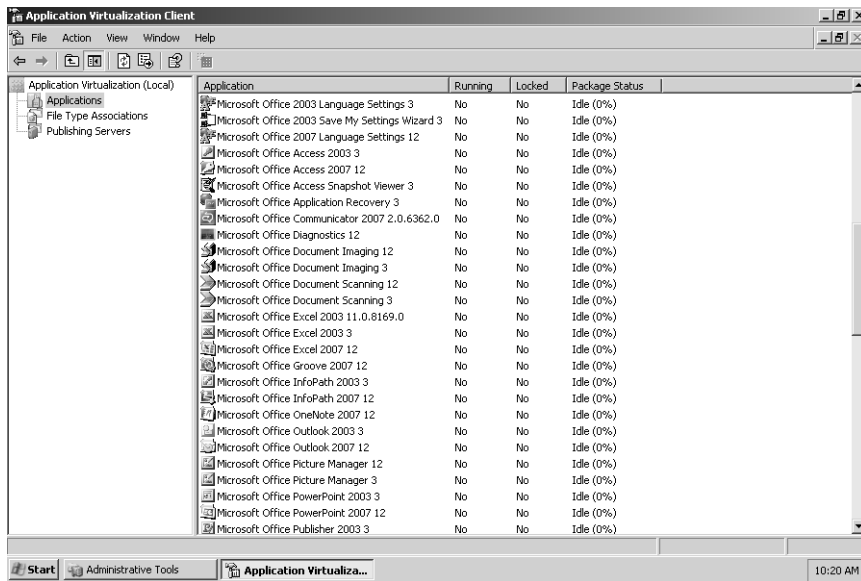


FIGURE 4-35 Managing applications using the Application Virtualization Client console.

You can also right-click on the Applications node itself to perform the following actions:

- Change the cache size and drive letter designation for the client.
- Change the log reporting level for the client.
- Modify user access permissions for the client.
- Configure the import search path where the client looks for .sft files when you try to import them.

File Type Associations

The File Type Associations node of the Application Virtualization Client console lets you add or delete a file type association for the application. When you add a new file association, you specify the file name extension, whether the new file type association should be global for all users, and which existing file type the new extension should be associated with.

Publishing Servers

The Publishing Servers node lets you set up new publishing servers and perform related tasks on the client. (See Figure 4-36.)

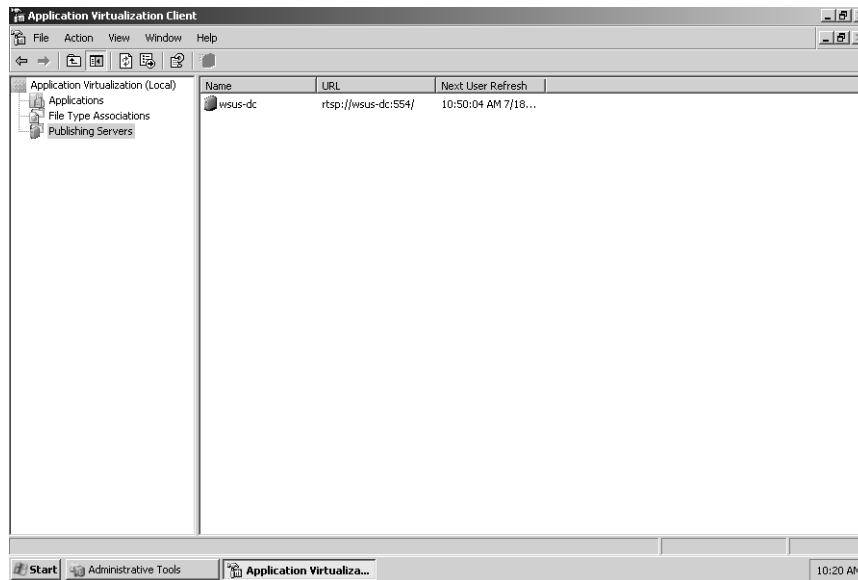


FIGURE 4-36 Managing publishing servers using the Application Virtualization Client console.

For example, to set up a new publishing server, first add the server by right-clicking on the Publishing Servers node and selecting New Server. Follow the steps of the wizard to specify a display name and select a server type. The supported server types are these:

- Application Virtualization Server—Uses RTSP as its streaming protocol
- Enhanced Security Application Virtualization Server—Uses RTSPS as its streaming protocol
- Standard HTTP Server—Uses HTTP as its streaming protocol
- Enhanced Security HTTP Server—Uses HTTPS as its streaming protocol

After you have added the publishing server, right-click on it and select Properties to display its Properties dialog box. You can use the tabs on this dialog box to configure the following:

- Server name and type
- Host name and port
- Whether to refresh publishing on user login
- Publishing refresh rate

Managing App-V Clients from the Command Line

You can also manage App-V Clients from the command line by using the SFTMIME command. For example, to add a virtual application package for all users of the computer, type **SFTMIME ADD PACKAGE:<name> /MANIFEST <path> /GLOBAL** at the command prompt.

For more information on using the SFTMIME command to manage App-V Clients, see the SFTMIME Command Reference on Microsoft TechNet at <http://technet.microsoft.com/en-us/library/cc817090.aspx>.

Direct from the Source: App-V Troubleshooting

The following are some tips for troubleshooting different aspects of an App-V system.

Troubleshooting Publishing and Streaming Issues

A common problem among those who are new to App-V is understanding how application publishing works with App-V and what paths, directories, and protocols are involved when using classic streaming-based publishing when a Management Server is involved. It's somewhat unfortunate that the publishing process does not take full advantage of the existing delivery channel—RTSP or its secure version RTSPS—that already exists between the server and client components, but that's just the way it is as of now.

Sometimes confusion also stems from the purpose of the various file formats used by App-V not being understood thoroughly. Each App-V virtual application package consists of a package data file (SFT) and a bunch of help files (an OSD file for describing one individual application from the package data file, an ICO file for creating the short-cut, and so on), some of which are delivered using different methods than the others.

When troubleshooting application publishing and streaming problems, you should double-check all the components involved. Following are a few things to check for that affect the delivery and visibility of the applications.

One thing to check is the content directory path, which is the file system path you need to select during the installation of every App-V server. This directory represents a logical starting point for the service that listens on the network for the clients' requests. The content directory path, as defined during installation (for example, C:\content\), is used solely by the App-V service on the server when it tries to find physical SFT files for streaming. If you ever see or define this path in any of the management screens, that's an error because the server itself handles SFT delivery through RTSP or RTSPS channels. When using the classic application delivery with App-V, SFT files cannot be published through UNC paths or HTTP URLs (except, of course, if you are using that new-fangled HTTP-streaming introduced in 4.5, but that's a whole different scenario).

Also check the package relative path. This path is the one you see under the Packages node in the Management Console for each version of each package (for example, myapp\package.sft). This path usually resolves correctly automatically when you have imported App-V packages, but sometimes it might be incorrect if the person who packaged the virtual application wasn't careful. The import procedure reads this relative path from the first OSD file for each package it imports. This path is the second piece of information that the App-V Management Server uses to find a package a client requests when it tries to stream something in. Just as the content directory path was the logical starting point, this relative path is the logical conclusion of that path. Together, they form a full, valid file system path to SFT file (for example, C:\content\ + myapp\package.sft = C:\content\myapp\package.sft).

Completely unrelated path settings from the ones just described are the OSD and ICO paths. These paths, as defined in the application publishing records (the screen you get when running Import in the Management Console), are delivered by the Management Server to the App-V Client when it issues a refresh operation against the server. Refresh, as the name implies, refreshes the client's list of applications that are known to the user under which the refresh is running.

Part of this procedure, in addition to getting the list of applications available for the user, is to get paths to the OSD and ICO files. The content of those files are not delivered as part of the refresh data itself, but rather as a separate reference. So you have a choice of which delivery channel you want to use: a file system path (effectively a UNC path) or an HTTP URL. And here's what causes so much confusion: because you can actually use a file system path as OSD and ICO paths, you are tricked into thinking that those paths can refer to content directory using server's local path (for example, C:\content\myapp\myapp.osd) or in the way relative package paths are used for SFT files (for example, myapp\myapp.osd). The issue, however, is that those paths are not interpreted by the server but by the client when it gets the paths as part of a refresh operation and the client doesn't have C:\content\ to get OSDs and ICOs from! To make matters worse, the Management Console defaults to using whatever path you used to browse to SPRJ (the project file that rules all other files) as OSD and ICO paths, unless you happened to set something called Default Content Path before the import.

Troubleshooting Virtual Service Issues

Not many packages contain virtual services because services are normally associated more with server-side software. However, sometimes virtual services do exist in an App-V package. Virtual services are very straightforward (the App-V Sequencer picks up newly created services during packaging) and people tend not to touch them. There are some catches to using them, and being aware of those oddities might help in the longer run.

The first issue with the virtual services is what the startup type of Automatic causes to happen on the client side. Because virtual services do not exist on the client system's real service list, nothing starts them automatically when you start your machine. As a result, the App-V Client must start virtual services just before the main application starts from the package. Sometimes these services will start fast enough, but there are some type of services and environmental conditions that cause them to take some time. And this additional time, much to the dismay of the user starting the application, results in delaying the startup of the actual application. And if there are many such services in the package, the delay can be even longer, causing the user to wonder if the start of the application failed for some reason.

The solution? Either set virtual services to start manually if possible or disable virtual services totally if they are not needed. In the case where such services were present in the package, the application launch time exceeded one minute solely because of slow-starting services, and changing to a manual start caused the launch time to drop to a reasonable level.

Another issue that might arise with virtual services is a conflict with the locally present identical service. This is not uncommon with some software licensing components that install themselves as services. If you happen to use multiple products that use that same licensing service, each one might contain a virtual copy if they are sequenced separately. Typically, what happens is that the copy that starts first (either the one on the virtual machine or the one on the local machine) will run perfectly, but any subsequent copies will not. The service will either terminate on start or consume lots of CPU time when trying to do something that overlaps with the existing instance.

The solution? There's no easy way out of this problem, but something worth trying is to disable all but one copy of the service. Usually, the locally installed service is preferred, as the ordering of which virtual application (and thus the virtual service in it) will launch first is unknown.

—Kalle Saunamäki, MVP

Key Features of App-V

The preceding overview of Microsoft Application Virtualization has already introduced you to many of the capabilities and features of App-V. However, to summarize, let's compare the key features of App-V to the earlier SoftGrid Application Virtualization platform. We'll examine these features under four broad areas:

- Dynamic Suite Composition
- Enhanced scalability

- Globalization
- Enhanced security

Dynamic Suite Composition

App-V now includes Dynamic Suite Composition (DSC), which provides a method for administrators to control which virtual applications will be combined to create a unified, virtual working environment for an application set. DSC also provides a way for administrators to specify mandatory or optional dependencies between virtual applications. This means that when a virtual application is run on the client, it will also launch the dependent virtual application's environment, allowing for the combination of both virtual environments.

DSC also enables a one-to-many scenario for middleware applications. For example, let's say that you have some applications that require the Java Runtime Environment (JRE). You first sequence the JRE into its own virtual application. Then you reset the Sequencer, install the JRE locally, and sequence the dependent application. This creates a dependency between the single virtual JRE package and the different virtual dependent applications that enables multiple virtual applications to share the same virtual JRE package. DSC also reduces the sequencing overhead because only one JRE needs to be sequenced instead of having to re-sequence the JRE into each individual package. Package updates are also simplified because you need to update only the single JRE package instead of multiple packages.

Enhanced Scalability

App-V provides numerous scalability improvements. For example, App-V has flexible deployment modes and is interoperable with Microsoft Systems Management Server (SMS), Microsoft System Center Configuration Manager (SCCM), and third-party ESD systems. App-V also supports a standalone mode for virtual application delivery and has increased supportability over the earlier SoftGrid version. These scalability enhancements can benefit enterprises of all sizes, especially those with branch offices and those that have existing ESD systems in place.

Other scalability enhancements in this version include the following:

- **Background streaming with autoloading options** The client stream policy can be set so that the entire virtual application will be delivered on first launch or on login. The application can also be used while it is still streaming in the background.
- **Offline availability** The virtual application can be accessed when offline as well as online.
- **More applications** The DSC capabilities described earlier, together with the enhanced support for side-by-side applications, expands the number of applications that can be serviced by the platform.

- **Application source root** The Application Source Root (ASR) is the capability to specify a server name through Group Policy or a script on the target client. When the manifest or domain controller refresh occurs, the .osd file in its current state is delivered to the client. However, at runtime, the ASR value replaces the DNS server name in the RSTP URL of the .osd file. This will now route the stream request to the ASR server name. This server is typically a server that is local to the client.
- **Windows Server 2008 Terminal Services support** Application Virtualization for Terminal Services now supports Microsoft Windows Server 2008 Terminal Services, 32-bit only.
- **Enhanced data metering** The App-V Windows Management Instrumentation (WMI) provider collects application usage information and provides a simplified way to pull the data into your organization's reporting store. Data metering can even occur while users are offline.
- **Microsoft Update** App-V includes Microsoft Update support for virtualized applications at sequencing time (but this is not available at runtime).
- **Backup and recovery** App-V includes Volume Shadow Copy Service (VSS) Writer support.
- **Enhanced management** You can manage your App-V system using tools such as the System Center Operations Manager 2007 Management Pack, ADM template, and Best Practice Analyzer.
- **Improved diagnostics** App-V has Watson integration and event log support on both the client and the server.
- **MSI creation capability** App-V allows for MSI creation for standalone use. App-V also supports streaming MSIs, where MSI sets up the virtual application and settings but the application is streamed from the server when the user clicks on the application.
- **Enhanced command-line interface** Additional capabilities for batch operations are provided by the SFTMIME command. Batch MSI creation is also supported.
- **Differential SFTs** App-V allows for the creation of SFTs with only sequenced differences (updates) for use with standalone mode only (merged by client action).

Globalization

The new globalization and localization features of App-V now support localized applications and operating systems. Specific enhancements include

- Installation on any Windows language version supported by the earlier SoftGrid version.
- Installation in mixed-language environments (server/client). For example, a Japanese employee traveling to his German branch office could use the Japanese App-V Client with the German App-V Server.

- Autodetecting the system and user locale, and autoloading the appropriate resource files.
- Respecting all user locale and regional settings.
- Sequencing non-English or localized applications.
- Support for foreign language applications with special characters.
- Foreign language Active Directory and server support.
- Run-time locale detection.
- Localization in 12 Languages: Brazilian Portuguese, Chinese (Simplified), Chinese (Traditional), Dutch (client only), French, German, Italian, Japanese, Korean, Russian, and Spanish.

Enhanced Security

The enhanced security features in this version of App-V include

- Support for Internet-facing scenarios where users run virtual applications over the Internet without the need of using a VPN connection. App-V can now securely provide virtual applications to users when both the App-V Server and the App-V Client are on untrusted networks.
- A secure-by-default configuration out-of-the-box that includes
 - Locked-down client privileges
 - TLS on by default
 - Kerberos support
 - Certificate-based server authentication

Key Benefits of App-V

Some of the key benefits of deploying an App-V infrastructure within your organization can include

- Centralized management of the entire application life cycle
- Faster application deployment
- Simplified application versioning
- Fewer side-by-side application compatibility issues
- Reduced need for regression testing
- On-demand application delivery
- Integrates with existing Terminal Services or ESD infrastructures

Usage Scenarios for App-V

App-V now supports a wide range of different usage scenarios, ranging from a full application virtualization infrastructure to a lightweight infrastructure to standalone deployment. Specifically, App-V supports the following usage scenarios:

- **Full Infrastructure** This scenario uses the App-V Management Server, which provides full streaming capabilities, Desktop Configuration Service, active/package upgrade, and basic licensing and metering. This infrastructure requires Active Directory and SQL Server and is an update to the existing SoftGrid Virtual Application Server that version 4.2 customers are familiar with using.
- **Lightweight Infrastructure** This scenario uses the App-V Streaming Server, which includes streaming capabilities such as active/package upgrade without the Active Directory or SQL Server requirements. However, it does not have a Desktop Configuration Service or licensing or metering capabilities. This service relies on the manual or scripted addition of a manifest file for virtual application configuration. The Desktop Configuration Service of the App-V Management Server can also be used in conjunction with the App-V Streaming Server such that the Management Server configures the application but the Streaming Server delivers it.
- **Standalone Mode** The App-V Sequencer now has an option to create an .msi file that automates the addition of the virtual application. The .msi contains metadata so that an ESD system can recognize it and control the virtualized applications. Standalone mode requires the App-V Client to go into standalone mode, which allows only .msi-based updates of the virtual applications. (Streaming is not allowed while in standalone mode.) This mode is meant for rarely connected users that need the power of virtualized applications but do not have access to a server.

For more information about various App-V usage scenarios, see the section titled “App-V Deployment Scenarios” earlier in this chapter.

Additional Resources

The resources listed in this section were either referred to in the chapter or provide additional information concerning concepts and products discussed in this chapter.

General

A general overview of the features and benefits of Microsoft Application Virtualization can be found at <http://www.microsoft.com/virtualization/solution-product-sgav.mspx>.

The launching page for App-V product information is <http://www.microsoft.com/systemcenter/softgrid/default.mspx>.

For detailed technical information concerning App-V, see the Application Virtualization TechCenter on Microsoft TechNet at <http://technet.microsoft.com/en-us/appvirtualization/default.aspx>.

Deployment App-V

Planning and Deployment Guide for the Application Virtualization System can be found at <http://technet.microsoft.com/en-us/library/cc843778.aspx>.

Also, be sure to review Microsoft Application Virtualization Management System Release Notes at <http://technet.microsoft.com/en-us/library/cc817171.aspx> prior to deploying App-V within your organization.

If you plan on upgrading your existing SoftGrid 4.2 system to App-V, be sure to review the Upgrading to Microsoft Application Virtualization 4.5 Frequently Asked Questions article found at <http://technet.microsoft.com/en-us/appvirtualization/cc664494.aspx>.

Managing and Maintaining App-V

Operations Guide for the Application Virtualization System can be found at <http://technet.microsoft.com/en-us/library/cc843770.aspx>.

Also, be sure to read the various white papers available on the Application Virtualization 4.5 Documentation section of the Application Virtualization TechCenter at <http://technet.microsoft.com/en-us/appvirtualization/cc843994.aspx>.

App-V Team Blog

To keep abreast of the latest developments and tips about App-V, subscribe to the RSS feed for the App-V Team Blog at <http://blogs.technet.com/softgrid/default.aspx>.

App-V Forums on TechNet

To ask questions about App-V or SoftGrid, or to help others with their questions, use the Microsoft SoftGrid Application Virtualization forum on Microsoft TechNet at <http://forums.microsoft.com/TechNet/default.aspx?ForumGroupID=497&SiteID=17>.

Chapter 5

Presentation Virtualization— Terminal Services

Another component of Microsoft's integrated Virtualization 360 strategy is Terminal Services, one of the core virtualization technologies available in Windows Server 2008. Terminal Services is Microsoft's presentation virtualization solution, and by leveraging this solution businesses can simplify application deployment, increase security, and make remote workers more efficient. This chapter examines the new and enhanced features and components of Terminal Services in Windows Server 2008, explains how each Terminal Services component works, summarizes their benefits, and looks at different usage scenarios whereby businesses can benefit from deploying them.

Understanding Presentation Virtualization

Presentation virtualization involves separating an application's user interface from the physical computer on which the application actually runs. Presentation thus allows you to run an application in one location (the user's computer or mobile device) while deploying, configuring, and maintaining the application in a different location (a centrally located server in the datacenter). Presentation virtualization thus fits within the overall concept of virtualization as being any technology that isolates or unbinds one layer of computing resources from another.

Windows Server 2008 Terminal Services provides just this kind of capability by decoupling application presentation (the user's experience of working with an application) from application execution (where the application is actually run). For more information on how Terminal Services works, see the section titled "Understanding Terminal Services" later in this chapter.

Implementing a presentation virtualization solution is a relatively straightforward process. After making appropriate planning decisions with regard to server placement, performance, capacity, and other issues, the administrator configures a Windows Server 2008 server as a terminal server by installing one or more Terminal Services role services on the computer. The administrator then installs the applications on the terminal server that users will need to perform their job.

Once the terminal server is configured and applications are properly installed, the terminal server can be used to "present" users of desktop or mobile computers or of mobile computing devices with just the applications the user needs to perform her job. The applications the user uses are actually running on the terminal server and are thus remote applications,

not local applications. Yet from the user's point of view these remote applications look and behave as if they were locally installed on the user's own computer.

Terminal Services can also be used to provide users with entire remote desktops, secure access to remote applications over the Internet, the ability to print from remote applications to a locally attached print device, and other features. In addition, terminal servers can be grouped together into server farms to provide load balancing and redundancy for larger deployments.

As we proceed through this chapter, we'll examine each of these different presentation virtualization technologies and features.

New Features of Terminal Services in Windows Server 2008

Terminal Services has been around on Windows platforms since Windows NT 4.0 Terminal Server Edition. As Terminal Services evolved through the Windows 2000 Server and Windows Server 2003 platform, new features and capabilities were added to enhance the flexibility, manageability, and security of Terminal Services. With Windows Server 2008, however, major enhancements were made to Terminal Services to provide organizations with more options for how they can implement a presentation virtualization solution that meets their business needs. This section summarizes these new features and enhancements of Terminal Services in Windows Server 2008, while later sections in this chapter dive deeper into the workings and benefits of each new technology.



More Info For more information concerning Windows Server 2008 Terminal Services, see the Windows Server 2008 Terminal Services Resource Kit from Microsoft Press (<http://www.microsoft.com/MSPress/books/12716.aspx>)

Enhancements to Terminal Services Core Functionality

The core functionality of the Terminal Services role has been significantly enhanced in Windows Server 2008. These enhancements were made to improve the user experience of remotely connecting to terminal servers and include a new version of the Remote Desktop Connection (RDC) client that has improved display capabilities, support for Plug and Play (PnP) device redirection for certain types of devices, support for Terminal Services single sign-on, and support for Microsoft Point of Service for .NET device redirection. The sections that follow briefly discuss each of these features.

Remote Desktop Connection 6.1

Windows Server 2008 includes Remote Desktop Connection (RDC) 6.1, a new version of the RDC client software used to remotely connect to a terminal server or to any Windows computer that has the Remote Desktop feature enabled using the Remote Desktop Protocol (RDP) 6.1. RDC is also available on the following Windows client platforms:

- Windows Vista with Service Pack 1
- Windows XP with Service Pack 2 or higher

Unless otherwise indicated, the display and device redirection enhancements described in the sections that follow are available when either Remote Desktop Connection 6.0 is used.

Remote Desktop Connection Display Improvements

The display improvements added in RDC 6.x include support for

- Widescreen monitors
- Monitor spanning
- Font smoothing
- Display data prioritization
- Desktop Experience

Widescreen Monitor Support RDC 5.x on previous versions of Windows supported only monitors having a display ratio of 4:3 and a maximum resolution of 1600 by 1200. With RDC 6.x, however, support for additional display resolution ratios up to 4096 by 2048 is now available, making it possible to use newer widescreen large monitors over remote connections. Such monitors typically support display resolutions of 1680 by 1050, 1920 by 1200, or higher, and can have aspect ratios of 16:9 or 16:10.

You can use the `Mstsc.exe` command and specify the width and height of the display in order to open Remote Desktop Connection using a custom display resolution. For example, the following command will launch the Remote Desktop Connection client using a display resolution of 1920 by 1200:

`mstsc.exe /w:1920 /h:1200`

Custom display resolutions can also be configured by manually editing the `.rdp` file for a saved Remote Desktop Connection configuration as follows:

```
desktopwidth:i:<value>
```

```
desktopheight:i:<value>
```

Monitor Spanning RDC 6.x allows you to spread the display of a remote session over multiple monitors if these monitors all use the same display resolution and the total resolution across all monitors does not exceed the maximum supported display resolution of 4096 by 2048.

You can use the `Mstsc.exe` command with the `/span` switch to open Remote Desktop Connection using monitor spanning. For example, the following command launches the Remote Desktop Connection client using monitor spanning:

mstsc.exe /span

Monitor spanning can also be configured by manually editing the `.rdp` file for a saved Remote Desktop Connection configuration as follows:

```
span:i:<value>
```

A value of 1 enables monitor spanning, while 0 disables the feature.

Font Smoothing RDC 6.x enables ClearType font smoothing to work over a remote session to a Windows Server 2008 terminal server. ClearType allows computer fonts to display smoothly when using an LCD monitor. ClearType is enabled by default on Windows Server 2008.

You can enable font smoothing over a remote session by opening the Remote Desktop Connection client, clicking Options, selecting the Experience tab, and selecting Font Smoothing. Note that enabling font smoothing over a remote session increases the amount of network bandwidth used by the connection.

Display Data Prioritization By default, RDP allocates 70 percent of a remote session's bandwidth for display, keyboard, and mouse traffic. The remaining 30 percent is allocated for other traffic, such as file transfer activities or printing. The reason for prioritizing display, keyboard, and mouse traffic is to ensure that the user experience is not degraded during bandwidth-intensive operations such as transferring files or printing documents over a remote session.

RDC 6.x allows you to change the prioritization by manually editing registry values found under the following key on your terminal server:

```
HKLM\SYSTEM\CurrentControlSet\Services\TermDD
```

Table 5-1 lists the registry values you can modify and the effect of modifying them. If these registry values do not exist on the client, create them as `DWORD` values. After making these registry changes, you must restart the terminal server for them to take effect.

TABLE 5-1 Registry Values for Configuring Display Data Prioritization

DWORD Value	Description
<i>FlowControlDisable</i>	By setting this value to 1, you disable display data prioritization. This means that all requests are handled on a first-in, first-out basis. The default setting for this value is 0.
<i>FlowControlDisplayBandwidth</i>	By increasing (or decreasing) this value compared to the value of <i>FlowControlChannelBandwidth</i> , you can give greater (or less) priority to display, keyboard, and mouse traffic. The default setting for this value is 70, and the maximum is 255.
<i>FlowControlChannelBandwidth</i>	By increasing (or decreasing) this value compared to the value of <i>FlowControlDisplayBandwidth</i> , you can give greater (or less) priority to any network traffic that is not display, keyboard, or mouse traffic. The default setting for this value is 30, and the maximum is 255.
<i>FlowControlChangePostCompression</i>	By setting this value to 1, you enable flow control to determine bandwidth allocation based on post-compression bytes. The default setting for this value is 0, which determines bandwidth allocation based on precompression bytes.

Desktop Experience Remote Desktop Connection reproduces the desktop of the terminal server over the remote session. By enabling the new Desktop Experience feature on your terminal server, the remote session looks and feels more like the local desktop when used with RDC 6.x. In particular, enabling the Desktop Experience feature makes Windows Vista features such as desktop themes, photo management, Windows Calendar, and Windows Media Player available in the remote session.

To install the Desktop Experience feature on a Windows Server 2008 terminal server, launch the Add Features Wizard from either the Server Manager console or the Initial Configuration Tasks screen.

Plug and Play Device Redirection for Media Players and Digital Cameras

RDC 6.x has enhanced device redirection functionality that supports redirecting Windows Portable Media devices, such as media players that use the Media Transfer Protocol (MTP) and digital cameras that support the Picture Transfer Protocol (PTP). You can enable redirection for PnP devices that have been plugged in and detected by your system. You can also redirect removable drives that are connected after your remote session has been established. You can also make PnP devices you will plug in later available for redirection.

Once your remote session has been established, any PnP device that has been redirected will be automatically installed on the terminal server, and PnP notifications will be displayed in the taskbar in your remote session. You will then be able to use this PnP device with applications running within your remote session.

To enable PnP device redirection, open a Remote Desktop Connection, click Options, select the Local Resources tab, click More, and enable PnP device redirection as desired. (See Figure 5-1.)



FIGURE 5-1 Configuring PnP device redirection on the Remote Desktop Connection client



Note The PnP Device Redirection Framework can also be used for other devices if the vendor makes the device support it.

Single Sign-On for Terminal Services

RDP 6.x supports single sign on (SSO) for Terminal Services, enabling users with domain accounts to log on a single time using a password or a smart card and gain access to remote servers without being prompted to enter their credentials a second time. SSO benefits users by removing the frustration of having to re-enter credentials when accessing a remote desktop or a remote application.

For SSO to work, the following requirements must be met:

- The terminal server must be a domain member and must be running Windows Server 2008.
- The user's computer must be a domain member and must be running Windows Vista or Windows Server 2008.
- The user's account must have appropriate privileges for logging on to both the user's computer and the terminal server.

Microsoft Point of Service for .NET Device Redirection

RDP 6.1 allows you to redirect devices that use the Microsoft Point of Service (POS) for .NET 1.11 if your terminal server is running an x86-based version of Windows Server 2008. Once Microsoft POS for .NET 1.11 has been configured on your terminal server, any Microsoft POS for .NET application installed on the terminal server will be able to access the Microsoft POS for .NET device as if the device was available locally. You can obtain Microsoft POS for .NET 1.11 from the Microsoft Download Center at <http://www.microsoft.com/downloads>.

Terminal Services RemoteApp

Terminal Services RemoteApp (TS RemoteApp) is a new feature of the Windows Server 2008 Terminal Services role that allows you to remote individual applications and not just entire remote desktops as previous versions of Terminal Services were limited to. RemoteApp programs look and feel to the user as if they were locally installed on the user's computer, though these programs are actually running on the terminal server instead.



More Info For more information about TS RemoteApp, see the section titled "Understanding TS RemoteApp" later in this chapter.

Terminal Services Web Access

Terminal Services Web Access (TS Web Access) is a new role service of the Windows Server 2008 Terminal Services role that simplifies the process of deploying both individual RemoteApp programs and entire remote desktops. Using TS Web Access, a user can use a Web browser such as Internet Explorer to connect to a Windows Server 2008 terminal server and launch RemoteApp programs on the terminal server. Users can also use TS Web Access to remotely connect to the desktop of any Windows computer that has the Remote Desktop feature enabled on it.



More Info For more information about TS Web Access, see the section titled "Understanding TS Web Access" later in this chapter.

Terminal Services Gateway

Terminal Services Gateway (TS Gateway) is another new role service of the Windows Server 2008 Terminal Services role that enables remote users to securely connect over the Internet to Windows Server 2008 terminal servers, RemoteApp programs, and computers with

Remote Desktop enabled that are hidden behind a corporate firewall. TS Gateway provides an alternative to virtual private network (VPN) connections as a means for secure access to resources on an organization's internal network.



More Info For more information about TS Gateway, see the section titled "Understanding TS Gateway" later in this chapter.

Terminal Services Session Broker

Terminal Services Session Broker (TS Session Broker) is another new role service of the Windows Server 2008 Terminal Services role that enables users to reconnect to an existing session in a load-balanced terminal server farm. TS Session Broker also includes a new feature called TS Session Broker Load Balancing that allows you to distribute the load between servers in a load-balanced terminal server farm.



More Info For more information about TS Session Broker, see the section titled "Understanding TS Session Broker" later in this chapter.

Terminal Services Licensing

Terminal Services Licensing (TS Licensing) is a role service of the Windows Server 2008 Terminal Services role that allows you to manage Terminal Services client access licenses (TS CALs) for users and devices that connect to your terminal servers. The TS Licensing role service supports managing TS CALs for terminal servers running Windows Server 2008, Windows Server 2003, and Windows 2000 Server.

TS Licensing is discussed briefly in the section titled "Understanding Terminal Services" later in this chapter. For more information about TS Licensing, see the Windows Server 2008 TechCenter on Microsoft TechNet at <http://technet.microsoft.com/en-us/windowsserver/2008/default.aspx>.

Other Enhancements

Two other enhancements to Terminal Services in Windows Server 2008 include

- Terminal Services EasyPrint
- Using Terminal Services together with Windows System Resource Manager

The sections that follow briefly describe these enhancements.

Terminal Services EasyPrint

Terminal Services EasyPrint (TS EasyPrint) allows users to print from a remote session or RemoteApp program to the local or network printers configured on the user's client computer without the need to install additional printer drivers on the terminal server. To accomplish this, TS EasyPrint uses the driver properties from the clients' locally installed print driver so that there is a more consistent printing experience between local and remote sessions.



More Info For more information about TS EasyPrint, see the sidebar titled "Direct from the Source: Understanding TS EasyPrint" in this chapter.



Note TS EasyPrint is available only in TS CAL sessions, not in administrative sessions.

Direct from the Source: Understanding TS EasyPrint

TS EasyPrint is a new feature in Windows Server 2008 that enables users to reliably connect to and print from a terminal server session to a redirected local or network printer installed on the client computer without the need to install printer drivers on the terminal server.

When a user prints from his session to a local printer, he sees the full printer properties dialog box from the local client and has access to all printer functionality. The TS EasyPrint universal driver acts as a proxy and redirects all user interface (UI) calls to the driver on the client. Administrators can also use Group Policy to limit the number of printers redirected to just the default printer, thereby reducing overhead and the number of printers that must be managed.

To use the TS EasyPrint feature in Terminal Services on Windows Server 2008, clients must be running Remote Desktop Connection 6.0 client and have the .NET Framework 3.0 Service Pack 1 (SP1) installed.

The TS EasyPrint feature works seamlessly in mixed platform environments including the following ones:

- Between x86 clients and x64 Windows Server 2008 terminal servers
- Between x64 clients and x86 Windows Server 2008 terminal servers

How TS EasyPrint Works

As shown in Figure 5-2, the document to be printed is rendered as an XPS (XML Paper Specification) document on the Windows Server 2008 terminal server and then transferred to the client, where it is printed using the local print driver. Because

XPS documents can be created and printed on both x86 and x64 platforms and are platform independent, there are not any cross-platform compatibility issues when using EasyPrint.

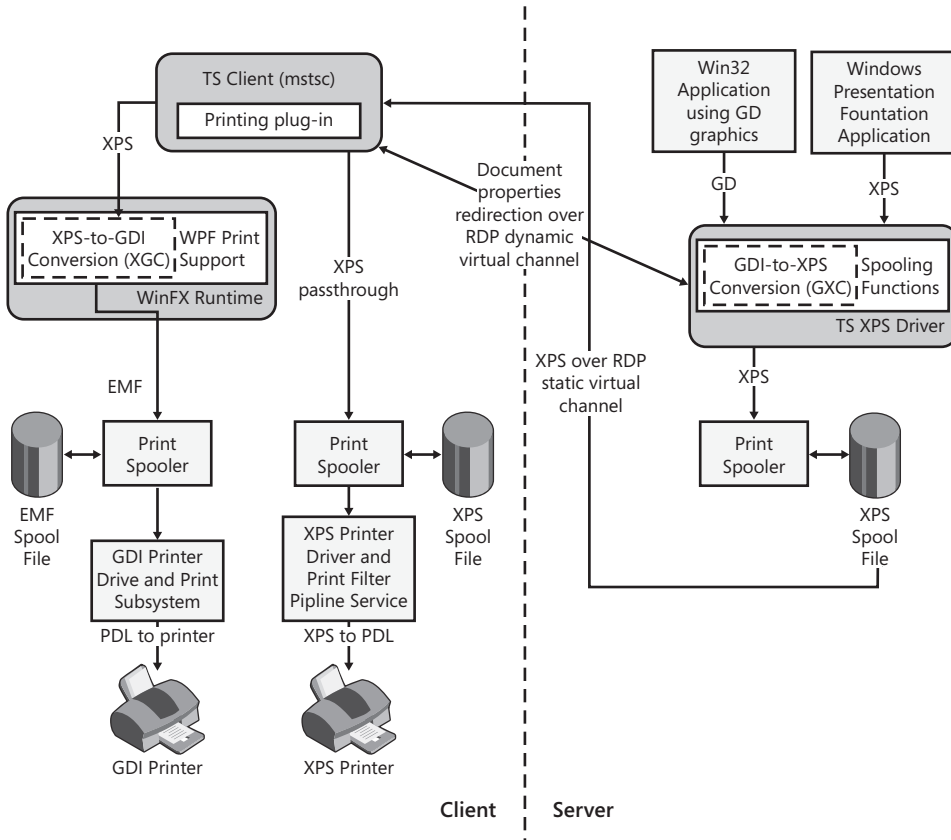


FIGURE 5-2 How TS EasyPrint works

The following steps outline the process that occurs when a Terminal Services user prints a document using TS EasyPrint:

1. A user chooses to print a document from an application in his Terminal Services session.
2. The common print dialog box is displayed, and the user selects a redirected printer.
3. The user selects Preferences or Properties to change the document properties before issuing the print job.
4. The TS EasyPrint driver is loaded for the printer and intercepts this call.

5. The TS EasyPrint driver redirects this call to the RDC client using a virtual channel, which in turn calls the actual printer driver on the client to invoke the Document Properties dialog box from the driver on the client.
6. The user makes the necessary changes to the document properties and clicks OK.
7. The RDC client transmits the user-selected options changes from the local printer driver to the TS EasyPrint Driver on the server.
8. The application reformats the document per the user-selected options and issues the print job.
9. The TS EasyPrint driver processes the job and passes it through the GDI-to-XPS conversion (GXC) routines.
10. GDI-based print jobs are routed through the GDI-to-XPS routines to convert the job to XPS format; WPF-based print jobs do not use the pass-through GDI-to-XPS conversion routines.
11. The server-side spooler generates an XPS spool file and sends it to the client using a static virtual channel.
12. The RDC client receives this XPS spool file.
13. The RDC client queries the printer driver to see if it supports XPS. If it does, the XPS spool file uses the XPS print path on the client. If the printer driver does not specifically support XPS, the XPS spool file is handed off to the WPF print support infrastructure for conversion to GDI using the XPS-to-GDI conversion routines.
14. The print job is then sent to the Print Spooler for printing.

Because the RDC client, *Mstsc.exe*, is a native Win32 application and the WPF printing infrastructure uses managed (.Net Framework) APIs, a managed wrapper is created to support TS EasyPrint. When a document is printed from a remote desktop session using the Easy Print driver on the terminal server, the RDC client calls the managed wrapper, *Tswpfwrp.exe*, to assist with processing the print job on the client. *Tswpfwrp.exe* is used only for TS EasyPrint redirected printer functionality and is invoked only when printing.

The wrapper (*Tswpfwrp.exe*) takes an XPS file and a printer name as command-line parameters and prints the file on the printer. It is not required for setting redirected printer or document properties.

Tswpfwrp.exe is included with the RDC 6.0 client. For any client computers that do not support the TS EasyPrint feature, only client printers that have a corresponding driver on the Windows Server 2008 terminal server can be redirected in a terminal server session.

To verify if a printer is using the TS EasyPrint functionality, view the properties of the printer connection within the remote session. Figure 5-3 shows the properties for an HP LaserJet printer that has been redirected from a client's workstation—note the printer connection specified in the Model field when the dialog box is opened from within the remote connection.

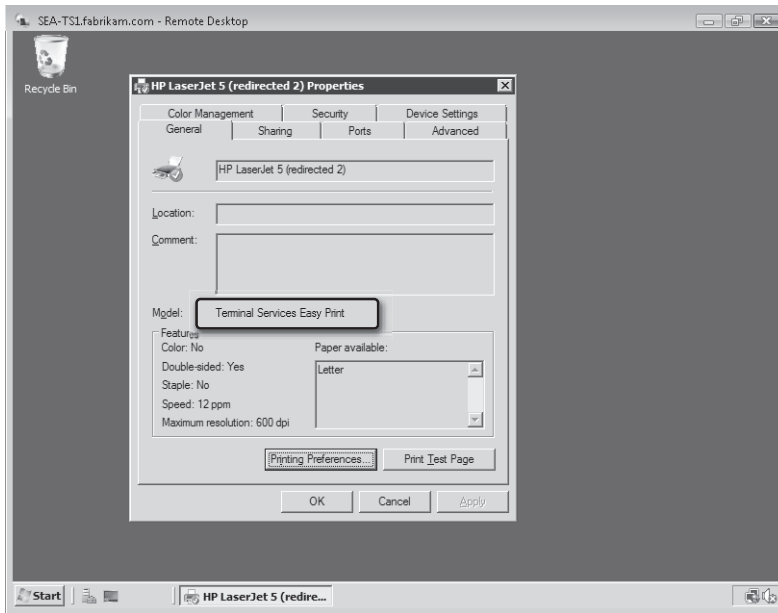


FIGURE 5-3 Verifying that TS EasyPrint is being used within a remote session

—CSS Global Technical Readiness (GTR) team.

Windows System Resource Manager

Windows System Resource Manager (WSRM) is a feature in Windows Server 2008 that enables you to control how processor and memory resources are allocated to processes, services, and applications running on the server. By providing a policy-based mechanism for making more efficient use of such resources, WSRM can help improve system performance and reduce issues arising from resource starvation. By using WSRM together with Windows Server 2008 Terminal Services, administrators can control the resources used by remote sessions and RemoteApp programs using the new per-session policy available for Windows Server 2008 Terminal Services.



More Info For more information about WSRM, see the Windows Server 2008 TechCenter on Microsoft TechNet at <http://technet.microsoft.com/en-us/windowsserver/2008/default.aspx>.

Features Comparison by Version

Table 5-2 compares the features of the Windows Server 2008 version of Terminal Services with the earlier Windows Server 2003 version of Terminal Services. The table also identifies features that require RDC 6.0, which is available on clients running Windows Vista with Service Pack 1 and Windows XP with Service Pack 3.

TABLE 5-2 Comparison of Terminal Services Features Between Windows Server 2008 and Windows Server 2003

	Windows Server 2008 Terminal Services	Windows Server 2003 Terminal Services	Requires RDC 6.0
Key Features			
TS Remote Desktops	✓	✓	
TS RemoteApp	✓		✓
TS Gateway	✓		✓
TS Web Access	✓		✓
TS EasyPrint ¹	✓		✓
Unified TS and Web Client	✓		✓
Experience Features			
24-bit color	✓	✓	
32-bit color	✓		✓
Font Smoothing	✓		✓
Display data prioritization	✓		✓
Large Resolution Support (4096 by 2048)	✓		✓
Monitor Spanning	✓		✓
Advanced Compression ²	✓		✓
Device Redirection			
TS Legacy Printer Redirection	✓	✓	
PnP Device Redirection Framework Support	✓		✓
Serial Port Redirection	✓	✓	
Sound Redirection	✓	✓	
Basic Clipboard Redirection	✓	✓	

¹ Requires .NET Framework 3.0 SP1 or later

² Configured using Group Policy

	Windows Server 2008 Terminal Services	Windows Server 2003 Terminal Services	Requires RDC 6.0
Advanced Clipboard Redirection	✓		✓
Security			
Smart Card Support	✓	✓	
Federal Information Processing Standards (FIPS) 140-1 Support	✓	✓	
Secure Sockets Layer (SSL) Authentication	✓	✓	
Network Level Authentication	✓		✓
CredSSP Single Sign-on ³	✓		✓
Network Access Protection Integration ⁴	✓		✓
RDP Signing	✓		✓
Wildcard SSL certificate sup- port ⁵	✓		✓
Enterprise Management			
Per-User License Tracking	✓		
Per-Device License Tracking and Enforcement	✓	✓	
License Diagnosis and Support Tools	✓		
Session Broker (session- based load balancing)	✓		
Session Directory (third- party NLB support)	✓	✓	
Windows System Resource Management Support	✓		
Full IPv6 Support	✓		✓

³ Windows Vista clients only⁴ Requires TS Gateway⁵ TS Gateway / NLB / RDP Signing

Understanding Terminal Services

Terminal Services is a Windows Server technology that allows multiple users to remotely and simultaneously run applications as if these applications were locally installed on their client computers. As mentioned earlier in this chapter, Terminal Services was first introduced with Windows NT 4.0 Terminal Server Edition as a means of providing users with a remote desktop on which they could run applications on a terminal server.

As Figure 5-4 shows, Terminal Services works by transmitting the key presses and mouse clicks on the user's computer to the terminal server, where they are accepted as input for actions performed on the user's remote desktop. The terminal server then transmits the user's remote desktop from the terminal server to the user's computer, where it is displayed on the user's monitor. Keyboard and mouse activity and display information is transmitted between the terminal server and the client by the RDP, which runs over a TCP/IP network via TCP port 3389.

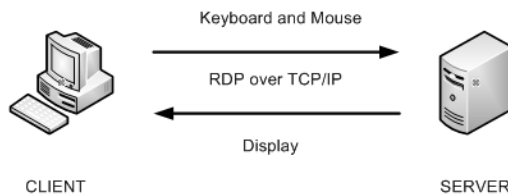


FIGURE 5-4 How Terminal Services works

The terminal server maintains a separate, independent remote desktop for each user. Terminal Services thus provides virtualized Windows session management so that users can treat their remote session as their own personal computer.

Installing the Terminal Services Role

The Terminal Services role can be installed on a computer running either an x86 or x64 version of a Full installation of Windows Server 2008 Standard, Enterprise, or Datacenter edition. Terminal Services is not available on a Server Core installation of Windows Server 2008. Terminal Services is also not available on Windows Server 2008 Web Edition or on the Itanium hardware platform.

To install the Terminal Services role, do one of the following:

- Launch the Add Roles Wizard from either the Server Manager console or the Initial Configuration Tasks screen. (See Figure 5-5.)
- Use the `Servmanagercmd.exe` command-line tool.

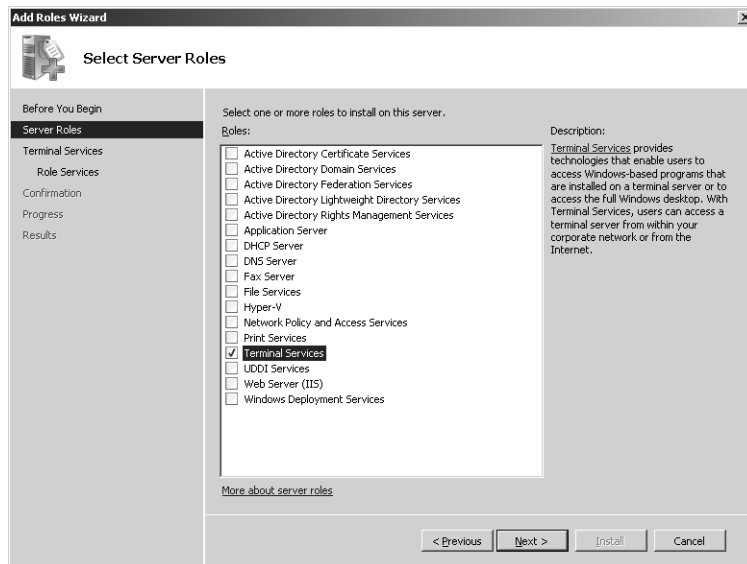


FIGURE 5-5 Installing the Terminal Services server role using the Add Roles Wizard

After you select the Terminal Services role and click Next, the Add Roles Wizard displays a page that shows the different Terminal Services role services you can install on your server. By selecting the first role service, which is named Terminal Server (as shown in Figure 5-6), you perform the following actions on your server:

- The server becomes a terminal server capable of supporting multiple simultaneous connections from remote computers and providing users of these computers with remote desktops.
- TS RemoteApp functionality is enabled to allow the terminal server to provide users of remote computers with the ability to run multiple RemoteApp programs on the terminal server.

Installing the other role services adds further Terminal Services functionality, such as TS Web Access, TS Gateway, TS Session Broker, and TS Licensing capabilities.



Tip The Terminal Services role should not be installed on a domain controller in a production environment for two reasons. First, allowing users to remotely run programs on a domain controller can increase security risks. Second, running user programs on a domain controller can degrade the performance of the domain controller. In a testing and development environment, however, it is acceptable to install the Terminal Services role on a domain controller. If you do decide, however, to install the Terminal Services role on a domain controller for testing purposes, don't forget to add the users group to the Allow Log On Through Terminal Services user right; otherwise, users won't be able to log on to the server.

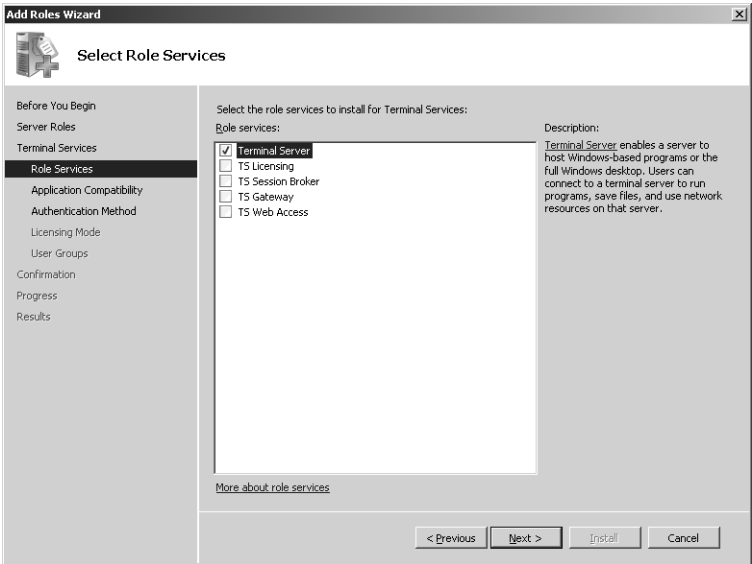


FIGURE 5-6 Choosing Terminal Services role services to install

During Terminal Services role installation, you also have the opportunity to configure licensing and security for your new terminal server. These options are described later in this chapter in various sections.

Terminal Services System Services

Depending on which Terminal Services role services you install on your server, one or more of the system services shown in Table 5-3 might be installed and running.

TABLE 5-3 System Services Underlying Different Terminal Services Components

System Service	Location	Details
Terminal Services (TermServices)	%systemroot%\system32\svchost.exe -k termsvcs %systemroot%\system32\termsrv.dll	Main Terminal Server service required for all Terminal Services and Remote Desktop functionality
Terminal Services Configuration (SessionEnv)	%systemroot%\system32\svchost.exe -k netsvcs %systemroot%\system32\sessenv.dll	Responsible for all Terminal Services and Remote Desktop related configuration and session maintenance activities that require SYSTEM context

System Service	Location	Details
Terminal Services Gateway (TSGateway)	%systemroot%\system32\svchost.exe -k tsgateway %systemroot%\system32\aaedge.dll	Provides Terminal Services Gateway functionality
Terminal Services Session Broker (Tssdis)	%systemroot%\system32\tssdis.exe	Provides Terminal Services Session Broker functionality
Terminal Services UserMode Port Redirector (UMRdpService)	%systemroot%\system32\svchost.exe -k LocalSystemNetworkRestricted %systemroot%\system32\umrdp.dll	Provides device redirection functionality

Remote Desktop

The Terminal Services system service (TermServices) is installed and started by default on all installations of Windows Server 2008, regardless of whether or not the Terminal Services role has been installed on the server. This is done to provide support for Remote Desktop, a feature of Windows Server 2008 and Windows Vista that allows up to two users to remotely connect to the computer over TCP port 3389 for the purposes of remotely administering the computer.



Note The Terminal Services system service is also installed and started by default on all installations of Windows Vista to provide support for Remote Assistance, a feature of Windows Vista that enables a user to view or control another user's desktop session. By using Remote Assistance, a user can invite a technical expert to connect to her computer to view her desktop and, if the user grants permission, to take control of her computer to provide assistance. In addition, a technical expert can offer Remote Assistance to a user without prior solicitation from the user. The user can then either accept or deny the offer for assistance. For more information about Remote Assistance in Windows Vista with Service Pack 1, see the Windows Vista Resource Kit, Second Edition by Mitch Tulloch, Tony Northrup, and Jerry Honeycutt, with the Windows Vista Team at Microsoft (Microsoft Press, 2008).

The Remote Desktop feature is not intended as a way of providing users with remote sessions for performing their job. Instead, it is intended only as a means of remotely managing servers and client computers. The experience of using Remote Desktop is essentially equivalent in look and feel with sitting at the local console of the server or client computer, although the responsiveness of the remote session depends on the available network bandwidth.

When you enable Remote Desktop on a computer running Windows Server 2008 or Windows Vista, you also have the option of specifying whether Network Level Authentication (NLA) is required when a remote client wants to establish a connection to your computer. Network Level Authentication provides additional security for remote connections. For more information concerning Network Level Authentication, see the section titled "Configuring Terminal Server Authentication" later in this chapter.



Note Unlike Remote Desktop for Administration in Windows Server 2003, the console session is now counted in the number of Remote Desktop connections on Windows Server 2008. This means that if there is an active console session on a Windows Server 2008 server, only one additional Remote Desktop connection is available. If a user attempts to log on to a Windows Server 2008 server when the Remote Desktop connection limit has been reached, the user receives a dialog box that allows him to disconnect (not log off) one of the other users.

Terminal Services Licensing

Microsoft licensing requirements require that each user or device that connects to the terminal server have its own Terminal Services client access license (TS CAL) in order to establish a valid connection with the server. These Terminal Services licenses are separate from and in addition to the valid Windows Server 2008 and Windows CALs required on a Windows-based network.

By installing the TS Licensing role service on a Windows Server 2008 system (not necessarily a terminal server), administrators can easily deploy, manage, and revoke TS CALs in a Terminal Services environment. TS Licensing has been enhanced in Windows Server 2008 to support per-user tracking and reporting, manual revocation of licenses, improved diagnostics, and a Windows Management Instrumentation (WMI) provider.

Terminal Services licensing can be configured either during the installation of the role or afterwards. Figure 5-7 shows the licensing configuration options in the Add Roles Wizard.

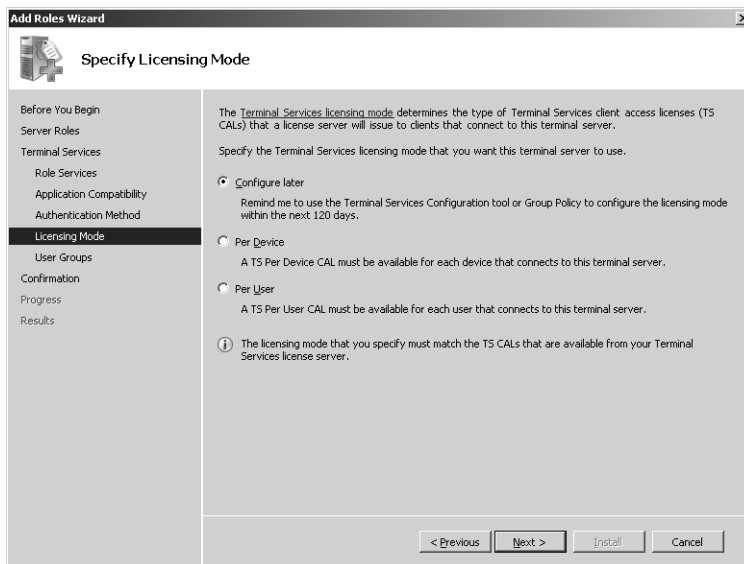


FIGURE 5-7 Licensing configuration options during role installation

Terminal Services can be licensed either per-device or per-user as desired. In addition, if you select the Configure Later option during role installation, you have a 120-day grace period before a Terminal Services license server (a server running the TS Licensing role service) must be deployed on your network. This grace period allows you to configure and test your terminal server deployment before rolling it out to your user environment.

For tips on planning licensing for your Terminal Services deployment, see the sidebar titled “Direct from the Source: Tips for Planning Terminal Services Licensing” in this chapter.

Direct from the Source: Tips for Planning Terminal Services Licensing

For environments with a single Terminal Services license server, if the license server becomes unavailable, previously licensed clients will still be able to connect to the terminal server or servers if their license has not expired. However, unlicensed clients will not be able to connect to the terminal server or servers because they cannot obtain a license. To provide a window to bring the license server back online without disrupting users, a redundant license server can be used.

Terminal server licensing server redundancy can be achieved using either of the following methods:

- Install all CALs on the primary license server and none on the secondary license server. This approach provides a period of redundancy in the event of a failure of the primary license server. By adding a second license server with no licenses, unlicensed clients will be able to connect and obtain a temporary license from this server if the primary license server is not available. Previously licensed clients can also still connect if their license has not expired.
- Install CALs on both the primary license server and the secondary license server. Each terminal server licensing server should ideally contain 50 percent of the available CALs. If the primary licensing server is not available or does not have valid CALs, clients are redirected to the secondary licensing server for license issuance.

Because licensed clients attempt to renew their license seven days prior to expiration, these redundant configurations help to ensure uninterrupted terminal server connectivity for up to seven days if one of the license servers fails.

It is also recommended that you regularly back up Terminal Services licensing data to protect the data from accidental loss because of hardware or storage failure. In the event that the original data on the hard disk is inaccessible for any reason, the licensing data can be restored from the archived copy. For additional security, a redundant license server can be used.

—CSS Global Technical Readiness (GTR) team

Terminal Server Security

Terminal Services security can be configured either during the installation of the role or afterwards. There are additional steps you must take to provide secure access to your terminal server:

- Specify an authentication method for your terminal server.
- Specify which groups of users are allowed access to your terminal server.

The sections that follow provide more details concerning these steps. In addition, the sidebar titled “Direct from the Source: Using SSL for Terminal Services Connections” provides additional information on how you can protect your terminal server.

Configuring Terminal Server Authentication

Terminal Services in Windows Server 2008 has been enhanced over previous versions of Terminal Services by the addition of support for Network Level Authentication (NLA). NLA is a new authentication method that completes the user authentication process before a remote session is established and the logon screen is displayed. NLA provides greater security and requires fewer initial resources during the authentication process. As Figure 5-8 shows, the option to require NLA can be configured during the installation of the Terminal Services role.

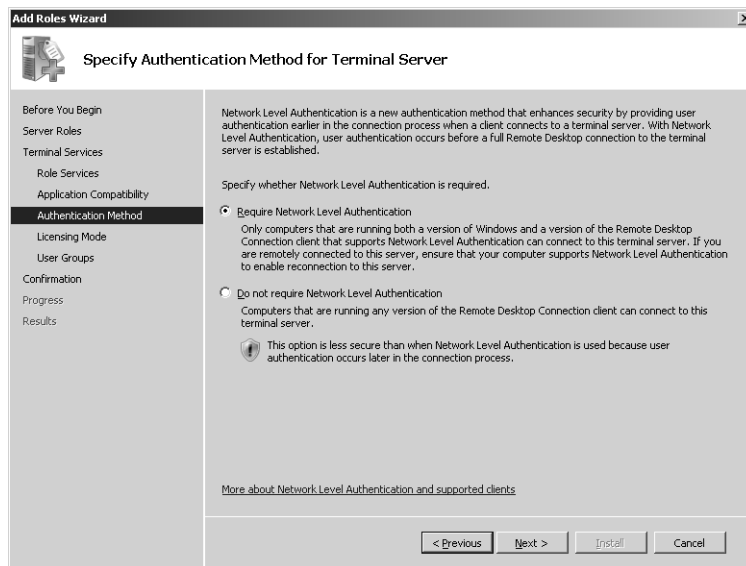


FIGURE 5-8 Requiring Network Level Authentication for remote connections to your terminal server

To use NLA for authenticating remote connection attempts to a Windows Server 2008 terminal server, the remote computer must be using RDC 6.0 client software. This means that the remote computer must be running Windows Server 2008, Windows Vista with Service Pack 1, or Windows XP with Service Pack 3.

Configuring Terminal Server Access

Before any users can establish remote sessions with your terminal server, you must add their appropriate security groups to the Remote Desktop Users group on your terminal server. You can do this either during the Terminal Services role installation process (as shown in Figure 5-9) or afterwards. By default, the local Administrators group on your terminal server has such access, which by default also provides access to members of the Domain Admins group.

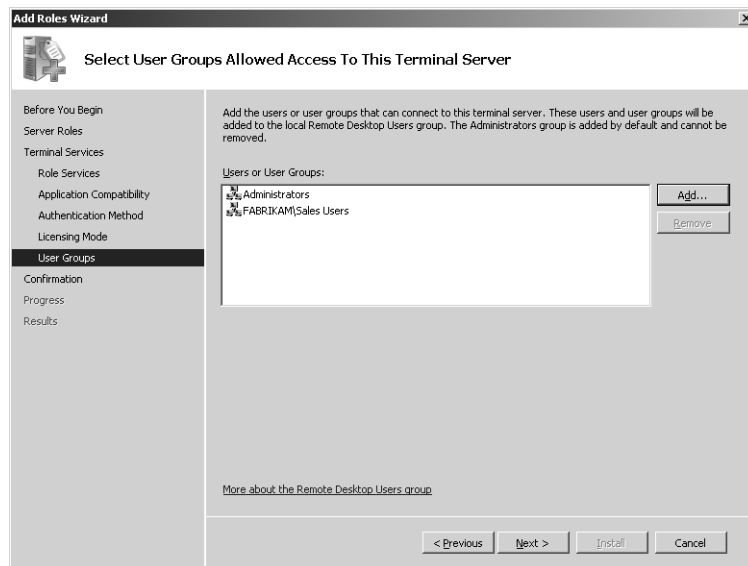


FIGURE 5-9 Allowing users access to your terminal server

Direct from the Source: Using SSL for Terminal Services Connections

By default, Terminal Services sessions use native RDP encryption. However, RDP does not provide authentication to verify the identity of a terminal server. You can enhance the security of Terminal Services sessions by using SSL (TLS 1.0) for server authentication and to encrypt terminal server communications. The terminal server and the client computer must be correctly configured for TLS to provide enhanced security. The three available security layers are shown in Table 5-4.

TABLE 5-4 RDP Security Layers

Security Layer	Description
SSL (TLS 1.0)	SSL (TLS 1.0) will be used for server authentication and for encrypting all data transferred between the server and the client.
Negotiate	The most secure layer that is supported by the client will be used. If supported, SSL (TLS 1.0) will be used. If the client does not support SSL (TLS 1.0), the RDP Security Layer will be used. This is the default setting.
RDP Security Layer	Communication between the server and the client will use native RDP encryption. If you select RDP Security Layer, you cannot use Network Level Authentication.

A certificate is needed to authenticate a terminal server when SSL (TLS 1.0) is used to secure communication between a client and a terminal server during RDP connections. You can select a certificate that you have already installed on the terminal server, or you can use the default self-signed certificate. Figure 5-10 shows how to enable SSL for terminal server connections using the RDP-Tcp Properties dialog box, which is accessed from the Terminal Services Configuration snap-in.

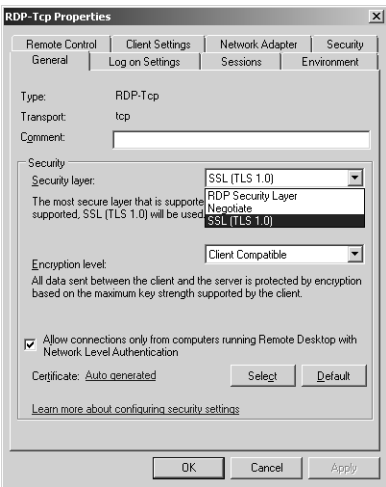


FIGURE 5-10 Configuring the security layer settings for your terminal server

For Terminal Services connections, data encryption protects data by encrypting it on the communications link between the client and the server. Encryption protects against the risk of interception of the client/server communication.

By default, Terminal Services connections are encrypted at the highest level of security available (128-bit). However, some older versions of the Terminal Services client application do not support this high level of encryption. If needed to support legacy clients, the encryption level of the connection can be configured to send and receive data at the highest encryption level supported by the client. There are four levels of encryption available, as shown in Table 5-5.

TABLE 5-5 RDP Encryption Levels

Level of Encryption	Description
Low	Data sent from the client to the server is encrypted using 56-bit encryption. Data sent from the server to the client is not encrypted.
Client Compatible	Encrypts client/server communication at the maximum key strength supported by the client. Use this level when the terminal server is running in an environment containing mixed or legacy clients. This is the default encryption level.
High	Encrypts client/server communication using 128-bit encryption. Use this level when the clients accessing the terminal server also support 128-bit encryption. When encryption is set at this level, clients that do not support this level of encryption will not be able to connect.
FIPS Compliant	All client/server communication is encrypted and decrypted with the FIPS encryption algorithms. FIPS 140-1 (1994) and its successor, FIPS 140-2 (2001), describe U.S. government requirements for encryption.

Figure 5-11 shows how to configure the terminal server encryption level using the RDP-Tcp Properties dialog box, which is accessed from the Terminal Services Configuration snap-in.

Terminal server authentication and encryption settings can be also configured by applying the following Group Policy settings:

- Set Client Connection Encryption Level
- Require Use Of Specific Security Layer For Remote (RDP) Connections
- Server Authentication Certificate Template
- Require User Authentication For Remote Connections By Using Network Level Authentication

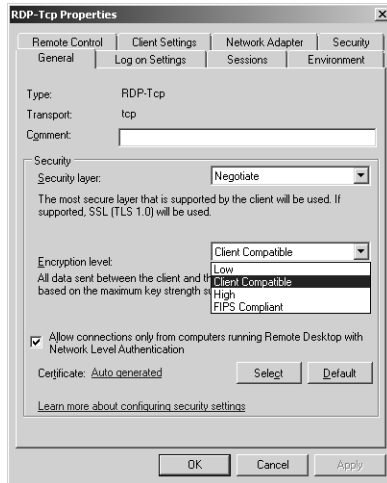


FIGURE 5-11 Configuring the encryption layer settings for your terminal server

These Group Policy settings are located in the following container:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Security

FIPS can be specified as the encryption level by applying the System Cryptography: Use FIPS Compliant Algorithms For Encryption, Hashing And Signing Group Policy setting located in the following container:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

—CSS Global Technical Readiness (GTR) team

Installing Applications on Terminal Servers

Applications developed for end-users of your system must be installed properly on a terminal server so that they can be accessed remotely. Before you install an application on a terminal server, make sure you understand any compatibility issues associated with the application when it is running in a Terminal Services environment.



Note Windows Server 2008 includes the same file and registry virtualization functionality included in Windows Vista for applications that are not compliant with User Account Control (UAC) and that require access to locations on your hard drive that are accessible only by administrators.

Make sure you install the Terminal Services role on your server before you install any applications that users will need to run within their remote sessions or as RemoteApp programs. If you install the Terminal Services role after you have installed your applications, the applications might not function correctly in a multi-user environment.

To install an end-user application on a terminal server, the terminal server must first be switched into TS-Install mode to ensure that the application will be able to run in a multi-user environment. Once your applications have been installed on your terminal server, you must switch the server back into TS-Execute mode before users can remotely connect to your server. You can switch between install and execute modes from the command-line using these commands:

change user /install

change user /execute

To determine the current install mode of your terminal server, use this command:

change user /query

You can also install applications on your terminal server by using the Programs portion of Control Panel (shown in Figure 5-12). If you do this on a Windows Server 2008 terminal server, an additional option, Install Application On Terminal Server, is displayed that is not available on a Windows Server 2008 computer that does not have the Terminal Services role installed. Clicking this option launches the Install Program From Floppy Disk Or CD-ROM Wizard, which walks you through the installation process by automatically switching the server to TS-Install mode, installs the program, and switches the server back to TS-Execute mode.

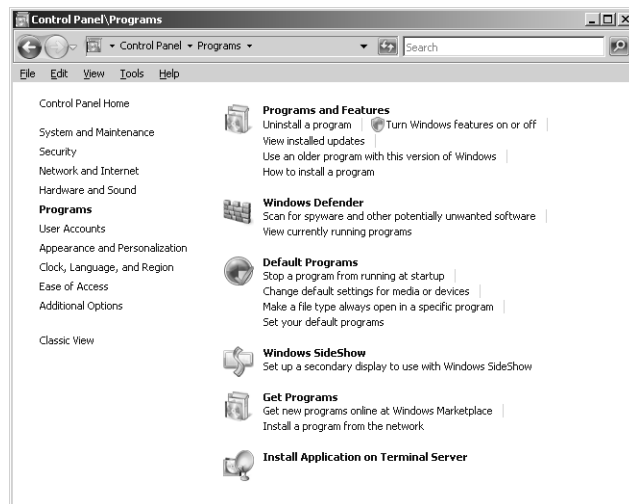


FIGURE 5-12 Installing an application on a terminal server

For additional tips on installing applications on terminal servers, see the sidebar titled “Direct from the Source: Best Practices for Installing Applications on Terminal Servers” in this chapter.

Direct from the Source: Best Practices for Installing Applications on Terminal Servers

Install related applications, or applications that have dependencies on other local applications, on the same terminal server. For example, you should install Microsoft Office as a suite on the same terminal server instead of installing individual Office programs on separate terminal servers. This reduces the installation, management, and servicing overhead required for the programs.

You should consider installing individual applications on separate terminal servers in the following circumstances:

- The application has compatibility issues that might affect other programs.
- The number of application users might exceed server capacity.
- The applications are resource (CPU, memory, and so forth) intensive and negatively affect performance when multiple instances are running at the same time.

It is also a good practice always to consult with the application vendor to ensure that the application being installed will function correctly for multiple users in a terminal server environment. Application vendors sometimes provide fixes or compatibility scripts for applications to ensure that they function correctly in a multi-user terminal server environment.

—CSS Global Technical Readiness (GTR) team

Managing Terminal Servers

Once the Terminal Services role has been installed and your terminal server has been configured, you’re ready to begin administering your terminal servers, licenses, and users. Windows Server 2008 includes a number of different tools and technologies for administering both local and remote terminal servers, including the following:

- Terminal Services MMC snap-ins
- Terminal Services command-line tools
- Terminal Services Group Policies
- Terminal Services WMI Provider

The following sections provide more information concerning each method or tool for managing Terminal Services. In addition, remote connection settings that are not configured at the computer, user, or group level can also be configured in the RDC client on a per-session basis.



Tip You can also install Terminal Services snap-ins and consoles on a computer running Windows Server 2008 that is not a terminal server or on a computer running Windows Vista with Service Pack 1. To do this on a computer running Windows Server 2008, use the Add Features Wizard to add the Terminal Services Tools component of Role Administration Tools under the Remote Server Administration Tools feature. To do this on a computer running Windows Vista SP1, install the Microsoft Windows Server 2008 Remote Server Administration Tools for Windows Vista Service Pack 1 update package (.msu file) for your platform (x86 or x64) after downloading this update from <http://support.microsoft.com/kb/941314>.

Terminal Services Microsoft Management Console Snap-ins

Installing the Terminal Services role with the Terminal Server role service installs several Microsoft Management Console (MMC) snap-ins for managing terminal servers on your network. These snap-ins are available as MMC consoles under Terminal Services in the Administrative Tools folder of your Start menu, but you can also add the snap-ins to new MMC consoles to customize your Terminal Services administration tools.

The three Terminal Services snap-ins that are available when you install the Terminal Server role service are

- Terminal Services Manager
- Terminal Services Configuration
- Remote Desktops



Note More snap-ins are available when you install additional Terminal Services role services on your terminal server. These snap-ins are discussed in their relevant sections later in this chapter.

Terminal Services Manager Terminal Services Manager (Tsadmin.msc) is an MMC console that can be used to manage users, sessions, and applications running on a terminal server. Using this console, you can perform the following tasks on both local and remote terminal servers:

- Connect to and disconnect from sessions
- Display information about servers, sessions, users, and processes
- Log off users
- Monitor sessions

- Remotely control a user's session
- Reset sessions
- Send messages to users
- Terminate processes



Note If you use Terminal Services Management on the terminal server itself, certain features such as Remote Control and Connect won't work. To use these features, you must run Terminal Services Management in a remote session from a client computer.

Figure 5-13 shows Terminal Services Management running on a terminal server named SEA-TS1 in the fabrikam.com domain. The Users tab shows three users currently connected to the server:

- **Administrator** The domain Administrator is currently logged on locally to the terminal server.
- **kberg** A user named Karen Berg is remotely connected to the terminal server from her Windows Vista desktop computer.
- **tallen** A second user named Tony Allen is remotely connected to the terminal server from his Windows Vista laptop.

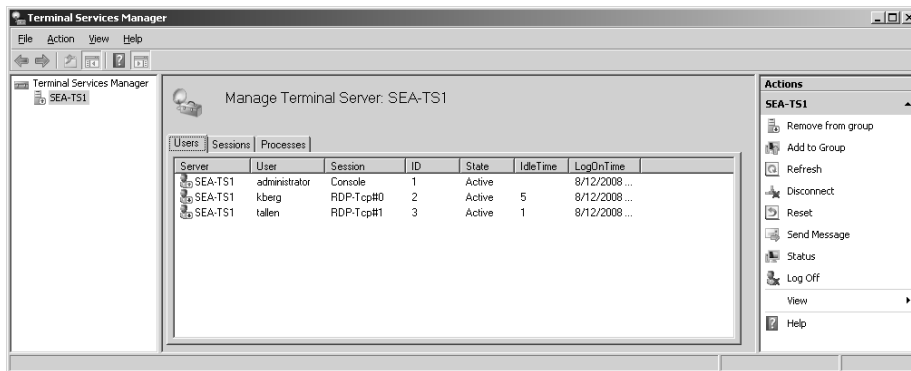


FIGURE 5-13 The Terminal Services Management console

By selecting a user in the center pane and clicking the appropriate link in the Actions pane at the right, the administrator can view the status of the user's connection, disconnect or log off the user, send the user a message, and perform other tasks. The Sessions tab displays active sessions with the terminal server and allows you to reset or disconnect sessions or send the computer involved a message. The Processes tab displays all running processes on the terminal server and allows you to end a process—for example, if the user's application is hung and needs to be forcefully terminated.

Terminal Services Manager in Windows Server 2008 has a new feature called Groups that replaces and enhances the Favorites feature of this tool on the earlier Windows Server 2003 platform. Using the Groups feature, an administrator can organize terminal servers into groups to more easily manage them. You can also import a list of terminal servers from a TS Session Broker farm.

Terminal Services Configuration Terminal Services Configuration (Tsconfig.msc) is an MMC console that can be used to configure various properties of a terminal server, including listeners, temporary folders, security, and licensing. Using this console, you can perform the following tasks on both local and remote terminal servers:

- Enable or disable automatic logons
- Enable or disable logons through the connection
- Enable or disable session remote control
- Name a connection
- Override user profile settings for wallpaper
- Set client device mapping and connection parameters
- Set connection time-outs
- Set permissions on the connection
- Set the level of encryption
- Set the maximum number of sessions allowed
- Set whether to disconnect broken connections
- Specify a connection transport and transport properties
- Specify a connection type
- Specify a program to run when a user logs on

Figure 5-14 shows Terminal Services Configuration connected to terminal server SEA-TS1 in the fabrikam.com domain. The default Terminal Services listener RDP-Tcp is currently selected, and using the Actions pane you can disable the connection or rename it.

If you double-click a connection, you can display the configurable properties of the connection. Double-clicking one of the items in the Edit Settings section at the bottom of the center pane brings up a different properties sheet that lets you configure the displayed settings. And clicking on the Licensing Diagnosis node in the left pane displays information that can help you troubleshoot licensing issues with your terminal server.

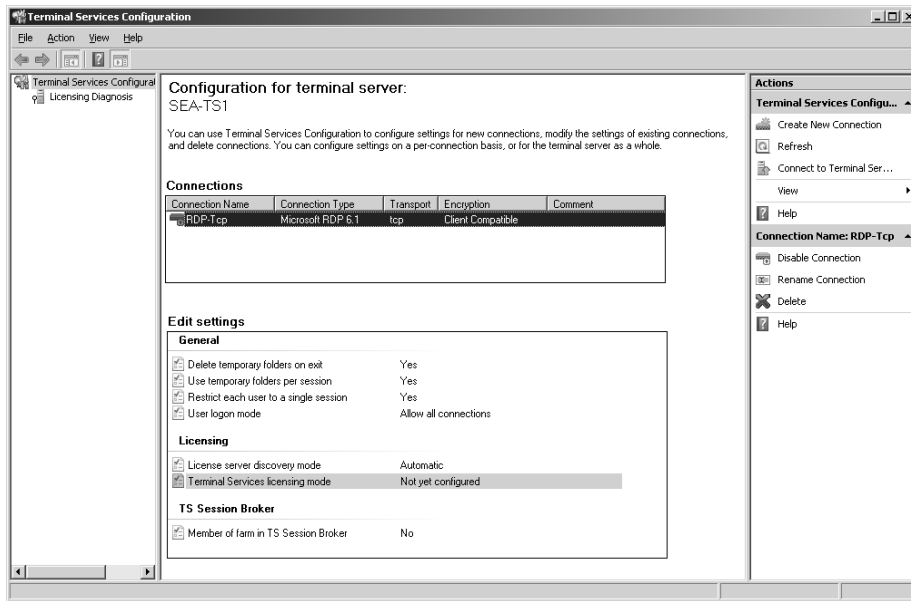


FIGURE 5-14 The Terminal Services Configuration console

Remote Desktops Remote Desktops (Tsmmc.msc) is an MMC console that can be used to manage Remote Desktop connections to terminal servers and other computers. Using this console, you can remotely administer multiple computers from a central location by connecting to the remote desktop of each computer.

Figure 5-15 shows the Remote Desktops console running on a terminal server and connected to two desktop computers, SEA-DESK155 and SEA-DESK175. The connection to SEA-DESK155 is selected and remotely displays the desktop of the computer.

By default, when you add a connection to the Remote Desktops console, the console connects you to an administrative session on the remote computer. This is equivalent to launching the Remote Desktop Connection client using the **/admin** option, which is new in Windows Server 2008 and Windows Vista with Service Pack 1. For more information about the new **/admin** option, see the article titled "Changes to Remote Administration in Windows Server 2008" in the Microsoft Knowledge Base at <http://support.microsoft.com/kb/947723>.

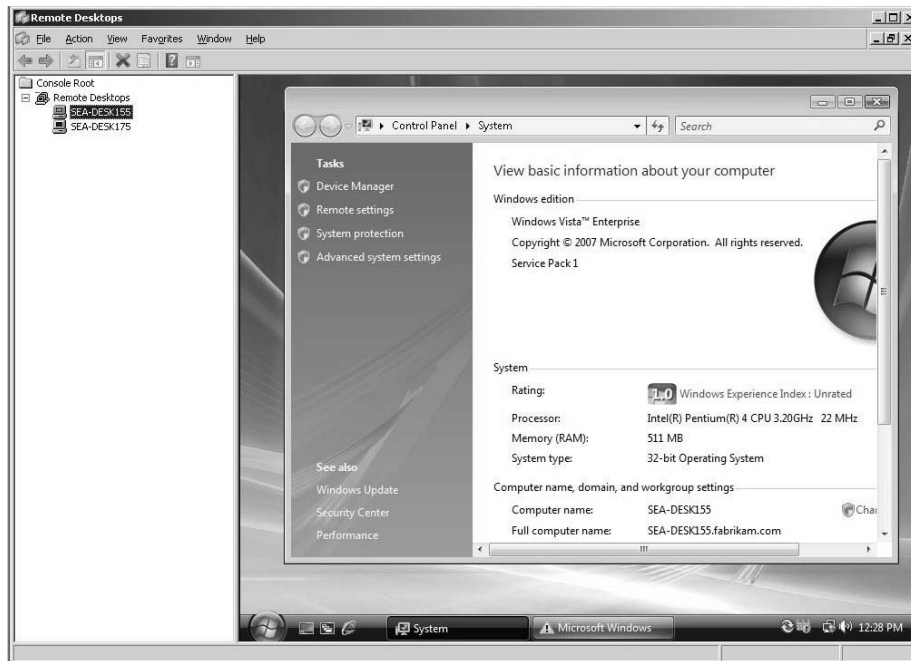


FIGURE 5-15 The Remote Desktops console

Active Directory Users and Computers You can also configure per-user Terminal Services settings using the Active Directory Users and Computers console. To do this, open the properties sheet for a user account and configure settings on the following four tabs relating to Terminal Services:

- **Remote Control** Used to enable or disable remote control, to specify the desired level of remote control (view or interact), and to require the user's permission to observe or control sessions.
- **Terminal Services Profile** Used to set the path to the Terminal Services user profile for each user, to set the path to the user's home folder, and to enable or disable terminal server logons for the user.
- **Environment** Used to specify a program to run when a user logs on, to specify that client drives and printers connect at logon, and to select to default to the client's main printer.
- **Sessions** Used to set the maximum duration on sessions, to set the maximum idle time for a session, to set the maximum time a disconnected session remains active, to specify whether to disconnect or reset a broken connection, and to modify settings for reconnecting disconnected sessions.



Note Many of these settings can also be configured using the Terminal Services Configuration snap-in or by configuring Group Policy settings. When settings configured using these different methods conflict, they will be overridden according to the following order of precedence:

1. Active Directory Users and Computers
2. Terminal Services Configuration snap-in
3. Group Policy

In other words, Group Policy settings trump any other method that Terminal Services settings have configured.

Terminal Services Command-Line Tools

Many aspects of Windows Server 2008 terminal servers can also be administered from the command line. Table 5-6 lists the Terminal Services command-line tools available in Windows Server 2008, while Table 5-7 lists Terminal Services command-line tools that have been deprecated and are no longer available in Windows Server 2008.

TABLE 5-6 Terminal Services Command-Line Tools Available in Windows Server 2008

Command	Description
Change	Changes terminal server settings for logons, Component Object Model (COM) port mappings, and install mode.
Change logon	Enables or disables logons from client sessions on a terminal server, or displays current logon status.
Change port	Lists or changes the COM port mappings to be compatible with MS-DOS applications.
Change user	Changes the install mode for the terminal server.
Chglogon	Enables or disables logons from client sessions on a terminal server, or displays current logon status.
Chgport	Lists or changes the COM port mappings to be compatible with MS-DOS applications.
Chguser	Changes the install mode for the terminal server.
Flattemp	Enables or disables flat temporary folders.
Logoff	Logs off a user from a session on a terminal server, and deletes the session from the server.
Msg	Sends a message to a user on a terminal server.
Mstsc	Creates connections to terminal servers or other remote computers.
Qappsrv	Displays a list of all terminal servers on the network.
Qprocess	Displays information about processes that are running on a terminal server.
Query	Displays information about processes, sessions, and terminal servers.

Command	Description
Query process	Displays information about processes that are running on a terminal server.
Query session	Displays information about sessions on a terminal server.
Query termserver	Displays a list of all terminal servers on the network.
Query user	Displays information about user sessions on a terminal server.
Quser	Displays information about user sessions on a terminal server.
Qwinsta	Displays information about sessions on a terminal server.
Reset session	Enables you to reset (delete) a session on a terminal server.
Rwinsta	Enables you to reset (delete) a session on a terminal server.
Shadow	Enables you to remotely control an active session of another user on a terminal server.
Tscon	Connects to another session on a terminal server.
Tsdiscon	Disconnects a session from a terminal server.
Tskill	Ends a process running in a session on a terminal server.
Tsprof	Copies the Terminal Services user configuration information from one user to another.

TABLE 5-7 Terminal Services Command-Line Tools That Have Been Deprecated in Windows Server 2008

Command	Function
Tsshutdn	Shuts down a Terminal Services server.
Register	Registers a program so that it has special execution characteristics.
Cprofile	Removes user-specific file associations from a user's profile.



Tip If you need to shut down or restart a Windows Server 2008 terminal server, you can use the Shutdown.exe command. Users who are remotely logged on to the server will receive a notification that a shutdown is in progress so that they can save their work. For more information, see <http://blogs.msdn.com/ts/archive/2007/06/15/introducing-terminal-services-server-drain-mode.aspx>.

Terminal Services Group Policies

You can use Group Policy to manage many aspects of your terminal servers. Table 5-8 lists the different types of Terminal Services Group Policy settings and where they can be found in the Group Policy Object Editor.

TABLE 5-8 Group Policy Settings for Administering Terminal Services

Type of Policy Setting	Path in Group Policy Editor
Computer Configuration Policy Settings	
Policy Settings for Terminal Server Connections	Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Connections
Policy Settings for Terminal Server Device and Resource Redirection	Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Device and Resource Redirection
Policy Settings for Terminal Server Licensing	Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Licensing
Policy Settings for Terminal Server Printer Redirection	Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Printer Redirection
Policy Settings for Terminal Server Profiles	Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Profiles
Policy Settings for Terminal Server Remote Session Environment	Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Remote Session Environment
Policy Settings for Terminal Server Security	Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Security
Policy Settings for Terminal Server Session Time Limits	Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Session Time Limits
Policy Settings for Terminal Server Temporary folders	Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Temporary folders
Policy Settings for Terminal Server TS Session Broker	Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\TS Session Broker
User Configuration Policy Settings	
Policy Settings for Remote Desktop Connection Client	User Configuration\Administrative Templates\Windows Components\Terminal Services\Remote Desktop Connection Client
Policy Settings for Terminal Server Connections	User Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Connections

Type of Policy Setting	Path in Group Policy Editor
Policy Settings for Terminal Server Device and Resource Redirection	User Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Device and Resource Redirection
Policy Settings for Terminal Server Printer Redirection	User Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Printer Redirection
Policy Settings for Terminal Server Remote Session Environment	User Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Remote Session Environment
Policy Settings for Terminal Server Session Time Limits	User Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Session Time Limits
Policy Settings for TS Gateway	User Configuration\Administrative Templates\Windows Components\Terminal Services\TS Gateway

Terminal Services WMI Provider

Terminal Services also includes a WMI provider to enable administration of terminal servers using WMI interfaces. These interfaces can be used for the following kinds of administration:

- Scripted administration using VBScript
- Scripted administration using Windows PowerShell
- Administration using the Microsoft System Center family of products
- Development of custom tools for administration

Windows Server 2008 Terminal Services includes five categories of WMI classes:

- Terminal Services Configuration Classes
- Terminal Services Gateway Classes
- Terminal Services License Server Classes
- Terminal Services RemoteApp Classes
- Terminal Services Session Broker Classes



More Info For more information on the WMI classes, properties, and methods supported by Windows Server 2008 Terminal Services, see the Terminal Services WMI Provider Reference in the MSDN Library at <http://msdn.microsoft.com/en-us/library/aa383515.aspx>.

Understanding TS RemoteApp

Terminal Services on previous Windows Server platforms could provide users only with entire remote desktops that included Terminal Services-enabled applications. This was sometimes confusing to users because it meant they had to contend with having two desktops—their local computer's desktop and the remote desktop presented to them via Terminal Services.

For example, at any given time a user might have several applications running on her local desktop plus additional applications running on her remote desktop. This presented users with interesting challenges. For instance, if a user wanted to quickly switch between applications on her local desktop, she could use the Alt+Tab or Alt+Esc keyboard accelerators to do this. But if the user wanted to do the same with applications on her remote desktop, she needed to use Alt+Page Up, Alt+Page Down, or Alt+Insert instead. And if she wanted to switch from a local application to a remote one, the easiest way was probably just to use the mouse! Such confusion and occasional frustration introduced by having two desktops created inefficiencies that resulted in loss of worker productivity.

With Windows Server 2008, however, Terminal Services now also provides the ability for terminal servers to provide users with access to individual applications running on a terminal server. These remote applications, known as RemoteApps, can be launched from the user's Start menu or desktop shortcuts, and when they are open they look and feel the same as locally installed programs. This look and feel extends to resizing, maximizing, minimizing, and cascading program windows; cut and paste operating between program windows; drag and drop support between multiple monitors; and notification icons displayed in the notification area. The result is that a user running both local and RemoteApp programs on his computer's local desktop might be unaware of the difference between a program installed locally and one running on a terminal server. RemoteApp thus integrates Terminal Services applications into the user's own desktop instead of presenting the user with a second, separate desktop.

The name of this new Terminal Services functionality in Windows Server 2008 is called Terminal Services RemoteApp (TS RemoteApp), and it is implemented as part of the core Terminal Server role service. The sections that follow go into further detail and demonstrate TS RemoteApp functionality at work.

How TS RemoteApp Works

TS RemoteApp requires Windows Server 2008 Terminal Services on the server side and RDC 6.0 on the client side. This means the client computer must be running either Windows Vista with Service Pack 1, Windows XP with Service Pack 3, or Windows Server 2008.

The process by which a RemoteApp program is launched on a terminal server is as follows:

1. When a remote user tries to launch a RemoteApp program, a new instance of Rpdinit.exe, the RemoteApp Logon Application, is started in the session space on the terminal server.
2. Rpdinit.exe then launches Rdpshell.exe, which provides the functionality for running the RemoteApp program's process. Rdpshell.exe replaces the usual Explorer.exe shell, which does not support RemoteApp functionality, and provides event hooks and APIs for monitoring the state of the user's taskbar, the position of windows, notification icons, and so on. Rdpshell.exe also opens a virtual channel that allows RemoteApp-specific commands to be transmitted from the client to the server.
3. Rpdinit.exe then monitors the RemoteApp program's process during the lifetime of the process. For example, if the process terminates abnormally, Rpdinit.exe will restart it.
4. If the user then launches additional RemoteApp programs on the same terminal server, these programs all share the same Terminal Services session with the first program launched above.



Note When you are using a RemoteApp program and save a document or other file you are working on with the program, the document or other file is saved within your user profile on the terminal server, not on your local workstation. The user profiles for Terminal Services users are stored on terminal servers under the %SystemDrive%\Users directory.

If you need to save a document or other file on your local computer instead of on the terminal server, save it to a redirected drive by browsing to \\tsclient in the Save file dialog box and selecting a redirected drive.

When a user terminates a RemoteApp program, the RemoteApp session between the user and the terminal server is placed into a disconnected state. The terminal server then applies heuristics to determine whether the RemoteApp session should remain disconnected or whether the user should be logged off from the terminal server to end the session. The termination logic for RemoteApp programs is configurable using Group Policy and basically works like this:

1. The user closes a RemoteApp program window on his desktop.
2. The terminal server checks the user's session to see whether there are any remaining active RemoteApp windows still open on the user's desktop. If the answer to this is Yes, the user's session remains connected.
3. If there are no remaining active RemoteApp program windows on the user's desktop, the terminal server next checks whether there are any RemoteApp program notification icons being displayed in the system tray on the user's desktop. If the answer to this is Yes, the user's session continues to remain connected.

4. If there are no RemoteApp program windows or notifications remaining on the user's desktop, the terminal server waits 20 seconds before terminating the user's session, just in case the user decides to launch another RemoteApp program immediately. If no RemoteApp program is launched during this time interval, the terminal server disconnects the user's session and the RDC client process exits. If another RemoteApp program is launched within the time interval, the user's session remains connected and the new process runs within the existing session.
5. Once the user's session has been disconnected, the session remains disconnected for a configurable period of time, after which the user is logged off from the disconnected session. The time interval between disconnection and logoff can be configured using the Group Policy setting Set Time Limit For Logoff Of RemoteApp Sessions. The reason for providing for the configurability of this time interval is because it is much faster to connect to a disconnected Terminal Services session than to start a new session.

Managing TS RemoteApp

To create, configure, and manage RemoteApp programs, you use the TS RemoteApp Manager console (Remoteprogram.msc), which is provided on Windows Server 2008 terminal servers as a snap-in and also as an MMC console found in the Terminal Services folder under Administrative Tools on the Start menu. Figure 5-16 shows the TS RemoteApp Manager console with no RemoteApp programs yet configured.

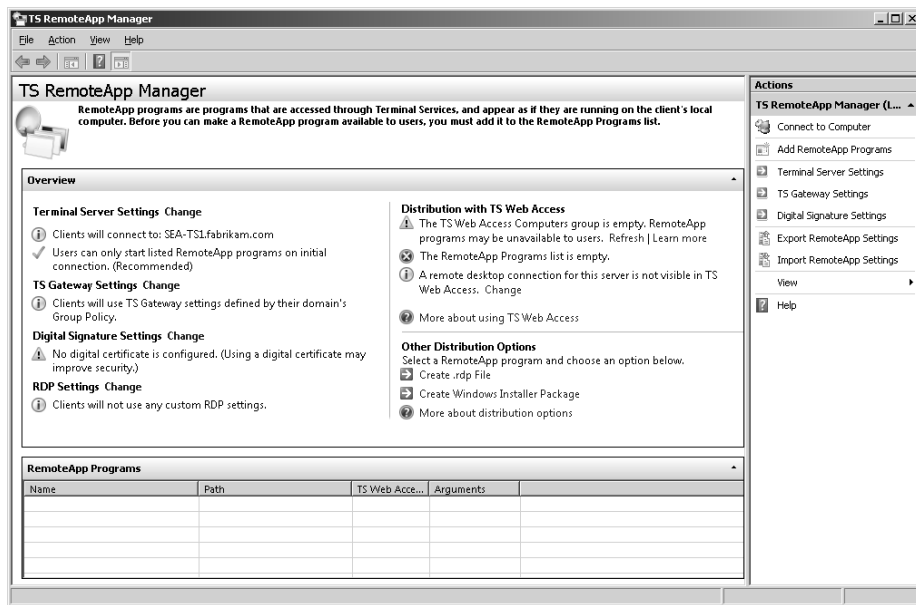


FIGURE 5-16 The TS RemoteApp Manager console

Using this console you can do the following:

- Create new RemoteApp programs and configure them.
- Package RemoteApp programs as .rdp or .msi files for deployment.
- Publish and unpublish RemoteApp programs via TS Web Access.
- Configure other terminal server settings.

See the next section for more information on using the TS RemoteApp Manager console.

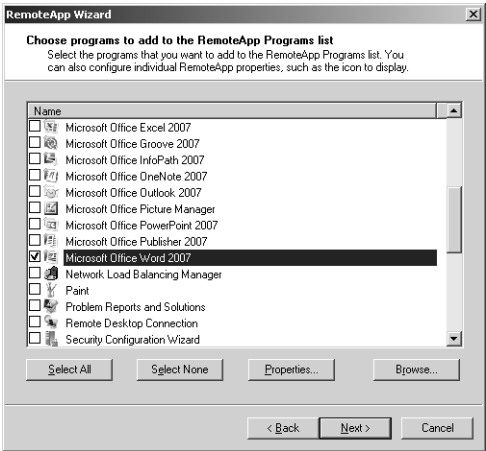
Deploying and Using RemoteApp Programs

RemoteApp programs must be deployed to users before they will be able to use them. There are several ways you can deploy RemoteApp programs to users:

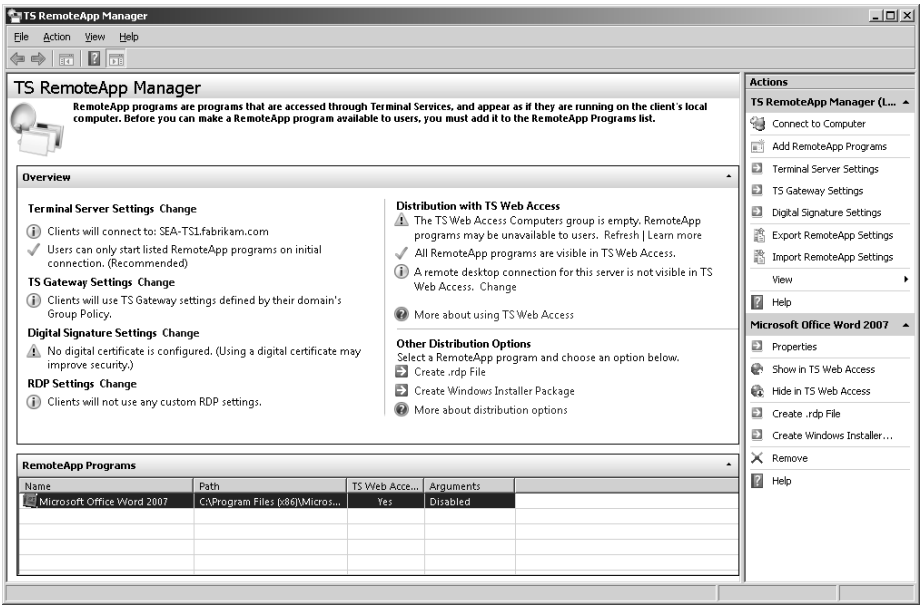
- By packaging the RemoteApp programs as Windows Installer (.msi) files and distributing them to users using the Software Installation feature of Group Policy
- By packaging the RemoteApp programs as either Remote Desktop Protocol (.rdp) files or Windows Installer (.msi) files and making them available to users by copying them to a network share
- By publishing the RemoteApp programs on the intranet or over the Internet using Terminal Services Web Access and, optionally, Terminal Services Gateway when greater security is required

For purposes of illustration, let's walk through the steps involved in the first RemoteApp deployment method listed earlier. For the following scenario, Microsoft 2007 Office System has been installed on a Windows Server 2008 terminal server named SEA-TS1 in the fabrikam.com domain. The goal is to create a RemoteApp program for Microsoft Office Word 2007, package this RemoteApp program as an .msi file, and deploy it to users in the Sales department so that Karen Berg, a user in this department, can launch the RemoteApp program on her Windows Vista SP1 computer, create a document, and save it in the Documents folder in her user profile on the terminal server.

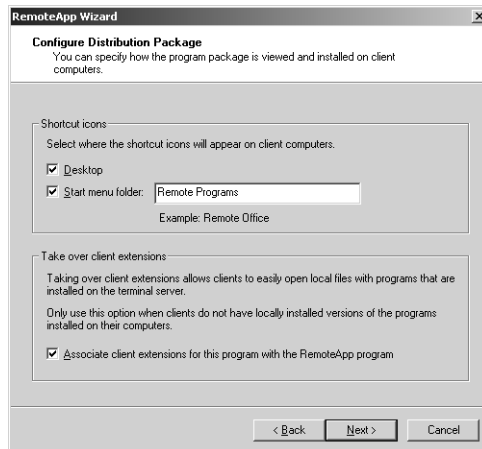
1. To create a RemoteApp program for Word 2007, start by opening TS RemoteApp Manager (shown previously in Figure 5-16) and click Add RemoteApp Programs in the Actions pane to launch the RemoteApp Wizard. In the Welcome screen, click Next, and then select the check box for Word 2007.



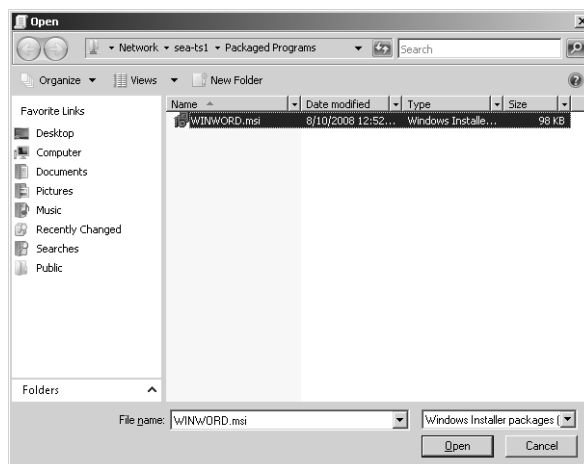
2. When the wizard is finished, the RemoteApp program is listed at the bottom of the center pane of the TS RemoteApp Manager console.



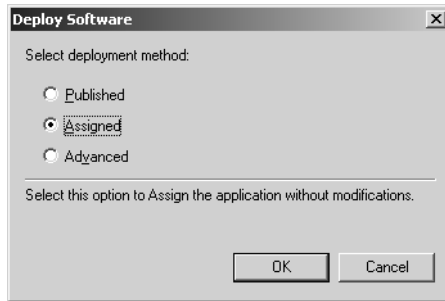
3. With the new RemoteApp selected, click Create Windows Installer Package in the Actions pane to launch the RemoteApp Wizard. This wizard walks you through the process of creating the package and lets you select the location where the package will be saved, configure TS Gateway settings if applicable, and assign a certificate to your package if this is needed. You can also choose whether the RemoteApp program, once deployed, will be displayed on the user's Start menu, on her desktop, or both (our choice here) and also whether double-clicking a file associated with the RemoteApp program (in this case, a .docx or .doc file, for example) will automatically launch the RemoteApp program to open the file.



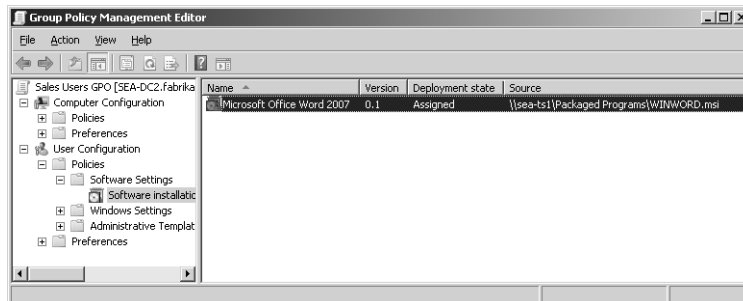
4. When the wizard finishes, the .msi package for the RemoteApp program is saved by default in the C:\Program Files\Packaged Programs directory on your terminal server. To deploy the RemoteApp program using Group Policy, you can either copy this package to a network share or share out the Packaged Programs folder—we'll choose the latter approach.
5. Once the Packaged Programs folder has been shared, use Group Policy Management to open the Group Policy object (GPO) you will use to deploy the RemoteApp program to users in the Sales department. In our scenario, users have their user accounts in the Seattle\Sales Users\Sales Users organizational unit, and a GPO named Sales users GPO is linked to this OU. Open this OU using the Group Policy Object Editor, right-click on User Configuration\Policies\Software Settings\Software Installation, and select New | Package. Browse the network to find the package, which is located at \\SEA-TS1\Packaged Programs\WINWORD.msi.



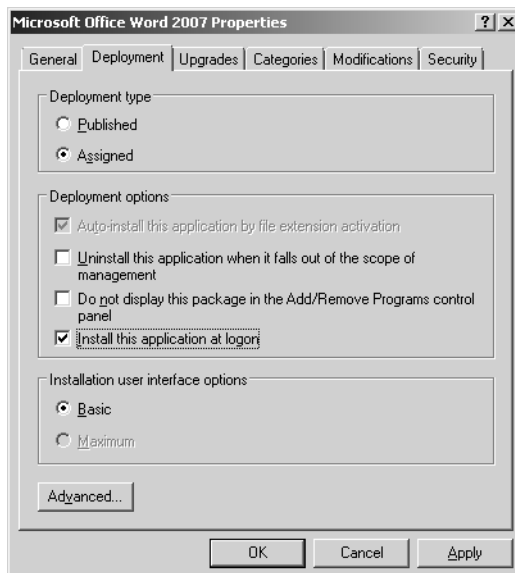
6. Choose the Assigned option to assign the package to the user accounts targeted by the Sales Users GPO.:



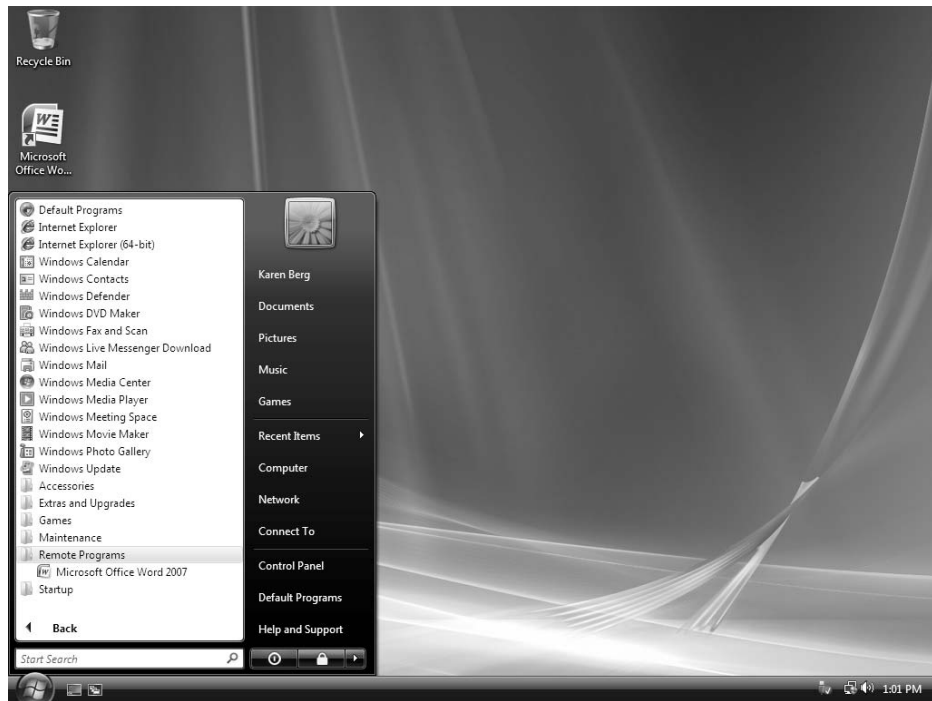
7. The package will now show up as assigned.



8. Double-click on the assigned package to open its properties, and then select Install This Application At Logon so that the package will be installed on the targeted user's computer when she next logs on.



9. Now the next time Karen Berg logs on to her computer, she will see a shortcut to Word 2007 on her desktop and another shortcut in a new Remote Programs folder on her Start menu.



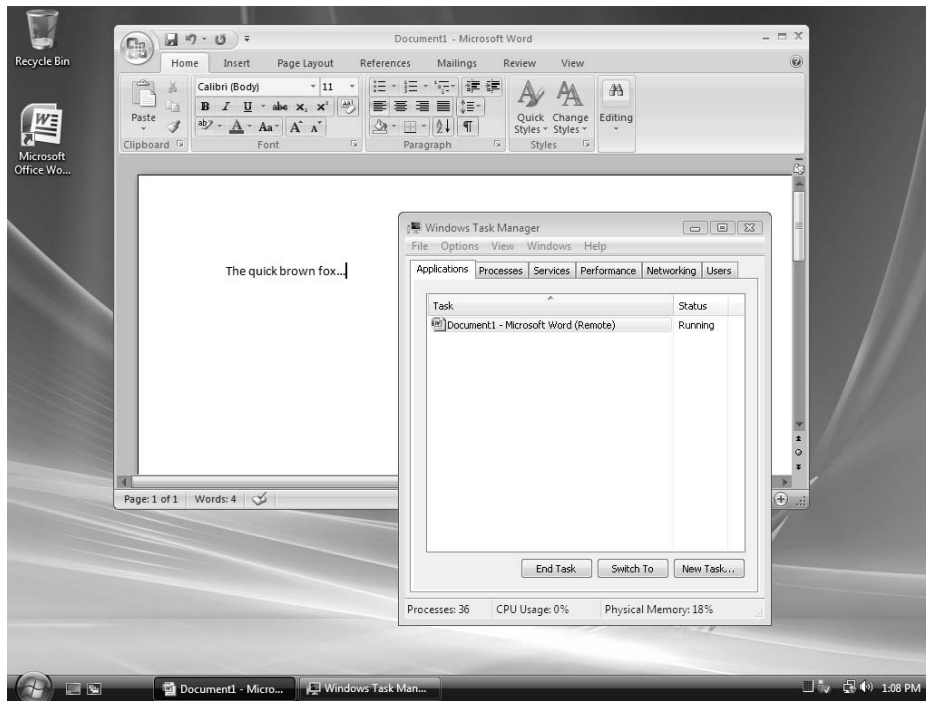
10. Karen then uses either shortcut to launch the RemoteApp program. The first thing that appears is the following notification (the Details button has been selected) because there is no certificate configured in this scenario for the RemoteApp program or for the terminal server.



11. Karen clicks the Connect button and is then required to specify the credentials she will use to run the RemoteApp program. She chooses to save her credentials so that she won't have to enter them again on subsequent uses of this program.



12. Karen clicks OK, and after a few seconds to establish a connection with the terminal server, Word 2007 appears on her desktop—only it's not running on her desktop, it's running on the terminal server. To verify this, she also opens Task Manager and observes that Word 2007 is listed as being "Remote."



Karen can now create a new document and save it just as easily as if Word 2007 had been installed locally on her computer. When she saves her document, it will be saved in her user profile on the terminal server.

Understanding TS Web Access

Terminal Services Web Access (TS Web Access) enables administrators to deploy RemoteApp programs via a Web browser to users on a corporate intranet. Using TS Web Access, a user who needs to run a RemoteApp simply connects to a special Web site, clicks on the RemoteApp program's icon, and the program starts on the user's desktop. Although deploying RemoteApp programs using Group Policy is effective for a large enterprise, TS Web Access can provide a simple means of deploying RemoteApp programs for small and medium-sized businesses because of its ease of use. In addition, by implementing TS Web Access together with TS Gateway, administrators can securely deploy RemoteApp programs to users over an unsecure Internet connection without the need of configuring a VPN for those users.

The experience of running RemoteApp programs deployed using TS Web Access is identical to the experience of launching them from .rdp files or from .msi files deployed using Group Policy. Whichever way a user launches a RemoteApp program, the user can interact with the program just as if it was locally installed on her computer.

TS Web Access also includes a customizable Web Part that provides flexibility in how you display RemoteApp programs you want to deploy. By using this customizable Web Part, administrators can also create their own customized Web page or Windows SharePoint Services site for deploying RemoteApps to users.

TS Web Access also provides users with the option of connecting to the remote desktop of any computer on which they have logon privileges. This feature is known as Remote Desktop Web Connection, and when implemented together with TS Gateway, it enables a user to remotely access the desktop of her corporate desktop computer over the Internet. For more information concerning TS Gateway, see the section titled “Understanding TS Gateway” later in this chapter.

How TS Web Access Works

TS Web Access is implemented as a separate role service of the Terminal Services role of Windows Server 2008 that must be installed together with the Terminal Server role before TS Web Access can be used. Installing the TS Web Access role service on a server also installs the Web Server (IIS) role along with some of its components, which is needed to host the Web site that users connect to using their Web browsers to launch RemoteApp programs.

Both the TS Web Access and Terminal Server role services must be present for TS Web Access to work. The simplest configuration is to install both the TS Web Access and Terminal Server role services on a single server. This server then functions as both your terminal server and a Web server, and users connect to the Web server using their Web browser and launch RemoteApp programs, which then run on the terminal server.

The TS Web Access and Terminal Server role services can also be installed on separate servers if needed. If this is done, however, you must add the computer account of the TS Web Access server to the TS Web Access Computers security group on your terminal server.

For larger deployments, you might install TS Web Access on a front-end Web server and have multiple terminal servers on the back end. You can then configure TS Web Access to populate its list of RemoteApp programs from all your terminal servers, including servers that belong to a Terminal Services farm. These terminal servers must all be running Windows Server 2008 and have the Terminal Services role installed with the Terminal Server role service.

To use TS Web Access, a client computer must have RDC 6.0 client software, which means the client must be running Windows Vista with Service Pack 1, Windows XP with Service Pack 3, or Windows Server 2008. RDC 6.0 client software includes an ActiveX control that enables the user to connect to the TS Web Access server, download the .rdp file for a RemoteApp program, and execute the program using the RDC client software. For an explanation of how this process works, see the sidebar titled “Direct from the Source: TS Web Access Connection Process” later in this chapter.

To connect to the TS Web Access server, a user opens a Web browser such as Internet Explorer and types **http://<server_name>/ts** in the address bar. See the section titled “Using TS Web Access to Deploy RemoteApp Programs” later in the chapter for a walkthrough of how this is done.

Direct from the Source: TS Web Access Connection Process

When a connection is made to a TS Web Access server to run a RemoteApp, the RDP file for the application is downloaded from the Web server and executed on the client. Here are the steps that occur in this process:

1. The Terminal Services ActiveX control, Mstscax.dll, creates an RDP file in the user %temp%\Low folder. The file name will start with TSPORTAL# followed by a random five-digit identifier. The file contains all of the settings needed for the RemoteApp.
2. The ActiveX control calls Mstsc.exe and passes the location of the temporary .RDP file as a parameter:

```
mstsc.exe /web/ webfilename:%userprofile%\Appdata\Local\Temp\Low\<RDP>
```

In this example, <RDP> is the name of the temporary .RDP file that was initially created by the ActiveX control.
3. The RDC client application, Mstsc.exe, reads the .rdp file and then immediately deletes it.
4. A terminal server session is created on the terminal server that is specified in the .rdp file.
5. The specified RemoteApp application starts on the terminal server.

This process can be viewed in real time by using Process Monitor (a Windows resource kit utility) to capture the file access on the client when it is executing the RemoteApp from the TS Web Access server.

—CSS Global Technical Readiness (GTR) team

Using TS Web Access to Deploy RemoteApp Programs

If you have the TS Web Access and Terminal Server role services installed on the same server, any RemoteApps you create using the default settings are automatically published on the Web page for TS Web Access. For example, in the section titled “Deploying and Using RemoteApp Programs” earlier in this chapter, we added Microsoft Office Word 2007

to the list of RemoteApp programs on terminal server SEA-TS1 in the fabrikam.com domain. Figure 5-17 shows TS RemoteApp Manager with Word 2007 listed as a RemoteApp program.

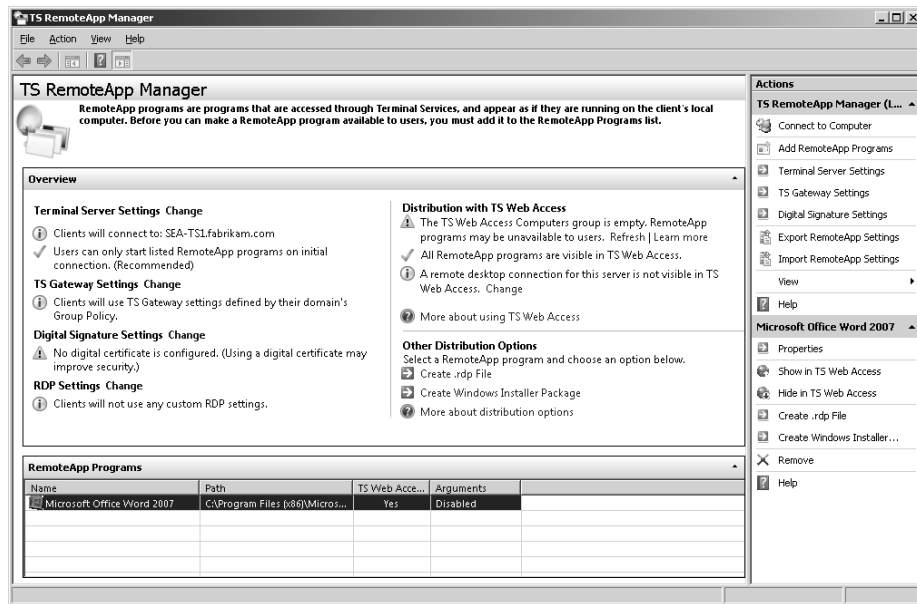


FIGURE 5-17 Word 2007 has been added as a RemoteApp program

You can see in Figure 5-17 that the TS Web Access setting for this RemoteApp program is displayed as Yes, which means that the program should be published in TS Web Access. This is because when you create a new RemoteApp using the RemoteApp Wizard, the default setting is to publish the new RemoteApp program using TS Web Access. If you decide later that you don't want to publish a RemoteApp program using TS Web Access, select the program and click Hide In TS Web Access in the Actions pane.

For this example, let's add a second RemoteApp program to our list: we'll use Microsoft Office Excel 2007 for this purpose. The procedure for doing this is the same as that described earlier in the section titled "Deploying and Using RemoteApp Programs." Now let's verify that Excel has been published by TS Web Access. To do this, select TS Web Access Administration from the Terminal Services folder under Administrative Tools on your Start menu. Doing this opens Internet Explorer and displays the Web page containing the Web Part that is used to deploy RemoteApp programs using TS Web Access. (See Figure 5-18.)



FIGURE 5-18 The TS Web Access Administration Web page

As you can see in Figure 5-18, TS Web Access Administration displays a Web page with three tabs:

- **RemoteApp Programs** Used to launch a RemoteApp program
- **Remote Desktop** Used to connect to the desktop of a remote computer
- **Configuration** Used to specify the name of the terminal server from which TS Web Access populates its list of RemoteApp programs



Note To perform advanced configuration for TS Web Access, use the Internet Information Services (IIS) Manager console to connect to the TS application under the Default Web Site.

Now when a user such as Karen Berg wants to run Excel on the terminal server, she simply types the following URL into Internet Explorer on her computer:

<http://SEA-TS1.fabrikam.com/ts>

Figure 5-19 shows what Karen sees when she does this. Note that the Configuration tab shown previously is not displayed because Karen is not an administrator of TS Web Access.

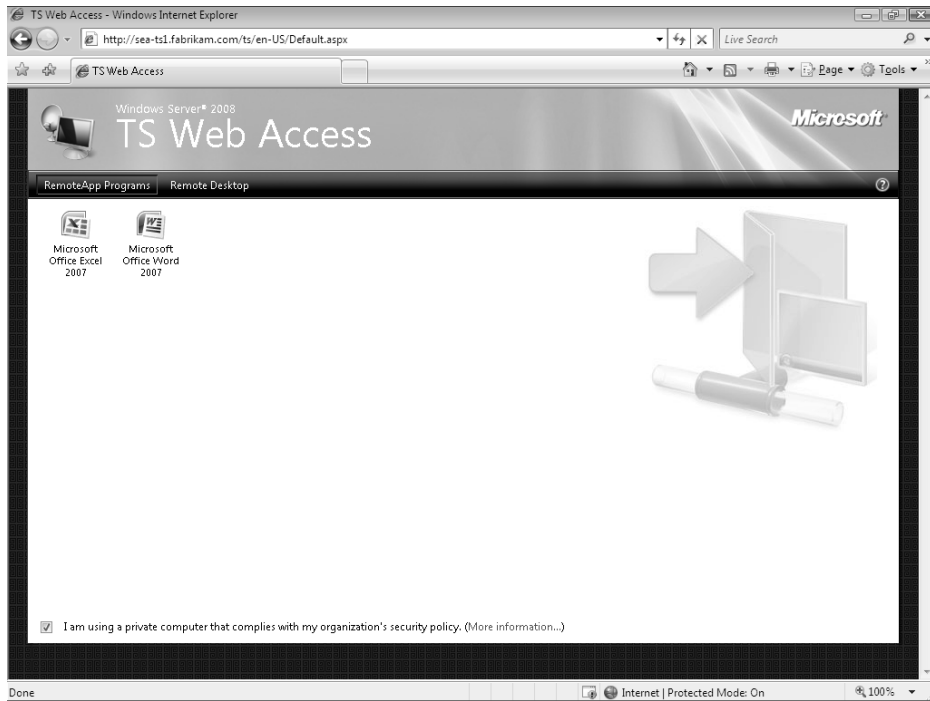


FIGURE 5-19 RemoteApp programs deployed using TS Web Access



Tip If the RemoteApp programs are not being displayed, click the yellow information bar in Internet Explorer to run the Terminal Services ActiveX Client software on your computer.

To launch Excel, Karen clicks on the icon for Excel on the TS Web Access Web page.

Using Remote Desktop Web Connection

Remote Desktop Web Connection is a feature of TS Web Access that allows a user to connect to the desktop of a remote computer directly from the TS Web Access Web site. For this to work, the remote computer must have Remote Desktop enabled, and the user must be a member of the Remote Desktop Users group on the remote computer. Remote Desktop Web Connection is especially useful when a user at home needs to connect to the desktop of his computer on the corporate network, and this can be done in a secure fashion by implementing TS Web Access together with TS Gateway.

To use Remote Desktop Web Connection, the user opens a Web browser such as Internet Explorer and types the following URL:

`http://<server_name>/ts`

Here `<server_name>` can be the fully qualified domain name (FQDN) or IP address of the Windows Server 2008 computer that has the TS Web Access role service installed. When the TS Web Access Web page appears as displayed in Figure 5-19 previously, the user then clicks on the Remote Desktop tab, which displays various connection options. The user specifies the FQDN or IP address of the computer he wants to connect to and configures the various connections as desired. (See Figure 5-20.)

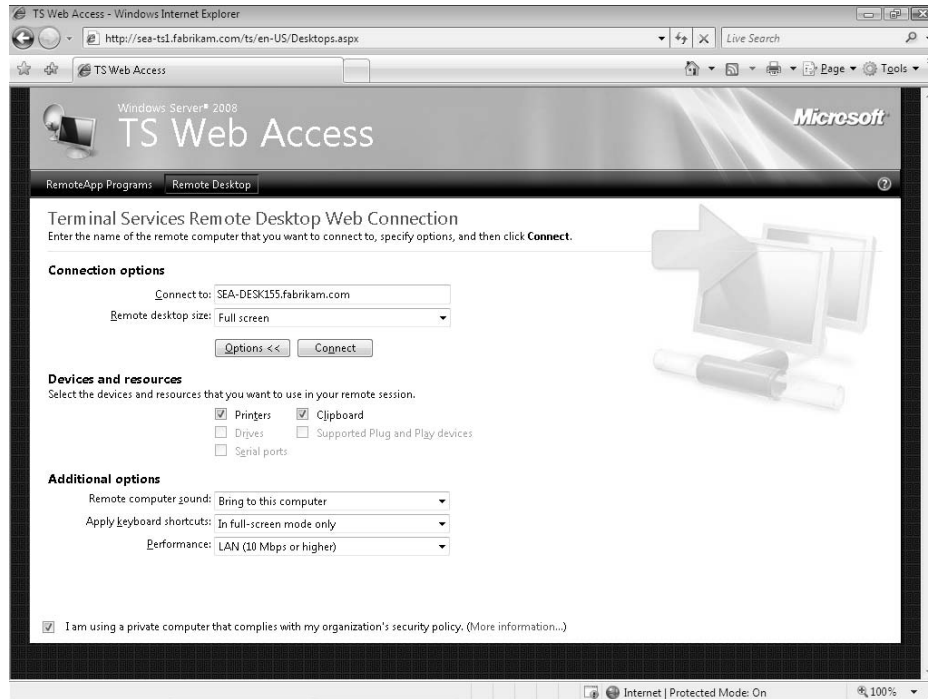


FIGURE 5-20 Using Terminal Services Remote Desktop Web Connection to connect to a remote computer

Clicking Connect initiates the process of connecting to the remote computer. If another user is currently logged on to the remote computer, a screen similar to Figure 5-21 is displayed.



Note If the other user is the same user—for example, if Karen Berg left herself logged on to her computer and later tries to connect to her computer remotely—she will automatically be logged off locally and the remote connection will be established.

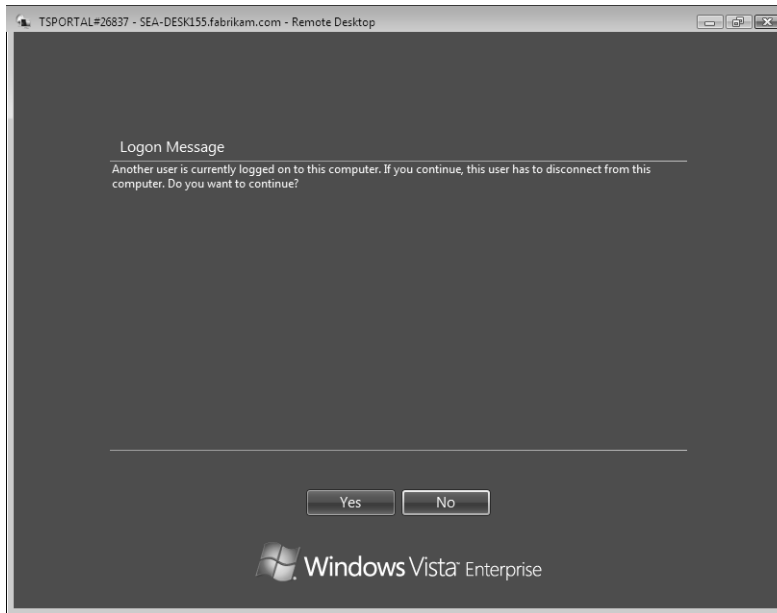


FIGURE 5-21 Another user is currently logged on to the remote computer

Clicking Yes alerts the other user that they have 30 seconds to either click OK, which disconnects the other user from his logon session (while leaving his session active and its applications running), or click Cancel to refuse the remote connection attempt. (See Figure 5-22.)

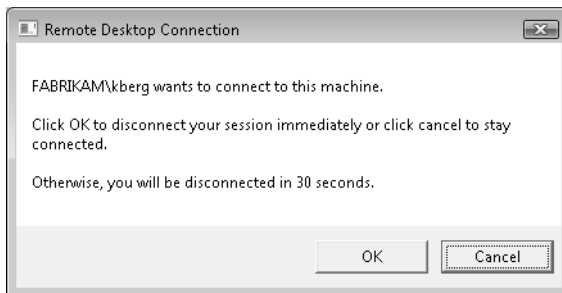


FIGURE 5-22 The user has the option of declining the remote connection attempt

If the other user clicks OK, the user attempting to establish a remote connection succeeds and the desktop of the remote computer is displayed. (See Figure 5-23.)



FIGURE 5-23 Remote Desktop Web Connection is connected to the desktop of the remote computer

Understanding TS Gateway

Terminal Services Gateway (TS Gateway) is a Windows Server 2008 Terminal Services role service that enables authorized remote users to connect to resources on an internal corporate network over the Internet using the Remote Desktop Protocol (RDP). The resources that external users can connect to via TS Gateway include terminal servers running RemoteApp programs and computers that have Remote Desktop enabled. By simplifying the task of enabling secure access to an organization's internal network from over the Internet, TS Gateway provides an alternative to deploying VPN servers and configuring VPN client software on users' computers. TS Gateway also allows organizations that block VPN connections at the firewall to still allow users to remotely connect to the corporate network from home or when travelling.

TS Gateway enhances security by allowing you to place terminal servers needed by external users for access inside the corporate network instead of on the perimeter network. With previous versions of Terminal Services, allowing external users RDP connectivity with terminal servers required that the terminal servers reside on the perimeter network. This configuration potentially exposed these terminal servers to attack from outside the corporate network, an unsatisfactory situation for most organizations. With TS Gateway, however, you can place these same terminal servers inside the corporate network. Only the TS Gateway server itself needs to reside on a screened subnet of the perimeter network. This means that only the TS Gateway server is directly exposed to outside attack. And the attack surface of the TS Gateway server is lower than that of a terminal server placed in a similar location because the only external port that needs to be open on the TS Gateway server is TCP port 443.

TS Gateway also enhances security by providing a point-to-point RDP connection between the remote client and the internal terminal server or a computer having Remote Desktop enabled. TS Gateway thus allows remote users to access anything on the corporate network that allows RDP access, provided they have appropriate privileges for doing so, including networks that are hidden behind firewalls or must be accessed across a Network Address Translation (NAT) device.

TS Gateway can also be implemented together with TS RemoteApp to allow authorized users to connect over the Internet to a terminal server on the corporate network and run individual RemoteApp programs on their desktop. A remote user at home or on the road can also use TS Gateway together with Terminal Services Remote Desktop Web Connection, a feature of TS Web Access, to securely connect to the desktop of her computer on the corporate network as if she is sitting at her desk in the office.

TS Gateway can be combined with several other Windows Server 2008 technologies for increased security and manageability:

- **Network Access Protection (NAP)** NAP is a health policy creation, enforcement, and remediation technology that is implemented on the server side with Windows Server 2008 and on the client side with Windows Vista SP1 and Windows XP SP3. It can be used together with TS Gateway to provide greater control of access to internal resources by enforcing health requirements. For example, you can use NAP together with TS Gateway to allow remote users to access RemoteApp programs only if their computers match the specified health requirements. These health requirements can include having the latest software updates applied to their computers, having required computer configurations, and so on.
- **Microsoft Internet Security and Acceleration (ISA) Server** ISA Server is Microsoft's integrated edge security gateway. ISA Server can be used together with TS Gateway to enhance security by allowing the TS Gateway server to be placed inside the corporate network while the ISA Server resides on a screened subnet of the perimeter network. In addition, the SSL connection between the remote user's RDC client software and the internal terminal server can be terminated at the ISA server, which is an Internet-facing server.

How TS Gateway Works

In previous versions of Terminal Services, RDP connectivity from outside the corporate network required that TCP port 3389 be left open in the organization's perimeter firewall. For security reasons, however, many businesses choose to keep this port closed to help safeguard computers on the internal network from unauthorized access. TS Gateway overcomes this limitation by transmitting RDP traffic over TCP port 443 using an encrypted HTTPS—Secure Sockets Layer/Transport Layer Security (SSL/TLS) over HTTP—tunnel. TS Gateway thus requires only that TCP port 443, the SSL/TLS port, be left open on perimeter firewalls, which is usually the case in most corporate environments.

Figure 5-24 shows a basic TS Gateway scenario where home office workers use TS Gateway to remotely connect to terminal servers and their company computers over the Internet.

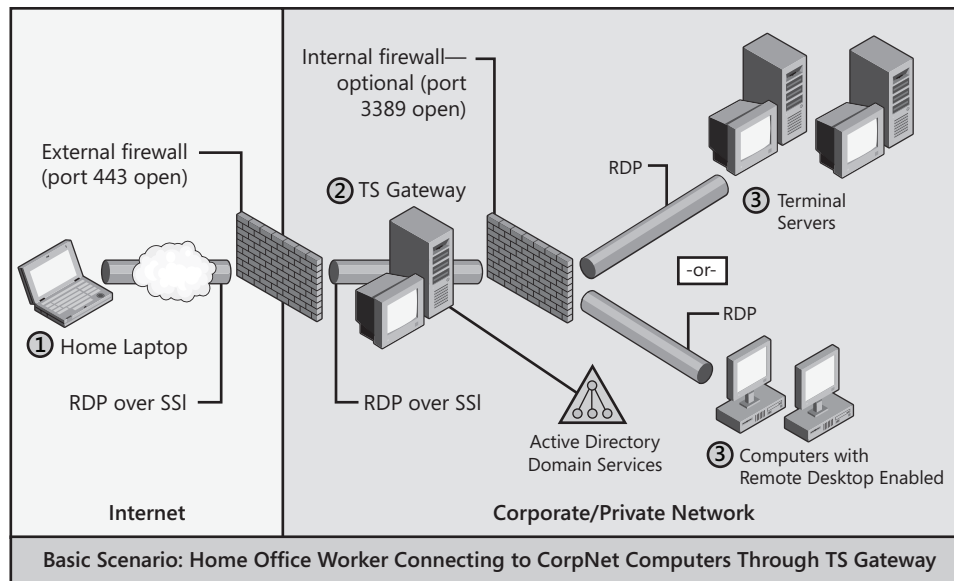


FIGURE 5-24 How TS Gateway works for the home office usage scenario

Implementing TS Gateway

Deploying and configuring a TS Gateway server involves the following high-level steps:

1. Install the TS Gateway role services on a new installation of Windows Server 2008. The computer must not have been upgraded from a previous Windows Server operating system version.
2. Obtain an SSL-compatible X.509 certificate, and install it on your new TS Gateway server. This certificate can be issued by a trusted public certification authority (CA) that participates in the Microsoft Root Certificate Program Members program, a certificate issued by Microsoft Certificate Services running on a server in your corporate network, or even a self-signed certificate that has been exported and imported into the computer certificate store of the client computers that will need to access the TS Gateway server from outside the corporate network.
3. Create a Terminal Services Connection Authorization Policy (TS CAP) on your TS Gateway server. This TS CAP allows administrators to specify the connection criteria that must be met to connect to the TS Gateway server. For example, a simple TS CAP might require a connecting user's account to be a member of a specific security group or it might require the user's computer to have a computer account that belongs to a specific group. The TS CAP could also require that the user use a smart card to connect

through the TS Gateway. Users and computers are granted access to the TS Gateway server provided they meet the conditions specified in the TS CAP. TS CAPs simplify administration and enhance security by providing administrators with greater control over which users and computers are allowed to access resources on the internal network. TS CAPs can also be used to control how device redirection is handled when users remotely connect to terminal servers. And you can create multiple TS CAPs to define different connectivity conditions for different groups of users and computers.

4. Create a Terminal Services Resource Authorization Policy (TS RAP) on your TS Gateway server. This TS RAP allows administrators to specify the internal resources (terminal servers, computers that have Remote Desktop enabled on them, or both) remote users will be allowed to connect to through the TS Gateway server. When you create a TS RAP, you can create a security group containing computer accounts and associate this group with the TS RAP. For example, a TS RAP might specify that users who are members of the HR Users security group are allowed to connect only to computers that are members of the HR Computers group. Then you could create a second TS RAP that specifies that users who are members of the Finance Users group are allowed to connect only to computers that are members of the Finance Computers group. Remote users using TS Gateway to connect to the internal corporate network are then granted access to computers on the network only if they meet the conditions specified in at least one TS CAP and one TS RAP.
5. Once you've installed the TS Gateway role service, obtained and installed a SSL certificate on your server, and configured at least one TS CAP and one TS RAP, the last step you need to perform is to configure the RDC client software on users' computers to use your TS Gateway server. For small-scale deployments, client configuration can be done manually through the Settings button on the Advanced tab of the Remote Desktop Connection dialog box. Clicking this button displays the TS Gateway Server Settings dialog box as follows:



For larger deployments, configuration can be done using Group Policy with the settings found at the following location:

User Configuration\Policies\Administrative Templates\Windows Components\Terminal Services\TS Gateway

6. Once your RDC clients have been properly configured, your remote users can begin to use TS Gateway to access resources on your organization's internal network. For example, users will be able to access internal terminal servers from over the Internet to run RemoteApp programs, and they will be able to access the desktop of their own remote computers, depending on how you have configured things.
7. At this point, you can start using TS Gateway Manager to further configure and maintain your TS Gateway server if desired. For example, you can limit the maximum number of simultaneous connections allowed through your TS Gateway server in order to optimize server performance or ensure compliance with your organization's security policies. And you can use TS Gateway Manager to view information about active connections from Terminal Services clients, including the following:
 - The domain and user ID of the user logged on to the client
 - The IP address of the client
 - The name of the target computer to which the client is connected
 - The target port through which the client is connected
 - The date and time when the connection was initiated
 - The length of time that the connection is idle, if applicable
 - The connection duration
 - The amount of data (in kilobytes) that was sent and received by the client through the TS Gateway server

You can also specify which types of events to monitor for the TS Gateway server, such as successful or unsuccessful connection attempts. These events will be displayed in Event Viewer under Application and Services Logs\Microsoft\Windows\Terminal Services-Gateway.

Understanding TS Session Broker

Terminal Services Session Broker (TS Session Broker) enables Terminal Services users to re-connect to an existing session in a load-balanced terminal server farm. TS Session Broker works by storing session state information, including the session ID, associated user name, and name of the terminal server on which the session resides for each connected user.



Note In previous versions of Terminal Services, this feature was known as Terminal Services Session Directory.

TS Session Broker also includes a new feature called TS Session Broker Load Balancing (SBLB), which enables administrators to distribute the session load between terminal servers in a load-balanced terminal server farm using DNS round robin. SBLB is easier to deploy than Windows NLB, and it is the recommended solution for terminal server farms that have between two to five servers, although there is no hard limit to the number of servers you can use with SBLB.



Note To participate in SBLB, the TS Session Broker server and the terminal servers in the farm must be running Windows Server 2008 Standard Edition or Enterprise Edition.



More Info For more information about implementing TS Session Broker load balancing, see the sidebar titled “Direct from the Source: Implementing Session Broker Load Balancing” in this chapter.

Direct from the Source: Implementing Session Broker Load Balancing

To load balance sessions in a terminal server farm, you can use the TS Session Broker Load Balancing feature together with DNS round robin. To configure DNS, you must create a DNS host resource record for each terminal server in the farm that maps the terminal server’s IP address to the terminal server farm name in DNS.

SBLB in Windows Server 2008 is managed based on the number of sessions. SBLB does more than just count the user sessions; it also has built-in black hole protection (logon throttling) and a max-session count.

Black-Hole Protection

Terminal Services Session Broker Load Balancing has two ways of protecting a server against the black-hole effect. One is by artificially making the load on a server higher during a logon to prevent a terminal server from being overrun by new logins. The load returns to normal when the logon process is finished. Another way the black hole effect is circumvented is by Terminal Services Session Broker itself. TS Session Broker on outstanding connections to the same terminal server can specify a limit on the number of connections.

As an example, consider a setting that allows no more than eight concurrent user logons per server. The max-session count determines a maximum amount of sessions

that every server in the farm can host. This limit prevents a degraded user experience for the users already connected to the terminal server if some terminal servers in the farm are not available. Of course, this is at the expense of new users not being able to set up a session at all, but if an administrator knows his system and knows how many users he can reasonably expect, this should not be a huge problem. The max-session limit, however, is something that needs to be manually configured; it is not automatically calculated by the terminal server and is, in fact, disabled by default. It is also not configurable via the graphical user interface (GUI). If you want to enable it, you need to set the *UserSessionLimit* key to the maximum amount of sessions you want to allow on that server. The *UserSessionLimit* registry key is located at:

HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server

Terminal server load balancing is generally deployed using one of two load-balancing technologies, SBLB Load Balancing or NLB.

Terminal Server Session Broker Load Balancing

To use SBLB to load balance user sessions, DNS entries must be configured.

To configure DNS, you must register the IP address of each terminal server in the farm to a single DNS entry for each farm. This creates a DNS Round Robin (DNSRR) configuration. All incoming Terminal Services clients try to connect to the first IP address for the single DNS entry. If this fails, the client automatically tries to connect to the next IP address in the list. This behavior provides fault tolerance if one of the terminal servers is unavailable. Although all clients initially connect to the first server's IP address, they are quickly redirected to the server in the farm according to the load-balancing configuration.

If a terminal server in the farm is unavailable or congested, the session redirects to a terminal server that can accept the connection.

To configure the system for load balancing, perform the following steps in sequence:

1. Install the TS Session Broker role service.
2. Populate the Session Broker Computers local group.
3. Join the terminal servers to the Session Broker, and configure them to participate in the load balancing.
4. Add DNS entries for all terminal servers.

Network Load Balancing

Network Load Balancing (NLB) is a solution that is not aware of the application it is load balancing. SBLB is an application-level load-balancing solution that is smarter, but it must be deployed with a network-level load-balancing solution to distribute the initial

connections to the farm. The easiest network-level solution to deploy is DNSRR, which complements SBLB pretty well. Alternatively, NLB works great, too, and it provides better detection of offline servers because DNS can suffer a 30 second delay when it picks a server that is offline from the list.

Here are a few deployment possibilities:

- **NLB only.** This option is the only out-of-box scenario for Windows Server 2003 Terminal Services machines. This option is harder to deploy, limited in scale, and not that great at load balancing.
- **DNSRR + SBLB.** This option requires Windows Server 2008 Terminal Services and Windows Server 2008 Session Broker. It is the easiest to deploy, but it still provides great load balancing (better than NLB).
- **NLB + SBLB.** This option requires Windows Server 2008 Terminal Services and Windows Server 2008 Session Broker. It offers better detection of offline servers because of the NLB heartbeat. A continuous heartbeat from each NLB node is confirmation that it is still available to service requests.
- **A hardware load balancer in place of NLB** in any of the aforementioned approaches. This option offers the best features of all, but can be expensive.

Essentially any form of load balancing—such as DNSRR, NLB, HWLB, and so forth—can be used to load balance the initial connections to the farm. Hardware load balancers generally provide efficient connection-distribution and network-level security features, but for many deployments, the session-based algorithm used by Session Broker provides better load distribution than the connection-based algorithms used by most hardware load balancers.

User Profiles

Session Broker does not manage user profiles. Users will get a new or independent profile on each server unless some other technology is implemented, such as roaming or mandatory profiles.

It is a recommended best practice to deploy either roaming profiles or mandatory profiles when deploying a load-balanced farm of terminal servers. The default of having different local profiles on each server results in a very bad user experience. It is also a best practice to redirect the My Documents and Desktop folders using the Folder Redirection technology because this reduces the size of the user profile and avoids issues with downloading huge profiles at logon.

—CSS Global Technical Readiness (GTR) team

Key Benefits of Terminal Services

The overview of Windows Server 2008 Terminal Services provided by the previous section has already introduced you to the key features and enhanced capabilities of this latest version of Terminal Services. The benefits of deploying Terminal Services in business environments derive mainly from the greater IT flexibility and increased security that results from running mission-critical line-of-business applications on secure, centrally located servers. The following is a quick summary of three key benefits your organization can experience from implementing a Windows Server 2008 Terminal Services presentation virtualization solution:

- Terminal Services allows you to accelerate application deployments and operating system migration—for example:
 - You can use Terminal Services to accelerate application deployment and maintenance and to simplify ongoing management of applications. Instead of having to update applications on each desktop, only the single shared copy of the application running on the terminal server needs to be installed and kept up to date with software updates.
 - You can use Terminal Services to deploy applications to a wide spectrum of clients, including older versions of Microsoft Windows on which these applications cannot natively run. The result is that computer hardware upgrades will not be required to deploy these applications, which saves you time and money.
 - Because Terminal Services applications are not installed locally, Terminal Services enables more streamlined desktop operating system images. This can help accelerate the adoption of new operating systems, such as Windows Vista, by your organization so that your business can benefit from the new features and enhanced capabilities of these operating systems. It can also help accelerate your adoption of thin clients, which can lower management costs.
- Terminal Services helps you secure mission-critical data and applications—for example:
 - When Terminal Services applications and data run on terminal servers located in a datacenter, you can be confident when users are running RemoteApp programs or accessing the desktop on remote computers because only encrypted keyboard and mouse strokes are transmitted over the network.
 - If your organization has regulatory compliance requirements to adhere to, the centralization provided by Terminal Services can help to greatly simplify the challenges associated with achieving such compliance.
 - TS RemoteApp used together with TS Gateway simply and securely provides remote connectivity for users outside the corporate firewall—from home, hotels, or customer sites to mission-critical internal applications and data—without the additional complexity involved of deploying and maintaining a VPN infrastructure.

- ❑ TS Gateway used together with NAP provides enhanced security by ensuring that client computers are scanned for the latest antivirus signature files and software updates before they are allowed to connect to resources on the corporate network. This configuration helps to ensure that unhealthy client computers are not allowed to access your terminal servers.
- Terminal Services allows you to improve worker efficiency—for example:
 - ❑ You can use TS RemoteApp together with TS Web Access to quickly and easily provide remote or mobile workers with the applications they need to do their work, whether they are connecting from their laptop, their home computer, or an airport kiosk. By simply accessing a secure Web page, they can launch applications or access data that are not installed or available on their computers.
 - Because RemoteApp programs appear no differently than local applications and are tightly integrated with the task bar and new Windows Vista features, users do not need retraining to use them—they can just click and work.
 - Terminal Services optimizes application performance for both high-bandwidth and low-bandwidth connections. This means that data-intensive applications such as enterprise resource planning (ERP) systems that typically slow end-user productivity can receive a performance boost when delivered to remote users via Terminal Services.

Terminal Services Usage Scenarios

Finally, I'll conclude this chapter by briefly describing six common usage scenarios involving Windows Server 2008 Terminal Services:

- Branch office
- Controlled partner access or outsourcing
- Easing the burden of regulatory compliance
- Merger integration
- Mobile workers
- Task workers

Branch Office

Deploying line-of-business software applications for users at multiple branch offices can be time-consuming and costly. Terminal Services can help reduce this cost by allowing you to run such software on terminal servers located at a central headquarters. Employees at branch

offices can then access these applications on an as-needed basis via remote desktops or as RemoteApp programs, even over low-bandwidth connections.

Controlled Partner Access or Outsourcing

The burden and complexity of deploying and maintaining line-of-business software applications on computers belonging to business partners or outsourcing firms can be significantly reduced by using Terminal Services. Partners and outsourced workers are able to access the applications they need to do their job without having to obtain and install these applications on their own computers. This can make for a smoother business relationship between your organization and your business partners or outsourcing firms, plus it provides added security by limiting the access these businesses will need to resources on your own corporate network.

Easing the Burden of Regulatory Compliance

By running applications and storing application data on centrally located servers, Terminal Services helps reduce the risk of accidental data loss caused, for example, by the accidental loss of a laptop. The zero-application footprint and data delivery model employed by Terminal Services also helps to ensure that as little data as possible resides on the client computing device. And by using TS Gateway together with TS RemoteApp, employees, partners, and customers no longer require full access to your corporate network and computers. Instead, you can limit the applications they can access even to using a single application, if needed.

Merger Integration

During a corporate merger, companies typically need to use consistent line-of-business applications on a variety of Windows operating system versions and configurations. Rather than going through the effort and incurring the high cost of deploying all your LOB applications to all the computers in the merged company, these applications can simply be installed on a terminal server and made available to those who need it via TS RemoteApp. This can be especially useful when an application is difficult to maintain, cannot be deployed easily, or has other management issues.

Mobile Workers

Organizations that support employees who work from home or work while traveling can implement a Terminal Services solution to help enable employee productivity anytime and anywhere. Terminal Services can also increase effective collaboration between users without

compromising security, and it can offer secure access to applications over low-bandwidth connections without requiring those applications to be installed on client computers.

Task Workers

Organizations that have structured task workers—such as call center employees, factory floor workers, or both—can use Terminal Services to provide such employees with a more productive user experience. Typically, task workers like these do not need to access very many applications to complete the tasks they have been assigned, and TS RemoteApp together with TS Web Access provides an easy way for them to access the applications they need, when they need them. A similar user experience can be provided even if the user's computer is an older desktop computer running an earlier version of Windows, a non-PC desktop computer, or a mobile computing device. Deploying applications for task workers in this way can help extend the reach of Windows-based applications within an enterprise and is a valuable, cost-effective way to deliver the right business tools to the people who need them.

Additional Resources

The resources listed in this section were either referred to in the chapter or provide additional information concerning concepts and products discussed in this chapter.

General

A general overview of the features and benefits of implementing presentation virtualization using Windows Server 2008 Terminal Services can be found on the Microsoft Virtualization site at <http://www.microsoft.com/virtualization/solution-tech-presentation.mspix>. Additional information on this topic can be found on the Windows Server 2008 product information site at <http://www.microsoft.com/windowsserver2008/en/us/ts-product-home.aspx>.

Deploying Terminal Services

The best resource for planning a Terminal Services deployment is the Windows Server 2008 Terminal Services Infrastructure Planning and Design (IPD) guide, which can be downloaded from the Microsoft Download Center at <http://www.microsoft.com/downloads/details.aspx?FamilyId=AD3921FB-8224-4681-9064-075FDF042B0C&displaylang=en>. You can also read this guide online in the TechNet Library on Microsoft TechNet at <http://technet.microsoft.com/en-us/library/cc268349.aspx>.

Before you try to implement a presentation virtualization solution using Windows Server 2008 Terminal Services, you need to be familiar with what's new in this version of Terminal Services. The best source of information for this is the Terminal Services Product Evaluation

section of the TechNet Library on Microsoft TechNet at <http://technet.microsoft.com/en-us/library/cc753679.aspx>.

A good way to become familiar with the key components of Windows Server 2008 Terminal Services are the following Step-By-Step guides:

- TS RemoteApp Step-by-Step Guide found at <http://technet.microsoft.com/en-us/library/cc730673.aspx>.
- TS Web Access Step-by-Step Guide found at <http://technet.microsoft.com/en-us/library/cc771354.aspx>.
- TS Gateway Step-by-Step Guide found at <http://technet.microsoft.com/en-us/library/cc771530.aspx>.
- TS Licensing Step-by-Step Guide found at <http://technet.microsoft.com/en-us/library/cc754034.aspx>.
- TS Session Broker Load Balancing Step-by-Step Guide found at <http://technet.microsoft.com/en-us/library/cc772418.aspx>.

All of these Step-by-Step guides and others can also be downloaded from the Microsoft Download Center at <http://www.microsoft.com/downloads/details.aspx?FamilyID=518d870c-fa3e-4f6a-97f5-acaf31de6dce&DisplayLang=en>.

Maintaining and Managing Terminal Services

Detailed information concerning Group Policy Settings for managing Terminal Services in Windows Server 2008 can be found in the TechNet Library on Microsoft TechNet at <http://technet.microsoft.com/en-us/library/cc753697.aspx>.

A reference listing all Terminal Services events in Windows Server 2008 can be very useful for troubleshooting purposes; you can find such a reference in the TechNet Library on Microsoft TechNet at <http://technet.microsoft.com/en-us/library/cc732506.aspx>.

The Terminal Services Management Pack for Microsoft Operations Manager 2008 can be used to monitor the individual Terminal Services components on Windows Server 2000, 2003, and 2008; you can download this Management Pack from the Microsoft Download Center at <http://www.microsoft.com/downloads/details.aspx?FamilyID=1428ecfd-8c3e-4779-a383-4c491d2684f3&DisplayLang=en>.

Terminal Services Client Software

The Remote Desktop Connection Client for Mac 2 lets you connect from your Macintosh computer to a Windows-based computer and then work with applications and files on the Windows-based computer; you can download the RDC Client for Mac 2 from the Microsoft

Download Center at <http://www.microsoft.com/downloads/details.aspx?FamilyID=803f9438-8df3-490f-92c6-0e0f92787db8&DisplayLang=en>.

Microsoft IT Showcase

You might like to learn about the MSIT pilot project of Windows Server 2008 Terminal Services and TS Gateway. This pilot was so successful that Microsoft IT went on to test the scalability and performance in their production environment. The white paper describing this project can be downloaded from the Microsoft Download Center at <http://www.microsoft.com/downloads/details.aspx?FamilyID=f7af4775-2755-4f73-9275-975ec815a78e&DisplayLang=en>.

Terminal Services Team Blog

Get the latest news and tips about Windows Server 2008 Terminal Services on the Terminal Services Team Blog at <http://blogs.msdn.com/ts>. This is one of the best blogs by product teams at Microsoft in terms of the quality and relevance of content for IT pros.

Terminal Services Webcasts

The following TechNet Webcasts include helpful demonstrations of different Windows Server 2008 Terminal Services technologies:

- Overview of Windows Server 2008 Terminal Services (Level 100) at <http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?EventID=1032355617&EventCategory=5&culture=en-US&CountryCode=US>
- A Technical Overview of Windows Server 2008 Terminal Services (Level 200) at <http://msevents.microsoft.com/cui/WebCastEventDetails.aspx?culture=en-US&EventID=1032345661&CountryCode=US>
- Deploying Remote Programs With Windows Server 2008 Terminal Services (Level 300) <http://msevents.microsoft.com/cui/WebCastEventDetails.aspx?culture=en-US&EventID=1032355965&CountryCode=US>
- Windows Server 2008 Terminal Services RemoteApp and Web Access (Level 300) at <http://msevents.microsoft.com/cui/WebCastEventDetails.aspx?culture=en-US&EventID=1032355811&CountryCode=US>
- Windows Server 2008: Centralizing Application Access With Terminal Services (Level 300) at <http://msevents.microsoft.com/cui/WebCastEventDetails.aspx?culture=en-US&EventID=1032336497&CountryCode=US>

- Windows Server 2008 Terminal Services Licensing (Level 300) at <http://msevents.microsoft.com/cui/WebCastEventDetails.aspx?culture=en-US&EventID=1032356770&CountryCode=US>
- Windows Server 2008 Terminal Services Session Broker (Level 300) at <http://msevents.microsoft.com/cui/WebCastEventDetails.aspx?culture=en-US&EventID=1032355536&CountryCode=US>
- Terminal Services Easy Print (Level 300) at <http://msevents.microsoft.com/cui/WebCastEventDetails.aspx?culture=en-US&EventID=1032355423&CountryCode=US>
- Windows Server 2008 Terminal Services Security and Authentication (Level 300) at <http://msevents.microsoft.com/cui/WebCastEventDetails.aspx?culture=en-US&EventID=1032355426&CountryCode=US>

Also be sure to see the following Webcasts from the “24 Hours of Windows Server 2008” series:

- 24 Hours of Windows Server 2008 (Part 04 of 24): Presentation Virtualization with Terminal Services RemoteApp (Level 200) at <http://msevents.microsoft.com/cui/WebCastEventDetails.aspx?culture=en-US&EventID=1032369742&CountryCode=US>
- 24 Hours of Windows Server 2008 (Part 05 of 24): Terminal Services Gateway and Terminal Services Web Access (Level 200) at <http://msevents.microsoft.com/cui/WebCastEventDetails.aspx?culture=en-US&EventID=1032369746&CountryCode=US>
- 24 Hours of Windows Server 2008 (Part 06 of 24): Deploying and Migrating to Terminal Server (Level 200) at <http://msevents.microsoft.com/cui/WebCastEventDetails.aspx?culture=en-US&EventID=1032370844&CountryCode=US>

Terminal Services Forum on TechNet

To obtain help with your questions and problems concerning Terminal Services, and to help others, use the Terminal Services forum on Microsoft TechNet at <http://forums.technet.microsoft.com/en-US/winserverTS/threads>.

Chapter 6

Desktop Virtualization—MED-V and VDI

Another pillar of Microsoft's integrated Virtualization 360 vision is *desktop virtualization*, which generally refers to any technology that creates an additional isolated operating system environment on a standard desktop computer. Microsoft's desktop virtualization technologies are rapidly evolving, and some of the products and solutions described in this chapter are still under development. This means that some of this chapter is based on prerelease product information and is therefore subject to change. Nevertheless, because these new technologies are powerful and exciting, it's important that you know about two emerging desktop virtualization technologies from Microsoft, namely Microsoft Enterprise Desktop Virtualization (MED-V) and Microsoft Virtual Desktop Infrastructure (Microsoft VDI).

Understanding Desktop Virtualization Technologies

Before we examine the MED-V and Microsoft VDI technologies in detail, we first need to understand how they differ. The term "desktop virtualization" is often used to describe two complementary technologies: server-based virtualization and client-hosted virtualization.

In both of these technologies, a standard desktop operating system (including applications, user data, and settings) is being encapsulated in a virtual machine that the user can access. In client-hosted desktop virtualization, this virtual machine resides and operates on the client itself. Server-based desktop virtualization, however, runs multiple virtual machines on a server while the user just gets a remote display to his PC or thin client, typically via the Microsoft Remote Desktop Protocol (RDP).

While in many cases both technologies can solve similar business problems, each technology has its pros and cons and fits some usage scenarios better than others. For example, when you want to have a thin-client desktop environment for a task-driven workforce such as a call center, the server-based solution is a great fit. On the other hand, if you need to provide a corporate desktop and set of applications to the laptop of an employee who travels a lot and who needs to be able to work offline or over a limited-bandwidth network connection, the client-hosted solution is the right one for you.

In other usage scenarios, it's basically a matter of whether the customer prefers a centralized computing environment and can invest in server farms, or if the customer prefers a decentralized environment that leverages endpoint device computing power.

By complementing each other, these two desktop virtualization technologies—client-hosted and server-based—together provide a complete solution for customer needs. And Microsoft offers both of these solutions—MED-V for client-hosted desktop virtualization and Microsoft VDI for server-based desktop virtualization.

Understanding Microsoft Enterprise Desktop Virtualization

Microsoft Enterprise Desktop Virtualization (MED-V) is an upcoming desktop virtualization technology that builds upon the highly popular and easy-to-use Microsoft Virtual PC 2007, a first-generation desktop virtualization product. This means that to understand how MED-V works, you need to begin by understanding Virtual PC.

The Foundation—Microsoft Virtual PC

First introduced in 2004 and based on earlier technology acquired from Connectix, Microsoft Virtual PC is a free software product that allows users to run multiple virtual machines directly on their desktop computers. Each virtual machine (VM) consists of a guest operating system, which is another instance of an operating system running concurrently with the host operating system, and is independent of the host hardware or setup. The guest operating system can be used to run applications the user needs on a separate operating system environment. Virtual PC works by emulating a standard PC hardware environment, which includes hardware devices such as the S3 Trio video card and the Intel 21140 network card, for compatibility with the greatest possible number of Microsoft Windows operating systems and applications. Virtual PC 2007 added support for hardware virtualization, which enables virtual machines to take advantage of virtualization extensions in newer AMD and Intel processes to achieve significantly increased performance when running virtual machines.

Most readers of this book are already familiar with Virtual PC, so we won't go any deeper into its capabilities and features. To learn more about Virtual PC and to download a copy, visit the Microsoft Virtual PC 2007 product page at <http://www.microsoft.com/windows/products/winfamily/virtualpc/default.mspx>. You can also find a wealth of tips and tricks for using Virtual PC on the blog of Ben Armstrong, the "Virtual PC Guy," which is found at http://blogs.msdn.com/virtual_pc_guy/default.aspx.



Tip Businesses that deploy Windows Vista Enterprise edition on users' computers can automatically benefit from being able to install up to four additional copies of the operating system (or previous operating system versions) in virtual machines running on top of a computer running Windows Vista Enterprise while requiring only a single license. For more information about Windows Vista Enterprise edition, a premium edition of Windows Vista designed for businesses and available exclusively to Microsoft Software Assurance customers, see <http://www.microsoft.com/licensing/sa/benefits/vista.mspx>.

Introducing Microsoft Enterprise Desktop Virtualization

Microsoft Enterprise Desktop Virtualization enhances deployment, management, and user experience for Virtual PC images to streamline operating system upgrades and to increase IT control and user flexibility in enterprise environments. With MED-V, application-to-operating system compatibility issues are minimized; operating system migrations are accelerated; and delivery and reconstitution of corporate desktops are made easy, simplifying support tasks, business continuity, and incorporation of heterogeneous IT environments.

Based on the technology acquired from Kidaro, MED-V adds four additional features on top of Virtual PC 2007. These mechanisms are designed to facilitate the creation, storage, delivery, and management of Virtual PC images to desktop computers. At a high level, the four additional technologies provided by MED-V are as follows:

- **Virtual images repository and delivery** Simplifies the process of creating, testing, delivering, and updating virtual images
- **Centralized management and monitoring** Manages the life cycle of virtual images, provisions virtual images to authenticated users according to Microsoft Active Directory users and groups, and aggregates client events for monitoring and reporting purposes.
- **User policy and data transfer control** An endpoint agent enforces usage policies and data transfer permissions on the virtual machine.
- **Seamless end-user experience** The user remains unaware of the virtualization running in the background and keeps one desktop environment.

Virtual Image Repository and Delivery

MED-V provides mechanisms for storing and delivering standard Virtual PC images (also called virtual images) onto user's desktop computers. These mechanisms simplify the process of creating, testing, deploying, and maintaining virtual images from a central location.

The virtual image repository and delivery capabilities provided by MED-V include

- A central repository for storing virtual images you create
- A format for packaging the MED-V client and virtual images for automatic deployment over the network, over the Web, or via removable media such as DVD media or USB key drives
- A client component that allows users to retrieve virtual images using a standard Web infrastructure, together with an automated process for keeping users' computers updated with the most recent image build without interrupting their work

- An efficient, bandwidth-conserving Trim Transfer mechanism for delivering virtual images over both high-speed local area network (LAN) and slow wide area network (WAN) connections
- A mechanism for automating the first-time setup of virtual machines—for example, by specifying a unique computer name, performing initial network setup, joining a domain, and performing other needed deployment steps
- The ability to remotely assign the amount of RAM allocated for use by Virtual PC on endpoint computers, which facilitates deployment of virtual images across diverse computers

For a closer look at some of these technologies, see the section titled “How MED-V Works” later in this chapter.

Centralized Management and Monitoring

MED-V provides the means for managing the entire life cycle of virtual machines deployed on desktop computers throughout an enterprise. The centralized management and monitoring capabilities provided by MED-V include

- A central management server that can be used to control virtual machines that have been deployed onto desktop computers
- Integration with Microsoft Active Directory Domain Services to enable provisioning of virtual images based on group membership or user identity
- The requirement that users must authenticate using a valid account before being granted access to the virtual desktop, regardless of whether the virtual machine is online or offline
- A central database of all client activity and events, making it easy for helpdesk personnel to remotely monitor for problem conditions and to facilitate troubleshooting
- The ability to revert a virtual machine back to its base image, making it easy for helpdesk personnel to support the virtual desktops

Usage Policy and Data Transfer Control

MED-V includes an agent on the endpoint (client) that can be used to enforce the application of corporate usage policies and permissions to virtual machines for specified users, groups, or both. The usage policy and data-transfer control capabilities provided by MED-V include

- The ability to configure an expiration date for a virtual machine and specify a time limit for offline use of the virtual machine.

- The ability to configure inbound and outbound data transfer between the virtual machine and the endpoint, regardless of whether data transfer is performed using copy/paste, file transfer, or printing.
- The ability to automatically redirect specified Web sites (such as the corporate intranet or sites that require an older version of the browser) from the endpoint browser to the virtual machine so that they run automatically when the browser installed on the virtual machine is started.

Seamless End-User Experience

MED-V provides a seamless experience for end-users, making users unaware of the virtual machines running in the background. Overall, it reduces the training required for deploying Virtual PC images by making the deployment process transparent to the end user and simplifying the work process with virtual machines. The end-user experience provided to users by MED-V includes

- Applications that are installed on the Virtual PC are made available (“published”) to the user via the Start menu, desktop shortcuts based on administrator policy, or both.
- Applications that are published to endpoints using MED-V and are installed in Virtual PC are made available to the user via the Start menu, desktop shortcuts, or both on the user’s computer.
- The user has access to any applications published to him via MED-V even when the user’s computer is disconnected from the corporate network (offline) or when network connectivity is limited.

How MED-V Works

The following description of how MED-V works is based on a prerelease version of the product and is subject to change. The upcoming sections cover the following topics:

- MED-V Terminology
- System requirements
- Supported applications
- Deploying packages
- Workspace initialization
- Using the workspace
- Configuring usage policies
- Managing and maintaining virtual images

MED-V Terminology

The following terminology is used for describing different components of a MED-V environment:

- **Host** The end user's physical computer, typically a desktop or laptop computer. It's also called an endpoint computer.
- **MED-V Client** Software that runs on the host that can download and run Virtual PC images seamlessly on the host, according to MED-V usage policies.
- **MED-V Image Repository** An IIS Web server that stores and distributes virtual images to endpoints.
- **MED-V Management Server** A MED-V server that authenticates, provisions, and controls all users of the system. Client-server communication is based on HTTP or HTTPS.
- **MED-V Server** The server that holds the main image repository and is the management server.
- **MED-V Package** A mechanism for installing Virtual PC, the MED-V client, and optionally a virtual image on a host.
- **Workspace** The Virtual PC image that the MED-V client runs on the host. It's also called a virtual machine or guest.

System Requirements

On the client side (the host computer), the requirements for running the MED-V client will be similar to the requirements for running Virtual PC. Specifically, if a user's computer is unable to run Virtual PC, it won't be able to run the MED-V client either. In addition, the initial version (v1) of the MED-V client will run only on 32-bit versions of Windows Vista and Windows XP.

The final system requirements for running the MED-V client will be determined prior to availability of the product. The system requirements for running Virtual PC 2007 Service Pack 1 (SP1) can be found at <http://www.microsoft.com/downloads/details.aspx?FamilyID=28c97d22-6eb8-4a09-a7f7-f6c7a1f000b5&DisplayLang=en>.

At the time of this writing, the supported guest operating systems that can run in Virtual PC on a host that runs MED-V include Windows XP SP2, Windows XP SP3, and Windows 2000 SP4. Support for running additional guest operating systems such as Windows Vista in future versions or service packs of MED-V is being investigated and might be possible for the release of MED-V v1.

On the server side (MED-V server), a Windows Server 2008 with IIS and Microsoft SQL Server is required but the system requirements are not yet defined. In addition, MED-V v1 will

require a separate server infrastructure for deploying and maintaining virtual images on endpoint computers. Future versions of MED-V might integrate these management capabilities with Microsoft's System Center family of products.

The MED-V server can be installed either on a member server belonging to an Active Directory Domain Services domain or on a standalone server when using a workgroup scenario. If a domain environment is being used, authentication and authorization of the user is performed against Active Directory Domain Services. If a workgroup environment is being used, authentication and authorization is performed using user and group accounts stored locally on the server.

Supported Applications

Because MED-V does not add any additional layer of virtualization functionality on top of Virtual PC, any application that has vendor support for running on Virtual PC should also run in MED-V without encountering any issues. There are no special restrictions on the type of applications that can run in MED-V workspaces. One of the key benefits of MED-V is helping enterprises deal with incompatibility between applications and the operating system. For instance, if a user needs to run an early version of Microsoft Internet Explorer and that version of Internet Explorer is not supported on Windows Vista, the administrator can use MED-V to deploy this early version of Internet Explorer to the user as part of a Windows XP virtual image. The user could then have two copies of Internet Explorer running simultaneously on her desktop—the most recent version (running on the host computer) and the earlier version (running in the MED workspace). From the user's perspective, both copies of Internet Explorer appear as if they were running on the local computer. MED-V does this by allowing users to run legacy applications within a virtual machine that has an earlier version of Microsoft Windows installed. The user can then access these applications either from a virtual desktop (as with Virtual PC running natively on a system) or by using application windows that are seamlessly integrated into the local desktop of the user's computer (similar to Terminal Services RemoteApp).

Microsoft Application Virtualization (App-V), which was described in Chapter 4, "Application Virtualization—App-V," also helps enterprises handle application compatibility issues, but it addresses challenges differently than MED-V does. Specifically, App-V lets you resolve conflicts that arise between different applications or different versions of the same application; MED-V, on the other hand, allows users to run older versions of Microsoft Windows concurrently with the local desktop of their computers, which can help with issues where legacy applications are unable to run natively on the most recent version of Windows installed on the user's computer.

Deploying Packages

MED-V packages are used to deploy full Virtual PC images to host computers as MED-V workspaces. These virtual images include a guest operating system, applications, and user data. Guest operating systems can be either domain members or standalone systems, and if the host computer is a domain member, the virtual machine can even belong to a different domain if needed. MED-V workspaces are fully functional virtual desktop computers and can be associated with any Active Directory Domain Services environment. For example, a workspace that is a domain member can be locked down using Group Policy.

MED-V packages are typically deployed onto host computers that already have Virtual PC installed on them. If a host computer does not have Virtual PC installed, a MED-V package can be constructed that will deploy Virtual PC together with the Virtual PC image being deployed to the host.



Note Local Administrator privileges on the host system are required in order to install a MED-V package. Alternatively, MED-V and Virtual PC can be installed using a software distribution mechanism such as Microsoft System Center Configuration Manager (SCCM).

When a MED-V package is installed on a host system and the workspace is active, a prespecified amount of RAM on the host system is allocated for running the Virtual PC image. In other words, when you create a MED-V package to deploy a virtual image to a host system, you can specify how much RAM the host system will use for running the virtual image using Virtual PC.

MED-V packages can be deployed over any network connection, including high-speed LAN connections, slow WAN links, or virtual private network (VPN) connections. You can also deploy virtual images to users on removable media, such as USB key drives or CD/DVD media, when network connectivity is not available for the user. Packages that are deployed via removable media can be encrypted so that only authorized users will be able to install and use the virtual images.



Note To enforce MED-V usage policies, Virtual PC images that have been deployed to host computers via MED-V packages will not run natively in Virtual PC on systems where the MED-V client has not been installed. In other words, users cannot bypass MED-V by running MED-V-deployed virtual images directly in Virtual PC. The reason this is not possible is because MED-V creates encrypted virtual images that can be accessed only by the MED-V client.

Workspace Initialization

After a MED-V package has been deployed to a host computer, the host has the following software installed:

- MED-V client software
- Virtual PC
- A virtual machine image

The next step is to initialize the MED-V workspace. Figure 6-1 illustrates the steps involved in the process of initializing the workspace on a host computer to which a MED-V package has been deployed.

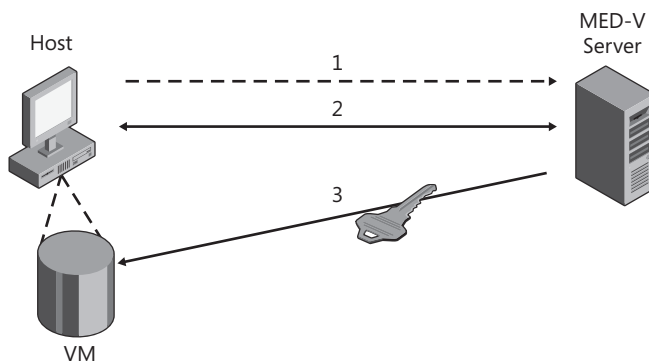


FIGURE 6-1 CONNECTION SEQUENCE FOR INITIALIZING THE WORKSPACE ON A HOST.

The steps involved in this initialization sequence are as follows:

1. When the MED-V client is installed and started on the host, the client tries to establish a communications channel with the MED-V server using a preconfigured port.
2. After this communications channel has been established, the user's credentials are authenticated against the MED-V server.
3. If user authentication is successful, the MED-V server provides the host with an encryption key that can be used to decrypt the virtual machine (VM) image that the MED-V server has previously deployed to the host. After the VM has been decrypted, the MED-V client running on the host uses Virtual PC to launch the VM, which initializes the MED-V workspace on the host. The user can then access either of the following:
 - ❑ The full virtual desktop of the active virtual machine. In this case, the virtual desktop is displayed as a separate window on the user's local desktop just like when using Virtual PC natively.

- ❑ Individual applications that the administrator has published from the virtual machine. Any application window that appears on the virtual desktop is fully integrated into the host desktop; this includes context menus, system tray icons, and system tray notifications. Applications from the system tray of the workspace are displayed as “shadow icons” in the system tray on the host. The way this works is that the virtual machine starts in the background when the MED-V client is launched, and the MED-V client can display applications running in the virtual machine as windows on the local desktop of the host. If the user closes all applications running in his workspace, the state of the virtual machine is saved. To restart the virtual machine, the user clicks the MED-V client icon in the system tray.



Note Any number of Virtual PC images can be installed on a host system. However, only one Virtual PC image can be running on the host at any given time. When starting the MED-V client, the user will be asked which workspace he would like to run if more than one is configured for him.

Using the Workspace

The MED-V workspace and the user’s local desktop are two separate and distinct entities, and by default there is no direct interaction between them. For example, if the user launches a local copy of Microsoft Office Word, creates a document, and tries to save the document, the document is saved by default in the Documents (in Windows Vista) or My Documents (in Windows XP) folder on her local computer. If, however, the user launches a copy of Word from within the workspace, creates a second document, and tries to save the document, this second document is saved by default in the Documents (or My Documents) folder in the user’s workspace—that is, in the virtual machine running in Virtual PC on the user’s computer. This means that by default the user will have two Documents (or My Documents) folders to deal with—the one on the local computer and the one in the user’s workspace.

Although this situation can be confusing to some users, administrators can give users permissions to use the MED-V file transfer tool (accessible from the MED-V tray menu) to copy files or directories between the host and the guest. Alternatively, they can work around this issue by implementing Folder Redirection on the host (the user’s physical computer), the workspace (the user’s virtual computer), or both computers. For example, an administrator could use Group Policy to redirect both Documents (or My Documents) folders—the physical one and the virtual one—to the same shared folder on a network file server.

In fact, because a virtual machine running Windows looks and behaves just like any physical computer running Windows, the full power of Group Policy can be used within an Active Directory Domain Services environment to manage user data and application settings within the workspace. For example, in addition to configuring Folder Redirection for MED-V virtual machines, you can also implement Roaming User Profiles and Offline Files if these are needed. For more information on using these different corporate roaming technologies, see Chapter 7, “User State Virtualization.”

Virtually anything a user can do on his physical host computer, he can also do in his MED-V workspace, provided the guest operating system and applications in the Virtual PC image are installed and configured appropriately. For example, if the virtual image includes third-party VPN client software, the user will be able to launch this software from within his workspace and use it to connect to a remote network to which he is authorized to connect.

It's important to realize, however, that MED-V provides users with two separate computers—their physical host computer and a virtual workspace—and that these two computers are completely separate and do not normally interact with one another. For example, the user cannot use Microsoft Outlook running in the workspace to open a PDF file attachment using Adobe Acrobat Reader running on the local desktop. Instead, the user needs a copy of Adobe Acrobat Reader installed in the virtual machine image. In other words, local applications and virtual applications cannot interact with one another unless they can do so as applications running on separate computers residing on the same network. Simple data exchange between the host and guest is possible, however, using a shared clipboard. The process for doing this is explained in the next section.

Configuring Usage Policies

MED-V usage policies allow administrators to configure the following kinds of behaviors:

- Set expiration dates for the virtual machine and time limits for offline work.
- Control inbound/outbound data transfer control (for example, copy/paste, file transfer, printing) between the virtual machine and the endpoint.
- Enable automatic redirection of predefined Web sites (for example, corporate intranet) from the endpoint browser to the virtual machine.
- Configure published applications. (Applications that are installed in the virtual machine become available through the user's Start menu.)

The MED-V Management Server is used to assign usage policies and data transfer control permissions, which are then enforced by an endpoint agent. The following are additional details concerning two of the policies you can configure.

Configuring Clipboard Behavior MED-V usage policies allow administrators to configure the behavior of the clipboard for copying/pasting between the workspace and the host computer. Options for configuring the sharing of clipboard data between the host and the workspace include

- Disabling shared clipboard functionality entirely
- Enabling one-way copy/paste functionality—for example, from the workspace to the host or from the host to the workspace
- Enabling two-way copy/paste functionality

Configuring Virtual Images to Expire MED-V allows administrators to configure Virtual PC images so that they will expire under certain conditions, including

- If a new connection to the MED-V server is not made within a specified interval of time
- At a date and time you specify

The way MED-V configures the expiration of virtual images is similar to the way App-V configures the expiration of applications. This is a security feature that ensures virtual desktops and applications will not be used outside of the purposes for which they are intended. This capability of configuring the expiration of virtual images is especially important because MED-V enables users to continue to use their virtual desktop and applications even when their computer becomes disconnected from the network—for example, by undocking a laptop computer from its docking station to take the computer home or on the road.

Managing and Maintaining Virtual Images

In MED-V v1, management of a MED-V environment is performed by using the MED-V Management console. Using this console, administrators can manage the inventory and versioning of Virtual PC images, create packages, and perform other related management tasks. In future versions of MED-V, such management functionality might be integrated into the Microsoft System Center family of products.

Virtual images can be retrieved by the MED-V client from the MED-V server using Microsoft Background Intelligent Transfer Service (BITS) version 2, which streams data over HyperText Transfer Protocol (HTTP) or Secure HTTP (HTTPS) sessions. The first time a virtual image is delivered to the host, the entire image must be streamed before the virtual image can start working. After this is done, however, if the image is later updated on the MED-V server, only the deltas between the old and new images must be streamed. This is possible because the MED-V client employs advanced de-duplication techniques to detect blocks in the virtual machine image that already exist on the host, and then it downloads only the missing blocks that might be needed. The result of this implementation is to significantly reduce the time it takes to launch applications that have been updated in virtual images stored in the repository on the server. This implementation also enables MED-V to work well in low-bandwidth scenarios—for example, over a slow WAN link or modem connection—because it significantly reduces the amount of data that needs to be downloaded when an image is distributed or updated over a low-bandwidth connection.

Administrators will need to maintain Virtual PC images stored in the repository on the MED-V server. For standardized virtual images that do not contain any user data, administrators can choose to create a master virtual image and then create a new version of this image in the repository. They can then update the new image by making configuration changes, installing or upgrading applications, applying service packs or software updates, and performing similar maintenance tasks on the image. Then the next time the client tries to run an application using the deployed image, the MED-V client on the user's computer will

download the deltas from the server, thus updating the local copy of the image on the user's computer.

For Virtual PC images that have already been deployed and that contain user data—for example, data stored within user profiles in the guest operating system—administrators can choose to update the deployed virtual image using traditional software maintenance methods. For example, they can deploy or upgrade applications on the guest by using Group Policy Software Installation. And they can ensure the guest is fully up to date with the latest critical security updates by using Group Policy to configure the guest to download software updates from Windows Update or from a server running Windows Server Update Services (WSUS). In this scenario, the virtual machine is being maintained in the same way that a physical system would be maintained using standard tools.

Key Benefits of MED-V

The ability for MED-V to allow you to deploy Virtual PC images onto Windows desktops and to manage them while maintaining a seamless end-user experience can provide businesses with many advantages, including the following:

- **Centralizing desktop management and deployment** MED-V lets you use policies to lock down corporate virtual machines and to easily deploy managed virtualized applications to any desktop computer, including less controlled assets such as employee PCs, contractor PCs, and desktop computers in partner subsidiaries, branch offices, and offshore operations. And because virtual machines deployed using MED-V live locally on the user's computer, users have access to their virtual desktop and applications even when their computers are disconnected from the corporate network. This makes MED-V an ideal solution for enterprises that have a large proportion of mobile users with laptops.
- **Maintaining support for running legacy applications when upgrading desktop operating systems** MED-V allows you to run legacy applications in a virtual machine running an older version of Microsoft Windows, thus accelerating the deployment of the latest version of Windows by resolving application incompatibility issues. MED-V also lets you test your migration plans using virtual machines instead of physical computers, and it reduces user training costs by making virtual desktops invisible and seamlessly integrating legacy applications into the user's local desktop.
- **Driving business continuity** MED-V allows you to rapidly reconstitute corporate-managed virtual desktops on any Windows computer independent of the underlying hardware. MED-V also lets you test and deploy software on different versions of Windows more easily because one failed application or operating system won't affect others.

- **Accelerating application development** MED-V reduces the time and work involved in deploying and reconfiguring applications on users' desktops, and it increases quality assurance by allowing you to test and document application functionality on multiple operating systems using virtual machines.

MED-V Usage Scenarios

Key usage scenarios for MED-V include the following:

- **Resolving application-to-operating system incompatibility, and accelerating the upgrade path to a new operating system** Businesses that need to continue to run legacy line-of-business applications on users' desktop computers can do so by using Virtual PC. Incompatibility between legacy applications and newer versions of Microsoft Windows can often be a primary blocking issue preventing an enterprise from upgrading to the latest version of Windows, such as Windows Vista, to take advantage of the many new features and enhancements offered by this version. By delivering those applications in a Virtual PC that runs a previous version of the operating system (for example, Windows XP or Windows 2000), MED-V allows administrators to break the tight dependency between a computer's underlying hardware and the operating system, and it can help remove such blocking issues so that your users can benefit from having the latest version of Windows deployed on their desktop computers. From the user's perspective, with MED-V, these applications are accessible from the Start menu and appear side by side with regular applications—so there is minimal change to the user experience.
- **Employee-managed desktops and laptops** Users such as teleworkers who use their computers for both personal and work reasons can benefit from being able to run a separate virtual operating system in addition to their standard PC operating system environment. For example, a user might have Windows Vista installed on her home computer or personal laptop (the host) and then run a corporate desktop in a virtual machine (the guest) using Virtual PC—two different operating systems running simultaneously for different purposes on the same physical device. MED-V allows the business to centrally manage and control all those virtual corporate desktops and apply IT and security policies even when the user is operating on a noncorporate device. This can eliminate the historic tradeoff between IT control and user flexibility.
- **Contractors and third parties** MED-V provides a corporate-managed IT environment (including the operating system and applications) on top of a host managed by a third party (that is, not by the user or by corporate IT). The deployment package (including virtualization software and the Virtual PC image) can be delivered via a DVD, via a USB, or over the Web. This increases usability and manageability of computers used

by contractors onsite or offshore, and it also simplifies the incorporation of different IT environments (for example, new branch offices or a new subsidiary from a merger or acquisition).

- **Business continuity** MED-V allows IT to rapidly reconstitute corporate-managed virtual desktops on any Windows desktop, independent of hardware or operating system configurations. This enables cost-effective desktop disaster recovery plans for any contingency that prevents employees from coming to the office, with no dependency on servers and no ongoing maintenance of recovery centers.
- **Work at home and portable corporate computing** MED-V allows users to gain full mobility with their corporate desktop environment. Virtual PCs can be carried anywhere on USB drives and used on any host (including home computers), while corporate control and manageability are maintained and all policies that normally apply to corporate desktops are enforced. The Virtual PC operates directly from the USB drive, and all user data and settings roam with the USB drive. MED-V thus enables flexible corporate computing by increasing the manageability and flexibility of enterprise client computing through delivering a corporate-managed Virtual PC on unmanaged devices.

MED-V Availability

At the time of this writing, MED-V v1 product availability is tentatively scheduled for the first quarter of 2009. MED-V will be made available to enterprises as part of the Microsoft Desktop Optimization Pack for Software Assurance, which currently includes the following five other key technologies that help enterprises manage their desktops more easily:

- Microsoft Application Virtualization
- Microsoft Asset Inventory Service
- Microsoft Advanced Group Policy Management
- Microsoft Diagnostics and Recovery Toolset
- Microsoft System Center Desktop Error Monitoring

For more information about the Microsoft Desktop Optimization Pack (MDOP), see Windows Vista For The Enterprise at <http://www.microsoft.com/windows/products/windowsvista/enterprise/features/tools.aspx>.

For more information about Microsoft's Software Assurance (SA) licensing program, see <http://www.microsoft.com/licensing/sa/default.aspx>.

Understanding Microsoft Virtual Desktop Infrastructure

Microsoft Virtual Desktop Infrastructure (VDI) is an emerging architectural model for desktop virtualization that allows client operating systems to run in server-based virtual machines. Microsoft VDI is designed to be a complete, end-to-end Microsoft desktop virtualization solution that can provide users with a rich, individualized desktop experience on both standard desktop PCs and thin clients while centralizing the storage, execution, and management of Windows desktops in the datacenter.

Microsoft VDI is not a product but an infrastructure design that employs virtualization technologies to provide a full desktop computing experience to users at lower costs than a traditional PC environment. Microsoft VDI reduces deployment, management, and support costs; facilitates key worker scenarios; and improves corporate governance.

One way to better understand Microsoft VDI is by comparing it with MED-V, which is described earlier in this chapter. With MED-V, the virtual machines “live” on the user’s desktop computers, running locally in the background using Virtual PC. This setup allows users to access their virtual desktop, applications, and data even when their computers are disconnected from the corporate network, which makes MED-V an ideal solution for enterprises that have mobile users who use laptop computers. MED-V also helps resolve application compatibility issues by providing users with multiple desktops running different versions of Microsoft Windows to ensure the availability of legacy applications that cannot run on the latest version of Windows.

With Microsoft VDI, on the other hand, the virtual machines “live” on servers running Windows Server 2008 with Hyper-V. This means that users’ desktops, applications, and data reside in the datacenter, where they can be managed more easily and deployed to a wide variety of clients ranging from rich clients (standard desktop PCs) to thin clients such as diskless workstations. VDI is therefore an ideal solution for businesses that need to provide desktop computing resources to contract or offshore workers, in work-from-home scenarios, and in industry sectors that require use of centrally located and managed desktops for regulatory or compliance reasons.

How Microsoft VDI Works

Because Microsoft VDI runs virtual machines on servers, it requires more infrastructure to deploy than other desktop virtualization solutions. Specifically, a typical implementation of Microsoft VDI (as illustrated in Figure 6-2) has the following five components:

- **Windows Server 2008 with Hyper-V** Microsoft Hyper-V is Microsoft’s hypervisor-based technology included as a key feature of 64-bit editions of Windows Server 2008. Hyper-V provides a scalable, reliable, and highly available server virtualization platform and is used by Microsoft VDI to virtualize the desktop infrastructure

needed by an enterprise. For more information about Hyper-V, see Chapter 2, “Server Virtualization—Hyper-V.”

- **System Center Virtual Machine Manager (VMM) 2008** VMM 2008 is a server application in the Microsoft System Center family of products that provides centralized administration of a virtual machine infrastructure, enables increased physical server utilization, and facilitates rapid provisioning of new virtual machines. For more information about VMM 2008, see Chapter 3, “Managing Virtualization—VMM 2008.”
- **Windows Vista Enterprise Centralized Desktop (VECD)** VECD is a flexible, subscription-based licensing option for enterprises that want to deploy Windows Vista in virtual machines running on servers, allowing you to centralize storage and execution of Windows in a datacenter. VECD allows unlimited installs of Windows Vista Enterprise on the server, is licensed by access device (PC or thin client), allows up to four running virtual instances per access device for a user at a given time, and can support running on both static and dynamic hosted desktop architectures. For more information about VECD, see <http://www.microsoft.com/windows/products/windowsvista/enterprise/benefits/licensing.mspx>.



Note VECD is a license for a Windows client to run on any type of VDI deployment, so it also applies to a VMware ESX Server or Citrix XenServer deployment of VDI as well as the Microsoft VDI offering.

- **Citrix XenDesktop, a session/connection broker partner solution** Citrix XenDesktop works together with Microsoft Hyper-V to dynamically assemble and deliver centrally running virtual Windows desktops on demand to users anytime and anywhere, as needed. The key component of Citrix XenDesktop for Microsoft VDI is the Citrix Desktop Delivery Controller, which manages connections between a user's client device and virtual desktop. By using Citrix XenDesktop together with Microsoft Hyper-V and VMM 2008 as part of a Microsoft VDI infrastructure, you can easily create pools of virtual desktops and virtual machines, provision virtual desktops to each virtual machine, stage these virtual machines for delivery to users, and broker sessions between client devices and virtual machines running on Hyper-V servers. These virtual machines can be managed by policies and are always on and are available to users immediately after logon. For more information about Citrix XenDesktop, see <http://www.citrix.com/English/ps2/products/product.asp?contentID=163057>.
- **Client devices** Microsoft VDI can dynamically provision server-running virtual desktops to a wide variety of clients, ranging from standard desktop PCs running Windows Vista or Windows XP to thin client computing devices running Windows XP Embedded, Windows CE, or some other operating system.

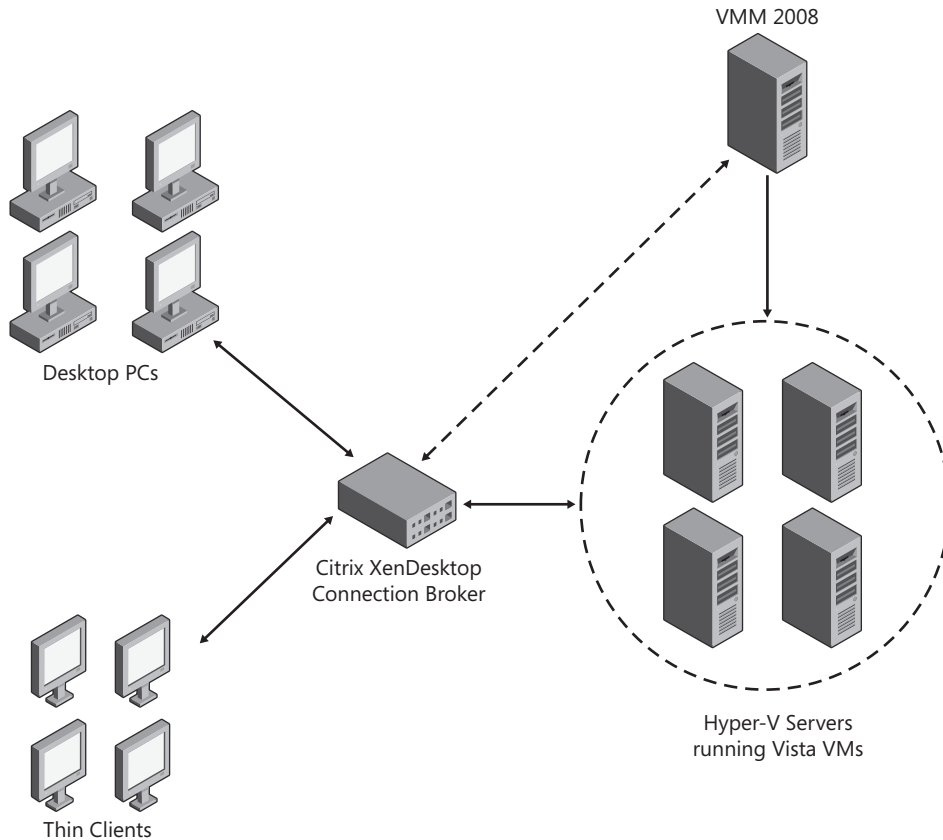


FIGURE 6-2 A typical Microsoft VDI infrastructure.

In addition to the technologies just mentioned, Microsoft VDI can also be integrated with other Microsoft virtualization solutions, such as Microsoft Application Virtualization (App-V) and Terminal Services RemoteApp, to provide an integrated enterprise dynamic desktop solution that can satisfy the full range of Windows optimized desktop scenarios, including mobile workers, task workers, office workers, contract/offshore workers, and workers requiring anywhere access on noncompany PCs. For more information on using Microsoft VDI together with App-V, see the section titled “Dynamic Architecture” later in this chapter.

Implementing Microsoft VDI

As indicated in the preceding section, Microsoft VDI is a flexible desktop virtualization solution that can be implemented in different ways, depending on the needs of your business. The two basic core architectures of Microsoft VDI are the static and dynamic architecture options. (See Figure 6-3.)

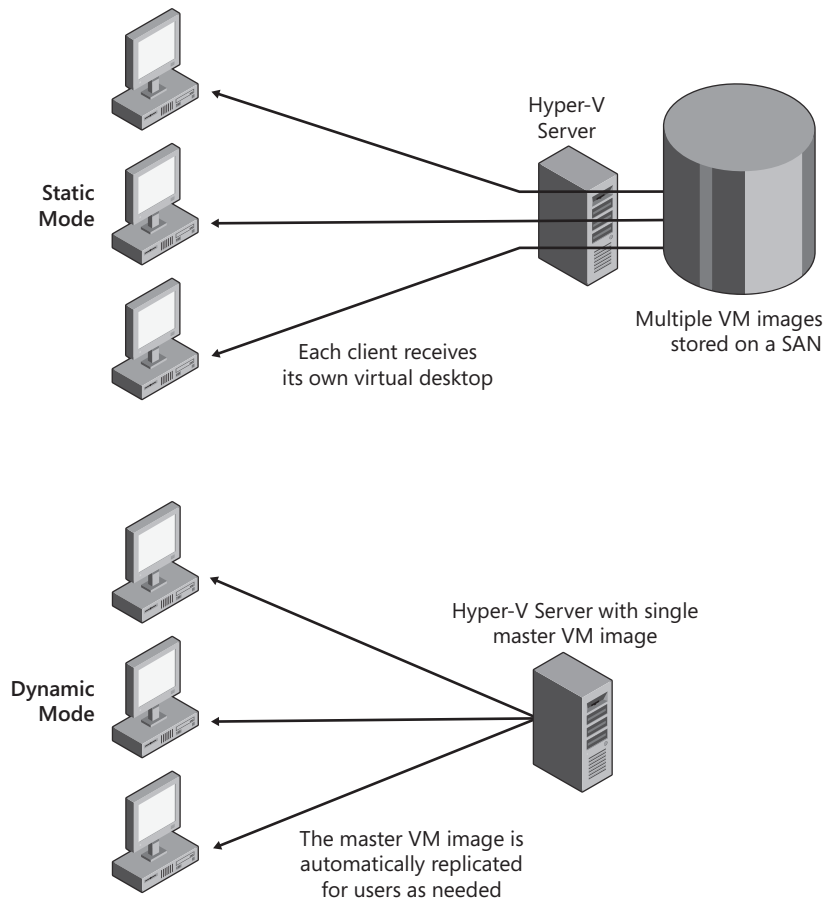


FIGURE 6-3 Core architectures for implementing Microsoft VDI.

Static Architecture

In the static (or persistent) architecture option, a one-to-one mapping exists between users and virtual machines. Each user has his own virtual machine, so the more users you have, the more virtual machines you need to create and manage. The virtual machines are stored on a storage area network (SAN) or on network-attached storage (NAS) and run on Hyper-V servers in the datacenter. Virtual desktops are presented via Microsoft VDI to either standard desktop PCs or thin clients as needed.

Dynamic Architecture

In the dynamic (or nonpersistent) architecture option, one master virtual machine image resides on the Hyper-V server, and Microsoft VDI automatically replicates this image as needed for users. Applications for users are provisioned onto the virtual machine using App-V based

on user profiles, and user data is stored centrally on the server via Folder Redirection. Having only a single virtual machine image to maintain reduces management overhead and support costs, and enables dynamic provisioning of desktop environments on demand.



Note Microsoft recommends using the dynamic architecture when implementing a VDI solution for your organization.

Managing Microsoft VDI

Figure 6-4 shows an example of the Microsoft Hyper-V Manager console managing a Microsoft VDI infrastructure. A primary component of Microsoft VDI is Windows Server 2008 with Hyper-V, and virtual machines running on Hyper-V servers can be managed using the Hyper-V Manager. Virtual machine settings, the creation of new virtual machines, and connecting directly to a virtual machine are all managed here. In this figure, there are three virtual machines that are all pieces of a Microsoft VDI infrastructure: a domain controller (vecd. demo), a Microsoft App-V server (AppV) and a Citrix XenDesktop Desktop Delivery Controller (DDC).

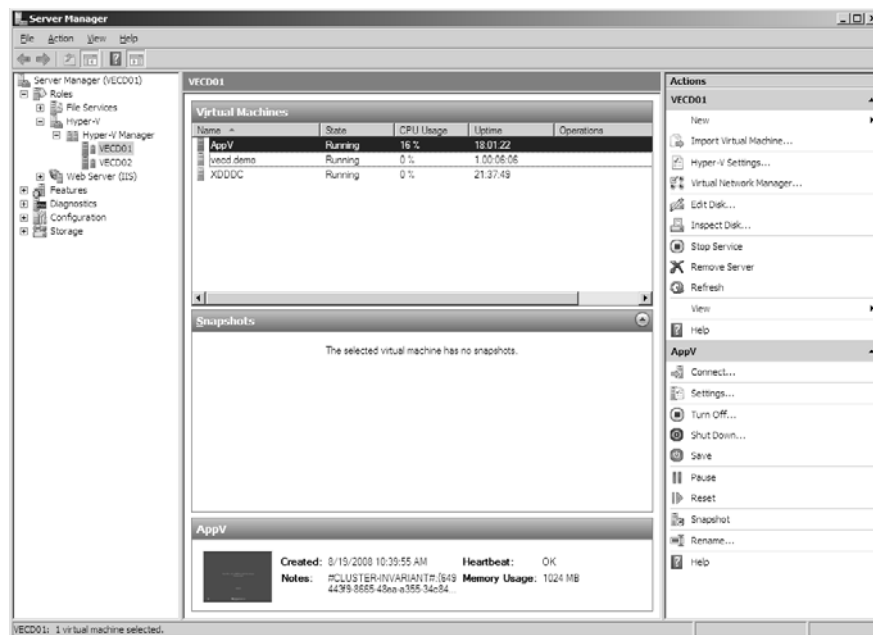


FIGURE 6-4 Hyper-V Manager managing three components of a Microsoft VDI infrastructure.

Figure 6-5 shows the System Center Virtual Machine Manager (VMM) 2008 Administration console managing the Microsoft VDI infrastructure. Using VMM, you can manage all of your company's virtual machines on all of your Hyper-V servers. For example, by managing the host servers, shown as VECD01 and VECD02 in this figure and the previous one, VMM can monitor the settings, jobs, and performance of all virtual machines running on their individual hosts. This figure shows two hosts and their corresponding virtual machines.

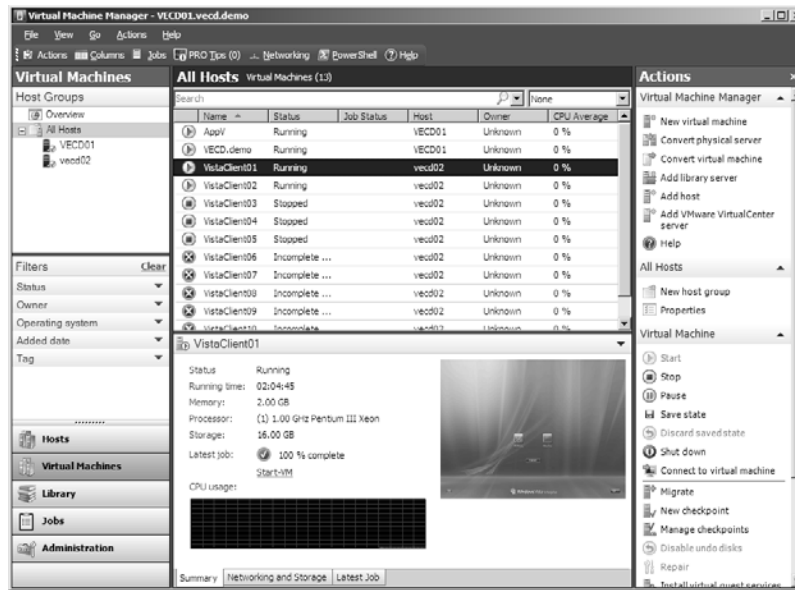


FIGURE 6-5 The VMM Administration console managing two hosts and their virtual machines.

Figure 6-6 shows an example of a Microsoft VDI logon scenario. In this figure, a user named Abby is logging on to her virtual machine via Internet Explorer. By typing the URL of the DDC, she gets a logon screen to access her virtual machine.

With Microsoft VDI, after a user logs on, she is automatically assigned a virtual machine based on her Active Directory profile. All her files and user settings are applied to whatever virtual machine she logs on to. Applications can be run virtually as well by using Microsoft Application Virtualization, as seen in the bottom right of Figure 6-7.

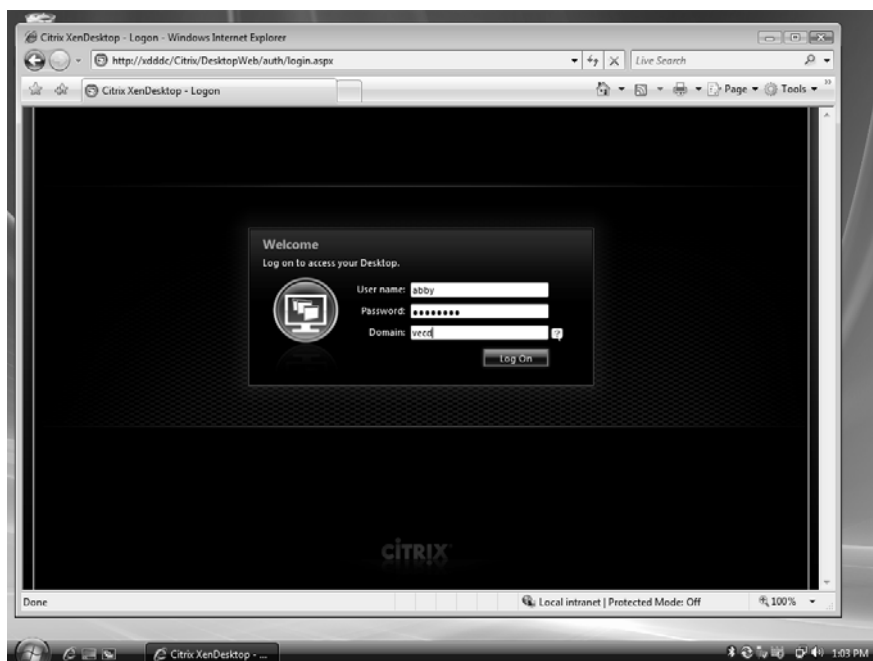


FIGURE 6-6 A user logging on to a virtual machine provisioned to her via Microsoft VDI.



FIGURE 6-7 A logged-on user accessing her applications via Microsoft VDI.

Key Benefits of Microsoft VDI

When it is released, Microsoft VDI will provide enterprises with the following benefits:

- Enterprises will see better enablement of flexible work scenarios, such as hot-desking and working from home. These scenarios can help businesses reduce the total cost of ownership (TCO) of deploying desktops and applications for users.
- Businesses will be able to enhance security and compliance. By storing user desktops and data on a SAN or NAS located in the datacenter, data security is enhanced and compliance with industry regulations is made simpler.
- Administrators will be able to manage desktop operating systems and applications more easily and efficiently. By running virtual machines on Hyper-V servers located in the datacenter, administrators have more control over these assets and can deploy and maintain them more easily.

Microsoft VDI Usage Scenarios

The key usage scenarios for Microsoft VDI are as follows:

- **Contract or offshore worker** The benefits of having a centrally hosted image, added security, and being able to facilitate compliance all make Microsoft VDI ideal for businesses that frequently use contract workers or offshore contractors.
- **Power users** The benefits of a centralized desktop environment that is flexible and easy to manage make Microsoft VDI together with App-V or TS RemoteApp an ideal solution for enterprises that require the full client desktop experience.
- **Working from home** Implementing Microsoft VDI together with Terminal Services Gateway will enable users to securely access corporate applications and user data from anywhere, anytime.

Microsoft VDI Availability

At the time of this writing, availability of Microsoft VDI is tentatively scheduled for late 2009. More information on Microsoft VDI will be published at <http://www.microsoft.com/vdi> as soon as it becomes available.

Direct from the Source: Reducing the Cost of Deploying Microsoft VDI

Although there is no doubt that VDI deployment provides flexibility and a richer user experience to centralized desktop deployment, the jury is still out on the TCO of VDI. The main concern is the cost of acquiring hardware. Here are a couple tips to reduce the cost:

Dynamic Deployment Where the Data and Application Are Removed from the Operating System Image

In a traditional desktop deployment model, each user gets a PC and the user data, applications, operating system, and preferences make up the unique identity of that desktop for the user. If corporations try to deploy VDI in a similar fashion, they end up centralizing all their desktops in the data center, but they have to store, deploy and manage an equal number of desktop VMs as the number of desktop computers. For example, if the corporation used to have 1000 PCs, now they have 1000 desktop VMs, and obviously that will require a lot of server memory and storage space.

The best way to reduce the number of VMs on a server is to remove the data and application from the VM image itself. This configuration is typically referred to as a *dynamic* or *pooled* VDI deployment architecture. IT can use the folder redirection and roaming profile capabilities in Windows Vista or Windows XP to centralize the user data and user preferences or settings outside each VM. At the same time, IT can also use application virtualization technology, such as Microsoft Application Virtualization or the Windows Server Terminal Services RemoteApp capability, to remove the footprint of the applications from the image as well. When a user log in, her user data, preferences, and applications will be deployed to a virtual desktop image based on her access specified in Active Directory and Group Policy. With a dynamic-deployment architecture, IT can reduce the storage and memory use requirements for each VM, and they can reduce the number of VM images required for different types of users.

Desktop Refresh Cycle Rate Follows the Storage

In a VDI dynamic-deployment model, storage becomes the most critical component. That includes determining where all data will be stored and whether redundancy, high availability, reliability, and performance will be required. Because the main resource bottleneck for VDI execution on a server is the server memory, the most cost-optimized option is to purchase a commodity enterprise server with as many memory slots as possible so that each memory slot can be filled with commodity memory sticks to maximize the VM density (for example, for less than \$10,000, you can have an HP Proliant DL580 G5 DP Quad core server with 32 GB of memory).

—Fei Lu, Sr. Product Manager, Desktop Virtualization, Windows Business Group

Additional Resources

The resources listed in this section were either referred to in the chapter or provide additional information concerning concepts and products discussed in this chapter.

General

For general information concerning Microsoft desktop virtualization technologies and solutions, see <http://www.microsoft.com/virtualization/solution-tech-desktop.mspx>.

Microsoft Virtual PC 2007

To learn more about Microsoft Virtual PC 2007 and to download a copy, visit the Microsoft Virtual PC 2007 product page at <http://www.microsoft.com/windows/products/winfamily/virtualpc/default.mspx>.

You can also find a wealth of tips and tricks for using Virtual PC on the blog of Ben Armstrong, the "Virtual PC Guy," which is found at http://blogs.msdn.com/virtual_pc_guy/default.aspx.

Microsoft Optimized Desktop Pack

For more information about the Microsoft Desktop Optimization Pack (MDOP), see Windows Vista For The Enterprise at <http://www.microsoft.com/windows/products/windowsvista/enterprise/features/tools.mspx>.

Software Assurance

For more information about Microsoft's Software Assurance (SA) licensing program, see <http://www.microsoft.com/licensing/sa/default.mspx>.

Windows Vista Enterprise Edition

To learn more about Windows Vista Enterprise edition, a premium edition of Windows Vista designed for businesses and available exclusively to Microsoft Software Assurance customers, see <http://www.microsoft.com/licensing/sa/benefits/vista.mspx>.

Windows Vista Enterprise Centralized Desktop

To learn more about Windows Vista Enterprise Centralized Desktop (VECD), a unique licensing option for running Windows Vista in virtual machine on servers, see <http://www.microsoft.com/windows/products/windowsvista/enterprise/benefits/licensing.msp>.

Microsoft Enterprise Desktop Virtualization

For information about Microsoft's acquisition of Kidaro, a leading provider of desktop virtualization solutions for businesses, see the news release at <http://www.microsoft.com/presspass/press/2008/mar08/03-12ExpandVirtualizationPR.msp>. Microsoft currently plans on rebranding Kidaro's technology as MED-V and rolling it into the Microsoft Desktop Optimization Pack for Software Assurance.

Microsoft Virtual Desktop Infrastructure

Information concerning Microsoft VDI will be published at <http://www.microsoft.com/vdi> as soon as it becomes available.

Chapter 7

User State Virtualization

The final part of Microsoft's integrated Virtualization 360 strategy is user state virtualization, which is based on three core technologies available in Windows Server 2008. These three technologies are Roaming User Profiles, Folder Redirection, and Offline Files. This chapter explains how these three technologies can be used together with Group Policy to implement an efficient and reliable user state virtualization solution for your enterprise.

Understanding User State Virtualization

As mentioned in Chapter 1, "Microsoft's Virtualization Solution," user state virtualization involves separating user profiles with their data and application settings from the users' computers. What does this mean, however, and why is this form of virtualization useful to enterprises?

Understanding User Profiles

On Microsoft Windows platforms, user data and application settings are stored within a structure called a user profile. A *user profile* consists of a directory structure plus a registry hive, which together define and describe the configurable environment of the user. This environment includes the following:

- The appearance and behavior of the user's desktop
- Settings for applications that have been configured by the user
- Documents, pictures, music, and other data files belonging to the user
- The user's favorites in Microsoft Internet Explorer
- Any other user-specific application settings and data

Each user who logs on to a Windows computer using her own user account can configure her desktop, create and save documents, and perform other user-specific actions. The results of these actions are then saved in the user's profile when the user logs off from the computer. For example, user Karen Berg might configure Microsoft Office Word 2007 to use landscape orientation as the default page layout instead of portrait. When Karen logs off from the computer, this application setting is saved in her user profile on the computer. The next time Karen logs on and starts Word 2007, the page layout is landscape. Karen's user profile thus allows her application settings to be preserved across logon sessions. In addition, any documents Karen creates using Word 2007 are saved by default within her Documents folder, one

of the subfolders within the folder structure of her user profile. The next time Karen logs on to the computer, her documents are readily available within her Documents folder so that she can begin working on them again.

What if another user decides to use the same computer that Karen has been using? In that case, a user profile is created for the other user as well and stored on the computer. User profiles thus allow multiple users to share a single computer and maintain their own unique desktop appearance, application settings, and data files. In addition, each folder is marked so that only the owner can view those files by default.

Where User Profiles Are Found

On computers running Windows Vista or Windows Server 2008, user profiles are stored under the Users folder on the %SystemDrive% volume. Figure 7-1 shows the user profiles of Karen Berg (FABRIKAM\kberg) and Tony Allen (FABRIKAM\tallen), two users who share a common computer running Windows Vista. There is also a user profile named Public, which is explained in the sidebar titled “Direct from the Source: Understanding the Public Folder” in this chapter.

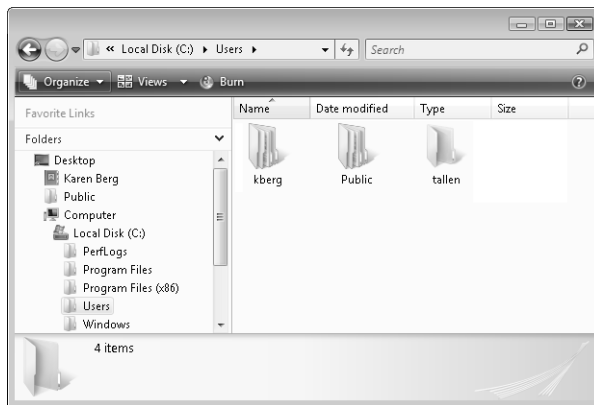


FIGURE 7-1 The user profiles for Karen Berg and Tony Allen are found under the C:\Users folder.

Figure 7-1 illustrates that each user’s profile folder is named after the logon user name of the user. The profile folder for Karen Berg is thus named kberg. When Karen logs off from her computer, her user profile unloads and is saved to the C:\Users\kberg folder on the computer. The next time Karen logs on to the computer, her profile is loaded from what was previously saved in the C:\Users\kberg folder, restoring her desktop and application settings and providing her with access to her documents and other files. Strictly speaking, the profile folders found under C:\Users are known as *local user profiles* because they are stored on the local computer. This is to distinguish them from roaming user profiles, which are stored elsewhere on the network, as described in the section titled “Understanding Roaming User Profiles” later in this chapter.

Direct from the Source: Understanding the Public Folder

The All Users profile in Windows XP has been renamed as the Public profile in Windows Vista to highlight that anything within this profile is publicly accessible to all users on the computer. The structure of the profile under the Public folder is similar to other user profiles.

It is important to note that as in Windows XP, the Public profile in Windows Vista does not have a per-user registry hive because it is a profile that is never loaded. All shared user settings are still written to HKEY_LOCAL_MACHINE as was done in Windows XP.

The Windows Explorer desktop shell continues to do its magic of aggregating certain Public profile folders, such as Desktop and Start Menu, with a regular user's profile folders at logon to provide them with one unified view for these folders. For example, any icon added to the desktop folder of the Public profile will be visible when any user logs on to that computer.

—CSS Global Technical Readiness (GTR) team

Structure of a User Profile

At first glance, the structure of a user profile looks quite simple and consists of a number of subfolders named Documents, Favorites, Searches, and so on. (See Figure 7-2.) As you might suppose, the Documents subfolder is the default location where applications such as Word or Excel save the user's work. Similarly, the Favorites subfolder is where Microsoft Internet Explorer keeps the user's favorites.

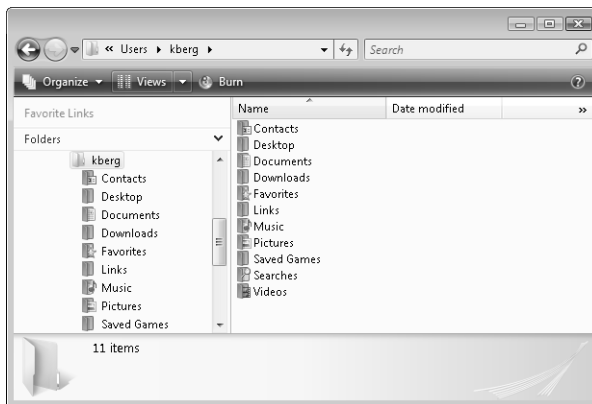


FIGURE 7-2 Simplified structure of a user profile.

If you make hidden files visible in Windows Explorer, an additional subfolder named AppData is displayed. This folder is where applications such as Word and Excel save settings for any

configuration changes made by the user to these programs. As you can see from Figure 7-3, the structure of this folder can be quite complex, depending on which applications and Windows features are installed on your computer. Note that these are file-based configurations as opposed to registry-based settings, which are stored in the profile file named *Ntuser.dat* as discussed next.

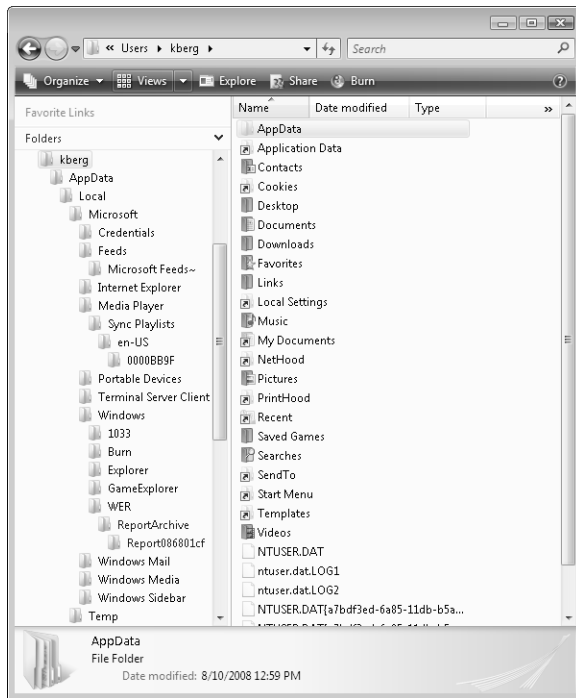


FIGURE 7-3 Directory structure under the *AppData* subfolder.

Making protected operating system files visible in Windows Explorer shows additional detail concerning the files and subfolders beneath a user's profile folder. In addition to subfolders such as *Documents* and *AppData* described earlier, the detailed view shown in Figure 7-4 displays the complete file and folder structure of a user's profile and includes directory junctions (shown as shortcut icons) and the registry hive *Ntuser.dat*, which contains all data under the *HKEY_CURRENT_USER* key of the registry. The user's profile hive maintains numerous environment preferences for the user, including Control Panel configurations, network connections, and settings for applications that use the registry.

For additional details concerning user profiles and how Windows Vista profiles differ from those used by Windows XP, see the sidebar titled "Direct from the Source: Inside Windows Vista's User Profile Structure" in this chapter.

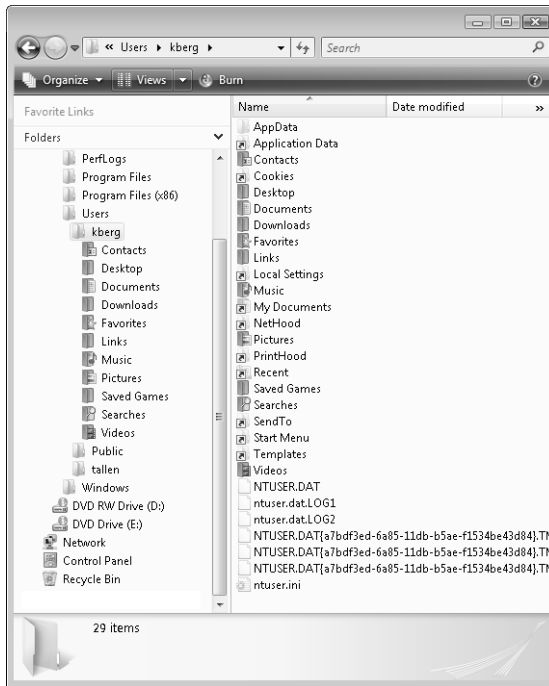


FIGURE 7-4 Full details of a user's profile folder.

Direct from the Source: Inside Windows Vista's User Profile Structure

The Windows XP profile namespace can be confusing for the end user because it is a mixture of application and user data folders at the root and provides no clean separation of user data from application data. Some of the problems with the way profiles are constructed in Windows XP include

- My Pictures, My Videos, and My Music folders are subfolders of My Documents, although they do not belong to the documents category. This structure makes little or no sense to the end user and presents a very unintuitive profile layout.
- The root of a user's profile in Windows XP is a mixture of both user and application data, and there is no clean separation of user data from application state data. For example, the Printhood and Nethood folders are peers of the My Documents folder.

- With Windows XP, there were no guidelines on how applications should store per-user data inside a user's profile. As a result, application writers often create new folders at the root of the profile instead of in the appropriate application data folders. Also, no guidelines existed on how to structure their folders within the application data folders.
- The profile layout as it existed in Windows XP had no easy way of allowing users to share their data with other users or a specific set of users, especially over the network.

Thus, in Windows XP, the profile namespace was a mixture of user and application data folders, causing the profile to look polluted. In the folder hierarchy, it does not make much sense for the My Pictures My Videos, and My Music folders to be subfolders of My Documents because they are media type folders and not really document type folders.

One of the key goals of Windows Vista was to flatten out the user data folders inside the profile for clarity and to provide a clean separation of user-managed data from application data. This has resulted in the birth of a new folder, AppData, under the profile root. The AppData folder allows such separation, and it is where all per-user application binaries/settings are stored. Also, part of the namespace cleanup is the removal of the "My" prefix for folders such as My Documents, which is now called Documents.

New Profile Namespace Details

Table 7-1 relates the Windows Vista profile folder names to the corresponding profile folder names Windows XP.

TABLE 7-1 Windows Vista vs. Windows XP Profile Folder Names

Folder Name in Windows Vista	Description	Name Change from Windows XP	Former Windows XP Location
Contacts	Default location for user's contacts	Does not exist	Does not exist
Desktop	Desktop items, including files and shortcuts	No change	%SystemDrive%\Documents and Settings\%username%\Desktop
Documents	Default location for all documents the user creates	My Documents	%SystemDrive%\Documents and Settings\%username%\My Documents
Downloads	Default location to save all downloaded content (for example, by Internet Explorer)	Does not exist	Does not exist

Folder Name in Windows Vista	Description	Name Change from Windows XP	Former Windows XP Location
Favorites	Internet Explorer favorites	No change	%SystemDrive%\Documents and Settings\%username%\Favorites
Music	Default location for user's music files	My Music	%SystemDrive%\Documents and Settings\%username%\My Documents\My Music
Videos	Default location for user's video files	My Videos	%SystemDrive%\Documents and Settings\%username%\My Documents\My Videos
Pictures	Default location for user's pictures	My Pictures	%SystemDrive%\Documents and Settings\%username%\My Documents\My Pictures
Saved Searches	Default location for Saved Searches	Does not exist	Does not exist
AppData	Default location for per-user application data and binaries. This is a hidden folder.	Does not exist	Does not exist
Links	Windows Explorer Favorite links folder	Does not exist	Does not exist
Saved Games	Default location for saved Games	Does not exist	Does not exist

AppData Folder

As described in the preceding text, in Windows Vista, the profile folder hierarchy has changed to provide clean separation of state through the new AppData folder. Note that this new folder is hidden by default at the root of the user's profile.

To get good state separation, however, it is critical to separate what portion of an application's state is computer dependent and what portion can actually roam with the user. Thus, the AppData folder in Windows Vista has the following hierarchy beneath it (as shown in Figure 7-5):

- **Local folder** This folder is for application data and settings that are computer-dependent and cannot roam with the user. The AppData\Local folder in Windows Vista is the same as the %SystemDrive%\Documents and Settings\%username%\Local Settings\Application Data folder in Windows XP.

- **LocalLow folder** This folder in the user's profile area allows low-integrity processes to have write access to it. Every process has an integrity level associated with it, and Windows Vista protects processes by marking them with integrity levels, which are essentially measurements of trust. A high integrity application is one that can perform tasks that modify system data. An example of this might be a disk partitioning application. By contrast, a low integrity application is one that can perform tasks that might potentially compromise the system. An example of this might be a Web browser. Windows Vista prevents applications that have lower integrity levels from modifying data used by applications that have higher integrity levels. Most processes run under the medium integrity level.
- **Roaming folder** This folder is for application data and settings that are not computer dependent and can therefore roam with the user. The AppData\Roaming folder in Windows Vista is the same as the %SystemDrive%\Documents and Settings\%username%\Application Data folder in Windows XP.

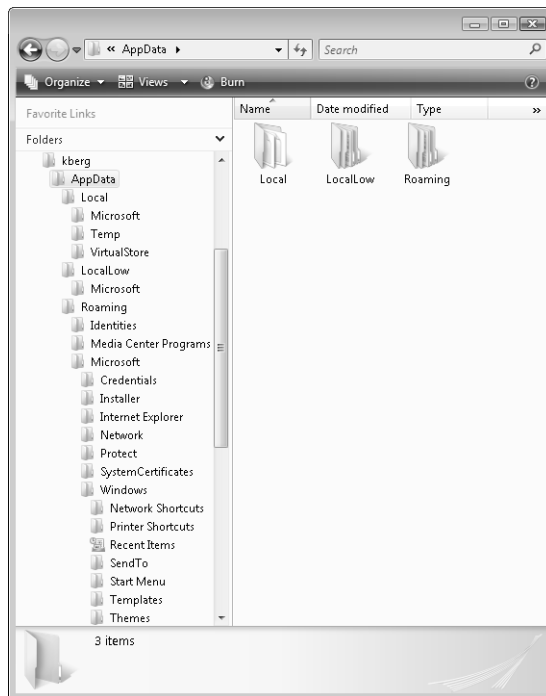


FIGURE 7-5 The Local, LocalLow, and Roaming subfolders beneath the AppData folder.



Tip The integrity level of an application can be viewed by using Process Explorer, one of the Windows Sysinternals tools, which you can get at <http://www.microsoft.com/sysinternals>.

Table 7-2 summarizes the differences between where Windows Vista and Windows XP store application data and settings that can or cannot be roamed.

TABLE 7-2 AppData—Windows Vista vs. Windows XP

Vista Folder Name	Description	Name Change from Windows XP	Former Windows XP Location
AppData	Used to separate per-user application data from user data. Has three subfolders underneath for further state separation.	—	Did not exist
Local	Application settings and data that do not roam with the profile. Usually either computer specific, or too large to roam effectively.	Local Settings\ Application Data	%SystemDrive%\ Documents and Settings\%username%\ Local Settings\ Application Data
LocalLow	Used for applications running with low rights—for example, applications started by protected mode Windows Internet Explorer	—	Did not exist
Roaming	Application-specific data, such as a custom dictionary, which is computer independent and should roam with a user's profile.	Application data	%SystemDrive%\ Documents and Settings\%username%\ Application Data

—CSS Global Technical Readiness (GTR) team

Limitations of Local User Profiles

Although local user profiles (user profile folders located on the user's local computer) have many advantages, they also have some important limitations. First, in many enterprise environments, users might use a different computer from day to day. This means that if a user customizes his desktop and creates and saves some documents on one computer on Monday and then logs on to a different computer on Tuesday, his desktop and documents won't travel with him—they still reside on the computer he used the day before. The result is that each time the user logs on to a different computer, he has to reconfigure his desktop and applications, and copy his documents from another location. From the user's perspective, this is quite frustrating; from a management perspective, worker productivity is diminished and costs can increase if the user calls the help desk in an attempt to find his data files.

Using local user profiles in a multi-use computing environment like this means that the user's application settings and data have been separated from the user, and some form of virtualization is needed to overcome this problem. As you will see in a moment, the solution is to use Roaming User Profiles and Folder Redirection, which combine to virtualize the user's profile.

Another type of limitation occurs when a company policy dictates that users not be allowed to customize their desktops or applications. For instance, an organization might require that each user's desktop display the company logo and therefore that users not be allowed to customize their desktop backgrounds. Although Group Policy can be used to lock down many aspects of a user's desktop and installed Windows applications, this is not enough when an organization's policy dictates that no changes should be allowed to a user's profile. A similar situation occurs when a company provides only a single user account for temporary workers. In this situation, it makes sense to configure this profile so that any customizations the user makes during his logon session are not saved when he logs off from the computer. In both these scenarios, the solution is to use a special type of roaming user profile known as a mandatory user profile, which is described later in this chapter in a sidebar titled "Direct from the Source: Mandatory and Super-Mandatory User Profiles."

Finally, although Roaming User Profiles solves the basic problem of virtualizing (separating) a user's profile from the computer he is using, this technology has two limitations of its own. First, if a user saves hundreds of documents within the Documents subfolder of his profile, the size of the user's profile can grow quite large. This can lead to long delays during logon and logoff as the user waits for his profile to load or unload. And second, if the user's computer becomes disconnected from the network, the user can become separated in a bad sense from his profile—that is, the user will still have his profile saved locally (as long as the "Delete Cached Copies Of Roaming Profiles" Group Policy setting isn't enabled), but he won't be able to save any new files to his roaming profile until network access is restored, plus any changes he makes to his profile won't be saved. These two issues are solved by combining Roaming User Profiles with two additional virtualization technologies: Folder Redirection and Offline Files.

The Solution: User State Virtualization

The solution to the limitations of having user profiles stored locally on each user's computer is thus to virtualize the user's profile, and that's the essence of user state virtualization on Windows platforms. In other words, user state virtualization separates the logical (the user's application settings and data) from the physical (where these settings and data are stored) so that instead of having the user's application settings and data stored on the user's local computer, they can be stored elsewhere—typically, on a centrally located file server on the network. And Roaming User Profiles, a feature of Windows since Windows NT, makes this possible. Folder Redirection, a feature first introduced in Windows 2000, enhances the

experience of implementing Roaming User Profiles on your network. And Offline Files, also introduced in Windows 2000, takes this one step further by providing users with full access to data stored in their user profiles even when their computers are disconnected from the corporate network.

All three of these well-known technologies—Roaming User Profiles, Folder Redirection, and Offline Files—have been enhanced and improved in Windows Vista, and they represent the core technologies behind Microsoft's implementation of user state virtualization. The sections that follow examine each of these three technologies in turn.

Understanding Roaming User Profiles

Roaming User Profiles (RUP) allows administrators to configure users' profiles so that instead of the profiles being stored on each user's local computer, they are stored on a central file server located on the corporate network. The structure of a roaming user profile is the same as that of the local user profile shown in Figure 7-4 earlier; only the location of the profile folder is different.

How RUP Works

By having profiles stored in a central location on the network, users can access their desktop, application settings, and data from any computer they have access to. What happens when RUP is configured is that when the user logs on to a computer, the user's roaming profile is copied from the file server and loaded on the computer. During the user's logon session, she might customize her desktop, configure available applications, and create and save documents in her Documents folder. Then when the user logs off from the computer, the modified profile is unloaded and copied back to the file server, replacing the previous copy of the profile on the server. If the user then logs on to a different computer, the user's modified profile is copied from the server and loaded, displaying the customizations and data saved during the previous session.

When a user logs on to a Windows computer for the first time, a profile needs to be created for the user. On a standalone computer, a local user profile is created from the default user profile. In Windows Vista, this default user profile is implemented as a folder named Default and is located at C:\Users\Default. By contrast, in Windows XP the default user profile was implemented as C:\Documents and Settings\Default Users.

If the computer is joined to a domain, however, Windows first checks to see whether there is a default network user profile. In Windows XP, this profile (if it existed) was named Default User and was located in the Netlogon share on domain controllers. In Windows Vista, however, the default network user profile must be named Default User.v2. The reason for this is

because Windows Vista cannot read a default network profile created from an earlier version of Windows.

Default network user profiles are optional—you don't need to create them if you don't want to. However, it makes sense to create a default network folder if you plan on implementing RUP in a domain-based environment. The reason for this is because it allows you to preconfigure the default network user profile so that the first time users log on to their computers, this preconfigured default network user profile will be downloaded to the user's computer and loaded as the user's profile.

Implementing RUP

Implementing RUP basically involves four steps:

1. Creating and configuring a default network profile that will be used as the basis for generating roaming user profiles for your users
2. Preparing a central location for storing roaming user profiles on your network
3. Configuring your user accounts to use roaming profiles
4. Testing to verify that RUP works as expected

Step 1: Create a Default Network User Profile

To see how this works in detail, you can log on to a Windows Vista computer as user Tony Allen in the fabrikam.com domain and configure Tony's desktop by choosing a different background, creating shortcuts on the desktop and Start menu, and so on. After you've configured Tony's profile as desired, you then use this profile as your default network user profile. To do this, log off as Tony Allen and log on to the same computer using the domain Administrator account. Press Windows Key+R to open the Run dialog box and type the path to the Netlogon share on a domain controller—for example, type **\\SEA-DC2\Netlogon**, and click OK. Then create a folder named Default User.v2 in the Netlogon share. This Default User.v2 folder is the profile folder for your default network user profile.

Note that your default network user profile must have ".v2" appended to it like this if the computers your roaming users will be using are running Windows Vista. This is because the user profiles of Windows Vista and Windows XP have different structures, making them incompatible. A computer running Windows Vista cannot read a user profile created from Windows XP, and vice versa. So if some of your users still have computers running Windows XP and you want them to be able to roam to other Windows XP computers on your network, you need to repeat the preceding procedure except for two differences: the computer you log on to in order to create the default network profile needs to be running Windows XP, not Windows Vista; and the folder you need to create in the Netlogon share needs to be named Default User, not Default User.v2.

After you've created the Default User.v2 folder in the Netlogon share, you're ready to copy the profile you customized earlier (Tony Allen's profile) to this folder. To do this, open System properties from Control Panel, select the Advanced tab, click the Settings button under User Profiles, select Tony Allen's profile, and click Copy To. In the Copy Profile To text box, type **\\SEA-DC2\Netlogon\Default User.v2** as the destination, and then click Change and configure the profile so that the Everyone built-in identity can use it. (See Figure 7-6.)

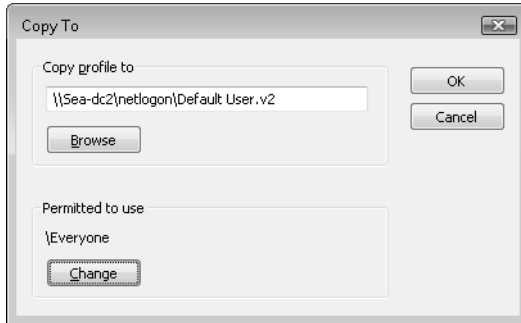


FIGURE 7-6 Copying the customized user profile to use it as the default network user profile.

Figure 7-7 verifies that the default network user profile has been properly created and is present in the Netlogon share on the domain controller.

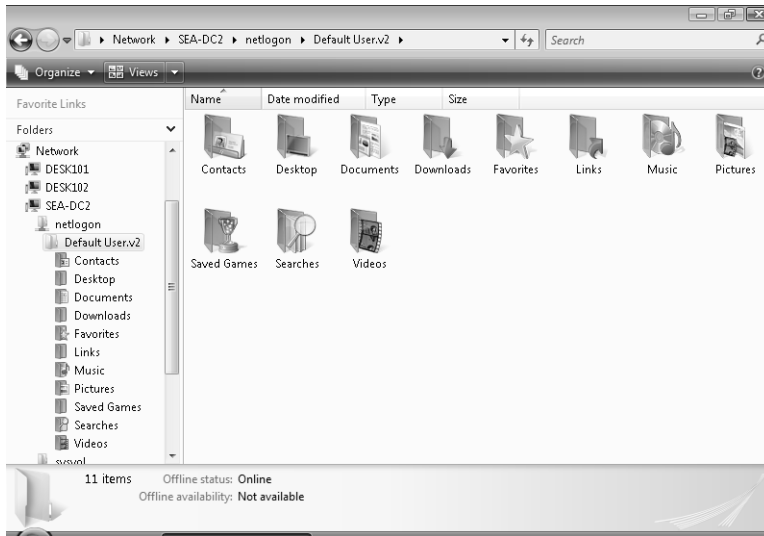


FIGURE 7-7 The default network user profile has been created.

Step 2: Prepare the Roaming Profile Storage Location

Your next step is to prepare a network share where roaming user profiles for your users will be stored. To do this, you might create a folder named C:\Profiles on domain controller SEA-DC2, configure the NTFS permissions on this folder so that the Users group has Full Control permission, and share the folder as Profiles with the Authenticated Users built-in identity having Full Control shared folder permission.

Step 3: Configure User Accounts to Use Roaming Profiles

The final step in implementing RUP for users on your network is to configure each domain user account to use the Profiles share you created as the location where the user's profile will be stored. To do this for a single user such as Karen Berg, use the Active Directory Users and Computers console on your domain controller to open the Properties for Karen's user account. Then select the Profile tab and type **\\SEA-DC2\Profiles\%username%** as the profile path for her account. (See Figure 7-8.)

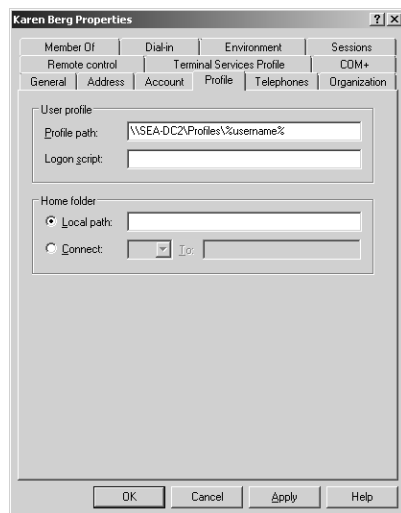


FIGURE 7-8 Configuring a user account to use a roaming user profile.

If you have many users who need to have RUP configured for them, you can do this by using Active Directory Services Interface (ADSI) scripting. You can also configure profile paths on a per-computer basis using Group Policy. Policy settings for configuring user profiles can be found in the following two locations in the Group Policy Object Editor:

- Computer Configuration\Policies\Administrative Templates\System\User Profiles
- User Configuration\Policies\Administrative Templates\System\User Profiles

One of these per-computer policies—Set Roaming Profile Path For All Users Logging Onto This Computer, which is shown in Figure 7-9—can be used to configure the profile path for the computers targeted by a Group Policy object. Note that policy overrides any per-user setting for profile paths configured in Active Directory. Additional policy settings for managing user profiles using Group Policy are summarized in Table 7-3, which also highlights the new policy settings available in Windows Vista for managing user profiles in an Active Directory environment.

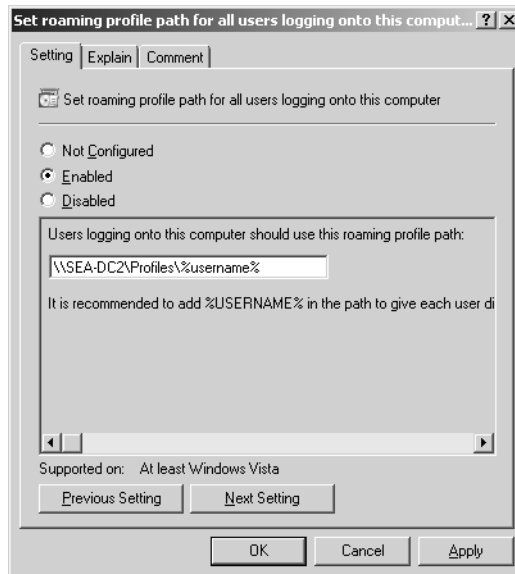


FIGURE 7-9 Configuring a roaming profile path using Group Policy.

TABLE 7-3 Per-Computer and Per-User Group Policy Settings for Managing User Profiles in an Active Directory Environment

Group Policy Setting	Supported in Windows Vista or Newer Only
Policies under Computer Configuration\Policies\Administrative Templates\System\User Profiles	
Add The Administrators Security Group To Roaming User Profiles	
Delete Cached Copies Of Roaming Profiles	
Delete User Profiles Older Than A Specified Number Of Days On System Restart	✓
Do Not Check For User Ownership Of Roaming Profile Folders	
Do Not Detect Slow Network Connections	
Do Not Forcefully Unload The User's Registry At User Logoff	✓

Group Policy Setting	Supported in Windows Vista or Newer Only
Do Not Log Users On With Temporary Profiles	
Leave Windows Installer And Group Policy Software Installation Data	
Maximum Retries To Unload And Update User Profile	
Only Allow Local User Profiles	
Prevent Roaming Profile Changes From Propagating To The Server	
Prompt User When A Slow Network Connection Is Detected	
Set Maximum Wait Time For The Network If A User Has A Roaming User Profile Or Remote Home Directory	✓
Set Roaming Profile Path For All Users Logging Onto This Computer	✓
Slow Network Connection Timeout For User Profile	
Timeout For Dialog Boxes	
Wait For Remote User Profile	
Policies under Computer Configuration\Policies\Administrative Templates\System\User Profiles	
Connect Home Directory To Root Of The Share	
Exclude Directories In Roaming Profile	
Limit Profile Size	
Network Directories To Sync At Logon/Logoff Time Only	✓

Step 4: Verify that RUP Works

After you’ve completed the steps just shown, you’ve prepared your environment for RUP. This means, for example, that when Karen Berg logs on to a computer she has not logged on to before, a new roaming user profile is generated for her from the default network user profile stored in Netlogon on the domain controller that authenticates her. When this roaming profile loads, her desktop appears and has the background and shortcuts configured previously using Tony Allen’s account. Karen can verify that she is using a roaming user profile by opening System in Control Panel, selecting the Advanced tab, and clicking Settings under User Profiles to display the User Profiles dialog box as shown in Figure 7-10.

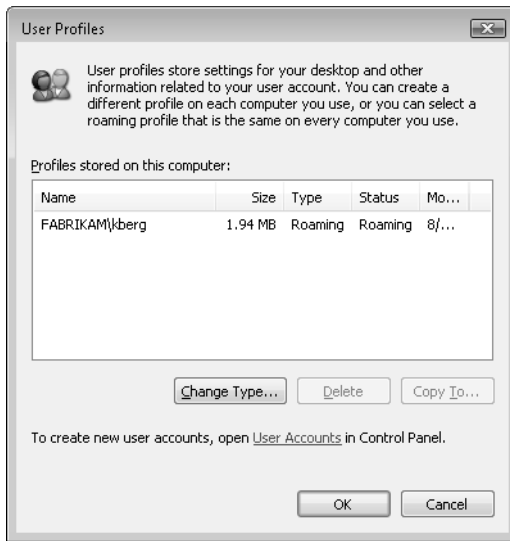


FIGURE 7-10 Verifying that the user's profile is a roaming profile.

In addition, if Karen browses to the Netlogon share on the domain controller, she will see her .v2 profile folder as shown in Figure 7-11.

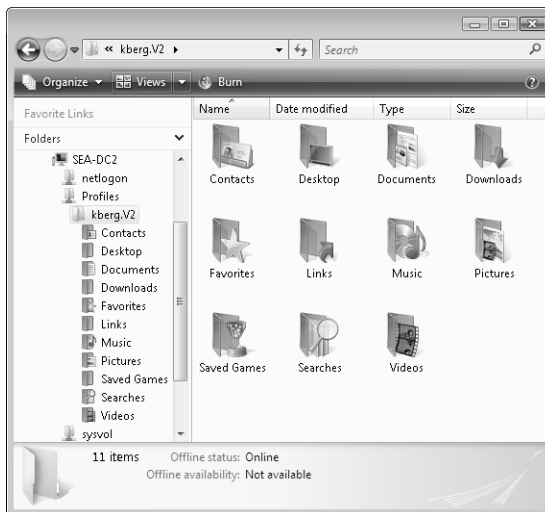


FIGURE 7-11 Verifying the user's roaming profile folder on the domain controller.



More Info For more information on implementing RUP in corporate environments, see the white paper titled "Managing Roaming User Data Deployment Guide," which is available from the Microsoft Download Center by using the link <http://go.microsoft.com/fwlink/?LinkId=73760>.

Direct from the Source: Mandatory and Super-Mandatory User Profiles

There are two types of mandatory profiles: normal mandatory profiles and super-mandatory profiles. A mandatory user profile is a special type of preconfigured roaming user profile that administrators can use to specify settings for users. With mandatory user profiles, a user can modify his desktop but the changes are not saved when the user logs off. The next time the user logs on, the mandatory user profile created by the administrator is downloaded.

User profiles become mandatory profiles when the administrator renames the NTuser.dat file (the registry hive) on the server to Ntuser.man. The .man extension causes the user profile to be a read-only profile.

Super-mandatory user profiles are similar to normal mandatory profiles, with the exception that users who have super-mandatory profiles cannot log on when the server that stores the mandatory profile is unavailable. Users with normal mandatory profiles can log on with the locally cached copy of the mandatory profile.

User profiles become super-mandatory when the folder name of the profile path ends in .man—for example, \\server\share\mandatoryprofile.man.

Only system administrators can make changes to mandatory user profiles.

—CSS Global Technical Readiness (GTR) team

Limitations of RUP

Although RUP achieves its goals of providing users with the ability to move between computers and enabling centralized backup of user data and settings, when implemented by itself RUP has several limitations that date back to Windows NT when RUP was designed. Specifically, the limitations are as follows:

- RUP can have poor performance because the entire profile of the user is synchronized between the client and the server. This can lead to slow logons and logoffs as the user waits for her profile to be copied to or from the server where roaming profiles are being stored. In particular, the user's first logon experience on a new computer can be time-consuming because all the settings and data for the user are downloaded to the client. RUP can have especially bad performance over slow wide area network (WAN) links, which can be a significant issue for small branch offices that do not have a domain controller at their site.

- RUP is inefficient in its design because it synchronizes a user's entire profile even if only a single setting or data file has changed within the user's profile during the current logon session. In addition, the profile is not copied to the file server until the user logs off from her computer, and this means that if the user's computer died while she was working, she would lose her work even if she had saved it during her session.
- While RUP allows multiple simultaneous logons by a user across several computers, sync issues can occur if users do this. For instance, if a user logs on to one computer, edits and saves a document stored in the Documents folder, leaves the computer logged on and then moves to a second computer, logs on, edits and saves the same document, and then logs off from both computers, the computer from which the user logs off of last will win. That is, the edits made to the document on that computer will be the only edits that will be preserved. The edits done on the other computer will be lost. It's important to remember that when conflicts like this occur, RUP resolves them on a last-writer-wins basis.
- RUP can lead to application inconsistencies. For instance, a user logs on to a computer and creates a shortcut on his desktop for running Microsoft Office Word. The user then logs off and logs on to a second computer—one that doesn't have Word installed. Because RUP is being used, the shortcut to Word is displayed on the second computer's desktop, but clicking this shortcut does not produce the expected result (launching Word) because the program is not installed on that computer. Note, however, that you can use the "Exclude Directories On Roaming Profile" Group Policy setting to prevent roaming the Desktop folder, which will prevent this inconsistency from arising.
- RUP is not easy to manage because it must be enabled on a per-user basis, either by manually configuring the Profile tab on the Properties sheet of each user account or by writing an ADSI script to configure the profile path for user accounts in batch mode. As described in the previous section, Windows Vista does include a new Group Policy setting for configuring a profile path, but this policy can be applied only at the per-computer level, not per user.
- In mixed environments where some client computers are running Windows Vista and others are running Windows XP, users are unable to roam between platforms because each platform uses its own unique user profile folder structure. In such environments, users must either be restricted to using only one client computing platform or live with having two separate profiles, one for Windows Vista and one for Windows XP. And if the latter is allowed, administrators need to allocate twice the storage space on the file server where roaming profiles are stored.

Because RUP alone only partially achieves the goal of efficiently virtualizing the user state information for a user, RUP should generally be implemented together with a second feature known as Folder Redirection, which is discussed next.

Understanding Folder Redirection

Folder Redirection (FR) was added to Windows 2000 to alleviate some of the performance issues associated with RUP, which was developed earlier for Windows NT. The main drag on the performance of RUP is the slow logon/logoff times that can result when users have a large number of files stored in their Documents folder (My Documents on Windows XP) or on their desktop. When the user logs on or off, these files must be copied to or from the network file server where roaming profiles are stored. So if a user has gigabytes of Word documents or Excel spreadsheets stored in his roaming profile and the network connection to his client computer is Fast Ethernet (100 Mbps), logon and logoff can take a half an hour or longer, which is certainly an unacceptable delay for most environments.

By redirecting the user's Documents folder to a network share, however, these Word and Excel files are no longer stored within the user's profile. The result is that logon times are reduced to only a few seconds, which is acceptable except for all but the most impatient and demanding users. The technology for doing this is FR, which when combined with RUP makes a more efficient user state virtualization experience. Another benefit of this is that the user's data is pretty much constantly synced. So, if a RUP user only rarely logs off (maybe he just lock his computer), his data will not go up to the server frequently. With FR, however, the data is much more likely to be up to date on the server, providing a nice backup mechanism.

How Folder Redirection Works

Folder Redirection is a client-side technology that provides the ability to change the target location of a certain set of folders within a user's profile. This redirection is transparent from the user and application's end, meaning that from the user's perspective the redirected folders look and behave as if they were in the file system on the local computer instead of in a share located somewhere on the network.

On the earlier Windows 2000 and Windows XP platforms, FR could be used only to redirect the following five folders from out of the user's profile to a network share:

- My Documents
- My Pictures
- Desktop
- Start Menu
- Application Data

These five folders were chosen for redirection either because of their importance (Start Menu and Application Data folders) or because they tend to be large in size (My Documents, My Pictures, and Desktop). Redirection of these folders could be achieved either through manually configuring the target of each folder or using Group Policy.

Beginning with Windows Vista, however, the number of folders that can be redirected out of a user's profile has been increased to 13 as the Group Policy setting shown in Figure 7-12 illustrates.

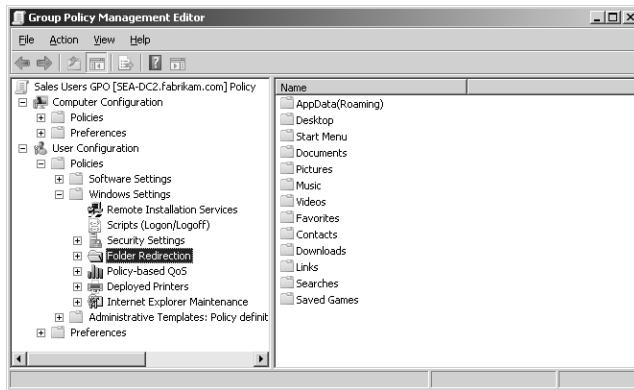


FIGURE 7-12 Configuring Folder Redirection using Group Policy.

After FR has been configured, many of the limitations associated with using RUP alone are overcome. For example, logon/logoff times are greatly improved because the user's data files are no longer stored within the user's roaming profile. When the user uses Word to open a .docx file stored within her Documents folder, she is actually opening a .docx file stored in a shared folder on a network file server and not a file stored locally on her client computer. If the .docx file is large and the network connection is slow, the document might take a little longer to open or save than if the file had been stored locally, but in most cases the delay will be only a few seconds, compared to possible delays of up to an hour if hundreds of such files were saved within the user's roaming profile.

FR can also be used in environments where users must roam between computers running Windows Vista and computers running Windows XP. In such a situation, the user will have two separate profiles as described earlier in this chapter. If you redirect the user's Documents folder out of her roaming profile, however, the user can at least access the contents of this folder when logged on to either platform. FR can even be implemented in small workgroup environments where Active Directory is not deployed, as illustrated in the next section.

FR can also be implemented alone without RUP to provide a partial user state virtualization solution. Using FR, users will be able to log on to any computer on the network and access their documents, pictures, Start menu items, and Internet Explorer favorites. Only user customizations stored within the Ntuser.dat file of a user's profile will not be roamed. For example, if the user configures a desktop background on one computer, logs off, and logs on to a second computer, she won't see the background she configured on the first computer.

Implementing FR in a Workgroup

In small networking environments such as a workgroup of a dozen client computers and a file server, FR can be configured manually on each client computer. To do this for user Tony Allen, for example, Tony would open the Properties of his Documents folder using Windows Explorer, select the Location tab, and type or browse to the network share where his Documents folder will be redirected to. Figure 7-13 shows the default location for Tony's Documents folder, which is C:\Users\Tony Allen\Documents on his local computer.

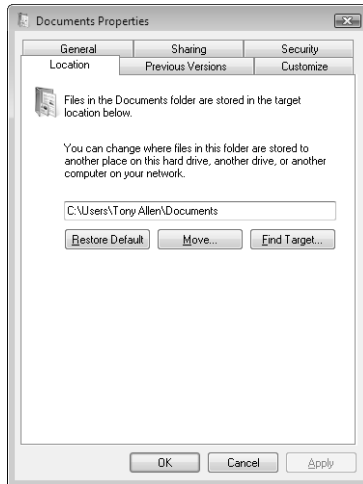


FIGURE 7-13 The default location for Documents is in the user's local profile.

To redirect his Documents folder, Tony types the following as the new target for his folder:

\\FILESRV\UserFolders\Tony Allen\Documents

This new path is a UNC path of the form:

\\<file server>\<shared folder>\<user's profile folder>\Documents

When he clicks Apply, a dialog box appears telling him that the target folder doesn't exist and asking if he wants to create it. Tony clicks OK and is then presented with an additional dialog box asking him if he wants to copy the contents of his local Documents folder to the remote one (good idea) or keep the original one and thus have two Documents folders to work with (not so good). Tony accepts the former, and the entire Documents folder is redirected from his local computer to the file server.

Obviously, manual configuration of FR like this can scale only for very small networks such as small workgroups. For networks that have Active Directory implemented and use RUP, a better way to implement FR is to use Group Policy as described in the next section.

Implementing FR with RUP

Implementing FR in an enterprise environment where Active Directory is deployed can be done either with or without using RUP. If RUP is configured, FR can significantly enhance the performance of RUP and allow sharing of user data between Windows XP and Windows Vista user profiles. If RUP is not configured, FR can provide a partial (that is, only file-based settings, not registry-based settings) user state virtualization solution that roams user data plus user-configurable application settings that support roaming. This section assumes you want to implement FR in an environment where RUP is already configured.

Implementing FR in an Active Directory environment involves the following steps:

1. Create a network share on a file server where redirected user folders will be stored.
2. Configure a Group Policy object (GPO) that targets the domain users for whom you need to implement FR by enabling and configuring Folder Redirection policy settings for this GPO.
3. Verify that your Folder Redirection policies work.

Step 1: Prepare the Redirected Folders Storage Location

Your first step is to prepare a network share where redirected folders for your users will be stored. To do this, you might create a folder named C:\UserFolders on domain controller SEA-DC2, configure the NTFS permissions on this folder so that the Users group has Modify permission, and share the folder as UserFolders with the Authenticated Users built-in identity having Full Control shared folder permission.

Step 2: Configure a GPO for FR

Your next step is to configure FR using Group Policy. For example, to implement FR for user accounts contained in the Sales Users organizational unit (OU), use Group Policy Object Editor on your domain controller to open the Sales Users GPO or some other GPO that targets this OU. Then expand the console tree to the following location (as shown in Figure 7-12 earlier):

User Configuration\Policies\Windows Settings\Folder Redirection



Important You must use the Group Policy Management Console from Windows Vista RTM or from Remote Server Administration Tools (RSAT) for Windows Vista SP1; otherwise, you will only see the Windows XP-style policy settings.

Now, to redirect the Sales users' Documents folder using this GPO, right-click on Documents in the right pane and select Properties. This opens the Folder Redirection policy for the Documents folder, and as Figure 7-14 illustrates, the Target tab provides you with three options for redirecting the folder:

- **Not Configured** This is the default state of the policy setting. For a folder that resides on the computer targeted by the GPO, this policy has no effect. If the folder has already been redirected and this policy is applied, the folder remains redirected.
- **Basic** This option enables you to redirect the folder to the same network share for all users targeted by the GPO and is the simplest way to implement FR using Group Policy.
- **Advanced** This option allows you to redirect the folder to different locations, depending on the security group to which each user account belongs. This option is useful, for example, in large enterprise environments where each department has its own file server.

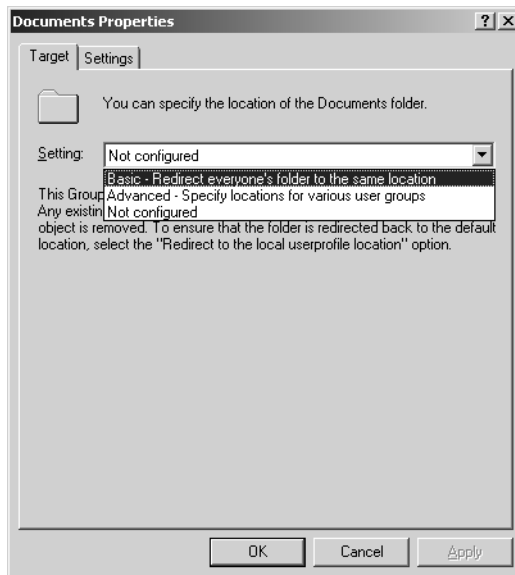


FIGURE 7-14 Redirection target options for Folder Redirection policies.

For this example, configure Basic redirection to redirect each user's Documents folder to UserFolders share on SEA-DC2. To do this, you select the Basic option, which causes the policy to display more options, as shown in Figure 7-15.

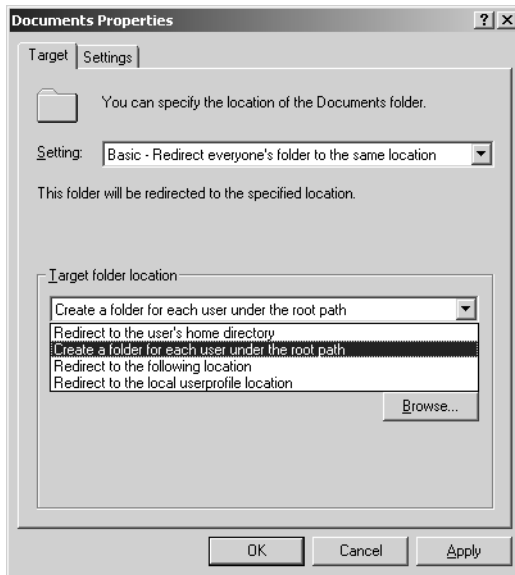


FIGURE 7-15 Further options for Basic redirection.

There are four possible types of Basic redirection you can choose from:

- **Redirect To The User's Home Directory** This option is available only for the Documents folder and redirects the Documents folder to the home folder path configured on the Profile tab of the Properties sheet for the user account in Active Directory. Note that you can also make the Pictures, Music, and Videos folders follow the Documents folder to the home directory by selecting the Also Apply Redirection Policy To Windows 2000, Windows 2000 Server, Windows XP, And Windows Server 2003 Operating Systems option on the Settings tab of the policy.
- **Create A Folder For Each User Under The Root Path** This option redirects the selected folder to the location specified by the Root Path setting, adding a folder named after the user logon name to this path. For example, if you used this option to redirect the Documents folder to the root path \\SEA-DC2\UserFolders, Folder Redirection creates the Documents folder under the path \\SEA-DC2\UserFolders\%username%, where %username% is the name of each user targeted by the policy.
- **Redirect To The Following Location** This option redirects the selected folder to the exact path specified by the Root Path setting. For example, you could use this option to allow multiple users to have the same Desktop or Start Menu.
- **Redirect To The Local Userprofile Location** This option redirects the selected folder back to the local user profile.

For this example, select the Create A Folder For Each User Under The Root Path option and then specify \\SEA-DC2\UserFolders as the Root Path for the redirected folders. (See Figure 7-16.)

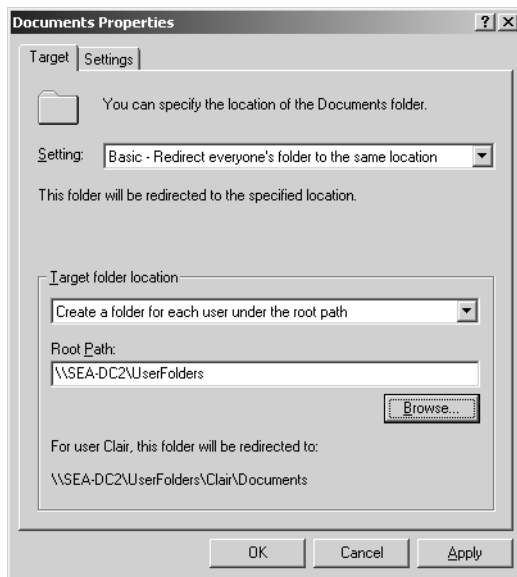


FIGURE 7-16 Basic redirection is configured to create a folder for each user in the network share.

Switching to the Settings tab displays further settings you can configure for this policy. (See Figure 7-17.)

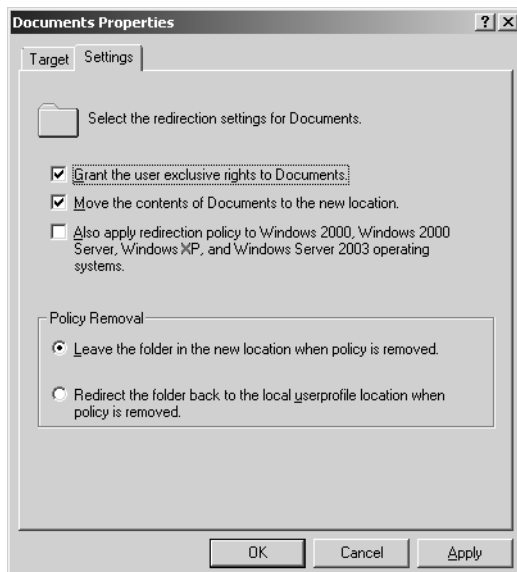


FIGURE 7-17 Settings tab of a Folder Redirection policy.

These settings can be used for the following purposes:

- **Grant The User Exclusive Rights To <folder>** Configures the NTFS permissions of a newly created %username% folder by allowing the user's account and the LocalSystem identity to have Full Control of the newly created folder.
- **Move The Contents Of <folder> To The New Location** Moves all user data in the selected folder to the new location.
- **Also Apply Redirection Policy To Windows 2000, Windows 2000 Server, Windows XP, And Windows Server 2003 Operating Systems** Tells the Folder Redirection snap-in extension to write the redirection policy in a format that can be recognized by previous Windows operating systems. If this setting is not selected, the snap-in extension writes the redirection policy in a format that can be used only by Windows Vista. This setting is available only for the Documents, Pictures, Application Data, Desktop, and Start Menu folders, which are the only folders that could be redirected on previous versions of Windows.
- **Policy Removal Settings** These two options determine what happens to the redirected folder when the policy no longer applies to a specific user—that is, when the policy has gone out of scope. Policies typically go out of scope when they are unlinked or deleted by the administrator, or when the user belongs to a group with specific permission not to apply the policy.

Here are the two choices you can select from:

- **Leave The Folder In The New Location When Policy Is Removed** Folder Redirection leaves the user's data files in the redirected location when the policy goes out of scope.
- **Redirect The Folder Back To The Local UserProfile Location When Policy Is Removed** Folder Redirection copies the files from the redirected location back to the user's local profile when the policy goes out of scope.

After you've configured your Folder Redirection policy for the Documents folder, you can configure similar policies for other folders you want to redirect for users targeted by the GPO.

Step 3: Verify that FR Works

To verify that FR works together with RUP, log on to a client computer as Karen Berg, a user in the Sales department. (Karen's user account has already been configured to use RUP earlier in this chapter.) When Karen logs on, she can use Windows Explorer to verify that her Documents folder has been moved to the server. (See Figure 7-18.)

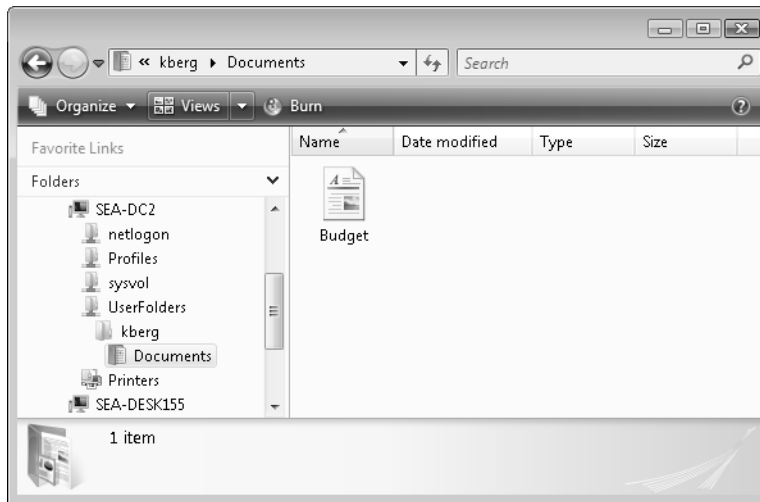


FIGURE 7-18 Karen's Documents folder has been redirected to the server.

See Also For more information on implementing FR with RUP in corporate environments, see the white paper titled "Managing Roaming User Data Deployment Guide," which is available from the Microsoft Download Center by using the link <http://go.microsoft.com/fwlink/?LinkId=73760>.

Limitations of FR/RUP

Although FR used together with RUP overcomes many of the limitations of using RUP alone, it still doesn't enable users to work on their documents when the network is down or when the network file server that hosts users' redirected documents goes down (although you can work on your documents locally while the network is down because you just use the cached profile). To overcome this limitation, a third user state virtualization technology is required—Offline Files.

Understanding Offline Files

Offline Files is a feature first introduced in Windows 2000 that enables users to access files stored in shared folders on network file servers even when those shares (or file servers or the network itself) become unavailable for some reason. Offline Files enhances the productivity of knowledge workers in several ways:

- It enables users to continue working with documents and other files even when the file servers hosting those documents are unavailable because of network interruption, server maintenance, or any other reason.

- It allows users located at branch offices to work with documents stored on file servers located at corporate headquarters even when the WAN link connecting the sites becomes congested or unreliable.
- It enables mobile users to work with documents stored on network shares while they travel, even when they don't have connectivity with the corporate network.

How Offline Files Works

When Offline Files is enabled on client computers in an environment where FR and RUP are configured, files that users copy or save into redirected folders are automatically made available for offline use by the user. Such files marked for availability offline are displayed with a green synchronization icon overlay as shown in Figure 7-19.



FIGURE 7-19 A document marked for availability offline.

A copy of each file made available offline is stored within a local cache called the client-side cache (CSC) on the user's computer. If the network connection with the file server where the user's redirected documents reside is available and the user tries to open the document, the network copy of the document is downloaded to the user's computer, the document is opened, and the user can begin working on the document. If the network connection to the server is down and the user tries to open the document, the local copy of the document is retrieved from the user's local Offline Files cache on the computer, the document is opened, and the user can begin working on the document. The key thing to understand is that the user experience is the same in both cases—the user doesn't need to know whether the network connection to the server is available or down.

Files and folders automatically transition to the offline state when the network connection goes down or drops below a given threshold (slow link). Users can also manually take folders offline so that they can work with local copies of the files in the folder instead of with the network copies. Taking a folder offline can be advantageous if the network connectivity with the file server becomes unreliable or congested because opening a document from the local cache can be faster in such cases than opening it from the network.

Users can also work offline with files stored in network shares outside of their own user profile. In this case, the user must manually mark a file for offline availability before a copy of the file can be stored in the user's local Offline Files cache. To mark a file as available offline, the user can right-click on the file and select Always Available Offline. (See Figure 7-20.)

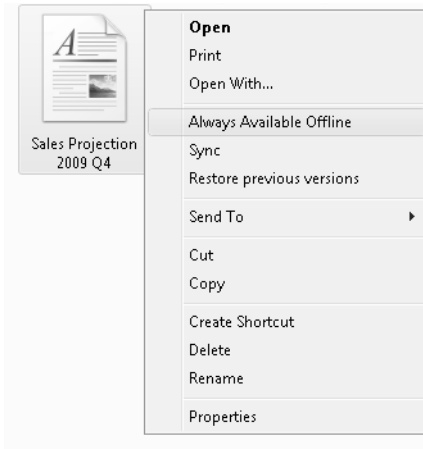


FIGURE 7-20 Marking a document for offline availability.

If a network share contains some files that are marked for availability offline and other files that are not marked, the unmarked files are displayed as icons without overlays. If the connection to the share goes down, however, the files not marked for offline availability change to ghosted icons with an X overlay as shown in Figure 7-21. These ghosted icons are placeholders representing files that are present on the network but unavailable in the user's local Offline Files cache.

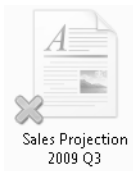


FIGURE 7-21 A file that is present on the network but unavailable offline.

For information concerning how Offline Files have been enhanced in Windows Vista compared with Windows XP, see the sidebar titled “Direct from the Source: Enhancements to Offline Files in Windows Vista” in this chapter.

Direct from the Source: Enhancements to Offline Files in Windows Vista

Offline Files functionality has been completely redesigned for Windows Vista to improve performance, reliability, flexibility, manageability, and ease of use. The following list summarizes the enhancements and changes to Offline Files in Windows Vista compared with Windows XP:

- The user experience of using Offline Files is now more seamless and less disruptive when a transition occurs between online and offline mode.

Synchronization occurs automatically when configured, and users are notified about sync conflicts by the appearance of the Sync icon in the notification area of the taskbar. By right-clicking or left-clicking this icon, users can choose from various options for resolving the conflict, including opening the new Sync Center utility in Control Panel, which is described later in this chapter. Synchronization of other files where no conflict occurs then continues in the background while the user decides how to resolve each conflict.

- The user also has a more consistent user-interface experience compared with Windows XP when files have been transitioned to offline mode. For example, if a network folder on Windows XP contains five files and two of them are made available for offline use, only those two files are visible when the user has the folder open in Windows Explorer while the server is unavailable. In the same scenario in Windows Vista, however, all five files are visible in Windows Explorer and the unavailable files are displayed with ghosted placeholders. (See Figure 7-21.) This change causes less confusion for users by providing a consistent view of the namespace on the file server regardless of whether any files are available offline. In addition, if you configure caching on the network folder so that all files that users open from the share automatically are made available offline, Offline Files automatically creates placeholders for all the files within the folder.
- The synchronization process has been streamlined and made more efficient by the use of a new sync algorithm known as Bitmap Differential Transfer (BDT). BDT keeps track of which blocks of a file in the local cache (also called client-side cache, or CSC) are being modified when you are working offline. Then, when a sync action occurs, BDT sends only blocks that have changed to the server. This provides a definite performance improvement over Windows XP, where the entire file is copied from the local cache to the server even if only a small portion of the file has been modified. In addition, because of the performance improvement brought about by BDT, any file type can now be marked for offline use in Windows Vista. This is an improvement over Windows XP, where certain file types (such as .pst and .mdb files) were excluded by default from being made available offline either because of their large size or frequency of modification. Note that BDT is used only when syncing from the client to the server, and not the other way around. Also, it works only for files that are modified in place and hence does not work for certain applications, such as Word, PowerPoint, and so on.
- Mobile users and users at branch offices where network latency is high now benefit from an improved slow-link mode of operation. When Windows Vista determines that the network throughput between the local computer and

the remote server has dropped below a specified level, Offline Files automatically transitions to the new slow-link mode of operation. When Offline Files is running in slow-link mode, all read and write requests are satisfied from the local cache and any sync operations must be manually initiated by the user. Offline Files continues running in slow-link mode until the user attempts to transition back to online mode by clicking Work Online on the command bar of Windows Explorer. After online mode is operational again, Windows Vista tests network throughput and packet latency every two minutes by default to determine whether to remain online or transition back to slow-link mode again.

- Offline Files in Windows Vista now lets you configure a limit for the total amount of disk space used for your local cache, which includes both automatically and manually cached files. In addition, you can also configure a second limit within this total local cache size limit to specify the total disk space that can be used for automatically cached files. By contrast, in Windows XP you could specify only a limit for the total amount of disk space to be used for automatically cached files; you had no way to limit the amount of disk space used in Windows XP for manually cached files.
- Limits for total cached files and automatically cached files can be configured using Group Policy. Note that after the limit for automatically cached files has been reached, least-recently used files drop out of the cache to make room for newer ones. By contrast, manually cached files are never removed from the cache unless you specifically delete them.
- Offline Files modes of operations now apply to individual Server Message Block (SMB) shared folders and Distributed File System (DFS) scopes. By contrast, Offline Files modes in Windows XP applied only to an entire network file server or domain-based DFS namespace. This means that in Windows Vista, for example, when a network error is detected when trying to connect to a file or folder within a DFS namespace, only the DFS link that includes that file or folder is transitioned from online mode to offline. When the same scenario occurred with Windows XP, the entire DFS namespace was taken offline.
- Offline Files in Windows Vista now allows each file within the local cache to be encrypted using the Encrypting File System (EFS) certificate of the user doing the encryption. By contrast, in Windows XP you could only encrypt the entire local cache using the Local System account. This change improves privacy of information by preventing access to cached files by other users of the computer. When the local cache is encrypted, the first user who makes a particular file available offline is the only user who will be able to access that file when working offline; other users will be able to access that file only when working

online. Encryption of the Offline Files cache can be configured using Group Policy; see the section “How Offline Files Works” earlier in this chapter for more information. Note that you cannot encrypt files that are currently in use. Also, when an encrypted file is made available offline, the file is automatically encrypted in the client-side cache.

- Offline Files in Windows Vista can also be programmatically managed using either the WMI provider or Win32/COM interfaces. For more information, see [http://msdn2.microsoft.com/en-us/library/cc296092\(VS.85\).aspx](http://msdn2.microsoft.com/en-us/library/cc296092(VS.85).aspx).

All changes to Offline Files in Windows Vista, including Bitmap Differential Transfer, are compatible with any Windows Server operating system that fully supports the SMB protocol, including Windows Server 2000, Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.



More Info For more information about new features and enhancements for Offline Files in Windows Vista, see “What’s New in Offline Files for Windows Vista” found at <http://technet2.microsoft.com/WindowsVista/en/library/bb819260-0fdc-4003-bc23-04-beac2108bd1033.msp?mfr=true>.

—Mitch Tulloch with the Windows Vista Team at Microsoft, excerpted from Chapter 14 of Windows Vista Resource Kit, Second Edition (Microsoft Press, 2008)

Modes of Operation

Offline Files in Windows Vista has four modes of operation:

- **Online mode** Provides users with normal access to files and folders stored on network shares and DFS scopes. In this mode, any changes made to files or folders are first applied to the network server and then applied to the local cache. Reads are always satisfied from the Offline Files cache to ensure the best possible end-user experience. Online mode is the default mode of operation.
- **Auto offline mode** Provides users with offline access to files and folders stored on network shares and DFS scopes. Offline Files automatically transitions a network share to auto offline mode whenever it detects a network error during a file operation with an SMB shared folder or DFS scope. In this mode, all file operations are performed against the local cache except for file operations that cannot be performed in auto offline mode, such as accessing previous versions of files. When Offline Files is in auto offline mode, it automatically tries to reconnect to the network share every two minutes. If the reconnection is successful, Offline Files transitions to online mode. Users cannot initiate a manual sync while Offline Files is in auto offline mode.

- **Manual offline mode** Provides users with offline access to files and folders stored on network shares and DFS scopes. Manual offline mode persists across restarting the computer. A transition to manual offline mode occurs when the user clicks Work Offline on the command bar of Windows Explorer when viewing a network share that contains files and folders marked for offline availability. The file operations that can be performed in manual offline mode are the same as those available for auto offline mode. The user can also manually synchronize an offline item by clicking Sync on the command bar of Windows Explorer. If the user forces synchronization of an offline item, the item remains offline.
- **Slow-link mode** Provides users with offline access to files and folders stored on network shares and DFS scopes. This mode becomes available only when the Configure Slow-Link Mode policy setting has been enabled and applied to the user's computer using Group Policy. When this is done, a network share containing files and folders marked for offline availability will automatically transition to slow-link mode when Offline Files is in online mode and network performance has fallen below a specified threshold.

When a file is marked for availability offline and the user tries to open the file, the file open operation is satisfied either from the network file server or the local client-side cache. Table 7-4 summarizes which copy of the file (cached or server) is used for different file operations under various Offline Files modes of operation.

TABLE 7-4 Where File Operations Are Satisfied from for Each Offline Files Mode of Operation

Mode	Open/Create File	Read from File	Write to File	Browse Folder
Online	Server	Cache (if in sync with server)	Server then cache	Server
Auto offline	Cache	Cache	Cache	Cache
Manual offline	Cache	Cache	Cache	Cache
Slow-link	Cache	Cache	Cache	Cache

Synchronization Offline Files

Synchronization of the locally cached and network copies of files marked for offline availability can be performed in two ways:

- Automatically
- Manually

Automatic synchronization occurs only when Offline Files is in online mode. Manual synchronization can be performed when Offline Files is in any of the following modes:

- Online mode

- Manual offline mode
- Slow-link mode

Manual synchronization can be performed in several ways:

- By clicking on the Sync button in the Windows Explorer toolbar when a folder containing files marked for offline availability is being displayed
- By right-clicking on a file or folder marked for offline availability and selecting Sync from the shortcut menu
- By right-clicking on the Sync icon in the Notification Area and selecting Sync All to synchronize all files marked for offline availability (as shown in Figure 7-22)

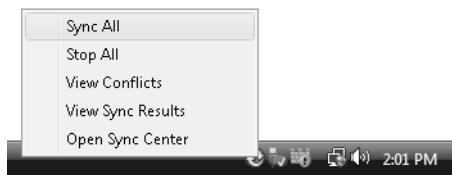


FIGURE 7-22 Synchronizing files marked for offline availability using the Sync icon in the Notification Area.

- By opening Sync Center from Control Panel and clicking Sync (as shown in Figure 7-23)



FIGURE 7-23 Using Sync Center to synchronize Offline Files.

Resolving Synchronization Conflicts

When a user modifies a file that has been made available for offline use, the locally cached and network copies of the file are now different. If a sync operation then occurs, what happens depends on which copy of the file has been modified. Specifically, if the locally cached copy has been modified while the network copy remains unchanged, the sync operation overwrites the network copy with the local copy because the local copy is the more recent version of the file. And if the locally cached copy remains unchanged while the network

copy has been modified, the sync operation overwrites the local copy with the network copy because the network copy is the more recent version of the file.

But if both the locally cached and network copies of the file are modified, a *sync conflict* occurs and a popup notification will appear. (See Figure 7-24.)

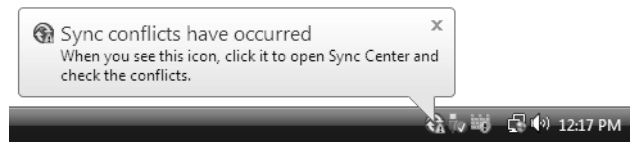


FIGURE 7-24 Popup notification of a sync conflict.

Clicking on this popup notification opens Sync Center with the View Sync Conflicts option selected. (See Figure 7-25.)

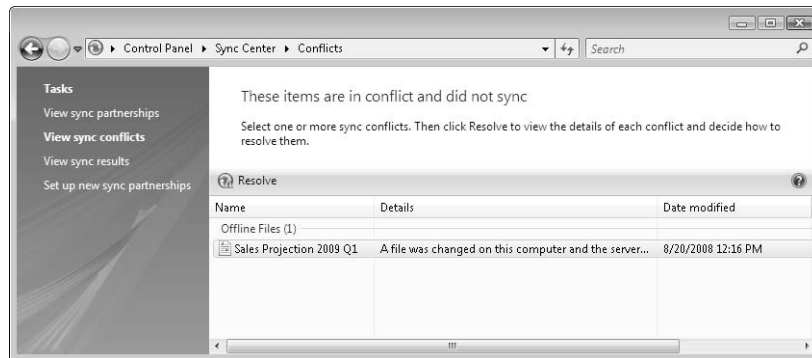


FIGURE 7-25 Sync Center indicates a sync conflict needs to be resolved.

Selecting the conflict and clicking Resolve displays a dialog box offering the user three options for resolving the conflict (as illustrated in Figure 7-26):

- Select which copy (locally cached or network) of the file should be considered the master copy and which copy should be updated.
- Choose to keep both copies of the file as is, in which case one copy of the file is renamed and both versions are then copied and stored in both locations (locally cached and network).
- Ignore the conflict, in which case the conflict will usually occur again the next time you try to sync the file.

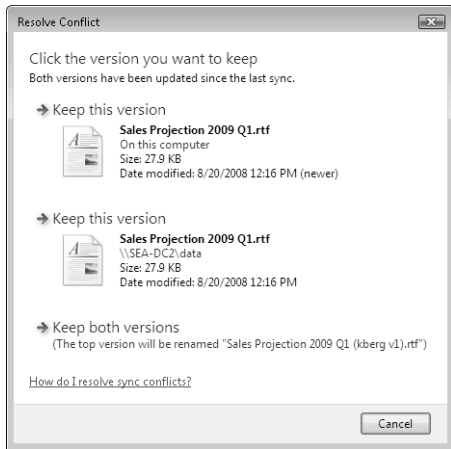


FIGURE 7-26 Options for resolving a sync conflict with a document.

Sync operations can also result when files marked for availability offline are added or deleted. For example, when the locally cached copy of a file is deleted, the network copy will also be deleted when the next sync operation occurs. And when a file is added to one location (the local cache or the network share) but not the other, the file will be copied to the other location when the next sync operation occurs.

Implementing Offline Files

Offline Files can be implemented either manually or by using Group Policy. To manually enable or disable Offline Files on his computer, a user can open the Offline Files tool from Control Panel. The General tab displays a Disable Offline Files button when Offline Files is enabled on the computer. (See Figure 7-27.)

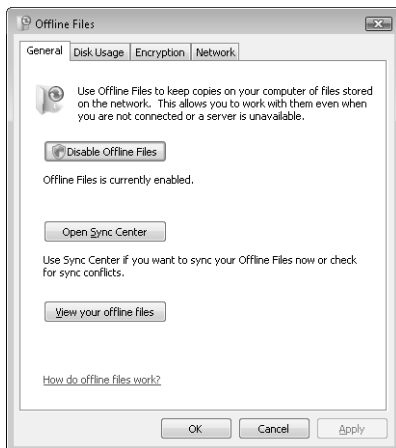


FIGURE 7-27 Offline Files has been manually enabled on the system.



Note If Offline Files has been disabled for targeted computers using Group Policy, the buttons on the General tab will be grayed out.

The shield icon on the button shown in Figure 7-27 indicates that enabling and disabling Offline Files is a privileged operation on a computer and requires local Administrator credentials. After manually enabling Offline Files, the computer must be restarted. Then when the user logs on, the Sync Center icon is displayed in the Notification Area and a popup message indicates that Offline Files is enabled. (See Figure 7-28.)

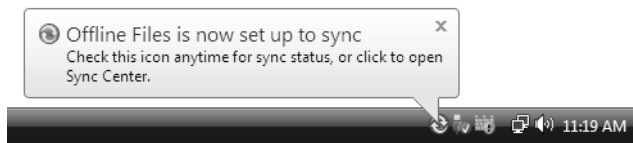


FIGURE 7-28 A popup message indicating that Offline Files has been enabled on the computer.

As an example, user Karen Berg in the fabrikam.com domain has RUP, FR, and Offline Files configured on her Windows Vista computer, with FR being configured to redirect her Documents folder out of her roaming user profile and into the UserFolders share on server SEA-DC2. When Karen opens her Documents folder from her Start menu, the files within this folder are all marked for offline availability. (See Figure 7-29.)



FIGURE 7-29 The files in Karen's redirected Documents folder are available offline.

If Help Desk informs Karen that the file server is going to be temporarily taken down for maintenance, she can transition her Documents folder and its contents from online mode to manual offline mode by clicking the Work Offline button on the Windows Explorer toolbar. The result is Figure 7-30, which looks and behaves the same as Figure 7-29 except for the changed toolbar buttons.



FIGURE 7-30 Karen's redirected Documents folder and its files have been manually taken offline.

Karen can now work with the locally cached copies of her files until Help Desk informs her that server maintenance has been completed. At that point, she can manually transition her Documents folder back to online mode by clicking Work Online in the Windows Explorer toolbar.

Of course, the beautiful thing about how Offline Files is implemented in Windows Vista is that Karen actually doesn't have to manually take her Documents folder offline and bring it back online again—this occurs automatically and transparently when the server is removed and returned from the network!

Configuring Offline Files

After Offline Files has been manually enabled, the user can further configure its operation by using the Offline Files tool in Control Panel. As shown previously in Figure 7-27, this tool has four tabs:

- **General** Allows the user to enable or disable Offline Files, open Sync Center, and view all offline files located in SMB shared folders, DFS scopes, and mapped network drives.

- **Disk Usage** Allows the user to view and configure the total disk space available for storing both automatically and manually cached offline files on her computer, view and configure the space available for storing temporary (automatically cached) offline files, and delete all temporary (automatically cached) offline files from the computer.
- **Encryption** Allows the user to encrypt or unencrypt the local Offline Files cache on her computer using EFS. The user can encrypt only the locally cached copies of her files, not the network copies.
- **Network** Allows the user to see whether slow-link mode is enabled for the computer and how often the computer checks the connection speed after the user manually transitions to online mode. The user cannot directly configure the settings on this tab because slow-link mode settings can be configured only by using Group Policy.



Tip Windows Vista indexes offline files by default. Indexing of offline files can be toggled on and off by using Indexing Options Control Panel.

Managing Offline Files Using Group Policy

In enterprise environments, administrators will want to enable and configure Offline Files using Group Policy. The policy settings for Offline Files have been enhanced in Windows Vista with several new policies, and these policy settings are found in two places in Group Policy Object Editor:

- Per-computer policy settings for Offline Files are found under Computer Configuration\Policies\Administrative Templates\Network\Offline Files.
- Per-user policy settings for Offline Files are found under User Configuration\Policies\Administrative Templates\Network\Offline Files.

Table 7-5 lists all the policies available in these locations for managing Offline Files on Windows 2000, Windows XP, and Windows Vista. The table also indicates which policy settings are per computer, which are per user, which apply to Windows Vista, and which are new to Windows Vista.

TABLE 7-5 Offline Files Policy Settings for Windows Vista and Earlier Windows Platforms

Policy Setting	Per Computer	Per User	Applies to Windows Vista
Action On Server Disconnect	✓	✓	
Administratively Assigned Offline Files	✓	✓	✓
Allow Or Disallow Use Of The Offline Files Feature	✓		✓

Policy Setting	Per Computer	Per User	Applies to Windows Vista
At Logoff, Delete Local Copy Of User's Offline Files	✓		
Configure Slow-Link Speed	✓		
Configure Slow-Link Mode	✓		✓ (New—replaces Configure Slow-Link Speed policy)
Default Cache Size	✓		
Encrypt The Offline Files Cache	✓		✓
Event Logging Level	✓	✓	
Files Not Cached	✓		
Initial Reminder Balloon Lifetime	✓	✓	
Limit Disk Space Used By Offline Files	✓		✓ (New—replaces Default Cache Size policy)
Non-Default Server Disconnect Actions	✓	✓	
Prevent Use Of Offline Files Folder	✓	✓	
Prohibit 'Make Available Offline' For These Files And Folders	✓	✓	
Prohibit User Configuration Of Offline Files	✓	✓	
Reminder Balloon Frequency	✓	✓	
Reminder Balloon Lifetime	✓	✓	
Remove 'Make Available Offline'	✓	✓	✓
Subfolders Always Available Offline	✓		
Synchronize All Offline Files Before Logging Off	✓	✓	
Synchronize All Offline Files When Logging On	✓	✓	
Synchronize Offline Files Before Suspend	✓	✓	
Turn Off Reminder Balloons	✓	✓	
Turn On Economical Application Of Administratively Assigned Offline Files	✓		✓ (New to Windows Vista)

Direct from the Source: CSC Server Settings for RUP/FR

When setting up a RUP or FR server, one thing to consider is how to set the CSC settings on the share. Regarding CSC, RUP/FR behaves quite differently: RUP uses its own synchronization algorithm to keep the local copy in sync with the server, so it does not rely on CSC. As a best practice, Microsoft always recommends that you configure the RUP server to disable CSC (with the setting Files Or Programs From This Share Will Not Be Available Offline). FR, on the other hand, depends heavily on CSC to provide synchronization between the client cache and the server. So the typical setting on an FR share is manual caching (Only The Files Or Programs The Users Specify Will Be Available Offline). You don't need to set it to auto caching (All Files And Programs That The Users Open From This Share Will Be Automatically Available Offline) because the FR client side automatically pins the folder so that it will always be available offline.

However, the preceding recommendation has an exception. Because Windows Vista and Windows XP have separate profiles on the server (Windows Vista has a .v2 suffix), if you have both Windows XP and Windows Vista clients in your organization and have RUP deployed on both platforms, you can't share data between them. To share a specific folder between them, you can deploy a special folder redirection policy for Windows Vista client computers to redirect only a certain folder (such as Favorites) to the Windows XP RUP share. In this configuration, you cannot disable CSC entirely on the RUP share. Instead, you need to set up manual caching to let CSC work against this share for Windows Vista. Don't worry about RUP in Windows XP, though—RUP tries to keep the CSC out of the picture by bypassing CSC to talk directly to the server.

—Ming Zhu, Software Design Engineer, Microsoft Windows Shell Team

Key Benefits of RUP, FR, and Offline Files

As you might already have guessed by this point from reading this chapter, implementing a user state virtualization solution using Roaming User Profiles, Folder Redirection, and Offline Files together with Group Policy in an environment where client computers are running Windows Vista can bring tangible benefits to companies looking to boost worker productivity and reduce management overhead. Let's briefly review the incremental benefits of implementing each of these three technologies in turn.

Benefits of RUP

Implementing RUP in enterprise environments can provide the following benefits:

- Users can roam between computers and access their own personalized desktop, application settings, and user data from any computer.

- Administrators can back up users' application settings and data centrally from a network file server.
- Administrators can use Group Policy to configure, manage, and lock down RUP according to the needs and requirements of the organization.
- Administrators can provide temporary workers with locked-down desktops by implementing mandatory RUP or, for even greater security, super-mandatory-RUP.

Benefits of FR with RUP

Implementing FR together with RUP in enterprise environments can provide the following benefits:

- Greatly reduced logon and logoff times for roaming users.
- Administrators can use Group Policy to redirect 13 key folders within a user's profile to a central network location where they can be easily backed up.
- Users can access their data files from computers running either Windows Vista or Windows XP.

Benefits of Offline Files with FR and RUP

Implementing Offline Files together with FR and RUP in enterprise environments can provide the following benefits:

- Users can continue transparently working with their data files when the network becomes unavailable, is congested, or functions intermittently.
- Mobile users can access files stored on network shares when they are away from the office and have no remote connectivity.
- Administrators can use Group Policy to configure most aspects of Offline Files functionality.

Usage Scenarios for RUP, FR, and Offline Files

Finally, we'll conclude this chapter with an imaginary description of how RUP, FR, and Offline Files can enhance the productivity of a knowledge worker named Karen Berg, a sales associate with Fabrikam Fine Furniture. Here is a typical day in Karen's life:

- 8:30 a.m.** After a busy commute on the freeway, Karen docks her Windows Vista laptop onto the corporate network, loads her user roaming user profile, opens her redirected Documents folder, and begins working on her sales proposal.

10:00 a.m. Karen gets called to a meeting in the building across the street. She turns off her laptop and leaves it docked in her office.

10:15 a.m. At the meeting, Karen realizes she needs a spreadsheet she was working on. She leaves the meeting room, finds a Windows Vista computer not being used, logs on using her roaming profile, opens the spreadsheet from the redirected Documents folder, makes a few changes, saves her changes, and copies it to a thumbdrive to bring into the meeting room.

11:30 a.m. Karen is back in her office again, and she uses her laptop to continue working on her proposal.

12:15 p.m. Suzie calls Karen and asks her if she wants to do lunch. Karen takes her laptop along with her so that she can work on her proposal after dessert.

1:30 p.m. Karen tries to connect to the wireless hot spot at the restaurant to access the virtual private network (VPN) into the corporate network, but she discovers the hot spot is down. No worries—Karen has access to her redirected Documents folder offline because her administrator had the foresight to implement Offline Files for the computers in her department.

2:30 p.m. Karen has a tension headache from too much caffeine—her third nonfat grande soy latte of the day. She decides to knock off work early and play a few rounds of golf, and then log on later from home using her laptop. She doesn't anticipate any problems finishing her proposal, even though her home DSL connection to the Internet has been flakey lately and she might have to use her laptop's built-in 56-Kbps modem—it's slow, but Offline Files in Windows Vista has a slow-link mode of operation that will cover that base.

1:30 a.m. Another busy day for a sales associate, as finally Karen hits the sack, her proposal nicely polished and ready to present at tomorrow morning's staff meeting.

Additional Resources

The resources listed in this section were either referred to in the chapter or provide additional information concerning concepts and products discussed in this chapter.

General

You can find detailed information about how RUP, FR, and Offline Files work and how they can be implemented in enterprise environments that have Windows Vista with Service Pack 1 deployed by reading Chapter 14, "Managing Users and Users Data" in *Windows Vista*

Resource Kit, Second Edition by Mitch Tulloch, Tony Northrup, Jerry Honeycutt, with the Windows Vista Team at Microsoft (Microsoft Press, 2008). For more information and to order a copy, see <http://www.microsoft.com/MSPress/books/12788.aspx>.

User Profiles

For a quick overview of user state migration and the process of moving user documents and settings from an earlier version of an operating system to a new version, see the “Quick Start Guide to Windows Vista User Profile Migration” in the Windows Server TechCenter on Microsoft TechNet at <http://technet2.microsoft.com/WindowsVista/nl/Library/1bd36fc2-1fc6-4edf-847f-d4be4305516a1043.msp?mfr=true>.

FR and RUP

For a helpful walk-through on how to implement FR together with RUP in corporate environments, see the white paper titled “Managing Roaming User Data Deployment Guide,” which is available from the Microsoft Download Center by using the link <http://go.microsoft.com/fwlink/?LinkId=73760>. This white paper is especially helpful for enterprises with mixed environments that have client computers running Windows Vista and Windows XP.

Offline Files

For detailed information concerning the changes and enhancements to Offline Files in Windows Vista, see “What’s New in Offline Files for Windows Vista” in the Windows Client TechCenter on Microsoft TechNet at <http://technet.microsoft.com/en-us/library/cc749449.aspx>.

Microsoft Bloggers

The Storage Team at Microsoft has a helpful post, “Using Offline Files with Samba/EMC Servers, and NAS Devices,” on their blog “The File Cabinet” at <http://blogs.technet.com/filecab/archive/2007/03/16/using-offline-files-with-samba-emc-servers-nas-devices.aspx>. Many other helpful posts concerning Offline Files can be found on their blog at <http://blogs.technet.com/filecab/archive/tags/Offline+Files/default.aspx>.

TechNet Webcasts

The following TechNet Webcasts include helpful demonstrations of user state virtualization technologies in Windows Vista:

Offline Files and Folder Redirection in Windows Vista (Level 300) at <http://msevents.microsoft.com/cui/WebCastEventDetails.aspx?culture=en-US&EventID=1032369737&CountryCode=US>

New Backup and Offline Files Features in Windows Vista (Level 300) at <http://msevents.microsoft.com/cui/WebCastEventDetails.aspx?EventID=1032306238&EventCategory=3&culture=en-US&CountryCode=US>

TechNet Forums

To obtain help with your questions and problems concerning RUP, FR, and Offline Files in Windows Vista, and to help others, use the appropriate Windows Vista forum on Microsoft TechNet at <http://forums.microsoft.com/TechNet/default.aspx?ForumGroupID=204&SiteID=17>.

Chapter 8

Building a Virtualization Infrastructure

Now that you've learned about the different products and features that make up Microsoft's Virtualization 360 vision, this final chapter covers some of the other tools and features you'll need to build and manage an integrated virtualization solution that can meet the needs of your business. Specifically, in this chapter we'll examine

- Microsoft Virtualization Solution Accelerators
- Microsoft System Center
- Virtualization Licensing

Microsoft Virtualization Solution Accelerators

Microsoft Solution Accelerators are collections of tools and best-practices documentation that allow IT professionals to proactively plan, deploy, integrate, and operate IT systems that use Microsoft products and solutions. Microsoft's growing list of Solution Accelerators are grouped together into suites covering the following areas:

- **Virtualization suite** Provides automated tools and guidance to enable you to assess your existing infrastructure and plan, deploy, and securely operate a virtualized environment using Microsoft virtualization products and solutions.
- **Desktop suite** Provides automated tools and guidance to enable you to assess your existing PC hardware and deploy Microsoft Windows desktop operating systems.
- **Server suite** Provides automated tools and guidance to enable you to assess your existing server hardware and plan, deploy, and securely operate Windows servers.
- **Security suite** Provides automated tools and guidance to enable you to proactively plan, deploy, integrate, and operate the security infrastructure of your organization.
- **IT Governance and Compliance suite** Provides automated tools and guidance to enable you to implement sound principles of IT service governance and manage the compliance infrastructure throughout your organization.
- **Microsoft Online Services suite** Provides automated tools and guidance to enable you to assess your existing infrastructure and plan for deployment of cloud-based Microsoft Online Services such as Exchange Online and more for your organization.

- **Collaboration suite** Provides automated tools and guidance to enable you to plan, deploy, integrate, and operate Microsoft SharePoint collaboration technologies.

Because this book focuses on implementing virtualization solutions, we'll examine only the Virtualization Solution Accelerators in more detail. The sections that follow cover the following topics:

- Infrastructure Planning and Design Guides for Virtualization
- Microsoft Assessment and Planning Toolkit 3.1
- Offline Virtual Machine Servicing Tool
- Other Solution Accelerators that are included in the Virtualization suite



More Info For more information concerning all currently available Microsoft Solution Accelerators, see <http://technet.microsoft.com/en-us/solutionaccelerators/default.aspx>.



Note There is some overlap between the different suites because some Solution Accelerators are included in several suites.

Infrastructure Planning and Design Guides for Virtualization

The Infrastructure Planning and Design (IPD) series provides guidance that leads you through making key decisions for proper implementation of Microsoft infrastructure products. These documents are intended for infrastructure architects who have a good grasp of how these products work, and they provide best practices guidance for the planning and design of Microsoft infrastructure products. The IPD series is constantly growing, as new guides are being added. The following guides are most relevant to planning a virtualization infrastructure:

- **Series Introduction** This guide provides an introduction to the entire series and includes information on the background and document structure of IPD guides. You should read this guide before using any of the other guides in this series.
- **Selecting the Right Virtualization Technology** This guide helps you rapidly and accurately choose which Microsoft virtualization technologies to use for specific business scenarios.
- **Microsoft Server Virtualization** This guide leads you step by step through the process of planning the implementation of server virtualization using Windows Server 2008 Hyper-V, Microsoft Virtual Server 2005 R2 SP1, or both.
- **Microsoft Application Virtualization 4.5** This guide helps you plan your App-V infrastructure and supersedes the earlier SoftGrid 4.2 guide from this series.

- **System Center Virtual Machine Manager 2008** This guide helps you plan and implement Virtual Machine Manager (VMM) 2008 for managing your virtualization infrastructure.

Other guides in this series that can assist in planning and designing a virtualization infrastructure include:

- Windows Server 2008 Terminal Services
- System Center Operations Manager 2007

Obtaining and Using the IPD Guides

The IPD guides are published in the Library section under Infrastructure Planning and Design on Microsoft TechNet at <http://technet.microsoft.com/en-us/library/cc196387.aspx>. You can quickly access these guides through the shortcut URL of <http://www.microsoft.com/IPD>, where you can also download the full series of IPD guides as the zipped archive named "IPD - All.zip." Alternatively, you can download only the guides you need from this same URL.



Note Additional IPD series guides will be made available as beta releases on the Microsoft Connect site at <http://connect.microsoft.com>.

IPD guides provide you with key information you can use to bring your infrastructure up to date. They can save your organization time and money by showing you how to strategically plan your infrastructure and help you avoid problems before they arise. You can use these guides to determine the scope of the services your infrastructure will provide, and the guides can help you decide whether you need to partially or completely redesign your infrastructure. The guides help to streamline your planning process by helping you to do the following:

- Define the technical decision flow of the planning process.
- List the decisions you will need to make and the commonly available options and considerations.
- Relate these decisions and options to your business in terms of cost, complexity, and other characteristics.
- Frame your decisions in terms of additional questions to help you understand your business needs.

Examining the App-V Guide

Most IPD guides consist of a Microsoft Office Word document together with an accompanying Microsoft Office PowerPoint slide deck (as shown in Figure 8-1).



FIGURE 8-1 IPD series Solution Accelerator for Microsoft App-V

IPD guide documents typically start by providing an overview of the technology, followed by a summary of the design process you will follow. They then provide step-by-step procedures that lead you through the process of determining the scope of your project, selecting the appropriate implementation model, implementing key components of your infrastructure, and validating the entire infrastructure plan. Most IPD guide documents also include job aids you can use to assist your implementation team in their planning and design process. The slide decks are useful for leading your infrastructure team through the planning and design process during your meetings together.

As an example of how these IPD guides can be used, the App-V guide document includes the following sections:

- **The Planning and Design Series Approach** Provides you with general information about the IPD series guides and how to use them.
- **Introduction to the Microsoft Application Virtualization Guide** Provides you with an introduction to the present guide and the assumptions used in creating this guide.
- **Application Virtualization in Microsoft Infrastructure Optimization** Places the guide within the larger context of Microsoft's Infrastructure Optimization (IO) Model, which groups IT processes and technologies across a continuum of organizational maturity. For more information about Microsoft's IO Model, see <http://www.microsoft.com/IO>. See also Chapter 1, "Microsoft's Virtualization Solution" in this book.
- **Application Virtualization Design Process** Provides an overview of the App-V infrastructure design process listing the decisions you will need to make, the decision flow, applicable scenarios, and what is out of the scope of this guide.
- **Step 1: Determine the Project Scope** Helps you determine the project's scope—that is, which applications will be available virtually, your target user population, their locations, and so on.

- **Step 2: Determine Which Model(s) Will Be Needed** Helps you choose which App-V infrastructure model you will implement. This model refers to the process by which virtualized applications are published and delivered to users. App-V can be implemented using three possible models:
 - ❑ **Standalone Model** Allows virtual applications to be MSI-enabled for distribution without streaming.
 - ❑ **Streaming Model** Uses application streaming without requiring Active Directory or a database, enabling administrators to stream from existing servers or via System Center Configuration Manager 2007 SP1 with R2 distribution points.
 - ❑ **Full Infrastructure Model** Allows for streaming of applications while also providing for built-in software distribution, management, and reporting capabilities.

Each model requires an App-V client to be installed on either your workstations or a terminal server. The guide also illustrates each possible model you can choose to implement. (See Figures 8-2 through 8-4.) Some organizations might even employ a combination of several models to meet the application virtualization needs of their business.

- **Step 3: Determine How Many Instances Will Be Needed for Each Model** Helps you determine how many instances of each model will be required to meet the infrastructure needs of your business.
- **Step 4: Client and Sequencer Considerations** Outlines various considerations relating to clients and sequencers that need to be taken into account when implementing App-V in a production environment. These considerations do not directly affect the decisions surrounding your infrastructure design, but they do have an impact on day-to-day operations and therefore should be carefully considered in advance. Considerations for deploying App-V include which App-V client to use (Desktop or Terminal Services), how you will deploy your terminal servers, sequencer computer placement, whether to use a virtual or physical sequencer, and so on.
- **Step 5: Design the Streaming Infrastructure** Helps you select a streaming server type for each location defined in your scope as determined by Step 1. For example, when planning an App-V deployment, you need to decide whether you will use App-V Streaming Servers, App-V Management Servers, or both for application streaming, or leverage existing file servers, IIS Web servers, or both. You also need to make decisions relating to the scaling of your streaming infrastructure, fault-tolerance, and maintaining applications across multiple streaming servers.
- **Step 6: Design the Full Infrastructure** If Step 3 determined that you should implement the Full Infrastructure Model, this step will determine the server resource scaling requirements and fault tolerance for each role. This step also needs to be repeated for each Full Infrastructure Model instance determined in Step 3.
- **Conclusion** Summarizes the results of using the guide, and provides links to additional resources that might be useful during the planning and design phase of your infrastructure deployment.

- **Appendix: Job Aid** A series of tables you can fill in to help you plan and design your App-V infrastructure. For example, the Application Categorization table of this guide helps you identify your locations, the number of users at each location, the available bandwidth at the location, the infrastructure model instance you plan on implementing at the location, the Streaming Instance Name for the location (if needed), and the Streaming Instance Fault-Tolerance Selection for the location (if needed).

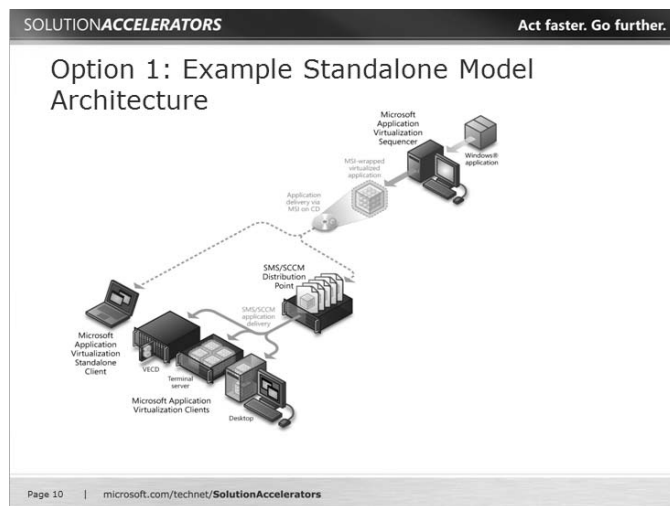


FIGURE 8-2 Diagram showing typical implementation of the Standalone Model of an App-V infrastructure

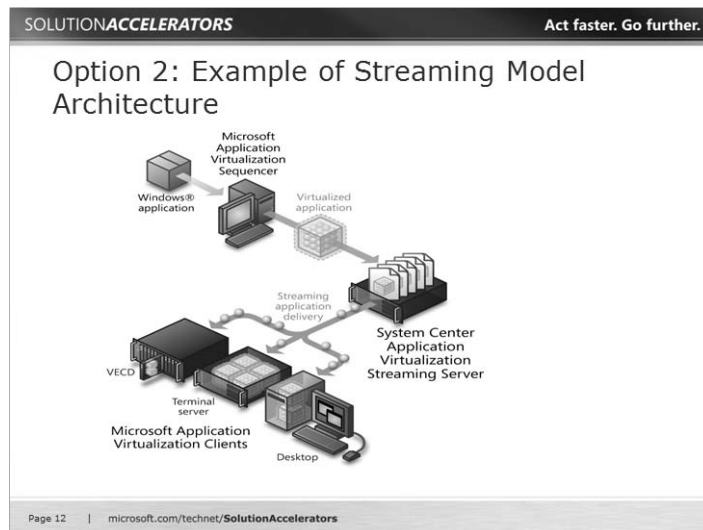


FIGURE 8-3 Diagram showing typical implementation of the Streaming Model of an App-V infrastructure

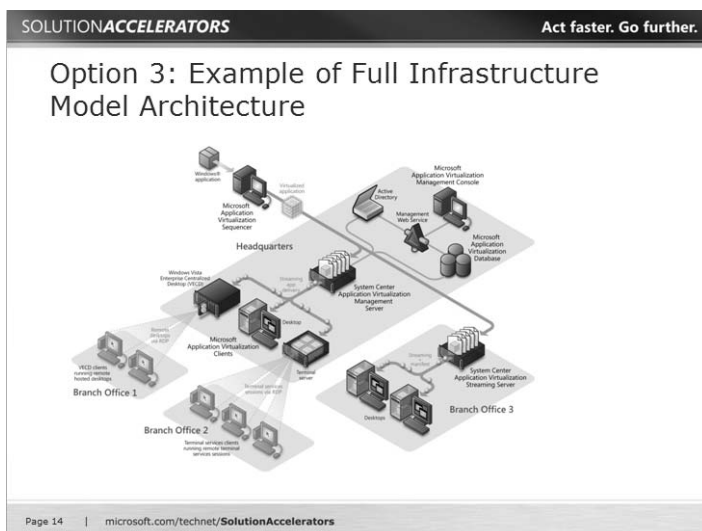


FIGURE 8-4 Diagram showing typical implementation of the Full Infrastructure Model of an App-V infrastructure

Microsoft Assessment and Planning Toolkit 3.1

The Microsoft Assessment and Planning (MAP) Toolkit 3.1 is a zero-footprint networkwide agentless tool you can use to quickly determine where your desktops and servers are and to autogenerate upgrade recommendations for multiple products, including server, desktop, and virtualization technologies. For purposes of planning, upgrading, or migrating your virtualization infrastructure, the MAP Toolkit covers the following scenarios:

- Hyper-V virtualization candidates assessment
- Microsoft Application Virtualization hardware compatibility assessment
- Windows Server 2008 hardware and device compatibility assessment, including server discovery
- SQL server discovery and assessment
- Windows Vista hardware and device compatibility assessment, including PC discovery
- Desktop Security Center assessment
- Office 2007 hardware compatibility assessment
- SNMP inventory reporting

The MAP Toolkit works by leveraging Windows Management Instrumentation (WMI) to gather information from Windows server and client computers on your network. To use the MAP Toolkit, all you need is a computer that has the MAP Toolkit installed, appropriate administrative credentials for the target computers that you want the MAP Toolkit to inventory

and assess, and other WMI requirements as described at <http://technet.microsoft.com/en-us/library/cc297229.aspx>. The MAP Toolkit is agent-less, which means that it works by remotely pinging each computer across your network and does this securely without the need for installing any agent software on the target computers.

The MAP Toolkit can be especially helpful for server consolidation projects by allowing you to determine which of your physical servers might be good candidates for Hyper-V virtualization. By capturing the workloads and utilization of each of your servers over a defined period of time, the MAP Toolkit can recommend a set of consolidated hosts for your existing servers. Specifically, the MAP Toolkit collects information about the CPU utilization, memory utilization, Network I/O, and Disk I/O rates of your physical servers. The MAP Toolkit can then autogenerate a set of proposal documents and detailed spreadsheets you can then use during your server consolidation planning process.

Obtaining the MAP Toolkit

You can download the MAP Toolkit 3.1 for free from the Microsoft Download Center for either x64 or x86 hardware platforms at <http://www.microsoft.com/downloads/details.aspx?FamilyID=67240b76-3148-4e49-943d-4d9ea7f77730&DisplayLang=en>. Alternatively, you can visit this TechNet home page for the MAP Toolkit and then click the download link: <http://www.microsoft.com/MAP>.

The MAP Toolkit 3.1 can be installed on Windows Server 2003, Windows Server 2008, Windows Vista, Windows Vista Service Pack 1, or Windows XP Professional. The MAP Toolkit 3.1 also requires the .NET Framework 2.0, Microsoft SQL Server 2005 Express Edition for storing inventory and assessment data, and Microsoft Office Word 2003 SP2 or Microsoft Office Word 2007 and Microsoft Office Excel 2003 SP2 or Microsoft Office Excel 2007 for generating reports.



Tip Make sure you install the .NET Programmability features of Excel 2007, as this is required for the MAP Toolkit to generate Excel spreadsheets.

Using the MAP Toolkit

The MAP Toolkit is easy to use. First, you download the appropriate version of the .msi installer file, and then install the MAP Toolkit on any computer that belongs to your domain and is running a version of Windows supported by the MAP Toolkit. Once the MAP Toolkit is installed, you can launch it from Microsoft Assessment and Planning Solution Accelerator under Programs on your Start menu. In this example, the MAP Toolkit has been installed on a computer running Windows XP with Service Pack 3 and which has Microsoft Office 2007 Enterprise Edition installed. The first screen of the MAP Solution Accelerator provides directions on how to configure and use the toolkit. (See Figure 8-5.)

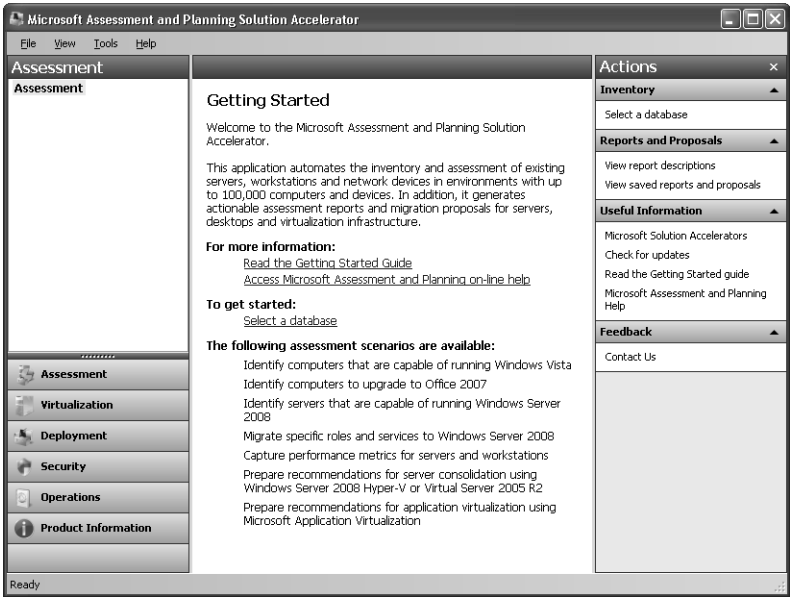


FIGURE 8-5 Initial screen of the MAP Toolkit Solution Accelerator

To begin using the MAP Toolkit, click **Select A Database** in the middle of the **Getting Started** pane. This opens a dialog box prompting you to either create a new inventory database or select an existing database. We'll create a new database named **SEATTLE** to store inventory information concerning the computers at the Seattle branch office of Contoso. (See Figure 8-6.)

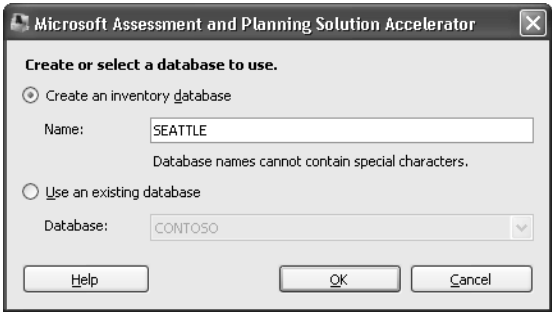


FIGURE 8-6 Creating a new database for the Seattle site of Contoso

Clicking **OK** in the preceding dialog box returns you to the MAP Toolkit, and you are ready to begin inventorying your environment. (See Figure 8-7.)

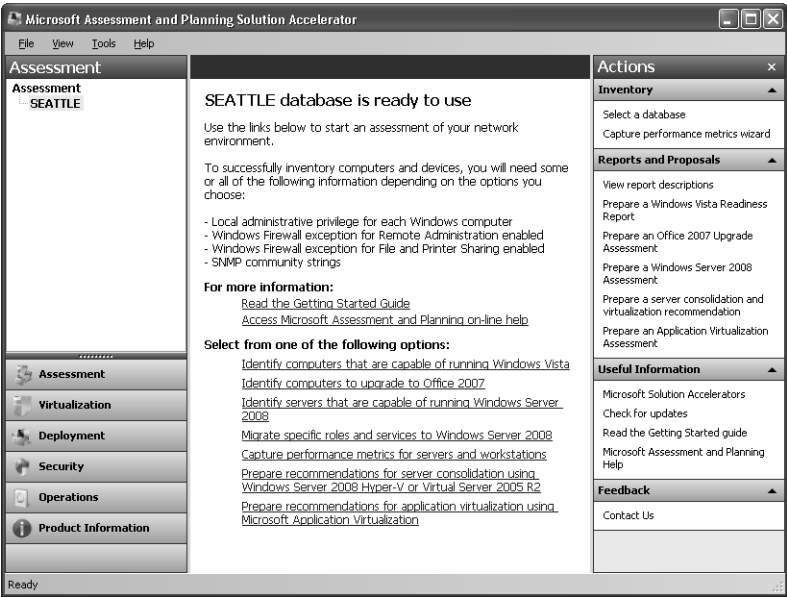


FIGURE 8-7 Select an assessment to perform against your environment.

For this example, we'll select Prepare Recommendations For Application Virtualization Using Microsoft Application Virtualization, which is the bottom option in the middle pane shown in Figure 8-7. Clicking this option launches the Assessment Wizard with Application Virtualization Assessment selected. (See Figure 8-8.)

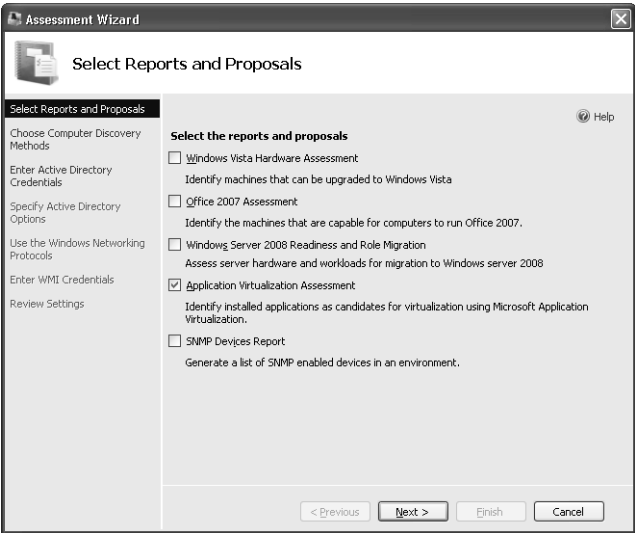


FIGURE 8-8 Initial page of the Assessment Wizard

The next page of the wizard lets you specify which methods will be used to identify the computers you want to inventory and assess. For this example, we'll find computers in Active Directory and also scan a range of IP addresses. (See Figure 8-9.)

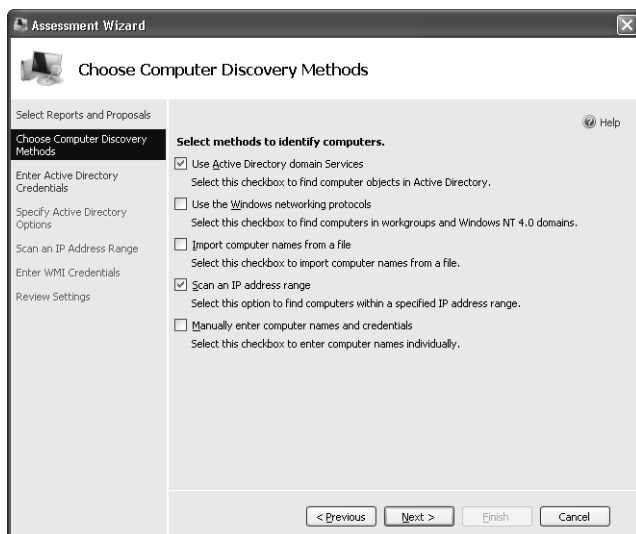


FIGURE 8-9 Specifying computer discovery methods

On the next page, we specify the Active Directory domain the target computers belong to and credentials for querying this domain. (See Figure 8-10.)

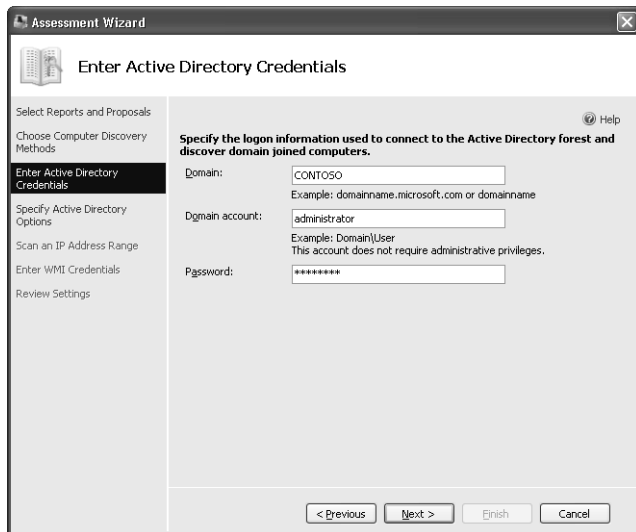


FIGURE 8-10 Specifying the domain of the target computers and credentials for connecting to the domain

On the next page, we can specify that either the entire forest be searched for computer accounts or only specified domains, containers, and organizational units. (See Figure 8-11.)

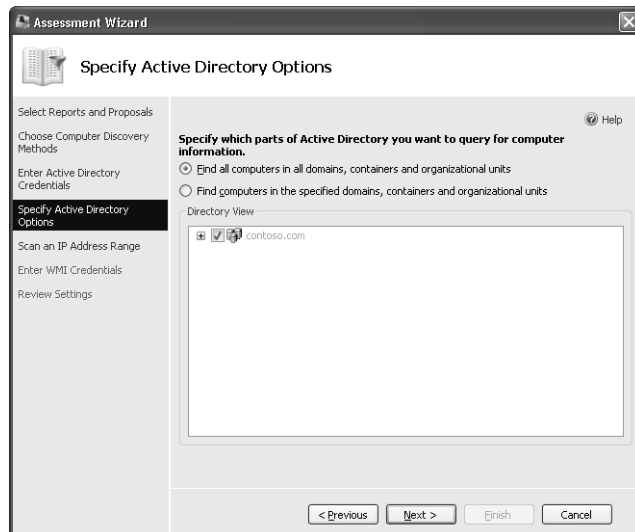


FIGURE 8-11 Specifying which parts of Active Directory to query for computer accounts

On the next page, we specify a range of IP addresses to scan for computers. (See Figure 8-12.) The MAP Toolkit will try to ping each IP address within the specified range.

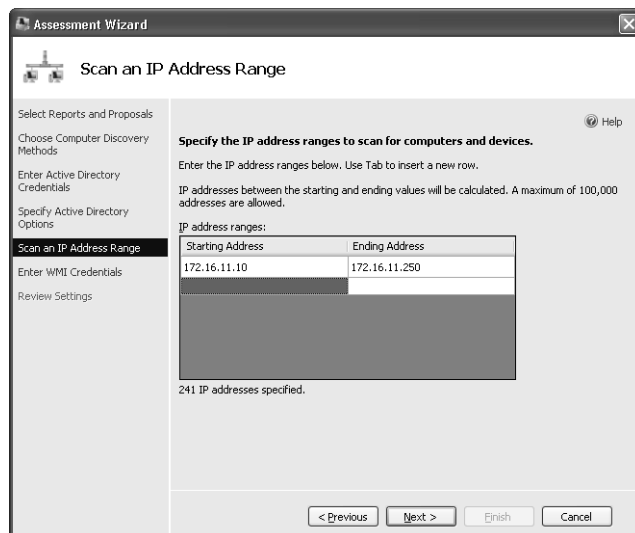


FIGURE 8-12 Specifying a range of IP addresses to scan for computers

On the next page, we are asked to specify credentials for remotely connecting to the discovered computers using WMI. (See Figure 8-13.)

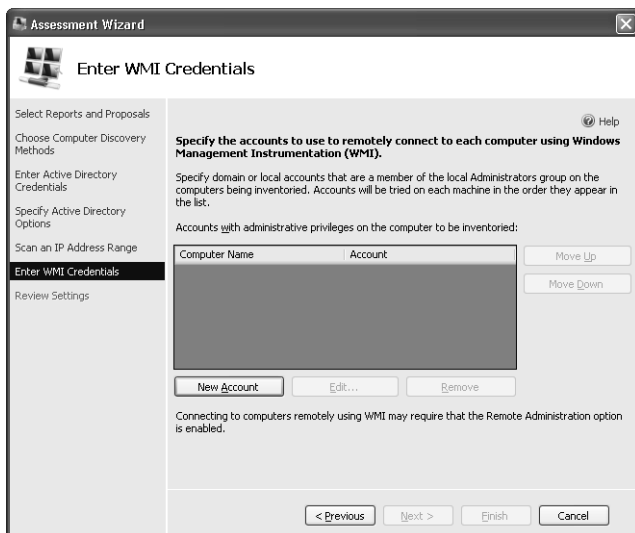


FIGURE 8-13 WMI credentials are needed to remotely connect to the discovered computers.

Clicking the New Account button brings up the Inventory Account dialog box. (See Figure 8-14.) In this dialog box, we specify the credentials of a domain or local account that should be used to remotely connect to the discovered computers using WMI.

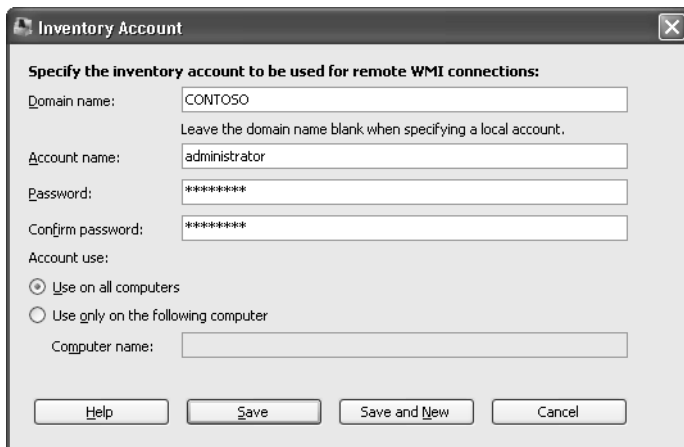


FIGURE 8-14 Specifying credentials for remotely connecting to the discovered computers using WMI

Once you've specified your WMI credentials, click Save to return to the Assessment Wizard (which is shown in Figure 8-15). You can also click Save And New to allow you to specify additional credentials, which is needed if one set of credentials will not be sufficient for remotely connecting to all target computers using WMI.

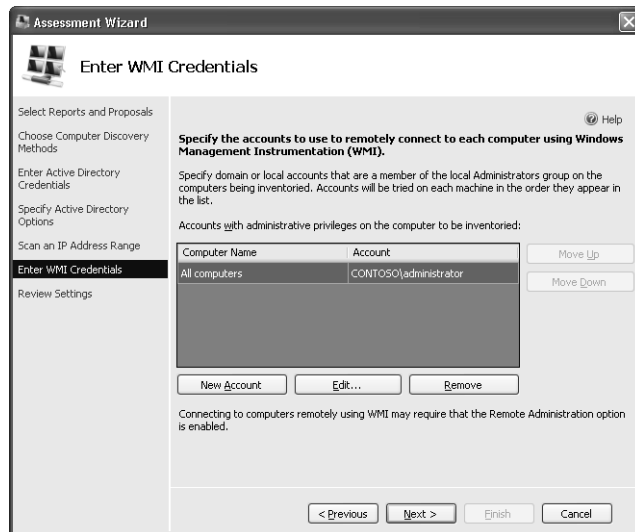


FIGURE 8-15 WMI credentials have been specified for remotely connecting to all target computers.

The final page of the wizard lets you review the settings you have specified. (See Figure 8-16.)



FIGURE 8-16 Review Settings page of the wizard.

Clicking Finish launches the assessment process, and a Status dialog box displays progress (as shown in Figure 8-17). The assessment process might take some time if you have many computers on your network or have specified a large range of IP addresses to scan for computers.

Once the assessment process has been completed, click Close to return to the MAP Solution Accelerator (shown in Figure 8-18).

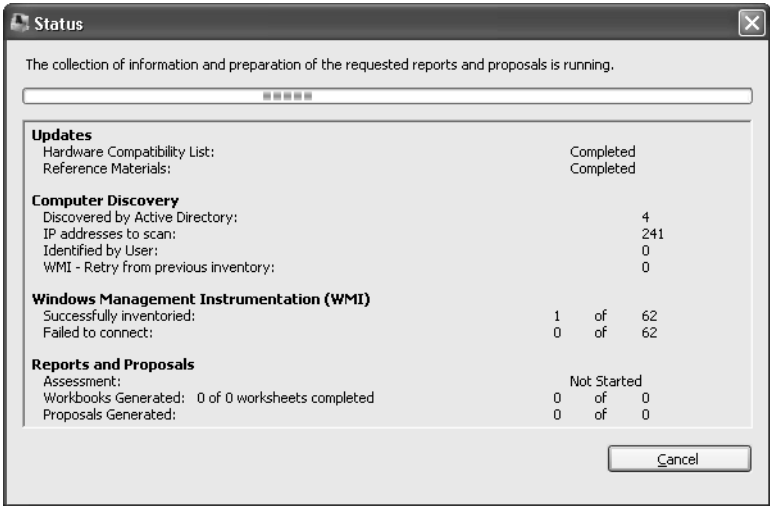


FIGURE 8-17 The assessment is underway.

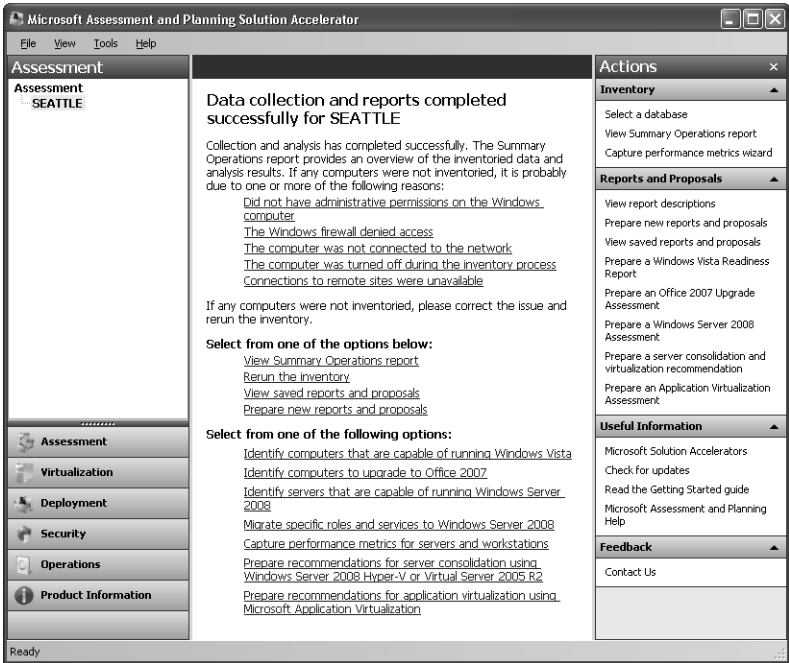


FIGURE 8-18 Click the View Saved Reports And Proposals link to view the reports generated by the assessment process.

To view the reports that were autogenerated by the assessment process, click the View Saved Reports And Proposals link in the middle pane of the MAP Toolkit as shown in Figure 8-18. Doing this opens a Windows Explorer folder that contains the proposal document (.doc file) and Excel workbook (.xls file) that were created. (See Figure 8-19.)

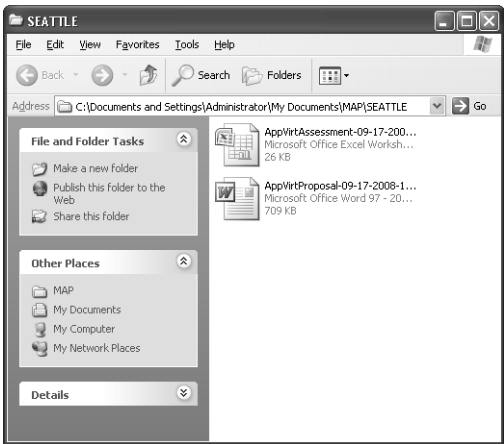


FIGURE 8-19 Proposal document and report spreadsheet created by MAP

The proposal document reviews the results of the assessment and makes recommendations (as shown in Figure 8-20).

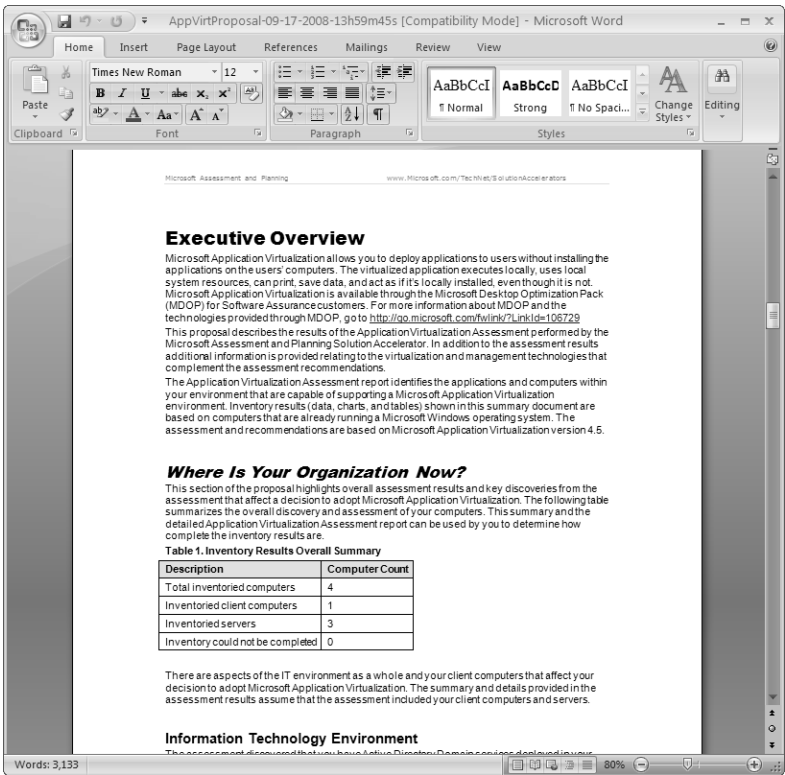


FIGURE 8-20 Proposal document with assessment results and recommendations

The Excel workbook reports the detailed results of the assessment. For example, for the Application Virtualization Assessment, this workbook has tabs that help you determine which computers are suitable for using as sequencing computers, which computers can be used for running the App-V Management Console, which computers can be used as App-V Streaming Servers, and so on. (See Figure 8-21.)

Computer Name	WMI Status	Microsoft Application Virtualization Sequencer	Reasons Not Capable
DESK103.contoso.com	Success	Capable	
SEA-DC1.contoso.com	Success	Not Capable	CPU less than 850 MHz
SEA-SRV1.contoso.com	Success	Capable	
SEA-WDS.contoso.com	Success	Not Capable	CPU less than 850 MHz

FIGURE 8-21 Excel workbook with detailed results of the Application Virtualization Assessment

For more information about how the MAP Toolkit works, see <http://www.microsoft.com/MAP>. To get a free download of this toolkit, go to <http://go.microsoft.com/fwlink/?LinkId=111000>.



Tip Another good source of news and information concerning the MAP Toolkit is the Microsoft Assessment and Planning Toolkit Team Blog found at <http://blogs.technet.com/MAPBLOG>.

Direct from the Source: Determining Hyper-V Server Virtualization Candidates

In addition to providing you with the Application Virtualization assessment feature, the MAP Toolkit can also help you determine which of your servers are suitable for Hyper-V virtualization or server consolidation. The trick is to understand that you need to conduct this in three steps (as shown in Figure 8-22):

1. Select the Windows Server 2008 Readiness And Role Migration report, and complete the server inventory.

- 2 Repeat the steps in the tool by using the Capture Performance Metrics Wizard, and monitor a selected set of servers you want to consider for consolidation.
- 3 Prepare recommendations for server consolidation.

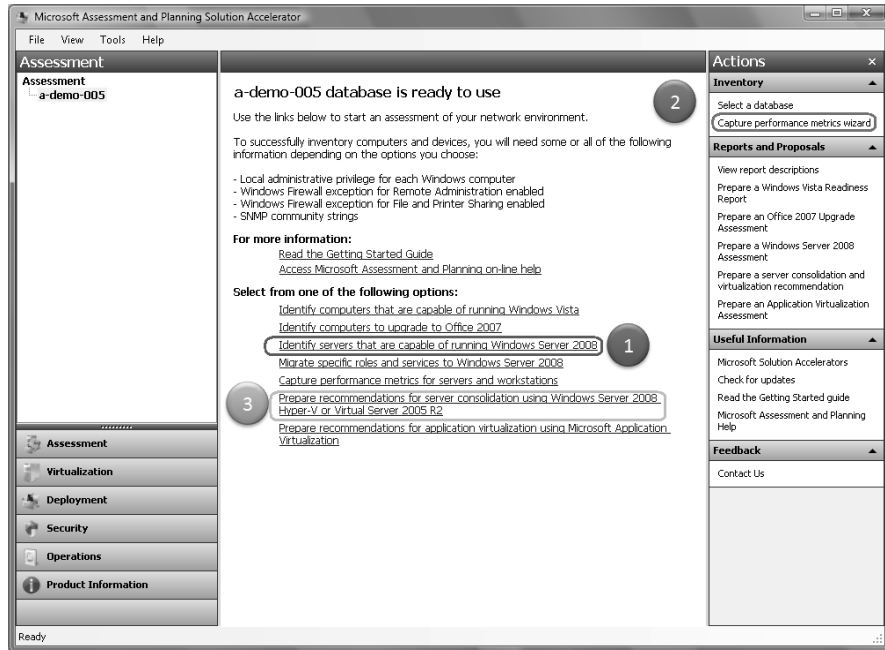


FIGURE 8-22 Three steps to use the MAP Toolkit to assess server virtualization candidates for Hyper-V

At the end of the third step, the MAP Toolkit generates a set of assessment proposals and reports showing which servers are good candidates for Hyper-V. (See Figure 8-23.)

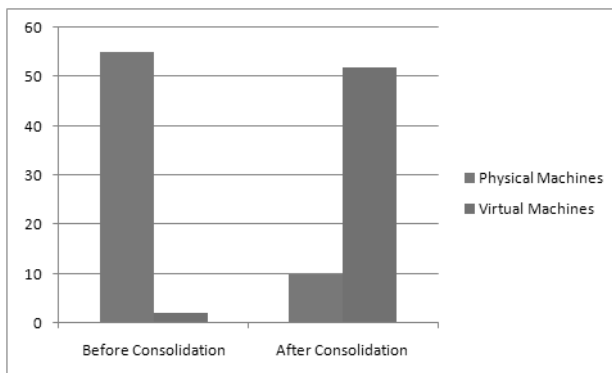


FIGURE 8-23 Autogenerated results from the MAP Toolkit for Hyper-V server consolidation

—Baldwin Ng, Senior Product Manager,
Microsoft Virtualization Solution Accelerators

Offline Virtual Machine Servicing Tool

Any company using more than a few virtual machines (VMs) will encounter the challenge of keeping virtual machines current with respect to operating system and application patches because the virtual machine might be offline for extended periods of time. As companies embrace virtualization, there will be more and more virtual machines offline, and that creates a maintenance challenge that requires an automated solution.

The Offline Virtual Machine Servicing Tool Solution Accelerator automates software updates for virtual machines that are stored in a System Center Virtual Machine Manager 2007/2008 (VMM) library. This tool works together with either System Center Configuration Manager (SCCM) 2007 or Windows Server Update Services (WSUS) to enable offline (nonrunning) virtual machines to automatically have operating system, antivirus, and application updates applied to keep them in compliance with IT policies. Because this tool uses VMM to manage virtual machines, it supports any virtual machine supported by VMM if the managed client operating system has either an SCCM or WSUS agent installed.

The Solution Accelerator (SA) provides a configuration user interface to manage the following information:

- Server designation for VMM so that the solution can connect to obtain VM information
- Server designation for the update server (either SCCM or WSUS) so that the SA can check on update status
- Groups of VMs to service
- Scheduling of servicing activity

This free tool is built on Windows Workflow Foundation and Windows PowerShell, which lends it great flexibility for tailoring to particular IT requirements. For more information about the Offline Virtual Machine Servicing Tool, see “Offline Virtual Machine Servicing Tool Executive Overview” in the Library section under Solution Accelerators on the Microsoft TechNet site at <http://technet.microsoft.com/en-ca/library/cc501231.aspx>. You can obtain this tool from the Microsoft Download Center at <http://www.microsoft.com/downloads/details.aspx?FamilyId=8408ECF5-7AFE-47EC-A697-EB433027DF73&displaylang=en>.

Other Solution Accelerators

Several other Solution Accelerators are included in both the Virtualization suite and in other suites as well:

- **Windows Server 2008 Security Guide** Provides recommendations for enhancing the security of computers running Windows Server 2008 that are members of an Active Directory domain.

- **Security Compliance Management** Provides best practices about how to plan, deploy, and monitor a security baseline and how to effectively monitor the compliance state of recommended security baselines for Windows Vista, Windows XP Service Pack 2 (SP2), and Windows Server 2003 SP2.
- **Microsoft Deployment Toolkit 2008 Update 1** Provides best practices and tools for automating desktop and server deployment of the following Microsoft Windows operating systems:
 - ❑ Windows Vista Business, Enterprise, and Ultimate (32 and 64 bit) RTM and SP1
 - ❑ Office Professional, Professional Plus, Enterprise, and Ultimate 2007
 - ❑ Windows Server 2003 R2 (32 and 64 bit)
 - ❑ Windows XP Professional with SP2 and SP3 (32 and 64 bit) or Windows XP Tablet PC Edition
 - ❑ Windows Server 2008 (32 and 64 bit)



Tip Always make sure you have the latest version of Microsoft Solution Accelerators. To receive e-mail notification when new or updated Solution Accelerators are released, use the subscription page at <http://www.microsoft.com/technet/solutionaccelerators/updates/default.msp>.

Microsoft System Center Solutions

Microsoft System Center solutions can help you manage an organization's physical and virtual infrastructure from the desktop to the datacenter. System Center solutions play a central role in Microsoft's vision for enabling IT organizations to benefit from self-managing, dynamic systems.

For the dynamic data center, System Center solutions enable

- Configuration management
- Server compliance
- End-to-end monitoring
- Data protection and recovery

For the dynamic desktop System Center solutions facilitate

- Adaptive application delivery
- Simplified Windows Vista deployment
- Endpoint security management
- Configuration compliance

- Client infrastructure monitoring
- Remote PC diagnostics and repair

Dynamic IT, Microsoft's strategy for providing critical technologies that enable IT to become more strategic, is Microsoft's vision for what an agile business looks like—where IT works closely with a business to meet the demands of a rapidly changing and adaptable environment.

System Center Management Suite Enterprise

System Center Server Management Suite Enterprise encompasses four core System Center products to provide a complete set of server management capabilities for managing applications and platforms that span both physical and virtual environments. System Center Server Management Suite Enterprise also provides the right to manage an unlimited number of operating system environments on a single virtual machine host. The four core System Center products within this suite include

- **System Center Configuration Manager 2007** A solution that comprehensively assesses, deploys, and updates servers, client computers, and devices across physical, virtual, distributed, and mobile environments. System Center Configuration Manager is optimized for Windows and is extensible so that it can control virtually any IT system.
- **System Center Operations Manager 2007** An end-to-end service-management product that works seamlessly with Microsoft software and applications, helping organizations increase efficiency while enabling greater control of their physical and virtual infrastructure.
- **System Center Data Protection Manager 2007** A solution for Windows backup and recovery that delivers continuous data protection for Microsoft application and file servers using seamlessly integrated disk and tape media.
- **System Center Virtual Machine Manager 2008** A product that allows unified management of physical and virtual machines, consolidation of underused physical servers, and rapid provisioning of new virtual machines.

System Center Essentials

System Center Essentials 2007 is specifically designed for midsize businesses with up to 500 client computers and 30 servers. It provides a unified management solution that enables midsize organizations to proactively manage their IT environment with increased efficiency. System Center Essentials provides monitoring and alert resolution for servers, clients, applications, hardware, and network devices; software distribution; update management; and software and hardware inventory.

Other System Center Products

Other System Center products include the following:

- **System Center Capacity Planner 2007** A predeployment capacity-planning and postdeployment change-analysis solution for Microsoft server applications such as Microsoft Exchange Server 2007, Windows SharePoint Services 3.0, and Microsoft Office SharePoint Server 2007. System Center Capacity Planner provides tools and guidance to deploy these servers efficiently, while also helping you plan for the future by enabling “what-if” analyses.
- **System Center Mobile Device Manager 2008** An end-to-end product for single-point access of line-of-business (LOB) applications and corporate data on devices running Windows Mobile 6.1. System Center Mobile Device Manager seamlessly provides secure access to sensitive corporate data on such devices in a seamless manner.
- **System Center Service Manager (currently in beta)** A new Microsoft System Center product designed to meet the needs of the modern IT help desk by providing capabilities for incident, problem, asset, and change management.

For more information about System Center Solutions, their benefits, how to purchase or try them out, and for partner and technical information, see the Microsoft System Center portal at <http://www.microsoft.com/systemcenter/en/us/default.aspx>.

Benefits of System Center for Virtualization

Implementing System Center solutions can have numerous direct benefits for your organization's virtualization infrastructure. For example,

- System Center Configuration Manager 2007 facilitates operating-system and application configuration management, patch management and deployment, and software upgrades for physical and virtual machines from the datacenter to the desktop.
- System Center Operations Manager 2007 provides end-to-end service management, server and application health monitoring and management, and performance reporting and analysis for physical and virtual machines.
- System Center Virtual Machine Manager 2008 allows management of virtual machines, server consolidation and resource utilization optimization, and Physical-to-Virtual (P2V) and Virtual-to-Virtual (V2V) conversions for managing your virtualized infrastructure and making more efficient use of your physical hardware resources.
- System Center Data Protection Manager 2007 provides live host-level virtual machine backup, in-guest consistency, and rapid recovery to eliminate downtime of both your physical and virtual infrastructure.

For more information about the benefits of System Center products for Microsoft virtualization environments, see <http://www.microsoft.com/virtualization/solution-product-sc.msp>.



Note System Center Data Protection Manager 2007 Service Pack 1 supports Hyper-V hosts.

Direct from the Source: Choosing a DPM 2007 Backup Solution

With Microsoft System Center Data Protection Manager (DPM) 2007, you can use disk-based storage, tape-based storage, or both. Figure 8-24 illustrates these backup solutions.

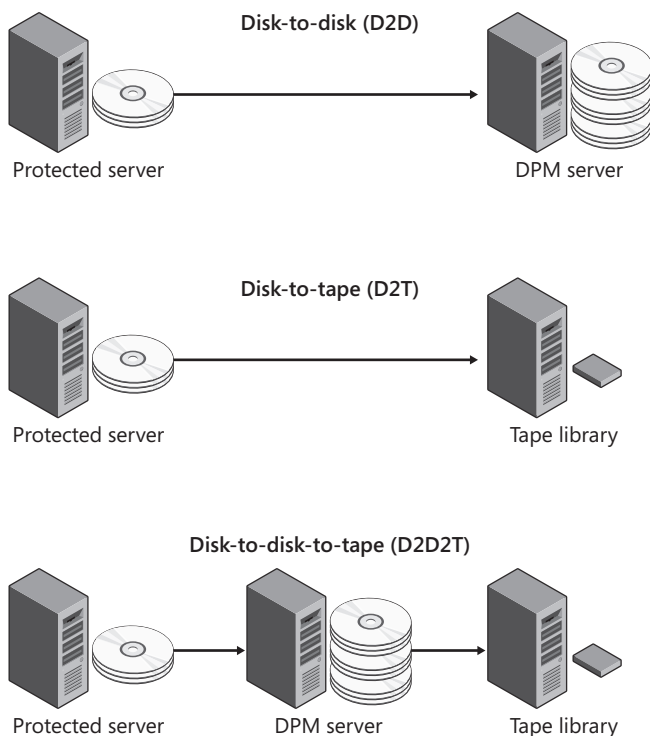


FIGURE 8-24 Backup solutions supported by DPM 2007

Tape-Based Backup and Archive

Traditional data archiving methods have relied on backing up data to tape media. This method is referred to as disk-to-tape (D2T). Tape is a popular medium for offsite storage, because magnetic tape and similar storage media offer an inexpensive and portable form of data protection that is particularly useful for long-term storage. A thorough disaster recovery plan based on tape media includes offsite storage of critical information to allow data recovery in situations where a facility is damaged or destroyed.

Using DPM, you can back up data from a server directly to tape. Data can be backed up to tape as frequently as daily for short-term protection, and it can be maintained as long as 99 years for long-term protection.

For long-term, tape-based protection, DPM backs up data from the replica in the storage pool to tape so that there is no impact on the protected server. If a file was open when the replica was synchronized last, the backup of that file from the replica will be in a crash-consistent state. A crash-consistent state of the file will contain all file data that was preserved to disk at the time of last synchronization. This applies only to file system backups. Application backups will always be consistent with the application state.

Disk-Based Protection and Recovery

With the advent of large and relatively inexpensive disk subsystems, organizations have begun to implement disk-based backup solutions, referred to as disk-to-disk (D2D). This method of backup is used to store data from one computer on the hard disk of another computer. One advantage of disk-based data protection is the potential to save time. Disk-based data protection eliminates the need to locate a specific tape required for a recovery job, load the tape, and position the tape to the correct starting point. The potential time savings and ease of use inherent in disk backup solutions encourages sending incremental data more frequently, which reduces the impact to the server being protected and on network resources. Additional benefits of this approach include

- **Increased reliability** The reliability of data recovery with disk-based data protection is also better than that of tape-based systems. Disk drives typically have much greater mean time between failure (MTBF) ratings than tape systems.
- **Faster recovery** Recovery of data from disk is quicker and easier than recovery from tape. Recovering data from disk is a simple matter of browsing through previous versions of the data on the DPM server and copying selected versions directly to the protected file server. In comparison, a typical file recovery from tape takes hours, which can be costly, and administrators in a medium-size datacenter can usually expect to perform 10 to 20 or more of these recoveries each month.

Using DPM and disk-based data protection, data can be synchronized as frequently as every 15 minutes and maintained as long as 64 days with 1 recovery point per day.

Combining Disk and Tape Backup Methods

You can also back up data from a disk-based replica. Often referred to as D2D2T or “disk-to-disk-to-tape,” this method combines the ease of use inherent to disk-based backup with the long-term and offsite storage capabilities of tape media by replicating data to disk for subsequent backup to tape. The primary advantage to this method is that the tape backup operation can occur at any time with no impact on the server that is being protected.

DPM allows administrators to schedule disk-based replication and backup to tape, providing the flexibility to create focused, detailed backup strategies that result in efficient

and economic data protection. When you need to restore a single file or an entire server, recovery is typically fast and simple, because once you identify the data to be restored, DPM locates the data and retrieves it from the disk-based replica. Should a disk replica fail, tape backups can be used to restore the replica and resume protection.

Determining Which Storage Method to Use

To determine which storage method to use, you must consider the relative importance of your organization's protection requirements.

- **How much data your organization can afford to lose** Realistically, not all data is equally valuable. Organizations must weigh the impact of loss against the costs of protection.
- **How quickly recovered data must be available** Recovery of data that is critical to ongoing operations will typically be more urgent than routine data. On the other hand, organizations should identify servers providing essential services during working hours that must not be disrupted by recovery operations.
- **How long your organization must maintain data** Long-term storage might be necessary for business operations, depending on the type and contents of the data. An organization might also be subject to legal requirements for data retention.
- **How much your organization can spend on data protection** When considering how much to invest in data protection, organizations must include not only the cost of hardware and media, but also the personnel costs for administration, management, and support.

—CSS Global Technical Readiness Team (GTR)

Virtualization Licensing

The bottom line businesses have to consider when making their purchasing decisions is cost. With the rapid growth and evolution of virtualization technologies, businesses see virtualization more and more as an essential component of their overall IT planning. Microsoft is of course aware of all this, and over the last few years Microsoft has been competitively evolving their licensing model for its virtualization technologies to address the changing needs of businesses in this area. Let's briefly look at how Microsoft virtualization licensing has evolved and how Microsoft virtualization solutions are licensed today.



Important This discussion of virtualization licensing is for informational purposes and is presented "as is" with no warranties. The information presented in this section is not meant to replace individual licensing agreements and should not be relied upon for compliance with official Microsoft licensing policies. For authoritative information concerning Microsoft licensing, see <http://www.microsoft.com/licensing>.

The Evolution of Microsoft Virtualization Licensing

In the fall of 2005, Microsoft made some important changes to its licensing of the use of virtualization products. These changes were primarily intended to address customer issues concerning maintaining a library of inactive (nonrunning) virtual machines. Before this change, a customer needed to purchase a license for a virtual machine even if the virtual machine was not running. This prevented many customers from effectively using virtual machines as “hot spares” or using them as backups for business-continuity purposes. In response to customer requests, Microsoft changed the licensing of its products so that only running virtual machines needed licenses. This change allowed customers to maintain a library of multiple inactive virtual machines on a storage area network (SAN) while only having to purchase licenses for running machines.

Then, in 2006, Microsoft made additional licensing changes in the area of virtualization. These changes included giving licensed users of Windows Server Enterprise Edition the right to run up to four virtual instances of the operating system at no additional cost over licensing a single physical instance of the operating system, and giving licensed users of Windows Server Datacenter Edition the right to run an unlimited number of virtual instances of the operating system. These licensing changes initially applied to Windows Server 2003 R2 and were later extended to Windows Server 2008. Similar licensing flexibility was also added for Microsoft SQL Server Enterprise Edition.

Further changes in 2007 to Microsoft’s server-based licensing for its Microsoft Hyper-V and Microsoft Virtual Server R2 SP1 virtualization platforms now allow customers to create and store multiple virtual machines while licensing only active instances of these machines. Deployment of virtual machines is simplified by decoupling licenses from a specific guest operating system, allowing customers to move active instances of a virtual machine from one licensed physical host server to another with no additional cost. In addition, Microsoft Server products are now licensed by processor, which enables customers to run multiple virtual instances of these products on a single physical host while licensing each instance by the number of virtual processors it uses, instead of by the number of physical processors on the host.

And most recently, in August 2008, Microsoft provided increased value and greater flexibility to customers through further changes to its virtualization licensing by updating its software licensing terms for over 40 of its server applications. These changes include waiving the previous 90-day reassignment rule to now allow customers to reassign licenses from one server to another within a server farm as often as might be needed. This change will reduce the number of licenses customers will require to support their IT systems and simplify the tracking of application instances or processors, because customers now can count licenses by server farm instead of by server. For more information on this latest change to Microsoft virtualization licensing, see “New Microsoft Licensing and Support Eases Path to Virtualization” on the Microsoft PressPass site at <https://www.microsoft.com/presspass/press/2008/08/08-19EasyPathPR.mspx>.

Licensing Terminology

The following is key terminology you need to be familiar with to understand how Microsoft Volume Licensing agreements work:

- **Server** A physical hardware system capable of running server software. Note that a hardware partition or blade is considered to be a separate physical hardware system and is therefore also a separate server
- **Instance** An instance of software is the set of files that make up the software, stored in executable form and ready to run. You create an instance of software by installing the software or by duplicating an existing instance. Instances of software can run on physical or virtual hardware systems.
- **Running instance** You run an instance of software by loading it into memory and executing its instructions. After this is done, the instance is considered to be running (regardless of whether or not its instructions continue to execute) until the instance is removed from memory.
- **Assigning a license** You assign a license by designating that license for one device or user. Such designation avoids sharing the license across more than one device or user at the same time. For example, once you have assigned a software license to a server, you are allowed to run the software on that server. You can use any method you want to ensure you have the correct number of licenses to cover your software use—in other words, ensuring you have assigned the correct type and number of licenses to your devices or users is your responsibility.
- **Operating system environment** An instance of an operating system, including any applications configured to run on it. Two types of operating system environments (OSEs) exist: physical and virtual. A physical OSE is configured to run directly on a physical hardware system. A virtual OSE is configured to run on a virtual (or otherwise emulated) hardware system.
- **Physical processor** A processor in a physical hardware system. Physical OSEs use physical processors.
- **Virtual processor** A processor in a virtual (or otherwise emulated) hardware system. Virtual OSEs use virtual processors. For licensing purposes, a virtual processor contains the same number of cores and threads as its underlying physical hardware system.
- **Client Access License** CALs are required for users or devices to connect to a server and are specific to a version of a product. This means you cannot use Windows Server 2003 CALs to connect to a Windows Server 2008 instance, and vice versa. Both Windows Server 2003 and Windows Server 2008 Standard and Enterprise Editions are licensed per server plus CALs. Windows Server 2003 and Windows Server 2008 Datacenter Edition are licensed by processor plus CALs.

- **System Center Server Management Suite Licenses** These include Virtual Machine Manager (VMM) as well as Enterprise Management Licenses (EMLs) for System Center 2007 Configuration Manager, Data Protection Manager, and Operations Manager. An Enterprise license provides rights to manage both the physical and virtualized instances running on a server. A Standard license provides rights to manage only the operating system and the hardware.

License Pricing

Table 8-1 lists server licensing pricing information in US dollars for Windows Server 2008 with Hyper-V as of February 2008. Note that licensing pricing information is subject to change at any time—individual volume licensing agreements might also differ.

TABLE 8-1 Server Licensing Pricing Information for Windows Server 2008 with Hyper-V

License Type	Number of VMs	Open License Pricing
Standard	1 physical and 1 virtual	\$719
Enterprise	4	\$2,334
Datacenter	Unlimited	\$2,381

Table 8-2 lists licensing pricing information in US dollars for System Center Server Management Suite Licenses as of February 2008. Note that licensing pricing information is subject to change at any time—individual volume licensing agreements might also differ.

TABLE 8-2 Licensing Pricing Information for System Center Server Management Suite Licenses

Applications Included	Open License Pricing
Virtual Machine Manager 2007	\$1,290, which includes the license plus two years of Software Assurance. Software Assurance is required to license the Server Management Suites. Price also includes the rights to manage unlimited OSEs on a single server.
Operations Manager 2007	
Configuration Manager 2007	
Data Protection Manager 2007	

Volume Licensing Briefs

For detailed information concerning volume licensing of Microsoft products, a good source to go to are the volume licensing briefs found on the Microsoft Volume Licensing site at <https://www.microsoft.com/licensing/resources/volbrief.aspx>. For IT decision makers looking for information concerning licensing of virtualization technologies, the following briefs are helpful:

- **Licensing Microsoft Server Products in Virtual Environments** Overview of Microsoft licensing models for server operating systems and server applications in virtual environments.

- **Licensing Microsoft Windows Server 2003 R2 to Run with Virtualization Technologies** Discusses how Microsoft Windows Server 2003 R2 and other Microsoft server products are licensed when they are used with other virtualization technologies.
- **Application Server License Mobility** Explains how you can take advantage of virtualization technologies by reassigning licenses across servers within a server farm. This applies to software licenses for certain server applications and all external connector licenses.
- **Licensing Windows Vista for Use with Virtual Machine Technologies** Overview of how to use Windows Vista operating system products with virtual machine technologies such as Microsoft Virtual PC and Windows Vista Enterprise Centralized Desktop (VECD).
- **Per-Processor Server Licensing Changes** Guide to server licensing changes in the per-processor model that includes sample customer scenarios.
- **Multicore and Hyperthreaded Processor Licensing** Clarifies existing Microsoft licensing policies for multicore and hyperthreaded processors.
- **Licensing Windows Server 2008 Terminal Services** Clarifies Microsoft licensing policies for Windows Server Terminal Services, including the components that are in the Windows Server 2008 operating system.



Note Microsoft Application Virtualization (App-V) is part of the Microsoft Desktop Optimization Pack (MDOP) for Software Assurance and is licensed accordingly. For more information about Microsoft's Software Assurance program, see <https://www.microsoft.com/licensing/sa/default.aspx>.

Conclusion

This book has provided you with an overview of Microsoft's integrated vision for virtualization from the desktop to the datacenter, a vision known as Virtualization 360. Microsoft virtualization solutions such as Hyper-V, VMM 2008, App-V, MED-V, VDI, Terminal Services, and Windows Vista Roaming Desktop can provide numerous benefits to businesses of all sizes. While this book has tried to provide as up to date a view as possible of Microsoft virtualization technologies and solutions, these technologies and solutions continue to evolve as Microsoft seeks to provide customers with more flexible solutions for implementing and managing virtual infrastructures.

The benefits of virtualization are many and clear, so get virtual now—see <http://www.microsoft.com/virtualization/getvirtualnow.aspx> for an event happening near you.

Resources

The resources listed in this section were either referred to in the chapter or provide additional information concerning concepts and products discussed in this chapter.

General

For information about the Microsoft Virtualization Launch events, see <http://www.microsoft.com/virtualization/getvirtualnow.aspx>. On this page, you can also find links to recordings of keynote talks from the September 8 kickoff event.

Microsoft Solution Accelerators

For more information concerning all current available Microsoft Solution Accelerators, see <http://technet.microsoft.com/en-us/solutionaccelerators/default.aspx>.

To receive e-mail notification when new or updated Solution Accelerators are released, use the subscription page at <http://www.microsoft.com/technet/solutionaccelerators/updates/default.aspx>.

Microsoft Infrastructure Planning and Design Guides

The IPD guides are published in the Library section under Infrastructure Planning and Design on Microsoft TechNet at <http://technet.microsoft.com/en-us/library/cc196387.aspx>. You can quickly access these guides through the shortcut URL of <http://www.microsoft.com/IPD>, where you can also download the full series of IPD guides as the zipped archive named "IPD - All.zip". Alternatively, you can download only the guides you need from this same URL.

Additional IPD series guides will be made available as beta releases on the Microsoft Connect site at <http://connect.microsoft.com>.

Microsoft Assessment and Planning Toolkit

You can download the MAP Toolkit 3.1 from the Microsoft Download Center for either x64 or x86 hardware platforms at <http://www.microsoft.com/downloads/details.aspx?FamilyID=67240b76-3148-4e49-943d-4d9ea7f77730&DisplayLang=en>. You can also quickly access the user guides through the shortcut URL <http://www.microsoft.com/MAP>.

Offline Virtual Machine Servicing Tool

For more information about the Offline Virtual Machine Servicing Tool, see Offline Virtual Machine Servicing Tool Executive Overview in the Library section under Resources For IT Professionals on the Microsoft TechNet site at <http://technet.microsoft.com/en-ca/library/cc501231.aspx>.

You can obtain the Offline Virtual Machine Servicing Tool from the Microsoft Download Center at <http://www.microsoft.com/downloads/details.aspx?FamilyId=8408ECF5-7AFE-47EC-A697-EB433027DF73&displaylang=en>.

Microsoft System Center Solutions

For more information about System Center Solutions, their benefits, how to purchase or try them out, and for partner and technical information, see the Microsoft System Center portal at <http://www.microsoft.com/systemcenter/en/us/default.aspx>.

For more information about the benefits of System Center products for Microsoft virtualization environments, see <http://www.microsoft.com/virtualization/solution-product-sc.mspx>.

Virtualization Licensing

For authoritative information concerning Microsoft licensing, see <http://www.microsoft.com/licensing>.

For detailed information concerning volume licensing of Microsoft products, a good source to go to are the volume licensing briefs found on the Microsoft Volume Licensing site at <https://www.microsoft.com/licensing/resources/volbrief.mspx>.

For more information about Microsoft's Software Assurance program, see <https://www.microsoft.com/licensing/sa/default.mspx>.

Index

A

- access speed (servers)
 - for Hyper-V, 44
 - for VMM 2008, 109
- access to terminal servers, 266
- access to virtual applications, managing, 212
- accounts, configuring for roaming profiles, 352
- Action menu (Virtual Machine Connection), 58
- Actions tab (virtual machine properties), 151
- Active Directory Domain Services (ADDS)
 - with MED-V, 316
 - with virtual applications groups, 216
- Active Directory Service Interface (ADSI), 200
 - configuring accounts for roaming profiles, 352
- Active Directory Users and Computers console, 276
 - configuring accounts for roaming profiles, 352
- Active state (virtual machines), 32
- Active Upgrade (App-V), 181
- Add Hardware setting (virtual machines), 53
- Add Roles Wizard, 260
- ADDS (Active Directory Domain Services)
 - with MED-V, 316
 - with virtual applications groups, 216
- Administration view (VMM Administrative Console), 116
- Administrator Console, VMM, 92, 98–100, 114–116
 - adding Library Servers, 134
 - connecting to virtual machines with, 150, 152–154
 - filters, 116
 - installing, 92, 111
 - managed hosts (VMM). *See* managed hosts (VMM)
 - managing Microsoft VDI, 333
 - managing virtual machines, 149–151
 - supported operating systems, 108
 - views, 115–116
- Administrator role, 161
- Administrators node (Management Console), 222
- ADO.NET, 104
- ADSI (Active Directory Service Interface), 200
 - configuring accounts for roaming profiles, 352
- Advanced folder redirection, 362
- All Hosts section (Hosts view), 118
- All Users profile, 341
- allocating CPU resources for virtual machine, 71
- AllSigned security context (Windows PowerShell), 97
- Always Automatically Turn On The Virtual Machine setting, 151
- antivirus software, Hyper-V and, 44
- anywhere-access scenario, 16
- App-V, 5, 181–244
 - additional resources on, 243
 - architecture of, 199–201
 - components of, 190–199
 - console for. *See* App-V Management Console
 - deployment resources, 244
 - deployment scenarios, 202–209
 - how it works, 183–190
 - key benefits of, 242
 - key features of, 239–242
 - Microsoft VDI, integrated with, 330
 - mobile worker scenario, 14
 - obtaining, 211
 - office worker scenario, 15
 - terminology of, 181–183
 - using Streaming Server, 183, 196, 203, 209–211
 - adding IIS to, 210
 - App-V Clients, 198, 234–237
 - installing, 199
 - App-V Data Store, 195
 - App-V Desktop Client, 182, 198
 - App-V for Terminal Services, 182, 241
 - App-V Management Console, 182, 196, 211–222
 - administrators, 222
 - application licenses, 218
 - applications, managing, 211–217
 - file type associations, 221
 - packages, managing, 217
 - provider policies, 221
 - reports, 220
 - servers, managing, 219
 - App-V Management Server, 182, 191–192
 - installing, 191
 - publishing on. *See* publishing applications
 - App-V Management Web Service, installing, 195
 - App-V Management Web Services, 195
 - App-V Sequencer, 182, 188, 197, 222–234
 - Q: drive, using, 182, 231–234
 - App-V Sequencer Console, 222, 227
 - App-V servers, managing, 219
 - App-V Streaming Server. *See* Streaming Server
 - App-V Terminal Services Client, 199, 209
 - App-V troubleshooting, 237–239
 - AppData subfolder (user profiles), 341, 345, 347
 - application context for Windows PowerShell, 98
 - Application Data folder, redirecting, 358
 - application deployment, Terminal Services and, 306
 - application groups, 216–217
 - application incompatibility, 3, 10
 - Application Licenses node (Management Console), 218
 - application management life cycle, 187–190
 - application presentation, decoupling. *See* presentation
 - virtualization; Terminal Services
 - Application Source Root (ASR), 241
 - Application Utilization report, 220
 - application virtualization, 5. *See also* Microsoft Application Virtualization (App-V)
 - Application Virtualization for Terminal Services, 182, 241
 - Applications node (App-V Management Console), 211–217
 - Applications node (Application Virtualization Client console), 234
 - Applist.xml, 211
 - Apply action (Snapshots pane), 69
 - Applying Snapshot state (virtual machines), 32
 - ASR (Application Source Root), 241
 - Assessment and Planning Toolkit, 414
 - assigning a license, defined, 411
 - authentication
 - Hyper-V Manager and VMConnect, 60
 - terminal servers, 262, 265, 267

418 auto offline mode (Offline Files)

- auto offline mode (Offline Files), 371
- automatic remediation (PRO), 102
- Automatic Start Action setting (virtual machines), 55
- Automatic Stop Action setting (virtual machines), 55
- automatic synchronization with Offline Files, 372
- Automatically Turn On The Virtual Machine If It Was Running When Virtual Server Stopped setting, 151
- availability
 - failover clustering with VMM 2008, 174
 - of file shares, 73
 - VMM Library Server, 110
- .avhd files, 69

B

- Background Intelligent Transfer Service (BITS), 324
- backup and recovery, 10
 - cloning virtual machines as backups, 157
 - Data Protection Manager 2007 solution for, 407–409
 - Terminal Services licensing data, 264
 - virtual applications, 241
 - VMM 2008 database, 137–139
- Basic folder redirection, 362
- Basic IT infrastructure, 8
 - advancing to Standardized infrastructure, 10
- benefits of virtualization, 7–16
 - to business, 9–11
 - to IT professionals, 12, 13
- BIOS classes (WMI), 76
- BIOS setting (virtual machines), 53
- BITS (Background Intelligent Transfer Service), 324
- black-hole protection, 303
- blogs
 - App-V, 244
 - Hyper-V, 85
 - Terminal Services, 311
 - user state virtualization, 383
 - VMM 2008, 180
- branch office scenario, 207, 307, 369
- business benefits to virtualization, 9–11
- business continuity, 10
 - with MED-V, 325
- business continuity scenarios, 82, 179

C

- CAL. *See* licensing
- cameras, plug-and-play redirection for, 249
- candidates for virtualization, Hyper-V servers as, 401
- Capacity Planner 2007, 406
- centralized management, MED-V, 316
- certificates for terminal server authentication, 267
- Change History tab (App-V Sequencer Console), 228
- Checkpoints tab (virtual machine properties), 151
- child partitions, 30, 35–37
 - creating new, 46, 61–65, 73
 - Hyper-V network model, 51
- Citrix Desktop Delivery Controller, 329
- Citrix XenDesktop, 329
- Citrix XenServer, 25
- ClearType font smoothing, with RDC, 248
- client access licenses. *See* licensing

- client-based desktop virtualization, 313. *See also* MED-V Client Layer, VMM, 95–103
- clipboard behavior, MED-V usage policies on, 323
- Clipboard menu (Virtual Machine Connection), 58
- cloning virtual machines, 157
- clustering (PRO), 102
- cmdlets, 96. *See also* Windows PowerShell
- CodePlex Project, 76
- Collaboration suite (Solution Accelerators), 386
- COM 1 and COM 2 settings (virtual machines), 54
- command-line tools for Terminal Services, 277
- commitment to virtualization (Microsoft's), 18
- communication within VMM layers, 93
- communications ports
 - for App-V, 201
 - for VMM, 94, 152
- compacting virtual hard disks, 50, 71
- compatibility problems, 3, 10, 188, 190
 - App-V and, 186
- compression, ring, 39
- concurrent licenses, 219
- Configuration Manager 2007, 406
- confix.xml file, 66
- conflicts, application, 188, 190
- conflicts, Offline Files synchronization, 373
- Connect action (Hyper-V Manager), 52
- connecting to virtual machines, 152
 - with Hyper-V. *See* Virtual Machine Connection tool
 - with Hyper-V (Virtual Machine Connection Tool), 59, 62
 - with VMM Administrator Console, 150, 152–154
- Connection Authorization Policy, Terminal Services (TS CAP), 300
- connection status, managed hosts, 122
- connections to TS Web Access servers, 292
- connections to virtual applications, 221
- connectivity for virtual networks, 50
- consolidation of servers, 10, 176
- consolidation of servers scenarios, 82, 178
- Contacts subfolder (user profiles), 344
- Content folder (virtual applications), 181, 191, 192–194
 - accessed by Management Server, 191
 - accessed by Streaming Server, 195
 - outsourcing, 194
- contract/offshore worker worker scenarios, 15, 326, 335
- contractors, single account for, 348
- controlled partner access scenario, Terminal Services, 308
- conversions, 176. *See also* P2V conversions; V2V conversions
- Convert action (virtual hard disks), 51
- Convert Physical Server (P2V) Wizard, 159
- Core VDevs, 33
- cost savings. *See* business benefits to virtualization
- CPU resource allocation with virtual machines, 71
- Create A Folder For Each User Under The Root Path option (Basic redirection), 363
- credentials
 - for connecting to virtual machines, 48, 152
 - lost when updating VMM, 112
 - terminal servers, 266
 - virtual applications, 218
 - VMware ESX Server hosts, 132
- CSC settings for RUP/FR, 380
- Custom Properties tab (virtual machine properties), 151
- Custom tab (managed hosts), 126
- customized desktops, 348

D

Data Protection Manager 2007, 406–409

Data Store, App-V, 195

data transfer control, MED-V, 316, 323

DCOM (Distributed Component Object Model), 93

Default Location for Virtual Hard Disks setting (Hyper-V Manager), 47

Default Location for Virtual Machine Configuration Files setting (Hyper-V Manager), 47

default network user profiles, 350

Default Server Group (App-V), 219

defense in depth, 27, 29

delegated administration of virtual machines, 175, 177

Delegated Administrator role, 162–164

Delete Saved Credentials setting (Hyper-V Manager), 48

Delete Snapshot action (Snapshots pane), 69

Delete Snapshot Tree action (Snapshots pane), 69

Deleting Snapshot state (virtual machines), 32

deleting virtual applications, 234

DEP (Data Execution Prevention), 38

deploying. *See also* installing

- App-V
 - resources on, 244
 - scenarios for, 202–209
- in application management life cycle, 187
- applications, Terminal Services and, 306
- Hyper-V, resources on, 84
- MED-V packages, 320
- Microsoft VDI, 336
- RemoteApp programs, 284–290
 - via Web browser. *See* TS Web Access
- Terminal Services, 309
- TS Gateway server, 300
- virtual machines with VMM 2008, 154
- VMM 2008, 105, 107, 180

Deployment tab (App-V Sequencer Console), 228

deprivileging, ring, 39

designs for operations, 12

Desktop Client, App-V, 182, 198

Desktop Experience feature, 249

Desktop folder, redirecting, 358

Desktop Optimization Pack (MDOP), 337

Desktop subfolder (user profiles), 344

Desktop suite (Solution Accelerators), 385

desktop virtualization, 5, 313–338

- additional resources on, 337
- basics of, 313
- MED-V. *See* MED-V (Microsoft Enterprise Desktop Virtualization)
- MED-V compared to VDI, 328
- VDI. *See* VDI (Virtual Desktop Infrastructure)

Details pane (managed hosts), 128

device drivers, virtualized, 24

device redirection, 249, 251

devices, virtualized, 24. *See also* virtual devices (VDevs)

Diagram view (VMM Administrative Console), 116

differential SFTs, 241

digital cameras, plug-and-play redirection for, 249

disabling virtual machines, 150

disaster recovery scenario, Hyper-V, 82. *See also* backup and recovery

discarding virtual machine state, 149

disk backups, 408–409. *See also* backup and recovery

disk space

- connecting storage to virtual machines, 62
- desktop refresh cycle rate (VDI), 336
- Hyper-V options for, 61
- Offline Files in Windows Vista, 370
- reducing with virtualization, 10
- server virtualization, 24
- tape and disk backups, 407–409
- for virtual machines, 61

Disk Usage tab (Offline Files applet), 378

Diskette Drive option (Media menu), 58

Diskette Drive setting (virtual machines), 54

display, virtual machine, 71

display data prioritization (RDC), 248

display support with RDC, 247

Distributed Component Object Model (DCOM), 93

Documents subfolder (user profiles), 341, 344

domain controllers with virtual machines, 73

Downloads subfolder (user profiles), 344

DPM 2007, 406–409

DSC (Dynamic Suite Composition), 182, 240

DVD Drive option (Media menu), 58

dynamic architecture, Microsoft VDI in, 331

Dynamic Data Center scenario (Hyper-V), 83

Dynamic IT, 8, 11, 21

dynamic provisioning, 11

Dynamic Suite Composition (DSC), 182, 240

dynamic VDI deployment architecture, 336

E

EasyPrint, Terminal Services, 253–256

Edit Disk action (virtual hard disks), 50

editing snapshots, 70

8.3 directory names when sequencing applications, 232

electronic software distribution. *See* ESD system, publishing applications using

EMLs (Enterprise Management Licenses), 412

emulated devices, 33

Enable Virtual LAN Identification For Parent Partition option, 49

encryption

- of communications over VMRC connections, 153
- Offline Files in Windows Vista, 370, 378
- terminal server connections, 268

Encryption tab (Offline Files applet), 378

Engine Layer, VMM, 103

- communications ports, 94
- interlayer communication, 93

enlightenments, 36

enterprise computing, trend toward virtualization, 2

Enterprise Desktop Virtualization (MED-V). *See* MED-V

Enterprise Edition, Windows Vista, 337

Enterprise Management Licenses (EMLs), 412

Environment tab (Active Directory Users and Computers), 276

ESD system, publishing applications using, 185, 202, 207

Essentials, System Center, 405

ESX Server hosts, adding, 130

Ethernet speed. *See* server speed

execution policy, Windows PowerShell, 97

.exp (export) files, 67

Expand action (virtual hard disks), 51

expiring virtual images, 324

exporting virtual machines, 65–67, 71

extensibility of Hyper-V, 79
 external virtual networks, configuring, 49

F

failover clustering with VMM 2008, 174
 VMM Library Server, 110
 Favorites subfolder (user profiles), 341, 345
 file associations for virtual applications, 214, 221
 File menu (Virtual Machine Connection), 57
 file server for streaming application packages. *See* SMB protocol
 for streaming application packages
 file share availability, 73
 file type associations for virtual applications, 214, 221, 235
 File Type Associations node (Application Virtualization Client
 console), 235
 File Type Associations node (Management Console), 221
 Files tab (App-V Sequencer Console), 229
 filters (VMM Administrator Console), 116
 FIPS-compliant encryption, 268
 fixed-size virtual hard disks
 configuring, 71
 converting virtual disk to, 51
 floppy disks, virtual, 47
 Folder Redirection (FR). *See* FR (Folder Redirection)
 font smoothing, with RDC, 248
 forums, TechNet. *See* TechNet forums and webcasts
 FR (Folder Redirection), 6, 358–366. *See also* Vista Roaming
 Desktop
 full infrastructure, App-V, 243
 Full Screen Mode option (View menu), 58

G

Gateway, Terminal Services. *See* TS Gateway
 General tab (Offline Files applet), 377
 General tab (virtual machine properties), 151
 Get-ExecutionPolicy cmdlet, 97
 Get-WmiObject cmdlet (Windows PowerShell), 77
 globalization features, App-V, 241
 Group Policy
 configuring accounts for roaming profiles, 352
 deploying RemoteApp programs, 286
 Folder Redirection (FR), 361
 Offline Files, 375, 378
 terminal server management, 278
 terminal server security, 268
 Groups feature, Terminal Services Manager, 274
 guest operating systems, 25, 39
 accessing with remote control, 152
 enlightened, 36
 network adapters with. *See* network adapters
 profiles for, 89, 135
 adding (creating), 136
 updating VMM and, 112
 that don't support Integration Services, 35
 where installed, 61

H

hard disks, virtual, 135
 creating new, 47

 creating virtual machines with, 63
 default locations for .vhd files, 70
 for guest operating systems, 61
 making changes to, 50
 hardware-assisted virtualization, 38, 39
 Hardware Configuration tab (virtual machine properties), 151
 hardware profiles, 89, 135
 adding (creating), 135
 updating VMM and, 112
 hardware requirements
 disk storage space, 61
 Hyper-V platform, 43
 network adapters, 49
 VMM (Virtual Machine Manager), 107
 hardware settings, virtual machines, 53, 143
 Hardware tab (managed hosts), 124
 health-based decisions (PRO), 102
 heartbeat, 36
 hidden files, making visible, 341
 host agents (VMM), 105
 installing, 119
 reassociating, 120
 updating, 120
 host clusters, managing (VMM), 129
 placing new VM on, 140
 host computer, 25
 host groups, 117–119
 automatic placement of virtual machines, 154
 host operating system, 136
 hosted virtualization, 26
 hosts
 adding to/removing from host groups, 119
 communication ports for, 95
 defined, 89
 displaying virtual machines on, 145
 load balancing, 102
 migrating virtual machines between, 65, 71, 79, 154–157
 supported operating systems, 108
 Hosts section (Hosts view), 118
 Hosts view (VMM Administrative Console), 115, 117
 HTTP protocol, 200
 loading .sft files, 193
 HTTPS protocol, 93, 200
 loading .sft files, 193
 Hyper-V controllers, 62
 Hyper-V Manager console, 45–56
 exporting and importing VMs, 65–67
 managing Microsoft VDI, 332
 working with snapshots, 67–69
 Hyper-V platform, 4, 23–87. *See also* server virtualization
 additional resources on, 83–87
 architecture of, 23–37, 79
 child partitions, 35–37
 parent partition, 30–35
 controlling virtual machines on, 152
 creating virtual machine, 61–65
 determining virtualization candidates, 401
 installing, 42–45
 Integration Services functionality, 41
 key benefits of, 81
 key features, 79–81
 managing with VMM 2008, 173
 with Microsoft VDI, 328

Hyper-V platform (*continued*)

- migrating virtual machines with, 65, 71, 79
 - storing Hyper-V configuration files, 64
 - supported guest operating systems, 39
 - system requirements, 37–39, 43
 - tools for managing, 74–78
 - as Type 1 hypervisor, 25
 - usage scenarios, 82
 - using Hyper-V Manager. *See* Hyper-V Manager console
 - V2V (virtual-to-virtual) conversions, 90, 160
 - Virtual Machine Connection tool, 56–60
 - working with virtual machines, 65–73
- Hyper-V RTM Update Package, 42
- Hyper-V servers
- candidates for virtualization, 401
 - managing, 46–51
- Hyper-V Settings action (Hyper-V Manager), 47
- hypercalls, 30
- hypervisors, 25–29

I

- .ico files, 185
 - delivering, 192
 - deployment scenarios, 202–209
 - as sequencing process output, 197
 - with standalone .msi deployments, 209
- IDE Controller setting (virtual machines), 54
- IDE controllers with Hyper-V, 62
- IIS for streaming application packages, 192, 203, 210
- Import Virtual Machine action (Hyper-V Manager), 47
- importing virtual applications, 211
- importing virtual machines, 47, 65–67, 71
- incompatibility problems, 3, 10, 188, 190
 - App-V and, 186
- Infrastructure Optimization Model, 7–9, 20
- Infrastructure Planning and Design Guides, 386–390, 414
- infrastructure requirements, VMM, 109
- initializing MED-V workspaces, 321
- Inspect Disk action (virtual hard disks), 51
- Installation directory (virtual applications), 182
- installing
 - App-V Clients, 199
 - App-V Management Server, 191
 - App-V Management Web Service, 195
 - Hyper-V, 42–45
 - Hyper-V Manager snap-in, 45
 - Integration Services, 70
 - MED-V packages, 320
 - on terminal servers, 269
 - best practices, 271
 - Terminal Services role, 259, 270
 - with TS Web Access, 291
 - Terminal Services system service, 262
 - Virtual Guest Services, 150
 - Virtual Machine Connection tool, 58
 - VMM (Virtual Machine Manager), 107, 110
 - upgrading from VMM 2007, 111–113
 - VMM Administrator Console, 92
 - VMM Agents, 119
 - VMM Self-Service Portal, 101
 - VMM Server, 110
 - VMware ActiveX control, 154
- instance, defined (in licensing), 411

- Integration Services, 36, 41
 - functionality to child partitions, 36
 - guest operating systems that don't support, 35
 - installing, 70
 - mixing machines that use and don't use, 44
 - replacing legacy network adapters, 56
- Integration Services setting (virtual machines), 55
- Intelligent Placement capability, 102, 177
- interlayer communication, VMM, 93
- internal virtual networks, configuring, 49
- Internet Security and Acceleration (ISA) Server, 299
- IPD guides, 386–390, 414
- ISA Server, 299
- iSCSI storage with Hyper-V, 62
- IT Governance and Compliance suite (Solution Accelerators), 385
- IT Infrastructure Optimization Model, 7–9, 20

J

- Jobs view (VMM Administrative Console), 115

K

- key/value pair exchange, 37
- keyboard accelerators with virtual machines, 60
- Keyboard setting (Hyper-V Manager), 48
- Kidaro, 338
- knowledge-driven management, 12

L

- LAN transfers, 155
- launching RemoteApp programs, 282
- legacy network adapters, 56
- Library Servers (VMM), 90, 91, 104–106
 - adding, 134
 - communication ports for, 95
 - requirements for, 133
 - supported operating systems, 108
 - VMM Server and, 105
 - VMM Server as default, 91
- Library view (VMM Administrative Console), 115
- licensing, 409–413
 - Software Assurance (SA) program, 337
 - Terminal Services, 252, 263
 - planning tips for, 264
 - virtual applications, 218
- lightweight infrastructure, App-V, 243
- Limit Process Functionality setting (Processor configuration), 72
- Links subfolder (user profiles), 345
- Linux distributions
 - with Hyper-V, 41
 - Integration Services enhancements for, 42
- load balancing
 - Hyper-V platform, 45, 79
 - TS Session Broker, 303
 - virtual machine hosts, 102
- Local folder (in AppData folder), 345, 347
- local user profiles, limitations of, 347
- localization features, App-V, 241
- LocalLow folder (in AppData folder), 346, 347
- logical IT infrastructure, 11
- logical processors, 38

M

machine conversions, 176. *See also* P2V conversions; V2V conversions

machine virtualization. *See* server virtualization

maintaining App-V, resources on, 244

maintaining Hyper-V, resources on, 84

maintaining Terminal Services, resources on, 310

Managed Computer Layer, VMM, 104–105

communications ports, 94

interlayer communication, 93

managed host agents (VMM), 105

installing, 119

reassociating, 120

updating, 120

managed hosts (VMM), 117–133

adding to/removing from host groups, 119

clusters, managing, 129

defined, 90

host groups, 117–119, 154

managed host agent management, 119

managing, 121–128

managing VMware with VMM, 130–133, 174

Networking view, 128

Management Console, App-V. *See* App-V Management Console

management interfaces for server virtualization, 24

management packs, 101

Management Server, App-V, 182, 191–192

installing, 191

publishing on. *See* publishing applications

management settings, virtual machines, 54

Management Suite Enterprise, 405

managing App-V, resources on, 244

managing RemoteApp programs, 283

managing terminal servers, 271–280

managing Terminal Services, resources on, 310

managing VDI, 332

managing virtual images, 324

managing virtual machines

with Hyper-V, 74–78

resources on, 84

with MED-V, 316

with VMM 2008, 149–151

managing virtualization. *See* VMM (Virtual Machine Manager)

mandatory user profiles, 356

manifest.xml file, 197

manual online mode (Offline Files), 372

manual synchronization with Offline Files, 373

MAP Toolkit, 391–401, 414

determining Hyper-V server candidates, 401

MDOP (Microsoft Desktop Optimization Pack), 337

MED-V (Microsoft Enterprise Desktop Virtualization), 5, 314–327

how it works, 317–325

key benefits of, 325

product availability, 327

usage policy and data transfer control, 316, 323

usage scenarios, 326

VDI compared to, 328

MED-V Management Server, 323

Media menu (Virtual Machine Connection), 58

media players, plug-and-play redirection for, 249

memory management, 24

memory requirements for Hyper-V, 38

Memory setting (virtual machines), 53

merger integration, Terminal Services for, 308

Merging Disk state (virtual machines), 32

microkernel hypervisors, 28–29

Microsoft

commitment to virtualization, 18

Dynamic IT, 11, 21

IT Infrastructure Optimization Model, 7–9, 20

virtualization technologies and solutions, 21

vision and strategy for virtualization, 16–19, 22

Microsoft Active Directory Domain Services (ADDS)

with MED-V, 316

with virtual applications groups, 216

Microsoft Application Virtualization (App-V). *See* App-V

Microsoft Application Virtualization for Terminal Services, 182, 241

Microsoft Application Virtualization Sequencer. *See* Sequencer utility

Microsoft Assessment and Planning Toolkit, 391–401, 414

determining Hyper-V server candidates, 401

Microsoft Background Intelligent Transfer Service (BITS), 324

Microsoft Deployment Toolkit 2008 Update 1, 404

Microsoft Desktop Optimization Pack (MDOP), 337

Microsoft Enterprise Desktop Virtualization (MED-V). *See* MED-V

Microsoft Hyper-V Manager console, 45–56

exporting and importing VMs, 47, 65–67

managing Microsoft VDI, 332

working with snapshots, 67–69

Microsoft Hypervisor component, 30

Microsoft Infrastructure Planning and Design Guides, 386–390, 414

Microsoft Internet Security and Acceleration (ISA) Server, 299

Microsoft IT Showcase, 311

Microsoft Online Services suite (Solution Accelerators), 385

Microsoft Operations Manager. *See* System Center Operations Manager

Microsoft Point of Service (POS) for .NET device redirection, 251

Microsoft Software Assurance (SA) program, 337

Microsoft Solution Accelerators, 385–404, 414

IPD guides, 386–390, 414

MAP Toolkit, 391–401, 414

Offline Virtual Machine Servicing Tool, 403, 415

Microsoft SQL Server, 103

App-V Data Store, 195

App-V Management Server and, 191

communication ports for, 95

configuring settings for, 110

Microsoft System Center, 17, 404–409, 415

Server Management Suite Licenses, 412

Virtual Machine Manager. *See* VMM (Virtual Machine Manager)

Microsoft Update support, 241

Microsoft VDI. *See* VDI

Microsoft Virtual PC 2007. *See* Virtual PC 2007

Microsoft Virtual Server. *See* Virtual Server

Microsoft Virtual Server 2005 Migration Toolkit (VSMT), 159

Microsoft Virtualization 360, about, 16–19

Microsoft Virtualization Licensing, 410

Microsoft Virtualization Solution Accelerators. *See* Microsoft Solution Accelerators

Microsoft Windows Installer files for virtual applications, 185, 186, 202, 209, 243

RemoteApp programs as, 284

Microsoft Windows Server 2000, 40, 42

Microsoft Windows Server 2003. *See* Windows Server 2003

Microsoft Windows Server 2008. *See* Windows Server 2008

Microsoft Windows Server 2008 Terminal Services. *See* Terminal Services

Microsoft Windows Vista. *See* Windows Vista

Microsoft Windows XP. *See* Windows XP

Microsoft's IT Infrastructure Optimization Model, 20

migrating virtual machines between hosts

- with Hyper-V, 65, 71, 79
- with VMM 2008, 154–157

MMC snap-in for Terminal Services, 271

Mobile Device Manager 2008, 406

mobile worker scenarios, 14, 307, 308, 327, 369

modes of operation, Offline Files, 371

MOM (Microsoft Operations Manager). *See* System Center Operations Manager

monitor spanning with RDC, 248

monitoring application installation for sequencing, 198, 223. *See also* Sequencer utility

Q: drive, using, 182, 231–234

monitoring server performance for Hyper-V, 45

- Hyper-V platform, 79

monolithic hypervisors, 26

motherboard, virtual. *See* Virtual Motherboard (VMB)

Mouse Release Key setting (Hyper-V Manager), 48

.msi files for virtual applications, 185, 186, 202, 209, 243

- RemoteApp programs as, 284

MSI Manifest, 186

MSIT project, 311

Mstscax.dll (Terminal Services ActiveX control), 292

Mstsc.exe client, 247, 292. *See also* Remote Desktop Connection

Music subfolder (user profiles), 345

My Documents folder, redirecting, 358

My Pictures folder, redirecting, 358

N

Name setting (virtual machines), 54

named licenses, 219

naming virtual machines, 142

NAP (Network Access Protection), 299

Negotiate layer (RDP), 267

.NET Remoting, 200

Network Access Protection (NAP), 299

Network Adapter setting (virtual machines), 54

network adapters, 49, 56

- adding to virtual machines, 53

network infrastructure requirements for VMM 2008, 109

network interface cards, 44

Network Level Authentication (NLA), Terminal Services, 262, 265

Network Load Balancing (NLB), 304

Network Service identity, 33

Network tab (Offline Files applet), 378

Network transfers (virtual machines), 155

network user profile, default, 350

networking

- configuring virtual networks, 49
- Hyper-V network model, 51
- server virtualization, 24

Networking tab (managed hosts), 124

Networking view (managed hosts), 128

Never Automatically Turn On The Virtual Machine setting, 151

New Application Wizard, 213

New Floppy Disk action (Hyper-V Manager), 47

New Hard Disk action (Hyper-V Manager), 47

New User Role Wizard, 162

- creating Delegated Administrator role, 162–164
- creating Self-Service User role, 165–169

New Virtual Machine action (Hyper-V Manager), 46

- creating VMs using passthrough disks, 63, 73
- creating VMs using VHDs, 63

NICs (network interface cards), 44

NLA (Network Level Authentication), Terminal Services, 262, 265, 267

NLB (Network Load Balancing), 304

non-Windows guest operating systems, 36

nonpersistent architecture, Microsoft VDI in, 331

Not Active state (virtual machines), 32

O

office worker scenario, 15

offline delivery of .sft files, 193

Offline Files, 6, 366–380. *See also* Vista Roaming Desktop

- how it works, 367–375
- implementing, 375–379
- Windows Vista enhancements, 368

offline P2V conversion, 158

Offline Virtual Machine Servicing Tool, 403, 415

offshore worker scenarios, 15, 326, 335

OLE DB interfaces, 200

online delivery of .sft files, 193

online mode (Offline Files), 371

online P2V conversion, 158

operating system environment, defined (in licensing), 411

operating systems

- host operating system, 136
- for P2V conversions, 159
- for V2V conversions, 160
- on virtualized servers. *See* guest operating systems
- VMM installation and, 108

operation-driven design, 12

Operations Manager 2007, 406

OpsMgr, 101–103

- Virtualization Candidates report, 158

optimizing server loading for Hyper-V, 45

- Hyper-V platform, 79

.osd files, 185

- delivering, 192
- deployment scenarios, 202–209
- as sequencing process output, 197
- with standalone .msi deployments, 209

OSD tab (App-V Sequencer Console), 230

outsourcing Content folder, 194

outsourcing scenario, Terminal Services, 308

overall status, managed hosts, 122

overloading servers with Hyper-V, 43

Owner property (virtual machines), 151

P

P2V agents (VMM), 105

P2V conversions, 158

- defined, 90
- online vs. offline, 158

Packages node (Management Console), 217

- ul style="list-style-type: none;">
- packaging RemoteApp programs, 284
- Pagefile.sys files on Hyper-V machines, 45
- parent partitions, 29, 30–35
 - Hyper-V network model, 51
 - virtualization stack (components of), 31
- partitions, 4, 30–35
 - creating new child partitions, 46, 61–65
 - Hyper-V network model, 51
 - with microkernel hypervisors, 29
- passthrough disks, 61
 - creating virtual machines with, 63, 73
 - storing Hyper-V configuration files, 64
- passwords
 - for guest operating system, setting, 144
 - lost when updating VMM, 112
- pausing virtual machines, 58, 149
 - snapshots and, 67
 - viewing paused VMs, 116
- per-computer settings, Offline Files, 378
- per-device licensing, Terminal Services, 264
- per-user licensing, Terminal Services, 264
- per-user settings, Offline Files, 378
- performance, server. *See* server speed
- Performance and Resource Optimization. *See* PRO
- permissions for virtual applications, 212, 214
 - licenses, 218
- persistent architecture, Microsoft VDI in, 331
- physical processor, defined (in licensing), 411
- physical servers
 - converting to virtual machines. *See* P2V conversions
 - Hyper-V and, 43
 - starting/stopping, 148, 151
- Pictures subfolder (user profiles), 345
- Placement tab (managed hosts), 126
- platform incompatibility, 3
- players, plug-and-play redirection for, 249
- plug-and-play device redirection, 249
- plug-in VDevs, 34
- PnP device redirection, 249
- Point of Service (POS) for .NET device redirection, 251
- pooled VDI deployment architecture, 336
- ports (communications)
 - for App-V, 201
 - for VMM, 94
 - connecting to virtual machines, 152
- POS for .NET device redirection, 251
- power requirements, reducing, 10
- power users, Microsoft VDI for, 335
- PowerShell. *See* Windows PowerShell
- presentation virtualization, 6, 245. *See also* Terminal Services
- pricing for licenses, 412
- printing with Terminal Services, 253–256
- prioritization of display data (RDC), 248
- private virtual networks, configuring, 49
- PRO (Performance and Resource Optimization), 175, 176
 - configuring settings for, 151
 - defined, 90
 - OpsMgr integration with VMM 2008, 102
 - VMM 2008 scenario, 179
 - Windows PowerShell cmdlets, 103
- processing requirements for virtual machines, 71
- processor, defined (in licensing), 411
- Processor setting (virtual machines), 53, 71
- product keys, lost when updating VMM, 112
- production environments
 - snapshots and, 68
 - Terminal Services role and, 260
- profile virtualization, 6, 339–384
 - about user profiles, 339
 - additional resources on, 382
 - FR (Folder Redirection). *See* FR (Folder Redirection)
 - key benefits of, 380
 - local user profiles, limitations of, 347
 - Offline Files. *See* Offline Files
 - RUP (Roaming User Profiles). *See* RUP
 - structure of user profiles, 341–347
 - usage scenarios, 381
 - where user profiles are found, 340
- profiles
 - application-specific, for Windows PowerShell, 97
 - for guest operating systems, 89, 135, 136
 - hardware profiles, 89, 112, 135, 136
 - updating VMM and, 112
 - user profiles. *See also* profile virtualization
 - with Session Broker, 305
 - structure of, 341–347
- Properties dialog box (virtual machines), 151
- protocols for VMM communications, 94
- Provider Policies node (Management Console), 221
- provisioning of servers, 10, 177
 - dynamic provisioning, 11
- provisioning of virtualized resources, 178
- Public profile, 341
- publishing applications, 185
 - defined, 182
 - RemoteApp programs as, 284
 - troubleshooting, 237–238
- publishing servers, creating, 236
- Publishing Servers node (Application Virtualization Client console), 236

Q

- Q: drive, 182, 231–234
- Quick Migration feature (Hyper-V), 38
- quota points, configuring, 151
- quotas for virtual machines, Self-Service User role, 169

R

- RAM requirements for Hyper-V, 38
- Rationalized IT infrastructure, 8
 - advancing to Dynamic infrastructure, 11
 - benefits over Standardized infrastructure, 10
- RDC (Remote Desktop Connection), 247, 310
 - display improvements in Windows Server 2008, 247
 - managing Hyper-V with, 74
- RDP encryption levels, 268
- RDP for remote users on corporate network. *See* TS Gateway
- RDP security layers, 267
- reassociating host agents, 120
- recovery. *See* backup and recovery
- Redirect To The Following Location option (Basic redirection), 363
- Redirect To The Local Userprofile Location option (Basic redirection), 363

Redirect To The User's Home Directory option (Basic redirection), 363

Register The Following Virtual Machines setting, 124

regression testing, App-V and, 187, 189

regulatory compliance, Terminal Services and, 308

Relative Weight setting (Processor configuration), 72

relocating VM configuration files, 64

Remote Assistance, 262

remote connections to virtual machines. *See* connecting to virtual machines

Remote Control tab (Active Directory Users and Computers), 276

Remote Desktop, 262

Remote Desktop Connection (RDC), 247, 310

 managing Hyper-V with, 74

Remote Desktop Web Connection, 295–297

Remote Desktops console (Tsmmc.msc), 275

Remote tab (managed hosts), 126

RemoteApp, 251, 281–290. *See also* Terminal Services

 deploying programs via Web browser. *See* TS Web Access

 managing Hyper-V with, 75

 Microsoft VDI, integrated with, 330

 secure remote connectivity, 306

RemoteSigned security context (Windows PowerShell), 97

Remove-VMHost cmdlet, 119

removing applications from client environment, 188, 190

removing hosts from host groups, 119

Rename action (Hyper-V Manager), 56

Rename action (Snapshots pane), 69

renaming virtual machines, 56

repairing virtual machines, 150

Reporting view (VMM Administrative Console), 116

Reports node (Management Console), 220

Reserves tab (managed hosts), 124

Reset Check Boxes setting (Hyper-V Manager), 49

resetting virtual machines, 58

resolving Offline Files conflicts, 373

resource allocation with virtual machines, 71

Resource Authorization Policy, Terminal Services (TS RAP), 301

resource dependencies, 137

resource optimization. *See* PRO (Performance and Resource Optimization)

resources

 maximizing through consolidation, 10, 176

 provisioning of, 178. *See also* provisioning of servers

 removing from VMM library, 136

restoring. *See* backup and recovery

Restricted security context (Windows PowerShell), 97

return on investment. *See* business benefits to virtualization

Revert action (Snapshots pane), 70

right-sizing of virtual machines (PRO), 102

rings, 39

Roaming folder (in AppData folder), 346, 347

Roaming User Profiles (RUP). *See* RUP

ROI. *See* business benefits to virtualization

Rpdinit.exe (RemoteApp Logon Application), 282

RTSP (Real-Time Streaming Protocol), 200. *See also* streaming application packages

RTSPS (Real-Time Streaming Protocol Secure), 201. *See also* streaming application packages

running instance, defined (in licensing), 411

running virtual machines, viewing, 116

RUP (roaming user profiles), 6, 349–357. *See also* Vista Roaming Desktop

additional resources on, 383

how it works, 349

 storage location for, 352

implementing, 350–356

implementing FR with, 361–366, 366, 380

key benefits of, 380

limitations of, 356

usage scenarios, 381

S

SA (Software Assurance), 337

SA (Solution Accelerator). *See* Microsoft Solution Accelerators

SAN transfers, 155

Saved Games subfolder (user profiles), 345

Saved Searches subfolder (user profiles), 345

saved virtual machines, viewing, 116

saving state of virtual machines, 58, 149, 151

SBLB (TS Session Broker Load Balancing), 302, 304

scalability

 App-V, 240

 Hyper-V, 79

scenarios for virtualization, 13–16, 22

 App-V deployment, 202–209

 MED-V (Microsoft Enterprise Desktop Virtualization), 326

 profile virtualization, 381

 server virtualization, 82

 Terminal Services, 307–309

 VDI (Virtual Desktop Infrastructure), 335

 VMM (Virtual Machine Manager), 178–179

scheduler (server virtualization), 24

SCSI controllers with Hyper-V, 62

 configuring, 54

 using for data drives, 71

SCVMM (System Center Virtual Machine Manager). *See* VMM (Virtual Machine Manager)

Scvmmrecover.exe tool, 138

security

 App-V features, 242

 authentication. *See* authentication

 configuring for VMware ESX Server hosts, 131

 hardware-based DEP, 38

 Terminal Services, 265–269, 306

 TS Gateway and, 298

Security Compliance Management, 404

security context for Windows PowerShell scripts, 97

Security suite (Solution Accelerators), 385

self-managing systems, 11

self-service portal, 92

Self-Service Portal, VMM, 101, 170–173

 creating self-service user role, 165–169

 installing, 101, 111

 supported operating systems, 108

 virtual machine owners, 151

Self-Service User role, 162, 165–169

 access to Self-Service Portal, 171

sequenced application packages, 182, 185

sequenced applications, 182, 184

 Q: drive, 182, 231–234

Sequencer utility (App-V), 182, 188, 197, 222–234

 Q: drive, using, 182, 231–234

sequencing, defined, 183

sequencing computer, defined, 183, 198

426 server, defined (in licensing)

- server, defined (in licensing), 411
- server-based desktop virtualization, 313. *See also* VDI
- server-based licensing, 410
- server considerations for Hyper-V, 43
- server consolidation scenarios, 82, 178
- Server Groups node (Management Console), 219
- Server Management Suite Enterprise, 405
- Server Management Suite Licenses, 412
- Server Message Block. *See* SMB protocol for streaming application packages
- server provisioning and consolidation, 10
- server settings (Hyper-V Manager), 47
- server speed
 - for Hyper-V, 44
 - for VMM 2008, 109
- server sprawl, 3
- Server suite (Solution Accelerators), 385
- server virtualization, 4, 23–87. *See also* Hyper-V platform
 - additional resources on, 83–87
 - benefits of Hyper-V for, 81
 - creating virtual machine, 61–65
 - guest operating systems with Hyper-V, 39
 - how it works, 23–29
 - Hyper-V architecture, 23–37, 79
 - Hyper-V Manager console
 - configuring server settings, 46–51
 - managing virtual machines, 52–56
 - installing Hyper-V, 42–45
 - Integration Services functionality, 41
 - management tools, 74–78
 - usage scenarios, 82
 - Virtual Machine Connection tool, 56–60
 - working with virtual machines, 65–73
- Service Manager (System Center), 406
- Session Broker, Terminal Services, 252, 302
 - load balancing, 303
- Session Broker Load Balancing (SBLB), 302, 304
- SessionEnv service, 261
- Sessions tab (Active Directory Users and Computers), 276
- Set-ExecutionPolicy cmdlet, 97
- Set Roaming Profile Path For All Users Logging Onto This
 - Computer policy, 353
- Set-VMMServer SCVMM cmdlet, 103
- Settings action (Hyper-V Manager), 53
- Settings tab (virtual machine properties), 151
- .sft files, 185
 - creating. *See* Sequencer utility
 - delivering, 193–194. *See also* streaming application packages
 - differential SFTs, 241
 - managing, 217
 - as sequencing process output, 197
 - with standalone .msi deployments, 209
 - streaming methods, 203
- SFTMIME command, 186, 237
- shutdown (child partition), 37
- shutting down virtual machines, 58, 149, 151
- single sign-on for Terminal Services, 250
- single-site deployment of App-V, 206
- slow-link mode (Offline Files), 372
- SMB protocol for streaming application packages, 193, 201, 203
- smoothing (font), with RDC, 248
- SMP support, Hyper-V, 79
- Snapshot action (Hyper-V Manager), 55, 68
 - Snapshot action (Snapshots pane), 70
 - snapshot differencing disk (.avhd) files, 69
 - Snapshot File Location setting (virtual machines), 55
 - snapshot trees, deleting, 69, 70
 - Snapshots folder, 66
 - snapshots of virtual machines, 55, 151
 - working with, 67–69
 - SoftGrid Application Virtualization, 5
 - Software Assurance (SA) program, 337
 - Software Audit report, 220
 - software requirements
 - MED-V (Microsoft Enterprise Desktop Virtualization), 318
 - VMM (Virtual Machine Manager), 107–109
 - VMM library, 133
 - Solution Accelerators, 385–404, 414
 - IPD guides, 386–390, 414
 - MAP Toolkit, 391–401, 401, 414
 - Offline Virtual Machine Servicing Tool, 403, 415
 - solutions for virtualization, resources on, 21
 - space requirements, reducing, 10
 - speed, servers
 - for Hyper-V, 44
 - for VMM 2008, 109
 - .spri files, 185
 - SQL Server, 103
 - App-V Data Store, 195
 - App-V Management Server and, 191
 - communication ports for, 95
 - configuring settings for, 110
 - SSL (Secure Sockets Layer)
 - encrypting communications over VMRC connections, 153
 - HTTP over. *See* HTTPS protocol
 - for Terminal Services connections, 268
 - SSO for Terminal Services, 250
 - standalone deployment of virtual applications. *See* .msi files for virtual applications
 - standard keyboard accelerators with virtual machines, 60
 - Standardized IT infrastructure, 8, 10
 - Start Menu folder, redirecting, 358
 - Starting state (virtual machines), 32
 - starting virtual machines, 149
 - state machine, 24
 - states for virtual machines, 32, 116
 - capturing. *See* snapshots of virtual machines
 - saving, 58, 149, 151
 - static architecture, Microsoft VDI in, 331
 - Status tab (managed host properties), 121
 - stopped virtual machines, viewing, 116
 - stopping virtual machines, 149
 - storage. *See* disk space
 - storage location
 - redirected folders, 361
 - snapshot files, 55
 - virtual hard disk files, 47, 70
 - virtual machine configuration files, 47, 64, 146
 - stored virtual machine, defined, 90
 - strategy for virtualization (Microsoft's), 16–19, 22
 - streaming application packages, 186, 192–194
 - defined, 183
 - troubleshooting, 237–238
 - Streaming Server (App-V), 183, 196, 203, 209–211
 - adding IIS to, 210
 - Summary tab (managed host properties), 121

super-mandatory user profiles, 356
 supporting applications, in general, 187, 190. *See also* updating
 Symmetric Multiprocessors (SMP), Hyper-V support for, 79
 synchronization with Offline Files, 369, 372
 resolving conflicts with, 373
 synthetic devices, 34
 System Center, 17, 404–409, 415
 benefits of, 406
 Essentials, 405
 Management Suite Enterprise, 405
 Server Management Suite Licenses, 412
 Virtual Machine Manager. *See* VMM (Virtual Machine Manager)
 System Center Operations Manager (OpsMgr), 101–103
 Virtualization Candidates report, 158
 System Center Virtual Machine Manager. *See* VMM
 System Error report, 221
 system files, storing on Hyper-V machines, 45
 system requirements, MED-V, 318
 system services, Terminal Services, 261
 System Utilization report, 220

T

Tag property (virtual machines), 151
 Taking Snapshot state (virtual machines), 32
 tape backups, 407, 408. *See also* backup and recovery
 task worker scenarios, 15, 308
 TCP ports for VMM communications, 94
 TechNet forums and webcasts
 App-V, 244
 Hyper-V, 87
 Terminal Services, 311
 user state virtualization, 384
 VMM 2008, 180
 technologies for virtualization, resources on, 21
 templates (VMM library), 90
 for virtual machines, 135
 creating new VM from, 141
 temporary workers, single account for, 348
 terminal server access, configuring, 266
 terminal server authentication, 262, 265
 terminal servers
 installing applications on, 269
 best practices, 271
 managing, 271–280
 Terminal Services, 6, 245–312
 additional resources on, 309
 App-V Terminal Services Client, 199, 209
 Application Virtualization for Terminal Services, 182, 241
 basics of presentation virtualization, 245
 deploying App-V with, 199, 209
 EasyPrint, 253–256
 Gateway, 251, 298–302
 secure remote connectivity, 306
 installing applications on terminal servers, 269, 271
 installing Terminal Services role, 259, 270, 291
 key benefits of, 306
 licensing, 252, 263, 264
 managing terminal servers, 271–280
 new features in Windows Server 2008, 246–258
 office worker scenario, 15
 Remote Desktop, 262
 Remote Desktop Connection (RDC), 310
 RemoteApp. *See* RemoteApp
 security, 265–269
 Session Broker, 252, 302, 303
 single sign-on for, 250
 system services, 261
 task worker scenario, 15
 usage scenarios, 307–309
 Web Access. *See* TS Web Access
 Terminal Services ActiveX control (Mstscax.dll), 292
 Terminal Services Configuration (Tsconfig.msc), 274
 Terminal Services Connection Authorization Policy (TS CAP), 300
 Terminal Services Manager (Tsadmin.msc), 271
 Terminal Services MMC snap-ins, 271
 Terminal Services Profile tab (Active Directory Users and
 Computers), 276
 Terminal Services RemoteApp. *See* RemoteApp
 Terminal Services Resource Authorization Policy (TS RAP), 301
 terminating RemoteApp programs, 282
 termination of installed applications, 188, 190
 TermServices service, 261, 262
 testing and development scenario (Hyper-V), 83
 time synchronization, 37
 toolbar, Virtual Machine Connection tool, 58
 tools for managing Hyper-V and virtual machines, 74–78
 Trim Transfer mechanism, 316
 troubleshooting App-V, 237–239
 TS EasyPrint, 253–256
 TS Gateway, 251, 298–302
 how it works, 299
 implementing, 300–302
 secure remote connectivity, 306
 security and, 298
 TS Gateway Manager, 302
 TS Licensing, 252, 263
 planning tips, 264
 TS RemoteApp, 251, 281–290. *See also* Terminal Services
 deploying programs via Web browser. *See* TS Web Access
 how it works, 281
 managing, 283
 managing Hyper-V with, 75
 Microsoft VDI, integrated with, 330
 programs, deploying and using, 284–290
 secure remote connectivity, 306
 TS Session Broker, 252, 302
 load balancing, 303
 TS Session Broker Load Balancing (SBLB), 302, 304
 TS Web Access, 251, 290–297
 connection process, 292
 deploying RemoteApp programs, 292–295
 how it works, 291
 Remote Desktop Web Connection, 295–297
 TS Web Access Administration page, 294
 Tsadmin.msc (Terminal Services Manager), 272
 Tsconfig.msc (Terminal Services Configuration), 274
 TSGateway service, 262
 Tsmmc.msc (Remote Desktops), 275
 Tssdis service, 262
 turning off virtual machines, 58, 149, 151
 turning on virtual machines, 151
 Type 1 hypervisors, 25
 Type 2 hypervisors, 26
 Type Clipboard Test option (Clipboard menu), 58

U

UMRdpService service, 262

underutilized physical servers, identifying, 158

uninstalling applications from client environment, 188, 190

unlimited licenses, 219

Unrestricted security context (Windows PowerShell), 97

updating, 187, 189

- host agents, 120
- virtual applications, 187, 189

upgrading

- virtual application packages, 217
- virtual applications, 181
- VMM, 111–113

usage policies, MED-V, 316, 323

usage scenarios. *See* scenarios for virtualization

user accounts, configuring for roaming profiles, 352

User Credentials setting (Hyper-V Manager), 48

user profiles. *See also* profile virtualization

- about, 339
- default network user profiles, 350
- local, limitations of, 347
- mandatory and super-mandatory, 356
- roaming. *See* RUP (roaming user profiles)
- with Session Broker, 305
- structure of, 341–347
- where found, 340

user roles, VMM 2008, 161–169, 175

- Delegated Administrator role, creating, 162–164
- Self-Service User role, creating, 165–169

user settings (Hyper-V Manager), 48

user state migration, resources on, 383

user state virtualization, 6, 339–384

- about user profiles, 339
- additional resources on, 382
- FR (Folder Redirection). *See* FR (Folder Redirection)
- key benefits of, 380
- local user profiles, limitations of, 347
- Offline Files. *See* Offline Files
- RUP (Roaming User Profiles). *See* RUP
- structure of user profiles, 341–347
- usage scenarios, 381
- where user profiles are found, 340

Users folder, 340

V

V2V conversions, 90, 160

VDevs (virtual devices), 33

VDI (Virtual Desktop Infrastructure), 5, 328–336, 338

VECD (Vista Enterprise Centralized Desktop), 15, 329, 338

version

- host agents, 122
- Virtualization service, 123

.vhd files, 47, 63, 70. *See also* virtual hard disks

VI3 environment, managing, 130–133, 174

Videos subfolder (user profiles), 345

Vid.sys component, 34

View menu (Virtual Machine Connection), 58

View Sync Conflicts option (Sync Center), 374

views, VMM Administrator Console, 115–116

virtual adapters for data drives, 71

virtual application groups, 216–217

virtual application management, 186

virtual application packages, 185

- creating. *See* Sequencer utility
- delivering, 193–194. *See also* streaming application packages
- differential SFTs, 241
- managing, 217
- as sequencing process output, 197
- with standalone .msi deployments, 209
- streaming methods, 203

virtual applications. *See also* App-V

- defined, 183
- file type associations, 214, 221, 235
- managing, 186, 234
- publishing, 182, 185, 237–238, 284
- sequencing. *See* sequenced application packages; sequenced applications
- streaming. *See* streaming application packages

Virtual COM subsystem, 184

Virtual Desktop Infrastructure. *See* VDI

virtual device drivers, 24

virtual devices (VDevs), 33

virtual directories, 184

virtual environment, App-V, 184. *See also* App-V Clients

Virtual File System tab (App-V Sequencer Console), 230

virtual file systems, 184, 225

virtual files, 184

virtual floppy disks, 47

Virtual Guest Services, installing, 150

virtual hard disk (.vhd) files, 47, 63, 70

virtual hard disks, 135

- creating new, 47
- creating virtual machines with, 63
- default locations for .vhd files, 70
- for guest operating systems, 61
- making changes to, 50

Virtual Hard Disks folder, 66

virtual hardware settings, virtual machines, 53, 143

virtual images, 315–316

- expiring, 324

Virtual Machine Bus (VMBus), 34

virtual machine configuration files

- created when taking snapshots, 69
- default location for, 47, 70

Virtual Machine Connection tool, 56–60

- connecting and managing VMs, 52
- creating virtual machines, 60
- installing, 58
- keyboard accelerators, managing, 60
- taking snapshots, 69

virtual machine hosts

- adding to/removing from host groups, 119
- communication ports for, 95
- defined, 89
- displaying virtual machines on, 145
- load balancing, 102
- migrating virtual machines between
 - with Hyper-V, 65, 71, 79
 - with VMM 2008, 154–157
- supported operating systems, 108

Virtual Machine Limit setting (Processor configuration), 72

Virtual Machine Management Service. *See* VMMS

Virtual Machine Manager. *See* VMM

Virtual Machine Manager Agent, 91, 105

Virtual Machine Manager Configuration Analyzer (VMMCA), 110

Virtual Machine Manager section (Hosts view), 118

- Virtual Machine Manager Self-Service Portal. *See* Self-Service Portal, VMM
- Virtual Machine Manager Server, 91
 - communication ports for, 95
 - installing, 110
 - Library Servers and, 105
 - supported operating systems, 108
- virtual machine memory contents files, 69
- virtual machine quotas, 169
- Virtual Machine Remote Control (VMRC), 152
- Virtual Machine Remote Control ActiveX Control, 99
- Virtual Machine Remote Control process (Vmrc.exe), 100
- Virtual Machine Reserve setting (Processor configuration), 72
- virtual machine saved state (.vsv) files, 69
- virtual machine templates (VMM library), 135
- Virtual Machine Viewer process, 99
- Virtual Machine worker processes (vmwp.exe), 33
- virtual machines
 - about, 2
 - best practices for configuring, 70
 - cloning, 157
 - connecting storage to, 62
 - converting physical computers to, 158
 - defined, 90
 - with Hyper-V. *See* Virtual Machine Connection tool
 - online vs. offline, 158
 - with VMM Administrator Console, 150, 152–154
 - creating with Hyper-V, 61–65, 73
 - creating with VMM 2008, 139–149
 - exporting virtual machines, 71
 - importing and exporting, 47, 65–67
 - keyboard accelerators with, 60
 - maintaining, 324
 - managing with Hyper-V Manager snap-in, 52–56
 - managing with MED-V, 316
 - managing with VMM 2008, 139–157
 - Offline Virtual Machine Servicing Tool, 403, 415
 - settings for, 150–151
 - snapshots. *See* snapshots of virtual machines
 - states of, 32
 - templates for (VMM library), 135
 - tools for managing, 74–78
 - working with, 65–73
- Virtual Machines folder, 66
- Virtual Machines view (VMM Administrative Console), 65, 71, 79, 115, 154–157
- Virtual Motherboard (VMB), 33
- Virtual Network Manager action (Hyper-V Manager), 49
- virtual network, selecting for VMs, 147
- Virtual PC 2007, 2, 5, 314, 337. *See also* MED-V
 - resources on, 20
- virtual processor, defined (in licensing), 411
- virtual registries, 184
- Virtual Registry tab (App-V Sequencer Console), 229
- Virtual Server, 2
 - controlling virtual machines on, 152
 - Hyper-V vs. Virtual Server 2005 R2, 80
 - migrating virtual machines, 65, 71, 79, 154–157
 - resources on, 20
 - V2V (virtual-to-virtual) conversions, 90, 160
 - VMM 2008 support for, 176
- Virtual Server 2005 Migration Toolkit (VSMT), 159
- Virtual Service Providers (VSPs), 34
- virtual services, 184
 - troubleshooting, 238
- Virtual Services tab (App-V Sequencer Console), 230
- VirtualCenter Server, adding, 130
- virtualization, benefits and uses of, 7–16
- virtualization, defined, 1
- virtualization, reasons for, 1–3
- virtualization, types of, 4–6
- Virtualization 360, about, 16–19
- Virtualization Candidates report, 158
- virtualization infrastructure, building, 385–415
 - additional resources on, 414
 - Microsoft Solution Accelerators, 385–404
 - Microsoft System Center solutions, 404–409
- Virtualization Infrastructure Driver (Vid.sys), 34
- virtualization licensing. *See* licensing
- virtualization scenarios. *See* scenarios for virtualization
- Virtualization service, 123
- Virtualization Service Clients (VSCs), 34, 36
- virtualization stack, 31
- Virtualization suite (Solution Accelerators), 385
- virtualization technologies and solutions, resources on, 21
- virtualization vision and strategy, 16–19, 22
- virtualized applications. *See* sequenced applications
- virtualized devices, 24
- virtualized infrastructure, 11
- virtualized resource provisioning, 178
- Virtualmachineviewer.exe process, 99
- virus protection software, Hyper-V and, 44
- visibility of protected operating systems files, 342
- vision for virtualization (Microsoft's), 16–19, 22
- Vista. *See* Windows Vista
- Vista Enterprise Centralized Desktop. *See* VECD
- Vista Roaming Desktop, 6, 14, 15
- VMB (Virtual Motherboard), 33
- VMBus mechanism, 34
- .vmc files, default location for, 47, 70
- VMConnect (Virtual Machine Connection tool), 56–60
 - connecting and managing VMs, 52
 - taking snapshots, 69
- VMM (Virtual Machine Manager), 17, 39, 87, 89–180, 406
 - additional resources on, 180
 - architecture of, 92–106
 - backing up and recovering database, 137–139
 - components of, 91–92
 - deploying
 - hardware requirements, 105
 - resources on, 180
 - software requirements, 107
 - installing, 110–113
 - upgrading from VMM 2007, 111–113
 - key benefits of, 176–177
 - key features of, 173–175
 - with Microsoft VDI, 329
 - OpsMgr integration with, 102
 - P2V conversions, 158
 - defined, 90
 - online vs. offline, 158
 - self-service portal. *See* Self-Service Portal, VMM
 - system and infrastructure requirements, 106–109
 - terminology of, 89
 - usage scenarios, 178–179
 - user role configuration, 161–169, 175
 - V2V conversions, 90, 160
 - working with managed hosts. *See* managed hosts (VMM)

430 VMM (Virtual Machine Manager) (*continued*)

VMM (Virtual Machine Manager) (*continued*)

- working with virtual machines, 139–157
- working with VMM library, 89, 133–139
- VMM 2007, upgrading, 111
- VMM Administrator Console. *See* Administrator Console, VMM
- VMM Agents, 91, 105
- VMM library, 89, 91, 105, 133–139
 - creating new library share, 110
 - deploying VMs from, 154
 - resources of, 105
- VMM Library Server, 90, 91, 104–106
 - adding, 134
 - communication ports for, 95
 - requirements for, 133
 - supported operating systems, 108
 - VMM Server and, 105
 - VMM Server as default, 91
- VMM Self-Service Portal. *See* Self-Service Portal, VMM
- VMM Server, 91
 - communication ports for, 95
 - installing, 110
 - Library Servers and, 105
 - supported operating systems, 108
- Vmmadmin.exe executable, 99. *See also* VMM Administrator Console
- VMMCA (Virtual Machine Manager Configuration Analyzer), 110
- VMMS (Virtual Machine Management Service), 32, 103
- VMRC (Virtual Machine Remote Control), 152
- Vmrcactivexclient.dll control, 99
- Vmrc.exe process, 100
- VMs. *See* virtual machines
- VMs tab (managed hosts), 123
- VMware ActiveX control, installing, 154
- VMware ESX Server, 25, 27, 173
 - adding hosts, 130
 - communication ports for, 95
 - configuring security for hosts, 131
 - controlling virtual machines on, 153
 - Hyper-V vs., 80
 - managing VMware with VMM, 130–133, 174
 - V2V (virtual-to-virtual) conversions, 90, 160
 - VMM 2008 support for, 176
- VMware Infrastructure 3 environment, managing, 130–133, 174
- VMware Server, 26
- VMware viewer process (Vmwareviewer.exe), 100
- VMware VirtualCenter Server, adding, 130
- Vmwareviewer.exe process, 100
- vmwp.exe process, 33
- volume licensing briefs, 412
- Volume Shadow Copy (VSS) service, 37
- VSCs (Virtualization Service Clients), 34, 36
- VSMT (Virtual Server 2005 Migration Toolkit), 159
- VSPs (Virtual Service Providers), 34
- VSS (Volume Shadow Copy) service, 37
- .vsv files, 69

W

- WCF (Windows Communication Foundation), 93
- Web Access, Terminal Server. *See* TS Web Access
- webcasts, TechNet
 - Terminal Services, 311
 - user state virtualization, 384
- widescreen monitor support (RDC), 247

- Windows Communication Foundation (WCF), 93
- Windows Hypervisor Interface Library (WinHv.sys), 34
- Windows Installer files for virtual applications, 185, 186, 202, 209, 243
 - RemoteApp programs as, 284
- Windows keyboard accelerators with virtual machines, 60
- Windows Management Instrumentation (WMI)
 - managing Hyper-V with, 32, 75
 - providers for Terminal Services, 280
 - providers for VMMS, 32, 75
- Windows operating system, Hyper-V-aware, 36
- Windows Portable Media devices, plug-and-play redirection, 249
- Windows PowerShell, 177
 - adding to server, 107
 - configuring for VMM 2008, 97
 - managing Hyper-V with, 76–78
 - PRO cmdlets, 103
 - with VMM 2008, 96–98, 103
- Windows Server 2000
 - with Hyper-V, 40
 - Integration Services enhancements for, 42
- Windows Server 2003
 - with Hyper-V, 40
 - Integration Services enhancements for, 41
 - supported for VMM installation, 108
 - Terminal Services, 256
- Windows Server 2008
 - failover clustering with VMM 2008, 174
 - Hyper-V. *See* Hyper-V platform
 - Integration Services enhancements for, 41
 - supported for VMM installation, 108
 - as supported guest operating systems, 40
- Windows Server 2008 Security Guide, 403
- Windows Server 2008 Terminal Services. *See* Terminal Services
- Windows System Resource Manager (WSRM), 256
- Windows Vista
 - Enterprise Centralized Desktop. *See* VECD
 - Enterprise Edition, 337
 - with Hyper-V, 40
 - Integration Services enhancements for, 42
 - Offline Files enhancements, 368
 - supported for VMM installation, 109
 - user profile structure, 343
- Windows XP
 - with Hyper-V, 41
 - Integration Services enhancements for, 42
 - profile namespace, 343
 - supported for VMM installation, 109
- WinHv.sys component, 34
- WinRM (Windows Remote Management), 93
- WMI. *See* Windows Management Instrumentation
- WMI providers, 32, 75, 280
- worker process, virtual machines. *See* Virtual Machine worker processes (vmwp.exe)
- workgroups, implementing Folder Redirection in, 360
- working from home scenarios, 327, 335
- workspace, MED-V, 321–323
- WSRM (Windows System Resource Manager), 256

X

- XenDesktop, 329
- XP. *See* Microsoft Windows XP

About the Author



Mitch Tulloch is lead author for the *Microsoft Windows Vista Resource Kit, Second Edition* (Microsoft Press, 2008) and is a widely recognized expert on Windows administration, networking, and security. Mitch has published almost 300 articles for different IT pro sites and magazines and has written almost two dozen books, including *Introducing Windows Server 2008* (Microsoft Press, 2007). His articles have been widely syndicated on IT sites such as ComputerWorld and TechTarget and have even been featured on news media sites like CNN. Mitch also writes a weekly editorial for IT World's Windows in the Enterprise newsletter, which is read by more than thirty thousand IT professionals around the world. Mitch has also been the

technical reviewer for numerous IT professional titles from Microsoft Press, and he has developed and taught graduate-level courses in Information Security Management (ISM) for the Masters of Business Administration (MBA) program of Jones International University.

Mitch has been repeatedly awarded Most Valuable Professional (MVP) status by Microsoft for his outstanding contributions in supporting both his local IT pro user group and the larger global community of IT professionals around the world. The Microsoft MVP Program recognizes individuals who share a deep commitment to building community among IT professionals and show a willingness to help others with their questions and problems. You can find out more about Microsoft's MVP Program at <http://mvp.support.microsoft.com>.

Mitch currently lives in Winnipeg, Canada. Prior to launching his own business in 1998, Mitch worked as a Microsoft Certified Trainer (MCT) for Productivity Point International. For more information about Mitch, see his Web site at <http://www.mtit.com>.