Microsoft

Installing and Configuring Windows Server 2012 R2

Exam Ref 70-410

Craig Zacker

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

Library of Congress Control Number: 2014931253
ISBN: 978-0-7356-8424-9

Printed and bound in the United States of America.

First Printing

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at mspinput@microsoft.com. Please tell us what you think of this book at http://www.microsoft.com/learning/booksurvey.

Acquisitions Editor: Anne Hamilton
Developmental Editor: Karen Szall
Editorial Production: Box Twelve Communications
Technical Reviewer: Brian Svidergol
Cover: Twist Creative • Seattle

Contents at a glance

	Introduction	*xi*
	Preparing for the exam	*xiii*
CHAPTER 1	**Installing and configuring servers**	**1**
CHAPTER 2	**Configuring server roles and features**	**71**
CHAPTER 3	**Configuring Hyper-V**	**131**
CHAPTER 4	**Deploying and configuring core network services**	**197**
CHAPTER 5	**Installing and administering Active Directory**	**257**
CHAPTER 6	**Creating and managing Group Policy**	**317**
	Index	*377*

Contents

Introduction **xi**

Microsoft certifications *xi*

Errata & book support *xii*

We want to hear from you *xii*

Stay in touch *xii*

Preparing for the exam **xiii**

Chapter 1 Installing and configuring servers **1**

Objective 1.1: Install servers 2

Planning for a server installation 2

Choosing installation options 6

Upgrading servers 12

Migrating roles 14

Objective summary 16

Objective review 17

Objective 1.2: Configure servers 18

Completing postinstallation tasks 18

Using Server Manager 26

Configuring services 36

Delegating server administration 37

Using Windows PowerShell Desired State Configuration (DSC) 37

Objective summary 39

Objective review 40

Objective 1.3: Configure local storage 41

Planning server storage 41

Understanding Windows disk settings 43
Working with disks 46
Objective summary 62
Objective review 63
Answers . . . 65

Chapter 2 Configuring server roles and features 71

Objective 2.1: Configure file and share access . . . 71
Creating folder shares 72
Assigning permissions 77
Configuring Volume Shadow Copies 86
Configuring NTFS quotas 87
Configuring Work Folders 89
Objective summary 90
Objective review 91
Objective 2.2: Configure print and document services . . . 92
Deploying a print server 92
Sharing a printer 99
Managing documents 103
Managing printers 104
Using the Print and Document Services role 106
Objective summary 111
Objective review 111
Objective 2.3: Configure servers for remote management . . . 112
Using Server Manager for remote management 113
Using Remote Server Administration Tools 121
Working with remote servers 122
Objective summary 123
Objective review 124
Answers . . . 125

Chapter 3 Configuring Hyper-V 131

Objective 3.1: Create and configure virtual machine settings . . . 131
Virtualization architectures 132

Hyper-V implementations 133
Installing Hyper-V 136
Using Hyper-V Manager 138
Configuring resource metering 152
Objective summary 154
Objective review 154

Objective 3.2: Create and configure virtual machine storage. 156
Virtual disk formats 156
Creating virtual disks 157
Configuring pass-through disks 163
Modifying virtual disks 164
Creating checkpoints 165
Configuring Storage Quality of Service (QoS) 166
Connecting to a storage area network (SAN) 167
Objective summary 173
Objective review 173

Objective 3.3: Create and configure virtual networks 174
Creating virtual switches 175
Creating virtual network adapters 181
Configuring NIC teaming in a virtual network environment 185
Creating virtual network configurations 188
Objective summary 190
Objective review 191

Answers. 192

Chapter 4 Deploying and configuring core network services 197

Objective 4.1: Configure IPv4 and IPv6 addressing 197
IPv4 addressing 198
IPv6 addressing 205
Subnetting IPv6 Addresses 210
Planning an IP transition 211
Objective summary 215
Objective review 215

Objective 4.2: Configure servers 216

Understanding DHCP 217
Deploying a DHCP server 222
Deploying a DHCP relay agent 227
Objective summary 230
Objective review 231
Objective 4.3: Deploy and configure the DNS service 232
Understanding the DNS architecture 232
Deploying a DNS server 241
Objective summary 249
Objective review 250
Answers 251

Chapter 5 Installing and administering Active Directory 257

Objective 5.1: Install domain controllers 257
Deploying Active Directory Domain Services 258
Objective summary 274
Objective review 275
Objective 5.2: Create and manage Active Directory users and computers 276
Creating user objects 276
Creating computer objects 285
Managing Active Directory objects 288
Objective summary 294
Objective review 294
Objective 5.3: Create and manage Active Directory groups and organizational units (OUs) 295
Working with groups 300
Objective summary 309
Objective review 310
Answers 311

Chapter 6 Creating and managing Group Policy 317

Objective 6.1: Create Group Policy Objects 317
- Understanding Group Policy Objects 318
- Configuring a Central Store 319
- Using the Group Policy Management Console 319
- Managing starter GPOs 322
- Configuring Group Policy settings 323
- Creating multiple local GPOs 324
- Objective summary 326
- Objective review 327

Objective 6.2: Configure security policies 328
- Defining local policies 328
- Using security templates 333
- Configuring local users and groups 336
- Unserstanding User Account Control (UAC) 339
- Objective summary 344
- Objective review 344

Objective 6.3: Configure application restriction policies 345
- Using software restriction policies 345
- Using AppLocker 352
- Objective summary 355
- Objective review 355

Objective 6.4: Configure Windows Firewall 357
- Understanding Windows Firewall settings 357
- Working with Windows Firewall 358
- Using the Windows Firewall control panel applet 359
- Using the Windows Firewall With Advanced Security console 363
- Objective summary 369
- Objective review 369

Answers. 371

Index *377*

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/

Introduction

Most books take a very low-level approach, teaching you how to use basic concepts to accomplish fine-grained tasks. Like the Microsoft 70-410 certification exam, this book takes a high-level approach, building on your existing knowledge of lower-level Microsoft Windows system administration and extending it into higher-level server concepts needed for Windows Server 2012 R2.

Candidates for this exam are Information Technology (IT) Professionals who have Windows Server 2012 R2 operating system knowledge and experience and want to validate the skills and knowledge necessary to implement the Windows Server 2012 R2 core infrastructure services.

The 70-410 exam is the first in a series of three exams that validate the skills and knowledge necessary to implement a core Windows Server 2012 R2 Infrastructure into an existing enterprise environment. This book covers the initial implementation and configuration of the Windows Server 2012 R2 core services, such as Active Directory and the networking services. This book, along with the Exam Reference books covering the 70-411 and 70-412 exams, will collectively illustrate the skills and knowledge necessary for implementing, managing, maintaining and provisioning services and infrastructure in a Windows Server 2012 R2 environment.

This book covers every exam objective, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions themselves and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the links you'll find in text to find more information and take the time to research and study the topic. Great information is available on MSDN, TechNet, and in blogs and forums.

Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

MORE INFO **ALL MICROSOFT CERTIFICATIONS**

For information about Microsoft certifications, including a full list of available certifications, go to *http://www.microsoft.com/learning/en/us/certification/cert-default.aspx*.

Errata & book support

We've made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed at:

http://aka.ms/ER410R2/errata

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, email Microsoft Press Book Support at mspinput@microsoft.com.

Please note that product support for Microsoft software is not offered through the addresses above.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

http://aka.ms/tellpress

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

Preparing for the exam

Microsoft certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. While there is no substitution for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. We recommend that you round out your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Training Guide and another study guide for your "at home" preparation and take a Microsoft Official Curriculum course for the classroom experience. Choose the combination that you think works best for you.

CHAPTER 3

Configuring Hyper-V

The concept of virtualizing servers has, in the past several years, grown from a novel experiment to a convenient lab and testing tool to a legitimate deployment strategy for production servers. Windows Server 2012 R2 includes the Hyper-V role, which enables administrators to create virtual machines (VMs), each of which runs in its own isolated environment. VMs are self-contained units that administrators can easily move from one physical computer to another, greatly simplifying the process of deploying network applications and services.

This chapter covers some of the fundamental tasks that administrators perform to create and deploy Hyper-V servers and VMs.

Objectives in this chapter:

- Objective 3.1: Create and configure virtual machine settings
- Objective 3.2: Create and configure virtual machine storage
- Objective 3.3: Create and configure virtual networks

Objective 3.1: Create and configure virtual machine settings

Server virtualization in Windows Server 2012 R2 is based on a module called a *hypervisor*. Sometimes called a *virtual machine monitor (VMM)*, the hypervisor is responsible for abstracting the computer's physical hardware and creating multiple virtualized hardware environments, called VMs. Each VM has its own (virtual) hardware configuration and can run a separate copy of an operating system (OS). Therefore, with sufficient physical hardware and the correct licensing, a single computer running Windows Server 2012 R2 with the Hyper-V role installed can support multiple VMs, which administrators can manage as if they were standalone computers.

> ***NOTE*** **REMOTEFX**
>
> **RemoteFX enables remote computers to connect Hyper-V guest VMs with an enhanced desktop experience, including graphics adapter virtualization, USB redirection, and intelligent encoding and decoding. Don't expect many questions about RemoteFX on the exam.**

This objective covers how to:

- Configure dynamic memory
- Configure smart paging
- Configure Resource Metering
- Configure guest integration services
- Create and configure Generation 1 and Generation 2 VMs
- Configure and use enhanced session mode

Virtualization architectures

Virtualization products can use several different architectures to share a computer's hardware resources among VMs. The earlier type of virtualization products, including Microsoft Windows Virtual PC and Microsoft Virtual Server, requires a standard OS installed on a computer. This becomes the "host" OS. Then you install the virtualization product, which adds the hypervisor component. The hypervisor essentially runs alongside the host OS, as shown in Figure 3-1, and enables you to create as many VMs as the computer has hardware to support.

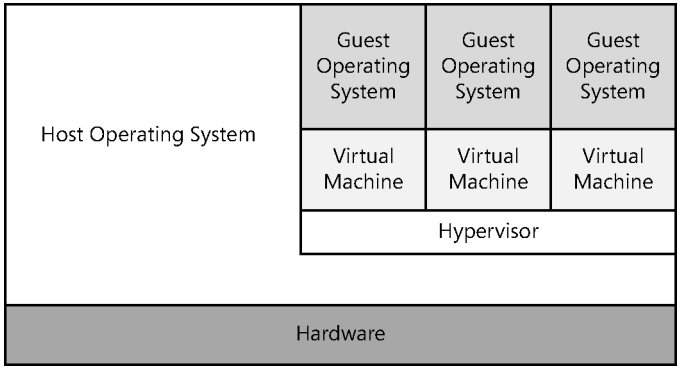

FIGURE 3-1 A hybrid VMM sharing hardware access with a host operating system

This arrangement, in which the hypervisor runs on top of a host OS, is called *Type II virtualization*. By using the Type II hypervisor, you create a virtual hardware environment for each VM. You can specify how much memory to allocate to each VM, create virtual disk drives by using space on the computer's physical drives, and provide access to peripheral devices. You then install a "guest" OS on each VM, just as if you were deploying a new computer. The host OS then shares access to the computer's processor with the hypervisor, with each taking the clock cycles it needs and passing control of the processor back to the other.

Type II virtualization can provide adequate VM performance, particularly in classroom and laboratory environments, but it does not provide performance equivalent to separate physical computers. Therefore, it is not generally recommended for high-traffic servers in production environments.

The virtualization capability built into Windows Server 2012 R2, called Hyper-V, uses a different type of architecture. Hyper-V uses Type I virtualization, in which the hypervisor is an abstraction layer that interacts directly with the computer's physical hardware—that is, without an intervening host OS. The term *hypervisor* is intended to represent the level beyond the term *supervisor,* in regard to the responsibility for allocating a computer's processor clock cycles.

The hypervisor creates individual environments called *partitions*, each of which has its own OS installed and accesses the computer's hardware via the hypervisor. Unlike Type II virtualization, no host OS shares processor time with the hypervisor. Instead, the hypervisor designates the first partition it creates as the parent partition and all subsequent partitions as child partitions, as shown in Figure 3-2.

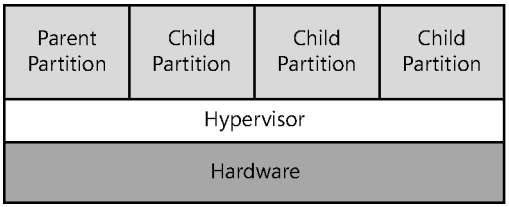

FIGURE 3-2 A Type I VMM, with the hypervisor running directly on the hardware

The parent partition accesses the system hardware through the hypervisor, just as the child partitions do. The only difference is that the parent runs the virtualization stack, which creates and manages the child partitions. The parent partition is also responsible for the subsystems that directly affect the performance of the computer's physical hardware, such as Plug and Play, power management, and error handling. These subsystems also run in the OSs on the child partitions, but they address only virtual hardware, whereas the parent, or root, partition handles the actual hardware.

NOTE **HYPER-V**

It might not seem like the Hyper-V role in Windows Server 2012 R2 provides Type I virtualization, because it requires the Windows Server OS to be installed and running. However, adding the Hyper-V role actually converts the installed instance of Windows Server 2012 R2 into the parent partition and causes the system to load the hypervisor before the OS.

Hyper-V implementations

Windows Server 2012 R2 includes the Hyper-V role only in the Standard and Datacenter editions. The Hyper-V role is required for the OS to function as a computer's primary partition, enabling it to host other VMs. No special software is required for an OS to function as a guest OS in a VM. Therefore, although Windows Server 2012 R2 Essentials does not include the Hyper-V role, it can function as a guest OS. Other guest OSs supported by Hyper-V include the current Windows workstation OSs and many other non-Microsoft server and workstation products.

Hyper-V licensing

The primary difference between the Standard and Datacenter editions of Windows Server 2012 R2 is the number of VMs they support. When you install a Windows Server 2012 R2 instance on a VM, you must have a license for it, just like when you install it on a physical machine. Purchasing the Datacenter edition allows you to license an unlimited number of VMs running Windows Server 2012 R2 on that one physical machine. The Standard license allows you to license only two virtual instances of Windows Server 2012 R2.

IMPORTANT **READERAID HEADER**

Readeraid. You might find that reports vary on the specific minimum requirements of Windows Server 2008. This is not uncommon for new operating systems because the minimum requirements change as the operating system moves from beta to the release candidate stage to the final RTM version. The requirements outlined in Table 1-1 are not finalized. You might be able to get Windows Server 2008 to install on a computer that does not meet these specifications, but the experience will be less than optimal.

Hyper-V hardware limitations

The Windows Server 2012 R2 version of Hyper-V contains massive improvements in the scalability of the system over previous versions. A Windows Server 2012 R2 Hyper-V host system can have up to 320 logical processors, supporting up to 2,048 virtual CPUs and up to 4 terabytes (TB) of physical memory.

One server can host as many as 1,024 active VMs and a single VM can have up to 64 virtual CPUs and up to 1 TB of memory.

Hyper-V can also support clusters with up to 64 nodes and 8,000 VMs.

NOTE **WINDOWS POWERSHELL**

Another major improvement in the Windows Server 2012 and Windows Server 2012 R2 versions of Hyper-V is the inclusion of a Hyper-V module for Windows PowerShell, which includes new cmdlets dedicated to the creation and management of the Hyper-V service and its VMs.

Hyper-V Server

In addition to the Hyper-V implementation in Windows Server 2012 R2, Microsoft provides a dedicated Hyper-V Server product, which is a subset of Windows Server 2012 R2. Hyper-V Server 2012 R2 includes the Hyper-V role, which it installs by default during the OS installation. With the exception of some limited File and Storage Services and Remote Desktop capabilities, the OS includes no other roles, as shown in Figure 3-3.

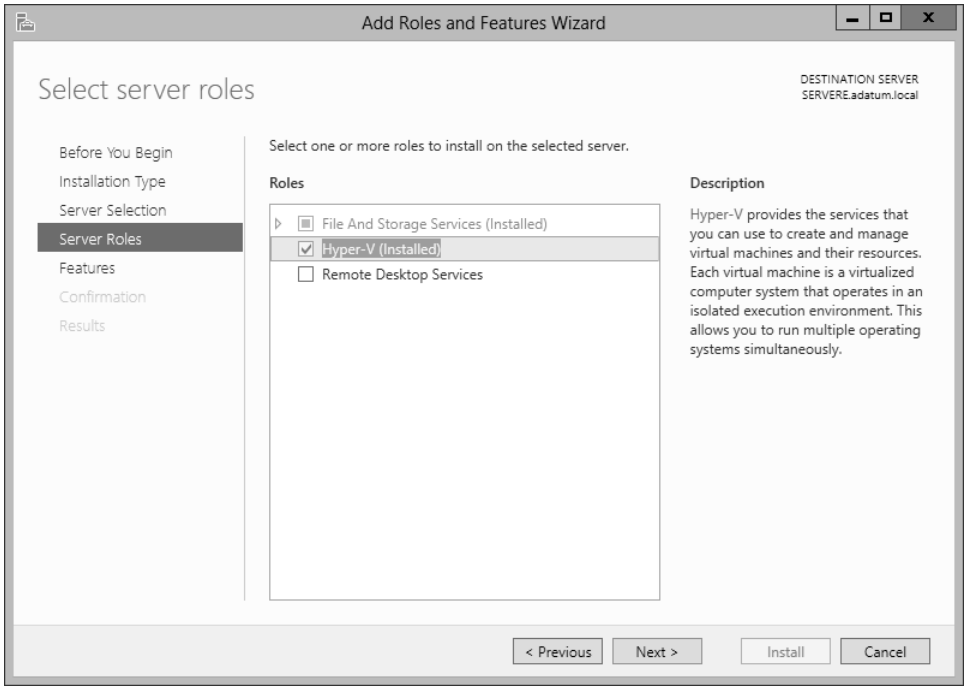

FIGURE 3-3 Roles available in Hyper-V Server

The Hyper-V Server is also limited to the Server Core interface, althoughas with all Server Core installationsit includes SCONFIG, a simple, script-based configuration interface, as shown in Figure 3-4. You can manage Hyper-V Server remotely by using Server Manager and Hyper-V Manager, just as you would any other Server Core installation.

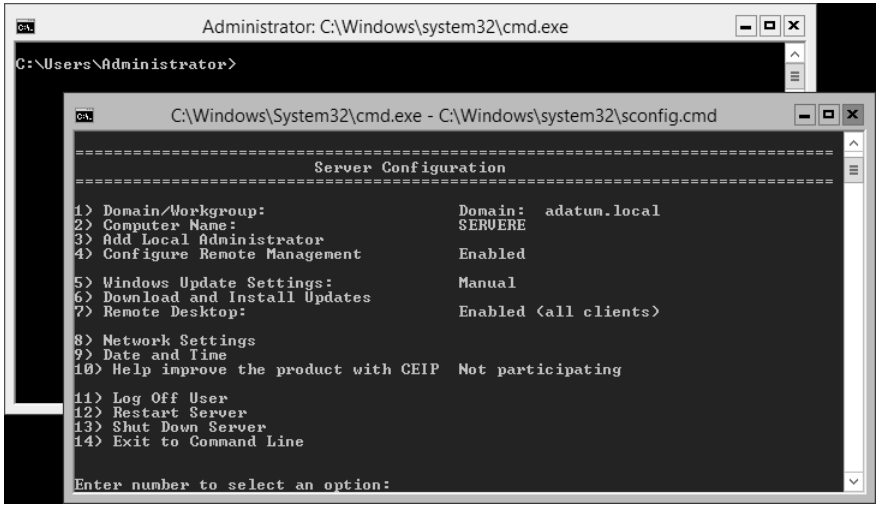

FIGURE 3-4 The Server Core interface in Hyper-V Server

Unlike Windows Server 2012 R2, Hyper-V Server is a free product, available for download from Microsoft's website. However, Hyper-V Server does not include any licenses for virtual instances. You must obtain and license all the OSs you install on the VMs you create.

Installing Hyper-V

Once you have the appropriate hardware, you can add the Hyper-V role to Windows Server 2012 R2 by using Server Manager, just as you would any other role.

Adding the Hyper-V role installs the hypervisor software, and, in the case of a full GUI installation, also installs the management tools. The primary tool for creating and managing VMs and their components on Hyper-V servers is the Hyper-V Manager console. Hyper-V Manager provides administrators with a list of all the VMs on the local host and enables administrators to configure the environments of both the servers and the individual VMs. There is also a set of Hyper-V cmdlets for Windows PowerShell that enables you to exercise complete control over VMs using that interface.

Microsoft recommends that you do not install other roles with Hyper-V. It is better to implement any other roles that you need the physical computer to perform within one of the VMs you create by using Hyper-V. In addition, you might want to consider installing Hyper-V on a computer by using the Server Core installation option. This will minimize the overhead expended on the partition. As with other roles, installing Hyper-V on Server Core excludes the graphical management tools, which you must install separately as a feature on another computer.

Before you can install the Hyper-V role on a server running Windows Server 2012 R2, you must have the appropriate hardware:

- A 64-bit processor that includes hardware-assisted virtualization. This is available in processors that include a virtualization option, such as Intel Virtualization Technology (Intel VT) or AMD Virtualization (AMD-V) technology.
- A system BIOS that supports the virtualization hardware, on which the virtualization feature has been enabled.
- Hardware-enforced Data Execution Prevention (DEP), which Intel describes as eXecute Disable (XD) and AMD describes as No eXecute (NX). This is a technology used in CPUs to segregate areas of memory. Specifically, you must enable the Intel XD bit (execute disable bit) or the AMD NX bit (no execute bit).

To install the Hyper-V role, use the following procedure.

1. In Server Manager, on the Manage menu, select Add Roles And Features. The Add Roles And Features Wizard starts, displaying the Before You Begin page.

2. Click Next to open the Select Installation Type page.
3. Leave the Role-Based Or Feature-Based Installation option selected and click Next. The Select Destination Server page opens.
4. Select the server on which you want to install Hyper-V and click Next. The Select Server Roles page opens.
5. Select the Hyper-V role. The Add Features That Are Required For Hyper-V dialog box appears.
6. Click Add Features to accept the dependencies and then click Next to open the Select Features page.
7. Click Next to open the Hyper-V page.
8. Click Next. The Create Virtual Switches page opens, as shown in Figure 3-5.

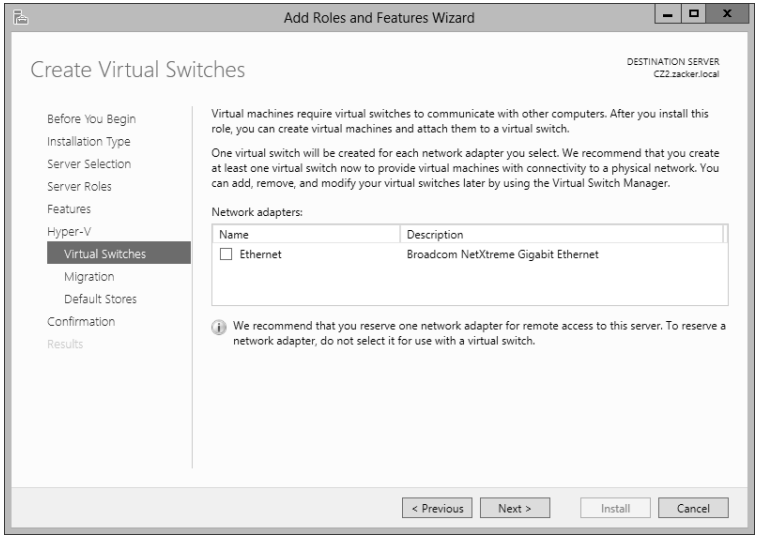

FIGURE 3-5 The Create Virtual Switches page of the Add Roles and Features Wizard

9. Select the appropriate check box for a network adapter and click Next. The Virtual Machine Migration page opens, as shown in Figure 3-6.

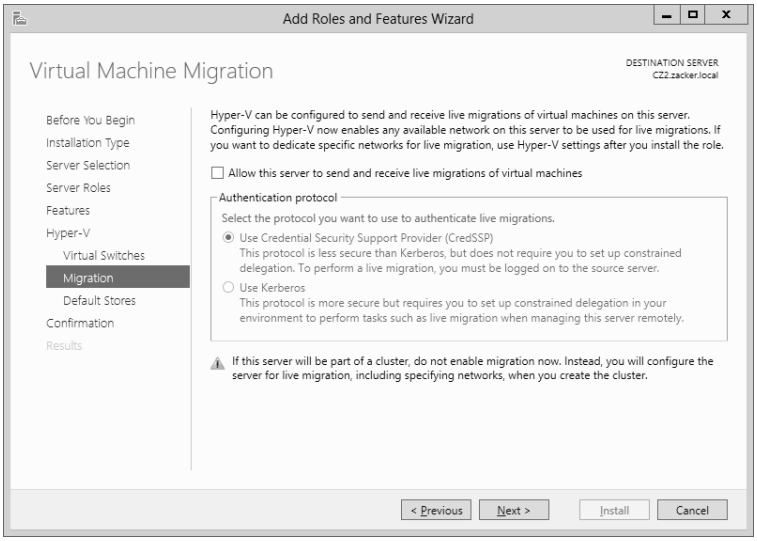

FIGURE 3-6 The Virtual Machine Migration page of the Add Roles and Features Wizard

10. Click Next to open the Default Stores page.
11. Specify alternatives to the default locations for virtual hard disk (VHD) and VM configuration files, if desired, and click Next. The Confirm Installation Selection page opens.
12. Click Install to move to the Installation Progress page as the wizard installs the role.
13. Click Close to close the wizard.
14. Restart the server.

Installing the role modifies the Windows Server 2012 R2 startup procedure so that the newly installed hypervisor is able to address the system hardware directly and then load the OS as the primary partition on top of that.

> ***NOTE*** **USING WINDOWS POWERSHELL**
>
> **You can also install the Hyper-V role by using the Install-WindowsFeature cmdlet, using the following syntax:**

```
Install-WindowsFeature –Name Hyper-V
-ComputerName <name> -IncludeManagementTools -Restart
```

Using Hyper-V Manager

Once you have installed the Hyper-V role and restarted the computer, you can begin to create VMs and deploy OSs on them by using the Hyper-V Manager console, which you can access from the Tools menu in Server Manager.

Like most of the Windows Server 2012 R2 management tools, including Server Manager itself, you can use the Hyper-V Manager console to create and manage VMs on multiple servers, enabling administrators to exercise full control over their servers from a central location.

To run Hyper-V Manager on a server that does not have the Hyper-V role, you must install the Hyper-V Management Tools feature. These tools are also found in the Remote Server Administration Tools feature

Once you install and launch the Hyper-V Manager console, you can add servers to the display by right-clicking the Hyper-V Manager node in the left pane and selecting Connect To Server from the shortcut menu. The Select Computer dialog box appears, in which you can type or browse to the name of a Hyper-V server.

The Hyper-V Manager console lists all the VMs on the selected server, as shown in Figure 3-7, along with status information about each one.

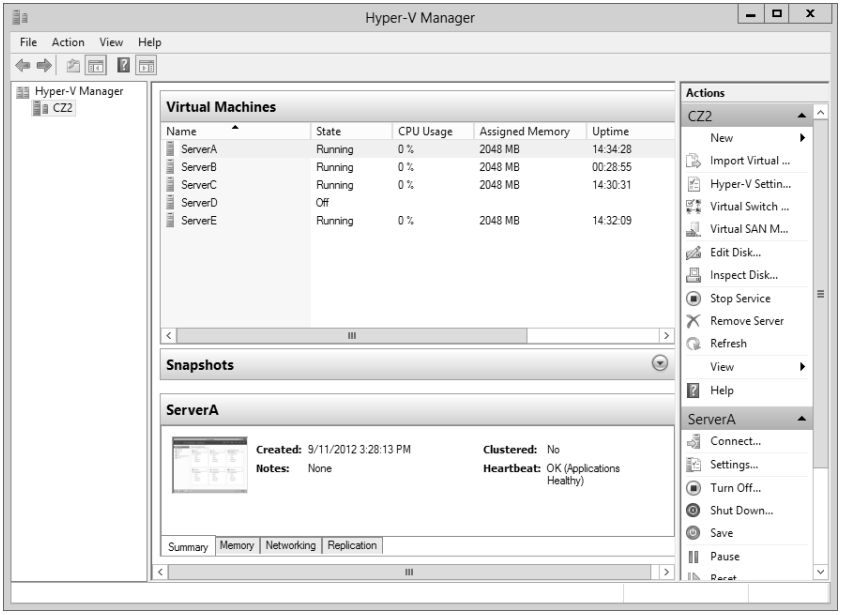

FIGURE 3-7 The Hyper-V Manager console

Creating a virtual machine

After installing Hyper-V and configuring it using Hyper-V Manager, you are ready to create VMs and install the OS on each one. By using Hyper-V Manager, you can create new VMs and define the hardware resources that the system should allocate to them. In the settings for a particular VM, depending on the physical hardware available in the computer and the limitations of the guest OS, administrators can specify the number of processors and the amount of memory allotted to a VM, install virtual network adapters, and create virtual disks by using a variety of technologies, including storage area networks (SANs).

By default, Hyper-V stores the files that make up VMs in the folders you specified on the Default Stores page during the role installation. Each VM uses the following files:

- A virtual machine configuration file in XML format with an .xml extension that contains the VM configuration information, including all settings for the VM
- One or more VHD (.vhd or .vhdx) files to store the guest OS, applications, and data for the VM

In addition, a VM can use a saved-state (.vsv) file if the machine has been placed into a saved state.

To create a new VM, use the following procedure.

1. In Server Manager, on the Tools menu, select Hyper-V Manager to open the Hyper-V Manager console.
2. In the left pane, select a Hyper-V server.
3. From the Action menu, select New, Virtual Machine. The New Virtual Machine Wizard starts, displaying the Before You Begin page.
4. Click Next to open the Specify Name And Location page.
5. In the Name text box, type a name for the VM, keeping in mind that the system will also use this name to create the VM files and folders. To create the VM files in a location other than the default, select the Store The Virtual Machine In A Different Location check box and type an alternate path in the Location text box. Then click Next. The Specify Generation page appears.

MORE INFORMATION **VM GENERATIONS**

For more information on the distinction between Generation 1 virtual machines and Generation 2 virtual machines, see "Creating Generation 1 and Generation 2 VMs" later in this chapter.

6. Specify whether you want to create a Generation 1 or Generation 2 virtual machine and click Next. The Assign Memory page opens.

MORE INFORMATION **MEMORY**

For more information on how Hyper-V uses memory, see "Allocating memory" later in this chapter.

7. In the Startup Memory text box, type the amount of memory you want the VM to use and click Next. The Configure Networking page opens, as shown in Figure 3-8.

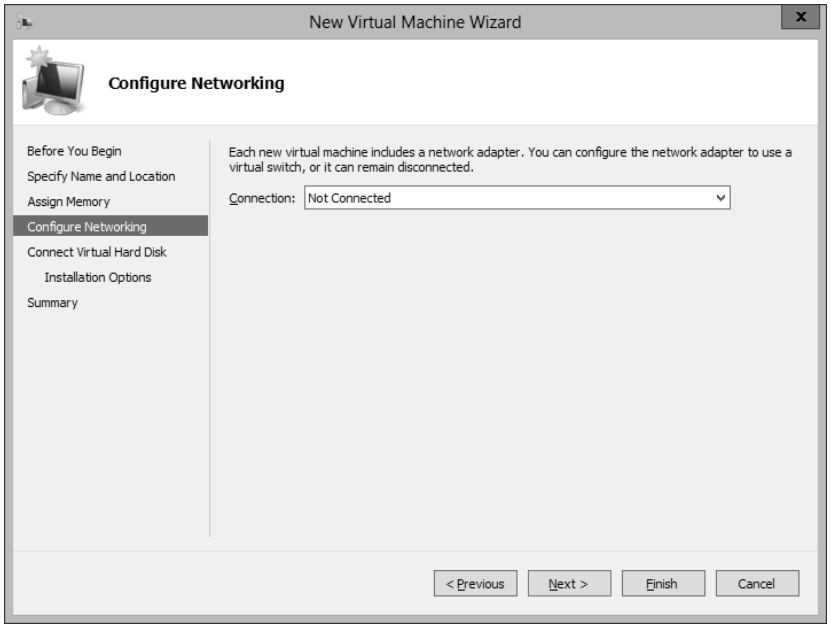

FIGURE 3-8 The Configure Networking page of the New Virtual Machine Wizard

8. From the Connection drop-down list, select a virtual switch and click Next. The Connect Virtual Hard Disk page opens, as shown in Figure 3-9.

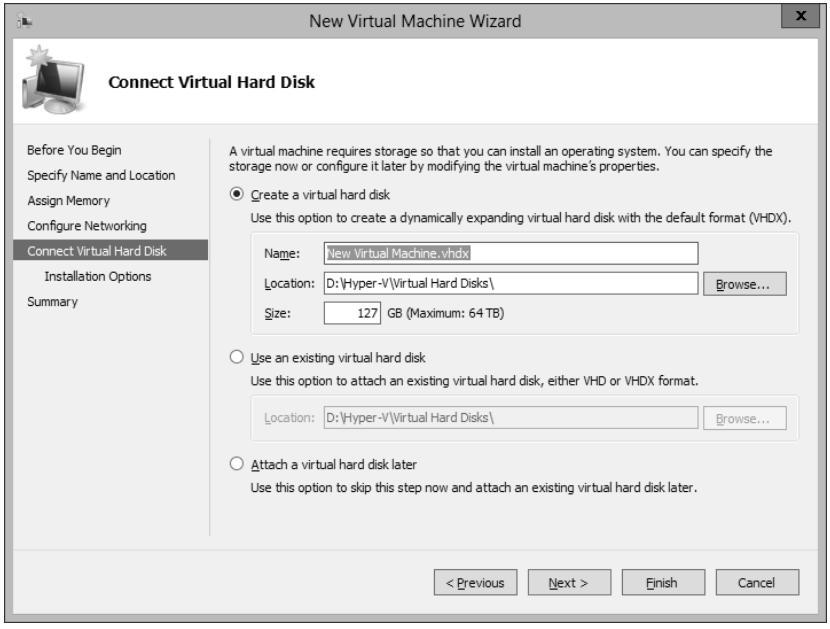

FIGURE 3-9 The Connect Virtual Hard Disk page of the New Virtual Machine Wizard

MORE INFORMATION **NETWORKS**

For more information on virtual switches and networking VMs, see Objective 3.3, "Create and configure virtual networks," later in this chapter.

9. Leave the Create A Virtual Hard Disk option selected and type values for the following fields:
   - **Name** Specifies the file name for the VHD, using the .vhdx format new to Windows Server 2012 R2
   - **Location** Specifies a location for the VHD other than the default you specified on the Default Stores page
   - **Size** Specifies the maximum size of the VHD

MORE INFORMATION **STORAGE**

By default, the wizard creates a VHD file that starts small and dynamically expands up to the maximum size you specify. For more information on Hyper-V storage, see Objective 3.2, "Create and configure virtual machine storage," later in this chapter.

10. Click Next. The Installation Options page opens.
11. Leave the Install An Operating System Later Option selected and click Next. The Completing The New Virtual Machine Wizard page opens.
12. Click Finish. The wizard creates the new VM and adds it to the list of VMs in Hyper-V Manager.

The VM that this procedure creates is the equivalent of a bare-metal computer. It has all the (virtual) hardware it needs to run, but it has no software.

NOTE **USING WINDOWS POWERSHELL**

To create a new VM by using Windows PowerShell, use the New-VM cmdlet with the following basic syntax:

```
New-VM –Name "VM name" –MemoryStartupBytes <memory>

–NewVHDSizeBytes <disk size>
```

For example, the following command creates a new VM called ServerA with 1 GB of memory and a new 60-GB VHD drive:

```
New-VM –Name "ServerA" –MemoryStartupBytes 1GB

–NewVHDSizeBytes 60GB
```

There are, of course, many more parameters for the New-VM cmdlet, which you can explore through the Get-Help cmdlet.

Each VM on a Hyper-V server consists of a collection of settings that specify the hardware resources in the machine and the configuration settings that control those resources. You can manage and modify those settings by using the Settings page for the particular VM.

Selecting a VM from the list in Hyper-V Manager displays a series of icons in the Actions pane. Clicking the Settings icon opens the Settings dialog box, shown in Figure 3-10, which is the primary configuration interface for that VM. Here, you can modify any of the settings that the New Virtual Machine Wizard configured for you.

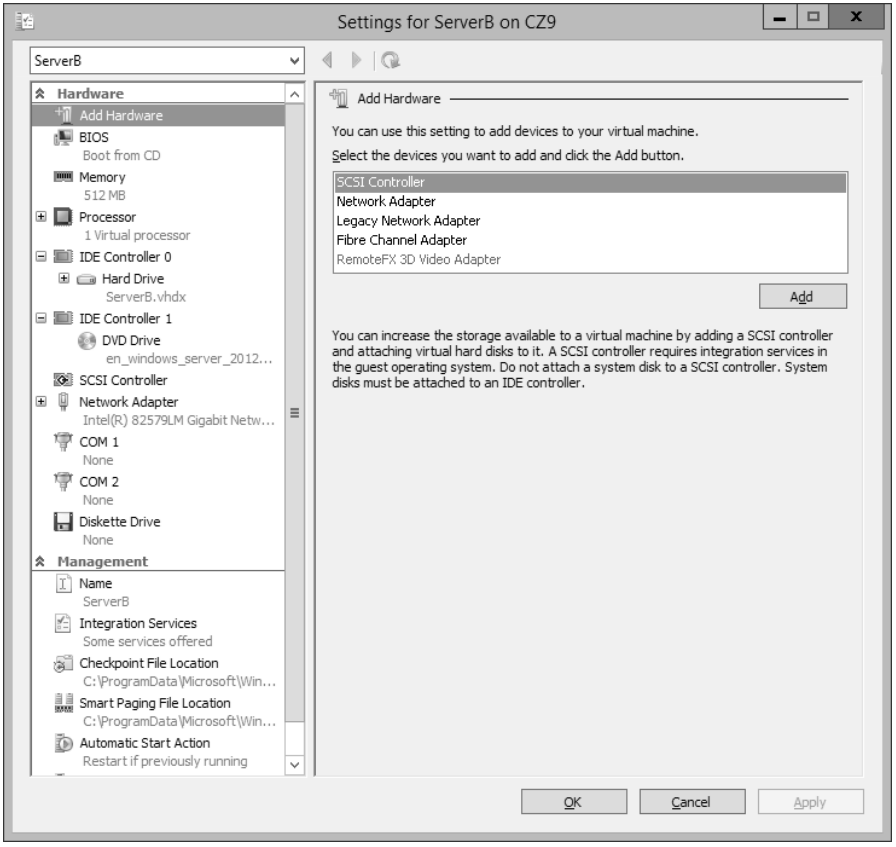

FIGURE 3-10 The Settings dialog box for a VM

Creating Generation 1 and Generation 2 VMs

In Windows Server 2012 R2, Hyper-V includes a new type of virtual machine, which it refers to as Generation 2. The VM type created by all previous versions is called Generation 1. When you create a new virtual machine in the Hyper-V manager, the New Virtual Machine Wizard includes a new page (shown in Figure 3-11) on which you specify whether you want to create a Generation 1 or Generation 2 VM. The New-VM cmdlet in Windows PowerShell also includes a new –Generation parameter.

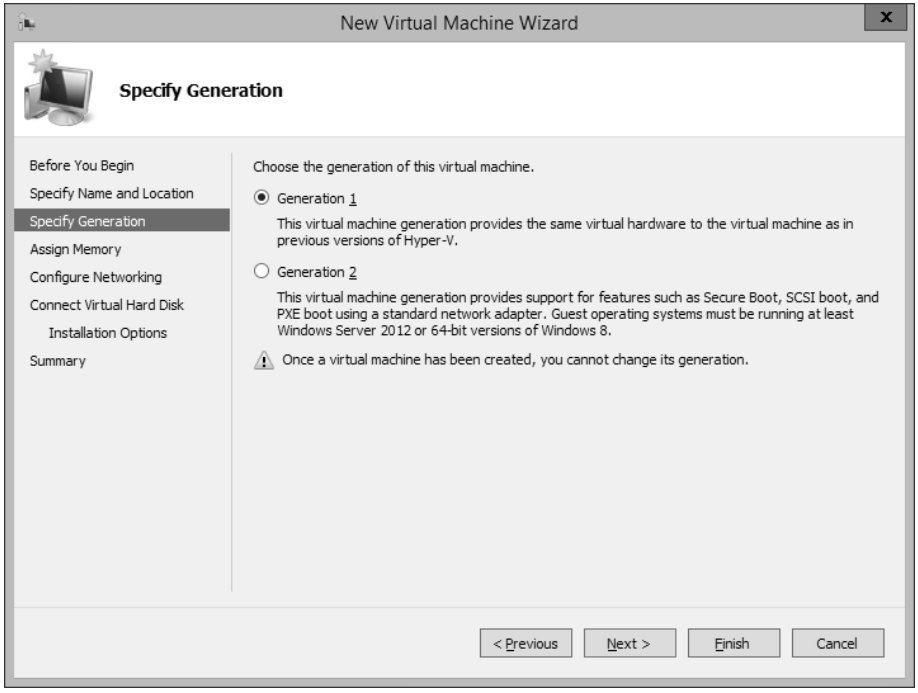

FIGURE 3-11 The Specify Generation page in the New Virtual Machine Wizard

Generation 1 VMs are designed to emulate the hardware found in a typical computer. To do this, they use drivers for specific devices, such as an AMI BIOS, an S3 graphics adapter, and an Intel chipset and network adapter. Generation 1 VMs that you create with Windows Server 2012 R2 Hyper-V are completely compatible with all previous Hyper-V versions.

Generation 2 VMs use synthetic drivers and software-based devices instead; they provide advantages that include the following:

- **UEFI boot** Instead of using the traditional BIOS, Generation 2 VMs support Secure Boot using the Universal Extensible Firmware Interface (UEFI), which requires a system to boot from digitally signed drivers and enables them to boot from drives larger than 2 TB with GUID partition tables.
- **SCSI disks** Generation 2 VMs omit the IDE disk controller used by Generation 1 VMs to boot the system and use a high-performance virtual SCSI controller for all disks, enabling the VMs to boot from VHDX files and support hot-disk adds and removes.

The end result is a Generation 2 virtual machine that deploys much faster than its Generation 1 counterparts and performs better as well. The limitations, however, are that Generation 2 VMs can only run the following guest operating systems:

- Windows Server 2012
- Windows Server 2012 R2
- Windows 8 64-bit
- Windows 8.1 64-bit

Installing an operating system

Once you have created a VM, you can install an OS on it. Hyper-V in Windows Server 2012 R2 supports all the following as OSs you can install in Generation 1 VMs:

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Home Server 2011
- Windows Small Business Server 2011
- Windows Server 2003 R2
- Windows Server 2003 SP2
- Windows 8.1
- Windows 8
- Windows 7 Enterprise and Ultimate
- Windows Vista Business, Enterprise, and Ultimate SP2
- Windows XP Professional SP3
- Windows XP x64 Professional SP2
- CentOS 6.0–6.2
- Red Hat Enterprise Linux 6.0–6.2
- SUSE Linux Enterprise Server 11 SP2

NOTE **GUEST OSS**

This is the official list of supported guest OSs at RTM. Other OSs might also function but have not been fully tested.

One of the advantages of installing software on VMs is that there are several ways to access the installation files. A VM, by default, has a DVD drive, which can itself be physical or virtual.

When you open the Settings dialog box for a Generation 1 VM and select the DVD drive in the Hardware list, you see the interface shown in Figure 3-12. In the Media section, you can select one of the following options for the drive:

- **None** The equivalent of a drive with no disk inserted
- **Image File** Points to a disk image file with a .iso extension stored on one of the host computer's drives or on a shared network drive
- **Physical CD/DVD Drive** Links the virtual DVD drive to one of the physical DVD drives in the host computer

In a Generation 2 VM, the DVD drive supports only the None option and the Image File option, as shown in Figure 3-12. The ability to mount an image file to a virtual DVD drive is particularly useful for administrators who download OS files as disk images. Once you have mounted an installation disk, either physically or virtually, you can click Start in the Actions pane of Hyper-V Manager, which is the equivalent of turning on the VM.

Starting a VM causes the thumbnail in the Hyper-V Manager to go live, displaying the contents of the computer's screen. To display the VM's activity at full size, click Connect in the Actions pane to open a new window for the VM. You can then interact with the VM through that window, just as if you were sitting at a physical computer's console.

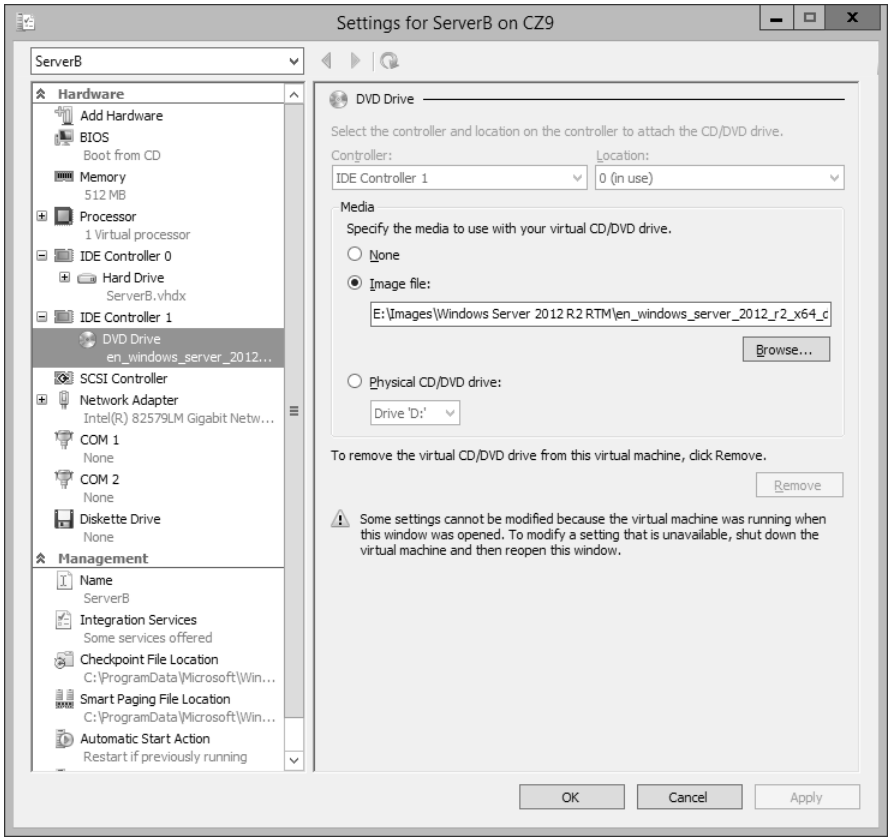

FIGURE 3-12 DVD drive settings for a VM

When the VM boots from the disk you mounted, the OS installation proceeds just as if you were using a physical computer. During the installation process, you can work with the VHD drive just as you would a physical one, creating partitions of various sizes and selecting one for the OS. When the installation is complete, the VM restarts, and you can then log on and use it in the normal manner.

Configuring Guest Integration Services

In some cases, certain Hyper-V guest OS features do not function properly using the OS's own device drivers. Hyper-V, therefore, includes a software package called Guest Integration Services, which you can install on your VMs for compatibility purposes.

Some of the functions provided by the Guest Integration Services package are as follows:

- **Operating System Shutdown** Enables the Hyper-V Manager console to remotely shut down a guest OS in a controlled manner, eliminating the need for an administrator to log on and manually shut the system down.
- **Time Synchronization** Enables Hyper-V to synchronize the OS clocks in parent and child partitions.
- **Data Exchange** Enables the Windows OSs on the parent and child partitions to exchange information, such as OS version information and fully qualified domain names.
- **Heartbeat** Implements a service in which the parent partition sends regular heartbeat signals to the child partitions, which are expected to respond in kind. A failure of a child partition to respond indicates that the guest OS has frozen or malfunctioned.
- **Backup** Enables backup of Windows VMs by using Volume Shadow Copy Services.
- **Guest Services** Enables administrators to copy files to a virtual machine without using a network connection.

The Windows Server 2012, Windows Server R2, Windows 8, and Windows 8.1 operating systems have the latest Guest Integration Services software built in, so there is no need to install the package on VMs running those OSs as guests. Earlier versions of Windows have earlier versions of the Guest Integration Services package that need to be upgraded, however, and some Windows versions do not include the package at all.

> ***NOTE*** **LINUX**
>
> **For Linux guest OSs, you must download and install the latest release of Linux Integration Services Version 3.4 for Hyper-V from the Microsoft Download Center. As of this writing, the latest version is 3.4 and is available at *http://www.microsoft.com/en-gb/download/details.aspx?id=34603*.**

To upgrade Guest Integration Services on a Windows guest OS, use the following procedure:

1. In Server Manager, on the Tools menu, select Hyper-V Manager. The Hyper-V Manager console starts.
2. In the left pane, select a Hyper-V server.
3. In the Actions pane, start the VM on which you want to install Guest Integration Services and click Connect. A Virtual Machine Connection window opens.
4. In the Virtual Machine Connection window, from the Action menu, select Insert Integration Services Setup Disk. Hyper-V mounts an image of the Guest Integration Services disk to a virtual disk drive and an Autoplay window appears.

5. Click Install Hyper-V Integration Services. A message box appears, asking you to upgrade the existing installation.
6. Click OK. The system installs the package and prompts you to restart the computer.
7. Click Yes to restart the computer.

Once you have installed or upgraded Guest Integration Services, you can enable or disable each of the individual functions by opening the Settings dialog box for the VM and selecting the Integration Services page, as shown in Figure 3-13.

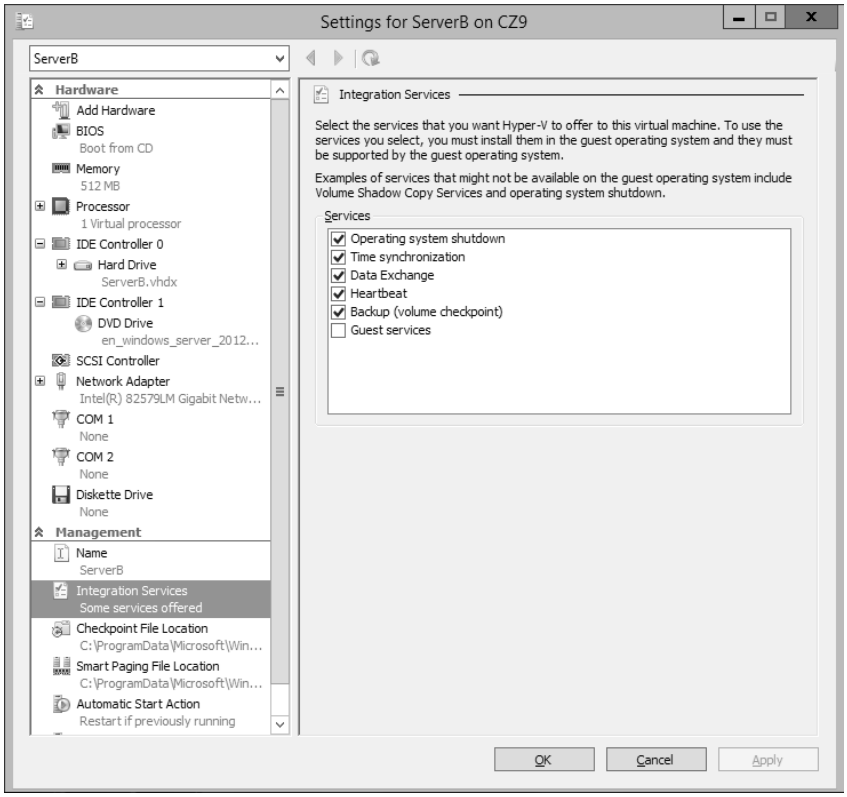

FIGURE 3-13 Integration Services settings for a VM

At this point, you are ready to configure and manage the VM just as if you were working on a physical server. This can include modifying the network configuration, enabling remote desktop, loading the appropriate roles and features, and installing applications.

Using Enhanced Session mode

In previous versions of Hyper-V, when you open a Virtual Machine Connection window in the Hyper-V Manager console, you receive mouse and keyboard connectivity plus a limited cut and paste functionality. To obtain any further access, such as audio or print functionality, you could establish a Remote Desktop Services connection to the VM, but this requires the computers to be connected to the same network, which is not always possible.

Starting in Windows Server 2012 R2, Hyper-V supports an enhanced session mode that enables the Virtual Machine Connection window to redirect any of the following local resources to VMs running Windows Server 2012 R2 or Windows 8.1:

- Display configuration
- Audio
- Printers
- Clipboard
- Smart cards
- USB devices
- Drives
- Supported Plug and Play devices

The enhanced session mode works by establishing a Remote Desktop Protocol connection between the host computer and the VM, but it does not require a standard network path because it uses VMBus instead. *VMBus* is a high-speed conduit between the various partitions running on a Hyper-V server.

Enhanced session mode is enabled by default in Windows 8.1, but in Windows Server 2012 R2, you must enable it on the Enhanced Session Mode Policy page of the Hyper-V Settings dialog box, as shown in Figure 3-14.

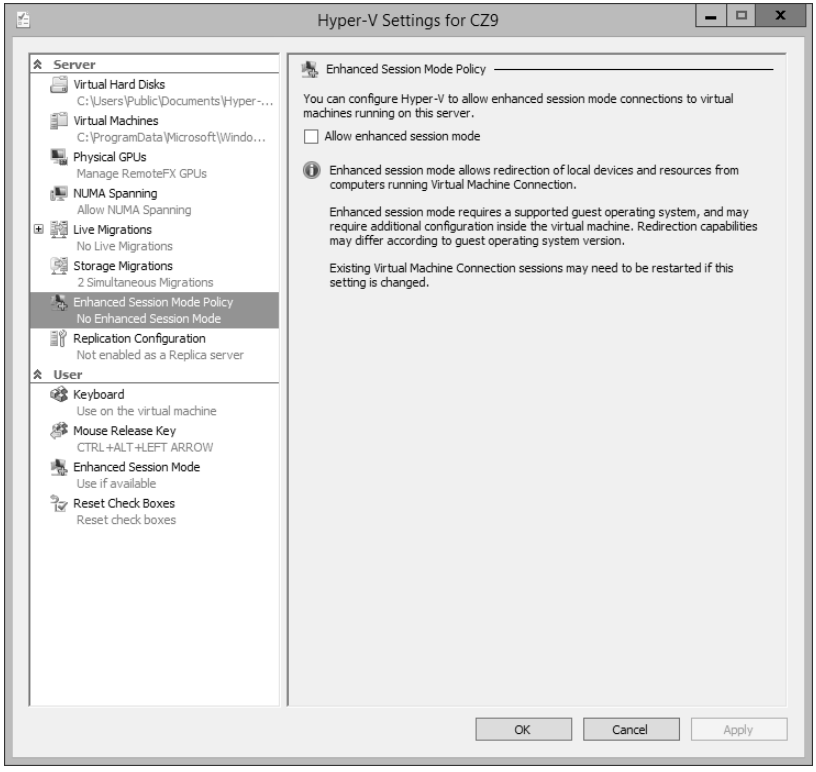

FIGURE 3-14 Enhanced Session Mode Policy settings

Allocating memory

Dynamic memory enables Hyper-V to adjust the amount of RAM allocated to VMs, depending on their ongoing requirements. Some computer components can be virtualized. You can take some disk space and create a virtual hard drive, and you can take an image file and create a virtual DVD drive. You can also create virtual network interface adapters and other components, which appear like the real thing in a VM. System memory is different, however. There is no substitute for memory, so all Hyper-V can do is take the physical memory installed in the computer and allocate it among the various VMs.

When you create a VM, you specify how much memory to allocate to the VM. Obviously, the amount of memory available for use is based on the physical memory installed in the computer.

After you have created the VM, you can modify the amount of memory allocated to it by shutting down the VM, opening its Settings dialog box, and changing the Startup RAM setting on the Memory page, as shown in Figure 3-15. This enables you to experiment with various amounts of memory, and set the optimum performance level for the system.

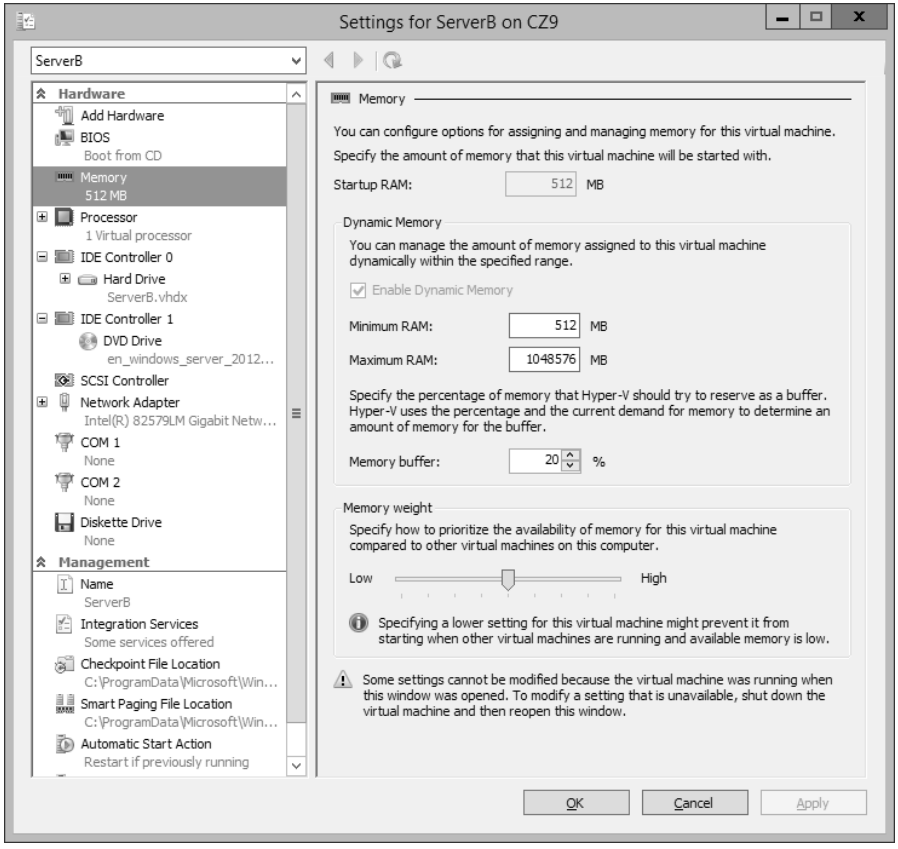

FIGURE 3-15 Memory settings for a VM

USING DYNAMIC MEMORY

In the first versions of Hyper-V, shutting down the VM was the only way to modify its memory allocation. In the Windows Server 2012 R2 version, however, you can use a feature called Dynamic Memory to automatically reallocate memory to the VM from a shared memory pool as its demands change. If a virtualized server starts to experience larger amounts of client traffic, for example, Hyper-V can increase the memory allocated to the system, and reduce it again when the traffic subsides.

To use Dynamic Memory, you must enable it by selecting the Enable Dynamic Memory check box on the VM's Memory settings page and then configure the following settings:

- **Startup RAM** Specifies the amount of memory that you want to allocate to the VM when it starts. When you are using Dynamic Memory, this value can be the minimum amount of memory needed to boot the system.
- **Minimum RAM** Specifies the smallest amount of memory the VM can use at any time. OSs can require more memory to start up than to run, so this value can be smaller than the Startup RAM value.
- **Maximum RAM** Specifies the largest amount of memory that the VM can use at any time. The value can range from a low equal to the Startup RAM value to a high of 64 GB.
- **Memory Buffer** Specifies a percentage that Hyper-V uses to calculate how much memory to allocate to the VM, compared to its actual utilization, as measured by performance counters. For example, with the Memory Buffer value set to 20 percent, a VM with applications and OS that consume 1 GB of memory will receive a dynamic allocation of 1.2 GB.
- **Memory Weight** Specifies a relative value that specifies the priority of this VM compared to the other VMs on the same computer. When the physical memory in the computer is insufficient to allocate the full-buffered amount specified for each VM, the VMs with the highest Memory Weight settings receive priority.

> ***NOTE*** **RAM**
>
> **You can reduce the Minimum RAM, increase the Maximum RAM, or change the Memory Buffer value or the Memory Weight value at any time, but to enable or disable Dynamic Memory, you must shut down the VM.**

In addition to configuring the VM settings, the guest VM must be running Windows Vista or later or Windows Server 2003 SP2 or later and have Windows Server 2012 R2 Guest Integration Services installed to use Dynamic Memory.

NOTE **USING WINDOWS POWERSHELL**

To configure the memory settings for a VM, use the Set-VMMemory cmdlet by using the following basic syntax:

```
Set-VMMemory <VM name> -DynamicMemoryEnabled $true
-MinimumBytes <memory> -StartupBytes <memory>
-MaximumBytes <memory> -Priority <value> -Buffer <percentage>
```

For example, to configure the memory settings for the VM ServerA, enabling Dynamic Memory and configuring values for all of its settings, use the following command:

```
Set-VMMemory ServerA -DynamicMemoryEnabled $true
-MinimumBytes 64MB
```

CONFIGURING SMART PAGING

Dynamic Memory was introduced in Windows Server 2008 R2 Hyper-V, but Windows Server 2012 R2 improves on the concept by adding the Minimum RAM setting. This makes it possible for Hyper-V to reduce the memory used by a VM to a level lower than that needed to start the system, reclaiming that memory for other uses.

The problem with having minimum RAM values that are lower than the startup RAM values is that it becomes possible to deplete the supply of physical memory with too many VMs running simultaneously at their minimum RAM values. If this occurs, a VM that has to restart might be unable to do so because there is not enough free memory to increase its memory allocation from its minimum RAM value to its startup RAM value.

To address this possibility, Hyper-V includes a feature called *smart paging*. If a VM has to restart and there is not enough memory available to allocate its startup RAM value, the system uses hard disk space to make up the difference and begins paging memory contents to disk.

Disk access rates are far slower than memory access rates, of course, so smart paging incurs a severe performance penalty, but the paging occurs only for as long as it takes to restart the VM and return it to its minimum RAM allocation.

Hyper-V only uses smart paging in specific conditions: when a VM must be restarted, there is no free memory available, and there are no other means available to free up the necessary memory.

You can select the Smart Paging File Location page in a VM's Setting dialog box to specify a location for the paging file. Selecting the fastest possible hard drive is recommended.

Configuring resource metering

Resource metering is a Windows PowerShell–based feature in Windows Server 2012 R2 Hyper-V that enables administrators to document VM usage by using a variety of criteria. There are various reasons why organizations might want to track the use of VMs. For large corporations, it might be a matter of internal accounting and controlling ongoing expenses,

such as wide area network (WAN) bandwidth. For service providers, it might be necessary to bill customers based on the VM resources they use.

Resource metering uses Windows PowerShell cmdlets to track a variety of performance metrics for individual VMs, including the following:

- CPU utilization
- Minimum, maximum, and average memory utilization
- Disk space utilization
- Incoming and outgoing network traffic

Resource metering statistics remain consistent, even when you transfer VMs between host systems by using Live Migration or move VHD files between VMs.

To use resource metering, you must first enable it for the specific VM that you want to monitor by using the Enable-VMResourceMetering cmdlet with the following syntax:

```
Enable-VMResourceMetering –VMName <name>
```

Once you have enabled metering, you can display a statistical report at any time by using the Measure-VM cmdlet with the following syntax:

```
Measure-VM –VMName <name>
```

In addition to metering resources for entire VMs, administrators can also create resource pools that enable them to monitor specific VM components, such as processors, memory, network adapters, and VHDs. You create a resource pool by using the New-VMResourcePool cmdlet and then enable metering for the pool by using Enable-VMResourceMetering.

By using techniques such as pipelining, administrators can use the resource metering cmdlets to gather data on VM performance and export it to applications or data files.

Thought experiment

Configuring virtual machine memory

In the following thought experiment, apply what you've learned about this objective to predict what steps you need to take. You can find answers to these questions in the "Answers" section at the end of this chapter.

Alice has a computer with 8 GB of memory installed and running Windows Server 2012 R2, which she has configured as a Hyper-V server. After creating eight VMs, each with a startup RAM value of 1,024 MB, Alice is having trouble getting all eight VMs to boot. What settings can she modify to resolve the problem without changing the startup RAM value?

Objective summary

- Virtualization is a process that adds a layer of abstraction between actual, physical hardware and the system making use of it. Instead of having the server access the computer's hardware directly, an intervening component called a hypervisor creates a VM environment, and the server OS runs in that environment.
- Virtualization is the process of deploying and maintaining multiple instances of an OS, called VMs, on a single computer.
- Microsoft Hyper-V is a hypervisor-based virtualization system for x64 computers starting with Windows Server 2008. The hypervisor is installed between the hardware and the OS and is the main component that manages the virtual computers.
- For licensing purposes, Microsoft refers to each VM that you create on a Hyper-V server as a virtual instance. Each Windows Server 2012 R2 version includes licenses for a set number of virtual instances; you must purchase additional licenses to license additional instances.
- To keep a small footprint and minimal overhead, Hyper-V Server contains only the Windows Hypervisor, Windows Server driver model, and virtualization components.
- Hyper-V in Windows Server 2012 R2 supports two types of VMs: Generation 1 and Generation 2. Generation 1 VMs are designed to emulate the hardware found in a typical computer and are compatible with previous versions of Hyper-V. Generation 2 VMs use synthetic drivers and software-based devices instead and can only run on the Windows Server 2012 R2 Hyper-V.
- Windows Server 2012 R2 Hyper-V supports an enhanced session mode that enables the Virtual Machine Connection window to redirect a variety of local resources to VMs running Windows Server 2012 R2 or Windows 8.1.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which of the following statements about Type I and Type II virtualization are true? (Choose all that apply.)
   - **A.** In Type I virtualization, the hypervisor runs on top of a host OS.
   - **B.** In Type I virtualization, the hypervisor runs directly on the computer hardware.
   - **C.** In Type II virtualization, the hypervisor runs on top of a host OS.
   - **D.** In Type II virtualization, the hypervisor runs directly on the computer hardware.

2. Which of the following types of server virtualization provides the best performance for high-traffic servers in production environments?

   A. Type I virtualization

   B. Type II virtualization

   C. Presentation virtualization

   D. RemoteApp

3. Which of the following Microsoft operating systems includes a license that enables you to license an unlimited number of virtual instances?

   A. Hyper-V Server

   B. Windows Server 2012 R2 Datacenter

   C. Windows Server 2012 R2 Standard

   D. Windows Server 2012 R2 Foundation

4. Which of the following Hyper-V features make it possible for a VM to function with a minimum RAM value that is lower than the startup RAM value? (Choose all that apply.)

   A. Smart paging

   B. Dynamic Memory

   C. Memory Weight

   D. Guest Integration Services

5. When you install the Hyper-V role on a server running Windows Server 2012 R2, the instance of the OS on which you installed the role is converted to what system element?

   A. The hypervisor

   B. The Virtual Machine Monitor

   C. The parent partition

   D. A child partition

6. Which of the following statements about Generation 1 and Generation 2 virtual machines are true? (Choose all that apply.)

   A. You must create a Generation 1 VM before you can create a Generation 2 VM.

   B. Generation 2 VMs deploy faster than Generation 1 VMs.

   C. Generation 2 VMs only support Windows 8.1 and Windows Server 2012 R2 as guest operating systems.

   D. Generation 2 VMs use the same device drivers as Generation 1 VMs.

Objective 3.2: Create and configure virtual machine storage

When you create a VM in Windows Server 2012 R2 Hyper-V, you emulate all the components that you typically find in a physical computer. When you virtualize memory, as discussed in Objective 3.1, "Create and configure virtual machine settings," you take a portion of the physical memory in the computer and dedicate it to a VM. The same is true with hard disk space. Hyper-V uses a specialized VHD format to package part of the space on a physical disk and make it appear to the VM as though it is a physical hard disk drive.

When you create a new Generation 1 VM in Hyper-V, the wizard creates a virtual storage subsystem that consists of two Integrated Drive Electronics (IDE) controllers and one Small Computer Systems Interface (SCSI) controller. The IDE controllers host the VM's system drive and its DVD drive. Like their physical equivalents, each IDE controller can host two devices, so you can create two additional virtual drives and add them to the system.

The SCSI controller in the default Generation 1 VM configuration is unpopulated, and you can create additional drives and add them to that controller to provide the VM with additional storage. In a Generation 2 VM, the system and DVD drives are connected to the default SCSI controller and there is no IDE alternative.

In a VM of either generation, you can also create additional SCSI controllers and add drives to them. By creating multiple drives and controllers, Hyper-V makes it possible to construct virtual storage subsystems that emulate almost any physical storage solution you might devise.

This objective covers how to:

- Create VHDs and VHDX
- Configure differencing drives
- Modify VHDs
- Configure pass-through disks
- Manage checkpoints
- Implement a virtual Fibre Channel adapter
- Configure storage Quality of Service (QoS)

Virtual disk formats

Windows Server 2012 R2 Hyper-V supports the original VHD disk image file and the new VHDX format. The original VHD format was created by a company called Connectix for its Virtual PC product. Microsoft later acquired the product and used the VHD format for all its subsequent virtualization products, including Hyper-V. There are three types of VHD files, as follows:

- **Fixed hard disk image** An image file of a specified size in which all the disk space required to create the image is allocated during its creation. Fixed disk images can be wasteful in terms of storage because they can contain large amounts of empty space, but they are also efficient from a performance standpoint because there is no overhead due to dynamic expansion.
- **Dynamic hard disk image** An image file with a specified maximum size, which starts small and expands as needed to accommodate the data the system writes to it. This option conserves disk space but can negatively affect performance.
- **Differencing hard disk image** A child image file associated with a specific parent image. The system writes all changes made to the data on the parent image file to the child image, to manage disk space or to facilitate a rollback at a later time.

VHD images are limited to maximum size of 2 TB and are compatible with all versions of Hyper-V and Microsoft Type II hypervisor products, such as Virtual Server and Virtual PC. Windows Server 2012 introduced an updated version of the format, which uses a VHDX filename extension.

VHDX image files can be as large as 64 TB, and they also support 4-KB logical sector sizes to provide compatibility with new 4-KB native drives. VHDX files can also use larger block sizes (up to 256 MB), which enable administrators to fine-tune the performance level of a virtual storage subsystem to accommodate specific applications and data file types. However, VHDX files are not backward compatible and can only be read by Windows Server 2012, Windows Server 2012 R2, Windows 8, and Windows 8.1 Hyper-V servers. If migrating your VMs from Windows Server 2012 R2 to an older version of Hyper-V is even a remote possibility, you should continue using the VHD file format.

Creating virtual disks

Windows Server 2012 R2 Hyper-V provides several ways to create virtual disk files. You can create them as part of a VM or create them at another time and add them to a VM. The graphical interface in Hyper-V Manager provides access to most of the VHD parameters, but the Windows PowerShell cmdlets included in Windows Server 2012 R2 provide the most granular control over the disk image format.

Creating a virtual disk with a VM

The New Virtual Machine Wizard includes a Connect Virtual Hard Disk page with which you can add a single disk to your new VM. The options for this disk are relatively limited and consist of the following:

- **Create A Virtual Hard Disk** Enables you to specify the name, location, and size of a new VHD. The wizard only allows you to create a dynamically expanding disk using the VHDX format, but you can also create fixed and differencing VHDX disks using Windows PowerShell.

- **Use An Existing Virtual Hard Disk** Enables you to specify the location of an existing VHD or VHDX disk, which the VM will presumably use as its system disk.
- **Attach A Virtual Hard Disk Later** Prevents the wizard from adding any virtual disks to the VM configuration. The assumption is that you will manually add a disk later, before you start the VM.

The object of this wizard page is to create the disk on which you will install the VM's OS or to select an existing disk on which an OS is already installed. The disk the wizard creates is always a dynamically expanding one connected to IDE Controller 0 on a Generation 1 VM or connected to the SCSI Controller on a Generation 2 VM.

> ***NOTE*** **VHDS**
>
> **It has become a common practice for Microsoft to release evaluation copies of its products as preinstalled VHD files as an alternative to the traditional installable disk images. After downloading one of these files, you can create a VM on a Hyper-V server and select the Use An Existing Virtual Hard Disk option to mount the VHD as its system drive.**

Creating a new virtual disk

You can create a VHD file at any time without adding it to a VM by using the New Virtual Hard Disk Wizard in Hyper-V Manager. To create a new virtual disk, use the following procedure.

1. In Server Manager, on the Tools menu, select Hyper-V Manager. The Hyper-V Manager console opens.
2. In the left pane, select a Hyper-V server.
3. From the Action menu, select New, Hard Disk to start the New Virtual Hard Disk Wizard, displaying the Before You Begin page.
4. Click Next to open the Choose Disk Format page.
5. Select one of the following disk format options:
   - **VHD** Creates an image no larger than 2 TB, using the highly compatible VHD format
   - **VHDX** Creates an image up to 64 TB, using the new VHDX format
6. Click Next to open the Choose Disk Type page.
7. Select one of the following disk type options:
   - **Fixed Size** Creates a disk of a specific size, allocating all of the space at once
   - **Dynamically Expanding** Creates a disk that can grow to the maximum size you specify as you add data
   - **Differencing** Creates a child drive that will contain changes made to a specified parent drive

8. Click Next. The Specify Name And Location page opens.
9. Specify a file name for the disk image in the Name text box and, if desired, specify a location for the file other than the server default. Click Next to open the Configure Disk page.
10. For fixed and dynamically expanding disks, select and configure one of the following options:
    - **Create A New Blank Virtual Hard Disk** Specifies the size (or the maximum size) of the disk image file to create
    - **Copy The Contents Of The Specified Physical Disk** Enables you to select one of the physical hard disks in the computer and copy its contents to the new disk image
    - **Copy The Contents Of The Specified Virtual Hard Disk** Enables you to select an existing virtual disk file and copy its contents to the new disk image
11. Click Next. The Completing The New Virtual Hard Disk Wizard page opens.
12. Click Finish.

The wizard creates the new image disk and saves it to the specified location.

NOTE **USING WINDOWS POWERSHELL**

You can create new VHD files by using Windows PowerShell, which gives you more control than is available through the graphical interface. To create a new disk image, use the New-VHD cmdlet with the following basic syntax:

```
New-VHD –Path c:\filename.vhd|c:\filename.vhdx
–Fixed|-Dynamic|-Differencing –SizeBytes <size>
[-BlockSizeBytes <block size>]
[-LogicalSectorSizeBytes 512|4096] [-ParentPath <pathname>]
```

When using the cmdlet to create a disk image, the extension you specify for the filename determines the format (VHD or VHDX); also, you can specify the block size and the logical sector size for the image, two things you cannot do in the GUI. For example, the following command creates a 400-GB fixed VHDX image file with a logical sector size of 4 KB:

```
New-VHD –Path c:\diskfile.vhdx –Fixed
–SizeBytes 400GB -LogicalSectorSizeBytes 4096
```

Adding virtual disks to virtual machines

Creating virtual disk image files as a separate process enables administrators to exercise more control over their capabilities, but after creating the VHD or VHDX files, you must add them to a VM for them to be useful.

To add a hard disk drive to a physical computer, you must connect it to a controller; the same is true with a VM in Hyper-V. When you open the Settings dialog box for a Generation 1 VM in its default configuration, you see three controllers labeled IDE Controller 0, IDE Con-

troller 1, and SCSI Controller. These correspond to the controllers you might find in a typical physical server computer.

Each IDE controller can support two devices and the default VM configuration uses one channel on IDE Controller 0 for the system hard disk and one channel on IDE controller 1 for the system's DVD drive. If you did not create a virtual disk as part of the new Virtual Machine Wizard—that is, if you chose the Attach A Virtual Hard Disk Later option—then you must add a hard disk image to IDE Controller 0 to use as a system drive. A Generation 1 VM cannot boot from the SCSI controller.

To add an existing virtual system drive to a VM, use the following procedure.

1. In Server Manager, on the Tools menu, select Hyper-V Manager to open the Hyper-V Manager console.
2. In the left pane, select a Hyper-V server.
3. Select a VM and, in the Actions pane, select Settings. The Settings dialog box for the VM appears.
4. Select IDE Controller 0, as shown in Figure 3-16.

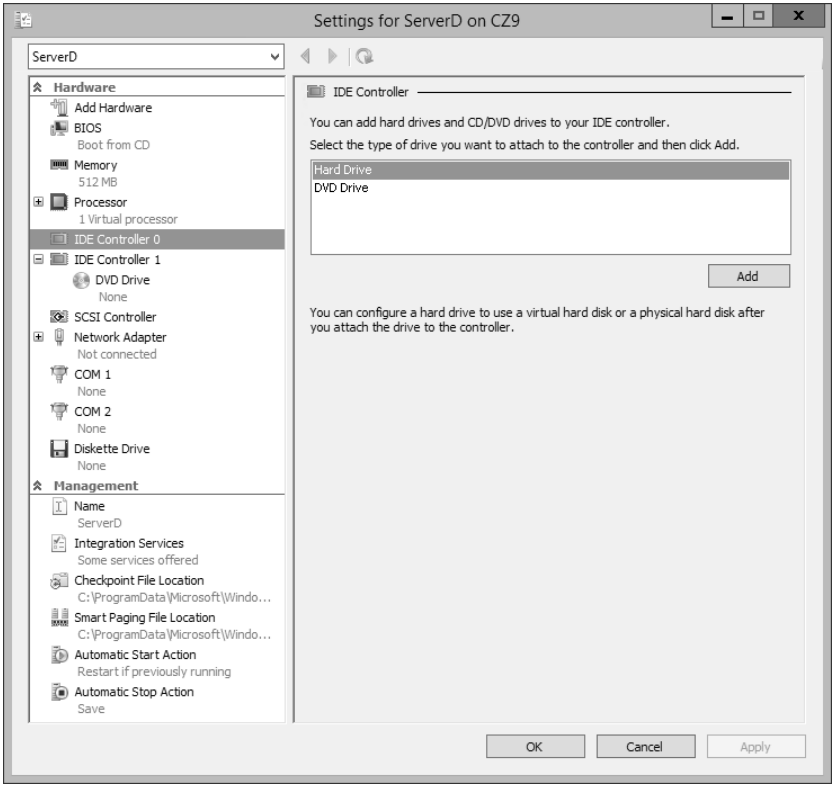

FIGURE 3-16 The IDE Controller interface in the Settings dialog box

5. In the IDE Controller box, select Hard Drive and click Add. The Hard Drive page opens, as shown in Figure 3-17.

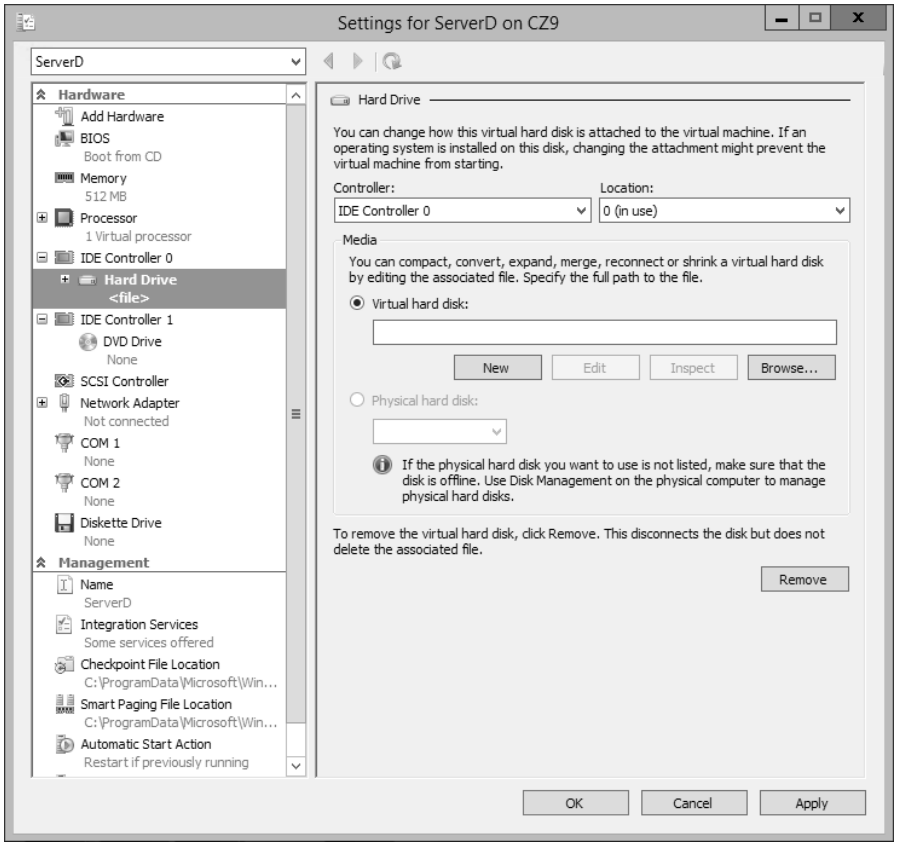

FIGURE 3-17 The Hard Drive interface in the Settings dialog box

6. In the Controller drop-down and the Location drop-down, select the IDE controller and the channel you want to use for the hard disk.
7. With the Virtual Hard Disk option selected, click Browse and select the disk image file you want to add.
8. Click OK to close the Settings dialog box.

Although you cannot use a SCSI drive as the system disk in a Generation 1 VM, you can add virtual data disks to the SCSI controller. In Generation 2 VMs, you must create a SCSI system disk to boot the machine. . Unlike the IDE connectors, which support only two devices each, a SCSI connector in Hyper-V can support up to 64 drives. You can also add multiple SCSI controllers to a VM, providing almost unlimited scalability for your virtual storage subsystem.

Creating differencing disks

A 1differencing disk enables you to preserve an existing virtual disk image file in its original state while mounting it in an operating system and even modifying its contents. For example, when building a laboratory setup, you can create a baseline system by installing a clean copy of an OS on a new virtual disk and configuring the environment to fit your needs. Then you can create a new child-differencing disk using your baseline image as the parent. All subsequent changes you make to the system will then be written to the differencing disk while the parent remains untouched. You can experiment on the test system as you wish, knowing that you can revert to your baseline configuration by just creating a new differencing disk.

You can create multiple differencing disks that point to the same parent image, enabling you to populate a lab network with as many VMs as you need, which saves disk space and eliminates the need to repeatedly install the OS.

To create a cloned version of a baseline installation with a differencing disk, use the following procedure.

1. **Install and configure the baseline VM** Create a new VM with a new disk image file and install a guest OS on it. Configure the OS as needed and install any roles, features, applications, or services you need.
2. **Generalize the parent image** Open an elevated command prompt on the baseline system and run the Sysprep.exe utility with the appropriate parameters for your requirements. Sysprep configures the system to assign itself a new, unique security ID (SID) the next time the computer starts. This enables you to create multiple cloned systems from a single disk image.
3. **Create a parent disk image** Once you have generalized the baseline installation, you no longer need the original VM. You can delete everything except the VHD or VHDX file containing the disk image. This will become your parent image. Open the Properties sheet for the image file and set the read-only flag to ensure that the baseline does not change.
4. **Create a differencing disk** By using the New Virtual Hard Disk Wizard or the New-VHD cmdlet for Windows PowerShell, create a new differencing disk pointing to the baseline image you created and prepared earlier as the parent image.
5. **Create a cloned VM** Create a new VM and, on the Connect Virtual Hard Disk page, attach the differencing disk you just created to it by using the Use An Existing Virtual Hard Disk option.

You can then proceed to create additional cloned VMs with differencing disks that all use the same parent. Each one can function independently and the parent disk will remain unchanged.

When you create a differencing drive by using the New Virtual Hard Disk Wizard, selecting the Differencing option on the Choose Disk Type page causes the Configure Disk page to

appear as shown in Figure 3-18. In the Location text box, specify the name of the file that you want to use as the parent image.

In the same way, if you create the differencing disk by using Windows PowerShell, you must run the New-VHD cmdlet with the –Differencing parameter and the –ParentPath parameter, specifying the location of the parent disk.

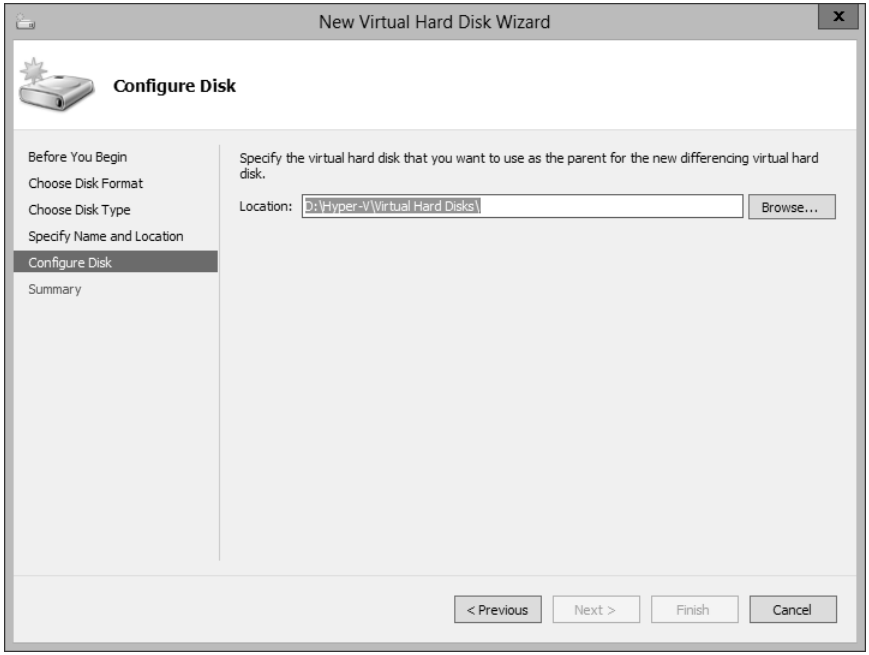

FIGURE 3-18 The Configure Disk page in the New Virtual Hard Disk Wizard

Configuring pass-through disks

This objective has thus far been concerned primarily with VHDs, areas of space on a physical disk drive allocated for use by VMs. However, it is also possible for VMs to access physical disks directly.

A pass-through disk is a type of virtual disk that points to a physical disk drive installed on the host computer. When you add a hard drive to any of the controllers in a VM, you have the option of selecting a physical hard disk as opposed to a virtual one.

To add a physical hard disk to a VM, the VM must have exclusive access to it. This means that you must first take the disk offline in the parent OS by using the Disk Management snap-in, as shown in Figure 3-19, or the Diskpart.exe utility. Once the disk is offline, it will be available for selection in the Physical Hard Disk drop-down list.

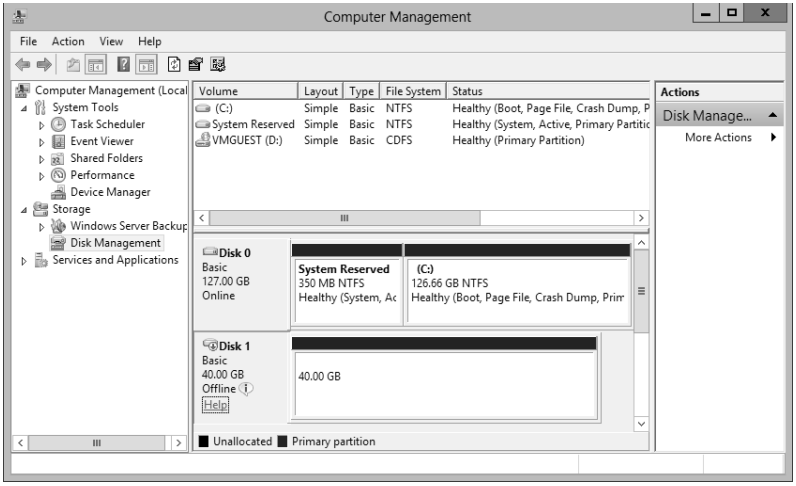

FIGURE 3-19 An offline disk in the Disk Management snap-in

Modifying virtual disks

Windows Server 2012 R2 and Hyper-V provide several ways for administrators to manage and manipulate VHD images without mounting them in a VM. Once you have created a VHD, whether you have attached it to a VM or not, you can manage it by using the Edit Virtual Hard Disk Wizard in Hyper-V Manager. To edit an existing VHD or VHDX file, use the following procedure.

1. In Server Manager, on the Tools menu, select Hyper-V Manager to open the Hyper-V Manager console.
2. In the left pane, select a Hyper-V server.
3. In the Actions pane, select Edit Disk. The Edit Virtual Hard Disk Wizard starts, displaying the Before You Begin page.
4. Click Next to open the Locate Disk page.
5. Type or browse to the name of the VHD or VHDX file you want to open and click Next. The Choose Action page appears.
6. Select one of the following functions:
   - **Compact** Reduces the size of a dynamically expanding or differencing disk by deleting empty space while leaving the disk's capacity unchanged
   - **Convert** Changes the type of format of a disk by copying the data to a new disk image file
   - **Expand** Increases the capacity of the disk by adding empty storage space to the image file

- **Shrink** Reduces the capacity of the disk by deleting empty storage space from the file
- **Merge** Combines the data on a differencing disk with that of the parent disk to form a single composite image file

7. Click Next to open the Completing The Edit Virtual Hard Disk Wizard page.
8. Complete any new pages presented by the wizard as a result of your selection and click Finish.

The options that appear on the wizard's Choose Action page depend on the current status of the image file you select. For example, the Merge option only appears if you choose a differencing disk, and the Shrink option does not appear unless there is free space in the file that the wizard can delete.

In addition to these disk-editing functions provided by Hyper-V Manager, it is possible to use the Disk Management snap-in on the Hyper-V host to mount a VHD or VHDX file as a drive and access its contents, just as if it were a physical disk.

To mount a VHD file, use the following procedure.

1. In Server Manager, on the Tools menu, select Computer Management to open the Computer Management console.
2. In the left pane, select Disk Management. The Disk Management snap-in opens.
3. From the Action menu, select Attach VHD. The Attach Virtual Hard Disk dialog box appears.
4. In the Location text box, type or browse to the image disk file you want to attach and click OK. The disk appears in the Disk Management interface.
5. Close the Computer Management console.

At this point, you can work with the virtual disk and its contents using any standard tools, just as you would a physical hard disk drive. To detach the VHD, you use the same procedure and select Detach VHD from the Action menu.

Creating checkpoints

In Hyper-V, a *checkpoint* is a captured image of the state, data, and hardware configuration of a VM at a particular moment in time. Creating checkpoints is a convenient way for administrators to revert a VM to a previous state at will. For example, if you create a checkpoint just before applying a system update, and the update is somehow problematic, you can apply the checkpoint and return the VM to the state in which it was before you applied the update.

EXAM TIP

Prior to Windows Server 2012 R2, the checkpoints in Hyper-V were known as snapshots. Checkpoints function in exactly the same way as snapshots; only the name is changed. You can expect to see either term on the 70-410 exam.

Creating a checkpoint is as simple as selecting a running VM in Hyper-V Manager and selecting Checkpoint from the Actions pane. The system creates a checkpoint file with an AVHD or AVHDX extension, in the same folder as the VHD file, and adds the checkpoint to the Hyper-V Manager display, as shown in Figure 3-20.

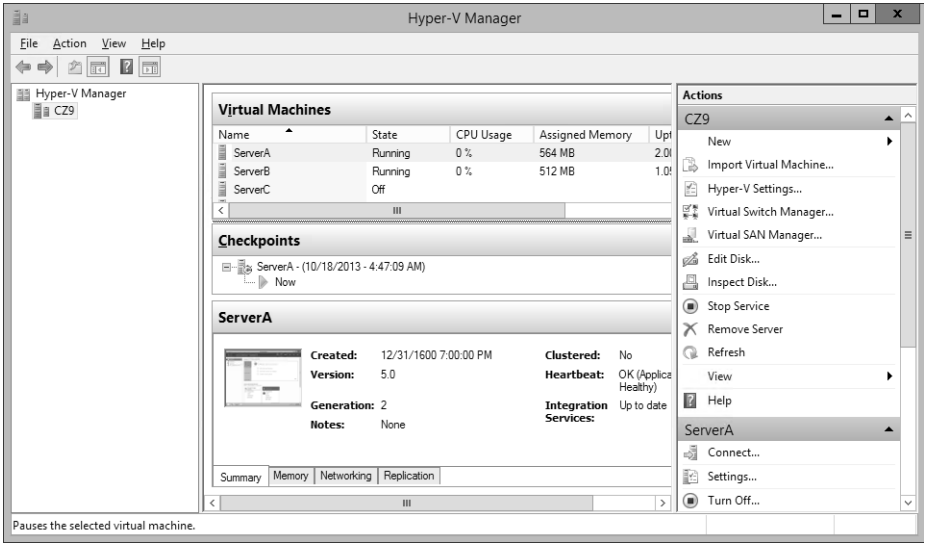

FIGURE 3-20 A checkpoint in Hyper-V Manager

Checkpoints are a useful tool for administrators implementing a test environment in Hyper-V, but they are not recommended for heavy use in production environments. In addition to consuming disk space, the presence of checkpoints can reduce the overall performance of a VM's disk subsystem. Administrators also should not use checkpoints on VMs containing databases—such as those created by SQL Server, Exchange, or Windows domain controllers—because the checkpointing process does not account for the current state of the database, and corruption might occur.

Configuring Storage Quality of Service (QoS)

Because it is common for there to be more than one virtual hard disk hosted by a single physical hard disk, it is possible for one virtual disk to monopolize the input/output capacity of a physical disk, causing the other virtual disks to slow down. To help prevent this, Windows Server 2012 R2 enables you to control the *Quality of Service (QoS)* for a given virtual hard disk.

QoS management in Hyper-V takes the form of controls that enables you to specify the minimum and maximum input/output operations per second (IOPS) for a disk. To configure

storage QoS, open the Settings dialog box for a VM, expand a hard drive component, and select Advanced Features to display the Advanced Features page shown in Figure 3-21.

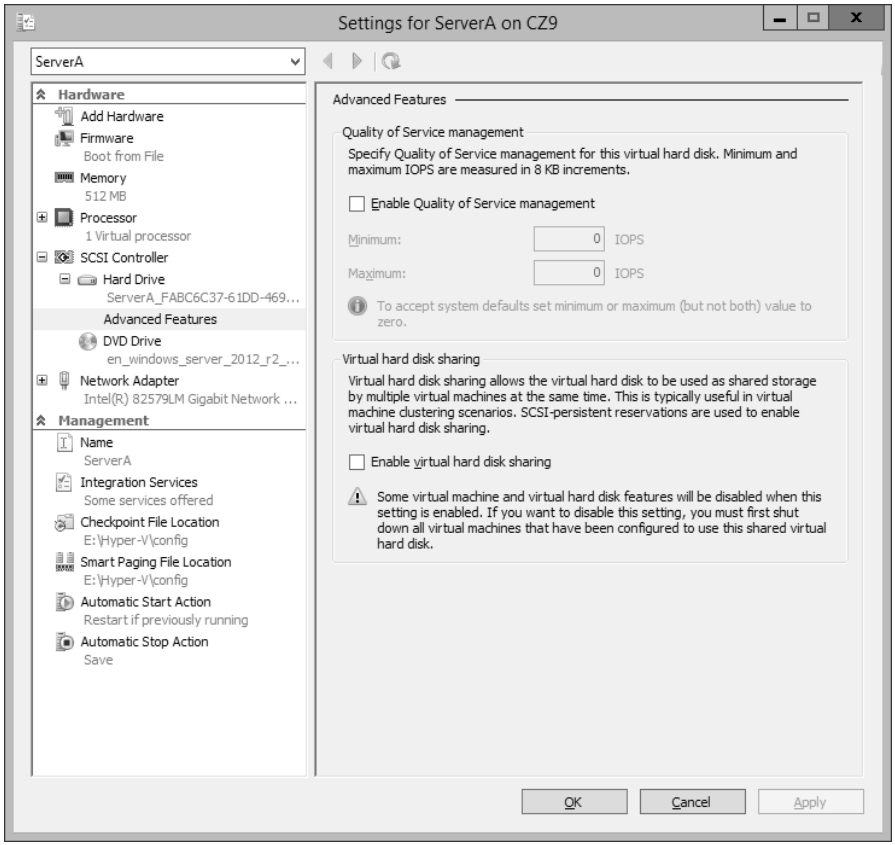

FIGURE 3-21 Storage Quality of Service controls in Hyper-V Manager

After selecting the Enable Quality of Service Management check box, you can specify Minimum IOPS values and Maximum IOPS values for the disk in 8 KB increments.

Connecting to a storage area network (SAN)

At its most basic level, a *storage area network (SAN)* is simply a network dedicated to high-speed connections between servers and storage devices. Instead of installing disk drives into servers or connecting them by using an external SCSI bus, a SAN consists of one or more drive arrays equipped with network interface adapters, which you connect to your servers by using standard twisted pair or fiber optic network cables. A SAN-connected server, therefore, typically has at least two network adapters, one for the standard local area network (LAN) connection and one for the SAN, as shown in Figure 3-22.

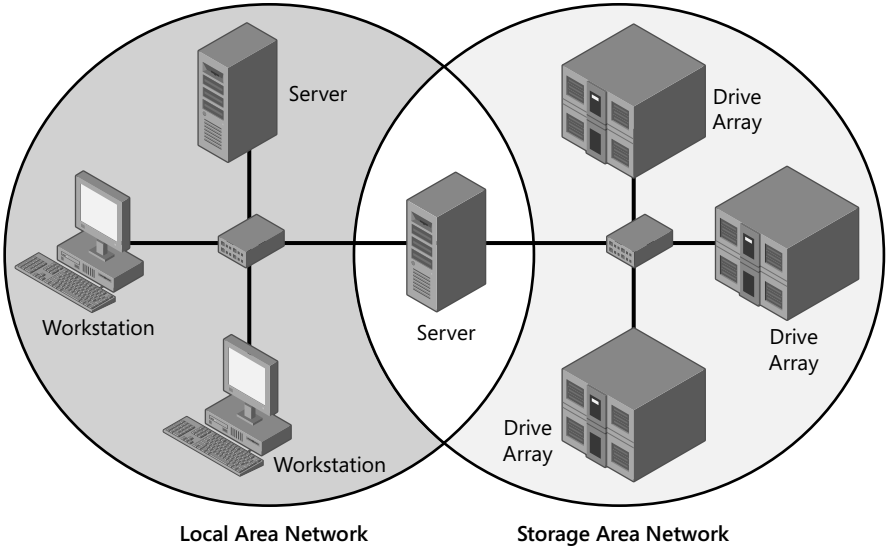

FIGURE 3-22 A server connected to a SAN

The advantages of SANs are many. By connecting the storage devices to a network instead of to the servers themselves, you avoid the limitations imposed by the maximum number of devices you can connect directly to a computer. SANs also provide added flexibility in their communications capabilities. Because any device on a SAN can conceivably communicate with any other device on the same SAN, high-speed data transfers can occur in any of the following ways:

- **Server to storage** Servers can access storage devices over the SAN just as if they were connected directly to the computer.
- **Server to server** Servers can use the SAN to communicate directly with one another at high speeds to avoid flooding the LAN with traffic.
- **Storage to storage** Storage devices can communicate among themselves without server intervention, for example, to perform backups from one medium to another or to mirror drives on different arrays.

Although a SAN is not in itself a high-availability technology, you can make it one by connecting redundant servers to the same network, as shown in Figure 3-23, enabling them to access the same data storage devices. If one server should fail, another can assume its roles by accessing the same data. This is called *server clustering*.

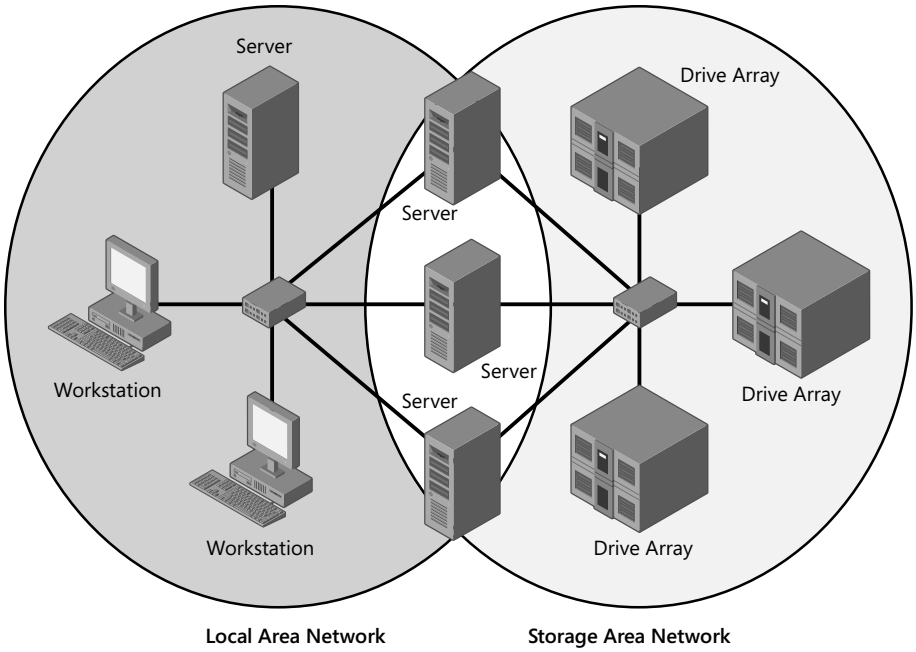

FIGURE 3-23 Multiple servers connected to a SAN

Because they use standard networking technologies, SANs can also greatly extend the distances between servers and storage devices. You can design a SAN that spans different rooms, different floors, or even different buildings, just as you would a standard computer network.

Servers and storage devices cannot exchange SCSI commands over a SAN connection the way they do when the devices are directly connected using a SCSI cable. To communicate over a SAN, servers and storage devices map their SCSI communications onto another protocol, such as Fibre Channel.

Using Fibre Channel

Fibre Channel is a versatile SAN communications technology supporting various network media, transmission speeds, topologies, and upper-level protocols. Its primary disadvantage is that it requires specialized hardware that can be extremely expensive.

MORE INFORMATION **FIBRE CHANNEL**

The nonstandard spelling of the word *fibre* in Fibre Channel is deliberate, to distinguish the term from fiber optic. Fibre Channel can run on either twisted-pair copper cables or it can run on optical cables, whereas the spelling *fiber* always refers to an optical medium.

Installing a traditional Fibre Channel SAN entails building an entirely new network with its own special medium, switches, and network interface adapters. In addition to the hardware costs, which can easily be 10 times those of a traditional Ethernet network, there are also installation and maintenance expenses to consider. Fibre Channel is a rather esoteric technology, with relatively few experts in the field. To install and maintain a Fibre Channel SAN, an organization must either hire experienced staff or train existing personnel on the new technology. However, there is also a variant called Fibre Channel over Ethernet (FCoE) that uses standard Ethernet hardware and is therefore much less expensive.

Connecting virtual machines to a SAN

The specialized networking technologies used to build Fibre Channel SANs have, in the past, made it difficult to use them with virtualized servers. However, since the Windows Server 2012 implementation, Hyper-V has supported the creation of virtual Fibre Channel adapters.

A Hyper-V Fibre Channel adapter is essentially a pass-through device that enables a VM to access a physical Fibre Channel adapter installed in the computer, and through that, to access the external resources connected to the SAN. With this capability, applications running on VMs can access data files stored on SAN devices and administrators can use VMs to create server clusters with shared storage subsystems.

To support virtual Fibre Channel connectivity, the physical Fibre Channel host bus adapter(s) in the host computer must have drivers that explicitly support virtual Fibre Channel. This support is relatively rare, but more manufacturers are expected to update their drivers to provide the necessary support. Your SAN must also be able to address its connected resources by using logical unit numbers (LUNs).

Assuming you have the appropriate hardware and software installed on the host computer, you implement the Fibre Channel capabilities in Hyper-V by first creating a virtual SAN by using the Virtual SAN Manager, accessible from Hyper-V Manager. When you create the virtual SAN, the World Wide Node Names (WWNNs) and World Wide Port Names (WWPNs) of your host bus adapter appear, as shown in Figure 3-24.

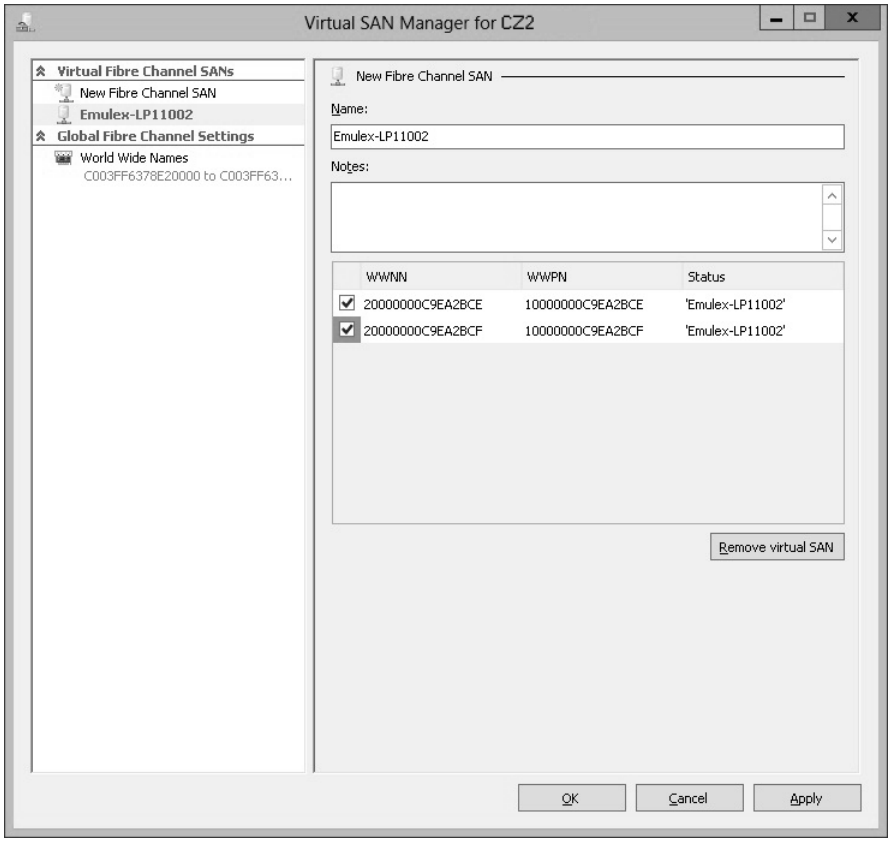

FIGURE 3-24 WWNNs and WWPNs in a virtual SAN

The next step is to add a Fibre Channel adapter to a VM from the Add Hardware page in the Settings dialog box. When you do this, the virtual SAN you created earlier is available on the Fibre Channel Adapter page, shown in Figure 3-25. Hyper-V virtualizes the SAN and makes the WWNNs and WWPNs available to the VM.

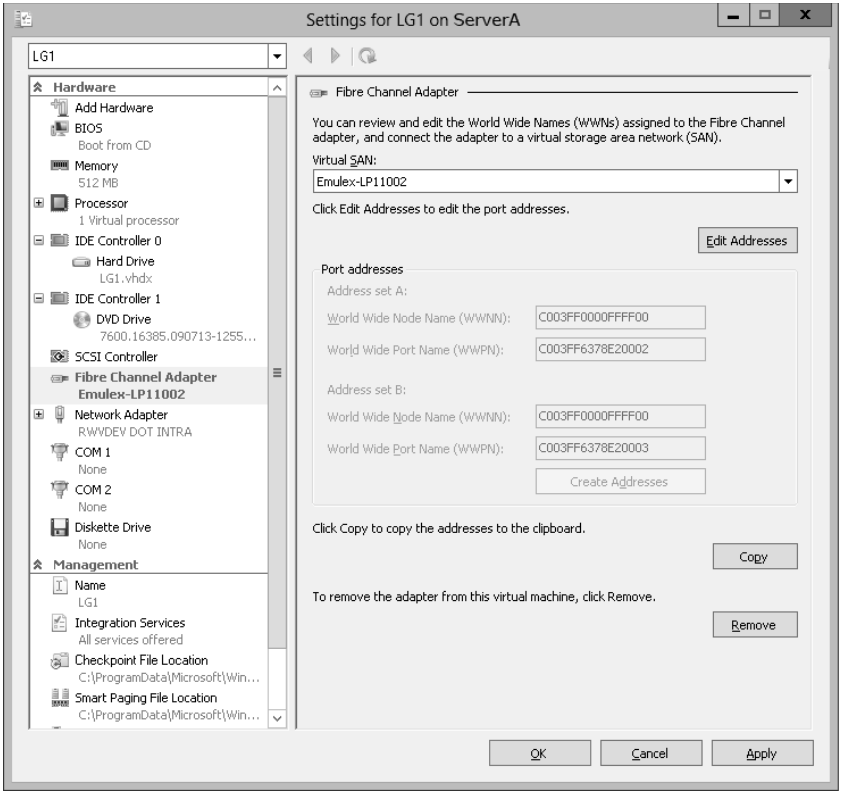

FIGURE 3-25 A Fibre Channel adapter in a VM

Thought experiment

Creating a VHD

In the following thought experiment, apply what you've learned about this objective to predict what steps you need to take. You can find answers to these questions in the "Answers" section at the end of this chapter.

Ed wants to create a new VHD file on his Hyper-V server by using Windows PowerShell. He runs the Get-Disk cmdlet and receives the following results:

Number	Friendly	Name	Operational Status	Total Size	Partition Style
0	WDC	WD5003ABYX-18WERA0	Online	465.76 GB	MBR
1	WDC	WD1002FAEX-00Z3A0	Online	931.51 GB	GPT

What command should Ed use to create a new 500-GB fixed VHD for his Server A VM, in the Windows Server 2012 R2 format, using data from the 465-GB drive on his computer, and a 4,096-byte sector size?

Objective summary

- Hyper-V uses a specialized VHD format to package part of the space on a physical disk and make it appear to the VM as though it is a physical hard disk drive.
- A dynamic hard disk image is an image file with a specified maximum size, which starts small and expands as needed to accommodate the data the system writes to it.
- A differencing hard disk image is a child image file associated with a specific parent image. The system writes all changes made to the operating system to the child image, to facilitate a rollback at a later time.
- VHDX image files in Windows Server 2012 R2 can be as large as 64 TB, and they also support 4-KB logical sector sizes to provide compatibility with new 4-KB native drives.
- A pass-through disk is a type of virtual disk that points to a physical disk drive installed on the host computer.
- In Hyper-V, a checkpoint is a captured image of the state, data, and hardware configuration of a VM at a particular moment in time.
- QoS management in Hyper-V takes the form of controls that enable you to specify the minimum and maximum input/output operations per second (IOPS) for a disk.
- The specialized networking technologies used to build Fibre Channel SANs have, in the past, made it difficult to use them with virtualized servers. However, Windows Server 2012 R2 Hyper-V supports the creation of virtual Fibre Channel adapters.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which of the following statements about VHDX files is *not* true?
   - **A.** VHDX files can be as large as 64 TB.
   - **B.** VHDX files can only be opened by computers running Windows Server 2012 and Windows Server 2012 R2.
   - **C.** VHDX files support larger block sizes than VHD files.
   - **D.** VHDX files support 4-KB logical sectors.
2. Which of the following must be true about a pass-through disk?
   - **A.** A pass-through disk must be offline in the guest OS that will access it.
   - **B.** A pass-through disk must be offline in the parent partition of the Hyper-V server.
   - **C.** A pass-through disk can only be connected to a SCSI controller.
   - **D.** A pass-through disk must be added to a VM with the Disk Management snap-in.

3. The Merge function only appears in the Edit Virtual Hard Disk Wizard under which of the following conditions?
   - **A.** When you select a VHDX file for editing
   - **B.** When you select two or more disks for editing
   - **C.** When you select a disk with free space available in it
   - **D.** When you select a differencing disk for editing
4. Which of the following are valid reasons *not* to take checkpoints of VMs? (Choose all that apply.)
   - **A.** Checkpoints can consume a large amount of disk space.
   - **B.** Each checkpoint requires a separate copy of the VM's memory allocation.
   - **C.** Each checkpoint can take several hours to create.
   - **D.** The existence of checkpoints slows down VM performance.
5. Which of the following is *not* required to add a Fibre Channel adapter to a Hyper-V VM?
   - **A.** You must create a Fibre Channel virtual SAN.
   - **B.** You must have a physical Fibre Channel adapter installed in the host computer.
   - **C.** You must have a Fibre Channel adapter driver that supports virtual networking.
   - **D.** You must have a SCSI cable connecting the Fibre Channel adapter to the storage devices.

Objective 3.3: Create and configure virtual networks

Networking is a critical part of creating a VM infrastructure. Depending on your network plan, the VMs you create on a Windows Server 2012 R2 Hyper-V server can require communication with other VMs, with the computers on your physical network, and with the Internet.

When you build a network out of physical computers, you install a network interface adapter in each one and connect it to a hardware switch. The same principle is true in a Hyper-V environment, except that you use virtual components instead of physical ones. Each VM you create has at least one virtual network adapter and you can connect that adapter to a virtual switch. This enables you to connect the VMs on your Hyper-V server in various network configurations that either include or exclude the systems on your physical network.

You can create multiple virtual switches on a Hyper-V server and multiple network adapters in each VM. This enables you to create a flexible networking environment that is suitable for anything from a laboratory or classroom network to a production environment. In addition, Windows Server 2012 R2 has added the ability to create extensions for virtual switches so that software developers can enhance their capabilities.

This objective covers how to:

- Implement Hyper-V Network Virtualization
- Configure Hyper-V virtual switches
- Optimize network performance
- Configure MAC addresses
- Configure network isolation
- Configure synthetic and legacy virtual network adapters
- Configure network interface card (NIC) teaming in VMs

Creating virtual switches

A *virtual switch*, like its physical counterpart, is a device that functions at Layer 2 of the Open Systems Interconnect (OSI) reference model. A switch has a series of ports, each of which is connected to a computer's network interface adapter. Any computer connected to the switch can transmit data to any other computer connected to the same switch.

Unlike physical switches, the virtual switches created by Hyper-V can have an unlimited number of ports, so administrators don't have to be concerned about connecting switches together or about uplinks and crossover circuits.

Creating the default virtual switch

The Windows Server 2012 R2 Add Roles and Features Wizard provides the opportunity to create virtual switches when you install the Hyper-V role. When you install Hyper-V on a server running Windows Server 2012 R2, the Create Virtual Switches page provides you with the opportunity to create a virtual switch for each of the physical network adapters installed in the host computer. These switches enable VMs to participate on the networks to which the physical adapters are connected.

When you create a virtual switch, the networking configuration in the host OS on the parent partition changes. The new virtual switch appears in the Network Connections window, and if you examine its properties, you can see that the switch is bound to the operating system's TCP/IP client, as shown in Figure 3-26.

Meanwhile, Hyper-V also changes the properties of original network connection representing the physical network interface adapter in the computer. The physical network adapter is now bound only to the virtual switch, as shown in Figure 3-27.

As a result, the computer's physical network configuration, in which its network adapter is connected to an external physical switch, is overlaid by the virtual network configuration created by Hyper-V. In this virtual configuration, the virtual switch is connected to the physical switch and the network adapter in the host OS is connected to the virtual switch. The

internal virtual network and the external physical network are joined into a single LAN, just as if you connected two physical switches.

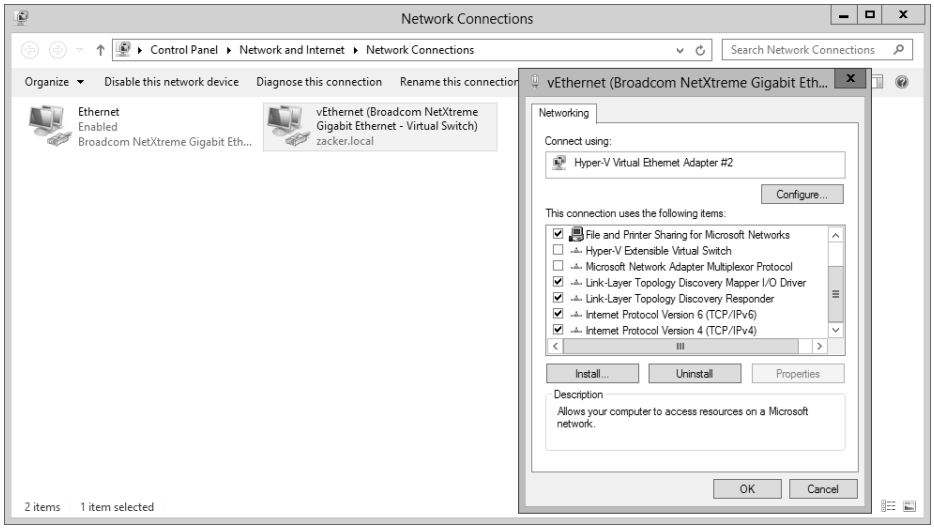

FIGURE 3-26 A virtual switch and its properties, displayed in the host OS

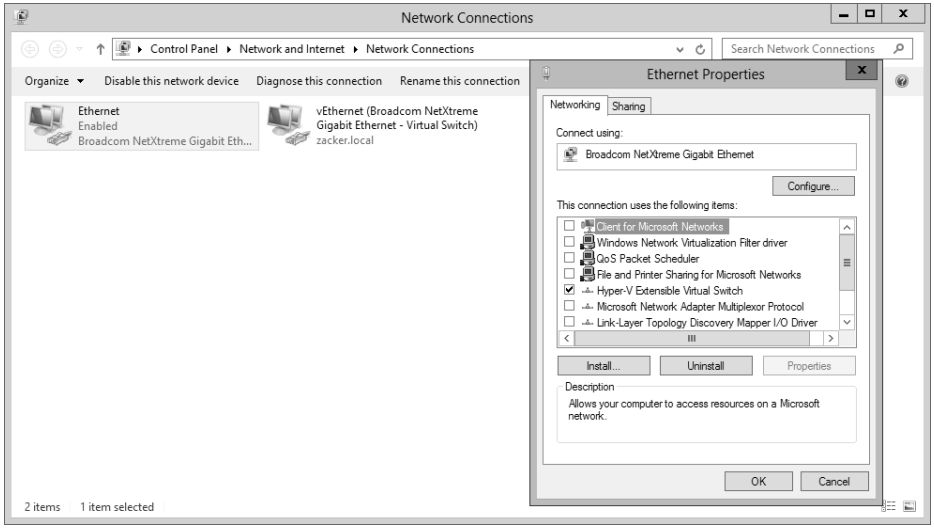

FIGURE 3-27 A network interface adapter in the host OS, bound to a virtual switch

Once Hyper-V has created the virtual switch and made these configuration changes, any new VMs that administrators choose to connect to the virtual switch become part of this conjoined network, as do any physical computers connected to the physical network through an external switch.

This type of virtual switch is, in Hyper-V terminology, an external network switch because it provides connections external to the Hyper-V environment. This is typically the preferred arrangement for a production network in which Hyper-V VMs provide and consume services for the entire network.

For example, a VM connected to this switch will automatically obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server on the physical network, if there is one. As an alternative, you could configure a VM as a DHCP server and let it provide addresses to all of the systems on the network, virtual or physical.

Perhaps more important, this arrangement can also enable your VMs to access the Internet by using the router and DNS servers on the external network. The VMs can then download OS updates from servers on the Internet, just as external machines often do.

There are situations in which this type of virtual switch is inappropriate. If you are creating a laboratory network for product testing or a classroom network, you might not want it to be accessible to or from the external network. In these cases, you must create a different type of virtual switch by using the Virtual Switch Manager in Hyper-V Manager.

Creating a new virtual switch

Hyper-V in Windows Server 2012 R2 supports three types of switches, which you must create in the Virtual Switch Manager before you can connect VMs to them.

To create a new virtual switch, use the following procedure.

1. In Server Manager, on the Tools menu, select Hyper-V Manager to open the Hyper-V Manager console.
2. In the left pane, select a Hyper-V server.
3. From the Actions pane, select Virtual Switch Manager. The Virtual Switch Manager dialog box for the Hyper-V server opens, as shown in Figure 3-28.

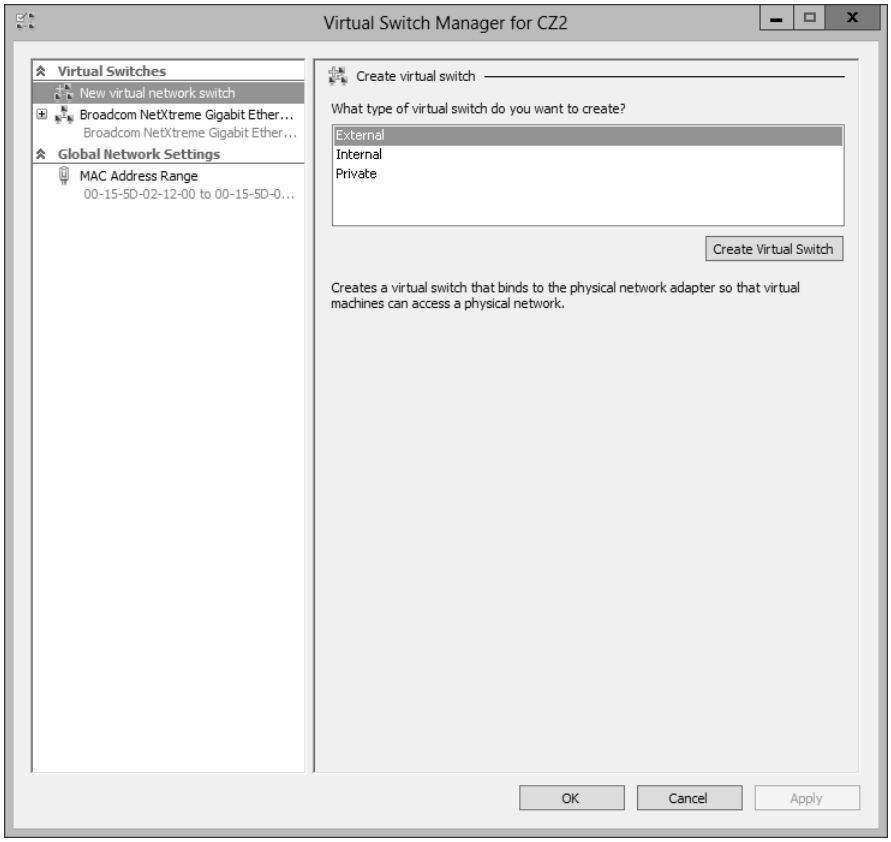

FIGURE 3-28 The Virtual Switch Manager dialog box

4. In the Create Virtual Switch section, select one of the following switch types:
   - **External** The virtual switch is bound to the networking protocol stack in the host OS and connected to a physical network interface adapter in the Hyper-V server. VMs running on the server's parent and child partitions can all access the physical network to which the physical adapter is connected.
   - **Internal** An internal network switch is bound to a separate instance of the networking protocol stack in the host OS, independent from the physical network interface adapter and its connected network. VMs running on the server's parent and child partitions can all access the virtual network implemented by the virtual switch; the host OS on the parent partition can access the physical network through the physical network interface adapter, but the VMs on the child partitions cannot access the physical network through the physical adapter.
   - **Private** A private network switch exists only in the Hyper-V server and is accessible only to the VMs running on the child partitions. The host OS on the parent

partition can access the physical network through the physical network interface adapter, but it cannot access the virtual network created by the virtual switch.

5. Click Create Virtual Switch to open the Virtual Switch Properties page.
6. Configure the following options, if desired:
   - **Allow Management Operating System To Share This Network Adapter** Selected by default when you create an external virtual switch, clearing this check box excludes the host OS from the physical network while allowing access to the child VMs.
   - **Enable Single Root I/O Virtualization (SR-IOV)** Enables you to create an external virtual switch that is associated with a physical network adapter capable of supporting SR-IOV. This option is only available when creating a new virtual switch; you cannot modify an existing virtual switch to use this option.
   - **Enable Virtual LAN Identification For Management Operating System** If your host computer is connected to a physical switching infrastructure that uses virtual LANs (VLANs) to create separate subnets, you can select this check box and enter a VLAN identifier to associate the virtual switch with a particular VLAN on your physical network.
7. Click OK. The new virtual switch appears in the left pane, in the list of virtual switches.

You can create additional virtual switches as needed. You can create only one external switch for each physical network adapter in the computer, but you can create multiple internal or private switches to create as many virtual networks as you need.

NOTE **USING WINDOWS POWERSHELL**

To create a new virtual switch by using Windows PowerShell, use the New-VMSwitch cmdlet with the following basic syntax:

```
New-VMSwitch <switch name> -NetAdapterName <adapter name>
[-SwitchType Internal|Private]
```

For example, to create an external switch called LAN Switch, you would use the following command:

```
New-VMSwitch "LAN Switch" -NetAdapterName "Ethernet"
```

Configuring MAC addresses

Every network interface adapter has a *Media Access Control (MAC) address*—sometimes called a hardware address—that uniquely identifies the device on the network. On physical network adapters, the MAC is assigned by the manufacturer and permanently entered in the adapter's firmware. The MAC address is a 6-byte hexadecimal value, the first three bytes of which are an organizationally unique identifier (OUI) that specifies the manufacturer, and the last three bytes of which identify the adapter itself.

The MAC address is essential to the operation of a LAN, so the virtual network adapters on a Hyper-V server need to have them. The server has at least one real MAC address, provided in its physical network adapter, but Hyper-V cannot use that one address for all the virtual adapters connecting VMs to the network.

Instead, Hyper-V creates a pool of MAC addresses during the installation of the role and it assigns addresses from this pool to VMs as you create them. To view or modify the MAC address pool for the Hyper-V server, you open the Virtual Switch Manager and, under Global Network Settings, select MAC Address Range, as shown in Figure 3-29.

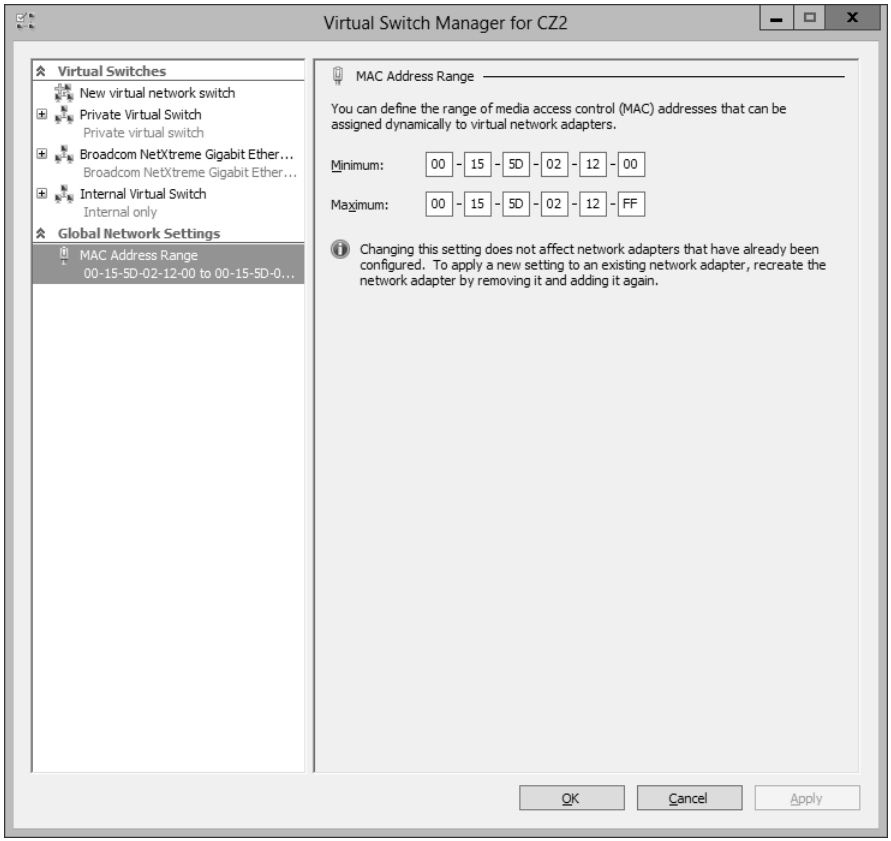

FIGURE 3-29 The MAC Address Range in the Virtual Switch Manager

The first three bytes of the MAC address range are always 00-15-5D, which is an OUI registered by Microsoft. The fourth and fifth bytes of the MAC address are the last two bytes of the IP address assigned to the server's physical network adapter, converted to hexadecimal notation. The sixth and last byte of the MAC address contains the range of values from 00 to FF, which provides 256 possible addresses.

The Hyper-V server assigns the MAC addresses to the network adapters in VMs as administrators create the adapters. The adapters retain their MAC addresses permanently or until the adapter is removed from the VM. The server reclaims any unused addresses and reuses them.

The default pool of 256 addresses is expected to be sufficient for most Hyper-V VM configurations, but if it is not, you can modify the Minimum and Maximum values to enlarge the pool. To prevent address duplication, you should change the second-to-last byte only, making it into a range of addresses like the last byte.

For example, the range illustrated in the figure provides 256 addresses with the following values:

```
00-15-1D-02-12-00 to 00-15-1D-02-12-FF
```

Modifying only the least significant digit, as in the following values, increases the pool from 256 to 4,096:

```
00-15-1D-02-10-00 to 00-15-1D-02-1F-FF
```

WARNING **MAC ADDRESSES**

When you modify the MAC address pool and you have other Hyper-V servers on your network, you must be careful not to create an overlap situation in which duplicate MAC addresses can occur or networking problems can result.

Creating virtual network adapters

Once you have created virtual switches in Hyper-V Manager, you can connect VMs to them by creating and configuring virtual network adapters. When you create a new VM, the default configuration includes one virtual network adapter. The New Virtual Machine Wizard includes a Configure Networking page, on which you can select one of the virtual switches you have created.

If you have created only the default external virtual switch when installing Hyper-V, then connecting a VM to that switch joins the system to the physical network. If you want to create additional network adapters in your VMs, you must use the following procedure.

1. In Server Manager, on the Tools menu, select Hyper-V Manager to open the Hyper-V Manager console.
2. In the left pane, select a Hyper-V server.
3. In the Virtual Machines list, select a VM and, in the Actions pane, click Settings. The Settings dialog box for the VM appears.
4. In the Add Hardware list, select Network Adapter and click Add. A new adapter appears in the Hardware list, as shown in Figure 3-307.

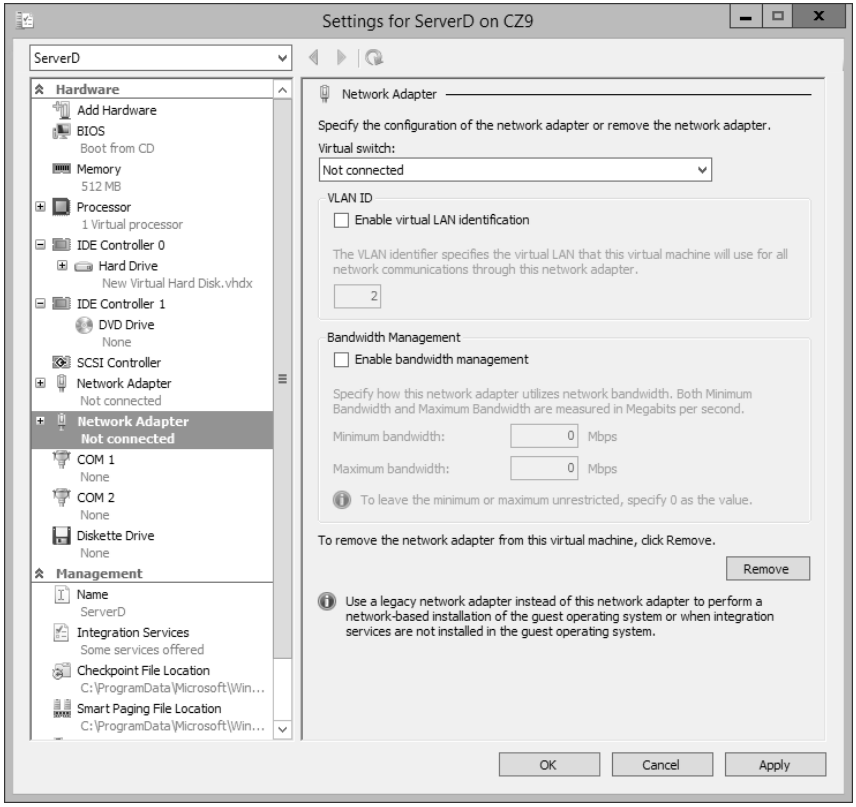

FIGURE 3-30 A new network adapter in the Settings dialog box

5. In the Virtual Switch drop-down list, select the switch to which you want to connect the network adapter.

6. If your host computer is connected to a physical switching infrastructure that uses VLANs to create separate subnets, you can select the Enable Virtual LAN Identification check box and enter a VLAN identifier to associate the network adapter with a particular VLAN on your physical network.

7. To control the amount of network bandwidth allocated to the network adapter, select the Enable Bandwidth Management check box and supply values for the Minimum Bandwidth and Maximum Bandwidth settings.

8. Click OK. The settings are saved to the VM configuration.

You can create up to 12 network adapters on a Windows Server 2012 R2 Hyper-V server: eight synthetic and four emulated.

Synthetic adapters and emulated adapters

Selecting the Network Adapter option on the Add Hardware page creates what is known in Hyper-V terminology as a synthetic network adapter. Hyper-V supports two types of network and storage adapters: synthetic and emulated (sometimes called legacy).

A *synthetic adapter* is a purely virtual device that does not correspond to a real-world product. Synthetic devices in a VM running on a child partition communicate with the parent partition by using a high-speed conduit called the VMBus.

The virtual switches you create in Hyper-V reside in the parent partition and are part of a component called the network Virtualization Service Provider (VSP). The synthetic network adapter in the child partition is a Virtualization Service Client (VSC). The VSP and the VSC are both connected to the VMBus, which provides interpartition communications, as shown in Figure 3-31. The VSP, in the parent partition, provides the VSC, in the child partition, with access to the physical hardware in the host computer; that is, the physical network interface adapter.

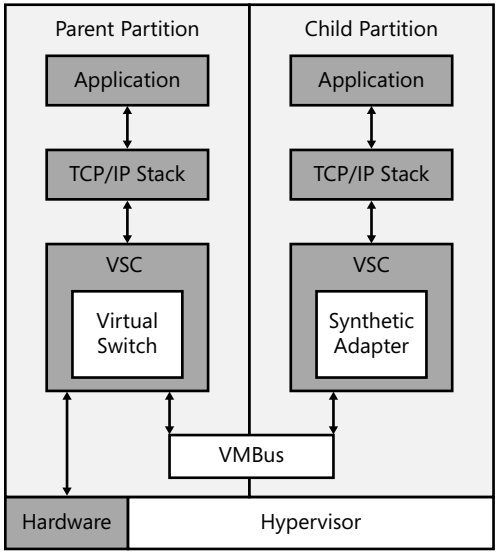

FIGURE 3-31 Synthetic network adapters communicate by using the VMBus

Because they have access to the hardware through the VMBus, synthetic adapters provide a much higher level of performance than the alternative, emulated adapters. Synthetic adapters are implemented as part of the Guest Integration Services package that runs on supported guest OSs. The main drawback of synthetic network adapters is that they are not operational until the OS is loaded on the VM.

An *emulated adapter*—sometimes called a *legacy adapter*—is a standard network adapter driver that communicates with the parent partition by making calls directly to the hypervisor, which is external to the partitions, as shown in Figure 3-32. This communication method is

substantially slower than the VMBus used by the synthetic network adapters and is therefore less desirable.

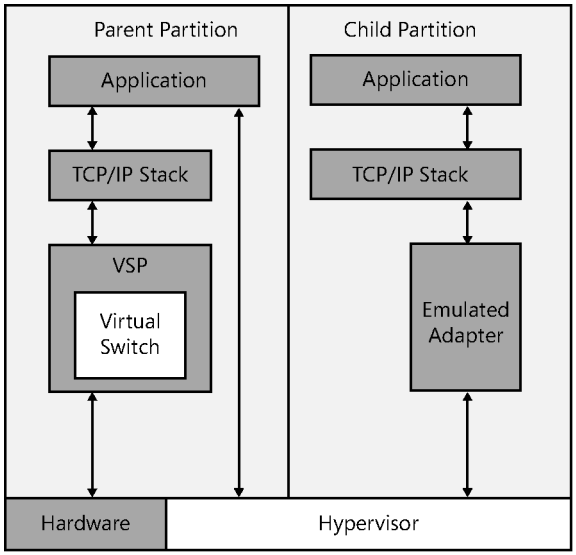

FIGURE 3-32 Emulated network adapters communicate by using the hypervisor

To install an emulated adapter, you use the same procedure described earlier, except that you select Legacy Network Adapter from the Add Hardware list. Unlike synthetic adapters, emulated adapters load their drivers before the OS, so it is possible to boot the VM by using the Preboot eXecution Environment (PXE) and then deploy an OS over the network.

This is one of two scenarios in which using an emulated adapter is preferable to using a synthetic adapter. The other is when you are installing an OS on your VMs that does not have a Guest Integration Services package available for it.

Configuring hardware acceleration settings

Some physical network interface adapters have features that are designed to improve performance by offloading certain functions from the system processor to components built into the adapter itself. Hyper-V includes support for some of these features, as long as the hardware in the physical network adapter supports them properly.

When you expand a network adapter in the Settings dialog box of a VM, you gain access to the Hardware Acceleration page. On this page, you can configure the following hardware acceleration settings:

- **Enable Virtual Machine Queue** *Virtual machine queue (VMQ)* is a technique that stores incoming packets intended for VMs in separate queues on the physical network adapter and delivers them directly to the VMs, bypassing the processing normally performed by the virtual switch on the parent partition.

- **Enable IPsec Task Offloading** Uses the components on the network adapter to perform some of the cryptographic functions required by IPsec. You can also specify the maximum number of security associations you want the adapter to be able to calculate.
- **Single-Root I/O Virtualization** Enables the virtual adapter to take advantage of the SR-IOV capabilities of the physical adapter.

Configuring advanced network adapter features

The Advanced Features page provides additional options for supporting network adapter capabilities, as follows:

- **Static MAC Address** By default, virtual network adapters receive a dynamically assigned MAC address from the Hyper-V server. However, you can opt to create a static MAC address by using this option. The only requirement is that no other adapter, virtual or physical, on the same network uses the same address.
- **Enable MAC Address Spoofing** When enabled, the port in the virtual switch to which the virtual network adapter is connected can send and receive packets that contain any MAC address. The virtual switch port can also learn of new MAC addresses and add them to its forwarding table.
- **Enable DHCP Guard** Prevents the adapter from processing messages sent by rogue DHCP servers.
- **Port Mirroring Mode** Enables the adapter to forward all the packets it receives over the network to another virtual adapter for analysis by using an application such as Network Monitor.
- **NIC Teaming** Enables the adapter to add its bandwidth to that of other adapters in the same guest OS in a NIC teaming arrangement.

Configuring NIC teaming in a virtual network environment

As explained in objective 1.2, "Configuring Servers," *NIC teaming* is a Windows feature that enables administrators to join multiple network adapters into a single entity for performance enhancement or fault tolerance purposes. Hyper-V virtual machines can also take advantage of NIC teaming, but they are limited to teams of only two, as opposed to the host operating system, which can have teams of up to 64 NICs.

To use NIC teaming in Hyper-V, you must complete three basic tasks, as follows:

1. Create the NIC team in the Windows Server 2012 R2 host operating system.
2. In Hyper-V Manager, create an external virtual switch using the NIC team.
3. Configure the network adapter in a virtual machine to connect to the virtual switch representing the NIC team.

Creating the NIC team

NIC teams must consist of physical network interface adapters, so before you can use a NIC team in a virtual machine, you must create it in the host operating system. After installing two NICs in the computer, you can create a NIC team with Server Manager in the usual manner, using the settings shown in Figure 3-33. Creating the team installs the Microsoft Network Adapter Multiplexor Driver, which appears as one of the components of the network connection representing the team.

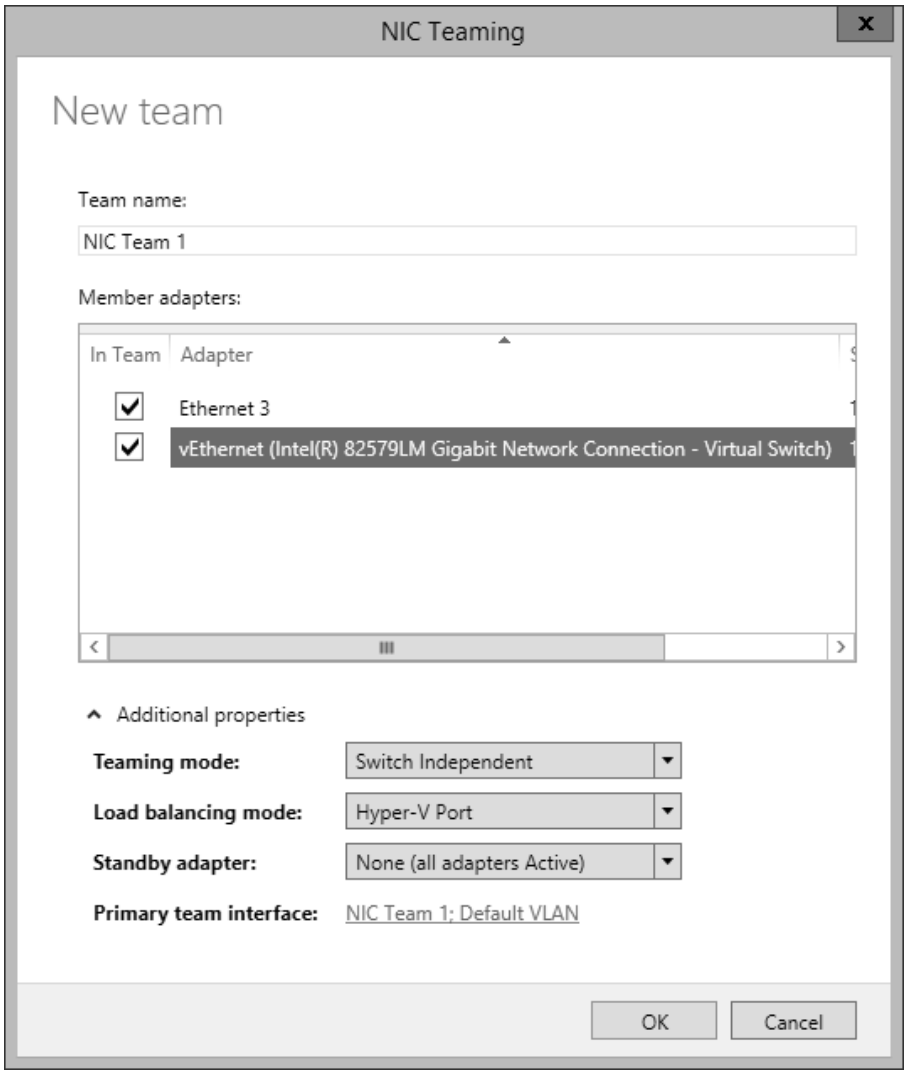

FIGURE 3-33 The NIC Teaming dialog box

Creating the team virtual switch

Once you have created the NIC team, you can open the Virtual Switch Manager and create a new virtual switch by selecting the External network option and choosing Microsoft Network Adapter Multiplexor Driver from the drop-down list, as shown in Figure 3-34.

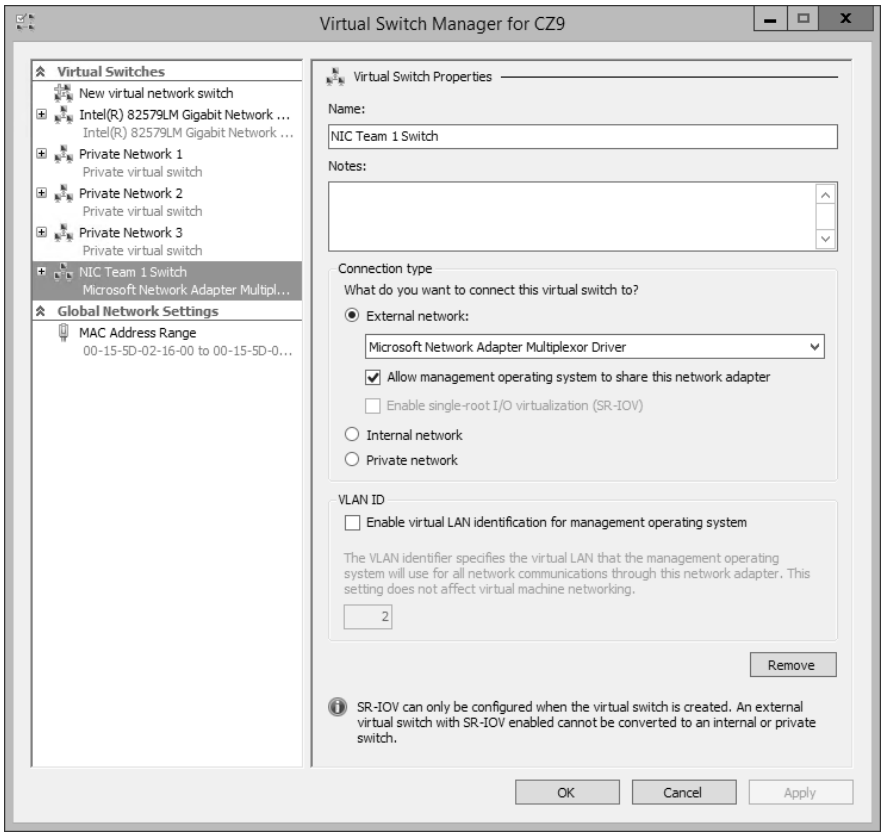

FIGURE 3-34 The Virtual Switch Properties settings for a NIC team switch

Configuring a NIC team virtual network adapter

To configure a virtual machine to use a NIC team, you must use the Settings dialog box to modify the properties for a virtual network adapter, configuring it to use the team switch you created in the previous section, as shown in Figure 3-35.

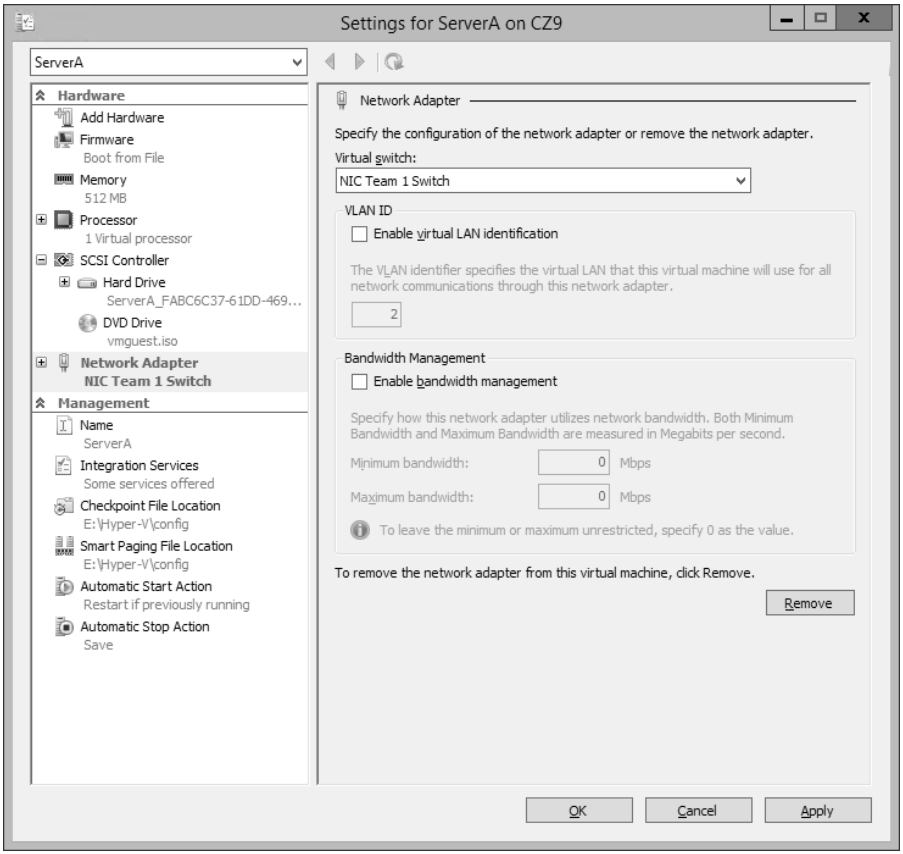

FIGURE 3-35 The Network Adapter settings for a NIC team adapter

Finally, you must open the Advanced Features page for the network adapter and select the Enable The Network Adapter To Be Part Of A Team In The Guest Operating System check box. At this point, the NIC team is operational for the virtual machine. You can unplug one of the network cables and the system will maintain its connection to the network.

Creating virtual network configurations

Hyper-V makes it possible to extend nearly any existing physical network configuration into its virtual space or create a completely separated and isolated network within the Hyper-V environment.

The basic default configuration of a Hyper-V VM connects its network adapter to an external virtual switch, thus attaching the guest OS on the VM to the outside network. The VM can then take advantage of services running on the outside network and send traffic through routers to other networks, including the Internet.

This type of arrangement can enable administrators to consolidate many physical servers into VMs on a single Hyper-V server, providing them all with access to the entire network.

There is no distinction here between the physical network and the virtual one in the Hyper-V space.

Extending a production network into virtual space

Keep in mind that a Hyper-V server can have multiple physical network adapters installed in it, which might be connected to different networks to separate traffic or they might be connected to the same network to increase available bandwidth. You might also have adapters dedicated to SAN connections for shared storage and server clustering.

Microsoft recommends the use of at least two physical network adapters in a Hyper-V server, with one adapter servicing the parent partition and the other connected to the child partitions. When you have more than two physical adapters in the server, you can create separate external virtual network switches for the physical adapters and connect each one to a separate VM.

Creating an isolated network

For testing and evaluation purposes or for classroom situations, administrators might want to create isolated network environments. By creating internal or private virtual switches, you can create a network that exists only within the Hyper-V space, with or without the parent partition included.

An isolated network such as this has limitations, however. If you want to install the guest OSs by using Windows Deployment Services or configure the VMs by using DHCP, you must install and configure those services on your private network. The guest OSs also do not have access to the Internet, which prevents them from downloading OS updates. In this case, you must deploy appropriate substitutes on the private network.

One way to provide your systems with updates is to install two network adapters on each of your VMs, connecting one to a private switch and one to an external switch. This enables the VMs to access the Internet and the private network.

Another method for creating an isolated network is to use VLANs. This is particularly helpful if you have VMs on different Hyper-V servers that you want to add to the isolated network. By connecting the network adapters to an external switch and configuring them with the same VLAN identifier, you can create a network within a network, which isolates the VLAN from other computers. You can, for example, deploy a DHCP server on your VLAN without it interfering with the other DHCP servers in your production environment.

Thought experiment

Configuring Hyper-V networking

In the following thought experiment, apply what you've learned about this objective to predict what steps you need to take. You can find answers to these questions in the "Answers" section at the end of this chapter.

Ralph has a Windows Server 2012 R2 Hyper-V server with one physical network adapter and one external virtual switch connected to that adapter. This arrangement enables the VMs on the server to automatically download OS updates from the Internet. However, Ralph wants to use the VMs on the Hyper-V server on an isolated test network on which he can evaluate new software products. The test network must have its own DHCP server that does not interfere with the DHCP server on the production network.

How can Ralph create the test network he needs for his VMs without changing the configuration that provides the machines with Internet access?

Objective summary

- Networking is a critical part of creating a VM infrastructure. Depending on your network plan, the VMs you create on a Windows Server 2012 R2 Hyper-V server can require communication with other VMs, with the computers on your physical network, and with the Internet.
- A virtual switch, like its physical counterpart, is a device that functions at Layer 2 of the OSI reference model. A switch has a series of ports, each of which is connected to a computer's network interface adapter. Any computer connected to the switch can transmit data to any other computer connected to the same switch.
- Hyper-V in Windows Server 2012 R2 supports three types of switches: external, internal, and private, which you must create in the virtual Switch Manager before you can connect VMs to them.
- Every network interface adapter has a MAC address—sometimes called a hardware address—that uniquely identifies the device on the network.
- Once you have created virtual switches in Hyper-V Manager, you can connect VMs to them by creating and configuring virtual network adapters.
- Selecting the Network Adapter option on the Add Hardware page creates what is known in Hyper-V terminology as a synthetic network adapter. Hyper-V supports two types of network and storage adapters: synthetic and emulated (sometimes called legacy).
- NIC teaming is a Windows feature that enables administrators to join multiple network adapters into a single entity for performance enhancement or fault tolerance purposes.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which of the following are valid reasons for using an emulated network adapter rather than a synthetic one? (Choose all that apply.)
   - **A.** You want to install the guest OS by using a Windows Deployment Services server.
   - **B.** There is no Guest Integration Services package available for the guest OS you plan to use.
   - **C.** The manufacturer of your physical network adapter has not yet provided a synthetic network adapter driver.
   - **D.** The emulated network adapter provides better performance.
2. Which of the following statements is *not* true about synthetic network adapters?
   - **A.** Synthetic adapters communicate with the parent partition by using the VMBus.
   - **B.** Synthetic adapters require the Guest Integration Services package to be installed on the guest OS.
   - **C.** Synthetic adapters provide faster performance than emulated adapters.
   - **D.** Synthetic adapters can start the child VM by using a PXE network boot.
3. What is the maximum number of ports supported by a Hyper-V virtual switch?
   - **A.** 8
   - **B.** 256
   - **C.** 4,096
   - **D.** Unlimited
4. Which of the following virtual switch types does *not* enable guest OSs to communicate with the parent partition?
   - **A.** External
   - **B.** Internal
   - **C.** Private
   - **D.** Isolated
5. How many dynamically assigned MAC addresses can a Hyper-V server provide by default?
   - **A.** 8
   - **B.** 256
   - **C.** 4,096
   - **D.** Unlimited

Answers

This section contains the solutions to the thought experiments and answers to the objective review questions in this chapter.

Objective 3.1: Thought experiment

Alice can enable Dynamic Memory on each of the eight VMs and set the minimum RAM value on each to 512 MB. This will enable each VM to start with 1,024 MB of memory and then reduce its footprint, allowing the next machine to start.

Objective 3.1: Review

1. **Correct answers:** B, C
   - **A. Incorrect:** In Type I virtualization, the hypervisor does not run on top of a host OS.
   - **B. Correct:** A Type I hypervisor runs directly on the computer hardware.
   - **C. Correct:** A Type II hypervisor runs on top of a host OS.
   - **D. Incorrect:** In Type II virtualization, the hypervisor does not run directly on the computer hardware.
2. **Correct answer:** A
   - **A. Correct:** Type I virtualization provides the best performance because the hypervisor runs directly on the computer hardware and does not have the overhead of a host OS.
   - **B. Incorrect:** Type II virtualization provides poorer performance than Type I because of the need to share processor time with the host OS.
   - **C. Incorrect:** Presentation virtualization is the term used to describe the Remote Desktop Services functionality in Windows. It is not designed for virtualizing servers.
   - **D. Incorrect:** RemoteApp is a technology for virtualizing individual applications and deploying them by using Remote Desktop Services.
3. **Correct answer:** B
   - **A. Incorrect:** Hyper-V Server does not include a license for any virtual instances.
   - **B. Correct:** Windows Server 2012 R2 Datacenter edition includes a license that enables you to create an unlimited number of virtual instances.
   - **C. Incorrect:** Windows Server 2012 R2 Standard edition includes a license that enables you to create two virtual instances.
   - **D. Incorrect:** Windows Server 2012 R2 Foundation edition does not include support for Hyper-V.

4. **Correct answers:** A, B, D

   A. **Correct:** Smart paging enables a VM to restart even if the amount of RAM specified as the startup value is unavailable. Smart paging causes the system to use disk space as a temporary substitute for memory during a system restart.

   B. **Correct:** Dynamic Memory enables you to specify a minimum RAM value that is smaller than the startup RAM value, but Smart paging enables the system to function with those parameters.

   C. **Incorrect:** Windows Memory Weight controls the allocation of memory among VMs, but it does not affect the ability of a system to start.

   D. **Correct:** Guest Integration Services is required for a guest OS to use Dynamic Memory.

5. **Correct answer:** C

   A. **Incorrect:** The instance of the OS on which you install Hyper-V does not become the hypervisor.

   B. **Incorrect:** The instance of the OS on which you install Hyper-V does not become the VMM.

   C. **Correct:** The instance of the OS on which you install the Hyper-V role becomes the parent partition.

   D. **Incorrect:** The instance of the OS on which you install the Hyper-V role does not become the child partition.

6. **Correct answer:** B

   A. **Incorrect:** You can create a new Generation 1 or Generation 2 virtual machine at any time.

   B. **Correct:** Because they use improved and synthetic drivers, Generation 2 VMs deploy faster than Generation 1 VMs.

   C. **Incorrect:** Generation 2 VMs can run Windows Server 2012, Windows Server 2012 R2, Windows 8, or Windows 8.1 as a guest operating system.

   D. **Incorrect:** Generation 2 VMs use improved and synthetic drivers, as compared to the legacy drivers in Generation 1 VMs.

Objective 3.2: Thought experiment

Ed should use the following Windows PowerShell command to create the VHD.

```
New-VHD –Path c:\servera.vhdx –Fixed –SizeBytes 500GB -LogicalSectorSizeBytes 4096 –
SourceDisk 0
```

Objective 3.2: Review

1. **Correct answer:** B

A. **Incorrect:** VHDX files can be as large as 64 TB, whereas VHD files are limited to 2 TB.

B. **Correct:** Windows Server 2012, Windows Server 2012 R2, Windows 8, and Windows 8.1 can all open VHDX files.

C. **Incorrect:** VHDX files support block sizes as large as 256 MB.

D. **Incorrect:** VHDX files can support the 4,096-byte block sizes found on some newer drives.

2. **Correct answer:** B

A. **Incorrect:** A pass-through disk must be online in the guest OS that will access it.

B. **Correct:** A pass-through disk must be offline in the parent container so that the guest OS can have exclusive access to it.

C. **Incorrect:** A pass-through disk can be connected to any type of controller.

D. **Incorrect:** You do not use the Disk Management snap-in to add a pass-through disk to a VM; you use Hyper-V Manager.

3. **Correct answer:** D

A. **Incorrect:** You can merge VHD or VHDX disks.

B. **Incorrect:** You can only select one disk for editing.

C. **Incorrect:** There is no free space requirement when merging a disk.

D. **Correct:** The Merge function appears only when you select a differencing disk for editing. The object of the function is to combine the data in the differencing disk with that of the parent.

4. **Correct answers:** A, D

A. **Correct:** Checkpoints consume disk space that could be better used for other purposes.

B. **Incorrect:** Checkpoints do not require a duplicate memory allocation.

C. **Incorrect:** Under typical conditions, checkpoints do not take several hours to create.

D. **Correct:** The Hyper-V server must locate and process checkpoints each time it accesses a VM's disk drives, slowing down its performance.

5. **Correct answer:** D

A. **Incorrect:** You must create a Fibre Channel SAN before you can add a Fibre Channel adapter to a VM.

B. **Incorrect:** You must have a physical Fibre Channel adapter before you can create virtual Fibre Channel components.

C. **Incorrect:** The driver for your physical Fibre Channel adapter must support virtual networking.

D. **Correct:** SCSI cables are not required for Fibre Channel installations.

Objective 3.3: Thought experiment

Ralph can create an isolated test environment without changing the virtual switch configuration by selecting the Enable Virtual LAN Identification check box on the network adapter in each VM and specifying the same VLAN identifier for each VM he wants on the test network.

Objective 3.3: Review

1. **Correct answers:** A, B

   A. **Correct:** A Windows Deployment Server installation requires the network adapter to support PXE, which emulated adapters do, but synthetic adapters do not.

   B. **Correct:** Synthetic adapter drivers are installed as part of the Guest Integration Services package; if there is no package for the guest OS, then there are no synthetic drivers.

   C. **Incorrect:** Synthetic adapter drivers are not provided by hardware manufacturers.

   D. **Incorrect:** Synthetic adapters provide better performance than emulated adapters.

2. **Correct answer:** D

   A. **Incorrect:** Synthetic adapters use the faster VMBus for communications with the parent partition; emulated adapters must use calls to the hypervisor.

   B. **Incorrect:** Synthetic adapter drivers are installed as part of the Guest Integration Services package on the guest OS.

   C. **Incorrect:** Because of their more efficient communication with the parent partition, synthetic adapters perform better than emulated adapters.

   D. **Correct:** Synthetic network adapters load with the Guest Integration Services on the guest OS, which prevents them from supporting PXE.

3. **Correct answer:** D

   A. **Incorrect:** Switches limited to eight connections would be insufficient for many Hyper-V installations.

B. **Incorrect:** Hyper-V switches are not limited to 256 connections.

C. **Incorrect:** Hyper-V switches are not limited to 4,096 connections.

D. **Correct:** Hyper-V virtual switches can support an unlimited number of connections.

4. **Correct answer:** C

A. **Incorrect:** External switches enable the guest OSs to communicate with the outside network and the parent partition.

B. **Incorrect:** Internal switches enable the guest OSs to communicate with the parent partition but not with the outside network.

C. **Correct:** Private switches enable the guest OSs to communicate with one another but not with the outside network or the parent partition.

D. **Incorrect:** Isolated is not a technical term referring to a type of virtual switch.

5. **Correct answer:** B

A. **Incorrect:** A pool of eight MAC addresses would be insufficient for many Hyper-V installations.

B. **Correct:** A Hyper-V server provides a pool of 256 MAC addresses by default. You can create more by modifying the default address range.

C. **Incorrect:** Hyper-V, by default, dedicates only one byte of the MAC address to a dynamic value, which is not enough to support 4,096 addresses.

D. **Incorrect:** Hyper-V creates a finite pool of MAC addresses by specifying minimum and maximum address values.

Index

Symbols

6to4 mechanism, IP transitioning, 213

A

AAAA (Address) resource records, 245
A (Address) resource records, 245
ABE (access-based enumeration), 76
access-based enumeration (ABE), 76
access control entries (ACEs), 77
access control list (ACL), 77
accessing
  files, configuring share access, 71–89
    folder shares, 72–77
    NTFS quotas, 87–88
    permissions, 77–86
    Volume Shadow Copies, 86–87
    Work Folders, 89
access tokens, 300
Account Operators group, 292
ACEs (access control entries), 77
ACL (access control list), 77
Action parameter (New Inbound Rule Wizard), 366
Activate instance ntds command, 268
Activate Scope page (New Scope Wizard), 224
active/active configuration (Switch Independent Mode), 22
Active Directory Administrative Center console, 277
  creating computer objects, 288
  creating single AD DS users, 278–282
Active Directory Domain Services. *See* AD DS
Active Directory-integrated zones, 243–244
Active Directory objects, management, 288–293
Active Directory Object Type page (Delegation of Control Wizard), 299
Active Directory Sites And Services console, 273
Active Directory tab
  adding servers in Server Manager, 114
Active Directory Users and Computers console, 277
  Copy Object-User Wizard, 282
  creating computer objects, 287
  creating user templates, 282–283
  New Object - User Wizard, 279
Active Directory Zone Replication Scope page (New Zone Wizard), 244
active/standby configuration (Switch Independent Mode), 22
adapters, virtual networks, 181–185
  advanced network adapter features, 185
  emulated adapters, 183–184
  hardware acceleration settings, 184–185
  synthetic adapters, 183–184
Add action, LDIFDE.exe utility, 284
Add-DnsServerPrimaryZone cmdlet, 245
Add Exclusions And Delay page (New Scope Wizard), 223
Add Features That Are Required dialog box, 32
Add Features That Are Required For Active Directory Domain Services dialog box, 258
Add Features That Are Required For Hyper-V dialog box, 137
adding
  print servers, 107, 107–108
  servers, Server Manager, 113–114
Additional Drivers dialog box, 100
Additional Options page (AD DS Configuration Wizard), 264
Additional Rules folder (Software Restriction Policies node), 346
Additive permission management task, 79
-addmbr <members> command-line parameter, 307
Add Or Remove Snap-Ins dialog box, 325

Add Printer Wizard, 99
Add/Remove Servers dialog box, 107
Address (AAAA) resource records, 245
Address (A) resource records, 245
addresses
  IPv4 addressing. *See* IPv4 addressing
  IPv6 addressing. *See* IPv6 addressing
Add Roles And Features Wizard
  Create Virtual Switches page, 137
  Virtual Machine Migration page, 137–138
AD DS
  Configuration Wizard, 259
  domain controllers, 257–273
    adding to existing domains, 263–265
    configuring the global catalog, 272–273
    creating a new child domain in a forest, 265–266
    creating a new forest, 259–263
    deploying IaaS on Windows Azure, 270–271
    Install from Media (IFM) option, 268–269
    installing AD DS on Server Core, 266–268
    installing AD DS role, 258–259
    removing, 271–272
    troubleshooting DNS SRV registration failure, 273
    upgrading AD DS, 269–270
  Installation Wizard, 259
  management of groups and OUs, 295–309
    creating OUs, 296–298
    using OUs to assign Group Policy settings, 298
    using OUs to delegate AD management tasks, 298–300
    working with groups, 300–309
  management of users and computers, 276–293
    Active Directory objects, 288–293
    creating computer objects, 285–288
    creating user objects, 276–285
Add Servers dialog box, 27, 114
Add Workstations To The Domain right, 291
administration
  AD DS
    domain controllers, 257–273
    management of groups and OUs, 295–309
    management of users and computers, 276–293
administrative tasks, configuring User Account Control, 340–341
Administrative Templates subnode, 323
Administrators and Nonadministrators Group Policy layer, 324
Administrators group, 292
ADMX files, 319
Adprep.exe functionality, 270
advanced network adapter features, 185
advanced NTFS permissions, assigning, 85
advanced permissions, 78–79
advanced printing configurations, 99
Advanced Security Settings dialog box, 79, 82
Advanced Sharing dialog box, 72–73
aggregation (NIC teaming), 22
allocating memory, Hyper-V Manager console, 150–153
allocation methods
  DHCP IP addresses, 217
Allocation Unit Size option, Configuring the Format Partition page, 59
Allow (access control entry), 79
Allowed Apps dialog box, 359, 362
allowing permissions, 79–80
Allow Management Operating System To Share This Network Adapter option, 179
Allow Manage This Printer permission, 104
All Servers home page (Server Manager), 27–28
AMD-V (AMD Virtualization) technology, 136
AMD Virtualization (AMD-V) technology, 136
anycast addresses, IPv6, 207
Anycast transmissions, IPv6 addressing, 206
APIPA (Automatic Private IP Addressing), 205
Application Identity service, AppLocker and, 354
application restriction policies (GP), 345–354
  AppLocker, 352–354
  configuring restriction properties, 349–352
  configuring rules, 347–349
  enforcing restrictions, 346–347
AppLocker, 352–354
architecture
  DNS, 232–241
    client-side resolver caching, 238
    DNS coomunications, 233–236
    forwarders, 239–240
    referrals and queries, 238–239
    reverse name resolution, 240–241
    server caching, 236–238
  permissions, 77–78
  virtualization, 132–133
  Windows print architecture, 93
Assign Drive Letter Or Path page (New Simple Volume Wizard), 58

Assign Drive Letter Or Path page (New Volume Wizard), 61
assigning
  IPv4 addresses, 203–205
  IPv6 addresses, 207–209
  user rights, 292
    local security policies, 331–333
assigning permissions, 77–86
  advanced NTFS permissions, 85
  allowing/denying permissions, 79–80
  basic and advanced permissions, 78–79
  basic NTFS permissions, 83–85
  combining share permissions with NTFS permissions, 85–86
  effective access, 80–81
  inherited permissions, 80
  NTFS authorization, 83
  setting share permissions, 81–83
  Windows permission architecture, 77–78
Assign The Following Drive Letter option, 58
Attach A Virtual Hard Disk Later option, Connect Virtual Hard Disk page, 158
attributes
  creating user accounts, 283
Audit Directory Service Access event category, 331
Audit Object Access event category, 331
audit policies, GPOs, 328–331
authentication, 276
Authentication Method parameter (New Connection Security Rule Wizard), 368
authorization, 276
automatic allocation
  definition, 217
Automatically Generate Rules Wizard, 354
Automatic Private IP Addressing (APIPA), 205

B

Backup function (Guest Integration Services), 147
Backup Operators group, 292
balancing (NIC teaming), 22
basic disks, 44
basic NTFS permissions, assigning, 83–85
basic permissions, 78–79
Basic User approach, enforcing restrictions, 346
bonding (NIC teaming), 22
BOOTP (Bootstrap Protocol), 218
Bootstrap Protocol (BOOTP), 218
boot threshold, 229
boot vendor information extensions, 218
Browse For A Group Policy Object dialog box, 325

C

caching
  DNS servers, 236–238
Canonical Name (CNAME) resource records, 245
capabilities, Server Core, 9–10
Central Store, configuring, 319
certificate rules, 348
Change Zone Replication Scope dialog box, 247
checkpoints, 165–166
child domains
  creating in a forest, 265–266
child partitions, 133
-chmbr <members> command-line parameter, 308
CIDR (Classless Inter-Domain Routing), 200–201
classes
  IPv4 addresses, 198–200
classful addressing, IPv4, 198–200
Classless Inter-Domain Routing (CIDR), 200–201
clients, DHCP, 217
client-side resolver caching, DNS, 238
client-sode caching, 76
cmdlets
  Add-DnsServerPrimaryZone, 245
  Enable-VMResourceMetering, 153
  Get-PhysicalDisk, 53
  Get-StorageSubsystem, 53
  Install-ADDSDomain, 266
  Install-ADDSDomainController, 266
  Install-ADDSForest, 266
  Install-WindowsFeature, 266
  Measure-VM, 153
  New-ADUser, 281
  New-GPO, 322
  New-StoragePool, 52
    options, 53
  New-VHD, 159
  New-VM, 142
  New-VMResourcePool, 153
  New-VMSwitch, 179
  Set-VMMemory, 152
  Uninstall-WindowsFeature, 11

CNAME (Canonical Name) resource records, 245
command-line tools, postinstallation tasks, 20–21
commands
  Activate instance ntds, 268
  Create Full|RODC, 269
  Get-Help, 267
  Ifm, 268
  Ntdsutil, 268
Comma-Separated Value Directory Exchange (CSVDE.exe) command-line tool, 277
  creating multiple AD DS users, 283–284
communications
  DHCP, 219–223, 220–224
    lease negotiation, 219–221
    lease renewal, 221–223
  DNS, 233–236
Compact function (Edit Virtual Hard Disk Wizard), 164
Compatability Report page (Setup program), 13
Completing The New Simple Volume Wizard page (New Simple Volume Wizard), 59
Computer Name/Domain Changes dialog box, 289–290
Computer Name tab, System Properties sheets, 289
computers, AD DS management, 276–293
  Active Directory objects, 288–293
  creating computer objects, 285–288
Configuration page (Routing and Remote Access Server Setup Wizard), 228
configurations
  virtual networks, 188–189
configuration scripts, DSC, 38
Configure DHCP Options page (New Scope Wizard), 223
Configure Networking page (New Virtual Machine Wizard), 140
Configure Remote Access Getting Started Wizard, 228
Configure Share Settings page (New Share Wizard), 75
configuring
  core network services
    DHCP service, 217–232
    DNS, 232–250
    IPv4 and IPv6 addressing, 197–214
  file and share access, 71–89
    folder shares, 72–77
    NTFS quotas, 87–88
    permissions, 77–86
    Volume Shadow Copies, 86–87
    Work Folders, 89
  global catalog, 272–273
Group Policy settings, 323–324
Hyper-V
  virtual machine settings, 131–155
local storage, 41–63
  disks, 46–63
  disk settings, 43–46
  planning storage needs, 41–43
print and document services, 92–110
  deploying print servers, 92–99
  document management, 103–104
  managing printers, 104–106
  Print and Document Services role, 106–110
  sharing printers, 99–103
printer security, 102–103
roles and features
  file and share access, 71–89
  print and document services, 92–110
  servers for remote management, 112–122
servers, 18–37
  delegating server administration, 37
  DSC (Desired State Configuration), 37–38
  postinstallation tasks, 18–25
  remote management, 112–122
  Server Manager tool, 26–35
  services, 36–37
software restriction policies (GP), 347–349
software restriction properties, 349–352
virtual machine settings, 131–155
  Hyper-V implementations, 133–136
  Hyper-V Manager, 138–154
  installing Hyper-V, 136–138
  resource metering, 152–153
  virtualization architectures, 132–133
virtual machine storage, 156–173
  checkpoints, 165–166
  connecting to a SAN, 167–172
  modifying virtual disks, 164–165
  pass-through disks, 163–164
  QoS (Quality of Service), 166–167
  virtual disk formats, 156–157
  virtual disks, 157–163
virtual networks, 174–188
  configurations, 188–189
  NIC teaming, 185–188
  virtual network adapters, 181–185
  virtual switches, 175–181
Windows Firewall, 116–118, 357–368
  control panel applet, 359–363

settings, 357–358
Windows Firewall with Advanced Security snap-in, 363–368
WinRM, 116–117
connections
SANs (storage area networks), 167–172
Fibre Channel, 169–170
virtual machines to SANs, 170–172
Connect Virtual Hard Disk page (New Virtual Machine Wizard), 141–142, 157
containers, 296
contextual tasks, addressing remote servers, 122
contracting IPv6 addresses, 206
control panel applet, Windows Firewall, 359–363
Convert function (Edit Virtual Hard Disk Wizard), 164
converting groups, AD DS, 308
Convert To GPT Disk option, 48
Convert To MBR Disk option, 48
Copy Object-User Wizard, 282
core network services
DHCP, 217–232
communications, 219–223
deploying DHCP relay agents, 227–230
deploying DHCP servers, 222–227
IP address allocation methods, 217
options, 218–220
DNS, 232–250
architecture, 232–241
deploying servers, 241–248
IPv4 and IPv6 addressing, 197–214
assigning IPv4 addresses, 203–205
assigning IPv6 addrersses, 207–209
CIDR (Classless Inter-Domain Routing), 200–201
introduction to IPv6 addressing, 205–206
IPv4 classful addressing, 198–200
IPv4 subnetting, 201–202
IPv6 address types, 206–207
planning an IP transition, 211–214
public and private IPv4 addressing, 201
subnetting IPv6 addresses, 210–211
supernetting, 202–203
Create And Attach Virtual Hard Disk dialog box, 49
Create A Virtual Hard Disk option, Connect Virtual Hard Disk page, 157
Create Full|RODC command, 269
Create Group window, AD Administrative Center console, 303–304
Create Organizational Unit window, AD DS Administrative Center console, 297
Create Server Group dialog box, 120–121
Create User window (Active Directory Administrative Center console), 278
Create Virtual Switches page (Add Roles and Features Wizard), 137
creating
checkpoints, 165–166
computer objects, AD DS, 285–288
differencing disks, 162–163
folder shares, 72–77
forests, 259–263
Group Policy settings
GPOs (Group Policy Objects), 317–325
software restriction policies, 345–354
Windows Firewall, 357–368
groups, AD DS, 303–305
OUs (organizational units), AD DS, 296–298
printer pools, 105
reservations, DHCP servers, 225–226
resource records, DNS, 245–247
Restricted Groups policies, 306
scope, DHCP servers, 222–224
server groups, 120–121
user objects, AD DS, 276–285
multiple users, 283–285
single users, 278–282
user templates, 282–283
virtual disks, 53–57, 157–163
virtual machine settings, 131–155
Hyper-V implementations, 133–136
Hyper-V Manager, 138–154
installing Hyper-V, 136–138
resource metering, 152–153
virtualization architectures, 132–133
virtual machine storage, 156–173
checkpoints, 165–166
connecting to a SAN, 167–172
modifying virtual disks, 164–165
pass-through disks, 163–164
QoS (Quality of Service), 166–167
virtual disk formats, 156–157
virtual disks, 157–163
virtual networks, 174–188
configurations, 188–189
NIC teaming, 185–188, 186–189
virtual network adapters, 181–185

virtual switches, 175–181, 177–179
zones, DNS servers, 242–245
creation permissions, 299
creation tools, creating AD DS user objects, 277–278
credential prompts, User Account Control, 340
Credentials For Deployment Operation dialog box, 263
CSVDE.exe (Comma-Separated Value Directory Exchange) command-line tool, 277
creating multiple AD DS users, 283–284
CSV files, 283
Custom Configuration page (Routing and Remote Access Server Setup Wizard), 228
Custom Filters node (Print Management console), 108–109
Customize Settings dialog box, 360

D

Dashboard page (Server Manager), 26–27
Datacenter edition, 3
Hyper-V licensing, 134
support for Hyper-V, 4
Data Exchange function (Guest Integration Services), 147
Data Execution Prevention (DEP), 136
Dcpromo.exe program, 259
Default Domain Controllers Policy GPO, 291
Default Gateway option, manual configuration of IPv4 addresses, 204
default installation, Server Core, 8
default rules, AppLocker, 354
Default Security Level setting (Software Restriction Policies node), 346
default virtual switches, 175–176
delegating
printer privileges, 37
server administration, 37
Delegation of Control Wizard, 298
Delete action, LDIFDE.exe utility, 284
deleting
groups, AD DS, 308–309
deletion permissions, 299
Deny (access control entry), 79
denying permissions, 79–80
DEP (Data Execution Prevention), 136
deploying
Active Directory IaaS on Windows Azure, 270–271
core network services
DHCP, 217–232
DNS, 232–250
IPv4 and IPv6 addressing, 197–214
DHCP relay agents, 227–230
DHCP servers, 222–227
configuring DHCP options, 224–225
creating a scope, 222–224
creating reservations, 225–226
PXE, 226–227
DNS servers, 241–248
configuring settings, 247–248
creating zones, 242–245
resource records, 245–248
Group Policy settings
GPOs (Group Policy Objects), 317–325
software restriction policies, 345–354
Windows Firewall, 357–368
printers with Group Policy, 109–110
print servers, 92–99
understanding Windows printing, 93–94
Windows print architecture, 93
Windows print flexibility, 94–99
roles to VHDs, 34–35
Deployment Configuration page (AD DS Configuration Wizard), 259–260, 265
Deploy With Group Policy dialog box, 109–110
deprecated IPv6 addresses, 207
-desc <description> command-line parameter, 305
Designated File Types properties, 350–351
Desired State Configuration (DSC), 37–38
DHCPACK message type, DHCP, 218
DHCPDECLINE message type, DHCP, 218
DHCPDISCOVER message type, DHCP, 218
DHCP (Dynamic Host Configuration Protocol), 217–232
communications, 219–223
lease negotiation, 219–221
lease renewal, 221–223
deploying DHCP relay agents, 227–230
deploying servers, 222–227
configuring DHCP options, 224–225
creating a scope, 222–224
creating reservations, 225–226
PXE, 226–227
IP address allocation methods, 209, 217
manual configuration of IPv4 addresses, 204–205
options, 218–220
DHCPINFORM message type, DHCP, 218

DHCPNAK message type, DHCP, 218
DHCPOFFER message type, DHCP, 218
DHCP Relay Agent Properties sheet, 229
DHCPRELEASE message type, DHCP, 218
DHCPREQUEST message type, DHCP, 218
dialog boxes
  Add Features That Are Required, 32
  Add Features That Are Required For Active Directory Domain Services, 258
  Add Features That Are Required For Hyper-V, 137
  Additional Drivers, 100
  Add Or Remove Snap-Ins, 325
  Add/Remove Servers, 107
  Add Servers, 27, 114
  Advanced Security Settings, 79, 82
  Advanced Sharing, 72–73
  Allowed Apps, 359, 362
  Browse For A Group Policy Object, 325
  Change Zone Replication Scope, 247
  Computer Name/Domain Changes, 289–290
  Create And Attach Virtual Hard Disk, 49
  Create Server Group, 120–121
  Credentials For Deployment Operation, 263
  Customize Settings, 360
  Deploy With Group Policy, 109–110
  File Sharing, 72
  Import Policy From, 336
  Move, 297
  New GPO, 320
  New Group, 339
  New Host, 246
  New Interface For DHCP Relay Agent, 229
  New Object-Group, 304
  New Path Rule, 347
  New User, 338
  NIC Teaming, 186
  Select A Domain From The Forest, 263
  Select GPO, 321
  Select Print Server, 107
  Select Users, 339
  Settings, new virtual machines, 143–144
  Shadow Copies, 86
  User Account Control Settings, 342
  Validation Results, 271
  Virtual Switch Manager, 177
differencing disks, 158, 162–163
differencing hard disk image VHD files, 157
directory services, definition, 257
Directory Services Restore Mode (DSRM), 262
direct printing, 95
Disabled state, Administrative Template settings, 323
disabling user accounts, 292–293
Disallowed approach, enforcing restrictions, 346
Disk Management snap-in, 45, 47
  creating simple volumes, 57
DiskPart.exe utility, 57
disks
  configuring local storage, 46–63
    adding physical disks, 47–48
    creating a simple volume, 56–60
    storage pools, 50–53
    striped, spanned, mirrored, RAID-5 volumes, 60–62
    VHDs (virtual hard disks), 48–50
    virtual disks, 53–57
  settings, 43–46
    disk types, 44–45
    partition style, 43–44
Disks tile (Server Manager), 47–48
disks, virtual
  creating, 157–163
  formats, 156–157
  modifying, 164–165
  pass-through disks, 163–164
  QoS (Quality of Service), 166–167
disk virtualization technology, Storage Spaces, 42–43
distinguished name (DN), users, 280
Distributed Scan Server option (Select Role Services page), 106
distribution groups, 301
Djoin.exe command-line tool, joining a domain while offline, 292
dn attribute, 283
DN (distinguished name), users, 280
DNS (Domain Name System), 232–250
  architecture, 232–241
    client-side resolver caching, 238
    DNS coomunications, 233–236
    forwarders, 239–240
    referrals and queries, 238–239
    reverse name resolution, 240–241
    server caching, 236–238
  deploying servers, 241–248
    configuring settings, 247–248
    creating zones, 242–245
    resource records, 245–248

DNS SRV registration failure, 273
DNS tab
  adding servers in Server Manager, 114
document services, configuring, 92–110
  deploying print servers, 92–99
    understanding Windows printing, 93–94
    Windows print architecture, 93
    Windows print flexibility, 94–99
  document management, 103–104
  managing printers, 104–106
  Print and Document Services role, 106–110
    adding print servers, 107–108
    deploying printers with Group Policy, 109–110
    viewing printers, 108–109
  sharing printers, 99–103
    configuring printer security, 102–103
    managing printer drivers, 101
    remote access Easy Print, 101–102
Domain Admins group, 270
Domain Controller Options page (AD DS Configuration Wizard), 260–261, 263
domain controllers
  installation, 257–273
    adding to existing domains, 263–265
    configuring the global catalog, 272–273
    creating a new child domain in a forest, 265–266
    creating a new forest, 259–263
    deploying IaaS on Windows Azure, 270–271
    Install from Media (IFM) option, 268–269
    installing AD DS on Server Core, 266–268
    installing AD DS role, 258–259
    troubleshooting DNS SRV registration failure, 273
    upgrading AD DS, 269–270
  removing, 271–272
domain local groups, AD DS, 301–302
Domain Name And DNS Servers page (New Scope Wizard), 224
Domain Name System. *See* DNS (Domain Name System)
domains
  adding domain controllers to existing domains, 263–265
  definition, 257
  joining computers to, 289–292
domain users, 277
Do Not Assign A Drive Letter Or Drive Path option, 58
down-level servers, 118–120
drivers
  printers, 101
Dsadd.exe command-line tool, 277
  creating computer objects, 288
  creating group objects, 304–305
  creating single AD DS users, 279–280
DSC (Desired State Configuration), 37–38
DSC Service, 38
Dsmod.exe command-line tool
  managing group objects, 307–308
DSRM (Directory Services Restore Mode), 262
dual IP stacks, IP transitioning, 212
DVD drive settings, virtual machines, 145–146
dynamic allocation
  assigning IPv6 addresses, 208–209
  definition, 217
Dynamically Expanding disks, 158
Dynamically Expanding VHD Type option, 49
dynamic disks, 45
dynamic hard disk image VHD files, 157
Dynamic Host Configuration Protocol. *See* DHCP (Dynamic Host Configuration Protocol)
Dynamic Memory, Hyper-V Manager console, 150–153
Dynamic Update page (New Zone Wizard), 244

E

Easy Print, 101–102
editions, 3
Edit Virtual Hard Disk Wizard, 164–165
effective access, assigning permissions, 80–81
elevation prompts, User Account Control, 341
emulated adapters, 183–184
Enable DHCP Guard (advanced network adapter feature), 185
Enabled state, Administrative Template settings, 323
Enable File And Folder Compression option, Configuring the Format Partition page, 59
Enable IPsec Task Offloading (hardware acceleration setting), 185
Enable MAC Address Spoofing (advanced network adapter feature), 185
Enable Single Root I/O Virtualization (SR-IOV) option, 179
Enable Virtual LAN Identification For Management Operating System option, 179

Enable Virtual Machine Queue (hardware acceleration setting), 184
Enable-VMResourceMetering cmdlet, 153
-EnclosureAwareDefault option (New-StoragePool cmdlet), 53
Endpoints parameter (New Connection Security Rule Wizard), 368
Enforcement properties, 350
enforcing restrictions, Group Policy, 346–347
enhanced session mode, 148–149
Enhanced Session Mode Policy settings, 149–150
Enterprise Admins group, 270
Essentials edition, 3
Executable Rules node, AppLocker, 353
eXecute Disable (XD), 136
Expand function (Edit Virtual Hard Disk Wizard), 164
Export Configuration Settings function, 259
expressing IPv6 network addresses, 206
External virtual switches, 178

F

FAT file systems, 46
fault tolerance, Storage Spaces, 54
FCoE (Fibre Channel over Ethernet), 170
features
  adding, Server Manager tool, 29–33
  configuring
    file and share access, 71–89
    print and document srevices, 92–110
    servers for remote management, 112–122
Features on Demand, 10–11
Fibre Channel, 169–170
Fibre Channel over Ethernet (FCoE), 170
File and Storage Services home page (Server Manager), 73
File and Storage Services role, 46–47
file hash rules, 353
files
  ADMX, 319
  configuring, 71–89
    folder shares, 72–77
    NTFS quotas, 87–88
    permissions, 77–86
    Volume Shadow Copies, 86–87
    Work Folders, 89
  CSV, 283
File Server Resource Manager quotas, 87
File Server role service, 73
File Sharing, 359–360
File Sharing dialog box, 72
File System option, Configuring the Format Partition page, 59
file systems, 46
Firewall
  configuring, 116–118
Firewall (Windows), 357–368
  control panel applet, 359–363
  settings, 357–358
  Windows Firewall with Advanced Security snap-in, 363–368
first bit values, IP addresses, 199
fixed hard disk image VHD files, 157
Fixed Provisioning Type option, 55
Fixed Size disks, 158
Fixed Size (Recommended) VHD Type option, 49
flexibility, Windows printing, 94–99
folder shares, creating, 72–77
forests
  creating, 259–263
  creating new child domains in, 265–266
Format Partition page (New Simple Volume Wizard), 58
formats
  virtual disks, 156–157
forwarders, DNS, 239–240
Forwarders tab (DNS server Properties sheet), 239–240
Foundation edition, 3

G

GC (Global Catalog)
  configuring, 272–273
  domain controllers, 261
general permissions, 299
Generation 1 VMs, 143–146
Generation 2 VMs, 143–146
Get-Help command, 267
Get-PhysicalDisk cmdlet, 53
Get-StorageSubsystem cmdlet, 53
Global Catalog (GC)
  configuring, 272–273
  domain controllers, 261
global groups, AD DS, 302
global routing prefixes, IP addresses, 210

global unicast addresses, IPv6, 206
GPMC (Group Policy Management Console), 319, 320
  creating/linking nonlocal GPs, 320–321
  security filtering, 321–322
GPOs (Group Policy objects), 109
GPOs (Group Policy Objects)
  creating, 317–325
    Central Store, 319
    configuring settings, 323–324
    Group Policy Management Console, 319–322
    local GPOs, 318, 324–325
    nonlocal GPOs, 319
    starter GPOs, 319, 322
GPT partition style, 44
group nesting, 301, 303
Group Policy
  assigning settings using OUs, 298
  creating GPOs, 317–325
    Central Store, 319
    configuring settings, 323–324
    Group Policy Management Console, 319–322
    local GPOs, 318, 324–325
    nonlocal GPOs, 319
    starter GPOs, 319, 322
  deploying printers, 109–110
  managing group membership, 306–308
  security policies, 328–342
    defining local policies, 328–333
    local users and groups, 336–339
    security templates, 333–336
    User Account Control, 339–342
  software restriction policies, 345–354
    AppLocker, 352–354
    configuring properties, 349–352
    configuring rules, 347–349
    enforcing restrictions, 346–347
    using multiple rules, 349
  Windows Firewall, 357–368
    control panel applet, 359–363
    settings, 357–358
    Windows Firewall with Advanced Security snap-in, 363–368
Group Policy Management Console (GPMC), 319–322
  creating/linking nonlocal GPOs, 320–321
  security filtering, 321–322
Group Policy Management Editor console, 118
Group Policy Management Editor window, 330
Group Policy Object Editor snap-in, 324
Group Policy Objects. *See* GPOs (Group Policy Objects)
Group Policy objects (GPOs), 109
groups
  access to SAM, 336
  Group Policy security policies, 336–339
groups, AD DS management, 295–309
  converting groups, 308
  creating groups, 303–305
  deleting groups, 308–309
  Domain Admins, 270
  Enterprise Admins, 270
  group memberships, 305–308
  group scopes, 301–302
  group types, 301
  nesting groups, 303
  Schema Admins, 270
group scopes, AD DS, 301–302
Guest Integration Services, 147–148
Guest Services function (Guest Integration Services), 147
GUI tools
  postinstallation tasks, 19–20

H

Hard Drive interface, Settings dialog box, 161
hardware acceleration settings, virtual network adapters, 184–185
hardware limitations, Hyper-V, 134
hardware requirements
  Hyper-V installation, 136
hardware requirements, server installation, 5
hash rules, 348
Heartbeat function (Guest Integration Services), 147
hop-count threshold, 229
host operating systems, hypervisor and, 132
Hyper-V
  configuring
    virtual machine settings, 131–155
    virtual machine storage, 156–173
    virtual networks, 174–188
  installation, 136–138
  licensing, 134
  server installation considerations, 4–5
hypervisor, 131
Hyper-V Manager console, 138–154
  creating virtual machines, 139–144

enhanced session mode, 148–149
Generation 1 and Generation 2 VMs, 143–146
Guest Integration Services, 147–148
memory allocation, 150–153
Hyper-V Server, 134–136

I

IaaS (Infrastructure as a Service)
Windows Azure, 270–271
ICANN (Internet Corporation for Assigned Names and Numbers), 201
ICMPv6 (Internet Control Message Protocol version 6), 214
IDE Controller interface, Settings dialog box, 160
IDE (Integrated Drive Electronics) controllers, 156
Ifm command, 268
IFM (Install from Media) option, 268–269
IIS Hostable Web Core feature, 89
implementations
Hyper-V, 133–136
importing
security templates into GPOs, 335–336
Import Policy From dialog box, 336
Import tab
adding servers in Server Manager, 114
in-addr.arpa domain, 240
Inbound Rules list, Windows Firewall with Advanced Security console, 364–365
Infrastructure as a Service (IaaS)
Windows Azure, 270–271
inheriting permissions, 80
Install-ADDSDomain cmdlet, 266
Install-ADDSDomainController cmdlet, 266
Install-ADDSForest cmdlet, 266
installation
AD DS role, 258–259
domain controllers. *See* domain controllers
Hyper-V, 136–138
Migration Tools, 15–16
network-attached print devices, 100
operating systems, 145–146
printers, 94
servers, 2–15
Features on Demand, 10–11
migrating roles, 14–15
Minimal Server Interface, 9–10
planning installation, 2–6
Server Core, 6–9
upgrades, 12–15
Install from Media (IFM) option, 268–269
Install-WindowsFeature cmdlet, 266
Integrated Drive Electronics (IDE) controllers, 156
Integration Services settings, virtual machines, 148
Intel Virtualization Technology (Intel VT), 136
Intel VT (Intel Virtualization Technology), 136
Interface ID, IP addresses, 210
Internal virtual switches, 178
Internet Control Message Protocol version 6 (ICMPv6), 214
Internet Corporation for Assigned Names and Numbers (ICANN), 201
Internet Printing option (Select Role Services page), 106
Internet Protocol Version 4 (TCP/IPv4) Properties sheet, 203–204
Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), 214
IP address aggregation (supernetting), 202–203
IP address allocation methods, DHCP, 217
IP addresses, 358
IP Address Lease Time extension, DHCP, 219
IP Address option, manual configuration of IPv4 addresses, 204
IP Address Range page (New Scope Wizard), 223–224
IPv4 addressing, 197–214
assigning IPv4 addresses, 203–205
CIDR (Classless Inter-Domain Routing), 200–201
classful addressing, 198–200
planning an IP transition, 211–214
public and private addressing, 201
subnetting, 201–202
supernetting, 202–203
IPv6 addressing, 197–214
address types, 206–207
assigning IPv6 addrersses, 207–209
introduction, 205–206
planning an IP transition, 211–214
subnetting IPv6 addresses, 210–211
ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), 214
isolated network environments, 189
iterative queries, DNS, 238

J

JOBD ("Just a Bunch of Disks") arrays, 42
joining computers to domains, 289–292
"Just a Bunch of Disks" (JBOD) arrays, 42

L

LDAP Data Interchange Formal Directory Exchange (LDIFDE.exe) utility, 277
  creating multiple AD DS users, 284
LDIFDE.exe (LDAP Data Interchange Formal Directory Exchange) utility, 277
  creating multiple AD DS users, 284
Lease Duration page (New Scope Wizard), 223
lease negotiation, DHCP, 219–221
lease renewal, DHCP, 221–223
legacy adapters, 183
licensing
  Hyper-V, 134
  server installation, 5
limitations
  Hyper-V hardware, 134
linking nonlocal GPOs, Group Policy Management Console, 320–321
link-local unicast addresses, IPv6, 207
local GPOs, 318, 324–325
Local Group Policy layer, 324
local groups, creating, 339
locally attached print devices, 95
locally attached printer sharing, 95–96
local policies, 328–333
local storage
  configuring, 41–63
    disks, 46–63
    disk settings, 43–46
    planning storage needs, 41–43
local users, 277
  Group Policy security policies, 336–339
Local Users And Groups snap-in, 337–339
Log On Locally right, 292
LPD Service option (Select Role Services page), 106

M

MAC addresses
  virtual switches, 179–180
MAC Address Range (Virtual Switch Manager), 180
Mail Exchanger (MX) resource records, 245
management
  AD DS groups and OUs, 295–309
    creating OUs, 296–298
    using OUs to assign Group Policy settings, 298
    using OUs to delegate AD management tasks, 298–300
    working with groups, 300–309
  AD DS users and computers, 276–293
    Active Directory objects, 288–293
    creating computer objects, 285–288
    creating user objects, 276–285
  Group Policy settings
    GPOs (Group Policy Objects), 317–325
    software restriction policies, 345–354
    Windows Firewall, 357–368
Manager (Hyper-V), 138–154
  creating virtual machines, 139–144
  enhanced session mode, 148–149
  Generation 1 and Generation 2 VMs, 143–146
  Guest Integration Services, 147–148
  memory allocation, 150–153
managing
  documents, 103–104
  printer drivers, 101
  printers, 104–106, 108
  print servers, 108
manual allocation
  assigning IPv6 addresses, 207–208
  definition, 217
manual IPv4 address configuration, 203–204
Maximum RAM setting, Dynamic Memory, 151
MBR partition style, 43
Measure-VM cmdlet, 153
-member <GroupDN> command-line parameter, 305
-memberof <GroupDN> command-line parameter, 305
memberships, AD DS groups, 305–308
memory allocation, Hyper-V Manager console, 150–153
Memory Buffer setting, Dynamic Memory, 151
Memory settings, virtual machines, 150
Memory Weight setting, Dynamic Memory, 151
Merge function (Edit Virtual Hard Disk Wizard), 165
Message extension, DHCP, 219
Message Type option, DHCP, 218–219
Microsoft Network Adapter Multiplexor Driver, 186
migration guides, 15
migration, servers, 14–15

Migration Tools, 14–15
Minimal Server Interface, 9–10
Minimum RAM setting, Dynamic Memory, 151
mirrored volumes
  configuring local storage, 60–62
  disks, 45
Mirror storage layout option, 54
Modify action, LDIFDE.exe utility, 284
modifying
  virtual disks, 164–165
Mount In The Following Empty NTFS Folder option, 58
Move dialog box, 297
multicast addresses, IPv6, 207
Multicast transmissions, IPv6 addressing, 206
multi-level subnet option, subnetting IPv6 addresses, 210
multiple local GPOs, creating, 324–325
multiple users, AD DS, 283–285
MX (Mail Exchanger) resource records, 245

N

Name parameter
  New Connection Security Rule Wizard, 368
  New Inbound Rule Wizard, 366
name resolution process, DNS, 240–241
name resolution requests (referrals), DNS, 238–239
Name Server (NS) resource records, 245
name servers, DNS, 232
namespace, DNS, 232
NAS (network attached storage) technologies, 42
ND (Neighbor Discovery) protocol, 209
Neighbor Discovery (ND) protocol, 209
nesting groups, 301, 303
Netdom.exe command-line utility, joining computers to domains, 290–291
Network Adapter settings, NIC team adapter, 188
Network And Sharing Center control panel, 359
network-attached print devices
  installation, 100
network-attached printer sharing, 98–99
network attached printing, 96–98
network attached storage (NAS) technologies, 42
Network Discovery, 359–360
Network File System (NFS), 73
networks
  virtual networks, 174–188
    configurations, 188–189
    NIC teaming, 185–188
    virtual network adapters, 181–185
    virtual switches, 175–181
network services
  DHCP, 217–232
    communications, 219–223
    deploying DHCP relay agents, 227–230
    deploying DHCP servers, 222–227
    IP address allocation methods, 217
    options, 218–220
  DNS, 232–250
    architecture, 232–241
    deploying servers, 241–248
  IPv4 and IPv6 addressing, 197–214
    assigning IPv4 addresses, 203–205
    assigning IPv6 addrersses, 207–209
    CIDR (Classless Inter-Domain Routing), 200–201
    introduction to IPv6 addressing, 205–206
    IPv4 classful addressing, 198–200
    IPv4 subnetting, 201–202
    IPv6 address types, 206–207
    planning an IP transition, 211–214
    public and private IPv4 addressing, 201
    subnetting IPv6 addresses, 210–211
    supernetting, 202–203
network zone rules, 349
New-ADUser cmdlet, 281
New Connection Security Rule Wizard, 367
New-GPO cmdlet, 322
New GPO dialog box, 320
New Group dialog box, 339
New Host dialog box, 246
New Inbound (or Outbound) Rule Wizard, 365
New Interface For DHCP Relay Agent dialog box, 229
New Object-Computer Wizard, 287
New Object-Group dialog box, 304
New Object - User Wizard, 279
New Path Rule dialog box, 347
New Scope Wizard, 223, 224–225
New Share Wizard, 73–74
New Simple Volume Wizard, 57
New-StoragePool cmdlet, 52
  options, 53
New Storage Pool Wizard, 50
New Team page (Server Manager), 23
New User dialog box, 338
New-VHD cmdlet, 159

New Virtual Disk menu, 53
New Virtual Machine Wizard
Configure Networking page, 140
Connect Virtual Hard Disk page, 141–142, 157
Specify Generation page, 144
New-VM cmdlet, 142
New-VMResourcePool cmdlet, 153
New-VMSwitch cmdlet, 179
New Zone Wizard, 244
NFS (Network File System), 73
NFS Share-Advanced option (File Share Profile list), 74
NFS Share-Quick option (File Share Profile list), 74
NIC teaming, 22–26
virtual networks, 185–188
configuring virtual network adapters, 187–188
creating NIC teams, 186
creating team virtual switches, 187
NIC Teaming dialog box, 186
NIC Teaming window, 23
NIC teams, creating, 186
No eXecute (NX), 136
noncontextual tasks, addressing remote servers, 122
noncontextual tools, addressing remote servers, 122
non-domain joined servers, 115–116
nonlocal GPOs, 319
creating and linking, , Group Policy Management Console, 320–321
Not Configured state, Administrative Template settings, 323
NS (Name Server) resource records, 245
Ntdsutil.exe command-line tool, 268
NTFS authorization
assigning permissions, 83
NTFS file system, 46
NTFS permissions, 77
advanced NTFS permissions, 85
basic permissions, 83–85
combining with share permissions, 85–86
NTFS quotas, configuring, 87–88
NX (No eXecute), 136

O

objectClass attribute, 283
Offline Files, 76
one-level subnet option, subnetting IPv6 addresses, 210
Open Systems Interconnect (OSI) reference model, 175
operating systems
installation, 145–146
operating systems, considerations for server installation, 3
Operating System Shutdown function (Guest Integration Services), 147
organizational units. *See* OUs
OSI (Open Systems Interconnect) reference model, 175
OUs (organizational units), AD DS management, 295–309
creating OUs, 296–298
using OUs to assign Group Policy settings, 298
using OUs to delegate AD management tasks, 298–300
Outbound Rules list, Windows Firewall with Advanced Security console, 364

P

Packaged App Rules node, AppLocker, 353
Parameter Request List extension, DHCP, 219
parent partition, 133
Parity storage layout option, 54
partitions, 133
partition style, disks, 43–44
pass-through disks, 163–164
path rules, 348–349, 353
PCL (printer control language), 94
Perform A Quick Format option, Configuring the Format Partition page, 59
permission inheritance, 80
permissions
assigning, 77–86
advanced NTFS permissions, 85
allowing/denying permission, 79–80
basic and advanced permissions, 78–79
basic NTFS permissions, 83–85
combining share permissions with NTFS permissions, 85–86
effective access, 80–81
inherited permissions, 80
NTFS authorization, 83
setting share permissions, 81–83
Windows permission architecture, 77–78
Permissions page (Delegation of Control Wizard), 299
physical disks

configuring local storage, 47–48
physical operating system environment (POSE) installation, 4
planning
IP transitions, 211–214
server installation, 2–6
installation requirements, 5–6
selecting Windows Server 2012 R2 edition, 3
server licensing, 5
supporting server roles, 3–4
supporting server virtualization, 4–5
server storage, 41–43
Pointer (PTR) resource records, 245
policies
Group Policy security policies, 328–342
defining local policies, 328–333
local users and groups, 336–339
security templates, 333–336
User Account Control, 339–342
Group Policy software restriction policies, 345–354
AppLocker, 352–354
configuring properties, 349–352
configuring rules, 347–349
enforcing restrictions, 346–347
using multiple rules, 349
Port Mirroring Mode (advanced network adapter feature), 185
port numbers, 358
POSE (physical operating system environment) installation, 4
postinstallation tasks
configuring servers, 18–25
command-line tools, 20–21
converting between GUI and Server Core, 21–22
GUI tools, 19–20
NIC teaming, 22–26
PowerShell, Windows, 277
creating computer objects, 288
creating single AD DS users, 281
creating user objects, 285
Preboot eXecution Environment (PXE), 184, 226–227
Predefined Rules parameter (New Inbound Rule Wizard), 366
Preferred DNS Server option, manual configuration of IPv4 addresses, 204
preparing
server upgrades, 12–14
Prerequisites Check page (AD DS Configuration Wizard), 262
primary zones, DNS servers, 242
Print and Document Services role, 106–110
adding print servers, 107–108
deploying printers with Group Policy, 109–110
viewing printers, 108–109
print clients, 95
print device, defined, 93
printer control language (PCL), 94
printer drivers
defined, 93
managing, 101
printer pools, creating, 105
printers
defined, 93
deploying with Group Policy, 109–110
installation, 94
management, 104–106
managing, 108
viewing, 108–109
printer sharing, 99–103
advanced printing configurations, 99
configuring printer security, 102–103
locally attached printer sharing, 95–96
managing printer drivers, 101
network-attached printer sharing, 98–99
network attached printing, 96–98
remote access Easy Print, 101–102
Print Management console, 106
Print Operators group, 292
print queue, 94
print queue window, 103
Print Server option (Select Role Services page), 106
print servers
adding, 107–108
defined, 93
deploying, 92–99
understanding Windows printing, 93–94
Windows print architecture, 93
Windows print flexibility, 94–99
managing, 108
print services, configuring, 92–110
deploying print servers, 92–99
understanding Windows printing, 93–94
Windows print architecture, 93
Windows print flexibility, 94–99
document management, 103–104

managing printers, 104–106
Print And Document Services role, 106–110
adding print servers, 107–108
deploying printers with Group Policy, 109–110
viewing printers, 108–109
sharing printers, 99–103
configuring printer security, 102–103
managing printer drivers, 101
remote access Easy Print, 101–102
private IPv4 addressing, 201
Private virtual switches, 178
privileges
delegating printer privileges, 37
Profile parameter
New Connection Security Rule Wizard, 368
New Inbound Rule Wizard, 366
Program parameter (New Inbound Rule Wizard), 365
properties
configuring software restriction properties, 349–352
Properties sheet
policy setting, 330
Properties sheets, AD Administrative Center/Users and Computers consoles, 288–289
Properties tile (Server Manager), 19–20
property-specific permissions, 299
Protocol And Ports parameter (New Inbound Rule Wizard), 366
protocol numbers, 358
-ProvisioningTypeDefault option (New-StoragePool cmdlet), 53
PTR (Pointer) resource records, 245
public IPv4 addressing, 201
publisher rules, 353
PXE (Preboot eXecution Environment), 226–227
PXE (Preboot eXecution Environment), 184

Q

QoS (Quality of Service), virtual hard disks, 166–167
Quality of Service (QoS), virtual hard disks, 166–167
queries
DNS, 238–239

R

RAID-5 volumes
configuring local storage, 60–62
disks, 46
Readeraid, 134
Read Only Domain Controller (RODC) domain controllers, 261
Rebinding (T2) time value extension, DHCP, 219
recursive queries, DNS, 238
referrals, DNS, 238–239
ReFS file system, 46
relay agents, DHCP, 227–230
remote access
Easy Print, 101–102
Remote Desktop Session Host role service, 101
Remote Server Administration tools, 121–122
remote server management
configuring servers, 112–122
Remote Server Administration tools, 121–122
Server Manager, 113–121
working with remote servers, 122
remote servers, 122
Remove Features page (Server Manager), 21–22
-Remove flag, 11
Remove Roles And Features Wizard, 10, 271
removing
domain controllers, 271–272
Server Graphical Shell feature, 10
renewal process, DHCP IP addresses, 221–223
Renewal (T1) time value extension, DHCP, 219
replication, 268
Requested IP Address extension, DHCP, 219
Requirements parameter (New Connection Security Rule Wizard), 368
reservations, DHCP servers, 225–226
-ResiliencySettingsNameDefault option (New-StoragePool cmdlet), 53
resolvers, DNS, 233
resource access, AD DS users, 276
resource metering, 152–153
resource records, DNS servers, 245–248
Restart The Destination Server Automatically If Desired function, 259
Restricted Groups policies, creating, 306
Reverse Lookup Zone Name page (New Zone Wizard), 247
reverse name resolution, DNS, 240–241
-rmmbr <members> command-line parameter, 308
RODC (Read Only Domain Controller) domain controllers, 261

roles
adding, Server Manager tool, 29–33
configuring
file and share access, 71–89
print and document srevices, 92–110
servers for remote management, 112–122
considerations for server installation, 3–4
deploying to VHDs, 34–35
Hyper-V Server, 134–135
Root Hints, configuring, 248–249
Root Hints tab (DNS server Proeprties sheet), 248–249
Router (Default Gateway) page (New Scope Wizard), 223–224
Routing And Remote Access console, 228
Routing And Remote Access Server Setup Wizard, 228
Rule Type parameter
New Connection Security Rule Wizard, 368
New Inbound Rule Wizard, 365

S

sales channels, server licensing, 5
SAM account name attribute, 280, 283
-samid <SAMName> command-line parameter, 305
SAM (Security Account Manager), 336
SANs (storage area networks), 167–172
Fibre Channel, 169–170
virtual machines to SANs, 170–172
Schema Admins group, 270
SCM (Security Compliance Manager) tool, 334
SCONFIG interface, 135
scope
DHCP servers, 222–224
IPv6 addresses, 206
-scope l|g|u command-line parameter, 305, 307
Scope parameter (New Inbound Rule Wizard), 366
scripting model, DSC, 38
Script Rules node, AppLocker, 353
SCSI disks, 144
SCSI (Small Computer Systems Interface) controllers, 156
-secgrp yes|no command-line parameter, 304, 307
secondary zones, DNS servers, 243
secure desktop, configuring User Account Control, 341
security
AD DS
authentication and authorization, 276
Group Policy security policies, 328–342
defining local policies, 328–333
local users and groups, 336–339
security templates, 333–336
User Account Control, 339–342
Group Policy software restriction policies, 345–354
AppLocker, 352–354
configuring properties, 349–352
configuring rules, 347–349
enforcing restrictions, 346–347
using multiple rules, 349
printers, 102–103
Security Account Manager (SAM), 336
Security Compliance Manager (SCM) tool, 334
security filtering, Group Policy Management Console, 321–322
security identifiers (SIDs), 83
Security Levels folder (Software Restriction Policies node), 345
Security Options node, GPOs, 332–333
security-related groups, 301
security templates, 333–336
creating, 335
importing into GPOs, 335–336
Security Template snap-in, 334
settings, 335
Security Templates snap-in, 334
Select A Domain From The Forest dialog box, 263
Select Destination Server page (Add Roles and Features Wizard), 30–31, 35
Select Disks page (New Volume Wizard), 61
Select Features page (Add Roles and Features Wizard), 32
Select GPO dialog box, 321
Select Installation Type page (Add Roles and Features Wizard), 29
Select Physical Disks For the Storage Pool page (New Storage Pool Wizard), 51
Select Print Server dialog box, 107
Select Server Roles page (Add Roles and Features Wizard), 31–32
Select The Profile For This Share page (New Share Wizard), 73–74
Select The Server And Storage Pool page (Server Manager), 53
Select The Storage Layout page (Server Manager), 53–54
Select Users dialog box, 339

self-allocation, assigning IPv6 addresses, 208–209
server caching
DNS, 236–238
Server Core
installing AD DS on, 266–268
Server Core installation option, 6–9
Server Core interface
Hyper-V Server, 135
Server for NFS role service, 73
Server Graphical Shell feature, removing, 10
server groups, creating, 120–121
Server Identifier extension, DHCP, 219
Server Manager, 26–35
adding roles and features, 29–33
adding servers, 26–29
deploying roles to VHDs, 34–35
remote management, 113–121
adding servers, 113–114
creating server groups, 120–121
down-level servers, 118–120
non-domain joined servers, 115–116
Windows Server 2012 R2 servers, 115–118
Server Message Blocks (SMB), 73
Server Operators group, 292
servers
adding, Server Manager, 113–114
adding, Server Manager tool, 26–29
configuring, 18–37
delegating server administration, 37
DSC (Desired State Configuration), 37–38
postinstallation tasks, 18–25
remote management, 112–122
Server Manager tool, 26–35
services, 36–37
DHCP, 222–227
configuring DHCP options, 224–225
creating a scope, 222–224
creating reservations, 225–226
PXE, 226–227
DNS, 241–248
configuring settings, 247–248
creating zones, 242–245
resource records, 245–248
installation, 2–15
Features on Demand, 10–11
migrating roles, 14–15
Minimal Server Interface, 9–10
planning installation, 2–6
Server Core, 6–9
upgrades, 12–15
print servers, 92–99
adding, 107–108
understanding Windows printing, 93–94
Windows print architecture, 93
Windows print flexibility, 94–99
SAN connections, 168–172
services
configuring servers, 36–37
Services tile (Server Manager), 36
setting
printer priorities, 104–106
share permissions, 81–83
settings
disks, 43–46
disk types, 44–45
partition style, 43–44
volumes, 45–46
VMs (virtual machines), 131–155
Hyper-V implementations, 133–136
Hyper-V Manager, 138–154
installing Hyper-V, 136–138
resource metering, 152–153
virtualization architectures, 132–133
Settings dialog box, new virtual machines, 143–144
Setup program, Compatability Report page, 13
Set-VMMemory cmdlet, 152
Shadow Copies dialog box, 86
share access, files
configuring, 71–89
folder shares, 72–77
NTFS quotas, 87–88
permissions, 77–86
Volume Shadow Copies, 86–87
Work Folders, 89
share permissions, 77, 81–83
Share Permissions tab (shared folders), 81
sharing folders, 72–77
sharing printers, 99–103
advanced printing configurations, 99
configuring printer security, 102–103
locally attached printer sharing, 95–96
managing printer drivers, 101
network-attached printer sharing, 98–99
network attached printing, 96–98
remote access Easy Print, 101–102
Shrink function (Edit Virtual Hard Disk Wizard), 165

SIDs (security identifiers), 83
Simple storage layout option, 54
simple volumes
  disks, 45
Single-Root I/O Virtualization (hardware acceleration setting), 185
single users, AD DS, 278–282
Small Computer Systems Interface (SCSI) controllers, 156
smart paging, 152–153
Smart Paging File Location settings, 152
SMB (Server Message Blocks), 73
SMB Share-Advanced option (File Share Profile list), 74
SMB Share-Applications option (File Share Profile list), 74
SMB Share-Quick option (File Share Profile list), 74
snap-ins
  Group Policy Object Editor, 324
  Local Users and Groups, 337–339
  Security Templates, 334
  Windows Firewall with Advanced Security, 363–368
snapshots, 165
SOA (Start of Authority) resource records, 245
SOA (Start Of Authority) tab (DNS server Properties sheet), 237–238
software restriction policies (GP), 345–354
  AppLocker, 352–354
  configuring restriction properties, 349–352
  configuring rules, 347–349
  enforcing restrictions, 346–347
Software Settings subnode, 323
spanned volumes
  configuring local storage, 60–62
  disks, 45
special permissions, 78
Specify An Alternate Source Path function, 259
Specify A Storage Pool Name and Subsystem page (New Storage Pool Wizard), 50–51
Specify Generation page (New Virtual Machine Wizard), 144
Specify The Provisioning Type page (Server Manager), 54
Specify The Size Of The Virtual Disk page (Server Manager), 55–56
Specify The Virtual Disk Name page (Server Manager), 53
Specify Volume Size page (New Simple Volume Wizard), 57
spooler (print queue), 94
Standard edition, 3
  Hyper-V licensing, 134
  support for Hyper-V, 4
standard permissions, 78
starter GPOs, 319, 322
Start of Authority (SOA) resource records, 245
Start Of Authority (SOA) tab (DNS server Properties sheet), 237–238
Startup RAM setting, Dynamic Memory, 151
stateless IPv6 address autoconfiguration, 208–209
states, Features on Demand, 11
Static MAC Address (advanced network adapter feature), 185
static teaming, 22
storage
  configuring local storage, 41–63
    disks, 46–63
    disk settings, 43–46
    planning storage needs, 41–43
  virtual machines, 156–173
    checkpoints, 165–166
    connecting to a SAN, 167–172
    modifying virtual disks, 164–165
    pass-through disks, 163–164
    QoS (Quality of Service), 166–167
    virtual disk formats, 156–157
    virtual disks, 157–163
storage area networks (SANs), 167–172
  Fibre Channel, 169–170
  virtual machines to SANs, 170–172
storage pools
  configuring local storage, 50–53
Storage Pools tile (Server Manager), 50
Storage Services role, 73
Storage Spaces, 42–43
striped volumes
  configuring local storage, 60–62
  disks, 45
stub zones, DNS servers, 243
subdomains of in-addr.arpa domain, 240–241
Subnet ID, IP addresses, 210
subnet mask, IP addresses, 198
Subnet Mask option, manual configuration of IPv4 addresses, 204
subnetting
  IPv4 addressing, 201–202
  IPv6 addresses, 210–211

Subtractive permission management task, 79
supernetting, IPv4 addressing, 202–203
Switch Dependent Mode, NIC teaming, 22
switches, virtual, 175–181
  creating a new switch, 177–179
  default virtual switches, 175–176
  MAC addresses, 179–180
Switch Independent Mode, NIC teaming, 22
sync shares, 89
synthetic adapters, 183–184
System Properties sheets, 289

T

Tasks To Delegate page (Delegation of Control Wizard), 299
TCP (Transmission Control Protocol) ports, 96
telephoneNumber attribute, 283
Teredo, IP transitioning, 214
TFTP (Trivial File Transfer Protocol), 227
Thin Provisioning Type option, 55
Time Synchronization function (Guest Integration Services), 147
time to live (TTL), 237
Transmission Control Protocol (TCP) ports, 96
Trivial File Transfer Protocol (TFTP), 227
Trusted Publishers properties, 351–352
TTL (time to live), 237
tunneling, IP transitioning, 212–213
two-level subnet option, subnetting IPv6 addresses, 210
Type II virtualization, 132
Type I virtualization, 133

U

UAC (User Account Control), Group Policy security, 339–342
UEFI boot, 144
Unicast transmissions, IPv6 addressing, 206
uninstalling features, Remove Features page, 21–22
Uninstall-WindowsFeature cmdlet, 11
unique local unicast addresses, IPv6, 207
universal groups, AD DS, 302
Unrestricted approach, enforcing restrictions, 346
upgrade paths, servers, 12
upgrades
  servers, 12–15
    preparing to upgrade, 12–14
    upgrade paths, 12
upgrading
  AD DS, 269–270
  Guest Integration Services, 147–148
USB-connected printers, 99
Use An Existing Virtual Hard Disk option, Connect Virtual Hard Disk page, 158
User Account Control Settings dialog box, 342
User Account Control (UAC), Group Policy security, 339–342
User Accounts control panel, configuring local users, 336–337
user objects, AD DS, 276–285
  creating
    multiple users, 283–285
    single users, 278–282
    user templates, 282–283
userPrincipalName attribute, 283
user rights
  local security policies, 331–333
user rights, assigning, 292
User Rights Assignment settings, 331–333
users
  AD DS, 276–293
    Active Directory objects, 288–293
    creating user objects, 276–285
  Group Policy security policies, 336–339
User-specific Group Policy layer, 324
user templates, AD DS, 282–283

V

Validation Results dialog box, 271
variable length subnet masking (VLSM), 200
VHDs (virtual hard disks)
  creating and mounting, 48–50
  deploying roles to, 34–35
VHDX image files, 157
viewing
  printers, 108–109
View Results page
  New Storage Pool Wizard, 52
  Server Manager, 56
virtual disks

configuring local storage, 53–57
creating, 157–163
formats, 156–157
modifying, 164–165
pass-through disks, 163–164
QoS (Quality of Service), 166–167
Virtual Hard Disk Format options, 49
virtual hard disks (VHDs)
creating and mounting, 48–50
deploying roles to, 34–36
Virtual Hard Disk Type options, 49
virtualization
considerations for server installation, 4–5
virtualization architectures, 132–133
Virtualization Service Client (VSC), 183
Virtualization Service Provider (VSP), 183
Virtual Machine Migration page (Add Roles and Features Wizard), 137–138
virtual machine monitor (VMM), 131
virtual machines. *See* VMs
virtual network adapters, 181–185
advanced network adapter features, 185
emulated adapters, 183–184
hardware acceleration settings, 184–185
synthetic adapters, 183–184
virtual networks
creating and configuring, 174–188
configurations, 188–189
NIC teaming, 185–188
virtual network adapters, 181–185
virtual switches, 175–181
virtual operating system environment (VOSE) installation, 4
virtual switches, 175–181
creating a new switch, 177–179
default virtual switches, 175–176
MAC addresses, 179–180
Virtual Switch Manager dialog box, 177
Virtual Switch Properties page, 179
Virtual Switch Properties settings, NIC team switch, 187
VLSM (variable length subnet masking), 200
VMBus, 183
VMM (virtual machine monitor), 131
VMs
connecting to SANs, 170–172
creating and configuring settings, 131–155
Hyper-V implementations, 133–136
Hyper-V Manager, 138–154
installing Hyper-V, 136–138
resource metering, 152–153
virtualization architectures, 132–133
creating and configuring storage, 156–173
checkpoints, 165–166
connecting to a SAN, 167–172
modifying virtual disks, 164–165
pass-through disks, 163–164
QoS (Quality of Service), 166–167
virtual disk formats, 156–157
virtual disks, 157–163
Volume Label option, Configuring the Format Partition page, 59
volumes
configuring local storage, 56–62
disks, 45–46
Volume Shadow Copies, 86–87
VOSE (virtual operating system environment) installation, 4
VSC (Virtualization Service Client), 183
VSP (Virtualization Service Provider), 183

W

windows
NIC Teaming, 23
Windows Azure
Infrastructure as a Service (IaaS), 270–271
Windows Firewall, 357–368
configuring, 116–118
control panel applet, 359–363
settings, 357–358
Windows Firewall With Advanced Security snap-in, 363–368
Windows Firewall With Advanced Security snap-in, 363–368
Windows Installer Rules node, AppLocker, 353
Windows PowerShell, 277
creating computer objects, 288
creating single AD DS users, 281
creating user objects, 285
installing AD DS on Server Core, 266–268
Windows Remote Management (HTTP-In) rules, 119
Windows Server 2012 R2 servers
managing, 115–118
Windows Settings subnode, 323
WinRM

configuring, 116–117
WINS Servers page (New Scope Wizard), 224
wizards
Active Directory Domain Services Configuration, 259
Active Directory Domain Services Installation, 259
Add Printer, 99
Add Roles And Features
Create Virtual Switches page, 137
Virtual Machine Migration page, 137–138
Automatically Generate Rules, 354
Configure Remote Access Getting Started, 228
Copy Object-User, 282
Delegation of Control, 298
Edit Virtual Hard Disk, 164–165
New Connection Security Rule, 367
New Inbound (or Outbound) Rule, 365
New Object - Computer, 287
New Object - User, 279
New Scope, 223
configuring DHCP options, 224–225
New Share, 73–74
New Simple Volume, 57
New Storage Pool, 50
New Virtual Machine
Configure Networking page, 140
Connect Virtual Hard Disk page, 141–142, 157
Specify Generation page, 144
New Zone, 244
Remove Roles And Features, 10, 271
Routing And Remote Access Server Setup, 228
Work Folders, configuring, 89
World Wide Node Names (WWNNs), 170–171
World Wide Port Names (WWPNs), 170–171
WWNNs (World Wide Node Names), 170–171
WWPNs (World Wide Port Names), 170–171

X

XD (eXecute Disable), 136

Z

zones, DNS servers, 242–245