Contents

Introduction ix
Microsoft certifications x
Acknowledgments x
Errata, updates, & book support xi
We want to hear from you xi
Stay in touch xi

Preparing for the Exam xii

Chapter 1 Install and configure servers 1
Objective 1.1: Install servers .................................................. 1
Minimum hardware requirements 2
Features on Demand 2
Objective summary 5
Objective review 6

Objective 1.2: Configure servers ........................................ 7
Installing roles and features 7
Converting a server with a GUI to or from Server Core 20
Minimal Server Interface 22
NIC teaming 24
Objective summary 28
Objective review 29

Objective 1.3: Configure local storage ................................. 30
Introducing Storage Spaces 30
Objective summary 37
Objective review 38

Answers .......................................................... 40

What do you think of this book? We want to hear from you!
Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/
Chapter 2  Configure server roles and features  45

Objective 2.1: Configure servers for remote management ................. 45
  Managing multiple servers with Server Manager  46
  Using Group Policy to enable remote management  57
Objective summary  60
Objective review  61

Answers .......................................................... 64

Chapter 3  Configure Hyper-V  67

Objective 3.1: Create and configure virtual machine settings .......... 67
  Hyper-V Module in Windows PowerShell  68
  Generation 1 and generation 2 virtual machines  69
  Enhanced session mode  72
  Dynamic Memory  74
  Resource Metering  77
  Non-uniform memory access (NUMA)  79
  RemoteFX  79
Objective summary  80
Objective review  81

Objective 3.2: Create and configure virtual machine storage .......... 82
  New VHDX disk format  82
  Virtual Fibre Channel adapter  86
  Storage Quality of Service (QoS)  88
Objective summary  89
Objective review  89

Objective 3.3: Create and configure virtual networks .................. 90
  Virtual switch extensions  91
  Network isolation  93
  Single-root I/O virtualization (SR-IOV)  95
  Bandwidth management  97
  Advanced features for virtual network adapters  99
Objective summary  100
Objective review  100

Answers .......................................................... 103
Chapter 4  Install and administer Active Directory 107
Objective 4.1: Install domain controllers .................................................. 107
  Installing domain controllers in the GUI 108
  Installing domain controllers with Windows PowerShell 113
  Install from Media (IFM) option without defragmentation 119
  Installing a domain controller in Windows Azure 120
Objective summary 127
Objective review 128
Answers .................................................................................................... 131

Chapter 5  Deploy, manage, and maintain servers 133
Objective 5.1: Monitor servers ..................................................................... 133
  Virtual machine resource pools 134
  Monitoring servers through Windows PowerShell 136
  Reviewing older monitoring features 137
Objective summary 139
Objective review 139
Answers .................................................................................................... 141

Chapter 6  Configure network services and access 143
Objective 6.1: Configure DirectAccess .......................................................... 143
  What is DirectAccess? 144
  Understanding IPv6 and DirectAccess 144
  Understanding the DirectAccess connection process 146
  Understanding DirectAccess infrastructure options 147
  Installing and configuring DirectAccess 153
Objective summary 170
Objective review 171
Answers .................................................................................................... 174

Chapter 7  Configure a network policy server infrastructure 177
Objective 7.1: Configure Network Access Protection .................................... 177
  How NAP works 178
  Configuring NAP 181
  SHV multi-configuration 183
Objective summary 188
## Objective review

### Chapter 8 Configure and manage Active Directory

#### Objective 8.1: Configure domain controllers
- Cloning domain controllers

#### Objective 8.2: Maintain Active Directory
- Restoring deleted objects in Active Directory

## Answers

### Chapter 9 Configure and manage Group Policy

#### Objective 9.1: Configure Group Policy processing
- Remote Group Policy update
- Windows PowerShell cmdlets for Group Policy

### Chapter 10 Configure and manage high availability

#### Objective 10.1: Configure failover clustering
- Cluster storage pools
- Cluster shared volumes (CSVs)
- Virtual hard disk sharing for guest clusters in Windows Server 2012 R2
- Dynamic quorum
- Dynamic witness in Windows Server 2012 R2
- Node drain
- Cluster-aware updating (CAU)
- Active Directory-Detached Clusters in Windows Server 2012 R2
- Configuring Cluster Properties in Windows PowerShell
Objective 10.2: Manage failover clustering roles

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a Scale-Out File Server (SoFS)</td>
<td>251</td>
</tr>
<tr>
<td>Assign role startup priority</td>
<td>253</td>
</tr>
<tr>
<td>Virtual machine application monitoring</td>
<td>254</td>
</tr>
<tr>
<td>Objective summary</td>
<td>259</td>
</tr>
<tr>
<td>Objective review</td>
<td>259</td>
</tr>
</tbody>
</table>

Objective 10.3: Manage virtual machine (VM) movement

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Live migration</td>
<td>261</td>
</tr>
<tr>
<td>Storage migration</td>
<td>274</td>
</tr>
<tr>
<td>VM network health protection in Windows Server 2012 R2</td>
<td>276</td>
</tr>
<tr>
<td>Objective summary</td>
<td>278</td>
</tr>
<tr>
<td>Objective review</td>
<td>278</td>
</tr>
</tbody>
</table>

Answers

Chapter 11 Configure file and storage solutions

<table>
<thead>
<tr>
<th>Objective 11.1: Implement Dynamic Access Control</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to Dynamic Access Control</td>
<td>286</td>
</tr>
<tr>
<td>Configuring claims-based authentication</td>
<td>287</td>
</tr>
<tr>
<td>Configuring file classification</td>
<td>291</td>
</tr>
<tr>
<td>Configuring access policies</td>
<td>302</td>
</tr>
<tr>
<td>Objective summary</td>
<td>307</td>
</tr>
<tr>
<td>Objective review</td>
<td>308</td>
</tr>
</tbody>
</table>

Answers

Chapter 12 Implement business continuity and disaster recovery

<table>
<thead>
<tr>
<th>Objective 12.1: Configure and manage backups</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate requirements for Windows Azure Backup</td>
<td>314</td>
</tr>
<tr>
<td>Performing Windows Azure Backups in Windows PowerShell</td>
<td>324</td>
</tr>
<tr>
<td>Objective summary</td>
<td>326</td>
</tr>
<tr>
<td>Objective review</td>
<td>327</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Objective 12.2: Configure site-level fault tolerance</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Hyper-V physical host servers</td>
<td>330</td>
</tr>
<tr>
<td>Configuring VMs</td>
<td>333</td>
</tr>
<tr>
<td>Performing Hyper-V Replica failover</td>
<td>342</td>
</tr>
<tr>
<td>Extending replication to a third site in Windows Server 2012 R2</td>
<td>347</td>
</tr>
<tr>
<td>Using Hyper-V Replica in a failover cluster</td>
<td>348</td>
</tr>
</tbody>
</table>
Chapter 13 Configure network services

Objective 13.1: Deploy and manage IPAM

What is IPAM?
Installing and configuring IPAM
Managing address space
Role-based access control for IPAM in Windows Server 2012 R2

Answers.

Chapter 14 Configure identity and access solutions

Objective 14.1: Implement Active Directory Federation Services (AD FS)

AD FS scenarios
How AD FS Works
Active Directory Federation Server Configuration Wizard
AD FS management console
Workplace Join
Windows PowerShell cmdlets for AD FS

Answers.
This book is written for IT professionals who want to earn the MCSA: Windows Server 2012 certification by passing the Microsoft exam “Exam 70-417: Upgrading Your Skills to MCSA Windows Server 2012.” Note that in January 2014, this exam was updated to cover the recent technology updates in Windows Server 2012 R2.

Exam 70-417 serves as a path to the Windows Server 2012 MCSA for those who have already earned the Windows Server 2008 certification that is named “MCITP: Server Administrator” and “MCSA: Windows Server 2008.” The book is therefore written specifically for IT professionals who have already earned this Windows Server 2008 certification and maintain the associated level of expertise in Windows Server 2008 or Windows Server 2008 R2.

Exam 70-417 also serves as an upgrade path to the Windows Server 2012 MCSA from certifications other than the Windows Server 2008 MCSA. These other certifications include MCITP: Virtualization Administrator, MCITP: Enterprise Messaging Administrator, MCITP: Lync Server Administrator, MCITP: SharePoint Administrator, and MCITP: Enterprise Desktop Administrator certifications. However, the assumed knowledge for readers of this book is only MCSA-level expertise in Windows Server 2008 or Windows Server 2008 R2.

One of the first things you need to understand about the 70-417 exam is that it is a condensed version of three other exams: Exam 70-410, Exam 70-411, and Exam 70-412. This set of three exams allows you to earn the Windows Server 2012 MCSA from scratch, without any prior certification. Together, these three exams include 18 domains of broader skills and 62 more specific objectives. Because the exams are intended for individuals who haven't yet earned Windows Server certification, the exams test new features in Windows Server 2012 as well as older features that haven't changed since Windows Server 2008 or even earlier.

On the 70-417 exam, only 14 of the original 18 domains and 22 of the original 62 objectives have been adopted from these three source exams. This smaller subset of material corresponds generally to the new features in Windows Server 2012. Approximately 75 percent of the questions on the 70-417 exam will assess your knowledge of new Windows Server 2012 features in some way. Approximately 25 percent of the questions will be “review” questions about features that have not changed since Windows Server 2008—questions you could have seen when you earned your existing certification. The questions that comprise this 25 percent can be taken from any of the 62 original objectives on exams 70-410, 70-411, or 70-412.

In order to create a book that is a manageable study tool, we've focused on covering the 75 percent of material that is new to Windows Server 2012 and that forms the core of the 70-417 exam. After all, the remaining 25 percent of what's covered on the exam draws upon the knowledge you already have already demonstrated when you earned your Windows Server 2008 certification. However, it's possible you will need to review some of these older topics,
so we’ve provided guidance throughout the book to help you identify any topics that might require further review.

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 for us 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 the book to find more information—and then take the time to research and study the topic. Valuable 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-premise and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

**MORE INFO ALL MICROSOFT CERTIFICATIONS**


**Acknowledgments**

I’d like to thank Anne Hamilton and Karen Szall at Microsoft for their long-standing support; Travis Jones, Adnan Ijaz, and Osama Sajid at Microsoft for answering low-level questions about Remote Management; Jeff Riley at Box Twelve Communications for his steady management and flexibility; and Mitch Tulloch and Brian Svidergol for their world-class technical review.
Errata, updates, & book support

We’ve made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

http://aka.ms/ER417R2

If you discover an error that is not already listed, please submit it to us at 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 and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to http://support.microsoft.com.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority and your feedback is 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.
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 kit 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.

Note that this training kit is based on publically available information about the exam and the author's experience. To safeguard the integrity of the exam, authors do not have access to the live exam.
This page intentionally left blank
CHAPTER 3

Configure Hyper-V

If you were to name the one server role that has seen the most changes between Windows Server 2008 R2 and Windows Server 2012, you’d have to say Hyper-V. To begin with, Hyper-V now has its own Windows PowerShell module, so the role is completely manageable at the Windows PowerShell prompt. Beyond this new command-line manageability, there are new improvements in memory configuration, storage, Resource Metering, security, extensibility, and other areas (such as fault tolerance) that aren’t even covered in this domain.

In Windows Server 2012 R2, the changes from the first release of Windows Server 2012 are more incremental but still significant. One highly visible change is that “snapshots” are now called “checkpoints,” so don’t be surprised when you see that word on the exam. Other important new features in Windows Server 2012 R2 Hyper-V include enhanced session mode, which improves the usability of VMs, and generation 2 VMs, which offer improved installation and startup times.

The good news is that none of these new features is particularly difficult to understand, at least at the level they will be tested on for the 70-417 exam. Your studying efforts in this area should therefore pay off well.

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

Of the features mentioned by Microsoft in the description of this exam objective, three are at least partially new to Windows Server 2012 (Dynamic Memory, Smart Paging, and Resource Metering) and two are new to Windows Server 2012 R2 (generation 2 virtual machines and enhanced session mode). A sixth topic, RemoteFX, was introduced in Windows Server 2008 R2 but has only recently been added to the objectives.

Beyond learning about these six topics, though, you should also know that all new and old settings in Hyper-V can now be configured at the Windows PowerShell prompt. From
that perspective, every virtual machine setting is new; any configuration option could be covered on the exam. You should be sure, therefore, to supplement your study of the new features in Windows Server 2012 and Windows Server 2012 R2 Hyper-V with a review of the new cmdlets related to virtual machine (VM) configuration in the Hyper-V module.

**This section covers the following topics:**
- Hyper-V module in Windows PowerShell
- Generation 1 and generation 2 virtual machines
- Enhanced session mode
- Dynamic Memory
- Smart Paging
- Resource Metering
- Non-uniform memory access (NUMA) topology
- RemoteFX

**Hyper-V Module in Windows PowerShell**

As you've already learned, Windows PowerShell in Windows Server 2012 and Windows Server 2012 R2 includes a new module called Hyper-V that provides a command-line administration interface for almost all VM settings. It's uncertain how many cmdlets will appear on the 70-417 exam, and there are too many of them (more than 150) to document here.

Instead, you can use Get-Command to review the names of these cmdlets so that you can at least recognize the most important ones. You can sort the output by the cmdlet nouns to make it easier to understand. (The noun portion of a cmdlet represents the object that is configured.)

For example, to see a list of all cmdlets in the module and group them by cmdlet noun, type the following:

```
Get-Command -Module Hyper-V | Sort Noun,Verb
```

If you want to see cmdlets that contain the string *VM* (and are likely to relate specifically to VM management and configuration), type the following:

```
Get-Command *VM* | Sort Noun,Verb
```

To further filter your results, you can use the wildcard character twice or more, as in the following example:

```
Get-Command *VM*adapter* | Sort Noun,Verb
```

You can then use Update-Help and Get-Help, optionally with the –Examples or –Full option, to get the latest documentation about any particular cmdlet that interests you.
Generation 1 and generation 2 virtual machines

Beginning with Windows Server 2012 R2, the New Virtual Machine Wizard now includes a Specify Generation page, shown in Figure 3–1.

![New Virtual Machine Wizard](image)

**FIGURE 3-1** Choosing the generation of a new VM

The concept of a VM generation is new to Windows Server 2012 R2, and you'll likely see one or more questions about this topic on the 70-417 exam. Generation 1 VMs, as they are now called, are the familiar VMs that have existed in all versions of Hyper-V since it was first introduced. Generation 2 VMs are a new option available only when the host system is running Windows Server 2012 R2.

Here are the changes in generation 2 VMs that you need to understand:

- **Removal of legacy emulated hardware devices**  Generation 1 VMs emulate a set of legacy hardware devices, including two IDE controllers, two COM ports, and a floppy disk drive. These emulated devices have been removed from generation 2 VMs. The advantage of removing support for emulated devices is faster boot times (by about 20 percent) and faster installations (by about 50 percent).

  Figure 3-2 and Figure 3-3 show the difference in the number of default hardware devices in generation 1 and 2 virtual machines. Each figure displays the complete list of hardware devices in a default VM of each generation.
Configure Hyper-V

FIGURE 3-2 Default hardware devices for a generation 1 VM

The generation 2 VM lacks both IDE controllers, COM ports, and the diskette drive.

FIGURE 3-3 Default hardware devices for a generation 2 VM

- **UEFI vs. BIOS**  Generation 1 VMs use Basic Input Output System (BIOS) as a firmware interface to initiate the boot process and begin loading the operating system. Generation 2 VMs use Unified Extensible Firmware Interface (UEFI) for the same purpose. The main advantage of UEFI is that it allows Secure Boot, an option that you can enable on the Firmware page of a VM’s settings, as shown in Figure 3-4. Secure Boot ensures that no malicious code is installed beneath the operating system and that the UEFI has not been altered from an approved version.
Objective 3.1: Create and configure virtual machine settings

CHAPTER 3

71

FIGURE 3-4 Enabling Secure Boot on a generation 2 VM

- **SCSI boot**  In generation 1 VMs, you can boot from IDE devices only. In generation 2 VMs, there are no IDE controllers, and you can boot from SCSI devices, including ISO files.

- **PXE boot-compatible network adapters**  In generation 1 VMs, only legacy network adapters are PXE-boot compatible. In generation 2 VMs, there are no more legacy network adapters, and normal network adapters are PXE-boot compatible.

- **Limited operating system support**  Generation 2 VMs support only the following guest operating systems:
  - Windows 8 (64-bit)
  - Windows Server 2012
  - Windows 8.1 (64-bit)
  - Windows Server 2012 R2

- **No RemoteFX support**  Generation 2 VMs do not support RemoteFX.

- **No Physical CD/DVD support**  Generation 2 VMs do not support physical CDs or DVDs. You must use ISO files instead.

- **No VHD support**  Generation 2 VMs do not support VHD files. You must use VHDX files. (The VM’s operating system must also be installed originally on a VHDX file, not on a VHDX that has been converted from VHD.)

- **No virtual floppy disk support**  Generation 2 VMs do not support VFD files.

**EXAM TIP**

To perform a network boot on a VM from a PXE-compatible adapter, select BIOS in a generation 1 VM’s settings, and Firmware in a generation 2 VM’s settings. Then adjust the Startup Order (for BIOS) or the Boot Order (for Firmware) so that the desired adapter is listed at the top.
Enhanced session mode

Enhanced session mode is a new feature in Windows Server 2012 R2 that improves the connectivity between a guest operating system and the host operating system. In short, enhanced session mode provides the VM connection window with most of the benefits of a Remote Desktop connection window, including the ability to copy and paste between the host operating system desktop and the guest VM.

Enhanced session mode isn’t enabled by default, and it’s available only when the guest is running Windows 8.1 or Windows Server 2012 R2. To enable enhanced session mode, you have to enable two options in Hyper-V Settings of the host computer: First, as shown in Figure 3-5, navigate to Enhanced Session Mode Policy in the Server menu on the left and then select Allow Enhanced Session Mode in the right pane. Second, as shown in Figure 3-6, navigate to Enhanced Session Mode in the User menu on the left and then select Use Enhanced Session Mode.
After you enable these two options, your next VM connection to a Hyper-V guest running Windows 8.1 or Windows Server 2012 R2 will open the window shown in Figure 3-7.

Clicking the down arrow next to Show Options reveals a Local Resources tab, which is similar to the tab of the same name available in a Remote Desktop Connection window. By default, remote audio on the VM is configured to be played on the host operating system, and the local printers and Clipboard data are shared through the VM connection. (The Clipboard allows copying and pasting between the host and guest machines.) Smart card readers in the host operating system are also redirected to the VM by default.
You can also use the Local Resources tab to configure the following resources in the VM connection window:

- **Drives**  Makes local drives on the host operating system available from within the VM. Drives can be selected individually
- **Other Supported Plug and Play (PnP) Devices**  Redirects PnP devices on the host, such as USB drives to the VM

**Dynamic Memory**

Dynamic Memory was introduced in Windows Server 2008 R2 Service Pack 1. Just one new configuration setting (Minimum RAM) has been added in Windows Server 2012 and Windows Server 2012 R2, but you should be prepared to be tested on any or all of the feature’s settings on the 70-417 exam.

If you haven’t had the chance to learn about this feature, remember the following point: Dynamic Memory pools the available RAM on a Hyper-V host for all running VMs for which Dynamic Memory is enabled. Using this pool, Dynamic Memory automatically modifies on the fly the amount of RAM assigned to each running VM as the need increases or decreases. The biggest benefit of Dynamic Memory is that it allows you to use your RAM resources in a highly efficient manner, dramatically increasing the number of VMs you can run on that Hyper-V host. (Marketing materials talk about the benefit Dynamic Memory offers in “improving consolidation ratios” on your virtualization servers. It’s good to know that phrase because you might find it on the exam.)

The second most important concept you need to remember about Dynamic Memory is that starting a VM often requires more memory than does running the VM after it starts, and dynamic RAM assignment in Windows Server 2012 naturally mirrors these changing needs. If, for example, you have 6 GB of RAM on a server and try to start 10 VMs at once, you might get an error message regardless of whether Dynamic Memory is enabled. However, only if Dynamic Memory is enabled might you be able to get them all up and running if you start them one at a time. The prototypical example that illustrates low memory usage after startup is with virtual desktop infrastructure (VDI), where you might have a pool of unused virtual machines available in case several people happen to need a desktop all at once. (If you see a scenario on the exam about VDI and desktop pools, expect Dynamic Memory to play a part in the solution somehow.)

Now let’s take a look at Dynamic Memory settings. They appear where you’d expect, which is in the Memory section of a VM’s settings in Hyper-V Manager, as shown in Figure 3-8. You also can enable and configure Dynamic Memory with Windows PowerShell by using the Set-VM cmdlet, which can be used to configure the various properties of a VM. Note that you can enable or disable Dynamic Memory only when the VM is in a stopped state. (Dynamic Memory does *not* mean you can manually adjust RAM settings while a VM is running.)
Objective 3.1: Create and configure virtual machine settings

CHAPTER 3

FIGURE 3-8 Configuring Dynamic Memory settings

The settings here affect how memory is assigned dynamically. You need to understand the implications of these settings on behavior and performance.

- **Startup RAM**  This value existed before Windows Server 2012, but it used to have a slightly different meaning. Before Windows Server 2012, the Startup RAM was both the amount of RAM used at startup and the minimum amount of RAM ever assigned to the VM.

  In Windows Server 2012 and Windows Server 2012 R2, the Startup RAM setting is now only the amount of RAM assigned at startup and is no longer the minimum RAM. If a running VM uses less RAM after startup, some of that RAM can now be reclaimed by other running VMs.

  Here is another important point to remember about Startup RAM: The more RAM you assign to a VM when it starts up, the faster it will be able to start up (of course). But don’t forget the flip side: If you set this level too high, you might temporarily (during startup) deprive other VMs of the RAM they need to perform at an acceptable level.

- **Minimum RAM**  This is the only new setting that has been added in Windows Server 2012 and Windows Server 2012 R2, so make sure you understand it. If you have enabled Dynamic Memory on a VM running on a Windows Server 2012 or Windows Server 2012 R2 host, by default this value is the same as the Startup RAM value. However, you can lower Minimum RAM to allow the amount of RAM allocated to the VM to decrease after startup.
Why would you want to manually lower the Minimum RAM level? One reason is that by allowing unused physical memory of a running VM to be reclaimed, you can make sure that physical memory is available to other VMs that might need it. On the other hand, by keeping the value higher, you can ensure that enough is available to the same VM when it restarts.

- **Maximum RAM**  This is the maximum amount of memory that can ever be dynamically assigned to the VM. There’s always a balancing act here. If you don’t set this value high enough, the VM’s performance could suffer. However, for a RAM-intensive workload, setting this value too high could deprive other VMs of needed RAM.

- **Memory Buffer**  This is the preferred amount of extra RAM (defined as a percentage) that is assigned to the system beyond what is determined to be needed to run the active workload at any given point. The default is set at 20 percent. You don’t normally have to change this setting, but if memory usage spikes intermittently on a VM, you might want to increase this percentage to help ensure that enough RAM is available when needed.

- **Memory Weight**  This parameter determines how available memory on the host is allocated among the different VMs running on the host. If you want to prioritize the performance and memory allocation of a given VM relative to other VMs, you would raise the memory weight setting on that VM.

**NOTE**  To review and configure Dynamic Memory settings in Windows PowerShell, use Get-VMMemory and Set-VMMemory.

**Smart Paging**

What if, with Dynamic Memory enabled, you have just enough RAM to start your VMs but not enough to restart a particular VM once they are all up and running? Maybe, for example, you used the last 256 MB of available RAM to start a VM running Microsoft Windows XP, and now you can’t restart a VM running Windows 8, which requires 512 MB of RAM to start. To prevent this kind of scenario from happening, Hyper-V in Windows Server 2012 and Windows Server 2012 R2 introduces a new feature called Smart Paging. **Smart Paging** allows a VM that’s being restarted to use disk resources temporarily on the host as a source for any additional memory needed to restart a VM. Then, once the VM has started successfully and its memory requirements decrease, Smart Paging releases the disk resources. The downside of Smart Paging, as you probably have guessed, is that performance is compromised. VMs restart, but slowly, with Smart Paging.

To minimize the performance impact of Smart Paging, Hyper-V uses it only when all of the following are true:

- The VM is being restarted.
- There is no available physical memory.
- No memory can be reclaimed from other VMs running on the host.

Smart Paging is **not** used in the following cases:
- A VM is being started from an “off state” (instead of a restart).
- Oversubscribing memory for a running VM is required.
- A VM is failing over in Hyper-V clusters.

Smart Paging is a new feature that is specifically mentioned in the objectives for the 70-417 exam, so don’t be surprised if it appears as an important element in a test question. With this in mind, be aware that the only configuration option for Smart Paging relates to the storage location for the Smart Paging file. Why would the location of the Smart Paging file ever matter in a test question? Well, if the disk on which the Smart Paging file is stored nears its capacity, there might not be enough disk space to allow a VM to restart. If this happens, the way to solve the problem would be to move the Smart Paging file to a disk with more space. (That’s assuming you can’t add more RAM to the host server, of course.)

**EXAM TIP**

If you create a checkpoint (formerly called a snapshot) of a live VM, the checkpoint will save the running memory. If you create a checkpoint of a stopped VM, no data in RAM needs to be saved. Therefore, if you want to reduce the size of your checkpoint file, shut down the VM before creating the checkpoint.

**Resource Metering**

Resource Metering is a new feature of Windows Server 2012 and Windows Server 2012 R2 that is designed to make it easy to build tools that measure VM usage of CPU, memory, disk space, and network. This feature was primarily designed for hosting VMs for a customer. In such a scenario, you need to know how much of your computing resources are used so that you can charge the customer accordingly.

You can use Resource Metering in Windows Server 2012 and Windows Server 2012 R2 to collect and report on historical resource usage of the following seven metrics:
- Average CPU usage by a VM
- Average physical memory usage by a VM
- Minimum physical memory usage by a VM
- Maximum physical memory usage by a VM
- Maximum amount of disk space allocated to a VM
- Total incoming network traffic for a virtual network adapter
- Total outgoing network traffic for a virtual network adapter

You can view this functionality in Windows PowerShell even though it is intended to be used primarily with additional tools.

To enable Resource Metering on a VM, use the `Enable-VMResourceMetering` cmdlet on the host server. For example, to enable Resource Metering on a VM named VSrv1, type the following at a Windows PowerShell prompt:

```
Enable-VMResourceMetering -VMName VSrv1
```
At this point, the Resource Metering counters start running. To view all Resource Metering statistics on the VM since you ran the last command, use the Measure-VM cmdlet. For example, type the following to display the Resource Metering data on VSrv1 for all seven metrics:

```powershell
Measure-VM -VMName VSrv1
```

Alternatively, you could save the usage statistics into a report with this command:

```powershell
$UtilizationReport = Get-VM VSrv1 | Measure-VM
```

You could then display the contents of the report at a later time with the following command:

```powershell
Write-Output $UtilizationReport
```

To reset the counters to start counting usage again from zero, you use the following command:

```powershell
Reset-VMResourceMetering -VMName VSrv1
```

To stop the counters from running on VSrv1, type the following:

```powershell
Disable-VMResourceMetering -VMName VSrv1
```

These metrics can be collected even when the VMs are moved between hosts using live migration or when their storage is moved using storage migration.

For the 70-417 exam, what’s most important to remember about Resource Metering is that it allows you to measure CPU, memory, disk, and network usage on a particular VM. You should also know the general steps required to configure Resource Metering, but you won’t have to know the specific syntax used in Windows PowerShell cmdlets.

**NOTE** If you want to measure Internet traffic as opposed to network traffic in general, you can use network metering port access control lists (ACLs), which are described later in this chapter.

**EXAM TIP**

Remember that Resource Metering doesn’t let you measure current resource usage. You can, however, use Task Manager to view current CPU and memory usage for individual VMs. To do so, open a Virtual Machine Connection to each VM, and then view the Processes tab in Task Manager. Each VM will appear as a separate instance of Virtual Machine Connection along with the current CPU and memory usage for that VM.

You can also use counters in Performance Monitor on the host server to track VM resource usage over time. For example, to measure CPU usage in one or more particular VMs, use the Hyper-V Hypervisor Virtual Processor counter set. To measure Dynamic RAM usage in on or more particular VMs, use the Hyper-V Dynamic Memory VM counter set.
Non-uniform memory access (NUMA)

Non-uniform memory access (NUMA) is a new configuration node beneath the Processor node in a VM’s settings. NUMA is a technology that improves system scalability by optimizing memory and memory bus usage in multi-processor systems. In Windows Server 2012 and Windows Server 2012 R2, VMs are NUMA-aware, which means that multi-processor VMs can access memory resources in a more optimal and scalable way. Generally speaking, you don’t need to change the default settings in the NUMA topology configuration area because they are automatically configured correctly based on the host server’s hardware. On rare occasions, however, it might be necessary to modify these settings if you have moved a VM between two physical hosts with different NUMA topologies. Configuring these settings is beyond the scope of the 70-417 exam, but you should know that the Use Hardware Topology button resets NUMA settings to the default settings.

**EXAM TIP**

Be sure to review VM settings that have not changed since Windows Server 2008. For example, you should know that Integration Services enable VM features such as time synchronization, host-backup awareness, and system shutdown awareness. Also review VM settings such as Resource Control, which allows you to prioritize CPU resources for certain VMs.

RemoteFX

RemoteFX is a set of technologies that improves video rendering, graphics, and overall user experience over the RDP protocol. RemoteFX can work only if a RemoteFX-compatible graphics processing unit (GPU) is available on the remote server to which clients are connecting over RDP.

RemoteFX can be used with Hyper-V. In this case, clients connect to remote VMs over RDP. All VMs on a physical host can share the GPU of that host, and each VM is configured with a virtual GPU (vGPU) that points to the physical GPU.

Here are the requirements for running RemoteFX with Hyper-V:

- Windows Server 2008 R2 SP1 or later
- DX11 vGPU with WDDM v1.2 driver
- SLAT-capable processor
- Remote Desktop Virtualization Host component of the Remote Desktop Services role must be installed (to enable RemoteFX vGPU)
- GPU or GPUs must be enabled for use with RemoteFX in Hyper-V Settings
- VMs must have the “RemoteFX 3D Video Adapter” hardware component added
- VMs must be generation 1


**Objective summary**

- In Windows Server 2012 and Windows Server 2012 R2, almost all VM settings can be configured in Windows PowerShell.
- Windows Server 2012 R2 introduces the option to create generation 2 virtual machines. Generation 2 virtual machines drop support for legacy hardware devices, but they boot faster and perform operating system installations faster. Generation 2 VMs also allow the option for Secure Boot, which ensures that no malicious software is installed beneath the operating system.
- Enhanced session mode is a new feature in Windows Server 2012 R2. It provides a VM connection with many of the benefits of a Remote Desktop connection, including the ability to share features with the host operating system such as printers, Clipboard data, and drives.
- Dynamic Memory pools all the memory available on a host server for all VMs hosted on that server. Because computers tend to use more memory when they are starting than when they are running, Dynamic Memory allows you to use available RAM much more efficiently.
- Important Dynamic Memory settings include Startup RAM, Minimum RAM, and Maximum RAM.
- Smart Paging allows VMs to use virtual (paged) memory to complete a restart operation when insufficient physical memory is available.
- RemoteFX improves graphics over RDP and can be used with Hyper-V to improve Remote Desktop connections to individual VMs. The physical host requires a compatible GPU, and you have to select this GPU in Hyper-V Settings and enable it for RemoteFX. You then need to add a RemoteFX 3D Video Adapter in each chosen VM. RemoteFX is not compatible with generation 2 VMs.
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 the chapter.

1. A server named HYPV1 is running Windows Server 2012 R2 and has been configured with the Hyper-V role. HYPV1 has 20 GB of RAM and is hosting 12 VMs. All VMs are running Windows Server 2012 R2 and have Dynamic Memory enabled.

One of the VMs hosted on HYPV1 is named VM1. VM1 is hosting a web application. VM1 averages five concurrent user connections to this web application and its performance is considered acceptable by users.

VM1 has the following memory settings:

- Startup Memory: 1024 MB
- Minimum Memory: 384 MB
- Maximum Memory: 4096 MB
- Memory Weight: Medium

You need to perform a scheduled restart of VM1 once per week. You have noticed during past scheduled restarts of VM1 that restarts have sometimes occurred only with the help of Smart Paging and have required several minutes to complete. You want to minimize downtime associated with restarting VM1 and reduce the likelihood that any restart operation will rely on Smart Paging. What should you do?

A. Increase the Startup Memory on VM1.
B. Increase the Minimum Memory setting on VM1.
C. Decrease the Maximum Memory on other VMs.
D. Change the Memory Weight setting on VM1 to High.

2. A server named HYPV2 is running Windows Server 2012 R2 and has been configured with the Hyper-V role. HYPV2 has 16 GB of RAM and is hosting 10 VMs. All VMs are running Windows Server 2012 R2 and have Dynamic Memory enabled.

One of the VMs on HYPV2 is named VM2. VM2 hosts a little-used application that is used for testing only and is not used for any other purposes. You attempt to restart VM2 but receive an error message indicating that there is insufficient memory to perform the operation.

You want to restart VM2 successfully. What should you do? (Choose all that apply.)

A. Increase the Startup Memory setting on VM2.
B. Decrease the Maximum Memory on other VMs.
C. Increase the Memory Buffer % setting on VM2.
D. Move the Smart Paging file to a disk with more space.
3. A server named HYPV3 is running Windows Server 2012 R2 and has been configured with the Hyper-V role. HYPV3 hosts a VM named VM3. You have been measuring the CPU, memory, network, and disk space usage of VM3 for the past 24 hours. You would now like to display the collected usage data at the Windows PowerShell prompt.

Which of the following commands should you type at an elevated Windows PowerShell prompt?

A. Enable-VMResourceMetering -VMName VM3  
B. Disable-VMResourceMetering -VMName VM3  
C. Measure-VM -VMName VM3  
D. $UtilizationReport = Get-VM VSrv1 | Measure-VM

**Objective 3.2: Create and configure virtual machine storage**

There are three topics in this objective that are most likely to be tested: VHDX, virtual Fibre Channel, and storage Quality of Service (QoS). Of these three, VHDX is the one feature you’re pretty much guaranteed to see on the 70-417 exam. Fortunately, though, all three topics are easy to understand.

This section covers the following topics:
- New VHDX disk format
- Virtual Fibre Channel adapter
- Storage Quality of Service (QoS)

**New VHDX disk format**

Virtual hard disk (VHD) files have a size limit of 2 TB, which can prevent you from virtualizing some workloads such as extra-large databases. To fix this problem, Windows Server 2012 and Windows Server 2012 R2 introduce a new VHDX file format, which has a 64 TB limit.

Size is the biggest advantage of the VHDX, so if it appears in a test question, it will most likely be in the context of a scenario in which you need to support files that are larger than 2 TB. What is the disadvantage of VHDX? Backward compatibility. If you need to migrate storage to servers running Windows Server 2008 R2 or earlier, use VHD. Also note that the larger
size of VHDX applies only to non-boot volumes. VHDX boot disks are also limited to 2 TB because of limitations found in the legacy AMI BIOS used in Hyper-V virtual machines.

Remember that VHDX is the default selection for a new VHD file, as shown in Figure 3-9, but you can opt to create a VHD just as easily.

![FIGURE 3-9 Creating a new VHDX](image)

You can also convert a disk from a VHDX to a VHD and vice versa, as long as the disk isn’t bigger than 2 TB. To do so, just select the virtual disk in the VM settings and click Edit, as shown in Figure 3-10.

**EXAM TIP**

Aside from Hyper-V Manager, you can also use Computer Management or the New-VHD cmdlet to create a new VHD or VHDX. (Note that New-VirtualDisk is different: That cmdlet is used to create a new virtual disk in a specific storage pool.) To convert a virtual hard disk between the VHD and VHDX formats in Windows PowerShell, use the Convert-VHD cmdlet.
EXAM TIP

Remember the purpose of the Physical Hard Disk option shown in Figure 3-10. This option is often called a “pass-through disk” and has been available since Windows Server 2008. With a pass-through disk, you add a physical disk (as opposed to a VHD or VHDX) to a VM. As stated in the description of the feature in Figure 3-10, you need to take a physical disk offline before you can attach it to a VM as a pass-through disk.

Then, in the Edit Virtual Hard Disk Wizard, choose the Convert option, shown in Figure 3-11.
Figure 3-11 Converting a virtual hard disk to VHD or VHDX

**NOTE** To convert a VHD to a VHDX file in Windows PowerShell, use the `Convert-VHD` cmdlet.

Although size is the biggest advantage of a VHDX, it isn’t the only advantage. VHDX files also offer the following benefits:

- Improved resiliency from power failure, thanks to a new disk log.
- Support for new low-cost storage options thanks to 4 KB sector disks.
- Better performance thanks to large block sizes.
- Support for user-defined file metadata. You could use metadata, for example, to include information about the service pack level of the guest operating system on the VM.

Any of these advantages could appear as requirements in a scenario question, so be sure to remember them.

Virtual Fibre Channel adapter

Before Windows Server 2012, you could provision storage from a Fibre Channel storage area network (SAN) and then use that storage in a guest VM. However, you had to prepare everything in the host operating system so that the source of the storage was transparent to the guest.

What’s new in Windows Server 2012 and later is that you can create a Fibre Channel adapter for your VM and then provision storage from your Fibre Channel SAN from within the guest operating system. This might be useful, for example, if you want to migrate to a virtual environment application that is already connected to specific logical unit numbers (LUNs) in your Fibre Channel SAN. Another advantage of the Fibre Channel adapter is that it allows you to cluster guest operating systems to provide high availability for VMs.

To configure virtual Fibre Channel, first use the Virtual SAN Manager option in the Actions pane of Hyper-V Manager to create a new virtual Fibre Channel SAN. Virtual Fibre Channel SANs are connected to one or more physical host bus adapters (HBAs). Then add a new Fibre Channel adapter to the VM. To add a new Fibre Channel adapter to a VM, first open the settings of the VM and select Add Hardware from the menu on the left. Lastly, select Fibre Channel Adapter and click Add, as shown in Figure 3-12.

![Figure 3-12 Adding a new virtual Fibre Channel adapter](image-url)
EXAM TIP

To configure a VM to connect to a Fibre Channel SAN, first create a virtual Fibre Channel SAN that connects to one or more physical HBAs.

You configure virtual Fibre Channel adapter settings by specifying a virtual SAN. Port addresses are supplied automatically, but you can edit them by clicking Edit Addresses. The port addresses include hexadecimal values representing the World Wide Node Name (WWNN) and World Wide Port Name (WWPN), as shown in Figure 3-13.

FIGURE 3-13 Configuring Fibre Channel settings

The Fibre Channel adapter in Hyper-V includes a few limitations you need to be aware of. First, the drivers for your HBAs must support virtual Fibre Channel. Second, you can’t use virtual Fibre Channel to connect to boot media for your VMs. Finally, you can’t use the Fibre Channel adapter with just any guest operating system. The guest has to be running Windows Server 2008 or later.
Storage Quality of Service (QoS)

Storage Quality of Service (QoS) is a new feature in Windows Server 2012 R2 that allows you to define a minimum and maximum level of I/O throughput for a virtual disk in Hyper-V. The throughput is defined as an input/output per second (IOPS) value, where each IO is considered to be 8 KB of data. The IOPS limits you set apply only to an individual disk, not to a VM in general.

To configure storage QoS, open the settings of a VM, expand the desired virtual disk in the Hardware menu on the left and then select Advanced Features. In the Advanced Features configuration area on the right, click Enable Quality Of Service Management, and then define a minimum and maximum level for the IOPS. You may leave one value set to zero to accept the system defaults. (Note that the minimum setting does not ensure that this minimum IOPS will be met. The minimum value merely defines a threshold that will trigger an event-based notification.)

Figure 3-14 shows the configuration settings for storage QoS.

![Figure 3-14 Configuring storage QoS settings](image-url)
Why would you need to define storage QoS? One potential application would be to honor different levels of service-level agreements (SLAs) for different clients or for different areas of your organization. For example, your organization might provide three levels of service to clients corresponding to three different ranges of IOPS.


Objective summary

- Windows Server 2012 and Windows Server 2012 R2 introduce VHDX files, which have a 64 TB size limit. (VHD files have a 2 TB limit.) Other advantages of the VHDX file format are improved resiliency from power failures, user-defined metadata, and better performance.
- You can convert a VHD to a VHDX and vice versa.
- Hyper-V in Windows Server 2012 and Windows Server 2012 R2 allows you to create virtual Fibre Channel adapters for virtual machines. If you have a Fibre Channel SAN and compatible HBA drivers, you can then provision SAN storage from within a guest VM.
- Storage Quality of Service (QoS) is a new feature in Windows Server 2012 R2 that allows you to define an acceptable range of IOPS for a selected virtual disk in Hyper-V. Each IO is defined as 8 KB.

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 the chapter.

1. You have a VHD that is stored on a server running Windows Server 2012 R2. The VHD is 1.5 TB in size and stores a rapidly growing database file that is 1.0 TB. You want to provide at least 4 TB of space for the database file. What should you do?
   
   A. Use the Edit Virtual Hard Disk Wizard and choose the Convert option.
   B. Use the Edit Virtual Hard Disk Wizard and choose the Expand option.
   C. Move the contents of the VHD to a new dynamically expanding disk.
   D. Move the contents of the VHD to a new differencing disk.
2. You work as a network administrator for Fabrikam.com. Fabrikam.com has a server room that includes 20 servers, 10 of which are virtualized on a server named HYPV4 running Windows Server 2012 R2.

The Fabrikam.com office recently experienced a power outage. After the power outage, the universal power supply connected to HYPV4 did not gracefully shut down HYPV4 or its 10 hosted virtual servers. Some VHDs were corrupted, which required you to restore the VHDs from backup, resulting in a loss of data.

You want to help ensure that future power outages do not corrupt data on your virtualized servers. What should you do?

A. Configure NIC teaming for every VM.
B. Convert the VHDs on your VMs to VHDX files.
C. Create Fibre Channel adapters for each VM and move the VHDs to shared storage.
D. Enable data deduplication on HYPV4.

3. You work as a network administrator for Fabrikam.com. One of your servers, named HYPV5, is running Windows Server 2012 R2 and has been configured with the Hyper-V role. HYPV5 hosts five VMs running Windows Server 2008 R2.

You want to attach new VHDs to the VMs hosted on HYPV5 to increase storage space to these VMs. Until now, the VMs have relied on locally attached storage on HYPV5 to store VHDs attached to the VMs. However, adequate storage space is no longer available on HYPV5 for any new VHDs.

Your network includes a Fibre Channel SAN, from which HYPV5 can already provision storage. You want to provision new storage from the Fibre Channel SAN and use it for the new VMs, and you want to achieve this with the least amount of administrative effort. What should you do? (Choose all that apply.)

A. Upgrade the VM operating systems to Windows Server 2012 R2.
B. From within the host operating system, provision new storage from the SAN.
C. From within the guest operating system, provision new storage from the SAN.
D. Convert the VHD files to VHDX files.

Objective 3.3: Create and configure virtual networks

This objective covers the bulk of the new features in Windows Server 2012 and Windows Server 2012 R2 Hyper-V, but it’s unclear which of these many features will actually appear on the 70-417 exam. Some, such as virtual switch extensions, are difficult to write questions about for an exam on Windows Server, as opposed to System Center Virtual Machine Manager or Windows development. Others are almost too easy: They can’t be set up in a question without giving the answer away, as is the case with bandwidth management, DHCP guard, and router advertisement guard. Still others, such as port ACLs, are constrained by a relative
Virtual switch extensions

The “virtual networks” that appeared in the Windows Server 2008 and Windows Server 2008 R2 interface have been replaced in Windows Server 2012 and Windows Server 2012 R2 by elements called virtual switches. From an administration point of view, virtual networks appear simply to have been renamed. Network adapters now connect to virtual switches instead of virtual networks, and just like the old virtual networks, virtual switches can be external, internal, or private.

But there is more to virtual switches than meets the eye at first glance. One of the key innovations in Windows Server 2012 and Windows Server 2012 R2 Hyper-V is that the functionality of these new virtual switches can be expanded through extensions provided by Microsoft or independent software vendors. You add these new extensions as you would install any new software.

Windows Server 2012 and Windows Server 2012 R2 allow for the following kinds of virtual switch extensions:

- Capturing extensions, which can capture packets to monitor network traffic but cannot modify or drop packets
- Filtering extensions, which are like capturing extensions but also can inspect and drop packets
- Forwarding extensions, which allow you to modify packet routing and enable integration with your physical network infrastructure

Once installed, extensions are made available to all switches but are enabled and disabled on a per-switch basis. To manage installed extensions for a virtual switch, from the Actions pane in Hyper-V Manager, select Virtual Switch Manager, as shown in Figure 3-15.
FIGURE 3-15 Opening the new Virtual Switch Manager

Then, in the Virtual Switch Manager dialog box that opens, expand the desired switch and select Extensions, as shown in Figure 3-16. In the Switch Extensions box, you can enable, disable, and rearrange the order of installed extensions.

FIGURE 3-16 Managing virtual switch extensions
By default, each switch has two extensions: Microsoft NDIS Capture, which is disabled, and Microsoft Windows Filtering Platform, which is enabled.

You can also use PowerShell to create, delete, and configure extensible switches on Hyper-V hosts. Use the Get-VMSwitchExtension cmdlet to display details concerning the extensions installed on a specific switch. To see the full list of cmdlets available to manage virtual switches in general, type `Get-Command *VMSwitch*` at a Windows PowerShell prompt.

If any questions about virtual switch extensions appear on the 70-417 exam, they will most likely involve fictional or hypothetical extensions. One possible scenario could involve two extensions that you need to enable but that don’t work well together. If such a problem were to occur and you wanted the functionality of both extensions, you could create two separate virtual switches, with one of these extensions enabled on each. Then you could connect chosen VMs to the appropriate switch, as needed.

**NOTE**  To manage virtual switch extensions in Windows PowerShell, you can use `Enable-VMSwitchExtension`, `Disable-VMSwitchExtension`, and `Get-VMSwitchExtension` cmdlets. For a complete list, use `Get-Command` to search for the string `*VMSwitchExtension*`.

**Network isolation**

You can isolate VMs from unwanted network traffic by using the `Add-VMNetworkAdapterAcl` cmdlet in Windows PowerShell. The feature is sometimes called port ACLs in Microsoft documentation, but on the 70-417 exam, it’s possible you will see this feature mentioned only by its associated cmdlets.

Each port ACL is like a firewall rule that allows or denies traffic associated with a Media Access Control (MAC) or IP address. If you configure the port ACL on a Hyper-V host running Windows Server 2012 or later, it remains in effect even if you move the VM to another host server.

For example, to deny both inbound and outbound traffic between the remote address 192.168.9.111 and the VM named Server12, type the following at an elevated Windows PowerShell prompt on the Hyper-V host:

```
Add-VMNetworkAdapterAcl -VMName Server12 -RemoteIPAddress 192.168.9.111 -Direction Both -Action Deny
```
You can then review the effects of this last action by using the Get-VMNetworkAdapterACL cmdlet. The specific command for this example and its associated output would be as follows:

```
Get-VMNetworkAdapterACL -VMName Server12
VMName: Server12
VMId: eefb383d-5070-4a74-a16b-3e46a5d2b90c
AdapterName: Network Adapter
AdapterId: Microsoft:EEFB383D-5070-4A74-A16B-3E46A5D2B90C\C3F8188F-EF58-480E-A00F-36F55F6CDA52
Direction   Address         Action
-----------   -------         ------
Inbound      Remote 192.168.9.111   Deny
Outbound     Remote 192.168.9.111   Deny
```

To remove the port ACL and the associated traffic restriction, use the Remove-VMNetworkAdapterACL cmdlet. For instance, following our example, you would type the following:

```
Remove-VMNetworkAdapterACL -VMName Server12 -RemoteIPaddress 192.168.9.111 -Direction Both -Action Deny
```

### Resource Metering through port ACLs

You can use the same Add-VMNetworkAdapterAcl cmdlet to meter traffic to or from a specific address. To achieve this, use the Meter action instead of Allow or Deny, as in the following example:

```
Add-VMNetworkAdapterAcl -VMName Server12 -RemoteIPaddress 192.168.9.111 -Direction Both -Action Meter
```

You would then use the Get-VMNetworkAdapterACL cmdlet to view the metered usage. The following shows the command used with the same example and the associated output:

```
Get-VMNetworkAdapterACL -VMName Server12
VMName: Server12
VMId: eefb383d-5070-4a74-a16b-3e46a5d2b90c
AdapterName: Network Adapter
AdapterId: Microsoft:EEFB383D-5070-4A74-A16B-3E46A5D2B90C\C3F8188F-EF58-480E-A00F-36F55F6CDA52
Direction   Address         Action
-----------   -------         ------
Inbound      Remote 192.168.9.111   Meter (1 Mbytes)
Outbound     Remote 192.168.9.111   Meter (0 Mbytes)
```

Metering usage through port ACLs might seem like an obscure feature, but don’t be surprised if it shows up on an exam question. In a way, it’s actually a showcase feature of Windows Server 2012 and Windows Server 2012 R2 because it allows virtual hosting providers to meter Internet usage (traffic to the default gateway) specifically as opposed to network usage in general. Like the Resource Metering feature, this base functionality is intended to be leveraged through scripts and programs.
Single-root I/O virtualization (SR-IOV)

Single-root I/O virtualization (SR-IOV) is an extension to the PCI Express (PCIe) standard that can improve network performance. SR-IOV support in Hyper-V is new to Windows Server 2012 and Windows Server 2012 R2. In Hyper-V, SR-IOV enables network traffic to bypass the software switch layer of the Hyper-V virtualization stack and reduce I/O overhead. If you assign only SR-IOV–enabled virtual network adapters and switches to a VM, the network performance of the VM can be nearly as good as that of a physical machine. In addition, the processing overhead on the host is reduced.

To enable SR-IOV, you first need to create a new virtual switch. (You cannot enable SR-IOV on any existing switch, such as the default virtual switch.) In Hyper-V Manager, from the Actions pane, select Virtual Switch Manager. In the Virtual Switch Manager window that opens, choose the option to create a new external virtual switch. Then, in the Virtual Switch Properties pane, in the Connection Type area (shown in Figure 3-17), select the Enable Single-Root I/O Virtualization (SR-IOV) check box. Supply a Name and any Notes for the new virtual switch and then click OK.

---

**FIGURE 3-17** Enabling SR-IOV on a new virtual switch
NOTE To create a new switch enabled for SR-IOV in Windows PowerShell, use the `New-VMSwitch` cmdlet with the `-EnableIOV $True` parameter.

After you create an SR-IOV–enabled virtual switch, open the settings of the VM for which you want to enable the adapter for SR-IOV and connect the network adapter to the new virtual switch you have just created. Then expand the Network Adapter settings in the Hardware pane, select Hardware Acceleration, and select the Enable SR-IOV check box, shown in Figure 3-18.

![Figure 3-18 Enabling SR-IOV on a virtual network adapter](image)

Finally, depending on your hardware configuration, you might need to install drivers within the guest operating system to fully enable SR-IOV. You can check the status of SR-IOV by clicking the Networking tab for a particular VM in Hyper-V Manager. If SR-IOV is active, this information is displayed as shown in Figure 3-19.
Objective 3.3: Create and configure virtual networks  

CHAPTER 3  

97

EXAM TIP

Remember that single-root I/O virtualization improves network performance on a VM by allowing a VM's network traffic to bypass virtual switches.

MORE INFO  


Bandwidth management

Bandwidth management is a new feature in Windows Server 2012 and Windows Server 2012 R2 Hyper-V that lets you set both a minimum and maximum Mbps of throughput for any virtual network adapter. In Windows Server 2008 R2, you could configure a maximum bandwidth but not a minimum. Now you can configure both a minimum and maximum for each virtual network adapter.

You enable and configure bandwidth management on a virtual network adapter in the settings of a VM, as shown in Figure 3-20. For either the Minimum Bandwidth setting or the Maximum Bandwidth setting, configuring a value of 0 leaves that setting unrestricted.
You can also use the `Set-VMNetworkAdapter` to configure minimum and maximum bandwidth on a virtual network adapter. As an alternative to specifying a value for Mbps, you can use this cmdlet to specify a relative bandwidth weight between 0 and 100 relative to other virtual network adapters. To ensure that all virtual network adapters are ensured an equal minimum or maximum bandwidth, you can assign the same bandwidth weight to all adapters. For example, by specifying a bandwidth weight of 1 to all network adapters on servers named Srv1, Srv2, and Srv3, the following command ensures that the same minimum bandwidth is assigned to those network adapters:

```
Get-VMNetworkAdapter -VMName Srv1,Srv2,Srv3 | Set-VMNetworkAdapter -MinimumBandwidthWeight 1
```

**EXAM TIP**

Bandwidth management is not available as an option on legacy network adapters. Bandwidth management is available only on standard network adapters in Hyper-V.

Advanced features for virtual network adapters

A number of new features can be enabled for virtual network adapters in Hyper-V. These options appear when you select Advanced Features after you expand a Network Adapter in the Hardware menu, as shown in Figure 3-21. The new features in this area are defined next.

- **DHCP Guard**  Helps safeguard against Dynamic Host Configuration Protocol (DHCP) man-in-the-middle attacks by dropping DHCP server messages from unauthorized VMs pretending to be DHCP servers.

- **Router Guard**  Helps safeguard against unauthorized routers by dropping router advertisement and redirection messages from unauthorized VMs pretending to be routers.

- **Port Mirroring**  Enables monitoring of a VM’s network traffic by forwarding copies of destination or source packets to another VM being used for monitoring purposes.

- **NIC Teaming**  In Windows Server 2012 and Windows Server 2012 R2, the NIC teaming feature can be configured for virtual network adapters as well as for physical network adapters.

---

**FIGURE 3-21** Configuring advanced features for a virtual network adapter

---

**EXAM TIP**

You need to remember the names and functions of these four features for the 70-417 exam.
NOTE To configure settings for a virtual network adapter (including those for SR-IOV, bandwidth management, DHCP guard, router advertisement guard, port mirroring, and NIC teaming), use the Set-VMNetworkAdapter cmdlet. Use Get-Help to learn about the specific syntax used to configure each feature.

Objective summary

- The functionality of virtual networks in previous versions of Windows Server has been replaced by virtual switches in Windows Server 2012 and Windows Server 2012 R2. Virtual switch features can be enhanced or expanded through extensions, which can be managed in the Hyper-V Manager interface.
- Port ACLs are like firewall rules that allow or deny traffic to a VM based on MAC or IP address. You can also use a port ACL to meter traffic between a VM and a specific address.
- SR-IOV is a way to optimize network performance between a Hyper-V guest and a physical network. To configure SR-IOV, you must create a new virtual switch enabled for SR-IOV, connect a VM’s network adapter to that switch, and then enable SR-IOV on the adapter. You might also have to install drivers within the guest operating system.
- Windows Server 2012 and Windows Server 2012 R2 include many new configurable options for network adapters, such as bandwidth management, DHCP guard, router advertisement guard, port mirroring, and NIC teaming.

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 the chapter.

1. You work as a network administrator for Fabrikam.com. Fabrikam.com includes its own cloud infrastructure, which is used to provide virtual hosting services to external customers. Customer servers are hosted as VMs on your servers running Windows Server 2012 R2. You want to block all traffic to and from the customer virtual servers except for communication with the default gateway. Which of the following cmdlets should you use on the host servers to isolate the guest VMs?

   A. Add-VMNetworkAdapterACL
   B. Set-VMNetworkAdapterVLAN
   C. Set-VMSwitchExtensionPortFeature
   D. New-NetFirewallRule
2. You install the Hyper-V role on a server running Windows Server 2012 R2 and then create a new VM. You now want to optimize network performance for the VM by enabling SR-IOV. What should you do? (Choose all that apply.)
   A. Create a new private switch.
   B. Enable SR-IOV on the virtual switch.
   C. Create a new external switch.
   D. Enable SR-IOV on the virtual network adapter.

3. You want to maximize security on a VM and help prevent man-in-the-middle attacks. Which of the following settings will help achieve this goal? (Choose all that apply.)
   A. Enable MAC Spoofing
   B. DHCP Guard
   C. Router Guard
   D. Port Mirroring
**Thought experiment**

**Configuring Hyper-V at Fabrikam**

In this thought experiment, apply what you've learned about this objective. You can find answers to these questions in the “Answers” section.

You work as a network administrator for Fabrikam.com, a hosting provider that uses a private cloud infrastructure to provide virtual hosting services to external customers.

Your cloud infrastructure is composed of 20 physical servers running Windows Server 2012 R2 with the Hyper-V role installed. Customer servers are hosted as VMs on these physical servers. Each physical server is equipped with 64 GB of RAM. Shared storage is provided by a Fibre Channel SAN.

Your goals are to use your physical resources as efficiently as possible and to provide a high level of security and performance for customers.

1. You are working with an in-house developer to create a tool that measures CPU, disk, and Internet usage for each customer VM. The developer wants to know how to access this raw information in Windows Server 2012 R2 so that he can build a tool around it. Which method should you show the developer to retrieve the desired usage information?

2. A customer has a database application hosted in your cloud. The application is running in a VM that is running Windows Server 2008 R2 and SQL Server 2008. The database is stored on a VHD drive (stored on the host server) whose size is fixed at 2 TB, but it will soon outgrow the space available. How can you provide more storage space for the database application in a way that minimizes the effort required for all stakeholders?

3. Your IT department has purchased two virtual switch extensions from independent software vendors. The first switch extension is a filtering extension that enables customers to search incoming packets for specific strings or patterns that are useful for security or market research. The second switch extension is a forwarding extension that forwards all incoming traffic received on a switch to any chosen IP address.

You want to be able to use these extensions to provide customers with the ability to search packets on the wire without significantly degrading network performance for services hosted on the customer VM. How can you achieve this goal?
Answers

This section contains the answers to the Objective Reviews and the Thought Experiment.

Objective 3.1: Review

1. **Correct answer:** B

   A. **Incorrect:** Increasing the Startup Memory value will only increase the likelihood that Smart Paging will be used during startup.

   B. **Correct:** Increasing the Minimum Memory setting will help ensure that more physical memory remains allocated to VM1 when a restart begins.

   C. **Incorrect:** This isn’t the best option because it could deprive other important applications of needed RAM.

   D. **Incorrect:** This setting would prioritize memory allocation to VM1 when needed. It wouldn’t ensure that more memory is allocated to VM1 at the time of a restart operation.

2. **Correct answer:** D

   A. **Incorrect:** Increasing the Startup Memory setting would decrease the possibility that VM2 will be able to start successfully because it will require HYPV2 to find more RAM to allocate to the startup operation. In addition, the fact that Smart Paging is not helping VM2 start indicates most likely that the drive that stores the Smart Paging file has run out of space.

   B. **Incorrect:** Decreasing the Maximum Memory on other VMs would have an unpredictable effect on the availability of RAM for VM2 during a restart operation. In addition, the other running VMs might host high-priority applications that need the memory. Finally, the fact that Smart Paging is not helping VM2 start most likely indicates that the drive that stores the Smart Paging file has run out of space.

   C. **Incorrect:** Increasing the Memory Buffer % setting would allocate more RAM to VM2 while it is running and would likely make some more memory available at the time of a restart. However, VM2 hosts only low-priority applications that are rarely used. Allocating RAM to VM2 while it is running would deprive other VMs of the RAM they might need to support good performance in higher priority applications. In addition, the fact that Smart Paging is not helping VM2 start most likely indicates that the drive that stores the Smart Paging file has run out of space.

   D. **Correct:** Both the host server and the guest VM are running Windows Server 2012 R2, which supports Smart Paging. If insufficient RAM is available for a restart operation, the Smart Paging feature will normally rely on disk storage as virtual memory to help perform the restart. If a guest VM cannot restart in this scenario, it is most likely because not enough free space is available on the disk that currently stores the Smart Paging file.
3. **Correct answer:** C

   **A. Incorrect:** This command would enable Resource Metering on the VM. However, according to the question, Resource Metering is already enabled.

   **B. Incorrect:** This command would stop the metering of resources on VM3 but would not display any usage statistics.

   **C. Correct:** This command would display usage statistics on VM3 because Resource Metering was enabled or reset.

   **D. Incorrect:** This command would save the resource data into a stored variable, not display it on the screen.

**Objective 3.2: Review**

1. **Correct answer:** A

   **A. Correct:** VHDs have a size limit of 2 TB. The Convert option allows you to change the disk type to a VHDX, which has a size limit of 64 TB.

   **B. Incorrect:** VHDs have a size limit of 2 TB; you need a VHD file that is larger than 4 TB. Choosing the Expand option would allow you to expand the size of the VHD from 1.5 TB to 2.0 TB.

   **C. Incorrect:** Creating a dynamically expanding VHD would not allow you to move beyond the 2 TB limit for VHD files. You need to convert the disk to a VHDX file.

   **D. Incorrect:** Creating a differencing VHD would not allow you to move beyond the 2 TB limit for VHD files. You need to convert the disk to a VHDX file.

2. **Correct answer:** B

   **A. Incorrect:** NIC teaming will help ensure against network outages, but it will not help ensure against data corruption after a power failure.

   **B. Correct:** VHDX files—unlike VHD files—contain a log that helps these virtual disks avoid corruption resulting from a power outage.

   **C. Incorrect:** Moving the VHDs to shared storage will not make them more resilient to power outages.

   **D. Incorrect:** Data deduplication allows data to be stored more efficiently, but it doesn’t help prevent corruption from power outages.
3. Correct answer: B
   A. Incorrect: You don’t need to upgrade. You can currently provide new storage for the VMs simply by provisioning new storage for the host server. You would need to upgrade to Windows Server 2012 or later only if you needed to provision storage directly from the guest operating system.
   B. Correct: You can provision storage from the SAN in the host operating system running Windows Server 2012 R2. Then you can configure new volumes on the host server and then store new VHDs for the VMs on those new volumes.
   C. Incorrect: You don’t need to provision new storage from the SAN from the guest operating system. To do this would require you to upgrade the guest operating systems to Windows Server 2012 or later. You would then need to create and configure virtual Fibre Channel ports. This set of actions would not allow you to achieve your goal with the least amount of administrative effort.
   D. Incorrect: Converting the VHD files to VHDX files would require you to upgrade the guest operating systems to Windows Server 2012 or later. In addition, converting to VHDX would not help you attach more available storage to your VMs.

Objective 3.3: Review

1. Correct answer: A
   A. Correct: You can use Add-VMNetworkAdapterAcl to create a port ACL and allow or deny traffic between a VM and any specified addresses.
   B. Incorrect: This cmdlet allows you to associate a VLAN ID with a network adapter. It does not isolate network traffic in a way that would be useful in this specific scenario.
   C. Incorrect: This cmdlet allows you to configure a feature on a virtual network adapter. It doesn’t allow you to restrict network traffic in a way that would be helpful in this scenario.
   D. Incorrect: This cmdlet allows you to restrict traffic between any address and the host server, not the guest VMs.

2. Correct answers: B, C, D
   A. Incorrect: You can enable SR-IOV only on an external switch.
   B. Correct: You need to enable SR-IOV on a new external virtual switch.
   C. Correct: You can enable SR-IOV only on a new switch. The switch must be external.
   D. Correct: You need to enable SR-IOV on the virtual network adapter connected to the new virtual switch.
3. **Correct answers:** B, C

   A. **Incorrect:** MAC spoofing enables you to choose a MAC address manually. It doesn’t prevent man-in-the-middle attacks.

   B. **Correct:** DHCP guard prevents man-in-the-middle attacks from unauthorized VMs pretending to be legitimate DHCP servers.

   C. **Correct:** Router guard prevents man-in-the-middle attacks from unauthorized VMs pretending to be legitimate routers.

   D. **Incorrect:** Port mirroring is used to forward traffic to a remote VM. It is not used to prevent man-in-the-middle attacks.

**Thought experiment**

1. To measure CPU and disk usage, use the `Enable-VMResourceMetering`, `Measure-VM`, and `Reset-VMResourceMetering` cmdlets. To measure Internet usage, create a port ACL that measures traffic specifically between a VM and the default gateway by using the `Add-VMNetworkAdapterAcl` cmdlet with the –Meter action.

2. Back up the VHD. Convert the VHD to a VHDX. Expand the new VHDX to a desired size up to 64 TB. (Only the host needs to be running Windows Server 2012 or later to support VHDX files. You don’t need to upgrade the guest operating system to Windows Server 2012 or later.)

3. Enable only the forwarding extension on the virtual switch currently used by the services hosted on the VM. Create a second virtual switch that enables only the filtering extension.
Index

Numbers & Symbols
6to4 transition technology, 145
802.1x enforcement, 179

A
acceptance transform rules, 398
access control, role-based access control for IPAM (IP Address Management) in Windows Server 2012 R2, 381–382
access control lists (ACLs), 287
access-denied assistance, file classification, 300–301
Access-Denied Assistance tab (FSRM Options dialog box), 300
access policies, configuring, 302–307
   central access rules, 302–306
   deploying central access policies to file servers, 306–307
access rules, 286
ACLs (access control lists), 287
Active Directory
   cloning domain controllers, 193–200
      adding source controllers to Cloneable Domain Controllers group, 194–195
      exporting VMs, 199–200
      importing VMs, 199–200
      Get-ADDCCloningExcludedApplicationList cmdlet, 195–198
      New-ADDCCloneConfigFile cmdlet, 198–199
      prerequisites, 194
   installing domain controllers, 107–127
   restoring deleted objects, 202–209
   AD Administrative Center, 205–207
   deleted object lifetimes, 208
   enabling AD Recycle Bin, 204–205
Windows PowerShell, 207–208
   updating files, 293–294
   updating folders, 293–294
Active Directory Administrative Center, 205–207
Active Directory Certificate Services (AD CS), 389
Active Directory-detached clusters, 246–247
Active Directory Domain Services Configuration Wizard, installing domain controllers, 107–127
   GUI, 108–112
   IFM option, 119–120
   Windows Azure, 120–127
   Windows PowerShell, 113–118
Active Directory Federation Services. See AD FS (Active Directory Federation Services)
Active Directory Recycle Bin, 203–208
Active Directory Rights Management Services (AD RMS), 389
AD CS (Active Directory Certificate Services), 389
Add-ADDSReadOnlyDomainControllerAccount cmdlet, 113, 117
Add-ADGroupMember cmdlet, 195
Add Authorization Entry dialog box, 332–333
Add-DAAppServer cmdlet, 166
Add-DAClient cmdlet, 157
Add-KdsRootKey cmdlet, 394
/Add-Package option (DISM utility), 20
Add-PswaAuthorizationRule cmdlet, 17
Add Relying Party Trust Wizard, 398
Add-RemoteAccessLoadBalancerNode cmdlet, 152
Add Roles and Features Wizard, 9–12, 361
ADDS deployment module, 113
Add Servers option (Server Manager), 47
Add-VMFibreChannelHba cmdlet, 88
Add-VMNetworkAdapterAcl cmdlet, 93–94
AD FS (Active Directory Federation Services), 389–407
   authenticating users, 391–392
   Configuration Wizard, 392–394
AD FS Proxy

Implementing, 391
management console, 395–403
Authentication Policies node, 399–403
Service node, 395–397
Trust Relationships node, 397–399
scenarios, 390–391
Windows PowerShell cmdlets, 406–407
Workplace Join, 403–406
AD FS Proxy, 390
Adprep /domainprep, 112
Adprep /forestprep, 112
AD RMS (Active Directory Rights Management Services), 389
advanced configuration options
(DirectAccess), 167–168
Advanced Security Settings for Permissions dialog box, 304
affinity groups, 121–122
/All argument (DISM utility), 19
Allow Replication from Any Authenticated Server security option, 332
Allow Replication from the Specified Servers security option, 332
All Servers section (Server Manager), 49–51
All (Write) and Local (Read) mode, 248
application-consistent recovery points, 338
application monitoring, virtual machines, 254–260
Application Server Setup page, configuring DirectAccess, 166–167
assigning
role startup priority, 253
SHV configurations to health policies, 186–188
asynchronous GPO processing, 224–225
authenticating users, AD FS, 390–392
Authentication and Ports, Hyper-V Replica, 331
Authentication page (Remote Access Server Setup Wizard), 161
Authentication Policies node (AD FS management console), 399–403
global policies, 399–402
Per Relying Party Trust node, 402–403
Authorization and Storage, Hyper-V Replica, 332–334
Automatic allocation, storage pools, 34
automatic file classification, 295–300
automatic node drain on shutdown, 242

B
Backup-GPO cmdlet, 223
Back Up Now option (Windows Azure Backup), 321–322
Backup Operators group, 324
backups, 313–326
Back Up Now option, 321–322
bandwidth throttling, 322–324
certificate requirements, 314
creating online backup schedules, 318–321
creating backup vaults in management portals, 315–316
creating self-signed certificates with Makecert.exe utility, 314–315
downloading Windows Azure Backup Agent, 316–317
installing Windows Azure Backup Agent, 316–317
performing backups in Windows PowerShell, 324–326
recovering data, 322
registering servers, 317
uploading certificates, 316
bandwidth management, virtual networks, 97–98
bandwidth throttling, 322–324
Basic Input Output System (BIOS), 70
Before You Begin page (Add Roles And Features Wizard), 11
Behind an Edge Device option (Network Topology page), 160
Best Practices Analyzer section (Server Manager All Servers page), 50
bidirectional access (DirectAccess), 144
BIOS (Basic Input Output System), 70
blocks (IP addresses), adding to IPM databases, 373–374
bring-your-own-device (BYOD) trend, Workplace Join, 403
business continuity
backups, configuring, 313–326
Back Up Now option, 321–322
bandwidth throttling, 322–324
certificate requirements, 314
creating online backup schedules, 318–321
creating backup vaults in management portals, 315–316
creating self-signed certificates with Makecert.exe utility, 314–315
downloading Windows Azure Backup Agent, 316–317
installing Windows Azure Backup Agent, 316–317
performing backups in Windows PowerShell, 324–326
recovering data, 322
registering servers, 317
uploading certificates, 316
site-level fault tolerance, configuring, 329–351
extending replication to a third site, 347–348
Hyper-V physical host servers, 330–333
Hyper-V Replica failover, 342–346
Hyper-V Replica in failover clusters, 348–352
virtual machines, 333–342
BYOD (bring-your-own-device) trend, Workplace Join, 403
caching, Group Policy, 224–225
Cancel Failover (unplanned failovers), 344
capturing virtual switch extensions, 91
case-sensitive string expressions, 298
CAU (cluster-aware updating), 242–246
Central Access Policies Configuration dialog box, 306
central access rules, creating, 302–306 .cer files, 315
Certificate Authentication, 400
Certificate-Based Authentication (HTTPS), 331
certificate requirements, Windows Azure Backup, 314
certificates, SSL (Secure sockets Layer), 392–394
Certificate Services, 394
Certificates node (AD FS management console), 396–397
checkpoints, 77
Choose Initial Replication Method page (Enable Replication Wizard), 339
Choose Replication VHDs page (Enable Replication Wizard), 335
Claim Rule Language, 399
claims
authentication, configuring, 287–291
defined, 286–287
defining user types, 288–290
defining device types, 288–290
rules for relying party trusts, 398–399
Claims Description node (AD FS management console), 397
Claims Provider Trusts node (AD FS management console), 398
Classification Parameters dialog box, 298–299
classifications, defined, 286
Classification tab (files and folders), 294
Clear-EventLog cmdlet, 136
Client Experience settings (DirectAccess), 170
Client Setup Wizard, configuring DirectAccess, 156–159
Cloneable Domain Controllers group, adding source domain controllers to, 194–195
cloning domain controllers, 193–200
adding source controller to Cloneable Domain Controllers group, 194–195
exporting/importing the VM of the source domain controller, 199–200
Get-ADDCCloningExcludedApplicationList cmdlet, 195–198
New-ADDCCloneConfigFile cmdlet, 198–199
prerequisites, 194
cluster-aware updating (CAU), 242–246
Cluster-Aware Updating dialog box, 244–245
cluster properties, configuring, 248–249
Cluster Shared Volume File System (CSVFS), 236
class shared volumes (CSVs), 236–239
cmdlets
Add-ADDSReadOnlyDomainControllerAccount, 113, 117
Add-ADGroupMember, 195
Add-DAApplServer, 166
Add-DAClient, 157
Add-KdsRootKey, 394
Add-PswaAuthorizationRule, 17
Add-RemoteAccessLoadBalancerNode, 152
Add-VMFibreChannelHba, 88
Add-VMNetworkAdapterAcl, 93, 94
AD FS, 406–407
Clear-EventLog, 136
Configure-SMRemoting.exe, 55
Convert-VHD, 83
Disable-VMEventing, 136
Disable-VMResourceMetering, 78
Disable-VMsWithitExtension, 93
complex DirectAccess infrastructure

Enable-ADOptionalFeature, 204
Enable-NetFirewallRule, 52
Enable-VMEventing, 136
Enable-VMResourceMetering, 77, 134
Enable-VMSwitchExtension, 93
Export-Counter, 136
Export-VM, 199
Get-ADComputer, 219, 220
Get-ADDCloningExcludedApplicationList, 195–198
Get-ADForest, 204
Get-ADObject, 207
Get-ADUser, 220
(Get-Cluster).DatabaseReadWriteMode, 249
(Get-ClusterNode Node2).NodeWeight, 249
(Get-Cluster).WitnessDynamicWeight, 248
Get-Command, 27, 68
Get-Counter, 136
Get-DACConnectionStatus, 169
Get-Event, 136
Get-EventLog, 136
Get-Help, 27
Get-NetLbfoTeam, 27
Get-OBPolicy, 326
Get-OBSchedule, 326
Get-VMFibreChannelHba, 88
Get-VMNetworkAdapterACL, 94
Get-VMResourcePool, 134
Get-VMSwitchExtension, 93
Get-WindowsFeature, 3, 8
Group Policy, 222–224
Import-Counter, 136
Import-VM, 199
Initialize-ADDeviceRegistration, 404
Install-ADDSDomain, 113, 116–117
Install-ADDSDomainController, 113, 116
Install-ADDSForest, 113, 115
Install-PswaWebApplication, 17
Install-WindowsFeature, 3, 9
Invoke-GpUpdate, 218–220
Logman.exe, 136
Measure-VM, 78
Measure-VMResourcePool, 135
MSOnlineBackup module, 324
New-ADDCCloneConfigFile, 198–199
New-Cluster, 247
New-Event, 136
New-ItemProperty -Name, 48
New-NetLbfoTeam, 27
New-OBPolicy, 325–326
New-OBSchedule, 325–326
New-StoragePool, 32
New-VHD, 83
New-VirtualDisk, 34
New-VMResourcePool, 135
New-VMSwitch, 96
Remove-VMFibreChannelHba, 88
Remove-VMNetworkAdapterACL, 94
Reset-VMResourceMetering, 78
Restore-ADObject, 207
Set-ADForestMode, 204
Set-ADFSProperties, 403
Set-ADObject, 208
Set-DAClient, 158
Set-DAClientDNSConfiguration, 164
Set-DANetworkLocationServer, 162
Set-DAServer, 162
Set-ExecutionPolicy RemoteSigned, 57
Set-Item wsman:\localhost\Client\TrustedHosts, 47
Set-OBMachineSetting, 324, 325
Set-OBPolicy, 326
Set-OBSchedule, 326
Set-RemoteAccessLoadBalancer, 152
Set-VM, 74
Set-VMFibreChannelHba, 88
Set-VMNetworkAdapter, 98
Start-DscConfiguration, 13
Start-OBBackup, 326
Start-OBRegistration, 324, 326
Suspend-ClusterNode, 241
Test-ADDSDomainControllerInstallation, 113, 115
Test-ADDSDomainControllerUninstallation, 113, 118–119
Test-ADDSDomainInstallation, 113
Test-ADDSForestInstallation, 113–114
Test-ADDSDReadOnlyDomainControllerAccountCreation, 113, 117–118
Uninstall-ADDSDomainController, 113, 118
Uninstall-WindowsFeature, 2
Update-FSRMClassificationPropertyDefinition, 293–294
Write-Output $UtilizationReport, 78
complex DirectAccess infrastructure, 151–152
Compress the Data That Is Transmitted Over the
Network check box, 334
-Computer parameter, Invoke-GpUpdate cmdlet, 218
Computer Management, 52, 83
-ComputerName option (Add-PswaAuthorizationRule cmdlet), 17
Configuration Friendly Name dialog box, 184
Configuration function (Windows PowerShell ISE tool), 13
-ConfigurationName option (Add-PswaAuthorizationRule cmdlet), 17
Configuration Wizard (AD FS), 392–394
Configure Additional Recovery Points page (Enable Replication Wizard), 336
Configure and Manage High Availability domain. See high availability
Configure Custom Fields dialog box, 376
Configure File and Storage Solutions domain. See Dynamic Access Control
Configure NAP Wizard, 181
Configure Network Services and Access domain. See DirectAccess, configuring
Configure Replication Frequency page (Enable Replication Wizard), 335
Configure Self-Updating Options Wizard, 245
Configure-SMRemoting.exe cmdlet, 55
configuring
access policies, 302–307
central access rules, 302–306
deploying central access policies to file servers, 306–307
backups. See Windows Azure Backup
claims-based authentication, 287–291
defining user and device claim types, 288–290
enabling Kerberos support, 290–291
cluster properties, 248–249
constrained delegation, 263
custom fields, 376
Data Collector Sets, 138–139
DirectAccess, 154–168
advanced configuration options, 167–168
Application Server Setup Wizard, 166–167
Client Setup Wizard, 156–159
Infrastructure Server Setup Wizard, 162–166
Remote Access Server Setup Wizard, 159–162
verifying configuration, 168–170
domain controllers, 193–200
adding source controllers to Cloneable Domain Controllers group, 194–195
exporting VMs of the source domain controllers, 199–200
Get-ADDCCloningExcludedApplicationList cmdlet, 195–198
importing VMs of the source domain controllers, 199–200
New-ADDCCloneConfigFile cmdlet, 198–199
prerequisites, 194
file classification, 291–301
access-denied assistance, 300–301
adding resource properties to resource property list, 293
automatic classification, 295–300
creating selected resource properties, 292
enabling selected resource properties, 292
manual classification, 294–295
updating Active Directory files, 293–294
Group Policy, 215–225
Remote Group Policy update, 216–222
Windows PowerShell cmdlets, 222–224
high availability
failover clustering, 234–248
failover clustering roles, 251–259
virtual machine movement, 260–277
Hyper-V
virtual machine settings, 67–80
virtual machine storage, 82–89
virtual networks, 90–100
Hyper-V Settings, 261
IPAM (IP Address Management), 361–371
adding servers, 367–371
connecting to servers, 363
manual configuration steps, 371
provisioning servers, 363–365
selecting servers, 367–371
Server Discovery, 366
Server Manager, 361–380
IP utilization thresholds, 378–379
local storage, 30–37
creating storage pools, 31–33
creating virtual disks, 34–37
installing Storage Spaces, 31
Minimal Server Interface, 24
NAP (Network Access Protection), 177–188
SHV multi-configuration, 183–188
PSWA, 17
servers, 7–28
Group Policy Based provisioning method, 368–370
installing roles and features, 7–20
Configuring Server Roles and Features domain

- Minimal Server Interface, 22–24
- NIC teaming, 24–28
- remote management, 45–60
- Server Core-GUI convertibility, 20–22
- site-level fault tolerance, 329–351
- extending replication to third sites, 347–348
- Hyper-V physical host servers, 330–333
- Hyper-V Replica failover, 342–346
- Hyper-V Replica in failover clusters, 348–352
- virtual machines, 333–342
- Configuring Server Roles and Features domain, 45–60
- Group Policy, 57–59
- managing multiple servers with Server Manager, 46–57
- Remote Server Administration Tools, 59–60
- Confirm Installation Selections page (Add Roles and Features Wizard), 11
- connection processes (DirectAccess), 146–147
- connection request policies (NAP processing), 179
- constrained delegation, configuring, 263
- Content Classifier classification method, 297
- Convert-VHD cmdlet, 83
- Copy-GPO cmdlet, 223
- Create Additional Hourly Recovery Points option, 337
- Create Central Access Rule page, 302–303
- Create Claim Type page, 289
- Create Classification Rule dialog box, 295–296
- Create Full NoDefrag %s (IFM menu), 119
- Create Sysvol Full NoDefrag %s (IFM menu), 119
- creating
  - central access rules, 302–306
  - CSVs (cluster shared volumes), 236–238
  - custom fields for IPM, 374–376
  - Data Collector Sets manually, 137–138
  - IP address range groups, 377–378
  - KDS root keys, 394
  - self-signed certificates, 314–315
  - SHV configurations, 184–186
  - SoFS (Scale-Out File Server), 251–252
  - storage pools, 31–33
  - virtual disks, 34–37
- virtual machine resource pools, 135
- virtual machine settings, 67–80
  - Dynamic Memory, 74–77
  - enhanced session mode, 72–74
  - generation 1 and 2 VMs, 69–71
  - Hyper-V Module in Windows PowerShell, 68–69
  - NUMA (non-uniform memory access), 79
- RemoteFX, 79–80
- Resource Metering, 77–78
- virtual networks, 90–100
- advanced features for virtual network adapters, 99–100
- bandwidth management, 97–98
- network isolation, 93–95
- SR-IOV, 95–98
- virtual switch extensions, 91–93
- CredSSP (Credential Security Support Provider), 262
- CSVFS (Cluster Shared Volume File System), 236
- CSVs (cluster shared volumes), 236–239
- live migration in failover clusters, 264–267
- CustomDCCloneAllowList.xml file, 196–197
- custom fields
  - applying to addresses and ranges, 376
  - configuring, 376
  - creating for IPM, 374–376

D

Data Collector Sets, 137–138
DCCloneConfig.xml files, 198
Dcgpofix command, 224
DC/NPS
  - manual configuration steps for managed infrastructure servers in IPAM, 371
- DCOM (Distributed Component Object Model), 52–53
- declarative management, DSC, 14
- Default Web Site (IIS), 17
- Delegation Authorization Rules, 399
- deleted object lifetime, 205, 208
- deleted objects (Active Directory), restoring, 202–209
  - AD Administrative Center, 205–207
  - deleted object lifetime, 208
  - enabling AD Recycle Bin, 204–205
  - Windows PowerShell, 207–208
- Deleted Objects container (Active Directory Administrative Center), 205–207
- deployment, servers, 133–139
  - reviewing older features, 137–139
  - virtual machine resource pools, 134–135
  - Windows PowerShell, 136–137
- Deployment Image Servicing and Management (DISM) utility, 17–20
- Deployment Scenario page (DirectAccess Client Setup Wizard), 156
Description property, 220
Desired State Configuration (DSC), 13–17
Device Registration Service (DRS), 404
DFSR (Distributed File System Replication), 209
DHCP
  manual configuration steps for managed infrastructure servers in IPAM, 371
  server logs, searching for leases by client names/addresses, 373–374
DHCP Guard, 99
diagnosing performance problems, 138
dialog boxes
  Add Authorization Entry, 332–333
  Advanced Security Settings for Permissions, 304
  Central Access Policies Configuration, 306
  Classification Parameters, 298–299
  Cluster-Aware Updating, 244–245
  Configuration Friendly Name, 184
  Configure Custom Fields, 376
  Create Classification Rule, 297
  Edit Global Authentication Policy, 399
  File Server Resource Manager Options, 299
  Hyper-V Settings, 262–263, 330
  IPAM Settings, 375
  Move Virtual Machine Storage, 264–265
  New Team, 26
  Permission Entry For Permissions, 304
Properties, 258
  Select Items, 319
  Select Resource Properties, 293
  Select Services, 255
  Settings (VMs), 341
DirectAccess
  benefits, 144
  Client Experience Settings, 170
  configuring, 154–168
    advanced configuration options, 167–168
    Application Server Setup Wizard, 166–167
    Client Setup Wizard, 156–159
    Infrastructure Server Setup Wizard, 162–166
    Remote Access Server Setup Wizard, 159–162
    verifying configuration, 168–170
  connection process, 146–147
  infrastructure options, 147–152
    complex, 151–152
    multidomains, 149–151
    multisites, 149–151
    server behind NAT, 148–149
simple, 147–148
  installing, 153–154
  IPv6 communication, 144–146
DirectAccessClientComponents module, 153
Directory Services Restore Mode (DSRM) password, 114
Directory tab, DCS, 138
/Disable-Feature switch (DISM utility), 19
Disable-VMEventing cmdlet, 136
Disable-VMResourceMetering cmdlet, 78
Disable-VMSwitchExtension cmdlet, 93
disabling Group Policy caching, 225
disaster recovery
  backups, configuring, 313–326
    Back Up Now option, 321–322
    bandwidth throttling, 322–324
    certificate requirements, 314
    creating online backup schedules, 318–321
    creating backup vaults in management portals, 315–316
    creating self-signed certificates with Makecert.exe utility, 314–315
    downloading Windows Azure Backup Agent, 316–317
    installing Windows Azure Backup Agent, 316–317
    performing backups in Windows PowerShell, 324–326
    recovering data, 322
    registering servers, 317
    uploading certificates, 316
  site-level fault tolerance, configuring, 329–351
    extending replication to a third site, 347–348
    Hyper-V physical host servers, 330–333
    Hyper-V Replica failover, 342–346
    Hyper-V Replica in failover clusters, 348–352
    virtual machines, 333–342
Disk Quotas Group Policy setting, 225
disk space requirements, 2
DISM (Deployment Image Servicing and Management) utility, 17–20
Distributed Component Object Model (DCOM), 52–53
Distributed File System Replication (DFSR), 209
Djoin.exe tool, 119
DNS
  manual configuration steps for managed infrastructure servers in IPAM, 371
  servers, registering, 123
DNS page (Infrastructure Server Setup Wizard), 163
Dynamic Access Control, 285–307
access policies, 302–307
central access rules, 302–306
deploying central access policies to file servers, 306–307
claims-based authentication, 287–291
defining user claim types, 288–290
defining device claim types, 288–290
enabling Kerberos support, 290–291
file classifications, 286–287, 291–301
access-denied assistance, 300–301
adding resource properties to resource property list, 293
automatic classification, 295–300
creating selected resource properties, 292
enabling selected resource properties, 292
manual classifications, 294–295
updating Active Directory files/folders, 293–294
Dynamic Memory, 74–77
DynamicQuorum cluster property, 248–249
dynamic quorum configuration, 240–241
dynamic witness, configuring failover clustering, 241

E
Edge option (Network Topology page), 160
Edit Global Authentication Policy dialog box, 399
Edit Virtual Hard Disk Wizard, 84–85
EKAU (Enhanced Key Usage), 331
Enable-ADOptionalFeature cmdlet, 204
Enable Corporate Compliance for DirectAccess Clients with NAP setting (Authentication page), 162
Enable Internet Bandwidth Usage Throttling For Backup Operations check box, 322
Enable-NetFirewallRule cmdlet, 52
Enable-NetFirewallRule-DisplayName command, 331
Enable Replication Wizard, 334–340
Enable This Computer as a Replica Server check box, 331
Enable-VMEventing cmdlet, 136
Enable-VMResourceMetering cmdlet, 77, 134
Enable-VMSwitchExtension cmdlet, 93
Enable Windows 7 Client Computers to Connect Via DirectAccess setting (Authentication page), 162
enabling
access-denied assistance, 300
Active Directory Recycle Bin, 204–205
bandwidth throttling, 322–324
Kerberos support for claims-based authentication, 290–291
replication on clustered VMs, 351
Endpoints node (AD FS management console), 396
enforcement points (NAP), 178
enforcement types (NAP), 179
Enhanced Key Usage (EKAU), 331
Enhanced session mode policy, 72
virtual machines, 72–74
Evaluation Type tab (Create Classification Rule dialog box), 298
EVENT CATALOG page, searching DHCP server logs for leases by client names/addresses, 373–374
Events section (All Servers page, Server Manager), 50
Event Trace Data option, manually creating DCS, 137
excluding items from backups, 320
Export Configuration Settings (Add Roles and Features Wizard), 12
Export-Counter cmdlet, 136
exporting source domain controller VMs, 199–200
Export-VM cmdlet, 199
Extended Protection for Authentication feature, 403
extending replication to third sites, 347

**F**

failover clustering
configuring, 234–248
Active Directory-detached clusters, 246–247
CAU (cluster-aware updating), 242–246
CSVs (cluster shared volumes), 236–239
dynamic quorum configuration, 240–241
dynamic witness, 241
node drain, 241
roles, 251–259
storage pools, 234–235
virtual hard disk sharing, 239–240
defined, 233
Hyper-V Replica, 348–351
Failover Cluster Manager, 234, 348
failovers
Hyper-V Replica, 342–346
TCP/IP settings, 340–341
feature files
reinstalling, 4–5
removing, 3
Features on Demand, 2–5
Federation Metadata file, 396
Fibre Channel adapters, 86–88
fields, custom fields
applying to addresses and ranges, 376
configuring, 376
creating for IPM, 374–376
file attributes, 286
file classifications, configuring, 291–301
access-denied assistance, 300–301
adding resource properties to resource property list, 293
automatic classification, 295–300
creating selected resource properties, 292
enabling selected resource properties, 292
manual classifications, 294–295
updated Active Directory files/folders, 293–294
File DSC resource, 15–16
File Replication Service (FRS), 209
files
 .cer, 315
 CustomDCCloningAllowList.xml, 196–197
 DCCloneConfig.xml, 198
 .pfx, 315
 VHD (virtual hard disk), 236
File Server Resource Manager Options dialog box, 299
File Server role service, 31
file solutions. See Dynamic Access Control
filtering virtual switch extensions, 91
firewall rules
Remote Group Policy update, 221–222
remote management, 59
First Failure response, 255
fixed provisioned spaces, 36
Folder Classifier classification method, 297
Folder Redirection Group Policy setting, 225
folders, configuring access-denied assistance, 301
-Force parameter (Invoke-GpUpdate cmdlet), 219
forwarding virtual switch extensions, 91
FRS (File Replication Service), 209
full installation, 20

generation 1 virtual machines, 69–71
generation 2 virtual machines, 69–71
Geo-Redundant Replication, 122
Get-ADComputer cmdlet, 219–220
Get-ADDCloningExcludedApplicationList cmdlet, 195–198
Get-ADForest cmdlet, 204
Get-ADObject cmdlet, 207
Get-ADUser cmdlet, 220
(Get-Cluster).DatabaseReadWriteMode cmdlet, 249
(Get-Cluster).DynamicQuorum cmdlet, 248
(Get-ClusterNode Node2).NodeWeight cmdlet, 249
(Get-Cluster).WitnessDynamicWeight cmdlet, 248
Get-Command, 27, 68
Get-Command-Module AD FS command, 407
Get-Counter cmdlet, 136
Get-DACConnectionStatus cmdlet, 169
Get-Event cmdlet, 136
Get-EventLog cmdlet

/Get-Features switch (DISM utility), 19
Get-GPInheritance cmdlet, 223
Get-GPO cmdlet, 223
Get-GPOReport cmdlet, 223
Get-GPPermission cmdlet, 223
Get-GPPrefRegistryValue cmdlet, 223
Get-GPRegistryValue cmdlet, 223
Get-GPResultantSetOfPolicy cmdlet, 223
Get-GPStarterGPO cmdlet, 223
Get-Help cmdlet, 27
/Get-ImageInfo switch (DISM utility), 18
Get-NetLbfoTeam cmdlet, 27
Get-OBPolicy cmdlet, 326
Get-OBSchedule cmdlet, 326
Getting Started Wizard, 154–155
Get-VMFibreChannelHba cmdlet, 88
Get-VMNetworkAdapterACL cmdlet, 94–95
Get-VMResourcePool cmdlet, 134
Get-VMSwitchExtension cmdlet, 93
Get-WindowsFeature cmdlet, 3, 8
global policies, AD FS management console, 399–402
gMSAs (group Managed Service Accounts), 394
Gpfixup command, 224
GPT (GUID Partition Table) partition style, 32
Gpupdate /sync command, 225
Graphical Management Tools and Infrastructure feature, 21
Group DSC resource, 15
group Managed Service Accounts (gMSAs), 394
Group Policy
  caching, 224–225
  configuring, 215–225
  Remote Group Policy update, 216–222
  Windows PowerShell cmdlets, 222–224
  deploying central access policies to file servers, 306–307
  enabling Kerberos support for claims, 290–291
  enabling remote management, 57–59
Group Policy Based provisioning method, configuring servers, 368
Group Policy Management Console, 218
Group Policy Remote Update firewall ports, 221
groups, security, IPAM server, 380
guest clusters, 239
GUIs, installing domain controllers, 108–112
GUID Partition Table (GPT) partition style, 32

H

hardware requirements, server installation, 2
health checks, SHV configuration, 185
health policies (NAP processing), 179, 186–188
Health Policy condition, network policies, 179
Health Registration Authority (HRA), 147
Health Registration Authority (HRA) servers, 179
high availability
  failover clustering, 234–248
    Active Directory-detached clusters, 246–247
    CAU (cluster-aware updating), 242–246
    CSVs (cluster shared volumes), 236–239
    dynamic quorum configuration, 240–241
dynamic witness, 241
  node drain, 241
  roles, 251–259
storage pools, 234–235
  virtual hard disk sharing, 239–240
virtual machine movement, 260–277
  live migration, 261–273
  storage migration, 274–276
High Availability Wizard, 251, 348
host clusters, 239
Hot Spare allocation, storage pools, 34
HRA (Health Registration Authority), 147, 179
Hyper-V
  configuring, 261
  virtual machine settings, 67–80
  virtual machine storage, 82–89
  virtual networks, 90–100
host clusters, 239
Hyper-V Module, Windows PowerShell, 68–69
Hyper-V Replica, 329–351
  configuring physical host servers, 330–333
  configuring virtual machines, 333–342
  failover TCP/IP settings, 340–341
  resynchronizing primary and replica VMs, 341–342
  extending replication to third sites, 347–348
  in failover clusters, 348–352
  failovers, 342–346
Hyper-V Replica Broker role, 348
Hyper-V Replica HTTP Listener, 331
Hyper-V Settings dialog box, 262–263, 330
IPAM Overview page preconfiguration

IaaS (infrastructure-as-a-service), 120
identity solutions. See AD FS (Active Directory Federation Services)
IFM (Install from Media) option, 119–120
/IgnoreCheck option (DISM utility), 20
Import-Counter cmdlet, 136
Import-GPO cmdlet, 223
Importing source domain controller VMs, 199–200
Import-VM cmdlet, 199
infrastructure
  DirectAccess, 147–152
    complex, 151–152
    multidomains, 149–151
    multisites, 149–151
    server behind NAT, 148–149
    simple, 147–148
NAP, 178–180
infrastructure-as-a-service (IaaS), 120
Infrastructure Server Setup Wizard, configuring
  DirectAccess, 162–166
Initialize-ADDDeviceRegistration cmdlet, 404
Install-ADDSDomain cmdlet, 113, 116–117
Install-ADDSDomainController cmdlet, 113, 116
Install-ADDSForest cmdlet, 113, 115
Installation Progress page (Add Roles and Features Wizard), 12
Install from Media (IFM) option, 119–120
installing
  Active Directory domain controllers, 107–127
  DirectAccess, 153–154
domain controllers, 107–127
  GUI, 108–112
  IFM option, 119–120
  Windows Azure, 120–127
  Windows PowerShell, 113–118
IPAM (IP Address Management), 361–362
Makecert utility, 314
roles, 7–20
  DISM (Deployment Image Servicing and Management), 17–20
  DSC (Desired State Configuration), 13–17
  PSWA (Windows PowerShell Web Access), 16–17
  Server Manager, 9–12
  Windows PowerShell, 8–9
servers, 1–5
  Features on Demand, 2–5
  hardware requirements, 2
  SSL (Secure Sockets Layer) certificates, 392–394
  Storage Spaces, 31
  Windows Azure Backup Agent, 316–317
Install-PswaWebApplication cmdlet, 17
Install-WindowsFeature cmdlet, 3, 9
Integration Services, 79
Invoke-GPUpdate cmdlet, 218–220, 223
IP addresses
  adding to IPAM databases, 372–374
  IPAM (IP Address Management), 359–360
    administrative solutions, 360
    configuring, 361–380
    installing, 361–380
    limitations, 360
    managing space, 372–380
    range groups, creating, 377–378
IP Address Management. See IPAM (IP Address Management)
IPAM Administrators group, 380
IPAM ASM Administrators group, 380
IPAM (IP Address Management), 360
  administrative solutions, 360
  configuring, 361–371
  adding servers, 367–371
  connecting to IPAM servers, 363
  manual configuration steps, 371
  provisioning IPAM servers, 363–365
  selecting servers, 367–371
  Server Discovery, 366
  Server Manager, 361–380
  starting Server Discovery, 366
installing, 361–362
  limitations, 360
managing IP address space, 372–380
  adding IP addresses to IPAM databases, 372–374
  applying custom fields to addresses and ranges, 376
  creating custom fields, 374–376
  creating IP address range groups, 377–378
  delegating administration, 380
  viewing/configuring IP utilization thresholds, 378–379
role-based access control in Windows Server 2012 R2, 381–382
IPAM IP Audit Administrators group, 380
IPAM MSM Administrators group, 380
IPAM Overview page preconfiguration, 362–381
IPAM servers

IPAM servers
  connecting to, 363
  local servers, manual configuration steps for
    managed infrastructure servers in IPAM, 371
  provisioning, 363
IPAM Settings dialog box, 375
IPAM Users group, 380
IP-HTTPS transition technology, 145
IPsec enforcement, 179
IP utilization thresholds
  configuring, 378–379
  viewing, 378–379
IPv6 communication, DirectAccess, 144–146
iSCSI Initiator, 307
iSCSI Target, 307
iSNS, 307
Issuance Authorization Rules, 398
Issuance Transform Rules, 398

K

KDS root keys, creating, 394
Kerberos, 262, 290–291
Knowledge Base (KB) article 2682011 performance
  update, 56

L

LastLogonDate property, 220
LBFO (Load Balancing and Failover), 24–28
LDP utility, 203
legacy emulated hardware devices, generation 2
  VMs, 69
limited operating system support, generation 2
  VMs, 71
live migration, virtual machines, 261–273
  failover clusters, 264–267
  nonclustered environments, 267–270
  processor compatibility, 270–272
  virtual switch name matching, 272–273
load balancing, DirectAccess, 151–152
Load Balancing and Failover (LBFO), 24–28
Locally Redundant Replication, 122
local storage, configuring, 30–37
  creating storage pools, 31–33
  creating virtual disks, 34–37
  installing Storage Spaces, 31
logical unit numbers (LUNs), 31, 236
Logman.exe cmdlet, 136
LUNs (logical unit numbers), 31, 236

M

maintenance, Active Directory, 202–209
  Administrative Center, 205–207
  deleted object lifetime, 208
  enabling Recycle Bin, 204–205
  Windows PowerShell, 207–208
Majority (Read And Write) mode, 248
Makecert.exe utility, 314–315
Manage Certificate option, Windows Azure, 316
Managed Object Format (MOF) files, 13
management
backups. See Windows Azure Backup
  Data Collector Sets, 138–139
  Group Policy, 215–225
    caching, 224–225
    Remote Group Policy update, 216–222
    Windows PowerShell cmdlets, 222–224
IP address space, 372–380
  adding IP addresses to IPAM databases, 372–374
  applying custom fields to addresses and
    ranges, 376
  creating custom fields, 374–376
  creating IP address range groups, 377–378
  delegating administration, 380
  viewing/configuring IP utilization
    thresholds, 378–379
servers, 133–139
  review of older features, 137–139
  virtual machine resource pools, 134–135
  Windows PowerShell, 136–137
virtual machine movement, 260–277
  live migration, 261–273
  storage migration, 274–276
  VM network health protection, 276–277
management console (AD FS), 395–403
Authentication Policies node, 399–403
  global policies, 399–402
  Per Relying Party Trust node, 402–403
Service node, 395–397
certificates, 396–397
claim descriptions, 397
endpoints, 396
Trust Relationships node, 397–399
claims provider trusts, 398
claims rules for relying party trusts, 398–399
Management page (Infrastructure Server Setup Wizard), 165–166
manual configurations, IPAM (IP Address Management), 371
manual file classification, 294–295
Master Boot Record (MBR) partition style, 32
Maximum RAM setting, Dynamic Memory, 76
MBR (Master Boot Record) partition style, 32
Measure-VM cmdlet, 78
Measure-VMResourcePool cmdlet, 135
Memory Buffer setting (Dynamic Memory), 76
Memory Weight setting (Dynamic Memory), 76
Metadata section, Endpoints node of AD FS management console, 396
metering virtual machine resource pools, 134–135
Microsoft Management Console (MMC) snap-ins, 52
Migrate a Cluster Wizard, 259
Minimal Server Interface, 22–24
Minimum RAM setting (Dynamic Memory), 75
mirror virtual disks, 35
MMC (Microsoft Management Console) snap-ins, 52
MOF (Managed Object Format) files, 13
monitoring servers, 133–139
review of older features, 137–139
virtual machine resource pools, 134–135
Windows PowerShell, 136–137
Move Virtual Machine Storage dialog box, 264–265
Move Wizard, 274
msDS-DeletedObjectLifetime attribute, 208
MSOnlineBackup module, 324
MS-Service class condition, network policies, 181
multidomain DirectAccess infrastructure, 149–151
multi-factor authentication, 399–402
Multi-Factor tab (Edit Global Authentication Policy dialog box), 401
multiple servers, managing with Server Manager, 46–57
All Servers section, 49–51
DCOM and WinRM, 51–53
non-domain-joined servers, 47–49
re-enabling Windows Server 2012 for remote management, 54–57
multisite DirectAccess infrastructure, 149–151
node drain, configuring failover clustering, 241
Node Majority quorum configuration, 240
NodeWeight cluster property, 249
nonclustered environments, 267–270
non-domain-joined servers, adding to Server Manager, 47–49
non-uniform memory access (NUMA), 79
NPS (Network Policy Server), 178
NRPT (Name Resolution Policy Table), 163
Ntdsutil command-line utility, 203, 206
Ntdsutil.exe tool, 119
NUMA (non-uniform memory access), 79

O

OBPolicy objects, 325
Offline Domain Join, 119
one-time passwords (OTPs), 151
OperatingSystem property, 220
Operations Status item (Remote Access Management Console), 168
OTPs (one-time passwords), 151

P

parity virtual disks, 35
PEAP (Protected Extensible Authentication Protocol), 179
Performance Counter Alert option, manually creating DCS, 138
Performance Counter option, manually creating DCS, 137
performance, diagnosing problems, 138
Performance section (All Servers page, Server Manager), 50
Permission Entry For Permissions dialog box, 304
Per Relying Party Trust node, AD FS management console, 402–403
.pfx files, 315
PhysicalDisk\%Disk Time (performance counter data), 138
Physical Hard Disk option, 84
physical host clusters, 239
physical host servers, configuring Hyper-V, 330–333
PKI (public key infrastructure), 149
planned failovers, 342–343
Port Mirroring, 99
predefined resource properties, 292
prerequisites, cloning domain controllers, 194
/PreventPending option (DISM utility), 20
Previous Versions tab, 324
primary servers, Hyper-V Replica, 330
Primary tab (Edit Global Authentication Policies dialog box), 400
primary VMs, resynchronizing, 341–342
primordial pools, 31–32
principals, 304
processor compatibility, virtual machine live migration, 270–272
Processor\%Processor Time (performance counter data), 138
processor requirements, 2
Properties dialog box, 258
properties tabs (DCS), 138
Protected Extensible Authentication Protocol (PEAP), 179
Protected Network option (Network Adapter settings), 276
Provision IPAM Wizard, 364
PSWA (Windows PowerShell Web Access), 16–17
public key infrastructure (PKI), 149
PXE boot-compatible network adapters, generation 2 VMs, 71

Q

Quick Migration, 267

R

RADIUS protocol, 178
RAM requirements, 2
-RandomDelayInMinutes, Invoke-GpUpdate cmdlet, 219
ranges (IP addresses), adding to IPM databases, 373–374
Read Access - Geo Redundant Replication, 122
recovering data, backups, 322
recovery points, 337
redundancy, 122–123
roles

Register Server Wizard, 317
regular expressions, 298
reinstalling feature files, 4–5
relying party trusts, AD FS management console, 398
Remote Access Management console, installing DirectAccess, 153–154
Remote Access Server Setup Wizard, configuring DirectAccess, 159–162
Remote Access Setup Wizard, 154
Remote Desktop Services Installation option, 11
RemoteFX, 79–80
Remote Group Policy update, 216–222
  firewall rules, 221–222
  Task Scheduler, 220–221
  updating GP in organizational units, 216–218
  updating GP with Invoke-GpUpdate cmdlet, 218–220
remote management, configuring servers for, 45–60
  Group Policy, 57–59
  managing multiple servers with Server Manager, 46–57
Remote Server Administration Tools, 59–60
remote servers, deploying roles and features
  Server Manager, 9–12
  Windows PowerShell, 8–10
remote updating mode, 243
Remote Volume Management, 52
Remove-GPLink cmdlet, 223
Remove-GPO cmdlet, 223
Remove-GPPrefRegistryValue cmdlet, 223
Remove-GPRegistryValue cmdlet, 223
Remove-VMFibreChannelHba cmdlet, 88
Remove-VMNetworkAdapterACL cmdlet, 94
removing feature files, 3
Rename-GPO cmdlet, 223
replica servers, Hyper-V Replica, 330
replication. See Hyper-V Replica
replica VMs, resynchronizing, 341–342
requirements
  failover cluster storage pools, 235
  server installation, 2
  Storage Spaces, 31
  VM Monitoring feature, 254
Requires keyword, configuring features in sequences, 16
Reset-VMResourceMetering cmdlet, 78
Resource Control VM setting, 79
Resource Metering, 77–78
ResourceMeteringEnabled status, 134
-ResourcePoolName parameter
  (Enable-VMResourceMetering cmdlet), 134
resource pools, virtual machines, 134–135
-ResourcePoolType parameter (Enable-VMResourceMetering cmdlet), 134
resource properties (Dynamic Access Control)
  adding to resource property lists, 293
  creating, 292
  defined, 286
  enabling, 292
  predefined, 292
Resource Property Lists container, 293
resources, DSC, 14–16
Restart The Service setting, 257
Restore-ADObject cmdlet, 207
Restore-GPO cmdlet, 223
restoring deleted objects (Active Directory), 202–209
  Administrative Center, 205–207
  deleted object lifetime, 208
  enabling Recycle Bin, 204–205
  Windows PowerShell, 207–208
resynchronizing primary and replica VMs, 341–342
retention setting, backups, 321
Reverse Replication Wizard, 344
Review Options page (Active Directory Domain Services Configuration Wizard), 110
RID Master, 108
RODC accounts, 117–118
role-based access control, IPAM (IP Address Management) in Windows Server 2012 R2, 381–382
roles
  configuring failover clustering, 251–259
    assigning role startup priority, 253–254
    SoFS (Scale-Out File Server), 251–252
    virtual machine application monitoring, 254–260
  configuring servers for remote management, 45–60
    Group Policy, 57–59
    managing multiple servers with Server Manager, 46–57
    Remote Server Administration Tools, 59–60
defined, 233
installing, 7–20
role startup priority, assigning

DISM (Deployment Image Servicing and Management), 17–20
DSC (Desired State Configuration), 13–17
PSWA (Windows PowerShell Web Access), 16–17
Server Manager, 9–12
Windows PowerShell, 8–9
role startup priority, assigning, 253
Router Guard, 99

S

-SafeModeAdministratorPassword parameter
(Test-ADDSForestInstallation cmdlet), 114
SAS (Serial Attached SCSI) disk array, 234
Save Template option, DCS, 138
scalability, failover clusters, 233
Scale-Out File Server role, 238
Scale-Out File Server (SoFS), 251–252
scenarios, AD FS, 390–391
Schedule Backup Wizard, 318–321
Sconfig configuration tool, 55–57
scope, classification rules, 296
SCSI boot, generation 2 VMs, 71
SDK (Software Development Kit), 314
seamless connectivity (DirectAccess), 144
searching DHCP server logs for leases by
client names/addresses, 373–374
Second Failure response, 255
Secure Sockets Layer (SSL) certificates, 314, 392–394
security groups (IPAM server), 380
Security Health Validator, 183
Select Destination Server page (Add Roles and Features
Wizard), 11
Select Groups page (DirectAccess Client Setup
Wizard), 157
selecting items for backup (Schedule Backup
Wizard), 318–319
Select Installation Type page (Add Roles and Features
Wizard), 11
Select Items dialog box, 319
Select Provisioning Method page, 367–368
Select Resource Properties dialog box, 293
Select Services dialog box, 255
Select The Storage Layout page (New Virtual Disk
Wizard), 34
self-signed certificates, creating with Makecert.exe
utility, 314–315
self-updates, 243
Serial Attached SCSI (SAS) disk array, 234
Server Core-GUI convertibility, 20–22
Server Core Installation, 20
Server Discovery
adding servers, 367–369
configuring IPAM (IP Address Management), 366
selecting servers, 367–369
starting, 366
Server Graphical Shell feature, 21
SERVER INVENTORY page, 367
Server Manager
configuring IPAM, 361–380
deploying roles and features on remote
servers, 9–12
managing multiple servers, 46–57
All Servers section, 49–51
DCOM and WinRM, 51–53
non-domain-joined servers, 47–49
re-enabling Windows Server 2012 for remote
management, 54–57
servers
adding, 367–369
configuring, 7–28
Group Policy Based provisioning
method, 368–370
installing roles and features, 7–20
Minimal Server Interface, 22–24
NIC teaming, 24–28
remote management, 45–60
Server Core-GUI convertibility, 20–22
installing, 1–5
Features on Demand, 2–5
hardware requirements, 2
monitoring, 133–139
review of older features, 137–139
virtual machine resource pools, 134–135
Windows PowerShell, 136–137
registering to enable backups, 317
Server With A GUI installation, 20
Service Communications certificate, 397
Service DSC resource, 15
service-level agreements (SLAs), 89
Service node (AD FS management console), 395–397
certificates, 396–397
claim descriptions, 397
directories, 396
Services section (All Servers page, Server Manager), 50
Set-ADForestMode cmdlet, 204
Set-ADFSProperties cmdlet, 403
Set-ADObject cmdlet, 208
Set-DAClient cmdlet, 158
Set-DAClientDNSConfiguration cmdlet, 164
Set-DANetworkLocationServer cmdlet, 162
Set-DAServer cmdlet, 162
Set-ExecutionPolicy RemoteSigned cmdlet, 57
Set-GPINheritance cmdlet, 223
Set-GPLink cmdlet, 223
Set-GPPassword cmdlet, 224
Set-GPPrefRegistryValue cmdlet, 224
Set-GPRegistryValue cmdlet, 224
Set-Item wsman:\localhost\Client\TrustedHosts cmdlet, 47
Set-OBMachineSetting cmdlet, 324, 325
Set-OBPolicy cmdlet, 326
Set-OBSchedule cmdlet, 326
Set-RemoteAccessLoadBalancer cmdlet, 152
Settings dialog box (VMs), 341
Set-VM cmdlet, 74
Set-VMFibreChannelHba cmdlet, 88
Set-VMNetworkAdapter cmdlet, 98
Shadow Copies settings, file servers, 324
shutdown, automatic node drain, 242
SHV (System Health Validator), 179, 183–188
assigning configurations to a health policy, 186–188
creating additional SHV configurations, 184–186
default configuration, 184
side-by-side store, 2
simple DirectAccess infrastructure, 147–148
simple virtual disks, 34
single-root I/O virtualization (SR-IOV), 95–98
single-sign-on (SSO) access, 389–390
site-level fault tolerance, configuring, 329–351
extending replication to third sites, 347–348
Hyper-V physical host servers, 330–333
Hyper-V Replica failover, 342–346, 348–352
virtual machines, 333–342
failover TCP/IP settings, 340–341
resynchronizing primary and replica VMs, 341–342
Size Of The Virtual Disk page (New Virtual Disk Wizard), 36
SLAs (service-level agreements), 89
Smart Paging, 76–77
snapshots, 77
SoFS (Scale-Out File Server), 251–252
Software Development Kit (SDK), 314
Software Installation Group Policy setting, 225
SoH (statement of health), 178
Specify Connection Parameters page (Enable Replication Wizard), 334
Specify Generation page (New Virtual Machine Wizard), 69
Specify Replica Server page (Enable Replication Wizard), 334
Specify Retention Setting page (Schedule Backup Wizard), 321
Specify The Provisioning Type page (New Virtual Disk Wizard), 36
SR-IOV (single-root I/O virtualization), 95–98
SSL (Secure Sockets Layer) certificates, 314, 392–394
SSO (single-sign-on) access, 389–390
Start-DscConfiguration cmdlet, 1 3
Starting Server Discovery, 366
Start-OBBackup cmdlet, 326
Start-OBRegistration cmdlet, 324, 326
startup priorities, assigning to roles, 253–254
Startup RAM setting (Dynamic Memory), 75
statement of health (SoH), 178
Stop Condition tab (DCS), 138
storage
configuring local storage, 30–37
creating storage pools, 31–33
creating virtual disks, 34–37
installing Storage Spaces, 31
virtual machines, 82–89
Fibre Channel adapters, 86–88
Storage QoS, 88–89
VHDX disk format, 82–85
storage accounts, 122–123
storage migration, virtual machines, 274–276
storage pools
creating, 31–33
failover clustering, 234–235
storage Quality of Service (QoS) virtual machines, 88–89
Storage Spaces, 30–37
creating storage pools, 31–33
creating virtual disks, 34–37
installing, 31
string expressions, 298
Subsequent Failures response, 255
Suspend-ClusterNode cmdlet, 241
switches
synchronous GPO processing

/Disable-Feature, 19
/Get-Features, 19
/Get-ImageInfo, 18
synchronous GPO processing, 224–225
System Configuration Information option, manually creating DCS, 137
System Health Validator, 179, 183–188
assigning configurations to a health policy, 186–188
creating additional SHV configurations, 184–186
default configuration, 184

T
Take No Action setting, 257
Task Scheduler, Remote Group Policy update, 220–221
TCP/IP settings, configuring Hyper-V VMs, 340–341
Teredo transition technology, 145
Test-ADDSDomainControllerInstallation cmdlet, 113, 115
Test-ADDSDomainControllerUninstallation cmdlet, 113, 118–119
Test-ADDSDomainInstallation cmdlet, 113
Test-ADDSForestInstallation cmdlet, 113–114
Test-ADDSReadOnlyDomainControllerAccountCreation cmdlet, 113, 117–118
test failovers, 345–346
TGT (ticket-granting ticket), 287
thin provisioning, 36
Throttling tab, 322
ticket-granting ticket (TGT), 287
Token-Decrypting certificates, 397
Token Issuance section, Endpoints node of AD FS management console, 396
Token-Signing certificates, 397
tokens, user authentication, 389
trust groups, 332
Trust Relationships node (AD FS management console), 397–399
claims provider trusts, 398
claims rules for relying party trusts, 398–399
relying party trusts, 398

U
UEFI (Unified Extensible Firmware Interface), 70
Uninstall-ADDSDomainController cmdlet, 113, 118
uninstalling domain controllers, Windows PowerShell, 118
Uninstall-WindowsFeature cmdlet, 2
unplanned failovers, 343–345
Update-FSRMClassificationPropertyDefinition cmdlet, 293–294
updating
Active Directory files/folders, 293–294
Group Policy
Group Policy Management Console, 216–218
Invoke-GpUpdate cmdlet, 218–220
uploading certificates to Windows Azure, 316
Use Computer Certificates setting (Authentication page), 161
Use Force Tunneling option, 158
Use Hardware Topology button, 79
user authentication, AD FS, 390–392
User Authentication setting (Authentication page), 161
user claims types, configuring claims-based authentication, 288–290
-UserName option (Add-PswaAuthorizationRule cmdlet), 17

V
verifying DirectAccess configuration, 168–170
VHD (virtual hard disk) files, 236
DISM utility, 18
VHDX disk format, 82–85
VHDX files, DISM utility, 18
VHDX sharing, 239
viewing IP utilization thresholds, 378–379
virtual disks, creating, 34–37
virtual hard disk (VHD) files, 236
virtual machines
application monitoring, 254–260
configuring Hyper-V, 333–342
failover TCP/IP settings, 340–341
resynchronizing primary and replica VMs, 341–342
configuring storage, 82–89
Fibre Channel adapters, 86–88
Storage QoS, 88–89
VHDX disk format, 82–85
creating and configuring settings, 67–80
Dynamic Memory, 74–77
enhanced session mode, 72–74
generation 1 and 2 VMs, 69–71
Hyper-V Module in Windows PowerShell, 68–69
NUMA (non-uniform memory access), 79
RemoteFX, 79–80
Resource Metering, 77–78
migration, 260–277
live migration, 261–273
storage migration, 274–276
VM network health protection, 276–277
resource pools, 134–135
virtual networks, 90–100, 124
advanced features for virtual network
adapters, 99–100
bandwidth management, 97–98
network isolation, 93–95
SR-IOV, 95–98
virtual switch extensions, 91–93
virtual private networks. See VPNs
virtual switch extensions, 91–93
Virtual Switch Manager, 91–92
virtual switch name matching, 272–273
VM Monitoring feature, 254
Volume Shadow Copy Service (VSS) copies, 338
VPNs (virtual private networks)
enforcement, 179
VPN icon, 170
VSSAdmin tool, 324
VSS (Volume Shadow Copy Service) copies, 338

W

WDS (Windows Deployment Services), 137
Web Application Proxy, 390
WIM (Windows Imaging), DISM utility, 18
Windows Azure, installing domain controllers, 120–127
Windows Azure Backup, 313–326
Back Up Now option, 321–322
bandwidth throttling, 322–324
certificate requirements, 314
creating an online backup schedule, 318–321
creating backup vault in management
portal, 315–316
creating self-signed certificate with Makecert.exe
utility, 314–315
performing in Windows PowerShell, 324–326
recovering data, 322
registering servers, 317
uploading certificates, 316
Windows Deployment Services (WDS), 137
Windows Firewall Remote Management, 52
Windows Imaging (WIM), DISM utility, 18
Windows Management Framework updates, 56
Windows Management Instrumentation (WMI), 52–54
Windows PowerShell
cmdlets. See individual names of cmdlets
deploying roles and features on remote servers, 8–9
DSC (Desired State Configuration), 13–17
Hyper-V Module, 68–69
installing domain controllers, 113–118
adding to existing domains, 115–116
first controller in new domain of existing
forests, 116–117
new forests, 114–115
RODC accounts, 117–118
monitoring servers, 136–137
performing Windows Azure Backups, 324–326
restoring deleted objects, 207–208
uninstalling domain controllers, 118
Windows PowerShell Classifier classification
method, 297
Windows PowerShell Web Access (PSWA), 16–17
Windows Remote Management (WinRM), 53–54
Windows Security Health Validator, 179, 183
Windows Server 2012 R2, role-based access control for
IPAM, 381–382
Windows Server Update Services (WSUS), 137
Windows SHVs, 179
Winrm Quickconfig command, 55
WinRM (Windows Remote Management), 53–54
WitnessDynamicWeight cluster property, 248
witnesses, configuring failover clustering, 241

Wizards

Active Directory Domain Services
Configuration, 107–127
Add Relying Party Trust, 398
Add Roles And Features, 9–12, 361
AD FS Configuration, 392–394
Configure NAP, 181
Configure Self-Updating Options, 245
configuring DirectAccess
Application Server Setup, 166–167
Client Setup, 156–159
Infrastructure Server Setup, 162–166
Remote Access Server Setup, 159–162
Remote Access Setup, 154
WMI (Windows Management Instrumentation)

- Edit Virtual Hard Disk, 84–85
- Enable Replication, 334–340
- Getting Started, 154–155
- High Availability, 251, 348
- Migrate A Cluster, 259
- Move, 274
- New Inbound Rule, 58
- New Storage Pool, 33, 234
- New Virtual Disk, 34–35
- Provision IPAM, 364
- Register Server, 317
- Reverse Replication, 344
- Schedule Backup, 318–321

WMI (Windows Management Instrumentation), 52–54
Workplace Join, AD FS, 403–406
World Wide Node Name (WWNN), 87
World Wide Port Name (WWPN), 87
Write-Output $UtilizationReport cmdlet, 78
WS-Management Protocol, 52
WSUS (Windows Server Update Services), 137
WWNN (World Wide Node Name), 87
WWPN (World Wide Port Name), 87