Introduction

Windows Server 2008 is the latest release of the Windows Server operating system. Over the years, it has evolved quite dramatically from the early days of Windows NT Server or even Windows 2000 Server. With the release of Windows 2008, Microsoft again has introduced a number of new technologies intended to help IT professionals improve their ability to provide network services to the clients they serve.

I've had the opportunity to write a book on every version of Windows Server over the past dozen years, and when my coauthors and I set out to write this book, we wanted to once again provide you, the reader, with a lot of really valuable information. Not just marketing fluff that talks about features and functions, but to really dig down into the product and share with you best practices on planning, preparing, implementing, migrating, and supporting a Windows 2008 environment.

Even though Windows 2008 released in early 2008, we've been fortunate enough to work with Windows Server Codename "Longhorn" since as early as 2005, so we've had almost three full years on an early adopter program. The thing about being involved with a product so early on is that our first experiences with Longhorn Server were without any documentation, Help files that provided guidance, or any shared experiences from others. We had to learn Longhorn Server from experience, usually the hard way, but that has given us a distinct advantage of knowing the product forward and backward better than anyone could ever imagine. And we started to implement Longhorn Server in production environments for a select group of our enterprise customers over a year before the product release—where organizations were depending on Longhorn Server to run key areas of their business.

So, the pages of this book are filled with years of experience with Windows 2008, live production environment best practices, and fully updated RTM code specifics that will hopefully help you design, plan, prototype, implement, migrate, administer, and support your Windows 2008 environment!

This book is organized into 11 parts, each part focusing on core Windows Server 2008 areas, with several chapters making up each part. The parts of the book are as follows:

▶ Part I: Windows Server 2008 Overview—This part provides an introduction to Windows 2008 not only to give a general technology overview, but also to note what is truly new in Windows 2008 that made it compelling enough for organizations to implement the technology in beta in production environments. We also cover basic planning, prototype testing, and migration techniques, as well as provide a full chapter on the installation of Windows 2008 as well as the new Server Core.

- ▶ Part II: Windows Server 2008 Active Directory—This part covers Active Directory planning and design. If you have already designed and implemented your Active Directory, you will likely not need to read through this section of the book in detail. However, you might want to look through the best practices at the end of each chapter because we highlight some of the tips and tricks new to Windows 2008 that are different from Windows 2000/2003. You might find that limitations or restrictions you faced when designing and implementing Windows 2000/2003 and Active Directory have now been revised. Topics such as federated forests, lightweight directory services, and identity lifecycle management capabilities might be of interest.
- ▶ Part III: Networking Services—This part covers DNS, DHCP, domain controllers, IPv6, and IIS from the perspective of planning, integrating, migrating, and coexisting. Again, just like in Part II, you might find the Notes, Tips, and best practices to have valuable information on features that are new in Windows 2008; they might have you reading these chapters in-depth to understand what's new and different that you can leverage after a migration to Windows 2008.
- ▶ Part IV: Security—Security is on everyone's mind these days, so it was a major enhancement to Windows 2008. We actually dedicated three chapters of the book to security, breaking the information into server-level security such as Public Key Infrastructure (PKI) certificate services; transport-level security such as IPSec and NAT traversal; and security policies, network access protection (NAP), and network policy server (NPS) that are new to Windows 2008.
- ▶ Part V: Migrating to Windows Server 2008—This part is dedicated to the migrations from Windows 2000/2003 to Windows 2008. We provide a chapter specifically on tips, tricks, best practices, and lessons learned on the planning and migration process to Windows 2008. We also have a chapter on application-compatibility testing of applications currently running on earlier versions of Windows Server and how to test and migrate applications to a Windows 2008 platform.
- Part VI: Windows Server 2008 Administration and Management—After you get Windows 2008 in place, you end up spending the rest of your time managing and administering the new operating system platform, so we've dedicated six chapters to administration and management. This section covers the administration and management of users, sites, organizational units, domains, and forests typical of a Windows 2008 environment. Although you can continue to perform tasks the way you did in Windows 2000/2003, because of significant changes in replication, background transaction processing, secured communications, Group Policy management, and Windows PowerShell management tools, there are better ways to work with Windows 2008. These chapters drill down into specialty areas helpful to administrators of varying levels of responsibility. This part of the book also has a chapter on managing Windows 2008 using System Center Operations Manager 2007.

- ▶ Part VII: Remote and Mobile Technologies—Mobility is a key improvement in Windows 2008, so this part focuses on enhancements made to Routing and Remote Access Service (RRAS) in addition to significant improvements in Terminal Services. Instead of just providing a remote node connection, Windows 2008 provides true end-to-end secured anytime/anywhere access functionality. The chapters in this part highlight best practices on implementing and leveraging these technologies.
- Part VIII: Desktop Administration—Another major enhancement in Windows 2008 is the variety of new tools provided to support better desktop administration, so this part is focused on desktop administration. The chapters in this part go in depth on client-specific group policies, the Group Policy Management Console, Windows Deployment Services (WDS), and desktop administration tools in Windows 2008.
- ▶ Part IX: Fault Tolerance Technologies—As networks have become the backbone for information and communications, Windows 2008 needed to be reliable and more manageable and, sure enough, Microsoft included several new enhancements in fault-tolerant technologies. The four chapters in this part address file system management and file-level fault tolerance in Distributed File System (DFS), clustering, Network Load Balancing, and backup and restore procedures. When these new technologies are implemented in a networking environment, an organization can truly achieve enterprise-level reliability and recoverability.
- ▶ Part X: Optimizing, Tuning, Debugging, and Problem Solving—This part of the book covers performance optimization, capacity analysis, logging, and debugging to help optimize and solve problems in a Windows 2008 networking environment.
- Part XI: Integrated Windows Application Services—The last part of this book covers core application services integrated in Windows 2008, including Windows SharePoint Services 3.0, Windows Media Services, and Hyper-V server virtualization.

It is our hope that the real-world experience we have had in working with Windows Server 2008 and our commitment to relaying information that will be valuable in your planning, implementation, and migration to a Windows 2008 environment will help you get up to speed on the latest in the Windows Server operating system software!

CHAPTER 1

Windows Server 2008 Technology Primer

 ${
m W}$ indows Server 2008 was launched on February 27, 2008, and to some it is just the next-generation server operating system that replaces Windows 2003, but for others it is a significant improvement to a 5-year-old operating system that will drastically improve how IT will support business and organizational initiatives for the next several years. To the authors of this book, we see the similarities that Windows 2008 has in terms of usability and common graphical user interfaces (GUIs) with previous versions of Windows Server that make it easy to jump in and start implementing the new technologies. However, after 3 1/2years of early adopter experience with Windows 2008, when properly implemented, the new features and technologies built in to Windows 2008 really address shortcomings of previous versions of Windows Server and truly allow IT organizations to help organizations meet their business initiatives through the implementation of key technologies now included in Windows 2008.

This chapter provides an overview of what's in Windows 2008, explains how IT professionals have leveraged the technologies to improve IT services to their organization, and acts as a guide on where to find more information on these core technology solutions in the various chapters of this book.

Windows Server 2008 Defined

Windows Server 2008 is effectively the sixth generation of the Windows Server operating system and on the surface looks and feels very much like a cross between Windows Server 2003 and Windows Vista. Upon initial bootup, shown in Figure 1.1, Windows 2008 looks like Windows Vista relative to icons, toolbars, and menus. However,

IN THIS CHAPTER

- ▶ Windows Server 2008 Defined
- When Is the Right Time to Migrate?
- Versions of Windows Server 2008
- What's New and What's the Same About Windows Server 2008?
- ► Changes in Active Directory
- Windows Server 2008 Benefits for Administration
- Improvements in Security in Windows Server 2008
- Improvements in Windows Server 2008 for Better Branch Office Support
- Improvements for Thin Client Terminal Services
- Improvements in Clustering and Storage Area Network Support
- Improvements in Server Roles in Windows Server 2008
- Identifying Which Windows Server 2008 Service to Install or Migrate to First

because Windows 2008 is more of a business functional operating system than a consumer or user operating system, things like the cute Windows Aero 3D interface are not installed and the multimedia features found in the Windows Vista Home or Ultimate versions of the operating system are not included, by default.



FIGURE 1.1 Windows 2008 desktop screen.

Under the surface, though, and covered through the pages of this chapter are highlighted the new technologies and capabilities built in to Windows 2008.

Windows 2008 Under the Hood

As much as there are a lot of new features and functions added in to Windows 2008 that are covered in chapters throughout this book, one of the first places I like to start is around the things in Windows 2008 that you don't see that make up some of the core capabilities of the new operating system. These are technologies that make the new operating system faster, more reliable, and do more things—but they aren't features that you have to install or configure.

Self-Healing NTFS

One of the new embedded technologies in Windows 2008 is self-healing NTFS. Effectively, the operating system has a worker thread that runs in the background, which makes corrections to the file system when NTFS detects a corrupt file or directory. In the past when there was a file system problem, you typically had to reboot the server for chkdsk to run and clean up file and directory corrupt errors.

This self-healing function is not something you will ever see running; however, it is an added capability under the hood in Windows 2008 that keeps the operating system running reliably and with fewer system problems.

Hot-Swappable Components

Included in Windows 2008 is the ability to hot swap core hardware components, such as replacing memory, processors, and PCI adapter cards to a server that supports this feature. In an IT environment where zero downtime means that an IT administrator cannot even shut down a system to replace failed components, having hot-swappable capabilities built in to the operating system helps organizations minimize system downtime.

In Windows 2008, with properly supported hardware, failed memory can be swapped out while the server is running. In addition, processor boards can be hot swapped, and PCI adapters such as network adapters or communications adapters can be added or removed from the system. Many IT operations already enjoy some of these capabilities as several server hardware vendors have provided plug-ins to Windows 2003 to support this type of functionality. However with this capability now built in to Windows 2008, an IT professional can perform the hot swaps and both the operating system and applications running on the operating system will acknowledge the hardware changes without the use of special add-in software components.

Server Message Block 2.0

Introduced in Windows Vista and now core to Windows 2008 is Server Message Block 2.0, more commonly called SMB2. SMB2 is a protocol that handles the transfer of files between systems. Effectively, SMB2 combines file communications and through a larger communications buffer is able to reduce the number of round-trips needed when transmitting data between systems.

For the old-timers reading this chapter, it is analogous to the difference between the copy command and the xcopy command in DOS. The copy command reads, writes, reads, writes information. The xcopy command reads, reads information and then writes, writes, writes the information. Because more information is read into a buffer and transferred in bulk, the information is transmitted significantly faster.

Most users on a high-speed local area network (LAN) won't notice the improvements when opening and saving files out of something like Microsoft Office against a Windows 2008 server; however, for users who might be copying up large image files or datasets between systems will find the information copying 10 to 30 times faster. The performance improvement is very noticeable in wide area network (WAN) situations on networks with high latency. Because a typical transfer of files requires short read and write segments of data, a file could take minutes to transfer across a WAN that can transfer in seconds between SMB2 connected systems because the round-trip chatter is drastically reduced.

For SMB2 to work effectively, the systems on both ends need to be Windows 2008 systems, Windows Vista systems, or a combination of the two. A Windows XP client to a Windows 2008 server will communicate over SMB 1.0 for backward compatibility and will not gain from this new technology.

SMB2 and the benefits of this embedded technology are discussed in more detail in Chapter 32, "Optimizing Windows Server 2008 for Branch Office Communications."

Parallel Session Creation

In Windows 2008, the Session Manager Subsystem (smss.exe) creates an instance of itself to initialize each session up to the number of processors in the server. In the past with

Windows 2003 or earlier, there was only a single instance of smss.exe, and, thus, system requests had to be handled sequentially. With parallel processing of sessions, technologies like Windows Terminal Services greatly benefit from this enhancement. Rather than having seven Terminal Services clients queued up to log on and run thin client sessions, on an eight-core processor server, each of the seven client sessions can simultaneously log on and run applications at processor speed.

Again, this is a technology that a network administrator does not install, configure, or run separately, but is now built in to Windows 2008, which ultimately improves the raw performance of applications and tasks that used to queue up serially on a server that can now be handled in parallel with each core processor handling the added tasks.

User Profile Hive Cleanup Service

Another technology built in to Windows 2008 is the User Profile Hive Cleanup Service. This service helps to ensure user sessions are completely terminated when a user logs off of a system. It removes temporary file content, cache memory content, and other information typically generated during a user session, but deemed unnecessary for longer-term storage.

This service is particularly useful for organizations using Windows 2008 Terminal Services where user sessions are routinely created on a server, and for security purposes, the user profile data is removed when the user logs off of the session.

Hyper-V

Hyper-V is a technology built in to the core of the operating system in Windows 2008 that greatly enhances the performance and capabilities of server virtualization in a Windows 2008 environment. In the past, virtual server software sat on top of the network operating system and each guest session was dependent on many shared components of the operating system.

Hyper-V provides a very thin layer between the hardware abstract layer of the system and the operating system that provides guest sessions in a virtualized environment to communicate directly with the hardware layer of the system. Without having the host operating system in the way, guest sessions can perform significantly faster than in the past, and guest sessions can operate independent of the host operating system in terms of better reliability from eliminating host operating system bottlenecks.

Hyper-V and server virtualization is covered in more detail in Chapter 37, "Deploying and Using Windows Virtualization."

Windows Server 2008 as an Application Server

As much as there have been significant improvements in Windows 2008 under the hood that greatly enhance the performance, reliability, and scalability of Windows 2008 in the enterprise, Windows servers have always been exceptional application servers hosting critical business applications for organizations. Windows 2008 continues the tradition of the operating system being an application server with common server roles being included in the operating system. When installing Windows 2008, the Server Manager console provides a list of server roles that can be added to a system, as shown in Figure 1.2.

Add Roles Wizard		×
Select Server Ro	les	
Before You Begin Server Roles Confirmation Progress Results	Select one or more roles to install on this server. Roles: Active Directory Oomán Services Active Directory Ughtweight Directory Services Active Directory Rights Management Services PhCP Server DNS Server Fax Server File Services Network Policy and Access Services Print Services Wordows Deployment Services Windows Deployment Services Mindows SharePoint Services More about server roles Active Directory Rights Network Server Vitualization (Installed) Mindows SharePoint Services	Description: Active Directory Certificate Services (AD C.S) used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications. Install Cancel

FIGURE 1.2 Server roles in Windows 2008.

The various server roles in Windows 2008 typically fall into three categories, as follows:

- ▶ File and print services—As a file and print server, Windows 2008 provides the basic services leveraged by users in the storage of data and the printing of information off the network. Several improvements have been made in Windows 2008 for file security (covered in Chapter 13, "Server-Level Security") and file server fault tolerance (covered in Chapter 28, "File System Management and Fault Tolerance").
- ▶ Domain services—In enterprise environments running Windows networking, typically the organization is running Active Directory to provide centralized logon authentication. Active Directory continues to be a key component in Windows 2008 with several extensions to the basic internal forest concept of an organization to expanded federated forests that allow Active Directories to interconnect with one another. There are several chapters in Part II, "Windows Server 2008 Active Directory," that address Active Directory, federated forests, lightweight directories, and so on.
- Application services—Windows 2008 provides the basis for the installation of business applications such as Microsoft Exchange, Microsoft Office SharePoint Services, SQL Server, and so on. These applications are initially made to be compatible with Windows 2008, and later are updated to leverage and take full advantage of the new technologies built in to the Windows 2008 operating system. Some of the applications that come with Windows 2008 include Windows Terminal Services for thin client computing access (covered in Chapter 25, "Terminal Services"), Windows Media Server for video and audio hosting and broadcasting (covered in Chapter 36,

"Windows Media Services"), utility server services such as DNS and DHCP (covered in Chapter 11, "DHCP/WINS/Domain Controllers," and Chapter 10, "Domain Name System and IPv6"), SharePoint document sharing and collaboration technologies (covered in Chapter 35, "Windows SharePoint Services 3.0"), and virtual server hosting (covered in Chapter 37).

This book focuses on the Windows 2008 operating system and the planning, migration, security, administration, and support of the operating system. Windows 2008 is also the base network operating system on top of which all future Windows Server applications will be built.

When Is the Right Time to Migrate?

When Windows 2008 first shipped at the beginning of 2008, many organizations wondered about the right time to migrate to the new operating system. It used to be that you waited until the first service pack shipped before installing any Microsoft product; however, Windows 2008 in the early adopter beta program proved to be so extremely reliable and dependable that many organizations were implementing Windows 2008 before the product launch. So, the decision of when to implement Windows 2008 comes down to the same decision on migration to any new technology—identify the value received by implementing Windows 2008, test the solution in a limited environment, and roll Windows 2008 out when you are comfortable that the product meets the needs of your organization.

This introductory chapter notes the many features and functions built in to Windows 2008 that have helped other organizations make the decision that Windows 2008 has significant value to plan a migration and new server implementation. Improvements in security, performance, and manageability provide benefits to organizations looking to minimize administration costs, while providing more functionality to users.

The cost and effort to migrate to Windows 2008 vary based on the current state of an organization's networking environment as well as the Windows 2008 features and functions the organization wants to implement. Some organizations begin their migration process to Windows 2008 by adding a Windows 2008 member server into an existing Windows 2000/2003 network. Others choose to migrate their Active Directory to Windows 2008 as their introduction to the new operating system.

Adding a Windows Server 2008 System to a Windows 2000/2003 Environment

Many organizations want to add in a specific Windows 2008 function such as Windows Server 2008 Terminal Services, Windows SharePoint Services, Windows Media Services, or so on. Such functions can be installed on Windows 2008 member servers in existing Windows 2000/2003 networking environments. This allows an organization to get Windows 2008 application capabilities fairly quickly and easily without having to do a full migration to Windows Server 2008. In many cases, a Windows 2008 member server can simply be added to an existing network without ever affecting the existing network. This addition provides extremely low network impact but enables an organization to prototype and test the new technology, pilot it for a handful of users, and slowly roll out the technology to the client base as part of a regular system replacement or upgrade process.

Some organizations have replaced all their member servers with Windows 2008 systems over a period of weeks or months as a preparatory step to eventually migrate to a Windows 2008 Active Directory structure.

Migrating from Windows 2000/2003 Active Directory to Windows Server 2008 Active Directory

For organizations that already have a Windows 2000 or 2003 Active Directory environment, migrating to Windows 2008 for Active Directory functionality can provide access to several additional capabilities that require a Windows network to be running on Windows 2008. Some of the Windows 2008 technologies that require implementation of the Windows 2008 Active Directory include Network Policy and Access Services, Windows 2008 Group Policy enhancements, and the full Windows 2008 Distributed File System.

Fortunately, organizations that already have Windows 2000 or 2003 Active Directory in place have completed the hard part of the Active Directory implementation process. Effectively, Windows 2008 uses the same Active Directory organizational structure that was created with Windows 2000 and 2003, so forests, domain trees, domains, organizational units, sites, groups, and users all transfer directly into Windows 2008 Active Directory. If the organizational structure in Windows 2000/2003 meets the needs of the organization, the migration to Windows 2008 is predominantly just the insertion of a Windows 2008 global catalog server into the existing Windows 2000 or 2003 Active Directory.

Of course, planning, system backup, and prototype testing—covered in Chapter 16, "Migrating from Windows 2000/2003 to Windows Server 2008"—help minimize migration risks and errors and lead to a more successful migration process. However, the migration process from Windows 2000/2003 to Windows 2008 is a relatively easy migration path for organizations to follow.

Versions of Windows Server 2008

Windows 2008 comes in the same release versions as the more recent server version releases from Microsoft with the addition of a Server Core version that provides a lighter GUI-less version of Windows 2008. The main versions of Windows 2008 include Windows

Server 2008, Standard Edition; Windows Server 2008, Enterprise Edition; Windows Server 2008, Datacenter Edition; Windows Web Server 2008; and Windows 2008 Server Core.

Windows Server 2008, Standard Edition

The Windows Server 2008, Standard Edition is the most common server version of the operating system. Unlike previous versions of Windows Server where basic functions and scalability for memory and processor support was limited to only the Enterprise or Datacenter Editions of the operating system, Windows Server 2008, Standard Edition is now the default version deployed by organizations.

With both 32-bit and x64-bit versions available, a basic Windows Server 2008 x64-bit Standard Edition system supports up to four core processors and 32GB of memory (a 32-bit Standard Edition system supports up to four core processors and 4GB of memory) and supports all of the server roles available in Windows 2008, with the exception of clustering and Active Directory Federation Services.

The Standard Edition is a good version of the operating system to support domain controllers, utility servers (such as DNS or DHCP), file servers, print servers, media servers, SharePoint servers, and so on. Most organizations, large and small, find the capabilities of the Standard Edition sufficient for most network services. See Chapter 34, "Capacity Analysis and Performance Optimization," for recommendations on choosing and tuning a Windows 2008 system that is right for its intended purpose.

Windows Server 2008, Enterprise Edition

With the Windows Server 2008, Standard Edition taking on the bulk of network services, the Windows Server 2008, Enterprise Edition is really focused on server systems that require extremely large-scale processing and memory capabilities as well as clustering or Active Directory Federation Services. From the basis of scalability of processing and memory capacity, applications like Windows virtualization or enterprise-class Exchange 2007 or SQL 2008 servers would benefit from the capabilities of the Enterprise Edition of Windows 2008.

Any time an organization needs to add clustering to its environment, the Enterprise Edition (or the Datacenter Edition) is needed. The Enterprise Edition is the appropriate version of operating system for high availability and high-processing demands of core application servers such as SQL Servers or large e-commerce back-end transaction systems.

For organizations leveraging the capabilities of Windows 2008 for Thin Client Terminal Services that require access to large sets of RAM and multiple processors, the Enterprise Edition can handle hundreds of users on a single server. Terminal Services are covered in more detail in Chapter 25.

The Enterprise Edition, with support for server clustering, can provide organizations with the nonstop networking demands of true 24/7, 99.999% uptime capabilities required in

high-availability environments. Windows Server 2008, Enterprise Edition supports a wide variety of regularly available server systems, thus allowing an organization its choice of hardware vendor systems to host its Windows 2008 application needs.

Windows Server 2008, Datacenter Edition

Windows Server 2008, Datacenter Edition is a high-end hardware version of the operating system that supports very large-scale data center operations. The Datacenter Edition supports organizations that need more than eight core processors. The Datacenter Edition is focused at organizations that need scale-up server technology to support a large central-ized data warehouse on one or limited numbers of server clusters.

As noted in Chapter 34 on performance and capacity analysis, an organization can scaleout or scale-up its server applications. Scale-out refers to an application that performs better when it is distributed across multiple servers, whereas scale-up refers to an application that performs better when more processors are added to a single system. Typical scale-out applications include web server services, electronic messaging systems, and file and print servers. In those cases, organizations are better off distributing the application server functions to multiple Windows Server 2008, Standard Edition or Enterprise Edition systems, or even Windows Web Server 2008 systems. However, applications that scale-up, such as e-commerce or data warehousing applications, benefit from having all the data and processing on a single server cluster. For these applications, Windows Server 2008, Datacenter Edition provides better centralized scaled performance as well as the added benefit of fault tolerance and failover capabilities.

NOTE

The Windows Server 2008, Datacenter Edition is sold only with proprietary hardware systems, so an organization cannot buy the Datacenter Edition software and build or configure its own 32-way multiprocessor system. The Datacenter Edition is developed and tested by a consortium of hardware vendors to strict standards for performance, reliability, and supportability.

Windows Web Server 2008

The Windows Web Server 2008 edition is a web front-end server version of the operating system focused on application server needs that are dedicated to web services requirements. Many organizations are setting up simple web servers as front ends to database servers, messaging servers, or data application server systems. Windows Web Server 2008 edition can be used as a simple web server to host application development environments or can be integrated as part of a more sophisticated web farm and web services environment that scales to multiple load-balanced systems. The Windows Server 2008 operating

system has significant improvements in scalability over previous versions of the Windows operating system, and an organization can license multiple web services systems at a lower cost per server to provide the scalability and redundancy desired in large web farm environments.

NOTE

For organizations looking to purchase the Windows Web Server edition to set up as a very low-cost file and print server or utility server (DNS, DHCP, domain controller), the Web edition does not provide traditional multiuser file or print access or utility services. You need to purchase the Windows Server 2008, Standard Edition to get capabilities other than web services.

Windows Server 2008 Server Core

New to Windows 2008 is a Server Core version of the operating system. Windows 2008 Server Core, shown in Figure 1.3, is a GUI-less version of the Windows 2008 operating system. When a system boots up with Server Core installed on it, the system does not load up the normal Windows graphical user interface. Instead, the Server Core system boots to a logon prompt, and from the logon prompt the system drops to a DOS command prompt. There is no Start button, no menu, no GUI at all.

👞 Administrator: D:\Windows\system32\cmd.exe	_ 🗆 ×
D:\Windows>	<u>^</u>
	000
	-

FIGURE 1.3 Windows 2008 Server Core.

Server Core is not sold as a separate edition, but rather as an install option that comes with the Standard, Enterprise, Datacenter, and Web Server Editions of the operating system. So, when you purchase a license of Windows Server 2008, Standard Edition, the DVD has both the normal Standard Edition code plus a Windows 2008 Standard Edition Server Core version.

The operating system capabilities are limited to the edition of Server Core being installed, so a Windows Server 2008, Enterprise Edition Server Core server has the same memory and processor limits as the regular Enterprise Edition of Windows 2008.

Server Core has been a great version of Windows for utility servers such as domain controllers, DHCP servers, DNS servers, IIS web servers, or Windows virtualization servers being that the limited overhead provides more resources to the applications running on the server, and by removing the GUI and associated applications, there's less of a security attack footprint on the Server Core system. Being that most administrators don't play Solitaire or use Media Player on a domain controller, those are applications that don't need to be patched, updated, or maintained on the GUI-less version of Windows. With fewer applications to be patched, the system requires less maintenance and management to keep operational.

What's New and What's the Same About Windows Server 2008?

From a Microsoft marketing perspective, Windows 2008 could be said to be faster, more secure, more reliable, and easier to manage. And it is true that the Windows 2008 operating system has all these capabilities. However, this section notes specifically which changes are cosmetic changes compared with previous Windows operating systems and which changes truly improve the overall administrative and end-user experience due to improvements in the operating system.

Visual Changes in Windows Server 2008

The first thing you notice when Windows 2008 boots up is the new Windows Vista-like graphical user interface (GUI). This is obviously a simple cosmetic change to standardize the current look and feel of the Windows operating systems. Just like with Windows Vista, a user can switch the new Windows GUI to look like the classic mode, and because most administrators have worked with Windows 2000/2003 for a long time, many tend to switch off the Vista GUI and configure the system to look like the classic version. It makes no difference whether the new GUI or the classic GUI is enabled; all the features and functions of the Windows 2008 operating system are the same in either mode.

Continuation of the Forest and Domain Model

Windows 2008 also uses the exact same Active Directory forest, domain, site, organizational unit, group, and user model as Windows 2000/2003. So if you liked how Active Directory was set up before, it doesn't change with Windows 2008 Active Directory. Even the Active Directory Sites and Services, Active Directory Users and Computers (shown in Figure 1.4), and Active Directory Domains and Trusts administrative tools work exactly the same.

There are several changes to the names of the Active Directory services as well as significant improvements within Active Directory that are covered in the section "Changes in Active Directory" a little later in this chapter.

Active Directory Users and Computers					
File Action View Help					
(=) 2 m 1 1 2 2 8 1 3 2 8 7 2 3.					
Active Directory Users and Comput Active Directory Users and Comput Saved Queries Computers Beddin	Name Builtin Computers Domain Cont ForeignSecur SeFO	Type builthOomain Container Organizational Container Organizational Container	Description Default container for upgr Default container for dom Default container for secu Default container for upgr	1	
< >					

FIGURE 1.4 Active Directory Users and Computers tool.

Changes That Simplify Tasks

Windows 2008 has added several new capabilities that simplify tasks. These capabilities could appear to be simply cosmetic changes; however, they actually provide significant benefits for administrative management.

Initial Configuration Tasks Application

One of these improvements is noticed soon after installing Windows 2008 on a system and booting the system up for the first time. The installation of Windows 2008 no longer requires you to enter in the server name, IP address, or administrator password when you install the operating system. It isn't until you boot the operating system and log on for the first time that you are presented with an Initial Configuration Tasks Wizard, shown in Figure 1.5, that provides you a list of tasks to perform that customizes your Windows 2008 server system. You can find more details on the Initial Configuration Tasks Wizard in Chapter 3, "Installing Windows Server 2008 and Server Core."

New Server Manager Tool

Another tool that has been added is the Server Manager console, shown in Figure 1.6. Server Manager consolidates all of the administrative management consoles from Windows 2000/2003 into a single management tool. Now instead of having to open up the Active Directory Users and Computers console, and then toggle to the DNS Server console, and load up and view information in a separate Terminal Services console, all of the information is in one screen.



FIGURE 1.5 Initial Configuration Tasks Wizard.



FIGURE 1.6 Server Manager.

Additionally, other tools like the Group Policy Management Console (GPMC) show up in Server Manager under the Features node and provide an administrator the ability to edit group policies, change policies, and apply policies from the same console that the administrator can make DNS changes, add users, and change IP configuration changes to site configuration settings.

PowerShell for Administrative Tasks

An add-in feature in Windows 2008, PowerShell is a full scripting language for administration tasks. PowerShell was first introduced in Exchange 2007 as the Exchange Management Shell (EMS) that underlies all functions of Exchange 2007 administration. PowerShell can be added to Windows 2008 as an additional feature using Server Manager.

PowerShell in Windows 2008 provides the ability for administrators to script processes, such as adding users, adding computers, or even more complicated tasks such as querying a database, extracting usernames, and then creating Active Directory users, and to provision Exchange mailboxes all from a PowerShell script.

All future server products released from Microsoft will have the PowerShell foundation built in to the core Windows 2008 operating system, thus making it easier for products running on Windows 2008 to use the same administrative scripting language. PowerShell is covered in detail in Chapter 21, "Automating Tasks Using PowerShell Scripting."

Increased Support for Standards

The release of Windows 2008 introduced several industry standards built in to the Windows operating system. These changes continue a trend of the Windows operating system supporting industry standards rather than proprietary Microsoft standards. One of the key standards built in to Windows 2008 is IPv6.

Internet Protocol version 6 (or IPv6) is the future Internet standard for TCP/IP addressing. Most organizations support Internet Protocol version 4 (or IPv4). Due to the Internet numbering scheme running out of address space in its current implementation of addressing, Internet communications of the future need to support IPv6, which provides a more robust address space.

Additionally, IPv6 supports new standards in dynamic addressing and Internet Protocol Security (IPSec). Part of IPv6 is to have support for the current IPv4 standards so that dual addressing is possible. With Windows 2008 supporting IPv6, an organization can choose to implement a dual IPv6 and IPv4 standard to prepare for Internet communications support in the future. IPv6 is covered in detail in Chapter 10.

Changes in Active Directory

As noted earlier in this chapter, Active Directory in Windows 2008 hasn't changed to the point where organizations with solid Active Directory structures have to make changes to their directory environment. Forests, domains, sites, organizational units, groups, and

users all remain the same. There are several improvements made in Active Directory and the breadth of functionality provided by directory services in Windows 2008.

The changes made in Active Directory are captured in the name changes of directory services as well as the introduction of a Read-Only Domain Controller service.

Renaming Active Directory to Active Directory Domain Services

In Windows 2008, Active Directory has been renamed to Active Directory Domain Services (AD DS). Active Directory Domain Services refers to what used to be just called Active Directory in the past with the same tools, architectural design, and structure that Microsoft introduced with Windows 2000 and Windows 2003.

The designation of Domain Services identifies this directory as the service that provides authentication and policy management internal to an organization where an organization's internal domain controls network services.

For the first time, AD DS can be stopped and started as any other true service. This facilitates AD DS maintenance without having to restart the domain controller in Directory Services Restore Mode.

Renaming Active Directory in Application Mode to Active Directory Lightweight Directory Service

Another name change in the directory services components from Microsoft is the renaming of Active Directory in Application (ADAM) to Active Directory Lightweight Directory Services (AD LDS). ADAM has been a downloadable add-in to Windows 2003 Active Directory that provides a directory typically used in organizations for nonemployees who need access to network services. Rather than putting nonemployees into the Active Directory, these individuals, such as contractors, temporary workers, or even external contacts such as outside legal counsel, marketing firms, and so on, have been put in ADAM and given rights to access network resources such as SharePoint file libraries, extranet content, or web services.

AD LDS is identical to ADAM in its functionality, and provides an organization options for enabling or sharing resources with individuals outside of the organizational structure. With the name change, organizations that didn't quite know what ADAM was before have begun to leverage the Lightweight Directory Services function of Active Directory for more than resource sharing but also for a lookup directory resource for clients, patients, membership directories, and so on. Active Directory Lightweight Directory Services is covered in detail in Chapter 8, "Creating Federated Forests and Lightweight Directories."

Expansion of the Active Directory Federation Services

That leads to the third Active Directory service called Active Directory Federation Services, or AD FS. Active Directory Federation Services was introduced with Windows 2003 R2 edition and continues to provide the linking, or federation, between multiple Active

Directory forests, or now with Windows 2008 Active Directory Federation Services, the ability to federate between multiple Active Directory Domain Services systems.

Effectively, for organizations that want to share information between Active Directory Domain Services environments, two or more AD DS systems can be connected together to share information. This has been used by organizations that have multiple subsidiaries with their own Active Directory implemented to exchange directory information between the two organizations. And AD FS has been used by business trading partners (suppliers and distributors) to interlink directories together to be able to have groups of users in both organizations easily share information, freely communicate, and easily collaborate between the two organizations.

Active Directory Federation Services is covered in detail in Chapter 8.

Introducing the Read-Only Domain Controller

Another change in Active Directory in Windows 2008 is the addition of a Read-Only Domain Controller, or RODC. The RODC is just like a global catalog server in Active Directory used to authenticate users and as a resource to look up objects in the directory; however, instead of being a read/write copy of the directory, an RODC only maintains a read-only copy of Active Directory and forwards all write and authentication requests to a read/write domain controller.

RODCs can also be configured to cache specified logon credentials. Cached credentials speed up authentication requests for the specified users. The cached credentials are stored in cache on the RODC system, not every object in the entire global catalog. If the RODC is shut down or powered off, the cache on the RODC is flushed, and the objects in cache are no longer available until the RODC connects back to a global catalog server on the network.

The RODC is a huge advancement in the area of security being that a RODC cannot be compromised in the same manner that a global catalog server can be in the event of a physical theft of a domain server. Organizations that require the functionality of a global catalog server for user authentication that have the global catalog server in an area that is not completely secure, such as in a remote office, in a branch office location, or even in a retail store outlet can instead put a RODC in the remote location.

Windows Server 2008 Benefits for Administration

Windows 2008 provides several new benefits that help organizations better administer their networking environment. These new features provide better file and data management, better performance monitoring and reliability tracking tools to identify system problems and proactively address issues, a new image deployment tool, and a whole new set of Group Policy Objects that help administrators better manage users, computers, and other Active Directory objects.

Improvements in the Group Policy Management

Windows 2008 introduces over 800 new Group Policy Objects specific to Windows 2008 and Windows Vista, along with several new components that expand on the core capabilities of Group Policy management that have been part of Windows 2000/2003 Active Directory. The basic functions of Group Policy haven't changed, so the Group Policy Object Editor (gpedit) and the Group Policy Management Console (GPMC) are the same, but with more options and settings available.

As mentioned earlier, the Group Policy Management Console can either be run as a separate MMC tool, or it can be launched off the *Features* branch of the Server Manager console tree, as shown in Figure 1.7. Group policies in Windows 2008 provide more granular management of local machines, specifically having policies that push down to a client that are different for administrator and nonadministrator users.

🛃 Group Policy Management	<u></u>
File Action View Window	Help
Group Policy Management Group Policy Management Group Policy Management Group Policy Commission Group Policy Obje Group Policy Obje Group Policy Obje Group Policy Obje Group Policy Modeling Group Policy Results	Default Domain Controllers Policy Scope Details Secope Details Delplay links in this location: companyabc.com The following sites, domains, and OUs are linked to this GPO:
a	Ad Remove Properties WMI Filtering This GPO is linked to the following WMI filter: Incone> Open

FIGURE 1.7 Group Policy Management Console.

Additionally, applications can now query or register with a network location awareness service within Group Policy management, which provides the identity where a user or computer object resides. As an example, a policy can be written that allows a user access to applications and files if they are on a local network segment, but blocks the user from accessing the same content when they are on a remote segment for security and privacy reasons. This addition to group policies adds a third dimension to policies so that now administrators can not only define who and what someone has access to, but also limit their access based on where they are.

Group policies are covered in detail in Chapter 27, "Group Policy Management for Network Clients," as well as in Chapter 19, "Windows Server 2008 Group Policies and Policy Management."

NOTE

When running the Group Policy Management Console to manage a Windows 2008 Active Directory environment, run the GPMC tool from a Windows 2008 server or a Windows Vista client system to have access to all of the editable objects available. If you run the GPMC tool from a Windows 2003 server or Windows XP client, you will not see all of the features nor have full access to edit all objects available.

This is because Windows 2008 now supports new template file formats (ADMX and ADML) that are only accessible from Windows 2008 and Windows Vista systems.

Introducing Performance and Reliability Monitoring Tools

Windows 2008 introduces new and revised performance and reliability monitoring tools intended to help network administrators better understand the health and operations of Windows 2008 systems. Just like with the Group Policy Management Console, the new Reliability and Performance Monitor shows up as a feature in the Server Manager console. By clicking on the Performance Diagnostic Console, the tool shows up in the right pane, as shown in Figure 1.8.

🛱 Reliability and Performance Monitor						
File Action View Favorites	Window Help					-151×1
Relability and Performance Monitoring Tools Performance Monitor Relability Monitor Data Collector Sets Ouser Defined System Event Trace Sessions Startup Event Trace Sess Reports Reports	Resource Overview					
🛨 🔂 System	CPU	14%	100% N	laximum Frequency		▽
	Disk	0 KB/sec	📕 47% Hi	ghest Active Time		▽
	Network	III 3 Kbps	📕 0% Net	work Utilization		▽
	Memory	0 Hard Faults/see	📕 34% Us	ed Physical Memory		▽
	Learn More					
	Resource V Performance Data Collect	iew Help te Monitor Help ttion Help	Create a E Monitor S Schedule	Data Collector Set and system Activity with Pe and Manage Data	Diagnosis Report rformance Monitor	
)					•

FIGURE 1.8 Windows Reliability and Performance Monitor.

The new tool keeps track of system activity and resource usage and displays key counters and system status on screen. The Reliability Monitor diagnoses potential causes of server instability by noting the last time a server was rebooted, what patches or updates were applied, and chronologically when services have failed on the system so that system faults can potentially be traced back to specific system updates or changes that occurred prior to the problem.

By combining what used to be three to four tools into a single console, administrators are able to look at system performance, operational tasks, and historical event information in their analysis of a server problem or system operations instability. You can find more details on performance and reliability monitoring in Chapter 34.

Leveraging File Server Resource Manager

File Server Resource Manager (FSRM) was a feature pack add-in to Windows 2003 R2 and has been significantly improved with the release of Windows 2008. FSRM is a quota management system of files on network shares across an enterprise. Rather than allowing employees to copy the entire content of their laptop to a network, or potentially back up their MP3 audio files onto a network, FSRM provides the ability to not only limit the amount of content stored on network shares, but also to set quotas (or limit storage altogether) on certain file types. So, a user could be limited to store 200GB of files on a network share, but of that limit, only 2GB can be allocated to MP3 files.

FSRM, shown in Figure 1.9, in Windows 2008 has been improved to allow the nesting of quotas to ensure the most restrictive policy is applied. Quotas can also transcend subfolders, so as new folders are created, or as policies are applied at different levels in a folder hierarchy, the policies still apply, and the rules are combined to provide varying levels of quota allocation to user data. Additionally, quotas are now based on actual storage, so if a file is compressed when stored, the user will be able to store more files within their allocated quota.

File Server Resource Manager is covered in detail in Chapter 28.

Introduction of Windows Deployment Services

Windows 2008 introduces a new tool called Windows Deployment Services (WDS), which is effectively an updated version of the Remote Installation Service (RIS) that has been available for the past several years. Unlike RIS, which was focused on primarily scripted installations and client images, WDS can distribute images of Windows Vista clients or Windows 2008 servers in a significantly more flexible and modifiable deployment process.

Like with RIS, Windows Deployment Services allows a client system to initiate a Preboot Execution Environment (PXE), effectively "booting" to the WDS server to see a list of images that can be deployed on the system. Alternately, an organization can create a Windows PE boot disc and have an image initiated from a CD or DVD.

With Windows 2008 and Windows Vista, the image can be created in Windows Imaging (WIM) format, which allows for the injection of patches, updates, or even new code to a WIM file without even booting the image file. This provides the organization with more than just static images that get pushed out like in RIS, but rather a tool that provides ongoing and manageable updates to image files.



FIGURE 1.9 File Server Resource Manager.

WDS also supports the imaging of Windows 2003 servers and Windows XP client systems in the same manner that RIS did in terms of pushing out images or using an unattend script file to send images to systems.

Windows Deployment Services is covered in detail in Chapter 26, "Windows Server Administration Tools for Desktops."

Improvements in Security in Windows Server 2008

Significantly more than just cosmetic updates are the security enhancements added to Windows 2008. As organizations are struggling to ensure their environments are secure, employees can depend on information privacy and content is protected for regulatory compliance reasons; having the tools to secure the environment is critical.

Enhancing the Windows Server 2008 Security Subsystem

Part IV of this book, "Security," is focused on security in the different core areas. Chapter 13 addresses core security subsystems of Windows 2008 as it relates to server systems. This includes the basics of server hardening, patching, and updating but also extends into new server security areas added to Windows 2008, such as device control level security, wireless access security, and Active Directory Rights Management Services (RMS). Windows 2008 has continued the "secure by default" theme at Microsoft and no longer installs components like Internet Information Services (IIS) by default. The good part about it is that components that are not core to the operation of a server are not installed on the system; however, it means every time you install software, you need to add basic components

and features. Getting to remember what has to be installed, configured, or made operational is important as servers are being built and added to a Windows Active Directory environment.

Transport Security Using IPSec and Certificate Services

Chapter 14, "Transport-Level Security," addresses site-to-site and server-to-server security, addressed through the implementation of IPSec encryption. Not new to Windows, IPSec has finally gotten several new Group Policy management components added to aid in the implementation and management of IPSec in the enterprise. Also not new to Windows but something that has been greatly enhanced is Microsoft's offering around Public Key Infrastructure (PKI), specifically Certificate Services. It seems like everything security related is somehow connected to certificates, whether that is file encryption using Encrypting File System (EFS), email encryption using S/MIME, remote mobile device synchronization using certificate access, or transport security using IPSec. Everything needs a certificate, and the ability of an organization to easily create and manage certificates is the focus of Chapter 14.

Security Policies, Policy Management, and Supporting Tools for Policy Enforcement

Completely new to Windows 2008 and a major focus for organizations are security policies and policy management around security systems. It used to be we would just lock down systems, make sure they were secure by default, and use our best judgment and best effort to secure a network. However with laws and regulations, or even human resource departments getting involved in information security, the root of all IT security practices fall on having set *security policies* defined so that IT can implement technologies to address the organization policies around information security. This is covered in detail in Chapter 15, "Security Policies, Network Policy Server, and Network Access Protection."

Chapter 15 goes beyond the policies and common best practices around policy management in an enterprise, and also digs into the underlying technologies that help organizations turn security policies into IT-managed technology services. Tools like the Network Policy Server in Windows 2008 allow policies to be defined, and the Network Policy Server enforces those policies, specifically around remote logon access, access over wireless network connections, or the integration of Network Access Protection (NAP) in querying a device and making sure the device (desktop, laptop, or mobile device) has the latest patches, updates, and antivirus software dictated by management to ensure a device is secure.

Improvements in Windows Server 2008 for Better Branch Office Support

Windows 2008 has greatly enhanced the technology offerings that provide better IT services to organizations with remote offices or branch offices. Typically, a remote or branch office has limited IT support or at least the site needs to have the same functionality and reliability as the main corporate or business office but without the budget to have

lots of redundant hardware and devices for full operational support. With the new Windows 2008 branch office resources, a remote location can now have high security, high performance, access to data without significant latency, and operational capabilities even if the remote site is dropped off the network due to a WAN or Internet connection problem.

The tools and technologies new or improved in Windows 2008 include Read-Only Domain Controllers, BitLocker Drive Encryption, distributed file server data replication, and distributed administration.

Details on the new technologies built in to Windows 2008 that better support remote and branch offices are covered in Chapter 32.

Read-Only Domain Controllers for the Branch Office

As covered in the section "Introducing the Read-Only Domain Controller" earlier in this chapter, the RODC provides a copy of the Active Directory global catalog for logon authentication of select users and communications with the Active Directory tree without having the security exposure of a full global catalog server in the remote location. Many organizations concerned with distributed global catalog servers chose to not place a server in a remote location, but rather kept their global catalog and domain controllers centralized. What this meant for remote and branch offices is that all logon authentication had to go across the WAN or Internet connection, which could be very slow. And in the event of a WAN or Internet connection failure, the remote or branch office would be offline because users could not authenticate to the network and access network resources until the WAN or Internet connection was restored.

Read-Only Domain Controllers provide a way for organizations to distribute authentication and Active Directory access without increasing their security risk caused by the distribution of directory services.

BitLocker for Server Security

BitLocker is a technology first introduced with Windows Vista that provides an organization the ability to do a full partition encryption of all files, documents, and information stored on the encrypted partition. When BitLocker was first introduced in Windows 2008 as a server tool, it was hard to understand why a server would need to have its drive volume encrypted. It made sense that a laptop would be encrypted in the event the laptop is stolen—so that no one could get access to the data on the laptop hard drive. However, when considering that servers are placed in remote locations—many times not in a locked server rack in a locked computer room but rather sitting in a closet or even under a cash register in the situation of a retail store with a server acting as the point-of-sale system servers with sensitive data are prevalent in enterprise environments.

So BitLocker provides encryption of the volume of a Windows 2008 server, and for organizations that are concerned that the server might be physically compromised by the theft of the server or physical attack of the system, BitLocker is a great component to implement on the server system.

Distributed File System Replication

Introduced in Windows 2000, improved in Windows 2003, and now a core component of the branch office offerings in Windows 2008, Distributed File System Replication (DFSR) allows files to be replicated between servers, effectively providing duplicate information in multiple locations. Windows 2008 has a much improved Distributed File System than what was available in Windows 2000/2003. In most organizations, files are distributed across multiple servers throughout the enterprise. Users access file shares that are geographically distributed but also can access file shares sitting on several servers in a site within the organization. In many organizations, when file shares were originally created years ago, server performance, server disk capacity, and the workgroup nature of file and print server distribution created environments in which those organizations had a file share for every department and every site. Thus, files have typically been distributed throughout an entire organization across multiple servers.

Windows 2008 Distributed File System Replication enables an organization to combine file shares to fewer servers and create a file directory tree not based on a server-by-server or share-by-share basis, but rather an enterprisewide directory tree. This allows an organization to have a single directory spanning files from multiple servers throughout the enterprise.

Because the DFSR directory is a logical directory that spans the entire organization with links back to physical data, the actual physical data can be moved without having to make changes to the way the users see the logical DFS directory. This enables an organization to add or delete servers, or move and consolidate information however it works best within the organization.

For branch office locations, DFSR allows for data stored on a file server in a remote location to be trickled back to the home office for nightly backup. Instead of having the remote location responsible for data backup, or the requirement of an organization to have tape drives in each of its branch offices, any data saved on the branch office can be trickle replicated back to a share at the main office for backup and recovery.

Or if the main office has data that it wants to push out to all remote offices, whether that is template files, company policy documents, standard company materials, or even shared data that a workgroup of users needs to access and collaborate on, DFSR provides the ability to push data out to other servers on the network. Users with access rights to the data no longer have to go across a WAN connection to access common data. The information is pushed out to a server that is more local to the user, and the user accesses the local copy of the information. If any changes are made to remote or centralized copies of data, those changes are automatically redistributed back to all volumes storing a copy of the data.

Distributed File Server Replication is covered in detail in Chapter 28.

Improvements in Distributed Administration

Lastly, for remote or branch offices that do have IT personnel in the remote locations, administration and management tasks have been challenging to distribute proper security rights. Either remote IT personnel were given full domain administrator rights when they should only be limited to rights specific to their site, or administrators were not given any administrative rights because it was too difficult to apply a more limiting role.

Windows 2008 Active Directory has now defined a set of rights specific to branch office and remote site administrators. Very similar to *site administrators* back in the old Exchange Server 5.5 days where an administrator was able to add users, contacts, and administer local Exchange servers, now network administrators in Active Directory can be delegated rights based on a branch or remote site role. This provides those administrators the ability to make changes specific to their branch location. This, along with all of the other tools in Windows 2008 specific to branch office and remote office locations, now provides better IT services to organizations with multiple offices in the enterprise.

Improvements for Thin Client Terminal Services

Windows 2008 has seen significant improvements in the Terminal Services capabilities for thin client access for remote users and managed users in the enterprise. What used to require third-party add-ons to make the basic Windows 2000 or 2003 Terminal Services functional, Microsoft has included those technologies into Windows 2008. These technologies include things such as the ability to access Terminal Services using a standard Port 443 SSL port rather than the proprietary Port 3389, or the ability to publish just specific programs instead of the entire desktop, and improvements in allowing a client to have a larger remote access screen, multiple screens, or to more easily print to remote print devices.

All of these improvements in Windows 2008 Terminal Services have made Terminal Services one of the easiest components to add to an existing Windows 2003 Active Directory to test out the new Windows 2008 capabilities, especially because the installation of a Windows 2008 Terminal Services system is just the addition of a member server to the domain and can easily be removed at any time.

All of these new improvements in Windows 2008 Terminal Services are covered in Chapter 25.

Improvements in RDP v6.x for Better Client Capabilities

The first area of significant improvement in Windows 2008 Terminal Services can be addressed in the update to the Remote Desktop Protocol (RDP) v6.x client, shown in Figure 1.10.

🔁 Remote D	esktop Conne	ction		_ 🗆 🗵
A	Remote Conne	Desktop ection		
General Dis	play Local Ret ngs Enter the name of Computer: [t User name: No You will be asked Allow me to s	tources Programs f the remote comp a.companyabc.com one specified d for credentials wh ave credentials	s Experience	Advanced
Connection	settings Save the current saved connectio Save	connection setting n. Save As	is to an RDP file	e or open a Open
	Connect	Cancel	Help	Options <<

FIGURE 1.10 Remote Desktop Protocol client for Terminal Services.

The new RDP client provides the following:

- Video support up to 4,096x2,048—Users can now use very large monitors across an RDP connection to view data off a Windows 2008 Terminal Services system.
- Multimonitor support—Users can also have multiple monitors supported off a single RDP connection. For applications like computer-aided design (CAD), graphical arts, or publishing, users can view graphical information on one screen and text information on another screen at the same time.
- Secured connections—The new RDP client now provides for a highly encrypted remote connection to a Terminal Services system through the use of Windows 2008 security. Organizations that need to ensure their data is protected and employee privacy is ensured can implement a highly secured encrypted connection between a Windows 2008 Terminal Services system and the remote client.

Terminal Services Web Access

Also new to Windows 2008 Terminal Services is a new role called Terminal Services Web Access, or TSWA. Terminal Services Web Access allows a remote client to access a Terminal Services session without having to launch the RDP 6.x client, but instead connect to a web page that then allows the user to log on and access their session off the web page. This simplifies the access method for users where they can just set a browser favorite to link them to a web URL that provides them Terminal Services access.

NOTE

Terminal Services Web Access still requires the client system to be a Windows XP, Windows Vista, Windows 2003, or Windows 2008 server system to connect to a Terminal Services session. A browser user cannot be running from an Apple Macintosh or Linux system and access Terminal Services Web Access. For non-Windows-based web clients, third-party vendors like Citrix Systems provides connector support for these types of devices.

Terminal Services Gateway

Terminal Services Gateway (TS Gateway) is a new addition to Windows 2008 Terminal Services and provides the connectivity to a Terminal Services session over a standard Port 443 SSL connection. In the past, users could only connect to Windows Terminal Services using a proprietary Port 3389 connection. Unfortunately, most organizations block nonstandard port connections for security purposes, and, thus, if a user was connected to an Internet connection at a hotel, airport, coffee shop, or other location that blocked nonstandard ports, the user could not access Terminal Services.

Now with Terminal Services Gateway, the remote user to the Terminal Services Gateway connection goes over Port 443 just like surfing a secured web page. Because of the use of SSL in web page access (any time someone accesses a web page with https://), effectively now a user can access Windows 2008 Terminal Services from any location.

Terminal Services Remote Programs

Lastly, another new server role added to Windows 2008 is called Terminal Services Remote Programs (TS Remote Programs). Terminal Services Remote Programs allows administrators to "publish" certain applications for users to access. These applications could be things like Microsoft Outlook, Microsoft Word, the company's time sheet tracking software, or a customer relationship management (CRM) program. Instead of giving users full access to a full desktop session complete with a Start button and access to all applications on the session, an organization can just publish a handful of applications that it allows for access.

Leveraging group policies and Network Policy Server, along with Terminal Services Remote Programs, the administrators of a network can publish different groups of applications for different users. So some users might get just Outlook and Word, whereas other users would get Outlook, Word, and the CRM application. Add in to the policy component the ability to leverage network location awareness (new to Windows 2008 covered in the earlier section "Improvements in the Group Policy Management"), the administrators of the network can allow different applications to be available to users depending on whether the user is logging on to the network on the LAN or from a remote location.

Beyond just limiting users to only the programs they should have access to by policy, Terminal Services Remote Programs minimizes the overhead for each user connection because the user no longer has a full desktop running, but only a handful of applications deemed necessary for the remote user's access.

Improvements in Clustering and Storage Area Network Support

Although clustering of servers has been around for a long time in Windows (dating back to Windows NT 4.0 when it was available, but really didn't work), clustering in Windows 2008 now not only works, but also provides a series of significant improvements that actually make clustering work a whole lot better.

As IT administrators are tasked with the responsibility of keeping the network operational 24 hours a day, 7 days a week, it becomes even more important that clustering works. Fortunately, the cost of hardware that supports clustering has gotten significantly less expensive; in fact, any server that meets the required specifications to run Windows Server 2008, Enterprise Edition can typically support Windows clustering. The basic standard for a server that is used for enterprise networking has the technologies built in to the system for high availability. Windows Server 2008, Enterprise Edition or Datacenter Edition is required to run Windows 2008 clustering services.

Clustering is covered in detail in Chapter 29, "System-Level Fault Tolerance (Clustering/Network Load Balancing)."

No Single Point of Failure in Clustering

Clustering by definition should provide redundancy and high availability of server systems; however, in previous versions of Windows clustering, a "quorum drive" was required for the cluster systems to connect to as the point of validation for cluster operations. If at any point the quorum drive failed, the cluster would not be able to failover from one system to another. Windows 2008 clustering removed this requirement of a static quorum drive. Two major technologies facilitate this elimination of a single or central point of failure, which include majority-based cluster membership verification and witness-based quorum validation.

The majority-based cluster membership allows the IT administrator to define what devices in the cluster get a vote to determine whether a cluster node is in a failed state and the cluster needs to failover to another node. Rather than assuming the disk will always be available as in the previous quorum disk model, now nodes of the cluster and shared storage devices participate in the new enhanced quorum model in Windows 2008. Effectively, Windows 2008 server clusters have better information to determine whether it is appropriate to failover a cluster in the event of a system or device failure.

The witness-based quorum eliminates the single quorum disk from the cluster operation validation model. Instead, a completely separate node or file share can be set as the file share witness. In the case of a GeoCluster where cluster nodes are in completely different locations, the ability to place the file share in a third site and even enable that file share to serve as the witness for multiple clusters becomes a benefit for both organizations with distributed data centers and also provides more resiliency in the cluster operations components.

Stretched Clusters

Windows 2008 also introduced the concept of stretched clusters to provide better server and site server redundancy. Effectively, Microsoft has eliminated the need to have cluster servers remain on the same subnet as has been the case in Windows clustering in the past. Although organizations have used virtual local area networks (VLANs) to stretch a subnet across multiple locations, this was not always easy to do and, in many cases, technologically not the right thing to do in IP networking design.

By allowing cluster nodes to reside on different subnets, plus with the addition of a configurable heartbeat timeout, clusters can now be set up in ways that match an organization's disaster failover and recovery strategy.

Improved Support for Storage Area Networks

Windows 2008 also has improved its support for storage area networks (SANs) by providing enhanced mechanisms for connecting to SANs as well as switching between SAN nodes. In the past, a connection to a SAN was a static connection, meaning that a server was connected to a SAN just as if the server was physically connected to a direct attached storage system. However, the concept of a SAN is that if a SAN fails, the server should reconnect to a SAN device that is now online. This could not be easily done with Windows 2003 or prior. SCSI bus resets were required to disconnect a server from one SAN device to another.

With Windows 2008, a server can be associated with a SAN with a persistent reservation to access a specific shared disk; however, in the event that the SAN fails, the server session can be logically connected to another SAN target system without having to script device resets that have been complicated and disruptive in disaster recovery scenarios.

Improvements in Server Roles in Windows Server 2008

The introduction of Windows 2008 added new server roles to Windows as well as enhanced existing roles based on feedback Microsoft received from organizations on features and function wish lists. Server roles are no longer installed by default on a Windows 2008 server and have to be selected for installation after the initial installation of the Windows operating system.

Some of the new or improved server roles in Windows 2008 include Internet Information Services 7.0, SharePoint Services, Rights Management Service, and Windows virtualization.

Introducing Internet Information Services 7.0

Internet Information Services 7.0 (IIS) is the seventh-generation web server service from Microsoft. Microsoft completely redesigned IIS 7.0 rather than just adding more functions and capabilities to the exact same IIS infrastructure as they have done for the past several years. The good part of the new IIS 7.0 is that it now provides organizations the ability to manage multiple web servers from a single console, rather than having to install

components and configure *each* web server individually. This requires organizations to rethink and redesign their web management tasks from pushing the same content to dozens of servers individually to a process where information is pushed to a Shared Configuration store where common information is posted and shared across all IIS 7.0 servers. Organizations can continue to post information the old way by pushing information individually to each server; however, to gain the advantage of the new IIS 7.0 services, redesigning how information gets posted should be changed to meet the new model.

The advantage of the new model of content posting is that information is stored, edited, and managed in a single location. At a designated time, the information in the single location is posted to each of the servers in the shared application hosting farm. This is a significant improvement for organizations managing and administering a lot of IIS web servers. This ensures that all servers in a farm are using the same content, have been updated simultaneously, and any changes are ensured to be propagated to the servers in the farm. Web administrators no longer have to worry that they forgot a server to update, or to stage an update at a time when each individual server could be updated in a fast enough sequence that the experience of all users was going to occur at around the same time.

IIS 7.0 is covered in detail in Chapter 12, "Internet Information Services."

Windows SharePoint Services

A significant update provided as part of the Windows 2008 client access license (CAL) is the ability to load and run Windows SharePoint Services. Now in its third generation, Windows SharePoint Services (WSS) is a document-storage management application that provides organizations with the capability to better manage, organize, and share documents, as well as provide teams of users the ability to collaborate on information. Windows SharePoint Services sets the framework from which the Microsoft Office SharePoint Services 2007 (MOSS) is built. MOSS leverages the core functionality of WSS and extends the capability into enterprise environments. WSS is the basis of document sharing and communications for organizations in the evolution of file and information communications.

Windows SharePoint Services is covered in detail in Chapter 35.

Windows Rights Management Services

Windows Rights Management Services (RMS) was available as a downloadable feature pack in Windows 2003 and is now included as an installable server role in Windows 2008. Windows Rights Management Services sets the framework for secured information sharing of data by encrypting content and setting a policy on the content that protects the file and the information stored in the file.

Organizations have been shifting to RMS rather than the old secured file folder primarily because users who should be saving sensitive information into a file folder frequently forget to save files in the folder, and thus sensitive information becomes public information. By encrypting the content of the file itself, even if a file with sensitive information is

stored in the wrong place, the file cannot be opened, and the information in the file cannot be accessed without proper security credentials to access the file.

Additionally, RMS allows the individual saving the file to set specific attributes regarding what the person would like secured about the file. As an example, a secured file in RMS can be set to not be edited, meaning that a person receiving the file can read the file, but they cannot select content in the file, copy the content, or edit the content. This prevents individuals from taking a secured file, cutting and pasting the content into a different file, and now saving the new file without encryption or security.

RMS also provides attributes to allow the person creating a file to prevent others from printing the file, and the file itself can have an expiration date so that after a given period of time, the contents of the file expire and the entire file is inaccessible.

Rights Management Services is covered in Chapter 13.

Windows Server Virtualization

A new technology that wasn't quite available at the time Windows 2008 shipped but is available on the original Windows 2008 DVD as beta code and became available for down-load after the product was formally released is Windows server virtualization (WSV), also known as Hyper-V. Hyper-V provides an organization the ability to create guest operating system sessions, like those shown in Figure 1.11, on a Windows 2008 server to get rid of physical servers, and instead make the servers available as virtual server sessions.



FIGURE 1.11 Windows virtualization guest sessions.

Instead of purchasing a new physical server every time a new server system needs to be placed on the network, a virtual server can be created that has all of the same operations and functions as the physical server itself. Or for organizations that are putting in place disaster recovery centers and server clustering for better server reliability and redundancy, virtualization allows the addition of these additional servers within the guest operating system space of a single server system.

Virtualization in Windows 2008 now supports 64-bit and 32-bit guest sessions, has a builtin tool that allows a snapshot of a virtual session so that the session can be protected or rolled back in the event of a guest image failure or corruption, and virtual sessions can span terabytes of disk storage and use 16GB, 32GB, or more of memory per guest session.

More details on Windows 2008 virtualization is covered in Chapter 37.

Identifying Which Windows Server 2008 Service to Install or Migrate to First

With the release of Windows 2008, organizations need to create a plan to install or migrate to Windows 2008 in a logical manner. What was covered so far in this chapter has been all of the top features, functions, and technologies built in to Windows 2008 that organizations have found as key technologies they implemented to improve technology-driven business processes.

Because Windows 2008 provides many different functions, each organization has to choose how to best implement Windows 2008 and the various networking features that meet its own needs. In small network environments with fewer than 20 to 30 users, an organization might choose to implement all the Windows 2008 features on a single server. However, in larger environments, multiple servers might be implemented to improve system performance as well as provide fault tolerance and redundancy, and, thus, a more staged implementation of core services needs to be taken.

Windows Server 2008 Core to an Active Directory Environment

For an organization that does not have Windows Active Directory already in place, that is the first place to start because Active Directory Domain Services is key to application and user authentication. For organizations that already have a fully operational Active Directory running on Windows 2000 or Windows 2003, upgrading to Active Directory Domain Services on Windows 2008 might be something that is addressed a little later in the upgrade cycle when AD DS 2008 functionality is needed.

Because Active Directory is more than a simple list of users and passwords for authentication into a network, but rather a directory that Microsoft has embedded into the policybased security, remote access security, and certificate-based security enhancements in Windows 2008, AD DS 2008 implementation does occur earlier in the migration cycle for organizations wanting to implement many of the new Windows 2008 technologies, such

as Network Policy Services, Windows Deployment Services, Terminal Services Remote Programs, and so on.

When Active Directory Domain Services is fully leveraged, an organization can have its Human Resources (HR) department add an employee to the organization's HR software. The HR software automatically creates a user in the Active Directory, generating a network logon, an email account, a voicemail account, and remote access capabilities, and then links pager and mobile phone information to the employee. Likewise, if an employee is terminated, a single change in the HR software can issue automated commands to disable the individual's network, email, remote logon, and other network functions.

Windows 2008 extends the capabilities of the Active Directory by creating better management tools, provides for more robust directory replication across a global enterprise, and allows for better scalability and redundancy to improve directory operations. Windows 2008 effectively adds in more reliability, faster performance, and better management tools to a system that can be leveraged as a true enterprise directory provisioning, resource tracking, and resource management tool. Because of the importance of Active Directory to the Windows 2008 operating system, plus the breadth of capabilities that Active Directory can facilitate, six chapters in Part II of this book are dedicated to Active Directory.

Windows Server 2008 Running Built-in Application Server Functions

As much as Active Directory tends to be one of the first things upgraded in a networking environment because so many applications require the latest Active Directory to be in place, the real business drivers for migrating to Windows 2008 typically come from the built-in application server programs that are available on Windows 2008.

Windows Server 2008 comes with several programs and utilities to provide robust networking capabilities. In addition to the basic file and print capabilities covered earlier in this chapter, Windows 2008 can provide name resolution for the network and enable high availability through clustering and fault tolerance, mobile communications for dialup and virtual private network connections, web services functions, and dozens of other application server functions.

When convincing management that an upgrade to Windows 2008 is important, the IT professional needs to sift through the technologies built in to Windows 2008 and pick those services that help an organization use technology to achieve its business initiatives. When planning the implementation of Windows 2008, a network architect needs to consider which of the server services are desired, how they will be combined on servers, and how they will be made redundant across multiple servers for business continuity failover.

For a small organization, the choice to combine several server functions to a single system or to just a few systems is one of economics. However, an organization might distribute server services to multiple servers to improve performance (covered in Chapter 34), distribute administration (covered in Chapter 18, "Windows Server 2008 Administration"), create server redundancy (covered in Chapter 29), create a disaster recovery strategy (covered in Chapter 31, "Recovering from a Disaster"), enable security (covered in Chapter 13), or to serve users in other remote site locations of the organization (covered in Chapter 32). Some of the built-in application server functions in Windows 2008 include the following:

- ► **Domain controller**—Like in previous versions of the Windows operating system, the domain controller allows users to authenticate to the domain for access to network resources.
- Global catalog server—The global catalog server is a domain controller that also stores a subset of AD DS objects from other domains in the forest. When an internal or external user with appropriate security rights wants to look at a list of Active Directory users in the forest, the global catalog server provides the list.
- ▶ DNS server—The domain name system (DNS) maintains a list of network servers and systems and their associated IP addresses, so a DNS server provides information about the devices connected to the network.
- ► DHCP server—The Dynamic Host Configuration Protocol (DHCP) assigns IPv4 and/or IPv6 network addresses to devices on the network. Windows 2008 provides the service function to facilitate DHCP addresses to network devices.
- Cluster server—When fault tolerance is important to an organization, clustering provides failover from one system to another. Windows 2008 provides the ability to link systems together so that when one system fails, another system takes over.
- ▶ Network policy server—NPS is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy. NPS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless and virtual private network (VPN) connections. NPS routes authentication and accounting messages to other RADIUS servers. It also acts as a health evaluation server for Network Access Protection (NAP).
- ► Terminal server—Instead of having a full desktop or laptop computer for each user on the network, organizations have the option of setting up simple, low-cost thin terminals for users to gain access to network resources. Windows 2008 Terminal Services allows a single server to host network system access for dozens of users.
- ▶ Remote access server—When a remote user has a desktop or laptop system and needs access to network services, Windows 2008 provides remote access services that allow the remote systems to establish a secure remote connection.
- ▶ Web server—As more and more technologies become web-aware and are hosted on web servers, Windows 2008 provides the technology to host these applications for browser-based access.
- Media server—With information extending beyond text-based word processing documents and spreadsheets into rich media such as video and audio, Windows 2008 provides a source for hosting and publishing video and audio content.
- ► Virtualization server—Windows 2008 provides the core capabilities to do server virtualization, providing the capability for an organization to consolidate physical servers into fewer host server systems, thus decreasing the total cost of IT operations.
Distributed File System (DFS) server—For the past decade, data files have been stored on file servers all around an organization. Windows 2008 provides Distributed File Systems that allow an organization to take control of distributed files into a common unified namespace.

These plus several other functions provide robust networking services that help organizations leverage the Windows 2008 technologies into solutions that solve business needs.

Windows Server 2008 Running Add-in Applications Server Functions

Although some of the newer, built-in server application functions in Windows 2008, such as Network Policy Server, server virtualization, Terminal Services Web Access, Media Server, and so on, provide key areas for organizations to select as initial areas to implement Windows 2008 technologies, other organizations might find add-in applications as being the key areas that drive an initial implementation of Windows 2008. Some of the add-in applications come from Microsoft, such as the Microsoft Exchange Server 2007 SP1 messaging system or Microsoft SQL Server 2008 database system. Other add-ins to Windows 2008 are provided by companies that provide human resource management applications; accounting software; document management tools; fax or voicemail add-ins; or other business, industry, or user productivity capabilities.

In earlier Windows Server operating systems, the core operating system provided simple logon and network connectivity functions; however, with Windows 2008, the operating system includes many core capabilities built in to the Windows 2008 operating environment. With integrated fault tolerance, data recovery, server security, remote access connectivity, web access technologies, and similar capabilities, organizations creating add-ins to Windows 2008 can focus on business functions and capabilities, not on core infrastructure reliability, security, and mobile access functionality. This off-loading of the requirement of third-party add-in organizations to implement basic networking technologies into their applications allows these developers to focus on improving the business productivity and functionality of their applications. Additionally, consolidating information routing, security, remote management, and so on into the core operating system provides a common method of communication, authentication, and access to users without having to load up special drivers, add-ins, or tools to support each and every new application.

Much of the shift from application-focused infrastructure components to core operating system-focused functionality was built in to Windows 2000 and then later enhanced in Windows 2003. There were many challenges to earlier versions of the Windows operating system; however, after being on the market for many years now, Windows 2008 add-ins have had several revisions to work through system functionality and component reliability between application and operating system. Fortunately, Windows 2008 uses the same application/operating system technology used in Windows 2003, so applications written for Windows 2003 typically need just a simple service pack update to be able to run on Windows 2008 if anything at all.

Summary

This introductory chapter was intended to highlight the new features, functions, migration tools, and management utilities in Windows Server 2008 that will help administrators take advantage of the capabilities of the new operating system. If Windows 2008 is seen as just a simple upgrade to Windows 2000/2003, an organization will not benefit from the operating system enhancements. However, when fully leveraged with the capabilities of the Windows 2008 operating system, an organization can improve services to its employees through the use of new tools and technologies built in to the operating system.

Because Windows 2008 is a relatively simple migration from existing Windows 2000 and Windows 2003 Active Directory environments, and Windows 2008 application servers can be added to existing Active Directory 2000 and 2003 domains, the migration process really is one where the IT administrators need to prioritize which Windows 2008 services to install or migrate to first, and to then plan and test the new technologies to make sure they improve IT services to the organization.

Best Practices

The following are best practices from this chapter:

- When implementing Windows 2008 for the first time, or migrating to Windows 2008 from a previous version of Windows, choose to implement the technologies in Windows 2008 that will provide the organization the most value in terms of employee productivity enhancements or regulatory compliance security improvements first.
- When considering adding a Windows 2008 server to an existing Windows 2000/2003 Active Directory environment, consider implementing things like Terminal Services Web Access, SharePoint Services, or Windows virtualization that have proven to be pretty easy to implement and provide a lot of value to organizations.
- ► To ultimately improve Windows security, tune and optimize Windows 2008 for a secured networking environment.
- ► Use Terminal Services in Windows 2008 to provide users access to local hard drives as well as to redirect the audio from a centralized Terminal Server to a remote system.
- ► Use Windows Deployment Services (WDS) to create client system images that can be quickly and easily rolled back through Group Policy.
- Windows 2008 virtualization can help organizations deploy clustering and add in disaster recovery data centers without having to add additional physical servers to the network.
- Remote and branch office locations greatly benefit from the use of Read-Only Domain Controllers, Distributed File System Replication, BitLocker security, and distributed administration tools built in to Windows 2008.

н

- Using the new Windows 2008 Server Manager can simplify the task of a network administrator trying to access information residing on different servers and in different server roles in the environment.
- ▶ It is best to run the Group Policy Management Console on a Windows 2008 or Windows Vista system to have access to all of the policy features available (compared with running GPMC on a Windows XP or Windows Server 2003 system).

Index

Symbols

% Disk Time counter, 1220 % Processor Time counter, 1219 -4 parameter Ping command, 1171 tracert command, 1173 -6 parameter Ping command, 1171 tracert command, 1173 6to4 addresses, 289 6to4 technology, 207 32-bit processors, Windows Server 2008 support, 74 50/50 failover approach, 309-310 64-bit processors, Windows Server 2008 support, 74 80/20 failover approach, 310 99.999% uptime, 1081 100/100 failover approach, 311-312 802.1x authentication, 418

A

-a parameter Arp command, 1175 Netstat command, 1175 Ping command, 1172 /a parameter (DCDiag command), 1178 A (Host) records, 258 AAAA records, 261 abbreviations for IPv6 addresses, 288 access administrative, 378-379 auditing, 388-389 to document libraries in WSS, 1253

to file systems FTP (File Transfer Protocol), 940 Services for Macintosh, 941 Services for NFS, 941 SFTP (Secure File Transfer Protocol), 941 Windows folder sharing, 940 WSS (Windows SharePoint Services), 941 WWW directory publishing, 940 granting to Terminal Servers, 809 logins restricting, 377-378 smartcards, 379 to OpsMgr. 720 physical, restricting, 377 troubleshooting, 1087-1092 Access 2007, integration with WSS, 1270-1271 access restriction (NAP), 416 access-based enumeration, 956-957 accidental deletion protection in Active Directory, 1067 account policies, Computer Configuration Windows Settings node, 872 account provisioning (ILM 2007), 232-233 accounts, Active Directory computer accounts pre-creating for WDS, 856-859 upgrading RIS images to WDS images, 859 acquisition of Virtual PC, 1314 actions in Task Scheduler, 596 task actions, 1185 Actions menu (WSS document libraries), 1254-1257 Actions pane (IIS Manager console), 334 activating Terminal Services License Server, 827-828 active directories, read-only domain services (RODC), 1114 Active Directory, 7, 13-14, 1223. See also domain controllers (DCs) adding NIS users to, 245 administering, 107 authentication modes, 110 authoritative restores, 1102-1103 backing up, 1066-1068

Cache % Hit (performance counter), 1225 Cache Page Fault Stalls/sec (performance counter), 1225 Cache Page Faults/sec (performance counter), 1225 Cache Size (performance counter), 1225 components, 111 computer accounts, pre-creating for WDS, 856-858 migration path, 858-859 upgrading RIS images to WDS images, 859 Computers folders, objects, 166 Container class objects, 166 containers, GPO administrative delegation, 578-579 cross-forest transitive trusts, 135, 143 CS (Certificate Services), 133 DDNS (Dynamic DNS), 124 design features (new), 143 designing, 139 development of, 107 DFS-R (Distributed File System Replication), 134 DNS (domain name system), 107, 123 Active Directory and foreign DNS, co-existing, 125 namespaces, 123-124 zone integration, 136 zones, comparing standard and AD-integrated, 125 domain rename tool, 135 domain trees. 109-110 domain trusts. 116-117 domains, 108-109, 865 designing, 139 fine-grained password policies, 142 namespaces, 141-142 placeholder structure, 158 renaming, 143, 160-163 special-purpose, 159-160 structure, choosing, 143-144 trusts. 140 DSAMain (database mounting tool), 134

empty-root domain model, 154-155 real-world design example, 157 selecting, 156 Exchange Server 5.5, 106 federated forests design model, 151-154 Folder icon, 172 forests, 110 trees, 150-151 functional levels, 110 GCs (global catalog servers), 114 global catalog, 114, 143, 325-326 GlobalNames DNS zones, 134 group designs, 177-178 group policies, 134 groups, 119, 168, 510 business function-based designs, 178-181 design model samples, 178 distribution groups, 169 domain local, 120, 170-171 geographical-based designs, 181-183 global, 120, 171 machine local, 120, 170 mail-enabled groups, 169-170 OUs (organizational units). comparing, 121 scopes, 170 security groups, 168-169 structure designs, 165 types of, 120 universal, 120, 171 infrastructure design. Group Policy infrastructure and, 562-563 infrastructure documentation, 703-704 Internet Information Server and Site Server, 107 Internet standards, Microsoft adoption, 108 KCC (Knowledge Consistency Checker), 188 Kerberos, 110, 188 LDAP (Lightweight Directory Access Protocol), 107, 113-114 lingering object removal, 136 managing with policies, 911-912 configuring restricted groups for domain security groups, 915

deploying software packages, 921-924 extending Group Policy functionality, 919-921 fine-grained password policies, 912-914 GPO modeling and, 926-929 managing group policies from administrative or remote workstations. 929-930 synchronous foreground refresh, 925-926 migration, 9, 33-34, 439 monitoring, 1223-1225 multiple domain model, 147-149 new features in, 16-18, 134, 448-449 NTLM (NT LAN Manager), 110 OM (operations master) roles, 114-115 organizational structure, 166 OUs (organizational units), 118, 166-167 administration, delegating, 174-175 business function-based designs, 178-179 design flexibility, 173 design model samples, 178 designs, 172-173 domain designs, 173 and domains, comparing, 118-119 geographical-based designs, 181-182 LDAP (Lightweight Directory Access Protocol), 166 objects, 166 structure, 146 structure design, 165 performance counters, 1224 placeholder domain model, 158 replication, 121, 186 collisions, 187 connection objects, 188-189 latency, 189-190 monitoring, 1224 multimaster replication, 186 Originating Writes, 123 property version numbers, 187 site link bridgeheads, 121-122 site links, 121-122

sites. 121-122 update sequence numbers, 186 replication compression disable support, 135 RODC, 211-214 schema, 112 schema attributes, deactivating, 135 security, 107, 125-126 servers, 743 services, 106 single domain model, 144-147 single forest model real-world design example, 151 trees, 150 site GPOs, 883 sites, 147, 190, 501 costs. 195 design, 198 domain controllers, promoting, 201-202 establishing, 198 ISTG, 204 KCC. 195 lingering objects, 203 link bridgeheads, 197 link bridging, 194 linked-value replication, 202 links, 192, 194, 200 multiple-site design, 199 replication compression, 203 replication schedules, 200 schema changes, 204 single-design, 199 SMTP replication, 201 subnet associations, 191, 200 topology examples, 207-210 universal group caching, 203 Windows Server 2003 improvements, 191, 201 structure, 108 subdomains, 149 TCP/IP, 107 time. 188 universal group caching, 326

universal group memberships, replicating, 135-136 Users folders, objects, 166 Windows Server 2003 domain functional level. 111 X.500 directory services, 111-112 **Active Directory Certificate Services** (AD CS), 402 CA roles in, 403 installing, 404-407 role services in, 403-404 Active Directory client certificate authentication (IIS), 362 Active Directory Domain Services (AD DS), 17.839 DNS in. 277 GlobalNames zone (GNZ), 280-281 impact of DNS, 277-278 non-Microsoft DNS implementation, 278 secondary zones, 278-279 site resolution, 278, 280 enabling for Services for NFS, 239-240 migration, 439 Active Directory Domain Services Wizard, RODC installations, 1118, 1120-1122, 1126-1129 Active Directory Federation Services (AD FS), 17, 133, 223 components of, 223-224 installing, 224-225 Web Agents, 224 wizards in, 226 Active Directory in Application Mode (ADAM), 17.218 Active Directory integration in OpsMgr, 721 Active Directory Lightweight Directory Services (AD LDS), 17, 133, 218 advantages of, 218-219 features of, 219 installing, 219-222 Active Directory Migration Tool, 461 Active Directory mode (TS Web Access deployment), 819 Active Directory Rights Management Services (AD RMS), 134, 408 installing, 409-411 requirements, 409

Active Directory Service Interfaces, 112 Active Directory Users and Computers snap-in, configuring Terminal Services, 811 Active Directory-integrated zones, 274 compared to standard DNS zones, 125 moving to application partitions, 460-461 active nodes, clustering, 999 active/active clusters, 1000 active/passive clusters, 999 ActivePerl scripting, 247 AD. See Active Directory ADAM (Active Directory in Application Mode), 17.218 Add Account Partner Wizard, 226 Add Applications Wizard, 226 Add Counters dialog box, 1163 Add Features link (Initial Configuration Tasks wizard), 88 -add parameter (Route command), 1176 Add Printer option (Windows), 527 Add Resource Partner Wizard, 226 Add Roles link (Initial Configuration Tasks wizard), 87 Add Roles Wizard, installing DNS, 254 Add-Content cmdlet (PowerShell), 674 add-in application server functions, 36 addresses. See also IPv4; IPv6 APIPA, 301-302 FODN, 298 Internet, 205 networks, 298 ADM file format. 551-552 ADM subfolder (GPOs), 540 administration, 587, 785 Active Directory, 107 Active Directory sites, 501-503 design best practices, 503 domain controllers, adding to sites, 505-506 site delegation, 509-510 site group policies, 503 site links. 502 site links, creating, 506-507, 509

sites, creating, 503-506 subnets, 502 subnets, creating, 505 administrative models, 499-501 delegated administration (GPOs), 884-885 group policies, 518 configuring, 521-523 creating, 519-521 troubleshooting, 523-525 viewing, 519 groups, 510 creating, 513 delegating control of, 514-515 distribution groups, 510 domain functionality levels, 512-513 multiple domain user administration, 512 populating, 514 scope of, 511 security groups, 510 single domain user administration, 512 in IIS 7.0, new features, 333 OUs, delegating, 174-175 with Print Management console, 525-526 adding print servers, 528 adding printers, 526-528 configuring, 526-527 custom filters, creating, 529-531 form management, 529 installing, 526 updating printer drivers, 529 of Services for NFS, 239 of Terminal Services, 833 with command-line tools, 834 disaster recovery, 835 remote management of, 835 role administration tools, 834 service packs and, 835 with Terminal Server Manager, 834 with WMI, 834 of UNIX Integration tools, 246-247

user profiles, 515 All Users profile, 517 default profiles, 516-518 local profiles, 516 mandatory profiles, 516 roaming profiles, 516 template profiles, 517 temporary profiles, 517 administration documentation, 702 Active Directory infrastructure documentation. 703-704 administration manual, 705 checklists, 703 configuration (as built) documents, 704-705 policy documents, 703 procedure documents, 702 security procedure documents, 706 server build procedure documents, 704 topology diagrams, 705 troubleshooting documents, 706 administration manual, 705 administration roles, branch offices, 1113 administration tools for Windows Media Services, 1286 administrative access, 378-379 Administrative console (Hyper-V), launching, 1322-1323 administrative consoles (OpsMgr), capacity limits, 726 administrative delegation DHCP, 313 GPOs. 577-579 administrative events (GPOs), 560-561 administrative models, 499-501 administrative tasks (GPOs) administrative delegation, 577-579 central store creating, 564-565 verifying usage of, 565-566 domain GPOs backing up and restoring, 575-577 creating, 570-571 Group Policy Modeling, 577 Group Policy Results, 577

links, creating/configuring, 571 order of processing, managing, 574 security filters, managing, 573-574 settings, viewing, 575 starter GPOs backing up and restoring, 567-570 creating, 566-567 status management, 572 WMI filters creating, 572-573 linking, 573 administrative templates (GPOs), 541, 550-553 central store, 541-542 custom templates, 553 for Windows 2000/XP/Server 2003, 551-552 for Windows Vista/Server 2008, 552-553 Administrative Tools role, 243 administrator passwords Server Core installations, changing for, 95 when to change, 635 Windows Server 2008 configurations, 84 administrator roles in IIS 7.0, 367-368 separation of (RODC), 1115 administrators, creating local group policies, 875-876 ADML file format, 552-553 ADMT 3.1 (Active Directory Migration Tool), 461 components of, 462 computer accounts, migrating, 468-470 groups, migrating, 466-467 installing, 462-463 prerequisites for, 463 user accounts, migrating, 467-468 wizards in, 470 ADMX file format, 552-553 ADMX Migrator, 559 adprep, preparing domain controllers with, 451-453 ADSI (Active Directory Service Interfaces), 112 ADSIEdit, removing phantom domain controllers, 457-458

Advanced Tools section (Server Manager roles pages), 590 Agent Action account (OpsMgr), 728 agentless exception monitoring (OpsMgr), 718 agents (OpsMgr), 719 capacity limits, 726 deployment, 723 installing, 729-731 security in, 727 alerting mechanisms, documenting, 710 alerts (OpsMgr), 716-717 alias cmdlets (PowerShell), 654-655 aliases in PowerShell, 654-655 /all parameter (lpconfig command), 1174 All Users host-specific profile (PowerShell), 660 All Users profile (PowerShell), 517, 660 all-in-one server (OpsMgr), 724 /allcompartments parameter (lpconfig command), 1174 allocating disks with Windows Server Backup, 1058-1060 hardware, compatibility testing, 491 Windows Server 2008, compatibility testing, 491 AllSigned execution policy (PowerShell), 661 alternate DHCP clients, 308 alternate hardware, complete PC restore to. 1099 -an parameter (Netstat command), 1175 analysis, processor usage, 1219 announcement files, creating, 1292 anonymous authentication (IIS 7.0), 362 antivirus programs, 389-390 on Terminal Servers, 801 APIPA (Automatic Private IP Addressing), 78, 301-302 Application Compatibility Toolkit (Microsoft), Windows Server 2008 upgrades, 89 Application Development role service (IIS 7.0), 339 application failure, troubleshooting, 1085-1086 application logs, 1153

application partitions DNS, 275 moving AD-integrated DNS zones to, 460-461 application pools (IIS Manager Connections pane), 335 application readiness, verifying for Big Bang migration, 444 application servers add-in functions, 36 built-in functions, 34-36 Windows Server 2008 as, 6-8 application service providers, Terminal Services for, 786 applications, 314 access, troubleshooting, 1092 compatibility, 473 for failover clusters deploying on, 1019-1021 selecting, 1004-1005 hosting applications, 660 included in Windows Server 2008, 7 installing, 492 on Terminal Servers, 809 inventory, 483 inventory sheets, 484 managing with WDS, 840 monitoring with Task Manager, 1147 NLB clusters, 1030 prioritizing, 485 services, compared, 483-484 shells versus, 640 Terminal Services hosted applications, planning for, 803 for Terminal Services users, 785 user requirements, 66 whether to upgrade, 44 Applications and Services Logs folder (Event Viewer), 1154 Applications tab (Task Manager window), 1147, 1194 AppManager Suite Web site, 1214 appreciation for technical resources during disaster recovery, 1083

approval for disaster recovery plan, 1049 archiving events, 1157 arguments (PowerShell), 646 Arp command, 1175 as built documentation, 704-705 ASDI, 112 ASP feature page (IIS 7.0 websites), 349 ASP.NET, IIS 7.0 features associated with, 346-348 ASP.NET impersonation (IIS 7.0), 362 ASP.NET role service (IIS 7.0), dependencies, 341 Assessment and Planning Solution Tool. 1212 assigning permissions to IIS 7.0 user accounts, 368-369 assumptions in disaster recovery, danger of, 1082 in migration documents, 60 asymmetrical encryption, 401 asynchronous zone transfer (AXFR), 267 attributes directories, 228 of schemas, deactivating, 135 audit collection services (OpsMgr), 718 audit policies, 605-606 categories and subcategories, 606-609 auditing access, file-level security, 388-389 Active Directory objects, 132 enabling for NTFS folders, 1089-1091 in SharePoint Server 2007, 1238 auditing services in IIS 7.0, 363 auditing tools, 605 audit policies, 605-606 categories and subcategories, 606-609 resource access auditing, 609-612 authentication BitLocker Drive Encryption, 1131 of FTP sites, 357 in IIS 7.0, 362-363 Network Authentication, 830 in RRAS systems, 743 EAP and PEAP authentication, 744 for L2TP/IPSec connections, 745

for PPTP connections, 744 selecting protocols, 745 Authentication feature page (IIS 7.0 websites), 349 authentication modes (Active Directory), 110 Authentication Rules feature page (IIS 7.0 websites), 349 authoritative restore of Active Directory, 1102-1103 authorization DHCP 315-316 for FTP sites, 358 Automated Deployment Services (WDS), 842 automatic DNS zone creation, 276 Automatic Private IP Addressing, 301 automatic reboots, Windows Server 2008 upgrades, 92 automatic updates, 87, 622-625 Automatic Updates client, 391 configuring, 394-396 automatically launching Hyper-V guest sessions, 1332-1333 availability, service availability, 997 Avg. Disk Queue Length counter, 1220 AXFR (asynchronous zone transfer), 267, 1227 AXFR Request Received (DNS zone transfer counter), 1227 AXFR Request Sent (DNS zone transfer counter), 1227 AXFR Response Received (DNS zone transfer counter). 1227 AXFR Success Received (DNS zone transfer counter), 1227 AXFR Success Sent (DNS zone transfer counter), 1227

B

- back-end enterprise messaging systems in failover clusters, 998 back-links in Active Directory authoritative restores, 1103 background information of networks (design
- documents), 54-55

Background Intelligent Transfer Service (BITS), 391 background section (migration documents), 60 backup and recovery process, creating for Big Bang migration, 445 backup documentation, 709-710 backup history, viewing, 1064 Backup utility (VSS), 988 backups, 1044 creating procedures for, 1051 developing strategy for, 1050-1051 DFS. 987 DHCP. 307 domain GPOs. 575-577 DVD media for. 1095 failover clusters. 1028 NLB nodes, 1039 requirements for OpsMgr, 723 starter GPOs, 567-570 strategy, 390 validating, 634 verifying, 626 VSS (Volume Shadow Copy Service), 938. 1073-1075 Windows Server 2008 installations, 79 Windows Server 2008 upgrades, 88 Windows Server Backup, 601-603, 1051 Active Directory backups, 1066-1068 backup files/folders, 1053 Certificate Services, 1068-1069 command-line utility, 1054 complete PC restore, 1099 DFS backups, 1071 DHCP backups, 1070-1071 DHCP service recovery, 1104 DNS backups, 1069 DVD backups, creating, 1062-1063 IIS backups, 1071 installing, 1054-1057 management with wbadmin.exe, 1063-1064 manual backups to remote server shares. 1060-1062 media management. 1051-1052, 1095

MMC snap-in for, 1054 options, setting, 1053-1054 role services, backing up, 1064-1073 scheduling backups, 1058-1060 System State backups, 1065 System State recovery, 1100-1104 volume recovery, 1096-1099 WINS backups, 1070 WSS backups, 1071-1073 WSS recovery, 1104-1107 balancing (load), 995 bandwidth throttling, 978 bare minimum services, identifying, 1046 **Baseline Configuration Analyzer, 1212** baselines, 711, 1169-1171 benchmark establishing, 1192-1193 workload characterizations, 1192 metric, establishing, 1191-1192 policy, establishing, 1191-1192 procedure, establishing, 1191-1192 Bash shell, 640 basic authentication (IIS 7.0), 362 basic compatibility testing, 480 basic disks, 942-943 converting to dynamic disks, 948 bcdedit.exe, 1075 BDC (Business Data Catalog), 1238 benchmark baselines establishing, 1192-1193 workload characterizations, 1192 benchmarks, websites for, 1193 Big Bang migration, 442-448 application readiness, verifying, 444 backup and recovery process, creating, 445 hardware compatibility, verifying, 444 phased approach versus, 442 prerequisites for, 443 single domain controller upgrade, 445-448 virtual domain controller rollback, 445 BIOS, configuring for guest operating system sessions, 1332 bit rates, media content, 1306

BitLocker Drive Encryption, 24-25, 1129 authentication, 1131 data volumes, 1130, 1138-1139 deployment scenarios, 1131 EFS versus, 1129 hardware requirements, 1131 installing command prompt installations, 1134 requirements for, 1130 Server Manager installations, 1133-1134 passwords, 1139 removing, 1140 system partition configuration, 1132-1133 TPM, 1130, 1135-1136 UEFI. 1130 USB keys, 1137-1138 **BITS (Background Intelligent Transfer** Service), 391 Block Policy Inheritance option (group policy configuration), 522-523 blocked PSObject information, viewing, 651 blocking GPO link inheritance, 545-546 blogs, Network Monitor, 1196 boot images adding to WDS servers, 848-850 WDS, 844 bootable media, creating with discover boot images and WAIK, 854-856 **BOOTP** (Bootstrap Protocol), 300 bootup from SANs (storage area networks), 945 startup options for, 1075 bottlenecks (performance), 1215 Bourne shell, 640 branch offices, 1111 administration role separation, 1113 BitLocker Drive Encryption, deployment scenarios, 1131 DFS. WAN utilization. 1141 domain controllers, removal/theft of, 1113 group policies, WAN utilization, 1142 IT support, 1114

Next Generation TCP/IP stacks, WAN utilization, 1140-1141 physical security, 1113 RODC, 1112 administrator role separation, 1115 benefits of, 1114-1115 credential caching, 1115 limitations of, 1117 read-only active directory domain services, 1114 read-only DNS. 1116 replication workload reduction, 1114 WAN utilization, 1140 SMB, WAN utilization, 1142-1143 support in Windows Server 2008, 23-26 bridgeheads (site links), 197 Active Directory replication, 121-122 bridging AD site links, 194 broadcast publishing, compared to on-demand publishing, 1295 broadcast publishing points, playlists, 1301 broadcasting captured broadcasts preparing, 1307 sessions, capturing, 1308-1309 live broadcasts, 1305 initiating, 1305-1307 pulling content, 1306-1307 pushing content, 1306 playlist broadcasting broadcast publishing points, 1301 configuring, 1300-1302 on-demand publishing points, 1300 starting playlists, 1302 real-time live starting, 1293 Windows Media Services configuration, 1291-1292 single video, 1294 configuring, 1294-1296 publishing points, 1296 browser-based forms in SharePoint Server 2007, 1238

budget compatibility testing, 479 estimating design documents, 54-55 migration documents, 62 building labs, 63 built-in application server functions, 34-36 built-in toolsets for capacity analysis (Task Manager), 1194-1195 Business Data Catalog (BDC), 1238 business function-based designs, 178-181 business goals and objectives, identifying, 40 business unit/departmental goals, 42-43 high-level business goals, 41 business owners, synchronizing disaster recovery with, 1082 business unit goals, identifying, 42-43

С

/c parameter (DCDiag command), 1178 C shell, 640 CA (Certificate Authority), 402-403 cabinet files creating starter GPOs from, 567 saving starter GPOs as, 568 Cache % Hit (Active Directory performance counter), 1225 Cache Page Fault Stalls/sec (Active Directory performance counter), 1225 Cache Page Faults/sec (Active Directory performance counter), 1225 Cache Size (Active Directory performance counter), 1225 caching credentials (RODC), 1115 caching universal group, 203, 326 caching-only DNS servers, 262 calendar events (WSRM), 1211 Calendar list in WSS, 1262-1264 CALs (client access licenses) installing, 828-829 types of, 804

Canonical Name (CNAME) records, 261 capacity analysis, 1189 % Disk Time counter, 1220 % Processor Time counter, 1219 AppManager Suite website, 1214 Assessment and Planning Solution Tool, 1212 Avg. Disk Queue Length, 1220 benchmark baselines, establishing, 1192-1193 benefits of, 1190 bottlenecks, 1215 Computer Measurement Group website, 1193 Interrupts/sec counter, 1219 MBCA (Microsoft Baseline Configuration Analyzer), 1212 metric baselines, establishing, 1191-1192 NetIQ Corporation website, 1214 Network Monitor, 1194, 1196 applying filters, 1199 capture filters, 1198 Capture tab, 1198 capturing network traffic, 1198, 1201 color filters, 1198 display filters, 1198 filtering captured streams, 1198-1199 new features of, 1197-1198 parsing captured network traffic data, 1202 removing filters, 1199 OpsMgr (Operations Manager), 1194, 1213 Pages/sec counter, 1216-1217 policy baselines, establishing, 1191-1192 procedure baselines, establishing, 1191-1192 Reliability and Performance Monitor, 1202 Data Collector Sets, 1204-1205 diagnosis reports, 1204, 1206 Performance Monitor, 1204 Reliability Monitor, 1203, 1205 Resource Overview window, 1203 SCCM (System Center Configuration Manager), 1194

SCCP (System Center Capacity Planner), 1213 Task Manager, 1194-1195 third-party toolsets, 1213 Transaction Processing Performance Council website, 1193 VeriTest website, 1193 workload characterizations, 1192 WSRM (Windows System Resource Manager), 1207 calendar events, 1211 installing, 1208 matching criteria rules, 1210 resource allocation policies, 1209-1211 Terminal Services resource allocations, 1212 capacity limits in OpsMgr, 726 capture filters (Network Monitor), 1198 capture images creating custom installations (WDS), 859-861 customizing install images with unattended answer files. 861-862 multicast images, 862-863 WDS (Windows 2008 Deployment Services), 844 Capture tab (Network Monitor), 1198 captured broadcasts preparing, 1307 sessions, capturing, 1308-1309 capturing media sessions, 1308-1309 screen content, 1309-1310 cascading connections in Terminal Services, 792 catalogs, 114 categories for audit policies, 606-607, 609 CD images, mounting, 1331-1332 CD-ROM updates, 621 CD/DVD writer drives, Windows Server Backup support for, 1052 CDs (Connected Directories), 228 **CEIP** (Customer Experience Improvement Program), 87, 1181

Central Administration console (WSS), 1237, 1276-1278 finishing WSS install, 1245-1247 Central Details pane (IIS Manager console), 334 central store (GPOs), 541-542 creating, 564-565 verifying usage of, 565-566 centralized administrative model, 500 Certificate Authority (CA), 402-403 certificate servers, 743 configuring, 754-755 Certificate Services, 23, 402 backing up, 1068-1069 certificates (SSL), 402 in IIS 7.0, 363-367 Certification Authority role service, 403 **Certification Authority Web Enrollment role** service, 404 Certified for Windows Server 2008, 493 CGI feature page (IIS 7.0 websites), 349 change control documentation, 713 change management documenting procedures, 710 importance of, 1077 role in disaster recovery process, 1077-1078 99.999% uptime, 1081 change-control committee, 1079-1080 delegation of responsibilities, 1080-1081 Project Management Office (PMO), 1078-1079 -change parameter (Route command), 1176 change-control committee, 1079-1080 character sets, support in DNS, 275 characterizations, workload (capacity analysis), 1192 checklists, 703 for compatibility testing, 477 for migration process, 698 child domains, adding to multiple domain model, 148 CHKDSK utility, 634 Clear-Content cmdlet (PowerShell), 675

ClearType, 794 CLI (command-line interface) in PowerShell, 646-647 shell as. 640 client access licenses (CALs) installing, 828-829 types of, 804 **Client Access Point, 999** client dialer (Connection Manager), 778-779 Client for NFS, configuring, 241 client-side caching (CSC), 956-957 troubleshooting DNS, 282 client-side Terminal Services, 788-789 clients Automatic Updates, 391, 394-396 DHCP, 301, 308 VPN clients, 741 cloning desktops (WDS), 842-843 CLR (common language runtime), 376 cluster heartbeats, 1000 cluster networks, configuring, 1015-1017 cluster quorum, 1000 configuring, 1018-1019 cluster resources, 1002 simulating failure, 1024-1025 cluster servers, 35 clustering, 997 active nodes, 999 active/active clusters, 1000 active/passive clusters, 999 Client Access Point, 999 cluster heartbeats, 1000 cluster quorum, 1000 clusters, 999 DHCP servers, 312 failbacks, 1001 failover clusters, 997-998, 1001, 1003 adding nodes to, 1016-1017 adding shared storage to, 1017-1018 applications, selecting, 1004-1005 backing up, 1028 configuring cluster networks, 1015-1017

configuring cluster quorum model, 1018-1019 configuring failover and failback options. 1021-1023 creating, 1013-1015 deploying, 1009-1011 deploying services or applications, 1019-1021 installing Failover Clustering feature, 1011 maintenance, 1026 migration/upgrades, 1027 operating systems, selecting, 1009 quorum models, 1003-1004 removing nodes, 1027 restoring, 1028-1030 running Validate a Configuration Wizard, 1011-1013 shared storage, 1005-1009 testing, 1022, 1024-1025 generic resources, 1000 LUN (Logical Unit Number), 1001 new features, 29-30 NLB. 799. 998 adding nodes to, 1037-1038 backing up, 1039 creating, 1033-1037 filtering modes, 1032 installing, 1030-1031 maintenance, 1039-1040 network cards, 1033 operation modes, 1033 port rules, 1031 restoring, 1039 nodes, 999 passive nodes, 999 resources, 999 Services and Applications group, 999 shared storage, 1000 single point of failure, removal of, 29 stretched clusters, 30 terminology, 999-1001 virtual cluster servers, 999 witness file share, 1000

CMAK (Connection Manager Administration Kit), 779-780 cmdlets (PowerShell), 647-648 alias cmdlets, 654-655 help features, 664-667 CNAME (Canonical Name) records, 261 collaboration benefits of documentation 686 with minimal learning curve, 1239 WSS, 1234 collaborative design decisions, Windows Server 2008 migration, 53-54 collisions (replication), 187 color filters (Network Monitor), 1198 COM objects, creating in PowerShell, 682-683 COM ports, configuring for guest operating system sessions, 1332 comma-delimited text files (.csv), 1157 command prompt BitLocker Drive Encryption installation, 1134 Server Core installations, launching in, 95 command shell (OpsMgr), 718, 720 command-line interface (CLI) in PowerShell, 646-647 shell as, 640 Web Server role service (IIS 7.0), installing, 341-342 command-line tools Terminal Services administration, 834 in Windows Server Backup, 1054 commands Arp. 1175 DCDiag, 1177-1178 Ipconfig, 1174 NetDiag, 1177 Netstat, 1175-1176 Nslookup, 1176 Pathping, 1173-1174 Ping, 1171-1172 Route, 1176 Run As. administrative access. 378-379 Tracert, 1172-1173 wecutil ac. 1154 winrm quickconfig, 1154

commands (PowerShell) aliases of, 654-655 formats for. 646 types of, 647 cmdlets, 647-648 functions, 648-649 native commands, 649 scripts, 649 **Common Http Features role service** (IIS 7.0), 338 common language runtime, 376 communication during disaster recovery, 1082 communication plans, 693-694 compatibility (system), 89 **Compatibility Report Page (Install Windows** wizard), 91 compatibility testing, 473-475 application inventory, 483 application priority, 485 applications versus services, 483-484 checklist. 477 goals, 478-481 budget, 479 documentation, 481 extent, 480 resources, 479 testing lab, 481 timeframe, 478-479 training, 480 user involvement, 481 inventory application sheets, 484 lab-testing, 491 applications, installing, 492 Certified for Windows 2008, 493 hardware allocation/configuration, 491 Windows Server 2008 allocation/ configuration, 491 levels of, 480 network systems inventory, 482-483 plan, documenting, 482 preparations, 475-482 prototype phase, 494-495 results, documenting, 493-494

scope, 475-478 vendor information, 485 incompatible applications, 488-489 service updates/patches, 488 states of compatibility, 486-489 testing plan, assessing, 490 tracking sheets, 485-486 upgrade decision matrix, 489-490 version upgrades, 488 Windows Server 2008-compatible applications, 487 complete compatibility testing, 480 complete PC restore with Windows Server Backup, 1099 compliance in SharePoint Server 2007, 1238 compliant clients health policy, creating, 422-423 network policy, creating, 423-425 compression, 937 AD replication, 203 Compression feature page (IIS 7.0 websites), 349 compulsory VPN tunnels, 430 computer accounts, migrating, 468-470 **Computer Configuration Administrative** Templates node, 873 Computer Configuration node, 865, 870-871 **Computer Configuration Software Settings** node, 871 **Computer Configuration Windows Settings** node, 871-873 computer GPO processing, 534-535 Computer Management tool, configuring **Terminal Services**, 810 Computer Measurement Group website, 1193 Computer Migration Wizard, 468-470 Computers folders, objects, 166 -ComputerToFind parameter (Nslookup command), 1176 conditional forwarding (DNS), 273 conditions in Task Scheduler, 596 task conditions. 1185-1186 configuration documentation, 704-705

configuration groups, 724 Configuration page (Server Manager), 596 Services snap-in, 600-601 Task Scheduler, 596-598 Windows Firewall with Advanced Security, 598-600 WMI Control, 601 Configure a DNS Server Wizard, 255-257, 276 **Configure Networking setting (Initial** Configuration Tasks wizard), 86 configuring, 804, 806, See also customizing Automatic Updates clients, 394-396 certificate servers, 754-755 Client for NFS. 241 cluster networks, 1015-1017 cluster quorum models, 1018-1019 DHCP (WDS), 848 DHCP server for NPS validation restrictions, 428-429 DNS, 255-257 domains for SID migration, 465-466 event subscriptions, 1154-1155 failover and failback options, 1021-1023 feature delegation in IIS 7.0, 369 firewall settings with group policies, 898-901 folder redirection, managing users with policies, 906-909 global deployment settings for RemoteApps, 817-818 global options in FSRM (File Server Resource Manager), 964 GPO links, 571, 887 group policies, 521-523 guest operating system sessions (Hyper-V), 1330 BIOS, 1332 CD/DVD images, 1331-1332 COM ports, 1332 IDE controllers, 1332 network settings, 1331 processors, 1332 RAM. 1330 SCSI controllers, 1332

hardware, compatibility testing, 491 IIS for WSS, 1244-1245 IIS 7.0 website properties, 346-351 Incoming E-Mail settings, 1247-1248 IPv6, 289 adding IPv6 host records, 292-294 DHCPv6 scope setup, 292-293 DHCPv6 server setup, 291-292 manually setting addresses, 290 licensing types on Terminal Servers, 828-829 network cards, NLB clusters, 1033 network protocols, Windows Server 2008 installations, 78 NPS. 758-763 OpsMgr settings, 720 "out-of-band" FTP service, 356-361 password synchronization, 245 Performance Monitor, 1164 playlist broadcasting, 1300-1302 Preference Item-Level Targeting, domain group policies, 895-897 Print Management console, 526-527 quotas with FSRM (File Server Resource Manager), 964-965 RADIUS clients, 762-763 real-time live broadcasts, Windows Media Services, 1291-1292 Remote Desktop, 897-898 restricted groups for domain security groups, 915 RRAS servers, 763-766 Server for NFS, 241 shadow copies, 988-989 single video broadcasts, 1294-1296 system partitions, BitLocker Drive Encryption, 1132-1133 Terminal Services, 810-812 Active Directory Users and Computers snap-in, 811 with Computer Management tool, 810 with Group Policy, 811-812 Local Security Policy snap-in, 810 sessions, 800 Terminal Services Configuration snap-in, 811

TS Session Broker settings, 825-826 video directories, 1297, 1299 Virtual Memory, 1217-1218 VPN clients, 766-769 WDS Servers, 845-848 Windows Media Services, 1290-1291 Windows Server 2008 Add Features link (Initial Configuration Tasks wizard), 88 Add Roles link (Initial Configuration Tasks wizard), 87 administrator passwords, 84 compatibility testing, 491 computer names, 86 domains. 86 feedback, 87 firewalls. 88 with Initial Configuration Tasks Wizard, 582-583 initial configurations, 83-84 networking, 86 remote desktops, 88 time zones, 85 updates, 87 Windows Update, 622-625, 901-902 WINS, push/pull partners, 320-321 **Connected Directories**, 228 Connection Manager, 778-779 Connection Manager Administration Kit (CMAK), 779-780 connection objects, replication, 188-189 connections authentication for, 744-745 VPN components needed for, 740-741 SSTP connections, preventing, 778 testing, 769-772 Connections pane (IIS Manager console), 334-335 Connections Strings feature page (IIS 7.0 websites), 347 connector framework (OpsMgr), 718 **Connector Namespaces**, 228 console redirection, 1075-1076

consolidation migration, 460 Container class objects, 166 containers (Active Directory), GPO administrative delegation, 578-579 content sources, indexing, 1238 control, nested delegation, 182-183 controllers, configuring for guest operating system sessions, 1332 controlling group memberships with restricted groups, 916-917 converting basic disks to dynamic disks, 948 video files, 1310 copy command, 5 Copy-Item cmdlet (PowerShell), 675 copying to default user profiles, 518 files/directories in PowerShell, 675 corrupted data, 1092 costs AD sites, 195 for site links. 507-509 counters % Disk Time, 1220 % Processor Time, 1219 AD (Active Directory) performance, 1224 adding with Performance Monitor, 1162-1163 Avg. Disk Queue Length, 1220 DC (domain controller) performance, 1226 DC (domain controller) zone transfer, 1227 DNS (domain controller) performance, 1226 Interrupts/sec, 1219 network traffic, monitoring, 1222 Pages/sec, 1216-1217 credential caching (RODC), 1115 cross-forest transitive trusts, 135, 140, 143 cross-forest trusts, 152-154 CSC (client-side caching), 956-957 CSs (Connector Namespaces), 228 csv (comma-delimited text file) format, 1157 csvde.exe, 1066 CTCP (Compound TCP/IP), Next Generation TCP/IP stacks, 1141

currency, customizing, 80 current user's host-specific profile (PowerShell), 660 current user's profile (PowerShell), 660 custom administrative templates (GPOs), 553 custom display resolutions for Remote Desktop Connection, 793 custom filters, creating in Print Management console, 529-531 custom installations, creating with capture images (WDS), 859-862 custom lists in WSS, 1265 custom resource allocation policies (WSRM). 1210-1211 custom Server Core installations, 94 custom topology, 978 custom views, creating, 1152-1153 Custom Views folder (Event Viewer), 1152 **Customer Experience Improvement Program** (CEIP), 87, 1181 customizing, 1015. See also configuring currency, 80 event logs, 1157-1158 keyboard preferences, 80 languages, 80 time, 80 WSS, 1240 WSS home pages, 1274-1276

D

-d parameter (Arp command), 1175 -d parameter (tracert command), 1173 /d: DomainName parameter (NetDiag command), 1177 daily maintenance procedures, 626-628 Data Collector Sets (Reliability and Performance Monitor), 1204-1205 creating, 1166-1167 definition, 1165 data compression on file systems, 937 data corruption/loss, troubleshooting, 1086, 1092-1094 data encryption on file systems, 937 data recovery, 1077 shadow copies, 989-990 data storage in OpsMgr, 719 data stores, accessing with providers (PowerShell), 658-659 data volume recovery with Windows Server Backup, 1096-1097 data volumes, BitLocker Drive Encryption, 1130, 1138-1139 Data Warehouse Reader account (OpsMgr), 728 Data Warehouse Write Action account (OpsMgr), 728 database servers in failover clusters. 998 database size in OpsMgr, 725-726 databases, maintaining DHCP, 314-315 WINS. 325 Datacenter edition of Windows Server 2008, 11 Datasheet view (WSS), requirements for, 1254 Date and Time property (events), 1151 /DCAccountEnum parameter (NetDiag command), 1177 DCDIAG (Domain Controller Diagnosis) utility, 630-634 DCDiag command, 1177-1178 DCL (Digital Command Language), 640 DCs. See domain controllers DDNS (Dynamic DNS), 124, 270, 275 Active Directory, 124 DHCP, 303 secure updates, 271-272 deactivating schema attributes, 135 **Dead Gateway Detection, Next Generation** TCP/IP stacks, 1141 /debug parameter (NetDiag command), 1177 debugging baselines, 1169-1171 **CEIP** (Customer Experience Improvement Program), 1181 **Event Viewer** Applications and Services Logs folder, 1154 custom views, 1152-1153

Custom Views folder, 1152 data organization, 1156 event archiving, 1157 event logs, 1155-1158 event properties, 1151 event subscriptions, configuring, 1154-1155 launching Event Viewer, 1150 overview, 1149-1151 security logs, 1158-1159 Subscriptions folder, 1154 Windows Logs folder, 1153 Reliability and Performance Monitor counters, 1162-1163 Data Collector Sets, 1165-1167 overview, 1159-1160 Performance Monitor, 1161-1164 Reliability Monitor, 1164-1165 reports, 1167-1168 Resource Monitor, 1160-1161 Software Error-Reporting Mechanism, 1181 System Startup and Recovery, 1178-1179 Task Manager, 1145-1146 application monitoring, 1147 network monitoring, 1148-1149 performance monitoring, 1147-1148 process monitoring, 1147 service monitoring, 1147 user activity monitoring, 1149 TCP/IP tools Arp command, 1175 DCDiag command, 1177-1178 lpconfig command, 1174 NetDiag command, 1177 Netstat command, 1175-1176 Nslookup command, 1176 overview, 1171 Pathping command, 1173-1174 Ping command, 1171-1172 Route command, 1176 Tracert command, 1172-1173 Windows Error Reporting, 1182 Windows Memory Diagnostics Tool, 1179-1180

DEC (Digital Equipment Corporation), 640 decentralized replication design example, 209-210 dedicated redirectors (Terminal Services), 799 Default Document feature page (IIS 7.0 websites), 349 default site collection (WSS), components of, 1248-1251 default user profiles, 516 copying to, 518 creating, 517 defining deployment team participants, 48-49 design team participants, 48-49 scope of work, 44-46 server roles, 385 Definition property in PowerShell elements, 666-667 definitions, working sets, 1216 defragmenting disks, 630 Delegate Control Wizard, 509-510 delegate permissions, selecting, 175 delegated administration (GPOs), 884-885 delegating administration (GPOs), 577-579 control, 369 completing tasks, 179 of groups, 514-515 nested control, 182-183 at site level. 509-510 OU administration, 174-175 tasks, 174 **Delegation of Control Wizard**, 174 -Delete parameter (Route command), 1176 deleting files/directories in PowerShell, 674 lingering objects, 203 starter GPOs, 570 departmental goals, identifying, 42-43 dependencies, ASP.NET role service (IIS 7.0), 341

deploying, 1009 DFS, 975 DFS types, selecting, 976 domain DFS namespaces, 976 NTFS permissions, 976 planning replication, 976-977 replication topologies, 977-978 standalone DFS namespaces, 976 failover clusters, 1009-1011 installation images, 850-853 NAP, reasons for, 416 operating systems (WDS), 840-841 printers, domain group policies, 892-896 services or applications on failover clusters, 1019-1021 software packages with domain GPOs, 921-924 Terminal Services, 804 configuration steps, 810-812 remote assistance, enabling, 806-807 Remote Desktop for Administration, enabling, 805-806 Terminal Server role service, deploying, 807-810 TS Gateway, deploying, 821-824 TS Licensing, deploying, 827-829 TS RemoteApp programs, deploying, 815-820 TS Session Broker, deploying, 824-826 TS Web Access, deploying, 812-815 updates, 396 deployment scenarios for OpsMgr, 723-724 deployment team participants, defining, 48-49 deprovisioning, 232 descriptions, forest, 162 design best practices for sites, 503 design decisions (collaborative), Windows Server 2008 migration, 53-54 design documents, 52, 690-693 design features (new) in Active Directory, 143 design phase (Windows Server 2008 migration), 52-53, 440 budget estimates, 54-55 collaborative design decisions, 53-54

design decisions, 55-56 design documents, 56 end state (technology configurations), 54-55 executive summaries, 54 network background information, 54-55 project goals and objectives, 54 solutions, implementation approach, 54-55 structured design documents, organizing information, 54-55 table of contents (sample), 54 design team participants, defining, 48-49 designing Active Directory, 139 domains, 139-140 Group Policy infrastructure, 562 Active Directory infrastructure and, 562-563 separating GPO functions, 563-564 group structures, 165 IIS 7.0 implementation, 336-337 designs business function-based, 178-181 distribution groups, 178 domain-to-domain trust design sample, 181 domains, OUs, 173 federated forests design model, 151-154 geographical-based, 181-183 groups, 177 best practices, 177 business function-based, 178-181 distribution. 178 geographical-based, 181-183 group naming standards, 178 model samples, 178 naming standards, 178 nesting, 178 OUs, 171-172 multiple domain model, 149 OU structures, 165 OUs. 172-173 business function-based designs. 178-179 domain designs, 173

flexibility, 173 geographical-based designs, 181-182 group policies, 175-176 model samples, 178 single domain model, 146-147 single forest model, 151 WINS environment, 323 Desktop Experience feature for Remote Desktop Connection, 794 desktop migration procedures, documenting, 697 desktops administration tasks, 863 cloning (WDS), 842-843 remote. Windows Server 2008 configuration, 88 -destination parameter (Route command), 1176 development in IIS 7.0, new features, 333 Device Manager, 595 DFS (Distributed File System), 938-939, 972 backing up, 987, 1071 benefits, 972 branch office WAN utilization, 1141 deploying, 975 DFS types, selecting, 976 domain DFS namespaces, 976 NTFS permissions, 976 planning replication, 976-977 replication topologies, 977 standalone DFS namespaces, 976 folder targets, 974 folders, 974 installing, 978 folders and replication groups, creating, 981-983 namespace and root, creating, 978-980 namespace servers, adding, 980-981 replication, 984 management tools, 984-987 namespace root, 974 namespace servers, 974 namespaces, 940, 972-974 referrals, 975

replication, 940, 973-974 best practices, 984 disabling, 986 terminology, 975 topologies, 977-978 servers, 36 terminology, 974-975 trees, 975 troubleshooting, 984-987 DFS Management console, 561 DFSR (Distributed File System Replication), 25, 134, 939, 973-975 DHCP (Dynamic Host Configuration Protocol), 297, 300, 418, 1070 addresses, 418 administrative delegation, 313 alternate clients, 308 APIPA, 301-302 backing up, 307, 1070-1071 clients, 301 configuring, 848 database maintenance, 314-315 **DDNS. 303** failover. 308 50/50 approach, 309-310 80/20 approach, 310 100/100 approach, 311-312 clustering, 312 standby scopes approach, 312 installing, 304-306 Multicast scopes, 313 Netsh. 314 new features, 307-308 predecessors, 300 relay agents, 302 restoring, 307 scopes, 304-306 security, 315 authorization, 315-316 domain controllers, 316-317

servers, 35, 300 clustering, 312 configuring for NPS validation restrictions, 428-429 secure DNS updates and, 271 Superscope, 313 DHCP service recovery, 1104 DHCPv6 scope, setting up, 292-293 DHCPv6 servers, setting up, 291-292 diagnosis reports (Reliability and Performance Monitor), 1204, 1206 diagnostics, 634 in IIS 7.0, new features, 332 Diagnostics page (Server Manager), 592 Device Manager, 595 Event Viewer, 592-593 Reliability and Performance Monitor, 593-595 diagrams, triangle (domains), 144 digest authentication (IIS 7.0), 362 digital certificates, 402 Digital Command Language (DCL), 640 Digital Dashboard Starter Kit, 1234 **Digital Equipment Corporation (DEC), 640** digitally signed drivers, Windows Server 2008 upgrades, 89 Digital Rights Management (DRM), 408 directories, 218 attributes, 228 integrating, networks, 299 metadirectories, 228 video configuring, 1297, 1299 files, viewing, 1299 WWW directory publishing, 940 Directory Browsing feature page (IIS 7.0 websites), 350 directory management in PowerShell, 672-676 directory services (X.500), 111-112 Directory Services Restore Mode (DSRM), 1101 password for, 1067-1068

directory synchronization, 223 disable port range mode (port filtering), 1032 disabling BitLocker Drive Encryption, 1140 DFS replication, 986 signature requirements, 89 starter GPOs, 570 disaster recovery access issues, troubleshooting, 1087-1092 change management role in, 1077-1078 99.999% uptime, 1081 change-control committee, 1079-1080 delegation of responsibilities, 1080-1081 Project Management Office (PMO), 1078-1079 DHCP service recovery, 1104 network outage scenario, troubleshooting, 1084 physical site failure, 1084-1085 server or system failure, 1085-1094 steps for, 1081 appreciation for technical resources, 1083 assumptions, danger of, 1082 communication, 1082 postmortem meetings, 1083 qualifying the failure, 1081 recovering infrastructure, 1083 scheduling technical resources, 1083 synchronizing with business owners, 1082 validating priorities, 1082 System State recovery, 1100 for domain controllers, 1101-1104 Terminal Services administration, 835 with Windows Server Backup, 1096 data volume recovery, 1096-1097 system volume recovery, 1097-1099 WSS recovery, 1104-1107 disaster recovery documentation, 64, 707-709 backup and recovery documents, 709-710 disaster recovery plans, 709

failover documentation, 710 monitoring and performance documents, 710 disaster recovery plan, 709, 1044 approval for, 1049 creating, 1044 bare minimum services, identifying, 1046 disaster recovery scenarios, evaluating, 1044-1046 documentation of Windows system environment, 1044, 1049-1050 prioritization in. 1046 RTO (Return to Operation), 1047-1048 single points of failure, identifying, 1044 SLA (service-level agreement), 1047-1048 solution overview document, 1048-1049 disaster recovery scenarios, evaluating, 1044-1046 discover images creating, 853-854 WDS (Windows 2008 Deployment Services), 844 discovery phase (Windows Server 2008 migration), 49-52, 440 disk allocation with Windows Server Backup, 1058-1060 Disk Defragmenter, 630 disk drive redirection with Terminal Services, 790 Disk Management console, 603-604, 946 adding disks to Windows 2008, 946-948 converting basic disks to dynamic disks. 948 creating fault-tolerant volumes, 948-950 disk space, checking, 629, 635 disk storage, Hyper-V requirements, 1318 disk subsystems, evaluating, 1219-1220 Diskpart.exe utility, 946 creating fault-tolerant volumes, 950-952

disks basic disks, 942-943 Disk Management console, 603-604, 946 adding disks to Windows 2008, 946-948 converting basic disks to dynamic disks, 948 creating fault-tolerant volumes, 948-950 Diskpart.exe utility, 946 creating fault-tolerant volumes, 950-952 dynamic disks, 943 external disk storage, 945-946 GPT (GUID Partition Table) disks, 942 Logical Disk object, 1220 MBR (Master Boot Record) disks, 942 partitions, 943 Physical Disk object, 1220 types of, 942-945 volumes, 943 Display Data Prioritization feature for Remote Desktop, 794 display features for Remote Desktop Connection, 793 custom display resolutions, 793 Desktop Experience feature, 794 Display Data Prioritization feature, 794 Font Smoothing feature, 794 monitor spanning, 793 display filters (Network Monitor), 1198 /displaydns parameter (lpconfig command), 1174 distinguished names (Active Directory), 113 distributed administration, 26 distributed administrative model, 500-501 Distributed File System. See DFS Distributed File System Replication (DSFR), 25, 134, 939, 973-975 distribution, media content, 1308 distribution groups, 169, 510 DNS (domain name system), 107, 123, 251, 1069, 1224 Active Directory, 123 Active Directory and foreign DNS, co-existing, 125

in AD DS environment, 277 GlobalNames zone (GNZ), 280-281 impact of DNS. 277-278 non-Microsoft DNS implementations, 278 secondary zones, 278-279 site resolution, 278, 280 AXFR (full zone transfers), 1227 AXFR Request Received (zone transfer counter), 1227 AXFR Request Sent (zone transfer counter), 1227 AXFR Response Received (zone transfer counter), 1227 AXFR Success Received (zone transfer counter), 1227 AXFR Success Sent (zone transfer counter), 1227 backing up, 1069 caching-only servers, 262 configuring, 255-257 dynamic DNS, 270, 275 **DHCP** 303 secure updates, 271-272 Dynamic Update Received/Sec counter, 1226 forwarders, 273-274 framework for, 253 hierarchy, 253-254 history of, 252-253 "island" problem, 257, 276 installing, 254-257 IPv6 host records, adding, 292-294 IXFR (incremental zone transfers), 1227 IXFR Request Received (zone transfer counter), 1227 IXFR Request Sent (zone transfer counter), 1227 IXFR Response Received (zone transfer counter), 1227 IXFR Success Received (zone transfer counter), 1227 IXFR Success Sent (zone transfer counter), 1227 monitoring, 1224, 1226-1227

namespaces, 123-124, 254 performance counters, 1226 queries. 268-269 read-only DNS, RODC, 1116 reasons for using, 252 Recursive Queries/Sec counter, 1226 Recursive Query Failure/Sec counter, 1226 resource records, 257 Canonical Name (CNAME) records, 261 Host (A) records, 258 list of. 261 Mail Exchanger (MX) records, 260 Name Server (NS) records, 259 Pointer (PTR) records, 261 Service (SRV) records, 259-260 Start of Authority (SOA) records, 258 Root Hints list, 273 scavenging, 272-273 Secure Update Received/Sec/Sec counter, 1226 Server Core installations, 96-97 servers, 35 TCP Query Received/Sec counter, 1226 TCP Response Sent/Sec counter, 1226 Time to Live (TTL) value, 270-271 Total Query Received/Sec counter, 1226 Total Response Sent/Sec counter, 1226 troubleshooting, 281 client-side cache problems, 282 with DNSCMD command-line utility. 284-285 with Event Viewer, 281-282 HOSTS file problems, 282 with IPCONFIG command-line utility. 283-284 with NSLOOKUP command-line utility, 282-283 with Reliability and Performance Monitor, 282 with TRACERT command-line utility, 284 UDP Query Received/Sec counter, 1226 UDP Response Sent/Sec counter, 1226 Unicode character support, 275 in Windows 2000/2003, 274-275

in Windows Server 2008, 275 application partitions, 275 automatic creation of DNS zones, 276 msdcs zone, 276-277 WINS and, 274 WINS integration, 317-318 zone transfers, 265-268 zones, 261-262 AD-integrated zones, 136, 274, 460-461 automatic creation of, 276 forward lookup zones, 262 GlobalNames zone (GNZ), 280-281 primary zones, 263 reverse lookup zones, 263 secondary zones, 263, 278-279 standard and AD-integrated, comparing, 125 stub zones, 263-265 DNS poisoning, 271 DNSCMD command-line utility, troubleshooting DNS. 284-285 document libraries in WSS, 1236, 1251-1261 accessing, 1253 advantages of. 1252 Edit menu options, 1259-1260 toolbar menus in. 1253-1258 training, importance of, 1261 document management, need for, 1239 documentation administration/maintenance documentation, 702 Active Directory infrastructure documentation, 703-704 administration manual, 705 checklists, 703 configuration (as built) documents, 704-705 policy documents, 703 procedure documents, 702 security procedure documents, 706 server build procedure documents, 704 topology diagrams, 705 troubleshooting documents, 706 baselining, 711

benefits of, 686-687 change management procedures, 710 compatibility testing, 481-482, 493-494 disaster recovery documentation, 64, 707-710 knowledge management, 689 knowledge sharing, 688-689 network configuration documentation, 706-707 performance documentation, 710-711 pilot results of migration process, 67 planning, 688 purpose of, 685 reporting documentation, 711-712 security documentation, 712-713 types of, 687 updating, 635 Windows Server 2008 implementation, 689 checklists, 698 communication plans, 693-694 design documents, 690-693 migration plans, 694-698 pilot test plans, 702 project plans, 690 support and project completion documents, 702 test plans, 699-701 training plans, 698-699 Windows system environment, 1044, 1049-1050 documents design, 52 migration, 53 budget estimates, 62 creating, 59 executive summaries, 60 migration background, 60 migration phase risks and assumptions, 60 migration process goals and objectives, 60 migration processes, 61-62 project plans, 62

project timeline and milestones, 60 team members' roles and responsibilities, 60 training plans, 61 structured design budget estimates, 54-55 end state (technology configurations). 54-55 executive summaries, 54 network background information, 54-55 organizing information, 54-55 project goals and objectives, 54 solutions, implementation approach. 54-55 table of contents (sample), 54 XML, forest descriptions, 162 Domain Controller Diagnosis (DCDIAG) utility, 630-634 domain controller GPOs, 882-883 domain controllers (DCs), 35 Active Directory deploying on Server Core, 197 monitoring, 1223-1225 multi-master replication, 114 multiple password policy implementation per domain, 127-128, 130-131 object audits, 132 replication, monitoring, 1224 restarting on, 126 adding to sites, 505-506 AXFR Request Received (DNS zone transfer counter), 1227 AXFR Request Sent (DNS zone transfer counter), 1227 AXFR Response Received (DNS zone transfer counter), 1227 AXFR Success Received (DNS zone transfer counter), 1227 AXFR Success Sent (DNS zone transfer counter), 1227 DHCP, 316-317 DNS (domain name system), monitoring, 1224. 1226-1227 Dynamic Update Received/Sec (DNS performance counter), 1226

Dynamic Update Received/Sec (DNS performance counter), 1226 GC/DCs. 326-327 IXFR Request Received (DNS zone transfer counter). 1227 IXFR Request Sent (DNS zone transfer counter), 1227 IXFR Response Received (DNS zone transfer counter), 1227 IXFR Success Received (DNS zone transfer counter). 1227 IXFR Success Sent (DNS zone transfer counter), 1227 performance counters, 1226 phantom domain controllers, removing, 457-458 preparing with adprep, 451-453 promoting, 201-202 Recursive Queries/Sec (DNS performance counter), 1226 Recursive Query Failure/Sec (DNS performance counter), 1226 removal of, 1113 replacing existing, 454-455 RODC (Read-Only Domain Controllers), 211, 327-329, 1112 Active Directory support, 134 administrator role separation, 1115 benefits of, 1114-1115 credential caching, 1115 deploying, 212, 214 ERODC, 1117 features of, 212 installing, 1117-1118, 1120-1129 limitations of, 1117 read-only active directory domain services, 1114 read-only DNS, 1116 replication workload reduction, 1114 WAN utilization, 1140 Secure Update Received/Sec/Sec (DNS performance counter), 1226 single domain controller upgrade for Big Bang migration, 445-448 System State recovery, 1101-1104

TCP Query Received/Sec (DNS performance counter), 1226 TCP Response Sent/Sec (DNS performance counter), 1226 theft of. 1113 time. 188 Total Query Received/Sec (DNS performance counter), 1226 Total Response Sent/Sec (DNS performance counter), 1226 UDP Query Received/Sec (DNS performance counter), 1226 UDP Response Sent/Sec (DNS performance counter), 1226 updating existing, 453-454 upgrading versus replacing, 450-451 virtual domain controller rollback for Big Bang migration, 445 Windows 2000/2003 domain controllers, removing, 457 zone transfer counters, 1227 domain DFS namespaces, 973, 976 domain functional level (Windows Server 2003), 111, 512-513 upgrading, 459-460 domain group policies, 865, 880-882, 886 backing up and restoring, 575-577 configuring firewall settings, 898-901 creating, 570-571, 887 managing User Account Control settings, 887-889 Preference Item-Level Targeting, configuring, 895-897 printers, deploying, 892-896 Remote Desktop, configuring, 897-898 software restriction policies, creating, 890-892 Windows Update settings, configuring, 901-902 wireless policies, creating, 902-905 domain Group Policy links, 563 domain local groups, 120, 170-171, 511 Domain Name System. See DNS domain naming master (OM role), 115 domain servers, 7

Domain Services, 17 domain trusts (Active Directory) explicit trusts. 116-117 external trusts, 117 replacing with OUs (organizational units), 182 transitive trusts, 116 domain-based certificate requests in IIS 7.0, creating, 365 domain-based namespaces, adding namespace servers to. 980-981 domain-to-domain trusts, 181 domains. See also DNS (domain name system) Active Directory, 108-109 forests, 110 subdomains, 109 trees, 109-110 child, adding to multiple domain model, 148 configuring for SID migration, 465-466 cross-forest transitive trusts, 140 DDNS (Dynamic DNS), 124 designing, 139 0Us, 173 empty-root domain model, 154-155 real-world design example, 157 selecting, 156 explicit trusts, 140 fine-grained password policies, 142 multiple domain model, 147 domains, adding, 148 real-world design example, 149 user administration in, 512 name determination, Windows Server 2008 installations, 78 namespaces, 141-142 OUs (organizational units), comparing, 118-119 placeholder domain model, 158 rename tool, 135 renaming, 143, 160-163 root, cross-forest trusts, 154 Server Cores, adding to, 97 shortcut trusts. 140

single domain model, 144 real-world design example, 146-147 selecting, 145 user administration in, 512 special-purpose, 159-160 structure, choosing, 143-144 subdomains in Active Directory, 149 shortcut trust, 117 transitive trusts, 140 triangle diagram, 144 trusts, 140 Windows Server 2003, domain functional level, 111 Windows Server 2008 configuration, 86 DOS, as shell, 641 DOSShell, 641 dot sourcing, scripts, 657 dotted-decimal format, 205 Download and Install Updates link (Initial Configuration Tasks wizard), 87 downloading Windows Media Services source files, 1288 Windows Server 2008 updates, 87 Drain mode (Terminal Services), 799-800 drivers digitally signed, Windows Server 2008 upgrades, 89 printer drivers, updating, 529 signing, 952 drives (PowerShell), 659 drizzling, 391 DRM (Digital Rights Management), 408 DSAMain (Active Directory database mounting tool), 134 DSRM (Directory Services Restore Mode), 1101 password for, 1067-1068 DVD backups, creating, 1062-1063 DVD images, mounting, 1331-1332 DVD media for backups, 1095 dynamic disks, 943 converting basic disks to, 948 Dynamic DNS. See DDNS

Dynamic Host Configuration Protocol. See DHCP dynamic IP addresses, Windows Server 2008 installations, 78

Dynamic Update Received/Sec (DNS performance counter), 1226

E

/e parameter (DCDiag command), 1178 -e parameter (Netstat command), 1175 e-mail, mail-enabled groups, 169-170 EAP (Extensible Authentication Protocol), 744 EC (Enforcement Client), 417 ECN (Explicit Congestion Notification), Next Generation TCP/IP stacks, 1141 Edit Disk option (Hyper-V), 1325 Edit menu options in WSS document libraries, 1259-1260 Edit Page interface (WSS site management), 1274-1276 editing features of PowerShell, 646 editing video tools, 1303 editions of Windows Server 2008, 10 EFS (Encrypting File System), 389, 408 BitLocker Drive Encryption versus, 1129 empty-root domain model, 154-155 real-world design example, 157 selecting, 156 EMS (Emergency Management Services) console redirection, 1075-1076 emulators, PDC (OM role), 115 **Enable Automatic Updating and Feedback link** (Initial Configuration Tasks wizard), 86 enabling, 806 AD DS lookup for Services for NFS, 239-240 auditing for NTFS folders, 1089-1091 remote assistance, 806-807 Remote Desktop for Administration, 805-806 ScheduledDefrag task, 598 server roles with Server Manager, 385-386

shadow copies for shared volumes, 1073-1075 starter GPOs. 566 VPNs on RRAS server, 432-435 encrypting files, 389 Encrypting File System (EFS), 389, 408 BitLocker Drive Encryption versus, 1129 encryption, 401 BitLocker Drive Encryption, 1129 authentication, 1131 data volumes, 1130, 1138-1139 deployment scenarios, 1131 EFS versus, 1129 hardware requirements, 1131 installing, 1130, 1133-1134 passwords, 1139 removing, 1140 system partition configuration, 1132-1133 TPM, 1130, 1135-1136 UEFI. 1130 USB keys, 1137-1138 data encryption on file systems, 937 EFS. 389. 408 BitLocker Drive Encryption versus, 1129 IPSec. 411-412 functionality in, 412 NAT-T. 412-413 private keys, 401 public keys, 401 SSL. 363 end state (technology configurations), design documents, 54-55 end users, supporting with WDS, 841 end-user satisfaction, verifying, 67 Enforce option (group policy configuration), 523 Enforcement Client (EC), 417 enforcement of GPO links, 543-544 enforcement policies for NPS, 418 Enforcement Server (ES), 417 Enterprise edition of Windows Server 2008, 10-11 upgrading Standard Edition to, 476

enterprise networks, 298 addressing, 298 directory integration, 299 name resolution, 298-299 network services, new features, 299 enterprise root CA, 403 enterprise subordinate CA, 403 environments Windows Server 2008, supporting, 68 WINS designing, 323 upgrading, 323-325 Equal per IIS Application Pool resource allocation policy templates (WSRM), 1209 Equal per Process resource allocation policy templates (WSRM), 1209 Equal per Session resource allocation policy templates (WSRM), 1209 Equal per User resource allocation policy templates (WSRM), 1209 ERODC (Enterprise Read-Only Domain Controllers), 1117 Error Reporting (Windows), 87 errors. 1182 Errors feature page (IIS 7.0 websites), 350 ES (Enforcement Server), 417 estimating budgets design documents, 54-55 migration documents, 62 ETS (Extended Type System), 650 evaluating disaster recovery scenarios, 1044-1046 disk subsystems, 1219-1220 Event ID property (events), 1151 event log information, gathering with PowerShell, 670-672 event logging (GPOs), 560-561 event logs, Computer Configuration Windows Settings node, 872 event subscriptions, configuring, 1154-1155 Event Viewer, 560-561, 592-593 Applications and Services Logs folder, 1154 custom views, creating, 1152-1153 Custom Views folder, 1152

data organization, 1156 event archiving, 1157 event logs customizing, 1157-1158 saving, 1155 viewing on remote servers, 1156 event properties, 1151 event subscriptions, configuring, 1154-1155 filtering events, 627 launching, 1150 monitoring, 626-628 overview, 1149-1151 security logs, 1158-1159 Subscriptions folder, 1154 troubleshooting DNS, 281-282 Windows Logs folder, 1153 events archiving, 1157 filtering, 1156 grouping, 1156 properties, 1151 sorting, 1156 Events section (Server Manager roles pages), 589 .evtx (log file) format, 1157 Excel 2007, integration with WSS, 1267-1269 Excel Services, 1238 Exchange Server 5.5, 106 execution policies in PowerShell, 661-663 executive summaries design documents, 54 migration documents, 60 explicit scope indicators (PowerShell), 656 explicit trusts, 116-117, 140 Export-Alias cmdlet (PowerShell), 655 exporting password keys, 464 to WSS lists, 1268-1271 Extended Type System (ETS), 650 extending Active Directory schema, 112 Extensible Authentication Protocol (EAP), 744 extensions, video files, 1308 external disk storage, 945-946

external disks, Windows Server Backup support for, 1052 external namespaces (DNS), 123-124, 141-142 external trusts, 117

F

-f parameter (Ping command), 1172 -f parameter (Route command), 1176 /f: LogFile parameter (DCDiag command), 1178 failback options, configuring, 1021-1023 failbacks, clusters, 1001 Failed Request Tracing Rules feature page (IIS 7.0 websites), 350 failover, DHCP, 308 50/50 approach, 309-310 80/20 approach, 310 100/100 approach, 311-312 clustering, 312 standby scopes approach, 312 Failover Clustering feature, installing, 1011 failover clusters, 995, 997-998, 1001-1003 adding nodes to, 1016-1017 adding shared storage to, 1017-1018 applications, selecting, 1004-1005 backing up, 1028 configuring cluster networks, 1015-1017 configuring cluster quorum model, 1018-1019 configuring failover and failback options, 1021-1023 creating, 1013-1015 deploying, 1009-1011 deploying services or applications, 1019-1021 installing Failover Clustering feature, 1011 maintenance, 1026 migration/upgrades, 1027 operating systems, selecting, 1009 guorum models, 1003-1004 removing nodes, 1027 restoring, 1028-1030

running Validate a Configuration Wizard, 1011-1013 shared storage, 1005-1009 testing, 1022, 1024-1025 failover documentation, 710 failover options, configuring, 1021-1023 failures, gualifying, 1081 FAT (file allocation table) format, 936 fault tolerance disks, types of, 942-945 external disk storage, 945-946 file systems, accessing, 940 Hyper-V guest sessions, 1335 system file stability, 952-953 system-level fault tolerance, 993-994 for Terminal Services, planning for, 803 fault-tolerance requirements (IIS 7.0), 337 fault-tolerant systems network hardware, 995-996 server storage, 996 service availability, 997 UPSs. 994-995 fault-tolerant volumes, 944 creating, 948-952 faults, memory, 1216 FC (Fibre Channel) storage arrays, 1007 feature delegation in IIS 7.0, configuring, 369 features installing, 587 list of, 585-587 of PowerShell, 643-644 Remote Server Administration Tools for, 614 Features page (Server Manager), 592 Features Summary window (Server Manager), 588-589 federated forests design model, 151-154 federation, 17, 223 federation proxy servers, 223 federation servers, 223 feedback CEIP.87 Windows Error Reporting, 87 Windows Server 2008, configuring for, 87

/ferr:ErrorLogFile parameter (DCDiag command), 1178 Fibre Channel (FC) storage arrays, 1007 file allocation table (FAT) format, 936 file formats, 936 file management in PowerShell, 672-676 File Replication Service (FRS), 939, 974 file screen exceptions, creating with FSRM (File Server Resource Manager), 969 file screen templates, creating with FSRM (File Server Resource Manager), 968-970 file screening on file systems, 937 file screens, creating with FSRM (File Server Resource Manager), 967-968 File Server Resource Manager, 21, 960-961 file servers, 7 in failover clusters, 997 File Services role, installing, 953-955 File Services tools, 939 file share deployment for RemoteApps programs, 820 file shares, data recovery, 989-990 File Signature Verification (Sigverif.exe), 952 file system integrity, checking, 634 file system services, troubleshooting with FSRM (File Server Resource Manager), 971 file systems accessing FTP (File Transfer Protocol), 940 Services for Macintosh, 941 Services for NFS, 941 SFTP (Secure File Transfer Protocol), 941 Windows folder sharing, 940 WSS (Windows SharePoint Services), 941 WWW directory publishing, 940 data compression, 937 data encryption, 937 DFS (Distributed File System), 938-939, 972, 984 backing up, 987 benefits, 972 deploying, 975 folder targets, 974

folders, 974 management tools, 984-987 namespace root, 974 namespace servers, 974 namespaces, 940, 972-974 referrals, 975 replication, 940, 973-975 terminology, 974-975 trees, 975 troubleshooting, 984-987 DFSR (Distributed File System Replication), 939 file screening, 937 management tools, 939 monitoring, 939 partition formats, 936 quota services, 936-937 reporting, 939 RSS (Remote Storage System), 938 security settings, Computer Configuration Windows Settings node, 872 volume formats, 936 VSS (Volume Shadow Copy Service), 937-938 File Transfer Protocol (FTP), 351, 940 file-level security, 386 access audits, 388-389 encryption, 389 NTFS, 386-387 share-level security, compared, 387 files auditing, 609-611 comma-delimited text files (.csv), 1157 encrypting, 389 LMHOSTS, 323 log file (.evtx) format, 1157 recovering with shadow copies, 1092 with Windows Server Backup, 1093-1094 text-file format (.txt), 1157 video converting, 1310 extensions, 1308

video directories, viewing, 1299 XML format, 1157 filtering Event Viewer events, 627 events, 1156 GPOs, 546-549 pull record filtering, 319 filtering modes, NLB clusters, 1032 filters custom filters, creating in Print Management console, 529-531 security filters (GPOs), managing, 573-574 WMI filters creating, 572-573 linking, 573 financial benefits of documentation, 686-687 fine-grained password policies, 127, 142, 912-914 firewall requirements in OpsMgr, 728 firewall rules for VPN tunneling protocols, 752-753 firewall settings, configuring with group policies, 898-901 firewalls physical security, 380 SSL relay and, 797-798 Windows Firewall with Advanced Security, 381, 598-600 creating inbound/outbound rules, 382-385 Server Manager integration, 381 Windows Server 2008 configuration, 88 /fix parameter DCDiag command, 1178 NetDiag command, 1177 Flexible Single Master Operations, 455 /flushdns parameter (lpconfig command), 1174 Folder icon (Active Directory), 172 folder redirection, configuring, 906-909 Folder Redirection setting, 956 folder shares, creating, 957-960 folder targets (DFS), 974 folders auditing, 609-611 Computers, objects, 166

DFS. 974 creating, 981-983 Event Viewer Applications and Services Logs, 1154 Custom Views, 1152 Subscriptions, 1154 Windows Logs, 1153 recovering with shadow copies, 1092 with Windows Server Backup, 1093-1094 sharing, 940 File Services role, installing, 953-955 Users, objects, 166 Font Smoothing feature for Remote Desktop Connection, 794 forcing replication, 189 Forefront product suite, 389 foreign DNS and Active Directory DNS, co-existing, 125 forest functional levels, upgrading, 459-460 forests Active Directory domain trees, 110, 150-151 cross-forest transitive trusts, 143 cross-forest trusts, root domains, 154 federated forests design model, 151-154 preparing with adprep, 451-453 single forest model real-world design example, 151 trees, 150 subdomains, shortcut trust, 117 user administration across, 512 XML documents, 162 form libraries in WSS, 1253 Format-Table cmdlet (PowerShell), 654, 670 forms managing in Print Management console, 529 in SharePoint Server 2007, 1238 forms authentication (IIS 7.0), 362 forward lookup zones, 262 forwarded events logs, 1153 forwarders (DNS), 273-274

FQDN (fully gualified domain name), 253, 298 framework for DNS, 253 free disk space, checking, 629, 635 FreeBSD shells, 640 FrontPage Server Extensions for IIS 7.0, 343 FRS (File Replication Service), 939, 974 FSM0. 455 FSRM (File Server Resource Manager), 21-22, 961-962 file screen exceptions, creating, 969 file screen templates, creating, 968-970 file screens, creating, 967-968 file system services, troubleshooting, 971 global options, configuring, 964 installing, 963-964 quota management features, 960 quota templates, creating, 966-967 quotas adjusting, 965-966 configuring, 964-965 reports, generating, 970-971 uses for. 962-963 FTP (File Transfer Protocol), 351, 940 FTP Authentication feature page (IIS 7.0 FTP sites), 357 FTP Authorization Rules feature page (IIS 7.0 FTP sites), 358 FTP Directory Browsing feature page (IIS 7.0 FTP sites), 358 FTP Firewall Support feature page (IIS 7.0 FTP sites), 358 FTP Logging feature page (IIS 7.0 FTP sites), 359 FTP Management snap-in (IIS 7.0), 340 FTP Messages feature page (IIS 7.0 FTP sites), 359-360 FTP Publishing Service role service (IIS 7.0), 339-340 FTP Server feature (IIS 7.0), 332, 340 FTP service in IIS 7.0 "out-of-band" FTP service configuring, 356-361 features. 352 installing, 353-354

"out-of-the-box" FTP service, installing, 353 secure FTP site, creating with SSL, 354-356 versions of, 351-352 FTP Sites folder (IIS Manager Connections pane), 335 FTP SSL Settings feature page (IIS 7.0 FTP sites), 360 FTP User Isolation feature page (IIS 7.0 FTP sites), 360-361 FTP, IP, and Domain Restrictions feature page (IIS 7.0 FTP sites), 358 full mesh topology, 977 full zone transfers (AXFR), 1227 full zone transfers (DNS), 267 fully gualified domain name (FQDN), 253, 298 functional levels (Active Directory), 110 upgrading, 459-460 Windows Server 2003 domain functional level. 111 functionality levels for domains, 512-513 functions (PowerShell), 648-649

G

-g parameter Arp command, 1175 Pathping command, 1174 Gantt charts, 58 -gateway parameter (Route command), 1176 gateway server (OpsMgr), 718 capacity limits, 726 GC/DCs (Global Catalog Domain Controllers), 326-327 GCs (global catalog servers), Active Directory, 35, 114 generic cluster resources, 1000 geographic-based management groups in OpsMgr, 724-725 geographical depth and breadth, Windows Server 2008 migration, 51-52 geographical diversity of users, migration testing, 66 geographical-based designs, 181-183
Get Important Updates for Installation page (Install Windows Wizard), 90 Get-Alias cmdlet (PowerShell), 655 Get-ChildItem cmdlet (PowerShell), 673 Get-Command cmdlet (PowerShell), 665-667 Get-Content cmdlet (PowerShell), 665, 676 Get-EventLog cmdlet (PowerShell), 670-672 Get-Help cmdlet (PowerShell), 664-665 Get-Item cmdlet (PowerShell), 672 Get-ItemProperty cmdlet (PowerShell), 676 Get-Location cmdlet (PowerShell), 672 Get-Member cmdlet (PowerShell), 650-651 Get-Process cmdlet (PowerShell), 654, 677-678 Get-Service cmdlet (PowerShell), 668-669 Get-WmiObject cmdlet (PowerShell), 679-681 global catalog Active Directory, 114 media, creating, 143 placement, 325-326 schema modifications, 204 Global Catalog Domain Controllers, 326-327 global deployment settings for RemoteApps, configuring, 817-818 global groups, 120, 171, 179, 511 global options, configuring in FSRM (File Server Resource Manager), 964 global scope in PowerShell, 655-656 GlobalNames zone (GNZ), 134, 280-281 goals business, identifying, 40 business unit/departmental goals, 42-43 high-level business goals, 41 of compatibility testing, 478-481 migration processes, 60 projects, design documents, 54 technical, identifying, 43-44 deployment team participants, defining, 48-49 design team participants, defining, 48-49 scope of work, defining, 44-46 timeframes (implementation or migration), determining, 46-48 GPLogview, 559

GPMC (Group Policy Management Console), 519, 554-555, 577 Group Policy Modeling, 926-929 installing, 886 performing remote Group Policy Results, 930 GPO results, managing Active Directory with policies, 926-929 GPOE (Group Policy Object Editor), 555-556 GPOs (Group Policy Objects), 534, 539, 877 Active Directory site GPOs, 883 administrative tasks administrative delegation, 577-579 central store, creating, 564-565 central store, verifying usage of, 565-566 domain GPOs, backing up and restoring, 575-577 domain GPOs, creating, 570-571 Group Policy Modeling, 577 Group Policy Results, 577 links, configuring, 571 links, creating, 571 order of processing, managing, 574 security filters, managing, 573-574 settings, viewing, 575 starter GPOs, backing up and restoring, 567-570 starter GPOs, creating, 566-567 status management, 572 WMI filters, creating, 572-573 WMI filters, linking, 573 administrative templates, 541, 550-553 custom templates, 553 for Windows 2000/XP/Server 2003, 551-552 for Windows Vista/Server 2008, 552-553 central store, 541-542 configuring GPO links, 887 creating new domain GPOs, 887 delegated administration, 884-885 domain controller GPOs. 882-883 domain GPOs. 880-882

event logging, 560-561 filtering, 546-549 link enforcement, 543-544 links. 543-544 blocking inheritance, 545-546 inheritance, 544-545 order of processing, 545-546 loopback processing, 549-550 policies and preferences, 878-880 policy settings, 542-543 processing, 534-536 computer GPO processing, 534-535 NLA (Network Location Awareness), 535 settings for, 535-536 user GPO processing, 535 replication, 561 restoring, 1104 scripts, 558 securing Terminal Services, 831 separating functions of, 563-564 slow link detection, 549-550 small businesses, 883-884 software installation GPOs, creating, 922-924 source starter GPOs, 520 starter GPOs, 542, 877 storage and replication, 539-541 GPT (GUI Partition Table) disks, 942 gpt.ini file (GPOs), 541 gpupdate.exe, 557-558 graphical user interface (GUI), 13, 640 Group Account Migration Wizard, 466-467 group delegation, 514-515 group designs, OUs, 171-172 group management (ILM 2007), 231 group membership (restricted groups) controlling, 916-917 modifying, 917-919 group policies, 518, 539, 865 Active Directory, 134 automatic client configurations, 394-396 branch office WAN utilization, 1142 configuring, 521-523 creating, 519-521

domain group policies, 865, 886 local group policies, 865, 875 benefits of. 874-875 management tools, 554 ADMX Migrator, 559 DFS Management console, 561 Event Viewer, 560-561 GPLogview, 559 **GPMC** (Group Policy Management Console), 554-555 GPO scripts, 558 GPOE (Group Policy Object Editor), 555-556 gpupdate.exe, 557-558 Microsoft Desktop Optimization Pack for Software Assurance, 558 Print Management console, 556-557 managing from administrative or remote workstations, 929-930 managing users, 905-906 configuring folder redirection, 906-909 MMC (Microsoft Management Console), 910-911 removable storage access, 909-910 need for. 866 processing, 534-536 computer GPO processing, 534-535 NLA (Network Location Awareness), 535 settings for, 535-536 user GPO processing, 535 restoring, 1104 security templates, 538 site group policies, 503 troubleshooting, 523-525 viewing, 519 Windows group policies, 866 local administrators user policies, 867 local computer policies, 867 local domain group policies, 868 local non-administrators user policies, 867 local security policies, 867 policy processing overview, 868-869 Security Configuration Wizard (SCW), 868

Group Policy, 539 configuring Terminal Services, 811-812 defined. 533-534 elements of, 539 administrative templates, 541, 550-553 blocking inheritance, 545-546 central store, 541-542 filtering, 546-549 GPO storage and replication, 539-541 GPOs (Group Policy Objects), 539 inheritance, 544-545 link enforcement, 543-544 links. 543-544 loopback processing, 549-550 order of processing, 545-546 policy settings, 542-543 slow link detection, 549-550 starter GPOs. 542 infrastructure design, 562 Active Directory infrastructure and, 562-563 separating GPO functions, 563-564 securing Terminal Services, 831 Group Policy Feature set, 870 **Computer Configuration Administrative** Templates node, 873 Computer Configuration node, 870-871 **Computer Configuration Software Settings** node, 871 **Computer Configuration Windows Settings** node, 871 User Configuration Administrative Templates node. 874 User Configuration node, 873 User Configuration Software Settings node, 874 User Configuration Windows Settings node, 874 Group Policy Management, new features in, 19-20 Group Policy Management Console (GPMC), 519, 554-555, 577, 886 Group Policy Modeling, 523-525, 577, 926-929 Group Policy Object Editor (GPOE), 555-556

Group Policy Objects. See GPOs Group Policy Results, 577 grouping events, 1156 groups, 510 Active Directory, 119, 168 domain local, 120 global, 120 machine local, 120 OUs (organizational units). comparing, 121 types of, 120 universal, 120 creating, 513 delegating control of, 514-515 designs, 177 best practices, 177 business function-based, 178-181 distribution groups, 178 geographical-based, 181-183 group naming standards, 178 group nesting, 178 model samples, 178 distribution groups, 169, 178, 510 domain functionality levels, 512-513 domain local, 120, 170-171 global, 120, 171, 179 machine local, 120, 170 mail-enabled groups, 169-170 migrating, 466-467 multiple domain user administration, 512 naming standards, 178 nesting, 178 permissions, assigning, 180 resource sharing, 177 policies, OU designs, 175-176 populating, 514 restricted groups controlling group membership, 916-917 modifying group membership, 917-919 scopes, 170, 511 security groups, 168-169, 510 Services and Applications group, 999 SID (Security ID), 172

single domain user administration, 512 structure designs, 165 types of, 120 universal, 120, 171 universal caching, 203 universal memberships, replicating, 135-136 guest operating system sessions (Hyper-V), 1326 configuration, 1330 BIOS. 1332 CD/DVD images, 1331-1332 COM ports. 1332 IDE controllers, 1332 network settings, 1331 processors, 1332 RAM, 1330 SCSI controllers, 1332 installation. 1327-1330 launching, 1332-1334 automatically, 1332-1333 manually, 1334 required components, 1327 saving state of, 1334 snapshots, 1334 creating, 1335 fault tolerance, 1335 image rollback, 1334-1335 reverting, 1336 GUI (graphical user interface), 13, 640 GUID Partition Table (GPT) disks, 942

Η

-h parameter Pathping command, 1174 tracert command, 1173 Handler Mappings feature page (IIS 7.0 websites), 350 hard drive failures (disaster recovery scenario), 1046 hard faults (memory), 1216 hardware compatibility testing, 444, 491 hot-swappable components, 5 monitoring, 629-630 network, fault-tolerant systems, 995-996 hardware configurations in Disk Management, 604 hardware failures (disaster recovery scenario), 1045 troubleshooting, 1087 hardware requirements IIS 7.0. 336 installing WSS, 1240-1241 OpsMgr. 722 Windows Server 2008 installations, 74 WSUS, 392 hardware-based disk arrays, 945 **HCAP** (Host Credential Authorization Protocol), 417 Health and Diagnostics role service (IIS 7.0), 339 health policy for compliant clients, creating, 422-423 for noncompliant clients, creating, 422 health policy compliance (NAP), 416 Health Registration Authority (HRA), 417 health state validation (NAP), 416 heartbeats (clustering), 1000 help features IT support for branch offices, 1114 in PowerShell, 664-667 hexadecimal numbers for IPv6 addressing, 286-287 hidden namespaces (DNS), 124 hierarchy DNS, 253-254 text. OU structures. 172 high-level business goals, identifying, 41 high-level migration project plan, 57 Hints file (DNS), 273 historical records, benefits of documentation, 686

history of DNS, 252-253 of ILM 2007. 226-227 of SharePoint, 1234-1235 of shells, 640-641 task history, 1187 of UNIX integration tools, 236 of virtualization, 1314 acquisition of Virtual PC, 1314 integration of Hyper-V, 1315-1316 Virtual Server 2005, 1314 Virtual Server 2005 R2, 1315 home pages (WSS), customizing, 1274-1276 honeypots, 388 Host (A) records, 258 Host Credential Authorization Protocol (HCAP), 417 host records (IPv6), adding in DNS, 292-294 host server settings (Hyper-V), 1324 Edit Disk option, 1325 Inspect Disk option, 1325 New Configuration Wizard, 1326 Stop Service option, 1326 virtual network switch management, 1324 virtualization settings, 1324 hosted applications for Terminal Services, planning for, 803 hosting applications, 660 HOSTS file, 252, 282 hot-swappable hardware components, 5 hotfixes. 620 HRA (Health Registration Authority), 417 HTTP Redirect feature page (IIS 7.0 websites), 350 HTTP Response Headers feature page (IIS 7.0 websites), 350 hub-and-spoke replication design example, 207-208 hub-and-spoke topology, 977 Hyper-V, 6 Administrative Console, launching, 1322-1323 connecting to different virtual server system, 1323

Edit Disk option, 1325 guest operating system sessions, 1326 configuration, 1330-1332 installation, 1327-1330 launching, 1332-1334 required components, 1327 saving state of, 1334 Inspect Disk option, 1325 installation, 1319 Server Manager, 1320-1322 Windows Server 2008 as host operating system, 1320 integration into Windows Server 2008, 1315-1316 managing with MMC, 1322-1323 with Server Manager, 1322 New Configuration Wizard, 1326 new features, 1316 running other services on, 1318-1319 server requirements, 1317-1318 as server role, 1317 snapshots, 1319, 1334 creating, 1335 fault tolerance, 1335 image rollback, 1334-1335 reverting, 1336 Stop Service option, 1326 virtual network switch management, 1324 virtualization settings, 1324

/I parameter (DCDiag command), 1178
-i parameter (Ping command), 1172
I Accept the License Terms option (Install Windows Wizard), 91
IDE controllers, configuring for guest operating system sessions, 1332
Identity Federation, 409
Identity Integration Feature Pack, 227

Identity Lifecycle Manager. See ILM 2007 identity management (ILM 2007), 229, 231-232 Identity Management for UNIX adding NIS users to Active Directory, 245 components of, 243-244 configuring password synchronization, 245 installing, 244-245 idle task conditions, 1185 IGMP Multicast mode (clusters), 1033 IHVs (Independent Hardware Vendors), 952 IIFP (Identity Integration Feature Pack), 227 **IIS (Internet Information Services)** backing up, 1071 configuration for WSS, 1244-1245 IIS 7.0 features associated with, 349-351 **IIS 6 Management Compatibility feature** (IIS 7.0), 339 IIS 6.0 legacy tools, starting, 353 IIS 7.0, 30-31, 331 fault-tolerance requirements, 337 FTP service "out-of-band" FTP service features, 352 "out-of-band" FTP service, configuring, 356-361 "out-of-band" FTP service, installing, 353-354 "out-of-the-box" FTP service, installing, 353 secure FTP site, creating with SSL, 354-356 versions of, 351-352 hardware and software requirements, 336 IIS Manager console, 333 nodes in Connections pane, 335 panes in, 333-334 starting, 336 installing, 337 modular-based installation, 337-340 Web Server role service, installing, 340-342 new features, 332-333 planning and designing, 336-337

security, 361 administrator roles, 367-368 auditing services, 363 authentication, 362-363 feature delegation, configuring, 369 logging, 369-370 SSL certificates, 363-367 user accounts, assigning permissions, 368-369 user accounts, creating, 368 Windows Server 2008 security, 362 upgrading to, 342-343 websites, 343 configuring properties of, 346-351 creating, 343-344 virtual directories, creating, 345 IIS Management Console feature (IIS 7.0), 339 **IIS Management Scripts and Tools feature** (IIS 7.0), 339 IIS Manager console, 333 nodes in Connections pane, 335 panes in, 333-334 starting, 336 IIS Server (IIS Manager Connections pane), 335 ILM (Identity Lifecycle Manager 2007), 226, 246 account provisioning, 232-233 group management, 231 history of, 226-227 identity management, 229, 231-232 IIFP, 227 installing, 229-230 management agents, 229 overview, 233 SQL Server database, 228 terminology, 228-229 image types, WDS (Windows 2008 Deployment Services), 844 images boot images adding to WDS servers, 848-850 WDS (Windows 2008 Deployment Services), 844

capture images creating custom installations, 859-861 WDS (Windows 2008 Deployment Services), 844 CD/DVD images, mounting, 1331-1332 discover images creating, 853-854 creating bootable media, 854-856 WDS (Windows 2008 Deployment Services), 844 installation images adding to WDS servers, 850 customizing with unattended answer files, 861-862 deploying, 850-853 WDS (Windows 2008 Deployment Services), 844 multicast images, 862-863 rollback, snapshots, 1334-1335 imaging systems (WDS), 842-843 Implementation phase (migration process), 441 implementation timeframes, determining, 46-48 Import-Alias cmdlet (PowerShell), 655 importing management packs (OpsMgr). 729-730 in-place upgrade, new hardware migration versus, 441-442 inbound rules (firewalls), creating, 382-385 Incoming E-Mail Settings, configuring, 1247-1248 incremental universal group membership replication, 171 incremental zone transfer (IXFR), 267-268, 1227 Independent Hardware Vendors, 952 indexing content sources, 1238 information for structured design documents, organizing budget estimates, 54-55 end state (technology configurations), 54-55 executive summaries, 54 network background information. 54-55 project goals and objectives, 54 solutions, implementation approach, 54-55 table of contents (sample), 54

information overload management. Windows Server 2008 migration, 52 Information Rights Management (IRM), 1238 infrastructure, recovering, 1083 infrastructure master (OM role), 115 inheritance, GPO link inheritance, 544-546 Initial Configuration Tasks Wizard, 14-15, 83-84, 582-583 Add Features link, 88 Add Roles link, 87 administrator passwords, 84 Configure Networking setting, 86 Download and Install Updates link, 87 Enable Automatic Updating and Feedback link, 86 Provide Computer Information section, 86 Set Time Zone link, 85 initial masters, 977 Innovate on Windows Server partner program, 493 Inspect Disk option (Hyper-V), 1325 Install Now page (Install Windows Wizard), 80 Install Windows Wizard, 90 Compatibility Report page, 91 Get Important Updates for Installation Page, 90 I Accept the License Terms option, 91 Install Now page, 80 Please Read the License Terms page, 82 Select the Operating System You Want to Install page, 91 Type Your Product Key for Activation page, 91 Upgrading Windows page, 92 Which Type of Installation Do You Want page, 82, 91 installation images adding to WDS servers, 850 deploying, 850-853 WDS (Windows 2008 Deployment Services), 844 installation media, manual installation of operating systems (WDS), 841 installing, 342, 804, 1009 AD CS, 404-407 AD FS, 224-225

AD LDS. 219-222 AD RMS, 409-411 ADMT 3.1, 462-463 agents (OpsMgr), 729-731 applications, 492 on Terminal Servers, 809 **BitLocker Drive Encryption** command prompt installations, 1134 Server Manager installations. 1133-1134 CALs (client access licenses), 828-829 DFS. 978 folders and replication groups, creating, 981-983 namespace and root, creating, 978-980 namespace servers, adding, 980-981 replication, 984 DHCP 304-306 DNS. 254-257 exported password keys, 464-465 Failover Clustering feature, 1011 features. 587 File Services role, 953-955 FSRM (File Server Resource Manager), 963-964 **GPMC** (Group Policy Management Console), 886 guest operating system sessions (Hyper-V), 1326 required components, 1327 step by step process, 1327-1330 Hyper-V server role, 1319 Server Manager, 1320-1322 Windows Server 2008 as host operating system, 1320 Identity Management for UNIX components, 244-245 IIS 7.0, 337 modular-based installation, 337-340 Web Server role service, installing, 340-342 ILM 2007, 229-230 management packs (OpsMgr), 729 Network Load Balancing feature, 1031

NLB clusters, 1031 applications/services, 1030 filtering modes, 1032 network cards, 1033 operation modes, 1033 port rules, 1031 NPS, 419-421, 756-757 "out-of-band" FTP service, 353-354 "out-of-the-box" FTP service, 353 PowerShell, 644-645 Print Management console, 526 Print Services Tools, 886 RODC. 1117 full Windows Server 2008 installations. 1118, 1120-1122 prerequisite tasks, 1117 staged installations, 1125-1129 Windows Server 2008 Server Core installations, 1122-1125 Server Core, 93 changing administrator passwords, 95 changing computer names, 96 custom installations, 94 DNS assignments, 96-97 domains, 97 feature configurations, 98 launching command prompt, 95 role configurations, 97-99 static IP address assignments, 96-97 Services for NFS, 238-239 SUA (Subsystem for UNIX-based Applications), 242-243 Telnet Server, 246-247 Terminal Server role service, 807-809 TS Licensing role service, 827 TS Session Broker, 825 TS Web Access role service, 812-814 WDS (Windows 2008 Deployment Services), 845 adding boot images to WDS servers, 848-850 adding installation images to WDS servers, 850

configuring DHCP, 848 configuring WDS servers, 845-848 deploying first install images, 850-853 Windows Media Encoder, 1304 Windows Media Services, 1289-1290 Windows Server 2008 32-bit processor support, 74 64-bit processor support, 74 computer name selection, 77 currency customization, 80 domain name determination, 78 edition selection, 75 file backups prior to installation, 79 hardware requirements, 74 Install Now page (Install Windows Wizard), 80 installation type selection, 82 IP address assignments, 78 keyboard preferences customization, 80 language customization, 80 licensing agreements, 82 location selection, 82-83 memory requirements, 74 network protocol configuration, 78 new installations versus upgrades, 75 OS selection, 81 Please Read the License Terms page (Install Windows Wizard), 82 product keys, 80 server task determination. 77 server type selection, 77 TCP/IP installations, 78 time customization, 80 unattended installations. 100 Which Type of Installation Do You Want page (Install Windows Wizard), 82 workgroup name determination, 78 Windows Server 2008 updates, 87 Windows Server Backup, 1054-1057 WINS, 319-320 WSRM (Windows System Resource Manager), 1208

WSS. 1240 checking for updates, 1243-1244 default site collection components. 1248-1251 finishing with Central Administration console, 1245-1247 IIS configuration, 1244-1245 Incoming E-Mail Settings configuration, 1247-1248 SMTP service installation, 1247-1248 system requirements, 1240-1241 WSUS, 392-394 Integrated Windows authentication (IIS 7.0), 362 integration directories, networks, 299 Office integration with WSS, 1266 Access 2007, 1270-1271 Excel 2007, 1267-1269 Word 2007, 1266-1267 WINS and DNS, 317-318 interfaces, 112, 639 Interix, 242 internal namespaces (DNS), 124, 142 Internet. See also IPv4; IPv6 addresses, dotted-decimal format, 205 DNS (domain name system) namespaces, 124 standards, Microsoft adoption, 108 Internet Information Server and Site Server, 107 Internet Information Services, See IIS Internet Protocol Security. See IPSec Internet Protocol version 4, 205, 288-289 Internet Protocol version 6. See IPv6 Interrupts/sec counter, 1219 Intersite Topology Generator Algorithm, 204 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), 207, 288 intranet, need for improvement, 1239 inventory applications, 483 network systems, 482-483 inventory sheets, applications, 484

IP addresses APIPA, 78 dynamic IP addresses, 78 number with IPv6, 285-286 static IP addresses, 78 Server Core installations, 96-97 Windows Server 2008 installations, assigning in, 78 IP and Domain Restrictions feature page (IIS 7.0 websites), 350 IP Security Policies on Active Directory. **Computer Configuration Windows Settings** node. 873 IPCONFIG command-line utility, 283-284, 1174 IPSec, 23, 411-412, 418, 431, 748 advantages of, 750-751 comparing with PPTP and SSTP, 749-750 connections, authentication for, 745 functionality in, 412 NAT-T, 412-413 IPv4, 205, 288-289 IPv4-compatible addresses, 289 IPv4-mapped addresses, 289 IPv6, 16, 205, 285 addresses, 206, 286-288 advantages, 207 compatibility with IPv4 6to4 addresses, 289 IPv4-compatible addresses, 289 IPv4-mapped addresses, 289 ISATAP, 288 configuring, 289 adding IPv6 host records, 292-294 DHCPv6 scope setup, 292-293 DHCPv6 server setup, 291-292 manually setting addresses, 290 migration, 207 new features, 286 number of IP addresses with, 285-286 structure, 205-206 IRM (Information Rights Management), 1238 ISAPI Filters feature page (IIS 7.0 websites), 350

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), 207, 288 ISCSI storage, 1008 ISDN records, 261 "island" DNS problem, 257, 276 ISTG (Intersite Topology Generator Algorithm), 204 IT support, branch offices, 1114 item-level targeting (GPOs), 880 iterative queries (DNS), 268-269 IXFR (incremental zone transfer), 267-268, 1227 IXFR Request Received (DNS zone transfer counter), 1227 IXFR Request Sent (DNS zone transfer counter). 1227 IXFR Response Received (DNS zone transfer counter), 1227 IXFR Success Received (DNS zone transfer counter), 1227 IXFR Success Sent (DNS zone transfer counter), 1227

J–K

-j parameter Ping command, 1172 tracert command, 1173 jetpack program, 315 junction points, 943 -k parameter (Ping command), 1172 KCC (Knowledge Consistency Checker), 188, 195 Kerberos, 110, 125-126, 188 KEY (Public Key) records, 261 keyboard preferences, 80 keyboard release key, setting, 1324 knowledge management, 689 knowledge sharing, 688-689 Korn shell, 640

L

/I parameter (NetDiag command), 1177 -I parameter (Ping command), 1172 L2TP (Layer 2 Tunneling Protocol), 431, 747-748 advantages of, 750-751 comparing with PPTP and SSTP 749-750 connections, authentication for, 745 firewall rules for, 753 L2TP/IPSec VPNs. 431-432 lab-testing compatibility, 491 applications, installing, 492 Certified for Windows Server 2008, 493 hardware allocation/configuration, 491 Windows Server 2008 allocation/ configuration, 491 labs building, 63 testing process results, 63-64 LAN diagnostic reports (Reliability and Performance Monitor), 1206 languages, customizing, 80 latency, replication, 189-190 launching Event Viewer, 1150 guest operating system sessions (Hyper-V), 1332-1334 automatically, 1332-1333 manually, 1334 PowerShell, 644-645 Task Manager, 1145-1146 Layer 2 Tunneling Protocol. See L2TP layers of security, 376 LDAP (Lightweight Directory Access Protocol), 106-107, 113-114, 166 Idifde.exe. 1066 learning curve for collaboration, 1239 legacy FTP service, 351 legacy systems, lack of ability to upgrade, 474 Level property (events), 1151 levels of transport-level security, 400 LGPO (Local Group Policy Object), 867 libraries, document libraries, 1251

licenses for Terminal Services deploying, 827-829 planning for, 803-804 licensing agreements Windows Server 2008 installations, 82 Windows Server 2008 upgrades, 91 Lightweight Directory Access Protocol, 106-107, 113-114, 166 lingering objects Active Directory, removing from, 136 deleting, 203 link enforcement (GPOs), 543-544 linked-value replication, 202 linking WMI filters to GPOs, 573 links, 121 AD sites, 192, 194 bridgeheads, 197 bridging, 194 replication schedules, 193 replication topology, 200 domain Group Policy links, 563 organizational unit Group Policy links, 563 site Group Policy links, 562-563 site links, 502 creating, 506-507, 509 links (GPOs), 543-544 blocking inheritance, 545-546 configuring, 571 creating, 571 inheritance, 544-545 order of processing, 545-546 managing, 574 Linux shells, 640 listing files/directories in PowerShell, 672-673 lists in WSS, 1236, 1251, 1261-1262 Calendar list, 1262-1264 custom lists, 1265 exporting to, 1268-1271 Tasks list, 1265 live broadcasts, 1305 initiating, 1305-1307 pulling content, 1306-1307 pushing content, 1306

LMHOSTS file, 323 load balancing, 995 Drain mode (Terminal Services), 799-800 with Network Load Balancing (NLB), 799 TS Session Broker, 798-799 WSRM (Windows System Resource Manager), 799 load testing, Windows Media Services, 1287-1288 Local Administrator account (OpsMgr), 728 local administrators user policies, 867 local computer policies, 537, 867 local domain group policies, 868 local group policies, 865 benefits of, 874-875 creating local administrators and non-administrators policies, 875-876 Local Group Policy Object, 867 local non-administrators user policies, 867 local policies, 536-538 local computer policies, 537 local user policies, 537 management tools, 554 ADMX Migrator, 559 DFS Management console, 561 Event Viewer, 560-561 GPLogview, 559 GPMC (Group Policy Management Console), 554-555 GPO scripts, 558 GPOE (Group Policy Object Editor), 555-556 gpupdate.exe, 557-558 Microsoft Desktop Optimization Pack for Software Assurance, 558 Print Management console, 556-557 multiple local policies, 537 security settings, Computer Configuration Windows Settings node, 872 security templates, 538 local resource redirection with Terminal Services, 789 .NET devices, 792 disk drives, 790

local time zones, 791 plug and play devices, 792 printers, 790-791 local scope in PowerShell, 656 local security policies, 867 Local Security Policy snap-in, configuring **Terminal Services**, 810 local site target servers, restricting access, 986-987 local time zone redirection with Terminal Services, 791 local user policies, 537 local user profiles, 516 log file (.evtx) format, 1157 logging **Event Viewer** Applications and Services Logs folder, 1154 custom views, 1152-1153 Custom Views folder, 1152 data organization, 1156 event archiving, 1157 event logs, 1155-1158 event properties, 1151 event subscriptions, configuring, 1154-1155 launching Event Viewer, 1150 overview, 1149-1151 security logs, 1158-1159 Subscriptions folder, 1154 Windows Logs folder, 1153 GPO events. 560-561 in IIS 7.0. 369-370 Task Manager, 1145-1146 application monitoring, 1147 network monitoring, 1148-1149 performance monitoring, 1147-1148 process monitoring, 1147 service monitoring, 1147 user activity monitoring, 1149 Logging feature page (IIS 7.0 websites), 351 Logical Disk object, 1220 Logical Unit Number (LUN), 1001

logins

restricting, 377-378 smartcards, 379 logs, 593 loopback processing GPOs, 549-550 policy processing, 869 looping videos, 1298 lost data, 1092 LUN (Logical Unit Number), 1001

Μ

Machine Key feature page (IIS 7.0 websites), 347 machine local groups, 120, 170 Machine subfolder (GPOs), 540 Macintosh computers, Services for Macintosh, 941 Mail Exchanger (MX) records, 260 mail-enabled groups, 169-170 Mailbox (MB) records, 261 maintenance, 587, 634, 833 daily maintenance procedures, 626-628 DHCP databases, 314-315 of failover clusters, 1026 importance of, 620 monthly maintenance procedures, 634-635 NLB nodes, 1039-1040 offline DFS servers, 985-986 guarterly maintenance procedures, 635-636 service packs (SPs) and updates, 620 automatic updates, 622-625 manual updates, 621 Windows Server Update Services (WSUS), 623, 625 weekly maintenance procedures, 629-634 WINS databases, 325 maintenance documentation, 702 Active Directory infrastructure documentation, 703-704 administration manual, 705

checklists, 703 configuration (as built) documents, 704-705 policy documents, 703 procedure documents, 702 security procedure documents, 706 server build procedure documents, 704 topology diagrams, 705 troubleshooting documents, 706 majority-based cluster membership, 29 management, 499, 833 Management Agents, 228 ILM 2007, 229 OpsMgr. 718 run profiles, 229 management groups (OpsMgr), 719-720 geographic-based groups, 724-725 multiple groups, 724 political-based groups, 725 security-based groups, 725 management packs (OpsMgr), 716, 719 importing, 729-730 installing, 729 third-party management packs, 721 Management Server Action account (OpsMgr), 728 management servers (OpsMgr), 718, 724, 726 Management Service feature (IIS 7.0), 339 management tools, 587 for auditing, 605 audit policies, 605-607, 609 resource access auditing, 609-612 for DFS, 984-987 Disk Management console, 946 adding disks to Windows 2008, 946-948 converting basic disks to dynamic disks, 948 creating fault-tolerant volumes, 948-950 Diskpart.exe utility, 946 creating fault-tolerant volumes, 950-952 for external disk storage, 945 for file systems, 939

FSRM (File Server Resource Manager), 961-962 file screen exceptions, creating, 969 file screen templates, creating, 968-970 file screens, creating, 967-968 file system services, troubleshooting, 971 global options, configuring, 964 installing, 963-964 quota templates, creating, 966-967 quotas, adjusting, 965-966 quotas, configuring, 964-965 reports, generating, 970-971 uses for. 962-963 in IIS 7.0, 333 new features, 332 nodes in Connections pane, 335 panes in IIS Manager console, 333-334 starting IIS Manager console, 336 for local/group policies, 554 ADMX Migrator, 559 DFS Management console, 561 Event Viewer, 560-561 GPLogview, 559 GPMC (Group Policy Management Console), 554-555 GPO scripts, 558 GPOE (Group Policy Object Editor), 555-556 gpupdate.exe, 557-558 Microsoft Desktop Optimization Pack for Software Assurance, 558 Print Management console, 556-557 PowerShell, 643 remote management, 612 PowerShell, 616 Print Management console, 618-619 Remote Server Administration Tools. 612-615 ServerManagerCmd.exe, 616-618 Windows Remote Management (WinRM), 615-616 security risks, identifying, 619

Server Manager, 587-588 Configuration page, 596-601 Diagnostics page, 592-595 Features page, 592 Features Summary window, 588-589 role-specific pages, 588, 590-592 Roles Summary window, 588-589 Storage page, 601-604 Share and Storage Management console, 957-960 site collection management (WSS), 1271 with Central Administration console. 1276-1278 with Edit Page interface, 1274-1276 with Site Settings page, 1272-1273 System Center Operations Manager 2007, 619-620 in WSS, 1237 Management Tools role service (IIS 7.0), 339 management-level reporting documentation, 711, 713 managing Active Directory with policies, 911-912 configuring restricted groups for domain security groups, 915 deploying software packages, 921-924 extending Group Policy functionality, 919-921 fine-grained password policies, 912-914 GPO modeling, 926-929 managing group policies from administrative or remote workstations, 929-930 synchronous foreground refresh, 925-926 group policies from administrative or remote workstations, 929-930 IIS 7.0, administrator roles, 367-368 information overload, Windows Server 2008 migration, 52 NLB clusters backups, 1039 maintenance, 1039-1040 restores, 1039

security filters (GPOs), 573-574 updates, WDS, 840 User Account Control settings, 887-889 volumes, NTFS quotas, 961 mandatory user profiles, 516 manual backup options, 1053 manual backups to remote server shares, 1060-1062, 1064 manual failover testing, 1023-1024 manual updates, 621 manually launching Hyper-V guest sessions, 1334 manually running scheduled backups, 1060 manually setting IPv6 addresses, 290 MAs. See Management Agents -mask parameter (Route command), 1176 Master Boot Record (MBR) disks, 942 master pages in SharePoint Server 2007, 1238 masters domain naming (OM role), 115 infrastructure (OM role), 115 multi-master replication (Active Directory), 114 RID (Relative ID) (OM role), 115 schema (OM role), 114 matching criteria rules (WSRM), 1210 MB (Mailbox) records, 261 MBCA (Microsoft Baseline Configuration Analyzer), 1212 MBR (Master Boot Record) disks, 942 mean time between failures (MTBF), 629 mean time to repair (MTTR), 629 media, 1281 creating for global catalog, 143 media content bit rates, 1306 distribution methods, 1308 pushing/pulling, 1305 screens, capturing, 1309-1310 media management in Windows Server Backup, 1051-1052, 1095 media servers, 35 media sessions, capturing, 1308-1309 media-based GC/DC replication, 201

members of teams, roles and responsibilities, 60 memberships incremental universal group membership replication, 171 universal groups, replicating, 135-136 memory guest operating system sessions (Hyper-V), 1330 hard faults, 1216 Hyper-V requirements, 1317 soft faults, 1216 system, monitoring, 1215-1217 Virtual Memory, configuration options, 1217-1218 Windows Memory Diagnostics tool, 89 Windows Server 2008 support, 74 Windows Server 2008 upgrades, testing for, 89 Memory Diagnostics tool (Windows), 89 metadata, 1236 metadirectories, 228 defined. 226 ILM 2007. 226 MIIS. 227 MMS, 226 Metaverse Namespaces, 228 metric baselines, establishing, 1191-1192 -METRIC parameter (Route command), 1176 Microsoft, adopting Internet standards, 108 Microsoft Application Compatibility Toolkit, Windows Server 2008 upgrades, 89 Microsoft Baseline Configuration Analyzer (MBCA), 1212 Microsoft Cluster Service (MSCS), 800 Microsoft Desktop Optimization Pack for Software Assurance, 558 Microsoft Identity Integration Server, 227 Microsoft Management Console (MMC) access, managing users, 910-911 Microsoft Metadirectory Services, 226 Microsoft Office SharePoint Services 2007 (MOSS), 31 Microsoft Update, 901

Microsoft Virtual Server Virtual Server 2005, 1314 Virtual Server 2005 R2, 1315 Microsoft Windows Firewall, 898 mid-level compatibility testing, 480 migrating compatibility testing, 473 computer accounts, 468-470 failover clusters, 1027 groups, 466-467 high-level migration project plan, 57 IPv6. 207 user accounts, 467-468 to Windows Server 2008, 39, 439 Active Directory, 33-34 add-in application server functions, 36 adding to Windows 2000/2003 environment, 8-9 Big Bang migration, 443-448 Big Bang versus phased migration, 442 budget estimates, 54-55, 62 built-in application server functions. 34-36 business goals and objectives. identifying, 40-43 collaborative design decisions, 53-54 design agreements, 56 design decisions, 55-56 design phase, 52-53 discovery phase, 49-51 end state (technology configurations), 54-55 end-user satisfaction, verifying, 67 environment, supporting, 68 executive summaries, 54, 60 Gantt charts, 58 geographical depth and breadth, 51-52 in-place upgrade versus new hardware migration, 441-442 information overload management, 52 lab testing process results, 63-64 labs, building, 63 migration background, 60 migration documents, creating, 59

migration phase risks and assumptions, 60 migration planning phase, 57 migration process goals and objectives, 60 migration processes, 61-62 migration scenarios, 442-443 migration/implementation phase, 67 multiple domain consolidation migration, 460-471 network background information, 54-55 objectives, identifying, 440 phased migration, 447, 449-461 phases of, 440-441 pilot phase, 64-65 pilot phase, rolling out, 66 pilot results, documenting, 67 pilot users, application usage requirements, 66 pilot users, geographical diversity, 66 pilot users, quantity of, 66 pilot users, role requirements, 66 planning, 33 problem solving, 67 project goals and objectives, 54 project plans, 57-58, 62 project scope, 40 project timeline and milestones, 60 prototype phase, 62-63 solutions, implementation approach, 54-55 speed and risk, comparing, 58 structured design documents, organizing information, 54-55 table of contents (sample), 54 team members' roles and responsibilities, 60 technical goals and objectives, identifying, 43-49 training plans, 61 when to migrate, 8 from Windows 2000/2003 Active Directory, 9

migration documents, 53 budget estimates, 62 creating, 59 executive summaries. 60 migration background, 60 migration phase risks and assumptions, 60 migration process goals and objectives, 60 migration processes, 61-62 project plans, 62 project timeline and milestones, 60 team members' roles and responsibilities, 60 training plans, 61 migration planning phase (Windows Server 2008 migration), 57 budget estimates, 62 executive summaries, 60 Gantt charts, 58 migration background, 60 migration documents, creating, 59 migration process goals and objectives, 60 migration processes, 61-62 project plans, 57-58, 62 project timeline and milestones, 60 risks and assumptions, 60 speed and risk, comparing, 58 team members' roles and responsibilities, 60 training plans, 61 migration plans, 694-698 migration processes, goals and objectives, 60 migration timeframes, determining, 46-48 migration/implementation phase (Windows Server 2008 migration), 67 end-user satisfaction, verifying, 67 environment, supporting, 68 MIIS (Microsoft Identity Integration Server), 227 milestones in migration document, 60 MIME Types feature page (IIS 7.0 websites), 351 mirrored volumes, 944 mixed administrative model, 501 MMC (Microsoft Management Console) access Hyper-V. 1322-1323 managing users, 910-911

MMS (Microsoft Metadirectory Services), 226 MMS snap-ins for Windows Server Backup, 1054 models federated forests design, 151-154 groups business function-based designs, 178-181 design samples, 178 geographical-based designs, 181-183 multiple domain, 147 domains, adding, 148 real-world design example, 149 OUs business function-based designs. 178-179 design samples, 178 geographical-based designs, 181-182 single domain, 144 real-world design example, 146-147 selecting, 145 single forest real-world design example, 151 trees, 150 modes, authentication (Active Directory), 110 modes of operation in Terminal Services Remote Desktop mode, 787-788 Terminal Server mode, 788 modifying group memberships with restricted groups, 917-919 modular-based installation (IIS 7.0), 332, 337-340 Modules feature page (IIS 7.0 websites), 351 monitor spanning for Remote Desktop Connection, 793 monitoring, 605, 629 applications, Task Manager, 1147 choosing objects to monitor, 1170-1171 Event Viewer, 626-628 file systems, 939 hardware, 629-630 networks, Task Manager, 1148-1149 with OpsMgr, 715 performance, Task Manager, 1147-1148 processes, Task Manager, 1147

reducing performance monitoring overhead, 1169-1170 Reliability and Performance Monitor counters, 1162-1163 Data Collector Sets, 1165-1167 overview, 1159-1160 Performance Monitor, 1161-1164 Reliability Monitor, 1164-1165 reports, 1167-1168 Resource Monitor, 1160-1161 services, Task Manager, 1147 Terminal Services performance, 833 user activity, Task Manager, 1149 monitoring and performance documentation, 710 monitoring rules (OpsMgr), 717 monitors (OpsMgr), 716 monthly maintenance procedures, 634-635 MOSS (Microsoft Office SharePoint Services 2007), 31 mount points, 943 mounting CD/DVD images, 1331-1332 Move-Item cmdlet (PowerShell), 675 moving AD-integrated DNS zones to application partitions, 460-461 files/directories in PowerShell, 675 MSCS (Microsoft Cluster Service), 800 msdcs zone, 276-277 MTBF (mean time between failures), 629 MTTR (mean time to repair), 629 multi-master replication (Active Directory), 114 multicast delivery, compared to unicast delivery, 1292 multicast images, creating, 862-863 Multicast mode (clusters), 1033 Multicast scopes (DHCP), 313 multimaster replication, 186, 975 Multipath I/O storage, 1008 multiple domain consolidation migration, 443, 460-471 **ADMT 3.1** components of, 462 installing, 462-463 prerequisites for, 463

computer accounts, migrating, 468-470 groups, migrating, 466-467 PES (Password Export Server), 464 installing, 464-465 setting Registry permissions, 465 SID migration, configuring domains for, 465-466 user accounts, migrating, 467-468 multiple domain model, 147 domains, adding, 148 real-world design example, 149 user administration in, 512 multiple host mode (port filtering), 1032 multiple local policies, 537 multiple management groups in OpsMgr, 724 multiple RRs (resource records), assigning, 263 multiple upgrades, 475 multiple-site designs, 199 MVs (Metaverse Namespaces), 228 MX (Mail Exchanger) records, 260 My Sites, 1237

Ν

-n parameter Netstat command, 1175 Pathping command, 1174 Ping command, 1172 /n:NamingContext parameter (DCDiag command), 1177 name resolution, 251 networks, 298-299 Name Server (NS) records, 259 names DDNS (Dynamic DNS), 124 distinguished (Active Directory), 113 DNS (domain name system), 123 Active Directory, 123 Active Directory and foreign DNS, co-existing, 125 namespaces, 123-124 zones, comparing standard and AD-integrated, 125

How can we make this index more useful? Email us at indexes@samspublishing.com

domain naming master (OM role), 115 domain rename tool, 135 publishing points, 1291, 1295 relative distinguished (Active Directory), 113-114 UPN (user principal name), 141 namespace root (DFS), 974 creating, 978-980 namespace servers (DFS), 974 adding to domain-based namespaces, 980-981 namespaces, 141 DFS. 940. 972-974 creating, 978-980 domain DFS namespaces, 976 standalone DFS namespaces, 976 DNS, 123-124, 254 external, 123-124, 141-142 hidden. 124 internal, 124, 142 published, 123-124, 141-142 naming domains, 143, 160-163 global groups, 179 groups, standards, 178 NAP (Network Access Protection), 415, 741 characteristics of, 416 reasons for deploying, 416 terminology, 417 NAT (Network Address Translation), 412 NAT-T (NAT Transversal), 412 native commands (PowerShell), 649 NBT Redirector: Bytes Total/sec (network traffic counter), 1223 NBT Server: Bytes Total/sec (network traffic counter), 1223 neighbor detection, Next Generation TCP/IP stacks, 1141 nested control delegation, 182-183 nesting groups, 178 permissions, assigning, 180 sharing resources, 177 OU (organizational unit) structures, 166

.NET Application Settings feature page (IIS 7.0 websites), 347 .NET Compilation feature page (IIS 7.0 websites), 346 .NET device redirection with Terminal Services, 792 .NET Framework integration in PowerShell, 649 Extended Type System (ETS), 650 reflection, 650 type accelerators, 651-652 .NET Globalization feature page (IIS 7.0 websites), 346 .NET objects, creating in PowerShell, 682-683 .NET Profile feature page (IIS 7.0 websites), 346 .NET Roles feature page (IIS 7.0 websites), 346 .NET Trust Levels feature page (IIS 7.0 websites), 347 .NET Users feature page (IIS 7.0 websites), 347 NetBIOS, 317 NetDiag command, 1177 NetIQ Corporation website, 1214 Netsh. 314 Netstat command, 1175-1176 network access issues, troubleshooting, 1087-1088 Network Access Protection (NAP), 415, 741 network access restriction policies, Computer **Configuration Windows Settings node, 873** network access types for NPS enforcement policies, 418 Network Address Translation (NAT), 412 Network Authentication, 830 network cards, NLB clusters, 1033 network configuration documentation, 706-707 network device documentation, 707 Network Device Enrollment Service role service, 404 Network File System, 238, 941 network list manager policies, Computer **Configuration Windows Settings node, 872** Network Load Balancing (NLB), 998 IIS 7.0 fault tolerance, 337 installing, 1031 in Terminal Services, 799

Network Location Awareness (NLA), 535, 549 Network Monitor, 1194, 1196 blogs, 1196 capture filters, 1198 Capture tab, 1198 captured streams, filtering, 1198-1199 filters applying filters, 1199 capture filters, 1198 color filters, 1198 display filters, 1198 removing filters, 1199 network traffic capturing, 1198, 1201 parsing captured data, 1202 new features of, 1197-1198 network operating system (NOS), whether to upgrade, 44 network outages (disaster recovery scenario), 1045 troubleshooting, 1084 network policy for compliant clients, creating, 423-425 for noncompliant clients, creating, 424. 426-428 RRAS, modifying, 434-435 Network Policy Server (NPS), 417, 741-743, 757 network policy servers, 35 Network Printer Installation Wizard, 528 network protocols, configuring, 78 network settings, guest operating system sessions (Hyper-V), 1331 network shared resources, adding printers as, 526-528 network subsystems, monitoring, 1221-1222 network systems, inventory, 482-483 network task conditions, 1186 network topology diagrams, 705 networking requirements for Terminal Services, planning for, 803 Networking tab (Task Manager), 1148-1149. 1195

networks addressing, 298 background information, design documents. 54-55 cluster networks, configuring, 1015-1017 directory integration, 299 enterprise, 298 addressing, 298 directory integration, 299 name resolution, 298-299 network services, 299 hardware, fault-tolerant systems, 995-996 monitoring, Task Manager, 1148-1149 name resolution, 298-299 NBT Redirector: Bytes Total/sec (network traffic counter), 1223 NBT Server: Bytes Total/sec (network traffic counter), 1223 NOS (network operating system), whether to upgrade, 44 resource distribution, viewing, 118 services, new features, 299 traffic, monitoring, 1222 VPN, 739 WAN, branch offices, 1140-1143 Windows Server 2008 configurations, 86 wireless, physical security, 380 New Configuration Wizard, 1326 new hardware migration, in-place upgrade versus, 441-442 New menu (WSS document libraries), 1254 New-Alias cmdlet (PowerShell), 655 New-Item cmdlet (PowerShell), 673-674 New-Object cmdlet (PowerShell), 682-683 Next Generation TCP/IP stacks, 1140-1141 NFS (Network File System), Services for NFS, 238, 941 NFS shared network resources, creating, 241-242 NIS users, adding to Active Directory, 245 NLA (Network Location Awareness), 535, 549 NLB (Network Load Balancing), 998 IIS 7.0 fault tolerance, 337 in Terminal Services, 799

NLB clusters, 1002-1003 adding nodes to, 1037-1038 backing up, 1039 creating, 1033-1037 installing, 1031 applications/services, 1030 filtering modes, 1032 network cards, 1033 operation modes, 1033 port rules, 1031 maintenance, 1039-1040 restoring, 1039 No Majority: Disk Only Quorum model (failover clusters), 1004 Node and Disk Majority Quorum model (failover clusters), 1003 Node and File Share Majority Quorum model (failover clusters), 1004 Node Majority Quorum model (failover clusters), 1003 nodes, 999 adding to failover clusters, 1016-1017 NLB clusters adding to, 1037-1038 backing up, 1039 maintenance, 1039-1040 restoring, 1039 removing, 1027 non-administrators, creating local group policies, 875-876 non-Microsoft DNS implementations, AD DS in, 278 non-Microsoft Kerberos realms, 408 non-Windows device integration in OpsMgr, 721 noncompliant clients health policy, creating, 422 network policy, creating, 424, 426-428 NOS (network operating system), whether to upgrade, 44 NPS (Network Policy Server role), 35, 417, 741-743 components of, 417-418 configuring, 758-763 enforcement policies for network access, 418

installing, 419-421, 756-757 RADIUS authentication in, 418-419 RRAS network policy, modifying, 434-435 validation process, 421 configuring DHCP server for, 428-429 health policy for compliant clients, creating, 422-423 health policy for noncompliant clients, creating, 422 network policy for compliant clients, creating, 423-425 network policy for noncompliant clients, creating, 424, 426-428 System Health Validator, creating, 421-422 NS (Name Server) records, 259 Nslookup command, 1176 troubleshooting DNS, 282-283 NT LAN Manager, 110 Ntbackup, 1050 NTFS (NT File System), 386, 936 file-level security, 386-387 self-healing NTFS. 4 share-level security, compared, 387 NTFS folders, enabling auditing, 1089-1091 NTFS permissions for namespace roots/folder targets, 976 troubleshooting, 1088-1091 validating, 1091 NTFS volumes, quota management, 960-961 NTLM (NT LAN Manager), 110 NTSDUTIL command-line utility, moving Operation Master (OM) roles, 455-457

0

-o parameter (Netstat command), 1175 objectives business, identifying, 40 business unit/departmental goals, 42-43 high-level business goals, 41

migration processes, 60 projects, design documents, 54 technical, identifying, 43-44 deployment team participants, defining, 48-49 design team participants, defining, 48-49 scope of work, defining, 44-46 timeframes (implementation or migration), determining, 46-48 objects Active Directory OUs (organizational units), 166 schema, 112 Computers folders, 166 connection, replication, 188-189 Container class, 166 Logical Disk, 1220 Users folders, 166 **OCSetup command-line program** command lines, 99 command options, 98 Server Core role/feature configurations, 98 Office integration with WSS, 1266 Access 2007, 1270-1271 Excel 2007, 1267-1269 Word 2007, 1266-1267 offline DFS servers, maintaining, 985-986 offline files, CSC (client-side caching), 956-957 OM (operations master) roles Active Directory, 114-115 domain naming master, 115 infrastructure master, 115 moving, 455-457 PDC emulators, 115 RID (Relative ID) master, 115 schema master, 114 on-demand publishing, compared to broadcast publishing, 1295 on-demand publishing points, playlists, 1300 on-demand video, 1294 one-way cross-forest trusts, 153 Online Responder role service, 404

operating systems for failover clusters, selecting, 1009 NOS (network operating system), whether to upgrade, 44 WDS, deploying, 840-841 Operation Master (OM) roles. See OM roles operation modes, NLB clusters, 1033 operational events (GPOs), 561 Operations Console (OpsMgr), 718, 720 operations database (OpsMgr), 717, 719, 726 operations database server (OpsMgr), 723 operations master, 114 **OpsMgr** (System Center Operations Manager), 715, 1194, 1213 accessing, 720 Active Directory integration in, 721 agents, 719 installing, 729-731 capacity limits, 726 components of, 717-718 data storage in, 719 database size, 725-726 deployment scenarios, 723-724 features of, 716-717 management groups, 719-720 geographic-based groups, 724-725 multiple groups, 724 political-based groups, 725 security-based groups, 725 management packs, 719 importing, 729-730 installing, 729 non-Windows device integration in, 721 performance monitoring, 721, 732 redundancy in, 726-727 reports in, 720-721 requirements agent deployment, 723 backups, requirements for, 723 hardware requirements, 722 software requirements, 722-723

security in, 727 agent security, 727 firewall requirements, 728 service accounts, 728 settings, configuring/viewing, 720 third-party management packs, 721 optimizing GPO processing, 548 group policies, 521-523 Terminal Services performance, 832-833 options startup options, 1075 in Windows Server Backup, 1053-1054 order of processing for group policies, 523 organizational benefits of documentation, 686 organizational unit Group Policy links, 563 organizational units, 118, 166 organizing Event Viewer data, 1156 information for structured design documents, 54-55 budget estimates, 54-55 end state (technology configurations), 54-55 executive summaries, 54 network background information, 54-55 project goals and objectives, 54 solutions, implementation approach, 54-55 table of contents (sample), 54 **Originating Writes, Active Directory** replication, 123 OS (Operating Systems) Windows Server 2008 installations, selecting for, 81 Windows Server 2008 upgrades, selecting for, 91 OUs (organizational units), 118, 166 Active Directory, 118-119, 166-167 administering, delegating, 174-175 designs, 172-173 business function-based designs, 178-179 domain designs, 173

flexibility, 173 geographical-based designs, 181-182 group policies, 175-176 model samples, 178 domain trusts, replacing, 182 domains, comparing, 118-119 group designs, 171-172 and groups, comparing, 121 network resource distribution, viewing, 118 structure, 146 design, 165 nesting, 166 text hierarchy, 172 Out-Csv cmdlet (PowerShell), 674 Out-Default cmdlet (PowerShell), 653 Out-File cmdlet (PowerShell), 674 "out-of-band" FTP service, 352 configuring, 356-361 features of, 352 installing, 353-354 "out-of-the-box" FTP service, 351, 353 outbound rules (firewalls), creating, 382-385 Outlook 2000 Team Folder Wizard, 1234 Output Caching feature page (IIS 7.0 websites), 351

Ρ

-P parameter (Netstat command), 1175 -p parameter Pathping command, 1174 Route command, 1176 Packet Internet Groper (Ping), 1171-1172 page layouts in SharePoint Server 2007, 1238 Pages and Controls feature page (IIS 7.0 websites), 347 Pages/sec counter, 1216-1217 parallel sessions, 5 parameters (PowerShell), 646 participants on teams, 48-49 partitions, 943 configuring, BitLocker Drive Encryption, 1132-1133 file formats for, 936 passive nodes, clustering, 999 Password Export Server, 464 password keys exporting, 464 installing exported, 464-465 Password Settings Objects (PSO), 127 attributes of, 128, 130 creating, 130-131 Password Synchronization role, 243 configuring, 245 passwords Active Directory, multiple password policy implementation per domain, 127-128, 130-131 administrator passwords Server Core installations, 95 when to change, 635 Windows Server 2008 configurations, 84 BitLocker Drive Encryption, 1139 for DSRM (Directory Services Restore mode), 1067-1068 fine-grained password policies, 127, 142, 912-914 PSO (Password Settings Objects), 127 attributes of, 128, 130 creating, 130-131 patch surfaces, 585 patches, 390, 488, 620 Pathping command, 1173-1174 PDC emulators (OM role), 115 **PEAP** (Protected Extensible Authentication Protocol), 744 performance, 1214. See also performance optimization baselines, 1169-1171 choosing objects to monitor, 1170-1171 monitoring OpsMgr, 721, 732 Task Manager, 1147-1148 reducing performance monitoring overhead, 1169-1170

Reliability and Performance Monitor, 20 counters, 1162-1163 Data Collector Sets. 1165-1167 overview. 1159-1160 Performance Monitor, 1161-1164 Reliability Monitor, 1164-1165 reports, 1167-1168 Resource Monitor, 1160-1161 Windows Media Services, 1284 performance counters AD (Active Directory), 1224 DC (domain controller), 1226 DNS (domain name system), 1226 performance documentation, 710-711 Performance Monitor, 282, 593-595, 1161-1164, 1202 adding counters with, 1162-1163 capacity analysis, 1204 configuring, 1164 performance optimization AXFR Request Received (DNS zone transfer counter), 1227 AXFR Request Sent (DNS zone transfer counter), 1227 AXFR Response Received (DNS zone transfer counter), 1227 AXFR Success Received (DNS zone transfer counter), 1227 AXFR Success Sent (DNS zone transfer counter), 1227 bottlenecks, 1215 Cache % Hit (Active Directory performance counter), 1225 Cache Page Fault Stalls/sec (Active Directory performance counter), 1225 Cache Page Faults/sec (Active Directory performance counter), 1225 Cache Size (Active Directory performance counter), 1225 DC, 1223 AD (Active Directory) replication, monitoring, 1224 AD (Active Directory), monitoring, 1223-1225 DNS (domain name system), monitoring, 1224, 1226-1227

Dynamic Update Received/Sec (DNS performance counter), 1226 GPO processing, 548 IXFR Request Received (DNS zone transfer counter). 1227 IXFR Request Sent (DNS zone transfer counter), 1227 IXFR Response Received (DNS zone transfer counter), 1227 IXFR Success Received (DNS zone transfer counter), 1227 IXFR Success Sent (DNS zone transfer counter), 1227 Recursive Queries/Sec (DNS performance counter), 1226 Recursive Query Failure/Sec (DNS performance counter), 1226 Secure Update Received/Sec/Sec (DNS performance counter), 1226 server roles, 1223 TCP Query Received/Sec (DNS performance counter), 1226 TCP Response Sent/Sec (DNS performance counter), 1226 Terminal Services, 832-833 Terminal Services Server, 1228 Total Query Received/Sec (DNS performance counter), 1226 Total Response Sent/Sec (DNS performance counter), 1226 UDP Query Received/Sec (DNS performance counter), 1226 UDP Response Sent/Sec (DNS performance counter), 1226 virtual servers, 1228 Performance role service (IIS 7.0), 339 Performance tab (Task Manager), 1147, 1195 performing remote Group Policy Results with **GPMC**, 930 permissions assigning to nested groups, 180 delegate, selecting, 175 for IIS 7.0 user accounts, assigning, 368-369

NTES namespace roots/folder targets, 976 validating, 1091 security groups, sharing, 168 share permissions, 955-956, 959 validating, 1088-1089 troubleshooting, 1088-1091 persistent aliases (PowerShell), creating, 655 PES (Password Export Server), 464 installing, 464-465 setting Registry permissions, 465 phantom domain controllers, removing, 457-458 phased migration, 443, 447, 449-461 AD-integrated DNS zones, moving to application partitions, 460-461 Big Bang migration versus, 442 domain and forest functional levels, 459-460 domain controllers preparing with adprep, 451-453 replacing existing, 454-455 updating existing, 453-454 upgrading versus, 450-451 Operation Master (OM) roles, moving, 455-457 phantom domain controllers, removing, 457-458 Windows 2000/2003 domain controllers, removing, 457 physical disaster (disaster recovery scenario), 1045 Physical Disk object, 1220 physical disks in Disk Management, 604 physical placement of Terminal Servers, planning for, 802 physical security, 376 access, restricting, 377 administrative access, 378-379 branch offices, 1113 firewalls, 380 logins, restricting, 377-378 smartcards, 379 wireless networks, 380

physical site failure scenario (disaster recovery), 1084-1085 picture library in WSS, 1253 pilot phase (Windows Server 2008 migration), 64-67.441 pilot test plans, 702 Ping command, 1171-1172 pipeline in PowerShell, 652-653 PKI (Public Kev Infrastructure), 401 certificates, 402 non-Microsoft Kerberos realms, 408 private kevs. 401 public kevs. 401 smart cards, 407 placeholder domain model, 158 placement, AD global catalog, 325-327 planning compatibility testing, 482 DFS replication, 976-977 documentation 688 for disaster recovery, 1044 IIS 7.0 implementation, 336-337 projects, 57-58, 62 for Terminal Services, 801 fault tolerance, 803 hosted applications, 803 licensing, 803-804 networking requirements, 803 physical placement of Terminal Servers, 802 Remote Desktop for Administration mode. 801 Terminal Server mode, 801-802 upgrades, 802 Windows Server 2008 implementation, 694 Windows Server 2008 migration, 33 playlist broadcasting broadcast publishing points, 1301 configuring, 1300-1302 on-demand publishing points, 1300 starting playlists, 1302 Please Read the License Terms page (Install Windows Wizard), 82

plug and play device redirection with Terminal Services, 792 PMO (Project Management Office), 1078-1079 PMTU (Path Maximum Transmission Units), Next Generation TCP/IP stacks, 1141 Point-to-Point Tunneling Protocol, See PPTP Pointer (PTR) records, 261 policies audit policies, 605-606 categories and subcategories, 606-609 GPOs. 878-880 group policies, 518, 536 automatic client configurations, 394-396 configuring, 521-523 creating, 519-521 OU designs, 175-176 troubleshooting, 523-525 viewing, 519 local policies, 536 managing Active Directory, 911-912 configuring restricted groups for domain security groups, 915 extending Group Policy functionality, 919-921 fine-grained password policies, 912-914 Read and Apply Group Policy, security properties, 176 policy baselines, establishing, 1191-1192 policy documentation, 703 policy management tools, 23, 554 ADMX Migrator, 559 DFS Management console, 561 Event Viewer, 560-561 GPLogview, 559 GPMC (Group Policy Management Console), 554-555 GPO scripts, 558 GPOE (Group Policy Object Editor), 555-556 gpupdate.exe, 557-558 Microsoft Desktop Optimization Pack for Software Assurance, 558 Print Management console, 556-557

policy processing, Windows group policies, 868-869 policy settings enforcing with NPS, 421 configuring DHCP server for, 428-429 health policy for compliant clients, creating, 422-423 health policy for noncompliant clients, creating, 422 network policy for compliant clients, creating, 423-425 network policy for noncompliant clients, creating, 424, 426-428 System Health Validator, creating, 421-422 GPOs, 542-543 political-based management groups in OpsMgr, 725 populating groups, 514 port rules, NLB clusters, 1031 port rules filtering mode, NLB clusters, 1032 portals, need for, 1239 ports (COM), configuring for guest operating system sessions, 1332 postmortem meetings after disaster recovery, 1083 power outages (disaster recovery scenario), 1045 power task conditions, 1186 PowerShell, 16, 616, 639 aliases in. 654-655 command-line interface (CLI) in, 646-647 commands formats for, 646 types of, 647-649 directory management in, 672-676 drives, 659 editing features of, 646 event log information, gathering, 670-672 explained, 641-643 features of, 643-644 file management in, 672-676 help features, 664-667 installing, 644-645 launching, 644-645

.NET and COM objects, creating, 682-683 .NET Framework integration, 649 Extended Type System (ETS), 650 reflection, 650 type accelerators, 651-652 pipeline in, 652-653 process management, 677-678 profiles, 659-660 providers, 658-659 Registry management, 676-677 scopes in, 655 global scope, 655-656 local scope, 656 private scope, 657-658 script scope, 656-657 security in, 661-663 service management in, 668-670 uses for, 643 variables in, 653-654 WMI in. 679-682 PPTP (Point-to-Point Tunneling Protocol), 431, 746-747 advantages of, 751 comparing with L2TP/IPSec and SSTP, 749-750 connections, authentication for, 744 firewall rules for, 752 pre-creating Active Directory computer accounts for WDS, 856-859 predefined tasks in Task Scheduler, 597 preference actions (GPOs), 880 preference common options (GPOs), 880 Preference Item-Level targeting, domain group policies, 895-897 preferences (GPOs), 878-880 preparing compatibility testing, 475-482 domain controllers with adprep, 451-453 prerequisites, 392 for ADMT 3.1, 463 for Big Bang migration, 443 domains, renaming, 161 for Identity Management for UNIX components, 244 for UNIX integration tools, 237-238

preventing SSTP connections, 778 primary zones, 263 Print Management console, 525-526, 556-557, 618-619 adding print servers, 528 adding printers, 526-528 configuring, 526-527 custom filters, creating, 529-531 form management, 529 installing, 526 updating printer drivers, 529 -Print parameter (Route command), 1176 print servers. 7 adding to Print Management console, 528 in failover clusters, 998 Print Services Tools, installing, 886 printer drivers, updating, 529 printer management, 525 printer redirection with Terminal Services, 790-791 printers adding as network shared resources. 526-528 auditing, 611-612 domain group policies, deploying, 892-896 Print Management console, 618-619 prioritization of applications, 485 in disaster recovery plan, 1046, 1082 private keys, 401 private scope in PowerShell, 657-658 procedural documentation, 702 procedure baselines, establishing, 1191-1192 process management in PowerShell, 677-678 processes monitoring, Task Manager, 1147 running on systems, 1195 Processes tab (Task Manager), 1147, 1194 processing order GPO links, 545-546 for group policies, 523 managing, 574

processors 32-bit, Windows Server 2008 support, 74 64-bit. Windows Server 2008 support, 74 configuring for guest operating system sessions, 1332 Hyper-V requirements, 1318 usage, analyzing, 1219 product keys Type Your Product Key for Activation page (Install Windows Wizard), 91 Windows Server 2008 installations, 80 Windows Server 2008 upgrades, 91 profiles, 515 PowerShell, 659-660 in Windows Firewall with Advanced Security, 599 project implementation documentation, 689 checklists, 698 communication plans, 693-694 design documents, 690-693 migration plans, 694-698 pilot test plans, 702 project plans, 690 support and project completion documents, 702 test plans, 699-701 training plans, 698-699 Project Management Office (PMO), 1078-1079 project plans, 62, 690 high-level migration, 57 project scope, Windows Server 2008 migration, 40 projects goals and objectives, design documents, 54 plans, 57-58 timelines and milestones, 60 properties event properties, 1151 of IIS 7.0 websites, configuring, 346-351 of "out-of-band" FTP sites, configuring, 356-361 Read and Apply Group Policy security, 176 property version numbers, replication, 187

Protected Extensible Authentication Protocol (PEAP), 744 protocols, 106-107, 166 prototype phase compatibility testing, 474, 494-495 Windows Server 2008 migration, 62-64.440 Provide Computer Information section (Initial Configuration Tasks Wizard), 86 providers (PowerShell), 658-659 Providers feature page (IIS 7.0 websites), 347 provisioning accounts (ILM 2007), 232-233 PSO (Password Settings Objects), 127 attributes of, 128, 130 creating, 130-131 PSObject, viewing blocked information, 651 PTR (Pointer) records, 261 Public Key (KEY) records, 261 Public Key Infrastructure. See PKI **Public Key Policies, Computer Configuration** Windows Settings node, 873 public keys, 401 published namespaces (DNS), 123-124, 141-142 publishing broadcast, 1295 on-demand, 1295 publishing points broadcast, playlists, 1301 delivery methods, 1291 names, 1291, 1295 on-demand, playlists, 1300 single video broadcasts, 1296 summary, 1292 pull partners, configuring, 320-321 pull record filtering, 319 pulling media content, 1305 live broadcasts, 1306-1307 push partners, configuring, 320-321 pushing media content, 1305 live broadcasts, 1306

Q

/q parameter DCDiag command, 1178 NetDiag command, 1177 -q parameter (Pathping command), 1174 qualifying disasters/failures, 1081 quarterly maintenance procedures, 635-636 queries (DNS), 268-269 query.exe, 834 quorum (clustering), 1000 quorum models, 1018 failover clusters, 1003-1004 quota management on NTFS volumes, 960-961 quota services on file systems, 936-937 quota templates, creating with FSRM (File Server Resource Manager), 966-967 auotas adjusting with FSRM (File Server Resource Manager), 965-966 configuring with FSRM (File Server Resource Manager), 964-965

NTFS volumes, 961

R

-r parameter (Netstat command), 1176
-R parameter

Ping command, 1172
tracert command, 1173

RADIUS authentication in NPS, 418-419
RADIUS clients, configuring, 762-763
RAID (Redundant Arrays of Inexpensive Disks), 996
RAID arrays, 945
RAID-1 volumes, 944
RAID-5 volumes, 944-945, 948
RAM

guest operating system sessions (Hyper-V), 1330
Hyper-V requirements, 1317

RARP (Reverse Address Resolution Protocol), 300 RDC (Remote Differential Compression) protocol, 939 RDP (Remote Desktop Protocol), 787 RDP port, changing, 830 RDP v6.x client, new features, 26-27 Read and Apply Group Policy, security properties, 176 Read-Only Domain Controllers. See RODC reading file information in PowerShell, 676 real-time live broadcasts starting, 1293 Windows Media Services configuration, 1291-1292 real-time reports, generating with FSRM (File Server Resource Manager), 970-971 reboots, Windows Server 2008 upgrades, 92 Receive Window Auto-Tuning (Next Generation TCP/IP stacks), 1140 recovering data, shadow copies, 989-990 recovery, 1077 recovery documentation, 707-710 recursive queries (DNS), 268-269 Recursive Queries/Sec (DNS performance counter), 1226 Recursive Query Failure/Sec (DNS performance counter), 1226 redirection with Terminal Services, 789 disk drives, 790 local time zones, 791 .NET devices, 792 plug and play devices, 792 printers, 790-791 reducing performance monitoring overhead. 1169-1170 redundancy in OpsMgr, 726-727 Redundant Arrays of Inexpensive Disks (RAID), 996 referral priority, setting, 986-987 referrals (DFS), 975 reflection in PowerShell, 650 /registerdns parameter (lpconfig command), 1174 Registry management in PowerShell, 676-677

Registry permissions, setting, 465 **Registry security settings, Computer** Configuration Windows Settings node, 872 registry.pol files (GPOs), 541 relative distinguished names (Active Directory), 113-114 Relative ID. 115 relay agents (DHCP), 302 /release parameter (lpconfig command), 1174 Reliability and Performance Monitor, 20, 1202 counters. 1162-1163 Data Collector Sets. 1204-1205 creating, 1166-1167 definition, 1165 diagnosis reports, 1204, 1206 overview, 1159-1160 Performance Monitor, 1161-1164 adding counters with, 1162-1163 configuring, 1164 Reliability Monitor, 593-595, 1164-1165, 1203, 1205 reports, 1167-1168 Resource Monitor, 1160-1161 Resource Overview window, 1203 troubleshooting DNS, 282 Reliability Monitor, 593-595, 1164-1165, 1203, 1205 **Remediation Server, 417** remote access, 737, 784 TS RemoteApp programs, deploying, 815-820 remote access servers, 35 remote administration. 26 with Remote Desktop Connection, 785 support with WDS, 841 remote applications, TS RemoteApp, 796 Remote Assistance, 789 enabling, 806-807 Remote Desktop, configuring, 897-898 Remote Desktop Connection, 785, 789, 793 custom display resolutions, 793 Desktop Experience feature, 794 Display Data Prioritization feature, 794 Font Smoothing feature, 794 monitor spanning, 793

Remote Desktop for Administration mode (Terminal Services) enabling, 805-806 planning for, 801 Remote Desktop mode (Terminal Services), 787-788 Remote Desktop Protocol (RDP), 787 remote desktops, Windows Server 2008 configuration, 88 Remote Differential Compression (RDC) protocol, 939 Remote Installation Service (RIS), 21, 842 remote management, 612 PowerShell, 616 Print Management console, 618-619 Remote Server Administration Tools, 612-615 ServerManagerCmd.exe, 616-618 terminal sessions, 835 Windows Remote Management (WinRM), 615-616 remote office support, 23 Remote Server Administration Tools, 612-615 remote server shares, manual backups to, 1060-1062, 1064 remote servers, viewing event logs on, 1156 remote shared folders, Windows Server Backup support for, 1052 remote shares creating IIS 7.0 websites, 344 creating virtual directories in IIS 7.0, 346 **Remote Storage Service**, 938 remote user support with Terminal Services, 786 Remote-Item cmdlet (PowerShell), 674 RemoteSigned execution policy (PowerShell), 662-663 removable storage access, managing users with policies, 909-910 Remove-ItemProperty cmdlet (PowerShell), 677 removing BitLocker Drive Encryption, 1140 cluster nodes, 1027 lingering objects from Active Directory, 136 Network Monitor filters, 1199

phantom domain controllers, 457-458 role services (IIS 7.0), 341 Windows 2000/2003 domain controllers, 457 Rename-Item cmdlet (PowerShell), 675 renaming domains, 143, 160 limitations, 161 prerequisites, 161 six steps, 161-163 files/directories in PowerShell, 675 /renew parameter (lpconfig command), 1174 repadmin utility, 189 replacing domain controllers, 450-451, 454-455 replication Active Directory, 121, 186 collisions, 187 connection objects, 188-189 latency, 189-190 monitoring, 1224 multimaster replication, 114, 186 Originating Writes, 123 property version numbers, 187 site link bridgeheads, 121-122 site links, 121-122 sites, 121-122 update sequence numbers, 186 compressing, 203 decentralized design example, 209-210 default schedule, 190 defined, 975 DFS, 940 best practices, 984 disabling, 986 planning, 976-977 DFSR (Distributed File System Replication), 939, 973-975 forcing, 189 of GPO files, 561 of GPOs. 539-541 hub-and-spoke design example, 207-208 incremental universal group memberships, 171

linked-value, 202 media-based GC/DC, 201 multimaster replication, 975 schedules selecting, 200 site links, 193 SMTP 201 topology compression, 203 domain controllers, promoting, 201-202 ISTG. 204 lingering objects, 203 linked-value replication, 202 multiple-site designs, 199 replication schedules, 200 schema changes, 204 single-site designs, 199 site design, 198 site links, 200 sites, establishing, 198 SMTP, 201 subnet associations, 200 universal group caching, 203 WAN design, 198 Windows Server 2003 improvements, 201 universal group memberships, 135-136 WINS, 322 replication compression disable support (Active Directory), 135 replication connections, 975 replication groups, 975 creating, 981-983 replication members, 975 replication partner acceptance, 319 replication topologies, 977-978 reporting file systems, 939 in Terminal Services, 786 reporting database (OpsMgr), 718-719 reporting database server (OpsMgr), 724 reporting documentation, 711-712

reports generating with FSRM (File Server Resource Manager), 970-971 in OpsMgr, 720-721 Reliability and Performance Monitor, 1167-1168 for security documentation, 713 requirements. See also prerequisites for AD RMS. 409 backups, requirements for (OpsMgr), 723 for Datasheet view (WSS), 1254 for external disk storage, 946 fault tolerance (IIS 7.0), 337 firewall requirements (OpsMgr), 728 hardware requirements IIS 7.0, 336 OpsMgr, 722 Windows Server 2008 installations, 74 installing WSS, 1240-1241 networking requirements, planning for Terminal Services, 803 OpsMgr agent deployment, 723 signature requirements, disabling, 89 software requirements IIS 7.0, 336 OpsMgr, 722-723 user requirements for Terminal Server mode, 801 Windows Media Encoder, 1303-1304 Windows Media Services, 1283-1284 for WSUS, 392 resolutions for Remote Desktop Connection, 793 resource access, auditing, 609-612 resource allocation policies (WSRM), 1209 custom resource allocation policies, 1210-1211 Equal per IIS Application Pool policy template, 1209 Equal per Process policy template, 1209 Equal per Session policy template, 1209 Equal per User policy template, 1209 scheduling policy enforcement, 1211 resource distribution of networks, viewing, 118

Resource Monitor, 1160-1161 Resource Overview window (Reliability and Performance Monitor), 1203 resource records (RRs), 257 assigning multiple, 263 Canonical Name (CNAME) records, 261 Host (A) records, 258 list of, 261 Mail Exchanger (MX) records, 260 Name Server (NS) records, 259 Pointer (PTR) records, 261 scavenging, 272-273 Service (SRV) records, 259-260 Start of Authority (SOA) records, 258 Time to Live (TTL) value, 270-271 resource segmentation, securing Terminal Services, 830-831 resources appreciation during disaster recovery, 1083 cluster, 999, 1002 simulating failure, 1024-1025 compatibility testing, 479 generic cluster resources, 1000 nested groups, sharing, 177 scheduling during disaster recovery, 1083 **Resources and Support section (Server** Manager roles pages), 590-591 responsibilities for disaster recovery, delegation of, 1080-1081 of team members, 60 Responsible Person (RP) records, 261 restarting Active Directory domain controllers, 126 Restore mode (Active Directory), password for, 1067-1068 restoring DHCP 307 domain GPOs, 575-577 failover clusters, 1028-1030 NLB nodes, 1039 starter GPOs, 567-570 Restricted execution policy (PowerShell), 661

restricted groups configuring for domain security groups, 915 controlling group membership, 916-917 modifying group membership, 917-919 security settings, Computer Configuration Windows Settings node, 872 restricting local site target server access, 986-987 logins, 377-378 physical access, 377 results, compatibility testing, 493-494 retail media activation keys (product keys), Windows Server 2008 installations, 81 Return to Operation (RTO) in disaster recovery plan, 1047-1048 Reverse Address Resolution Protocol (RARP), 300 reverse lookup zones, 263 reverting snapshot sessions (Hyper-V), 1336 RFC, Next Generation TCP/IP stacks, 1141 RID (Relative ID) master (OM role), 115 **Rights Management Services**, 31, 408 RIS (Remote Installation Service), 21 RIS images, upgrading to WDS images, 859 risks compared to speed, 58 in migration documents, 60 security risks, identifying, 619 roaming user profiles, 516 RODC (Read-Only Domain Controllers), 18, 211, 327-329, 1112 Active Directory support, 134 administrator role separation, 1115 benefits of. 1114-1115 for branch offices, 24 credential caching, 1115 deploying, 212, 214 ERODC, 1117 features of, 212 installing, 1117 full Windows Server 2008 installations. 1118.1120-1122 prerequisite tasks, 1117

staged installations, 1125-1129 Windows Server 2008 Server Core installations, 1122-1125 limitations of, 1117 read-only active directory domain services, 1114 read-only DNS, 1116 replication workload reduction, 1114 WAN utilization. 1140 role administration tools for Terminal Services, 834 role services in AD CS, 403-404 backing up, 1064 Active Directory, 1066-1068 Certificate Services, 1068-1069 DFS, 1071 DHCP, 1070-1071 DNS, 1069 IIS, 1071 System State, 1065 WINS, 1070 WSS. 1071-1073 IIS 7.0 adding/removing, 341 ASP.NET, dependencies, 341 FTP Publishing Service, 339-340 Management Tools, 339 Web Server, 338-342 list of, 584 Role Services section (Server Manager roles pages), 589 role-specific pages (Server Manager), 588, 590-592 roles, 1223 list of. 583-585 OM (operations master), 114-115 Remote Server Administration Tools for, 613 role-specific pages (Server Manager), 588, 590-592 servers defining, 385 enabling with Server Manager, 385-386 of team members, 60 user requirements in migration process, 66

Roles Summary window (Server Manager), 588-589 rollback (images), snapshots, 1334-1335 rolling blackouts (disaster recovery scenario), 1045 root domains, cross-forest trusts, 154 Root Hints list (DNS), 273 root management server (OpsMgr), 718, 727 root of DNS hierarchy, 254 Route command, 1176 RP (Responsible Person) records, 261 **RRAS** (Routing and Remote Access Service), 417, 737, 743 authentication in, 743 EAP and PEAP authentication, 744 for L2TP/IPSec connections, 745 for PPTP connections, 744 selecting protocols, 745 VPN features in, 738-739 RRAS network policy, modifying, 434-435 RRAS servers, 741 configuring, 763-766 enabling VPNs on, 432-435 RRs (resource records), 257 assigning multiple, 263 Canonical Name (CNAME) records, 261 Host (A) records, 258 list of, 261 Mail Exchanger (MX) records, 260 Name Server (NS) records, 259 Pointer (PTR) records, 261 scavenging, 272-273 Service (SRV) records, 259-260 Start of Authority (SOA) records, 258 TTL (Time to Live) value, 270-271 **RSS** (Remote Storage Service), 938 RTO (Return to Operation), in disaster recovery plan, 1047-1048 rule groups (firewalls), 384 rules (firewalls), creating, 382-385 Run As accounts (OpsMgr), 728 Run As command, administrative access, 378-379 run profiles, management agents, 229

S

-s parameter Arp command, 1175 Netstat command, 1176 -S parameter Ping command, 1172 tracert command, 1173 /s:DomainController parameter (DCDiag command), 1177 sample VPN scenario, 753-755 certificate server configuration, 754-755 NPS configuration, 758-763 NPS installation, 756-757 RRAS server configuration, 763-766 SSTP connection prevention, 778 SSTP troubleshooting, 775-777 unhealthy VPN clients, 772-774 VPN client configuration, 766-769 VPN connection testing, 769-772 SANs (storage area networks), 30 booting from, 945 SAS (Serial Attached SCSI) storage arrays, 1007 saving event logs, 1155 guest operating system session state (Hyper-V), 1334 starter GPOs as cabinet files, 568 scale-out applications, 11 scale-up applications, 11 scaling Terminal Services, 832 scavenging in DNS, 272-273 SCCM (System Center Configuration Manager), 1194 SCCP (System Center Capacity Planner), 1213 scheduled backup options, 1054 scheduled replication, 978 scheduled reports, generating with FSRM (File Server Resource Manager), 971 ScheduledDefrag task, enabling, 598 schedules, replication selecting, 200 default. 190

scheduling backups with Windows Server Backup, 1058-1060 resource allocation policies (WSRM), 1211 tasks, 596-598 technical resources during disaster recovery, 1083 schema Active Directory, 112 attributes, deactivating, 135 modifications, 204 preparing with adprep, 451-453 schema master (OM role), 114 scope of compatibility testing, 475-478 DHCP 304-306 DHCPv6 scope, setting up, 292-293 groups, 170, 511 domain local, 170-171 global, 171 machine local, 170 universal. 171 Multicast, 313 in PowerShell, 655 global scope, 655-656 local scope, 656 private scope, 657-658 script scope, 656-657 of projects, 40 standby failover approach, 312 SuperScope (DHCP), 313 for TS licensing, 804 of work, defining, 44-46 screen content, capturing, 1309-1310 screening, 937 script scope in PowerShell, 656-657 scripting, 641 with ActivePerl, 247 in SUA (Subsystem for UNIX-based Applications), 243 scripts dot sourcing, 657 GPOs. 558 PowerShell, 649 signing, 661

SCSI controllers, configuring for guest operating system sessions, 1332 SCW (Security Configuration Wizard), Windows group policies, 868 SDK and Configuration service account (OpsMgr), 728 search engines, need for, 1239 searches, WINS, 319 secondary zones, 263 in AD DS environment, 278-279 Secure File Transfer Protocol (SFTP), 941 Secure Socket Tunneling Protocol, 748 Secure Sockets Laver, 363 Secure Update Received/Sec (DNS performance counter), 1226 Secure Update Received/Sec/Sec (DNS performance counter), 1226 secure updates to dynamic DNS, 271-272 securing Terminal Services, 829 with GPOs. 831 Network Authentication, 830 RDP port, changing, 830 resource segmentation, 830-831 user access. 830 TS Web Access, 814 security access, restricting, 377 Active Directory, 107, 125-126 Kerberos, 125-126 multiple password implementation per domain, 127-128, 130-131 AD CS. 402 CA roles in, 403 installing, 404-407 role services in, 403-404 AD RMS, 408-409 installing, 409-411 requirements, 409 antivirus programs, 389-390 backup strategy, 390 BitLocker Drive Encryption, 1129 authentication, 1131 data volumes, 1130, 1138-1139

deployment scenarios, 1131 EFS versus, 1129 hardware requirements, 1131 installing, 1130, 1133-1134 passwords, 1139 removing, 1140 system partition configuration, 1132-1133 TPM, 1130, 1135-1136 UEFI, 1130 USB keys, 1137-1138 CLR (common language runtime), 376 **DHCP** 315 authorization, 315-316 domain controllers, 316-317 EFS, 407, 1129 encryption, 401 file-level. 386 access audits, 388-389 encryption, 389 NTFS, 386-387 share-level security, compared, 387 group policies, 518 configuring, 521-523 creating, 519-521 troubleshooting, 523-525 viewing, 519 Group Policy, defined, 533-534 for IIS 7.0, 361 administrator roles, 367-368 auditing services, 363 authentication, 362-363 feature delegation, configuring, 369 logging, 369-370 SSL certificates, 363-367 user accounts, assigning permissions, 368-369 user accounts, creating, 368 Windows Server 2008 security, 362 improvements in Windows Server 2008, 22-23 IPSec. 411-412 functionality in, 412 NAT-T, 412-413
lavers of, 376 local policies, 536 NAP 415 non-Microsoft Kerberos realms, 408 in OpsMgr, 727-728 permissions on shares, 955-956, 959 physical, 376 access, restricting, 377 administrative access, 378-379 branch offices, 1113 firewalls, 380 logins, restricting, 377-378 smartcards, 379 wireless networks, 380 PKI, 401-402 in PowerShell, 661-663 PSO (Password Settings Objects), 127 attributes of, 128, 130 creating, 130-131 Read and Apply Group Policy properties, 176 Server core installations, administrator passwords, 95 server roles defining, 385 enabling with Server Manager, 385-386 share-level, compared to NTFS, 387 smart cards. 407 transport-level, 23, 400 encryption, 401 levels of, 400 VPNs. 430-435 Trustworthy Computing initiative, 376 VPNs. 430 enabling on RRAS server, 432-435 L2TP/IPSec, 431-432 RRAS network policy, modifying, 434-435 tunneling protocol, 431 tunnels, 430 Windows Firewall with Advanced Security, 381 creating inbound/outbound rules, 382-385 Server Manager integration, 381

Windows Server 2008 administrator passwords, 84 firewalls, 88 WSUS, 390-391 Automatic Updates client, 391, 394-396 installing, 392-394 requirements, 392 updates, deploying, 396 Windows Update, 390-391 Security Configuration Wizard (SCW), Windows group policies, 868 security documentation, 712-713 security filtering (GPOs), 547-548 managing, 573-574 security groups, 168-169, 510 Security ID, 168 security logs, 1153, 1158-1159 security policies, 23 security procedure documentation, 706 security risks, identifying, 619 Security role service (IIS 7.0), 339 Security Settings node, 871-873 security templates, 538 security-based management groups in OpsMgr, 725 segmenting resources, securing Terminal Services, 830-831 Select the Operating System You Want to Install page (Install Windows Wizard), 91 selecting applications for failover clusters, 1004-1005 authentication protocols, 745 clustering technologies, 1001 failover clusters, 1002 NLB. 1002-1003 DFS types, 976 operating systems for failover clusters, 1009 VPN tunneling protocols, 749-750 firewall rules for, 752-753 L2TP/IPSec advantages, 750-751 PPTP advantages, 751 SSTP advantages, 751-752

self-healing NTFS, 4 separating GPO functions, 563-564 Serial Attached SCSI (SAS) storage arrays, 1007 Serial Port Console Redirection (SPCR), 1075 Server 2008. See Windows Server 2008 server build procedure documentation, 704 Server Certificates feature page (IIS 7.0 websites), 351 Server Core edition of Windows Server 2008, 12-13 AD domain controllers, deploying on, 197 installing, 93 changing administrator passwords, 95 changing computer names, 96 custom installations, 94 DNS assignments, 96-97 domains, 97 feature configurations, 98 launching command prompt, 95 role configurations, 97-99 static IP address assignments, 96-97 Windows Server Backup, 1056-1057 server failure scenario (disaster recovery), troubleshooting, 1085-1094 server farms in IIS 7.0, new features, 333 Server for Network Information Services (SNIS), 243 Server Manager, 14-15, 587-588 BitLocker Drive Encryption installation, 1133-1134 command-line tool for, 616-618 Configuration page, 596 Services snap-in, 600-601 Task Scheduler, 596-598 Windows Firewall with Advanced Security, 598-600 WMI Control, 601 configuring Hyper-V, 1322 Diagnostics page, 592 Device Manager, 595 Event Viewer, 592-593 Reliability and Performance Monitor, 593-595

Features page, 592 Features Summary window, 588-589 Hyper-V server role installation, 1320-1322 installing Windows Server Backup, 1054-1055 role-specific pages, 588, 590-592 Roles Summary window, 588-589 server roles, enabling, 385-386 Storage page, 601 Disk Management, 603-604 Windows Server Backup, 601-603 Windows Firewall with Advanced Security integration, 381 server message block (SMB) protocol, 940 Server Message Block 2.0 (SMB2), 5 server migration procedures, documenting, 696-697 -Server parameter (Nslookup command), 1176 server roles, 583 list of, 6-8 new features, 30-33 for performance optimization, 1223 server types for OpsMgr, 723-724 server virtualization, 6, 32-33 ServerManagerCmd.exe, 616-618 installing Windows Server Backup, 1055-1056 servers Active Directory servers, 743 in AD FS. 223-224 certificate servers, 743 configuring, 754-755 DC, 1223 AD (Active Directory) replication, monitoring, 1224 AD (Active Directory), monitoring, 1223-1225 DNS (domain name system), monitoring, 1224, 1226-1227 DFS, taking offline, 985-986 DHCP, 300, 312 domain. 7 file, 7

GCs (global catalog servers), Active Directory, 114 Internet Information Server and Site Server. 107 Microsoft Virtual Server Virtual Server 2005, 1314 Virtual Server 2005 R2, 1315 NPS configuring, 758-763 installing, 756-757 pilot phase (Windows Server 2008 migration), 65 print, 7 adding to Print Management console, 528 RRAS servers, 741 configuring, 763-766 security roles defining, 385 enabling with Server Manager, 385-386 storage, 996 Terminal Services Server, performance optimization, 1228 upgrading from Mixed mode to Native mode, 859 virtual cluster servers, 999 virtual servers, performance optimization, 1228 virtualization, 1313 WDS servers adding boot images, 848-850 adding installation images, 850 configuring, 845-848 Service (SRV) records, 259-260 site resolution, 278, 280 service accounts for OpsMgr security, 728 service availability, 997 service management in PowerShell, 668-670 service packs (SPs), 620 automatic updates, 622-625 manual updates, 621 Terminal Services administration, 835 Windows Server Update Services (WSUS), 623, 625

service updates/patches, compatibility, 488 service-level agreements (SLAs) in disaster recovery plan, 1047-1048 IIS 7.0 fault tolerance, 337 services Active Directory, 106 administering, 107 DNS (Domain Name System), 107 Exchange Server 5.5, 106 Internet Information Server and Site Server, 107 LDAP (Lightweight Directory Access Protocol), 107 security, 107 TCP/IP (Transmission Control Protocol/Internet Protocol), 107 applications, compared, 483-484 deploying on failover clusters, 1019-1021 DHCP client, 301 DHCP server, 300 monitoring, Task Manager, 1147 network, new features, 299 NLB clusters, 1030 running on Hyper-V, 1318-1319 X.500 directory, 111-112 Services and Applications group, 999 Services for Macintosh, 941 Services for NFS. 941 administration of, 239 configuring, 241 enabling AD DS lookup for, 239-240 installing, 238-239 Services snap-in, 600-601 Services tab (Task Manager), 1147, 1195 Session 0 isolation in Terminal Services, 795-796 Session Manager Subsystem (smss.exe), 5 Session State feature page (IIS 7.0 websites), 347 sessions media, capturing, 1308-1309 parallel sessions, 5 **Terminal Services** configuring, 800 remote management of, 835

Set Time Zone link (Initial Configuration Tasks Wizard), 85 Set-Alias cmdlet (PowerShell), 655 Set-Content cmdlet (PowerShell), 674 Set-ExecutionPolicy cmdlet (PowerShell), 663 Set-ItemProperty cmdlet (PowerShell), 676-677 Set-Location cmdlet (PowerShell), 676 Set-Service cmdlet (PowerShell), 670 /setclassid parameter (lpconfig command), 1174 settings in Task Scheduler, 596 Settings menu (WSS document libraries), 1256-1258 setup logs, 1153 Sfc.exe (System File Checker), 953 SFTP (Secure File Transfer Protocol), 941 SFU (Windows Services for UNIX), 235 SHA (System Health Agent), 417 shadow copies, 938 configuring, 988-989 data recovery, 989-990 enabling for shared volumes, 1073-1075 recovering data with, 1092 of shared folders, 938 shadow.exe, 834 Share and Storage Management console, 957-960 share permissions troubleshooting, 1088-1091 validating, 1088-1089 share-level security, compared to NTFS, 387 Shared Configuration stores, 31 shared folders, shadow copies of, 938 shared resources (NFS), creating, 241-242 shared storage, 1000 adding to failover clusters, 1017-1018 failover clusters, 1005-1009 shared volumes, enabling shadow copies for, 1073-1075 SharePoint, 31, 941, 1071, 1233 history of, 1234-1235 SharePoint 3.0 Central Administration tool. data recovery, 1105 SharePoint Portal Server 2001, 1234

SharePoint Portal Server 2003, 1235 SharePoint Server 2007, additional features of, 1237-1238 SharePoint Team Services, 1234 shares access-based enumeration, 956-957 creating, 957-960 data recovery, 989-990 defined, 387 folders, 940 File Services role, installing, 953-955 offline files, CSC (client-side caching), 956-957 permissions on, 955-956, 959 synchronization, 957 sharing security group permissions, 168 SHAs (System Health Agents), 742 shells, 639 applications versus, 640 explained, 639-640 history of, 640-641 shortcut trusts, 117, 140 /showclassid parameter (lpconfig command), 1174 shuffling videos, 1298 SHV (System Health Validator), 417, 742 creating, 421-422 SID (Security ID), 168 groups, 172 migration, configuring domains for, 465-466 security groups, 168 sign-on integration with SharePoint Server 2007, 1238 signature requirements, disabling, 89 signing drivers, 952 with File Signature Verification (Sigverif.exe), 952 scripts, 661 Sigverif.exe (File Signature Verification), 952 Simple mode (TS Web Access deployment), 819 simple volumes, 943 simulating cluster resource failure, 1024-1025

single domain controller upgrade for Big Bang migration, 445-448 single domain model, 144 real-world design example, 146-147 selecting, 145 user administration in, 512 single forest model real-world design example, 151 trees, 150 single host mode (port filtering), 1032 single point of failure identifying, 1044 removal of, 29 Single Sign-On (Terminal Services), 792-793 single video broadcasts, 1294 configuring, 1294-1296 publishing points, 1296 single-label names (DNS), 280-281 single-site designs, 199 site administration, 501-503 design best practices, 503 domain controllers, adding to sites, 505-506 site delegation, 509-510 site group policies, 503 site links, 502 creating, 506-507, 509 sites, creating, 503-506 subnets, 502 creating, 505 site binding (SSL), 366 site collection management (WSS), 1271 with Central Administration console. 1276-1278 with Edit Page interface, 1274-1276 with Site Settings page, 1272-1273 site delegation, 509-510 Site Directory in SharePoint Server 2007, 1237 site group policies, 503 site Group Policy links, 562-563 site link bridgeheads, Active Directory replication, 121-122

site links, 502 Active Directory replication, 121-122 creating, 506-507, 509 site management tools (WSS), 1237 site policies, Active Directory site GPOs, 883 site resolution in AD DS environment, 278, 280 Site Settings page (WSS site management), 1272-1273 sites Active Directory, 190 costs, 195 design, 198 domain controllers, promoting, 201-202 establishing, 198 ISTG, 204 KCC, 195 lingering objects, 203 link bridgeheads, 197 link bridging, 194 linked-value replication, 202 links, 192, 194, 200 multiple-site design, 199 replication, 121-122 replication compression, 203 replication schedules, 200 schema changes, 204 single-design, 199 SMTP replication, 201 subnet associations, 191, 200 topology examples, 207-210 universal group caching, 203 Windows Server 2003 improvements, 191, 201 structure. 147 WSS, 1237 size of database in OpsMgr, 725-726 /skip:TestName parameter DCDiag command, 1178 NetDiag command, 1177 SLA (service-level agreement) in disaster recovery plan, 1047-1048 IIS 7.0 fault tolerance, 337 slow link detection. 535, 549-550

small businesses (GPOs), 883-884 smartcards, 379, 407 SMB (server message block) protocol, 940 SMB (Server Message Blocks), branch office WAN utilization, 1142-1143 SMB2 (Server Message Block 2.0), 5 smss.exe (Session Manager Subsystem), 5 SMTP E-Mail feature page (IIS 7.0 websites), 347 SMTP replication, 201 SMTP service, installing, 1247-1248 snapshots (Hyper-V), 1319, 1334 creating, 1335 fault tolerance, 1335 image rollback, 1334-1335 reverting, 1336 SNIS (Server for Network Information Services), 243 Snover, Jeffrey, 642 SOA (Start of Authority) records, 258 soft faults (memory), 1216 software corruption (disaster recovery scenario), 1046 Software Error-Reporting Mechanism, 1181 software installation GPOs, creating, 922-924 software packages, deploying with domain GP0s, 921-924 software requirements Hyper-V disk storage, 1318 overview, 1317 processors, 1318 RAM. 1317 IIS 7.0. 336 installing WSS, 1240-1241 for OpsMgr, 722-723 software restriction policies creating, 890-892 security settings, Computer Configuration Windows Settings node, 873 solution overview document (disaster recovery plan), 1048-1049 solutions to problems, implementation approach (design documents), 54-55

Sort-Object cmdlet (PowerShell), 678 sorting events, 1156 source domains, installing exported password keys, 464-465 source files, downloading (Windows Media Services), 1288 Source property (events), 1151 source starter GPOs, 520 spanned volumes, 944 SPCR (Serial Port Console Redirection), 1075 special-purpose domains, 159-160 speed and risk, comparing, 58 SPs (service packs), 620 automatic updates, 622-625 manual updates, 621 Windows Server Update Services (WSUS), 623, 625 SQL Server databases (ILM 2007), 228 SRV (Service) records, 259-260 site resolution, 278, 280 SSL (Secure Sockets Layer), creating FTP sites, 354-356 SSL certificates in IIS 7.0, 363-367 SSL relay, 797-798 SSTP (Secure Socket Tunneling Protocol), 748-749 advantages of, 751-752 comparing with PPTP and L2TP/IPSec, 749-750 preventing connections, 778 troubleshooting, 775-777 staging folders, 977 stand-alone DFS namespaces, 973, 976 stand-alone root CA, 403 stand-alone subordinate CA, 403 standard and AD-integrated DNS zones, comparing, 125 Standard edition of Windows Server 2008, 10 upgrading to Enterprise Edition, 476 standards group naming, 178 Internet, Microsoft adoption, 108 support for, 16 standby scopes failover approach, 312

Start of Authority (SOA) records, 258 Start Page (IIS Manager Connections pane), 335 Start-Service cmdlet (PowerShell), 670 starter GPOs, 542, 877 backing up and restoring, 567-570 creating, 566-567 starting IIS 6.0 legacy tools, 353 IIS Manager console, 336 live broadcasts, 1305-1307 playlists, 1302 real-time live broadcasts, 1293 startup options, 1075 state, guest operating system sessions (Hyper-V), 1334 static IP addresses Server Core installations, 96-97 Windows Server 2008 installations, 78 status (GPOs) changing, 548-549 managing, 572 Stop Service option (Hyper-V), 1326 Stop-Process cmdlet (PowerShell), 678 Stop-Service cmdlet (PowerShell), 669 storage of GPOs, 539-541 servers, 996 shared storage, 1000 adding to failover clusters, 1017-1018 failover clusters, 1005-1009 storage area networks (SANs), 30 booting from, 945 storage capacity, 635 storage limits, 965 storage management external disk storage, 945-946 RSS (Remote Storage Service), 938 Storage page (Server Manager), 601 Disk Management, 603-604 Windows Server Backup, 601-603 storage reports, generating with FSRM (File Server Resource Manager), 970-971 stretched clusters, 30

striped volumes, 944 structured design documents budget estimates, 54-55 end state (technology configurations), 54-55 executive summaries, 54 network background information, 54-55 organizing information, 54-55 project goals and objectives, 54 solutions, implementation approach, 54-55 table of contents (sample), 54 structures Active Directory, 108, 166 authentication modes, 110 domain trees. 109-110 domains, 108-109 forests. 110 functional levels, 110 Kerberos, 110 NTLM (NT LAN Manager), 110 placeholder domains, 158 sites, 147 subdomains, 109 Windows Server 2003 domain functional level, 111 domains, choosing, 143-144 groups, designs, 165 OUs (organizational units), 146 designs, 165 nesting, 166 text hierarchy, 172 stub zones, 263-265 SUA (Subsystem for UNIX-based Applications), 242 installing, 242-243 scripting in, 243 UNIX tool support, 243 subcategories for audit policies, 606-607, 609 -SubCommand parameter (Nslookup command), 1176 subdomains in Active Directory, 149 multiple domain model domains, adding, 148 real-world design example, 149 shortcut trust, 117

subnets. 502 AD sites association, 191 creating, 505 site associations, 200 Subscriptions folder (Event Viewer), 1154 Subsystem for UNIX-based Applications. See SUA subsystems disk, evaluating, 1219-1220 network, monitoring, 1221-1222 Superscope (DHCP), 313 support, 833 branch offices, 1114 end users and remote administration (WDS). 841 support and project completion documents, 702 symmetrical encryption, 401 synchronizing directories, 223 disaster recovery with business owners, 1082 shares, 957 synchronous foreground refresh, managing Active Directory, 925-926 System Center Capacity Planner (SCCP), 1213 System Center Configuration Manager (SCCM), 842, 1194 System Center Operations Manager. See OpsMgr System Diagnostics reports (Reliability and Performance Monitor), 1206 system failures, 1081 troubleshooting, 1085-1094 System File Checker (Sfc.exe), 953 system file stability, 952-953 System Health Agent (SHA), 417, 742 System Health Validator (SHV), 417, 742 creating, 421-422 system logs, 1153 system memory, monitoring, 1215-1217 system partitions, configuring (BitLocker Drive Encryption), 1132-1133 system performance disk subsystems, evaluating, 1219-1220 monitoring, 1214-1215

NBT Redirector: Bytes Total/sec (network traffic counter), 1223 NBT Server: Bytes Total/sec (network traffic counter), 1223 network subsystems, monitoring, 1221-1222 processor usage, analyzing, 1219 system memory, monitoring, 1215-1217 thrashing, 1217 System Performance reports (Reliability and Performance Monitor), 1206 system requirements. See also prerequisites; requirements for external disk storage, 946 installing WSS. 1240-1241 Windows Media Encoder, 1303-1304 Windows Media Services, 1283-1284 Windows Server 2008 installations, 74 System Resource Manager, 1207 system services, Computer Configuration Windows Settings node, 872 System Services section (Server Manager roles pages), 589 System Stability Index, 1164 System Startup and Recovery, 1178-1179 System State, backing up, 1065 System State recovery, 1100 for domain controllers, 1101-1104 system volume recovery with Windows Server Backup, 1097-1099 system-level fault tolerance, 993-994 systems disk subsystems, evaluating, 1219-1220 fault-tolerant network hardware, 995-996 server storage, 996 service availability, 997 UPSs, 994-995 network subsystems, monitoring, 1221-1222 processes running, 1195 SYSVOL folder, restoring, 1103

Т

table of contents (sample), design documents, 54 tape devices, lack of backup support for, 1052 Task Category property (events), 1151 Task Manager, 1194 application monitoring, 1147 Applications tab, 1194 capacity analysis, 1194-1195 launching, 1145-1146 network monitoring, 1148-1149 Networking tab, 1195 performance monitoring, 1147-1148 Performance tab, 1195 process monitoring, 1147 Processes tab. 1194 service monitoring, 1147 Services tab. 1195 user activity monitoring, 1149 Users tab. 1195 window, 1194 window tabs. 1194-1195 Task Scheduler, 596-598 overview. 1182-1183 task actions. 1185 task conditions. 1185-1186 task history, 1187 task settings. 1186-1187 trigger options, 1183-1185 tasks. See also Task Scheduler actions, 1185 conditions, 1185-1186 creating, 1156 delegating, 174 delegation control, 179 desktop administration tasks, 863 history, 1187 settings, 1186-1187 Tasks list in WSS, 1265 TCP Query Received/Sec (DNS performance counter), 1226 TCP Response Sent/Sec (DNS performance counter), 1226

TCP/IP (Transmission Control Protocol/Internet Protocol), 107, 298 Arp command, 1175 CTCP, Next Generation TCP/IP stacks, 1141 DCDiag command, 1177-1178 Ipconfig command, 1174 NetDiag command, 1177 Netstat command, 1175-1176 Next Generation TCP/IP stacks, 1140-1141 Nslookup command, 1176 overview, 1171 Pathping command, 1173-1174 Ping command, 1171-1172 Route command, 1176 Tracert command, 1172-1173 Windows Server 2008 installations, 78 team members, roles and responsibilities, 60 Team Productivity Update for BackOffice 4.5, 1234 teams, 48-49 technical goals and objectives, identifying, 43-44 deployment team participants, defining, 48-49 design team participants, defining, 48-49 scope of work, defining, 44-46 timeframes (implementation or migration), determining, 46-48 technical reporting documentation, 712 technical resources during disaster recovery, 1083 Telnet Server, installing, 246-247 template profiles, 517 templates administrative templates (GPOs), 541, 550-553 central store, 541-542 custom templates, 553 for Windows 2000/XP/Server 2003, 551-552 for Windows Vista/Server 2008, 552-553 file screen templates, creating with FSRM (File Server Resource Manager), 968-970

quota templates, creating with FSRM (File Server Resource Manager), 966-967 security templates, 538 temporary user profiles, 517 Terminal Server Manager, 834 Terminal Server mode (Terminal Services), 788 planning for, 801-802 Terminal Server role service deploying, 807-810 installing, 807-809 terminal servers, 35 Terminal Services, 783-784 administration, 833 with command-line tools, 834 disaster recovery, 835 remote management of, 835 role administration tools, 834 service packs and updates, 835 with Terminal Server Manager, 834 with WMI. 834 for application service providers, 786 cascading connections in, 792 client-side services, 788-789 deployment, 804 configuration steps, 810-812 remote assistance, enabling, 806-807 Remote Desktop for Administration, enabling, 805-806 Terminal Server role service, deploying, 807-810 TS Gateway, deploying, 821-824 TS Licensing, deploying, 827-829 TS RemoteApp programs, deploying, 815-820 TS Session Broker, deploying, 824-826 TS Web Access, deploying, 812-815 Drain mode, 799-800 granular session configuration, 800 local resource redirection, 789 disk drives, 790 local time zones, 791 .NET devices, 792 plug and play devices, 792 printers, 790-791

new features, 26-28 NLB (Network Load Balancing) in, 799 operational overview, 787 optimizing performance, 832-833 planning for, 801 fault tolerance, 803 hosted applications, 803 licensing, 803-804 networking requirements, 803 physical placement of Terminal Servers, 802 Remote Desktop for Administration mode. 801 Terminal Server mode, 801-802 upgrades, 802 reasons for using, 784 Remote Desktop Connection, 785, 793 custom display resolutions, 793 Desktop Experience feature, 794 Display Data Prioritization feature, 794 Font Smoothing feature, 794 monitor spanning, 793 Remote Desktop mode, 787-788 remote user support via, 786 reporting in, 786 scaling, 832 securing, 829 with GPOs. 831 Network Authentication, 830 RDP port, changing, 830 resource segmentation, 830-831 user access, 830 Session 0 isolation, 795-796 Single Sign-On, 792-793 Terminal Server mode, 788 TS Gateway, 797-798 TS RemoteApp, 796 TS Session Broker, 798-799 TS Web Access, 796 user applications for, 785 WSRM (Windows System Resource Manager), 799 WSRM resource allocations, 1212

Terminal Services Configuration snap-in, 811 Terminal Services Gateway (TS Gateway), 28 Terminal Services Remote Programs (TS Remote Programs), 28 Terminal Services Server, performance optimization, 1228 Terminal Services Web Access (TSWA), 27 test plans 699-701 /test:TestName parameter DCDiag command, 1178 NetDiag command, 1177 testing compatibility, 473-475 application inventory, 483 application priority, 485 applications versus services, 483-484 applications, installing, 492 basic, 480 budget, 479 Certified for Windows Server 2008, 493 checklist. 477 complete, 480 documentation, 481 extent. 480 goals, 478-481 hardware allocation/configuration, 491 inventory application sheets, 484 lab-testing, 491 mid-level. 480 network systems inventory, 482-483 plan, documenting, 482 preparations, 475-482 prototype phase, 494-495 resources. 479 results, documenting, 493-494 scope, 475-478 testing lab, 481 timeframe, 478-479 training, 480 user involvement, 481 vendors, 485 Windows Server 2008 allocation/configuration, 491

failover clusters, 1022, 1024-1025 load testing, Windows Media Services, 1287-1288 TS Gateway, 823-824 UPS (uninterruptible power supply), 634 VPN connections, 769-772 VPN health remediation, 772-774 testing labs compatibility testing, 481 results, 63-64 text hierarchy, OU structures, 172 text-file format (.txt), 1157 thin clients, Terminal Services, 26-28 third-party management packs in OpsMgr, 721 third-party toolsets for capacity analysis, 1213 thrashing, 1217 time AD. 188 domain computers, 188 Windows Server 2008 installations. customizing in, 80 Time to Live (TTL) value, 270-271 time zone redirection with Terminal Services, 791 time zones, Windows Server 2008 configurations, 85 timeframes (compatibility testing), 478-479 timeframes (implementation or migration), determining, 46-48 timelines in migration document, 60 toolbar menus in WSS document libraries. 1253-1258 tools folders (Server Manager roles pages), 590-592 toolsets built-in for capacity analysis (Task Manager), 1194-1195 third-party for capacity analysis, 1213 topologies, replication compression, 203 domain controllers, promoting, 201-202 ISTG. 204 lingering objects, 203 linked-value replication, 202

multiple-site designs, 199 replication schedules, 200 schema changes, 204 single-site designs, 199 site design, 198 site links, 200 sites, establishing, 198 SMTP, 201 subnet associations, 200 universal group caching, 203 WAN design, 198 Windows Server 2003 improvements, 201 topology diagrams, 705 Total Query Received/Sec (DNS performance counter), 1226 Total Response Sent/Sec (DNS performance counter), 1226 TPM (Trusted Platform Modules), BitLocker Drive Encryption, 1130, 1135-1136 Tracert command, 284, 1172-1173 tracking sheets, vendor compatibility, 485-486 traffic of networks, monitoring, 1222 training benefits of documentation, 686 compatibility testing, 480 in WSS document libraries, importance of, 1261 Training and Support phase (migration process), 441 training plans, 61, 698-699 **Transaction Processing Performance Council** website, 1193 transitive trusts, 116, 140, 143 Transmission Control Protocol/Internet Protocol. See TCP/IP transport-level security, 23, 400 AD CS, 402 CA roles in, 403 installing, 404-407 role services in, 403-404 AD RMS, 408-409 installing, 409-411 requirements, 409 EFS, 407

encryption, 401 IPSec, 411-412 functionality in. 412 NAT-T. 412-413 levels of, 400 PKI, 401 certificates, 402 non-Microsoft Kerberos realms, 408 private keys, 401 public keys, 401 smart cards, 407 VPNs. 430 enabling on RRAS server, 432-435 L2TP/IPSec, 431-432 RRAS network policy, modifying, 434-435 tunneling protocol, 431 tunnels, 430 trees Active Directory domains, 109-110 Active Directory forests, 150-151 cross-forest transitive trusts, 143 DFS. 975 federated forests design model, 151-154 single forest model, 150-151 triangle diagrams (domains), 144 triggers options, 1183-1185 in Task Scheduler, 596 troubleshooting, 634, 1171. See also debugging access issues, 1087-1092 data corruption/loss, 1092-1094 with Diagnostics page (Server Manager), 592 Device Manager, 595 Event Viewer, 592-593 Reliability and Performance Monitor, 593-595 DFS. 984-987 DNS. 281 client-side cache problems, 282 with DNSCMD command-line utility. 284-285 with Event Viewer, 281-282

HOSTS file problems, 282 with IPCONFIG command-line utility, 283-284 with NSLOOKUP command-line utility, 282-283 with Reliability and Performance Monitor, 282 with TRACERT command-line utility, 284 documentation for, 706 file system services with FSRM (File Server Resource Manager), 971 GPOs. 548 group policies, 523-525 in IIS 7.0, new features, 332 network outage scenario (disaster recovery), 1084 physical site failure scenario (disaster recovery), 1084-1085 server or system failure scenario (disaster recovery), 1085-1094 SSTP 775-777 trusts cross-forest, 152 one-way, 153 root domains, 154 cross-forest transitive, 140, 143 domain (Active Directory), 140 explicit trusts, 116-117 external trusts, 117 replacing with OUs, 182 transitive trusts, 116 domain-to-domain, trust design sample, 181 shortcut, 140 shortcut between subdomains, 117 Trustworthy Computing initiative, 376 **TS. See Terminal Services** TS Easy Print, 791 TS Gateway, 28, 797-798 deploying, 821-824 TS Licensing, deploying, 827-829 TS Remote Programs, 28 TS RemoteApp, 796 deploying, 815-820

TS Session Broker, 798-799 deploying, 824-826 TS Web Access, 796 deploying, 812-815 for RemoteApps, 819 tsclient machine name, 790 tskill.exe, 834 tsshutdn.exe, 834 TSWA (Terminal Services Web Access), 27 TTL (Time to Live) value, 270-271 tunneling protocols (VPN), 431, 745-746 comparing, 749-750 firewall rules for, 752-753 IPSec, 748, 750-751 L2TP, 747-748, 750-751 PPTP, 746-747, 751 SSTP, 748-749, 751-752 tunnels (VPNs), 430 txt (text-file format), 1157 type accelerators (PowerShell), 651-652 for WMI, 681-682 Type Your Product Key for Activation page (Install Windows Wizard), 91 types (of objects) Extended Type System (ETS), 650 type accelerators, 651-652

U

/u:Domain\UserName /p:{* |Password|""} parameter (DCDiag command), 1178
UAC (User Account Control), 887
UDP Query Received/Sec (DNS performance counter), 1226
UDP Response Sent/Sec (DNS performance counter), 1226
UEFI (Unified Extensible Firmware Interfaces), BitLocker Drive Encryption, 1130
unattended Windows Server 2008 installations, 100
unhealthy VPN clients, controlling, 772-774

unicast delivery, compared to multicast delivery, 1292 Unicast mode (clusters), 1033 Unicode, support in DNS, 275 Uninterruptible Power Supplies (UPS), 994 testing, 634 universal group caching, 203, 326 universal group memberships, replicating, 135-136 universal groups, 120, 171, 511 UNIX integration tools, 235-236 administration of, 246 ActivePerl scripting, 247 installing Telnet Server, 246-247 Client for NFS, configuring, 241 components in, 237 history of, 236 Identity Management for UNIX adding NIS users to Active Directory, 245 components of, 243-244 configuring password synchronization, 245 installing, 244-245 improvements to, 237 NFS shared network resources, creating, 241-242 prerequisites for, 237-238 Services for NFS, 941 administration of, 239 configuring, 241 enabling AD DS lookup for, 239-240 installing, 238-239 SUA (Subsystem for UNIX-based Applications), 242 installing, 242-243 scripting in, 243 UNIX tool support, 243 UNIX shells, 640 unpopulated placeholder domains, 158 Unrestricted execution policy (PowerShell), 663 update sequence numbers, 186

updates, 390, 620 automatic updates, 87, 622-625 checking for, 1243-1244 for compatibility, 488 deploying with WSUS, 396 documentation, 635 existing domain controllers, 453-454 managing, WDS, 840 manual updates, 621 printer drivers, 529 secure updates to dynamic DNS, 271-272 Terminal Services administration, 835 Windows Server 2008, 87 Windows Server Update Services (WSUS), 623,625 upgrade decision matrix, 489-490 upgrades, 342, 441 compatibility testing, 473 domain and forest functional levels, 459-460 to domain controllers versus replacing, 450-451 failover clusters, 1027 to IIS 7.0, 342-343 to legacy systems, lack of ability for, 474 multiple upgrades, 475 RIS images to WDS images, 859 servers from Mixed mode to Native mode, 859 Standard Edition to Enterprise Edition, 476 Terminal Services, planning for, 802 versions, compatibility, 488 Windows Media Services platform to Windows Server 2008, 1286 Windows Server 2008, 88 automatic reboots, 92 digitally signed drivers, 89 Get Important Updates for Installation page (Install Windows Wizard), 90 license agreements, 91 new installations versus, 75-76 OS selection, 91

physical memory tests, 89 process overview, 90-92 product keys, 91 server backups, 88 system compatibility verification, 89 upgrade verification, 92 WINS environment, 323-325 Upgrading Windows page (Install Windows Wizard), 92 Upload menu (WSS document libraries), 1254 UPN (user principal name), 141 UPS (uninterruptible power supply), 634, 994-995 USB (Universal Serial Buses), BitLocker Drive Encryption, 1137-1138 user access, securing Terminal Services, 830 **User Account Control, 887** managing, 887-889 User Account Migration Wizard, 467-468 user accounts in IIS 7.0 assigning permissions, 368-369 creating, 368 migrating, 467-468 User Activity tab (Task Manager), 1149 user administration, 512 **User Configuration Administrative Templates** node, 874 User Configuration node, 865, 873 User Configuration Software Settings node, 874 User Configuration Windows Settings node, 874 user GPO processing, 535 user group policy configurations, 905 user management, group policies, 518 configuring, 521-523 creating, 519-521 troubleshooting, 523-525 viewing, 519 user migration procedures, documenting, 698 User Name Mapping service, 240 user principal name, 141 User Printer Preferences extension, deploying printers, 895-896

User Profile Hive Cleanup Service, 6 user profiles, 515 All Users profile, 517 default profiles, 516 copying to, 518 creating, 517 local profiles, 516 mandatory profiles, 516 roaming profiles, 516 in SharePoint Server 2007, 1237 template profiles, 517 temporary profiles, 517 user requirements for Terminal Server mode, 801 User subfolder (GPOs), 540 users compatibility testing involvement, 481 end-user satisfaction, verifying, 67 granting access to Terminal Servers, 809 managing with policies, 905-906 configuring folder redirection, 906-909 Microsoft Management Console (MMC), 910-911 removable storage access, 909-910 monitoring, Task Manager, 1149 pilot phase of migration testing, 66 remote support with Terminal Services, 786 Terminal Services usage by, 785 Users folders, objects, 166 Users tab (Task Manager window), 1195 USNs (update sequence numbers), 186

V

/v parameter
 DCDiag command, 1178
 NetDiag command, 1177
 -v parameter (Ping command), 1172
 Validate a Configuration Wizard, running, 1011-1013

validating backups, 634 disaster recovery priorities, 1082 NTFS permissions, 1091 share permissions, 1088-1089 validation process (NPS), 421 configuring DHCP server for, 428-429 health policy for compliant clients, creating, 422-423 health policy for noncompliant clients, creating, 422 network policy for compliant clients, creating, 423-425 network policy for noncompliant clients, creating, 424, 426-428 System Health Validator, creating, 421-422 variables in PowerShell, 653-654 vendors, compatibility information, 485 incompatible applications, 488-489 service updates/patches, 488 states of compatibility, 486-489 testing plan, assessing, 490 tracking sheets, 485-486 upgrade decision matrix, 489-490 version upgrades, 488 Windows Server 2008-compatibility applications, 487 verifying, 629 application readiness for Big Bang migration, 444 backups, 626 central store usage (GPOs), 565-566 end-user satisfaction, 67 hardware compatibility for Big Bang migration, 444 VeriTest website, 1193 versions upgrading for compatibility, 488 of Windows Media Services, comparing, 1284-1285 Windows Server 2008 Datacenter edition, 11 Enterprise edition, 10-11

Server Core edition, 12-13 Standard edition, 10 Web Server edition, 11-12 VHD (Virtual Hard Disk) files, 1053 video looping, 1298 screen content, capturing, 1309-1310 shuffling, 1298 single video broadcasts, 1296 video directories configuring, 1297, 1299 files, viewing, 1299 video files converting, 1310 extensions, 1308 video-editing tools, 1303 View menu (WSS document libraries), 1258 viewing backup history, 1064 blocked PSObject information, 651 files, video directories, 1299 GPO settings, 575 group policies, 519 network resource distribution, 118 OpsMgr settings, 720 **Reliability and Performance Monitor** reports, 1168 views, creating custom views, 1152-1153 virtual cluster servers, 999 virtual directories in IIS 7.0, creating, 345 virtual domain controller rollback for Big Bang migration, 445 Virtual Hard Disk (VHD) files, 1053 Virtual Machine Manager (VMM), 1316 Virtual Memory System (VMS), 640 configuration options, 1217-1218 virtual network switch management (Hyper-V), 1324 Virtual PC, acquisition of, 1314 virtual private network. See VPN Virtual Server 2005, 1314 Virtual Server 2005 R2, 1315

virtual servers, performance optimization, 1228 virtualization. 32-33 definition, 1313-1314 history of, 1314 acquisition of Virtual PC, 1314 integration of Hyper-V, 1315-1316 Virtual Server 2005, 1314 Virtual Server 2005 R2, 1315 Hyper-V, 6 Administrative Console, 1322-1323 connecting to different virtual server system, 1323 Edit Disk option, 1325 guest operating system sessions, 1326-1334 Inspect Disk option, 1325 installation, 1319-1322 integration into Windows Server 2008. 1315-1316 managing with MMC, 1322-1323 managing with Server Manager, 1322 New Configuration Wizard, 1326 new features, 1316 planning implementation, 1318 running other services on, 1318-1319 server requirements, 1317-1318 as server role, 1317 snapshots, 1319, 1334-1336 Stop Service option, 1326 virtual network switch management, 1324 virtualization settings, 1324 overview, 1313 server requirements, 1318 servers, 35 VMM (Virtual Machine Manager), 1316 virtualization settings (Hyper-V), 1324 viruses, antivirus programs, 389-390 VMM (Virtual Machine Manager), 1316 VMS (Virtual Memory System), 640 volume media activation keys (product keys), Windows Server 2008 installations, 81

volume recovery with Windows Server Backup, 1096 data volume recovery, 1096-1097 system volume recovery, 1097-1099 volume shadow copies, 938 Volume Shadow Copy Service. See VSS volumes, 943 BitLocker Drive Encryption, 1130, 1138-1139 fault-tolerant volumes, 944 creating, 948-952 file formats for. 936 mirrored volumes, 944 mount points, 943 NTFS, guota management, 960-961 RAID-5 volumes, 944-945 simple volumes, 943 spanned volumes, 944 striped volumes, 944 VSS. 987 Backup utility, 988 data recovery, 989-990 shadow copies, configuring, 988-989 voluntary VPN tunnels, 430 VPN (virtual private network), 418, 430, 737, 743 Active Directory servers, 743 certificate servers, 743 clients, 741 configuring, 766-769 unhealthy clients, controlling, 772-774 CMAK (Connection Manager Administration Kit), 779-780 components needed for, 740-741 Connection Manager, 778-779 connections, testing, 769-772 explained, 739-740 features in RRAS, 738-739 L2TP/IPSec, 431-432 NPS (Network Policy Server), 741-743 RRAS network policy, modifying, 434-435 RRAS servers, 432-435, 741

sample scenario, 753-755 certificate server configuration, 754-755 NPS configuration, 758-763 NPS installation, 756-757 RRAS server configuration, 763-766 SSTP connection prevention, 778 SSTP troubleshooting, 775-777 unhealthy VPN clients, 772-774 VPN client configuration, 766-769 VPN connection testing, 769-772 tunneling protocols, 431, 745-746 comparing, 749-750 firewall rules for, 752-753 IPSec, 748, 750-751 L2TP, 747-748, 750-751 PPTP, 746-747, 751 SSTP, 748-749, 751-752 tunnels, 430 VSS (Volume Shadow Copy Service), 937-938, 987, 1073-1075 Backup utility, 988 data recovery, 989-990 shadow copies, configuring, 988-989 shared storage, 1008

W

w parameter
Pathping command, 1174
Ping command, 1172
WAIK (Windows Automated Installation Kit), creating bootable media with discover boot images, 854-856
WAN (Wide Area Networks), branch offices
DFS, 1141
group policies, 1142
Next Generation TCP/IP stacks, 1140-1141
RODC, 1140
SMB, 1142-1143
WAN infrastructure documentation 707

wbadmin.exe, 1054, 1063-1064 WDS (Windows 2008 Deployment Services), 21-22.843-844 boot images, 844 capture images, 844 cloning or imaging systems, 842-843 creating custom installations with capture images, 859-861 customizing install images using unattended answer files, 861-862 multicast images, 862-863 desktop administration tasks, 863 discover images, 844 creating, 853-854 creating bootable media, 854-856 image types, 844 installation images, 844 installing, 845 adding boot images to WDS servers, 848-850 adding installation images to WDS servers, 850 configuring DHCP 848 configuring WDS servers, 845-848 deploying first install images, 850-853 managing, updates and applications, 840 operating system deployment, 840-841 precreating Active Directory computer accounts, 856-859 supporting end users and remote administration, 841 upgrading servers from Mixed mode to Native mode, 859 web access, TS Web Access, 796 deploving, 812-815 Web console (OpsMgr), 718, 720 web pages (WSS), 1236 web parts, customizing WSS, 1240 Web Server edition of Windows Server 2008, 11-12 Web Server role service (IIS 7.0), 338-339 installing, 340-342 web servers, 35

Web Sites folder (IIS Manager Connections pane), 335 websites AppManager Suite, 1214 Computer Measurement Group, 1193 in IIS 7.0, 343 configuring properties of, 346-351 creating, 343-344 virtual directories, creating, 345 NetIO Corporation, 1214 Transaction Processing Performance Council, 1193 VeriTest Labs, 1193 Windows Media Load Simulator, 1287 wecutil gc command, 1154 weekly maintenance procedures, 629-634 Well Known Service (WKS) records, 261 Where-Object cmdlet (PowerShell), 654, 668-669, 678 Which Type of Installation Do You Want page (Install Windows Wizard), 82, 91 wiki page libraries in WSS, 1253 Windows, as shell, 641 Windows 2000/2003 administrative templates for, 551-552 DNS in, 274-275 migration to Windows Server 2008, 439 Big Bang migration, 443-448 Big Bang versus phased migration, 442 in-place upgrade versus new hardware migration, 441-442 migration scenarios, 442-443 multiple domain consolidation migration, 460-471 objectives, identifying, 440 phased migration, 440-441, 447-461 Windows 2000/2003 domain controllers, removing, 457 Windows 2000/2003 environment adding Windows Server 2008 to, 8-9 migrating to Windows Server 2008 Active Directory, 9 Windows 2008, adding disks to, 946-948

Windows 2008 Group Policy Management, 878 Windows Automated Installation Kit, 854-856 Windows Deployment Services, 21, 839-840 Windows Error Reporting, 87, 1182 Windows firewall, Windows Server 2008 configuration, 88 Windows Firewall with Advanced Security, 381, 598-600 creating inbound/outbound rules, 382-385 security settings, Computer Configuration Windows Settings node, 872 Server Manager integration, 381 Windows folder sharing, 940 Windows group policies, 866 local administrators user policies, 867 local computer policies, 867 local domain group policies, 868 local non-administrators user policies, 867 local security policies, 867 policy processing overview, 868-869 Security Configuration Wizard (SCW), 868 Windows Internet Naming Service. See WINS Windows Logs folder (Event Viewer), 1153 Windows Management Instrumentation, 834 Windows Media Encoder, 1302-1303 captured broadcasts preparing, 1307 sessions, capturing, 1308-1309 installing, 1304 live broadcasts, 1305 initiating, 1305-1307 pulling content, 1306-1307 pushing content, 1306 requirements, 1303-1304 screen content, capturing, 1309-1310 video file conversions, 1310 Windows Media Load Simulator, 1287 Windows Media Services, 1281-1282 administration tools, 1286 captured broadcasts preparing, 1307 sessions, capturing, 1308-1309

configuring, 1290-1291 downloading source files, 1288 installing, 1289-1290 live broadcasts, 1305 initiating, 1305-1307 pulling content, 1306-1307 pushing content, 1306 load testing, 1287-1288 Media Encoder, 1307 new features, 1282-1283 performance, 1284 playlist broadcasting broadcast publishing points, 1301 configuring, 1300-1302 on-demand publishing points, 1300 starting, 1302 real-time live broadcasts configuring, 1291-1292 starting, 1293 single video broadcasts, 1294 configuration, 1294-1296 publishing points, 1296 system requirements, 1283-1284 upgrading platform to Windows Server 2008, 1286 version comparison, 1284-1285 video directories configuring, 1297, 1299 files, viewing, 1299 Windows Media Encoder, 1302 Windows Memory Diagnostics tool, 89, 1179-1180 Windows PowerShell, 644 Windows Remote Management (WinRM). 615-616 Windows Rights Management Services, 31 Windows Script Host (WSH), 641 Windows Server 2003 Active Directory new features, 448-449 administrative templates for, 551-552 Windows Server 2003 domain functional level, 111

Windows Server 2008 Active Directory new features, 449 administrative templates for, 552-553 allocating, compatibility testing, 491 as application server, 6-8 applications included in, 7 configuring Add Features link (Initial Configuration Tasks Wizard), 88 Add Roles link (Initial Configuration Tasks Wizard), 87 administrator passwords, 84 compatibility testing, 491 computer names, 86 domains, 86 feedback, 87 firewalls, 88 with Initial Configuration Tasks Wizard, 582-583 initial configurations, 83-84 networking, 86 remote desktops, 88 time zones, 85 updates, 87 Datacenter edition, 11 desktop of, 3-4 DNS in, 275 application partitions, 275 automatic creation of DNS zones, 276 "island" problem, 276 msdcs zone, 276-277 Enterprise edition, 10-11 features in installing, 587 list of, 585-587 implementation documentation, 689 checklists, 698 communication plans, 693-694 design documents, 690-693 migration plans, 694-698 pilot test plans, 702

project plans, 690 support and project completion documents, 702 test plans, 699-701 training plans, 698-699 installing 32-bit processor support, 74 64-bit processor support, 74 computer name selection, 77 currency customization, 80 domain name determination, 78 edition selection, 75 file backups prior to installation, 79 hardware requirements, 74 Install Now page (Install Windows Wizard), 80 installation type selection, 82 IP address assignments, 78 keyboard preferences customization, 80 language customization, 80 licensing agreements, 82 location selection, 82-83 memory requirements, 74 network protocol configuration, 78 new installations versus upgrades, 75 OS selection. 81 Please Read the License Terms page (Install Windows Wizard), 82 product keys, 80 server type selection, 77 task determination, 77 TCP/IP installations, 78 time customization, 80 unattended installations, 100 Which Type of Installation Do You Want page (Install Windows Wizard), 82 workgroup name determination, 78 migrating to, 39 Active Directory, 33-34 add-in application server functions, 36 adding to Windows 2000/2003 environment, 8-9 Big Bang migration, 443-448

Big Bang versus phased migration, 442 budget estimates, 54-55, 62 built-in application server functions. 34-36 business goals and objectives, identifying, 40-43 collaborative design decisions, 53-54 design agreements, 56 design decisions, 55-56 design phase, 52-53 discovery phase, 49-51 end state (technology configurations), 54-55 end-user satisfaction, verifying, 67 environment, supporting, 68 executive summaries, 54, 60 Gantt charts. 58 geographical depth and breadth, 51-52 in-place upgrade versus new hardware migration, 441-442 information overload management, 52 lab testing process results, 63-64 labs, building, 63 migration background, 60 migration documents, creating, 59 migration phase risks and assumptions, 60 migration planning phase, 57 migration process goals and objectives, 60 migration processes, 61-62 migration scenarios, 442-443 migration/implementation phase, 67 multiple domain consolidation migration, 460-471 network background information, 54-55 objectives, identifying, 440 pilot phase, 64-66 pilot results, documenting, 67 pilot users, application usage requirements, 66 pilot users, geographical diversity, 66 pilot users, quantity of, 66

pilot users, role requirements, 66 phased migration, 440-441, 447, 449-461 planning, 33 problem solving, 67 project goals and objectives, 54 project plans, 57-58, 62 project scope, 40 project timeline and milestones, 60 prototype phase, 62-63 solutions, implementation approach, 54-55 speed and risk, comparing, 58 structured design documents, organizing information, 54-55 table of contents (sample), 54 team members' roles and responsibilities, 60 technical goals and objectives, identifying, 43-49 training plans, 61 when to migrate, 8 from Windows 2000/2003 Active Directory, 9 new features in Active Directory, 13-18 BitLocker, 24-25 branch office support, 23-26 in clustering, 29-30 **DFSR**, 25 for distributed administration, 26 FSRM, 21-22 in Group Policy Management, 19-20 GUI, 13 hot-swappable components, 5 Hyper-V, 6 IIS 7.0, 30-31 Initial Configuration Tasks Wizard, 14-15 parallel session creation, 5 PowerShell, 16 Reliability and Performance Monitor, 20 RMS, 31-32 security improvements, 22-23

self-healing NTFS, 4 Server Manager, 14-15 in server roles, 30-33 SMB2.5 standards, support for, 16 in Terminal Services, 26-28 User Profile Hive Cleanup Service, 6 WDS, 21-22 WSS, 31 WSV, 32-33 roles in, list of, 583-585 security in, 362 Server Core edition, 12-13 signature requirements, disabling, 89 Standard edition, 10 startup options, 1075 updates, downloading/installing, 87 upgrades, 88 automatic reboots, 92 digitally signed drivers, 89 Get Important Updates for Installation page (Install Windows Wizard), 90 license agreements, 91 new installations versus, 75-76 OS selection, 91 physical memory tests, 89 process overview, 90-92 product keys, 91 server backups, 88 system compatibility verification, 89 verification of, 92 Windows Media Services platform to, 1286 Web Server edition, 11-12 Windows Server 2008 UNIX Integration tools, 235 Windows Server 2008 Windows Deployment Services, 843 Windows Server 2008-compatible applications, 487

Windows Server Backup, 601-603, 1051 backup files/folders, 1053 command-line utility, 1054 DHCP service recovery with, 1104 DVD backups, creating, 1062-1063 installing, 1054-1057 management with wbadmin.exe, 1063 manual backups to remote server shares, 1064 viewing backup history, 1064 manual backups to remote server shares, 1060-1062 media management in. 1051-1052. 1095 MMC snap-in for, 1054 options, setting, 1053-1054 recovering data with, 1093-1094 role services, backing up, 1064 Active Directory, 1066-1068 Certificate Services, 1068-1069 DFS. 1071 DHCP 1070-1071 DNS. 1069 IIS. 1071 System State, 1065 WINS, 1070 WSS. 1071-1073 scheduling backups, 1058-1060 System State recovery with, 1100 for domain controllers, 1101-1104 volume recovery with, 1096 complete PC restore, 1099 data volume recovery, 1096-1097 system volume recovery, 1097-1099 WSS recovery with, 1104-1107 Windows Server Update Services (WSUS), 390, 623, 625 Windows Server virtualization (WSV), 32-33 Windows Services for UNIX (SFU), 235 Windows SharePoint Services. See WSS Windows System Resource Manager (WSRM), 799, 833, 1207 calendar events, 1211 installing, 1208

matching criteria rules, 1210 resource allocation policies, 1209 custom policies, 1210-1211 scheduling policy enforcement, 1211 Terminal Services resource allocations, 1212 Windows Time Service, 188 Windows Update, 390-391, 901 configuring, 622-625, 901-902 Windows virtualization, 1313 Windows Vista, administrative templates for, 552-553 Windows XP. administrative templates for. 551-552 WinRM (Windows Remote Management), 615-616 winrm guickconfig command, 1154 WINS (Windows Internet Naming Service), 253, 297, 317, 1070 backing up, 1070 database maintenance, 325 DNS integration, 274, 317-318 environment designing, 323 upgrading, 323-325 installing, 319-320 LMHOSTS file, 323 NetBIOS resolution, 317 new features, 318 pull record filtering, 319 push/pull partners, 320-321 replication, 322 replication partner acceptance, 319 searches, 319 wired network (IEEE 802.3) policies, 872 wireless network (IEEE 802.11) policies, 873 wireless networks, physical security, 380 wireless policies (domain group policies), creating, 902-905 witness file share, clustering, 1000 witness-based quorum validation, 29 WKS (Well Known Service) records, 261

wмi in PowerShell, 679-682 Terminal Services administration, 834 WMI Control. 601 WMI filtering (GPOs), 548 creating, 572-573 linking, 573 wireless policies, 902 [WMI] type accelerator, 681 [WMIClass] type accelerator, 681 [WMISearcher] type accelerator, 682 Word 2007, integration with WSS, 1266-1267 work, defining scope of, 44-46 Worker Processes feature page (IIS 7.0 websites), 351 workflows in SharePoint Server 2007, 1238 workgroups, name determination, 78 working sets, 1216 workload characterizations (capacity analysis), 1192 workspaces (WSS), 334, 1237 wrapper playlists, creating, 1293 WSH (Windows Script Host), 641 WSRM (Windows System Resource Manager). 799, 833, 1207 calendar events, 1211 installing, 1208 matching criteria rules, 1210 resource allocation policies, 1209 custom policies, 1210-1211 scheduling policy enforcement, 1211 Terminal Services resource allocations, 1212 WSS (Windows SharePoint Services), 31, 941, 1071, 1233-1235 backing up, 1071-1073 Central Administration console tools, 1237 customizing, 1240 document libraries, 1236, 1251-1261 accessing, 1253 advantages of, 1252 Edit menu options, 1259-1260 toolbar menus in, 1253-1258 training, importance of, 1261

features of, 1236-1237 installing, 1240 checking for updates, 1243-1244 default site collection components. 1248-1251 finishing with Central Administration console. 1245-1247 IIS configuration, 1244-1245 Incoming E-Mail Settings configuration, 1247-1248 SMTP service installation, 1247-1248 system requirements, 1240-1241 lists, 1236, 1251, 1261-1262 Calendar list, 1262-1264 custom lists, 1265 exporting to, 1268-1271 Tasks list, 1265 management tools, 1237 need for, 1238-1239 Office integration, 1266 Access 2007, 1270-1271 Excel 2007, 1267-1269 Word 2007, 1266-1267 recovery, 1104-1107 SharePoint Server 2007 additional features, 1237-1238 site collection management, 1271 with Central Administration console, 1276-1278 with Edit Page interface, 1274-1276 with Site Settings page, 1272-1273 site management tools, 1237 sites. 1237 web pages, 1236 workspaces, 1237 WSUS (Windows Server Update Services), 390-391, 623, 625 Automatic Updates client, 391, 394-396 installing, 392-394 requirements, 392 updates, deploying, 396 Windows Update, 390-391 WSV (Windows Server virtualization), 32-33 WWW directory publishing, 940

X–Z

X.500 directory services, 111-112 xcopy command, 5 XML documents, forest descriptions, 162 XML format, 1157 zone transfer counters of DC (domain controller), 1227 zone transfers (DNS), 265-268 zones AXFR (full zone transfers), 1227 DNS (domain name system), 125, 261-262 AD-integrated zones, 274 automatic creation of, 276 forward lookup zones, 262 GlobalNames zone (GNZ), 280-281 primary zones, 263 reverse lookup zones, 263 secondary zones, 263, 278-279 standard and AD-integrated, comparing, 125 stub zones, 263-265 IXFR (incremental zone transfers), 1227