

THE ADDISON-WESLEY MICROSOFT TECHNOLOGY SERIES

The background of the cover features a photograph of several evergreen trees heavily laden with snow. The sky is a deep blue. Overlaid on the image is a semi-transparent grid of squares in various shades of blue and white.

THE COMPLETE GUIDE TO **WINDOWS SERVER 2008**

JOHN SAVILL

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

The author and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:

U.S. Corporate and Government Sales
(800) 382-3419
corpsales@pearsontechgroup.com

For sales outside the United States please contact:

International Sales
international@pearsoned.com

Visit us on the Web: www.informit.com/aw

Library of Congress Cataloging-in-Publication Data:

Savill, John, 1975-

The complete guide to Windows server 2008 / John Savill.
p. cm.

ISBN 0-321-50272-8 (pbk. : alk. paper) 1. Microsoft Windows server. 2. Operating systems (Computers)
I. Title.

QA76.76.O63S35654 2008
005.4'476—dc22

2008025996

Copyright © 2009 Pearson Education, Inc.

All rights reserved. Printed in the United States of America. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, write to:

Pearson Education, Inc
Rights and Contracts Department
501 Boylston Street, Suite 900
Boston, MA 02116
Fax (617) 671 3447

ISBN-13: 978-0-321-50272-8

ISBN-10: 0-321-50272-8

Text printed in the United States on recycled paper at Edwards Brothers in Ann Arbor, Michigan.

First printing September 2008

PREFACE

Everyone knows the saying, “Be careful what you wish for.” It had long been my goal to write a complete guide to Windows Server, but I never felt I had sufficient time to do justice to the subject. In the middle of 2006, I convinced myself that I could organize my time to allow the undertaking of writing a book on the largest Microsoft server release ever—from scratch. I started writing the book a few months later and finished the final copy editing in June 2008, basically two years from start to finish. Fortunately, Microsoft delayed the release of Windows Server 2008 enough that this book will hit bookshelves while Windows Server 2008 is still new to the market.

With this book, I tried to create a resource that explains the major features of Windows Server 2008, when to use them, how to design the best implementation, and how to manage the deployed environment.

Windows Server 2008 has so many features that I had to leave some out. Those features not discussed are ones I felt would not be interesting to most readers; however, I point out what is not covered and suggest some resources. Windows 2008 is trying to put books out of business; however, although the online help is great, it is task focused. Therefore, I encourage you to follow the online help tool. I concentrate on items that require more design, decision, or are just cool.

Windows Server 2008 is very customer-focused and focuses on a key number of areas such as virtualization, the Web, and security. Usability is also a major area for Windows 2008. A customer does not point to a server and say “that’s my windows server”; a customer says “that’s my domain controller” or “that’s my file server.” Windows Server 2008 is designed around how the server is used. Only the basic functions are installed; additional components are installed as roles, and features are added to the server and their management tools accessed through a single server manager interface.

Design of Microsoft-based systems will change in the future. I predict that the process we perform today to design the best practice implementation for our environment will be automated entirely within ten years—

and I'll need a new day job. Think of the process today: We look at the environment and how to use it and then create a design following experience and best practices. We have a number of tools today to help with this: Best Practice Analyzers that check that an installation follows guidelines; System Center Capacity Planner that allows a designer to input information about locations, users, servers, and bandwidth and then creates a server design that services needs; and Microsoft Solution Accelerators that help create solutions with Microsoft technologies. The next step is bringing these together. System Center Configuration Manager and System Center Operations Manager can ascertain the information needed about an environment. This information can then be automatically fed into Capacity Planner-type solutions to produce a best practice design and periodically verify that the design still meets requirements. With the move to virtualization, the design tools will partner with deployment technologies to automatically build new virtual machines for services, as needed, without administrator intervention. Microsoft already has a direction to this type of environment with the Dynamic Systems Initiative. Our involvement will likely be telling these tools about new initiatives and services needed to know what infrastructure to put in place. New versions of software such as Exchange can be downloaded and applied automatically, assuming organizations still have local servers and software. It's entirely possible everything will be a service offered by a "cloud" on the Internet which companies subscribe to.

So with all of that, why is there snow on the cover? Snow makes anything look calm and beautiful. I hope the cover is calming. If ever you start panicking about content in this book, just stop and look at the cover. Like they said in the book *The Hitchhiker's Guide to the Galaxy*, "Don't panic."

Audience for This Book

I've written this book with the IT administrator and architect in mind. Although a background from Windows and networking in general is advantageous, I introduce the basics of each subject, explain how the technologies work, and then build on that transferred understanding until we get to advanced concepts and best practices.

This is not a Microsoft Certified IT Professional study guide, although I did take the exams for both the MS ITP Server Administrator and Enterprise Administrator without studying. I used what I knew from writing this book and easily passed all the exams with high marks. So if you

understand and can apply the information in this book, I would expect you to do well on the Microsoft exams.

This Book's Organization

It would be great if you could sit and read this book from start to finish. Although you may not be able to learn all the features, you may remember items that are possible in day-to-day work and then re-read details of specific features. In the same manner that a chef expects you to eat all courses of a meal instead of picking at each one, I expect this book to be “digested” more like a buffet. You might want to consume the parts relevant to you. I urge you, however, to read a chapter at a time, and not just part of a chapter because each one builds on a subject. In addition, I typically start each chapter with details for you to thoroughly understand the concepts so that we can cover other concepts more quickly.

I want to teach you to drive, not to understand the internal parts of the engine. I'm not big on giving detail on components that don't do you any good from a design or management perspective, but I do give internal details when it aids in learning a technology.

Structure of This Book

This book is made up of 24 chapters:

- **Chapter 1, “Windows 101: Its Origins, Present, and the Services It Provides,”** introduces the major new features of Windows Server 2008. It highlights the key differentiators between the editions of Windows Server 2008 from Web edition through Datacenter.
- **Chapter 2, “Windows Server 2008 Fundamentals: Navigating and Getting Started,”** walks you through the key interface and management components of Windows Vista and Windows Server 2008. The log-on experience for Windows in both workgroup and domain environments is detailed along with the changes to how the built-in Administrator account is handled in Vista and 2008. The chapter discusses User Access Control and how it impacts how to use Windows. Also, key Windows elements, including the Start menu, task bar, and the system tray, are examined along with the available customizations.

Most of your time with Windows Server 2008 is spent in Task Manager, Explorer, and the Microsoft Management Console, so Chapter 2 looks at the major elements of these powerful tools and finishes off with a quick look at the Control Panel.

- **Chapter 3, “Installing and Upgrading Windows Server 2008,”** walks you through the basic system requirements of Windows Server 2008 in terms of memory, processor, and disk space. Windows Server 2008 has a number of activation options, and this chapter looks at both Multiple Activation Keys and Key Management Service.

The next section walks through performing an upgrade from Windows Server 2003 SP1 to Windows Server 2008, and the various options and limitations associated with an in-place upgrade. The chapter ends with automating local installations using XML answer files.

- **Chapter 4, “Securing Your Windows Server 2008 Deployment,”** discusses security. It looks at authentication and authorization methods, along with the importance of the physical environment that houses your servers. It also discusses BitLocker and how to use it most efficiently.

This chapter also looks at the built-in certification service in Windows Server 2008, Active Directory Certificate Services (ADCS), and how it is used in (and out) of an organization.

Finally, Chapter 4 discusses the Security Configuration Wizard and the Security Configuration and Analysis tool that can increase the security of an environment. Increasing network security is handled via the Windows Firewall and IPsec, which this chapter details, along with more information on the User Access Control.

- **Chapter 5, “File System and Print Management Features,”** looks at the facilities that the Windows Server 2008 platform provides for the critical storing of an organization’s data. After discussing the new capabilities of NTFS, this chapter looks at creating and managing volumes for data storage. The file permission and ownership capabilities are explained and the concept of shares are introduced and walked through. Then, more advanced subjects are covered, including using quotas to control how much data users can store, file screening technologies to control how the storage is used, and reporting capabilities.

The second section of Chapter 5 deals with print management, which has taken some big steps in Windows Server 2008. For the

deployment of printers to users, Group Policy can now be used to assign printers to users based on their physical location so that as a user moves, he can be assigned printers that are physically close to him. The chapter closes with a detailed look at printer configuration options.

- **Chapter 6, “TCP/IP,”** starts from the ground up with Internet Protocol (IP). Network Address Translation (NAT) is explored as a means for sharing public IP addresses between multiple computers on a private network. Then, this chapter looks at Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) as methods to provide levels of reliability and extra service to IP communication.

Chapter 6 rounds off with a look at troubleshooting IP communication through various utilities. It also looks at tracing network traffic, which is invaluable for resolving issues and understanding more complex protocols.

- **Chapter 7, “Advanced Networking Services,”** looks at two main capabilities that make the Internet Protocol more usable and manageable in an environment: Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS). The chapter ends with a brief look at WINS and how its capabilities are hopefully no longer required.

- **Chapter 8, “Remote Access and Securing and Optimizing the Network,”** looks at extending the visibility of our enterprises resources to external users in a controlled manner via a virtual private network (VPN). It also looks at the different types of VPN that are available and the pros and cons of each. NAT is explained and its impact on VPNs explored.

Finally, Chapter 8 looks at one of the major features in Windows Server 2008: Network Access Protection (NAP). It walks through the various types of NAP available, how to use NAP, and how best to configure it. It looks at implementation options for NAP to ensure the most secure environment while minimizing potential impact to the organizations users, thus, avoiding business impact.

- **Chapter 9, “Terminal Services,”** kicks off with an overview of Terminal Services (TS) before walking through the basic steps to enable Remote Desktop and then use Remote Desktop. New security features related to Remote Desktop are examined. Licensing is key with TS, and licensing options are documented and advice given

on which of the licensing modes work in different types of organizations.

The next section looks at installing the full TS role in Windows Server 2008 and its role services, which include TS Gateway for access over SSL and Remote Applications to enable seamless application execution on a terminal server without having a full desktop on the remote server visible. Tied in with Remote Applications, the chapter looks at TS Web, which gives a Web-based portal to launch remote applications.

As TS becomes more important in an organization, it will be necessary to ensure that users can get sessions and good responses, so that multiple terminal servers are pooled together into a farm. Chapter 9 looks at the technologies to facilitate terminal server farms.

- **Chapter 10, “Active Directory Domain Services Introduction,”** looks at the history of domains in Windows and the basic building blocks of Active Directory Domain Services (ADDS). It looks at trust relationships and how they are a core part of Active Directory (AD) hierarchical structure. The chapter then expands on the structure of ADDS by looking at features such as Organization Units, Global Catalog servers, and the special Flexible Single Master of Operations (FSMO) roles.

Replication is key to ADDS, and this chapter looks at the site components that document to ADDS the physical structure of the environment, the subnets for each location, and the links between each location. Chapter 10 ends with a look at the various domain and forest modes that enable additional features.

- More advanced AD concepts are explored in **Chapter 11, “Designing and Installing Active Directory.”** This chapter begins by adding a replica domain controller to an existing domain to give the domain high availability and support for more users and distributed environments.

For Windows Server Core installations and automated AD deployments, an unattended approach is required. The unattended answer format is explored along with an easy way to create the answer file that is new in Windows Server 2008.

Management functions related to the FSMO domain controllers are explored, including normal movement of FSMO actions and exception FMO movement options. The last setting the chapter looks at is Global Catalog creation.

The next section deals with creating a new domain, but more importantly, the reasons of when and why a new domain is created. Steps related to verifying a new domain controller are described. The chapter then looks at demoting a domain controller to a normal member server.

One of the major new features in Windows Server 2008 is the Read-Only Domain Controller (RODC); the chapter looks in detail at the capabilities of RODC, its usage considerations, and the restrictions. Chapter 11 closes with a detailed look at the various types of trust relationships and how to create them.

- **Chapter 12, “Managing Active Directory and Advanced Concepts,”** looks at managing AD, backing up and restoring the AD, and other more advanced features. It looks at AD management tools, both graphical and command line-based.

This chapter also looks at how backing up the AD has changed in Windows Server 2008, using new AD snapshots and restoring deleted objects.

Chapter 12 closes with a look at changing the replication technology from FRS to DFS-R when you are running a pure Windows Server 2008 domain controller environment.

- **Chapter 13, “Active Directory Federated Services, Lightweight Directory Services, and Rights Management,”** deals with the other role services that complement ADDS, namely Active Directory Lightweight Directory Services (AD LDS), Active Directory Rights Management Services (AD RMS), and Active Directory Federated Services (AD FS).

- **Chapter 14, “Server Core,”** starts with an overview of server core followed by how to perform a Windows Server 2008 installation for a server core instance. When the installation is complete, the hard part is configuring and managing because you don’t have the same local graphic tools available that are normally present in a full Windows Server 2008 instance.

The various command line utilities are explored to perform configuration in addition to walking through configurations that can be done with limited graphical tools such as the Registry editor. Along with this configuration, the chapter explores how to keep a server core patched and what applications can be installed on a server core installation. Finally this chapter looks at managing a server core installation.

- **Chapter 15, “Distributed File System,”** discusses one of the greatest challenges in a distributed environment: managing data and making the data available to all users in a timely fashion. The Distributed File System (DFS) consists of two components: Distributed File System Namespace (DFSN) and Distributed File System Replication (DFSR).

Chapter 15 closes with a look at best practices to design a DFSR topology and how to troubleshoot and monitor the overall health of replication.

- **Chapter 16, “Deploying Windows,”** starts with a brief history of deployment and then introduces the technologies required to deploy modern operating systems (OSs).

Installing and configuring WDS is covered, along with the considerations of running WDS and DHCP together and separately. After WDS installation is explained, the process of importing images is introduced and the process discussed. Automated installations are key in large environments, and the process of creating an unattended answer file using the Windows System Image Builder is explained.

Chapter 16 also looks at creating custom images from reference installations and then maintaining the images by installing fixes, additional drivers, and even language packs. Finally, multicast deployments are explored.

- **Chapter 17, “Managing and Maintaining Windows Server 2008,”** looks at the major tasks and utilities that relate to managing and maintaining Windows Server 2008. The majority of the chapter is spent exploring Server Manager: how to manage the roles and features of Windows Server 2008 using Server Manager and, more than just management actions, how Server Manager gives consolidated insight into each role and is a go-to point to troubleshoot.

Chapter 17 then looks at Windows Server Backup, the major changes in Windows Server 2008, and details on the Volume Shadow Copy Service (VSS).

Patch Updates are critical to keeping your environment healthy and secure. The chapter looks at the options for patching systems, their advantages and disadvantages, and finally, the Registry.

- **Chapter 18, “Highly Available Windows Server 2008,”** looks at the two high availability features of Windows Server 2008: Network Load Balancing (NLB) and Failover Cluster. Validating hardware for Windows Server 2008 clustering is shown, as well as the process

to create and manage a Failover Cluster. Chapter 18 finishes with the migration options from a Windows 2003-based failover cluster.

- **Chapter 19, “Virtualization and Resource Management,”** focuses on two main virtualization technologies: machine virtualization and the new hypervisor-based virtualization solution in Windows 2008, Hyper-V, including how to install Hyper-V, and best practices of configuring and managing. We then complete the section with a look at high availability solutions for Hyper-V through failover-clustering.

Chapter 19 closes with Windows Server Resource Management. It is not a virtualization technology but allows multiple applications/services to be run on a single OS instance while allocating a specific amount of memory and processor to processor. This allocation of resources allows performance guarantees to be made when consolidating multiple OSs running an application, down to a single OS instance running multiple applications.

- **Chapter 20, “Troubleshooting Windows Server 2008 and Vista Environments,”** starts with the basic building blocks of the OS in terms of processes, threads, jobs, and handles—these are key items that are manipulated when troubleshooting. The chapter looks at the boot options for Windows and then delves into the Windows Recovery Environment (RE) that fixes problem systems from outside of Windows.

The Reliability and Performance Monitoring interface gives access to performance attributes of an OS instance in addition to a historical view of issues on the system for a general “health” view.

The Event Viewer is covered extensively because it is the main portal to see what is going on in the Windows installation. When there are problems, an event log is typically written to see the system events, pertinent event logs, and how to receive specific event logs from other systems in our environment.

Chapter 20 closes with a look at System Center, which has solutions that help monitor an environment and preemptively troubleshoot and resolve issues before users are impacted. It’s better to fix something before it’s a problem.

- **Chapter 21, “Group Policy,”** starts with an overview of Group Policy, its architecture, and basic usage, before going into detail about the Group Policy Management Console (GPMC), the tool of choice for group policy management. Using the GPMC, advanced

concepts are covered, such as using no override, block inheritance, and filtering capabilities. Resultant Set of Policy features are explored that help ascertain how policy is applied for a user/computer and how policy is applied in different circumstances, for example, if the user was moved to another Organizational Unit.

Chapter 21 then looks at features that are new to Windows Server 2008, including the new Starter GPO functionality and Group Policy Preferences capability to set initial configurations for a computer that the user can override.

- **Chapter 22, “The Command Prompt and PowerShell,”** kicks off with a look at the old style command prompt (cmd.exe) environment with information on customization and how to access and set environment variables, before moving onto more advanced concepts such as chaining commands and redirecting output.

The Windows Scripting Host is explored as a way to create more complicated sequences of logic with some VBScript examples.

PowerShell is explored with focus on its structure and capabilities for forming complex action sequences. PowerShell can interact with the environment including system processes, the Registry, and file systems. Scripting with PowerShell is explored and some scripts are showcased to further explain capabilities and error handling features.

- **Chapter 23, “Connecting Windows Server 2008 to Other Environments,”** discusses integration with UNIX and NetWare, an important capability in mixed environments. Windows Server has capabilities to integrate and migrate with both UNIX and NetWare environments

- **Chapter 24, “Internet Information Services,”** looks at the Internet Information Services role in Windows Server 2008. The chapter starts with the new architecture that is a radical change from in previous versions, giving administrators and developers greater power to customize IIS processing.

The configuration of IIS is explained, as well as the various levels of configuration made possible by the new configuration architecture of IIS 7. The process of IIS role service installation is shown along with the steps required to create and access new web sites.

The chapter looks at new capabilities in IIS 7 including URL authorization that allows specific users to access a site and new management delegation capabilities. IIS is one of the roles supported by

Windows Server Core, and the restrictions associated with this IIS support are communicated. Chapter 24 concludes with the Windows Web Server 2008 SKU.

Code and Command Entry

Some code statements presented in this book are too long to appear on a single line. In these cases, a code continuation character (➤) indicates that the following line is a continuation of the current statement. Scripts can be found at www.savilltech.com/completeguidetowindows2008.

SERVER CORE

This chapter looks at a new feature in Windows Server 2008, an installation option known as a Server Core installation (as opposed to a full installation). Windows Server Core is not a separate product or even a separate license; it simply installs a bare metal server installation with the components needed to run a small set of core network roles, such as domain controller service and file service features, without everything else...which includes the exclusion of the familiar Windows Explorer GUI. You start with a detailed overview of Windows Server Core, which details the roles that it can fulfill, and then you look at ways to install Server Core. Finally, you learn how to configure and use your GUI-less Server Core environment.

Overview of Windows Server Core

In nearly all environments today, servers are designated for a single purpose. Often when you go to a client's site, the conversation is "these are the domain controllers, here are the file servers" and so on. Microsoft recognizes this specialization of servers. This recognition can be seen in the role-based nature of Windows Server 2008. However, even though your domain controllers, for example, need only a limited number of services to function (and maybe domain name system [DNS]), the server has a plethora of unneeded components. These components bloat the server, requiring the server to have more resources to function than are needed for its main function. Most importantly, the more components the system has installed, the more possible vulnerabilities it has. The more components there are, the greater the attack surface and the more patches required, resulting in more management overhead.

The typical server has the full .NET Framework, Internet Explorer, Media Player, and Outlook Express, all of which will likely never be used but still have to be managed.

With Windows Server Core, the “extra” parts of Windows Server 2008 have been removed, leaving a much thinner core operating system than with a normal Windows Server 2008 full installation. Because it has far fewer components, you benefit from having a reduced attack surface and less to manage and maintain. Server Core has only the critical components of the operating system necessary to support the various roles and features made available on a Windows Server Core installation. Many of the non-value-add legacy and client components are missing from Server Core.

This much smaller footprint, and optimized installation based around specific roles such as a domain controller or file server, means the following:

- As already discussed, Server Core presents less attack surface because it involves fewer components with less possible vulnerabilities.
- Because you have fewer components installed, fewer patches apply to a Server Core installation than to a normal full installation. You often hear of an urgent patch related to an Internet Explorer vulnerability. If Internet Explorer is not installed, you don’t need to apply that patch. Microsoft believes there will be a large reduction in the number of patches needed for a Server Core install compared to a full installation. It’s not possible to know how many patches will be released for Windows Server 2008 or what components the patches will be applicable to. But if a core version had been available for Windows 2000, it would have required 60 percent fewer patches than a full installation, and if available for Windows 2003 there would have been a 40 percent reduction in patches. The servicing stack in Windows Server 2008 downloads and applies only fixes that apply to components installed on the system. No actions or special Windows Update site is required that is Server-Core-specific.
- Administrators can focus more on their technology area without having to be so worried about general Windows knowledge because all the extra parts are no longer installed.
- With fewer components running, the installation uses fewer system resources and becomes more reliable because the fewer different components executing, the less chance of problems occurring.
- Less disk space. A typical core installation uses 1GB of disk space for the install and additional disk space for its actual operation. In

terms of other resources, there is not a great deal of difference, although obviously with fewer components, fewer resources are used overall. But remember: A Windows 2008 install alone requires 512MB of RAM.

The Server Core is available as an installation option for the Standard, Enterprise, and Datacenter editions of Windows Server 2008 and is available on both the x86 and x64 architectures.

Because the Server Core is a minimal installation of Windows, not all the full Windows Server components can run. For example, because the .NET Framework is not present in Server Core, which in turn means no Common Language Runtime (CLR), no managed code can run. That means no PowerShell. A Server Core installation has many “nots”:

- There is no Explorer-based shell, so the Start button, taskbar notification area (system tray), and taskbar are eliminated. There are no fancy wall papers, screen savers (a default screen saver shows the Windows Server 2008 logo), and no Aero Glass. Explorer itself is not available, which means no My Computer. Because you have no system tray, you get no balloon notifications, which also means no password prompts because they are balloon notifications.
- No Explorer means no Internet Explorer, no Search, no Run, and no Help, but you do get Notepad.
- No .NET Framework. This is because the .NET Framework is monolithic, meaning all or nothing. And .NET has a lot of multimedia-related code and other components that do not fit the Server Core model. However, a “core” version of the .NET Framework is expected for the Windows Server 2008 R2 timeframe. This means no managed code, which requires .NET.
- No Microsoft Management Console (MMC), which means no snap-ins either. That is an issue because nearly everything is managed with the MMC.
- Only two Control Panel applets.

So let's get it clear. With Server Core, there is no graphical interface, no management tools, no Explorer, no Control Panel applets? Before you get freaked, this is a great feature. The advantages of the reduced overhead are worth a little hardship. You do have a shell, but it's the command

prompt. However, if you think about it, nearly every MMC snap-in you have today can connect to a remote computer, which helps you manage your GUI-less Server Core installation.

What do you get? Much more than in the early builds of Longhorn when the only roles available were Active Directory Domain Servers (a domain controller), DNS, DHCP and File Servers. You are a lot further than that now. As you've seen, with Windows Server you have roles, which are important components of Windows Server 2008, and features, which are less important than their older, driving Role brothers. Table 14-1 provides a list of the roles and features available in Windows Server Core. Note there are no relationships between the roles and features; they are in a table only to save space.

Table 14-1 Windows Server Core Roles and Features

Server Core Roles	Server Core Features
Active Directory Domain Services (ADDS)	BitLocker Drive Encryption (and remote admin tools)
Active Directory Lightweight Directory Services (formally known as ADAM)	Failover Clustering
DHCP Server	Multipath I/O
DNS Server	NAP Client
File Services	QoS (Qwave)
Internet Information Services (IIS)	Removable Storage Management
Print Services	Simple Network Management Protocol (SNMP) Services
Streaming Media Services	Subsystem for UNIX-based applications
Windows Server Virtualization (Hyper-V)	Telnet Clients
	Windows Process Activation Service
	Windows Server Backup
	WINS Server

Don't forget that Server Core is not a separate operating system. It just takes advantage of the highly componentized nature of Windows Server and deploys only the most critical components. Core still has the same kernel as a normal installation in addition to other core components such as

the Hardware Abstraction Layer (HAL), memory manager, security subsystem, Winlogon, file systems, networking subsystem, Windows File Protection, Distributed Component Object Model (DCOM), and remote procedure call (RPC), and device drivers for NIC, disk, and basic video. Many of the other drivers have been removed from Core, such as audio drivers and modem drivers. However, you can add them manually. Imagine a print server, however; print drivers are also not included with Server Core because Windows Server 2008 has nearly 1GB of printer drivers. Instead of including drivers in Server Core for a role that might not be used, the print drivers are not included. When you enable the Print Server role, the spooler starts, and drivers need to be manually added using the Print Management Console remotely from a Windows Vista/Windows 2008 machine.

Also included are features such as the event log, which is critical to nearly all components of Windows, performance counters, WS-Management for remote management, and Windows Management Instrumentation (WMI).

Think of Server Core as a subset of the full Windows installation. If a core kernel patch is released, the same patch for Windows Server is applicable to a Server Core installation. How do you use this? What do you get to manage this Server Core environment? Let's look at installing Server Core, and then you can see the usable environment.

Installation

Server Core installation does not warrant its own section because it's the same as a normal installation of Windows Server 2008. The install media is placed into the server or the server boots over the network, and a product key is entered that identifies the particular edition of Windows Server 2008. In this case, it needs to be Standard, Enterprise, or Datacenter. The only difference is during the actual installation, after entering the product key, you select the type of Windows Server 2008 installation, full or core, as shown in Figure 14-1.

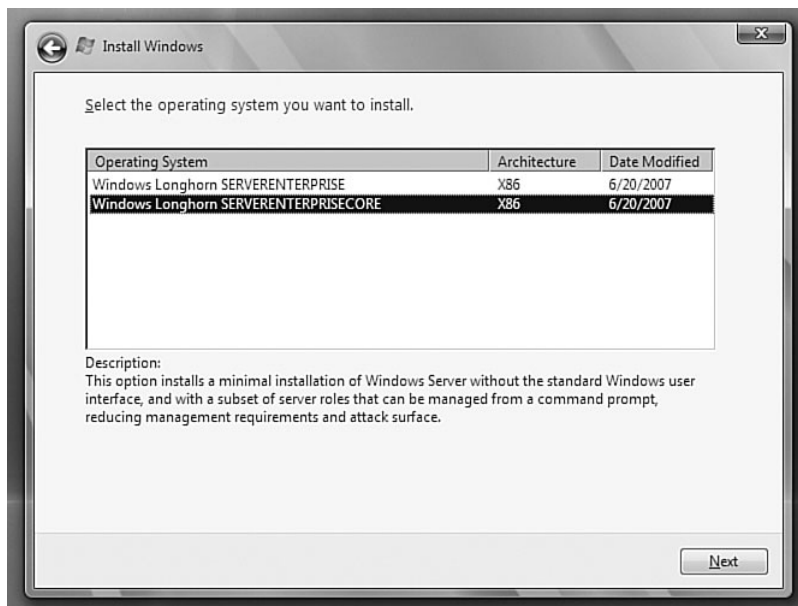


FIGURE 14-1 The description is your first clue that your command-line skills are about to get much better.

When the installation is complete, you get the familiar and comfortable Press Ctrl+Alt+Del to Log On dialog with the pretty Windows Server logo at the bottom. If you press the secure attention sequence, you are prompted to enter logon credentials, so for now all you can do is log on with the administrator account with a blank password.

So far, this is looking great, as Figure 14-2 shows. After clicking the logon button, you are prompted to change the password as normal, and you set a new administrator account password. The normal process of applying local policy and preparing the desktop takes place, and then your Server Core desktop loads, as shown in Figure 14-3.

Note that you cannot upgrade from Windows Server 2003 to Server Core; only fresh installations of Server Core are supported. You also cannot upgrade from Server Core to the full Windows Server 2008 product, nor can you downgrade from Windows Server 2008 to Server Core. If you need to switch between versions, perform a clean installation.



FIGURE 14-2 So far this Server Core environment looks familiar.

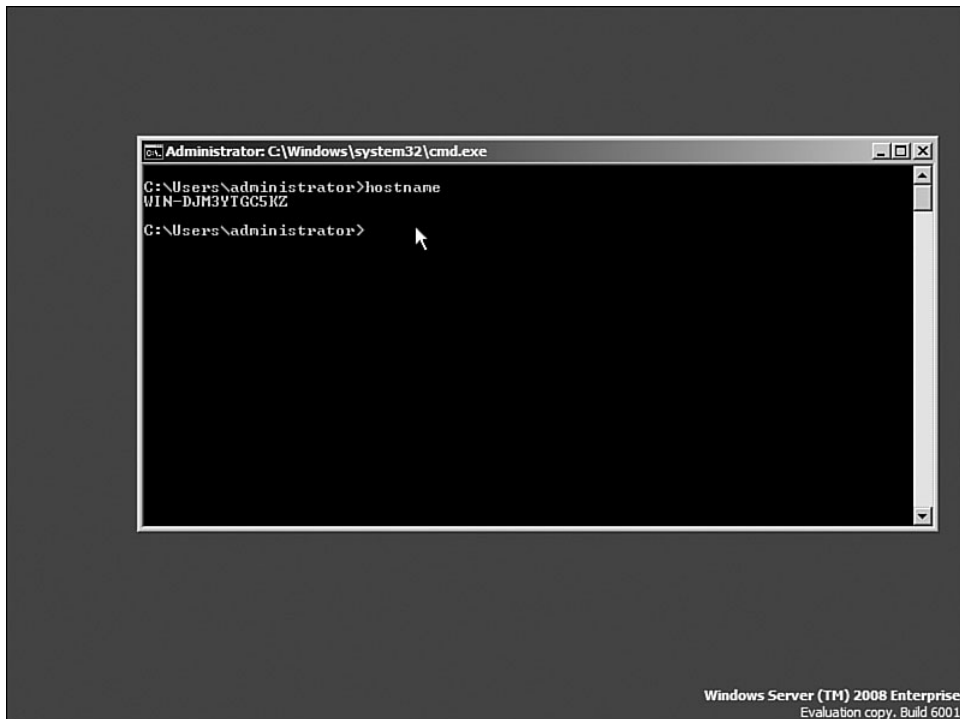


FIGURE 14-3 In keeping with trends from server-based computer to client/server back to server-based, you are now back to a command prompt server environment.

Server Core Configuration

Now that Server Core is installed, first you need to configure it. Without the normal graphical elements, you don't have the nice Initial Configuration Tasks (ICT) interface that you would normally use to configure Windows Server 2008 server, so you have two options:

- Manually configure the server using command-line tools.
- Automate the configuration using answer files during the actual installation.

The second option is the way to go for any sizable deployment. One of the big pushes of the latest operating system has been zero-touch deployments, so you can automate the install and configuration of all the main components. However, this does take up-front effort and planning but is definitely an option. Other areas of the book talk about unattended installations, so for now concentrate on the manual configuration of the server. However, if you go the unattended route, Server Core uses the same unattended syntax as Windows Vista and a normal server. Use the Windows System Image Manager from the Windows Automated Installation Kit (WAIK) to help create the unattended eXtensible Markup Language (XML) answer file. There are some advantages to using the unattended XML, however, because some items are quite hard to configure in Server Core. For example, configuring screen resolution is quite complex without the Display Control Panel applet! The display options are part of the Microsoft-Windows-Shell-Setup component, and a sample code extract for an unattend.xml is shown here:

```
<settings pass="oobeSystem">
  <component name="Microsoft-Windows-Shell-Setup"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMICConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <Display>
      <HorizontalResolution>1280</HorizontalResolution>
      <VerticalResolution>1024</VerticalResolution>
      <ColorDepth>16</ColorDepth>
    </Display>
  </component>
</settings>
```

If you examine the content of the install.wim file for Windows Server 2008, you see that a CORE version exists for each operating system. If you are using Windows Deployment Services (WDS) or any other XML installation, select the CORE post-fixed version, as shown in Figure 14-4.

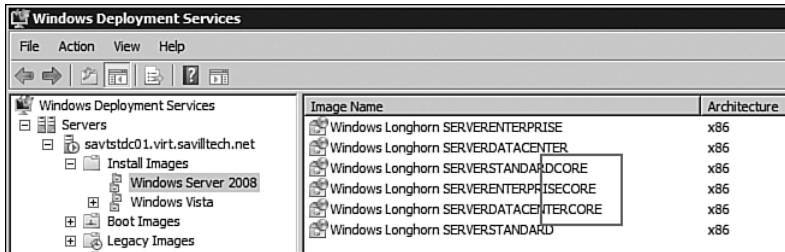


FIGURE 14-4 The core versions of the main Server 2008 editions.

Let's look at the main things you normally do when you configure a new server:

- Set the administrator password.
- Set the machine name.
- Set static TCP/IP v4 details.
- Set the time zone.
- Join a domain.
- Set keyboard and international settings.
- Set the default scripting engine.
- Activate the server.
- Install patches.
- Configure the firewall.
- Configure the server pagefile.
- Enable Remote Desktop.
- Configure hardware.
- Add roles and features.

You would normally do all this via GUI interfaces. For example, you would use Network and Sharing Center to configure IP settings, Windows Update for patches, and so on, but none of these interfaces are available. You can still set all of these things using the command line and some Server Core-specific commands. However, most of these are standard commands and can be used on normal installations for configuration and for scripted communication.

Setting the Administrator Password

The Winlogon and security subsystem in Core is the same as in a standard installation of Windows Server 2008, so to change the password of the logged-on account, just press Ctrl+Alt+Delete as you would normally do. Select the Change a Password link from the menu, and the normal change password dialog displays.

Passwords can also be changed via the `net user` command as on any other Windows installation by passing the username and the new password or passing the wildcard (*) character to be prompted for the new password, as shown in Figure 14-5. To change a domain account password, add the `/domain` switch.

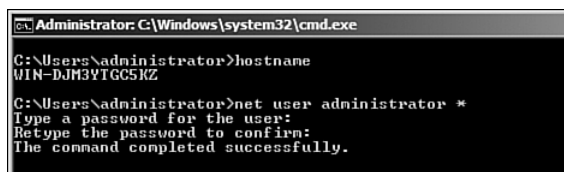


FIGURE 14-5 The `net user` command is an easy way to manage local account passwords.

Setting the Server Name

In the first screen, you viewed the server name using the `hostname` command. However, to change the server name, use the `netdom` command with the `renamecomputer` switch. To avoid having to type in the long default computer name, use the `%computername%` environment variable and then pass the new server name with the `/NewName` switch:

```
C:\Windows\System32>netdom renamecomputer %computername% /New  
Name:savtstcore01
```

This operation will rename the computer WIN-DJM3YTG5KZ to savtstcore01.

Certain services, such as the Certificate Authority, rely on a fixed machine name. If any services of this type are running on WIN-DJM3YTG5KZ, then a computer name change would have an adverse impact.

Do you want to proceed (Y or N)?

y

The computer needs to be restarted in order to complete the operation.

The command completed successfully.

This change does not take immediate effect; a reboot is required by selecting the Restart option from the Ctrl+Alt+Del screen shutdown options as shown in Figure 14-6 or by using the `shutdown /r /t 0` command. When the reboot is complete, the server has taken the new name, which you can verify by rerunning the `hostname` command.

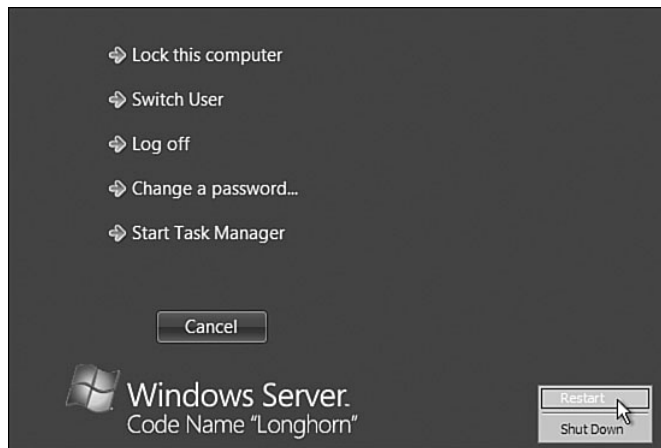


FIGURE 14-6 Although you don't have a Start menu, access shutdown options via the Ctrl+Alt+Del menu.

Setting Static TCP/IP v4 Information

By default, the new installation has been dynamically allocated an IP address. However, in most cases a server needs static IPv4 information, which can be seen with the `ipconfig /all` command. It will show DHCP Enabled set to Yes.

Because you can't use the normal Network interface to set the IP properties, instead use the `netsh` command. However, before you can set the

IP properties, check which interface you are configuring. By default your server has two network interfaces: the “real physical” interface and a second IntraSite Automatic Tunnel Addressing Protocol (ISATAP) tunneling interface, which sends IPv6 packets over an IPv4 network by encapsulating the IPv6 packet in the IPv4 header. You need to configure the physical connection and not the ISATAP one, so list your interfaces to identify the index of the physical adapter.

```
C:\Users\administrator>netsh interface ipv4 show interfaces
```

Idx	Met	MTU	State	Name
---	---	---	-----	-----
2	10	1500	connected	Local Area Connection
1	50	4294967295	connected	Loopback Pseudo-Interface 1

When the adapter is identified, which in this case is index 2, the IP details can be set. They most likely consist of an IP address, a subnet mask, a gateway, and one, possibly two, DNS servers.

To set the IP address, subnet mask, and gateway, run the following and change the information for your environment:

```
C:\Users\administrator>netsh interface ipv4 set address
➤name="2" source=static address=192.168.1.232
➤mask=255.255.255.0 gateway=192.168.1.1
```

You can now add the DNS servers. The primary DNS server gets an index of 1, the secondary DNS server gets an index of 2.

```
C:\Users\administrator>netsh interface ipv4 add dnsserver
➤name="2" address=192.168.1.230 index=1
```

```
C:\Users\administrator>netsh interface ipv4 add dnsserver
➤name="2" address=192.168.1.10 index=2
```

If you need to configure primary and secondary Windows Internet Name Service (WINS) servers, use the same syntax as for adding DNS servers but use `winsserver` instead of `dnsserver`. The first index would be the primary WINS server and the second index the secondary WINS server.

If you now examine the IP information with `ipconfig/all`, the configured settings are displayed, as shown in the following example:

```
C:\Users\administrator>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : savtstcore01
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . . . :
Description . . . . . : Intel 21140-Based PCI
Fast Ethernet Adapter (Emulated)
Physical Address. . . . . : 00-03-FF-0E-0D-F9
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . :
fe80::c49a:b729:8c8b:471e%2 (Preferred)
IPv4 Address. . . . . : 192.168.1.232 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.230
                        192.168.1.10
NetBIOS over Tcpi. . . . . : Enabled
```

If you need to remove a DNS server, or more likely a WINS server, after you finally get it killed off, use the `del` keyword instead of `add`. For example:

```
Netsh interface ipv4 del winsserver name="2"
address=192.168.1.10
```

Setting the Time Zone

The date and time are easy to set using the `date` and `time` command lines, but using a command-line method to set the time zone is trickier. There are Registry areas for the time zone. However it's not necessary to use the Registry. Remember that Control Panel is unavailable in Server Core except for two applets. The Date and Time Control Panel applet is one of them; start it via the following command:

```
control timedate.cpl
```


After loading the applet, perform the normal date/time and time zone configurations, as shown in Figure 14-7. Note that in a domain environment, the time synchronizes; however, you might need to set the time zone.

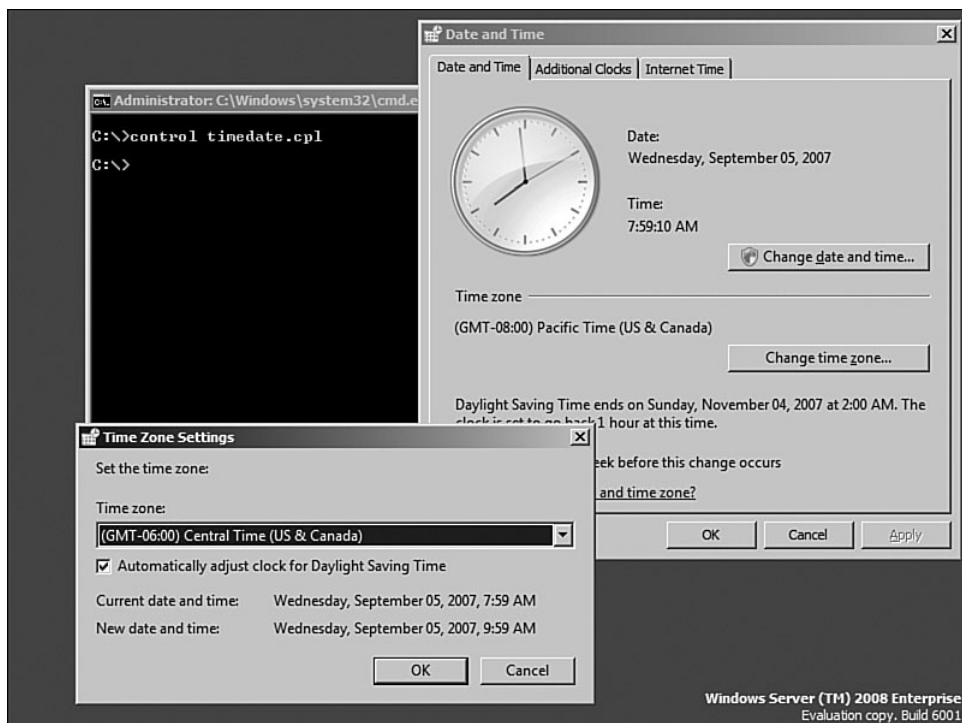


FIGURE 14-7 At last, a graphical way to configure something.

Joining a Domain

It is most likely your servers are part of a domain, and unless the server was preprovisioned during deployment or used an answer file, you need to configure your server to join a domain. After the IP configuration is configured with the correct DNS servers, the computer name is set, and the time configuration is correct, you can join the domain.

To join a domain, use the same command that you used to rename the computer: `netdom`. Full help can be seen by running `netdom join /?`, which gives information on specifying a specific organizational unit (OU) to place the computer into. However, at the most basic level, pass the domain you want to join, the account to use to perform the join, and its password:

```
C:\>netdom join %computername% /domain:virt.savilltech.net
➡/userd:administrator /passwordd:*
Type the password associated with the domain user:
*****
The computer needs to be restarted in order to complete the
operation.

The command completed successfully.
```

Replace the domain name with your domain, and then restart the server. After the reboot, you can log on as a domain user, which confirms the domain join operation worked successfully. You can also verify your connectivity to the domain using the `netdom /verify` command as in the following example:

```
C:\Users\administrator.VIRT>netdom verify %computername%
➡/domain:virt.savilltech.net
The secure channel from SAVTSTCORE01 to the domain VIRT.
SAVILLTECH.NET has been verified. The connection
is with the machine \\SAVTSTDC01.VIRT.SAVILLTECH.NET.

The command completed successfully.
```

Configuring International Settings

The second Control Panel applet available in Server Core is the Regional and Language Options applet. It enables the configuration of the keyboard layouts, languages, and location. To launch the applet, run the following command and configure as a normal installation:

```
Control intl.cpl
```

Setting the Default Scripting Engine

With Server Core, you do a lot via various scripts executed by the Windows Scripting Host, which has a GUI and a command-line engine. By default the GUI engine is the preferred tool, which goes against the idea of managing Server Core from the command line and requires you to remember to put `cscript` at the start of your scripts to process the script using the command-line interpreter.

To change the Windows Scripting Host to use the command-line interpreter by default, use the following command:

```
C:\Windows>cscript //H:CScript //NOLOGO //s
Command line options are saved.
The default script host is now set to "cscript.exe".
```

If you've enabled `cscript` as the default engine, you don't need to type it every time.

Activating the Server

Server Core includes the `Slmgr.vbs` script, which when passed with the `-ato` switch, performs an automated activation of the operating system. `Slmgr.vbs` is not a Server Core feature; it is present in Windows Vista and full Windows Server 2008 deployments and is the main license manager for the Vista/2008 products.

Because Server Core has no taskbar or system tray, you do not receive any prompts to activate the server, so remember to do so shortly after the installation of Server Core.

Before you activate, check your status to see how far into your initial 30-day grace period you are by using the `-xpr` switch as shown here:

```
C:\Windows\System32>cscript slmgr.vbs -xpr
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.

Initial grace period ends 10/4/2007 2:48:10 PM
```

There is also more information available via the `-dli` switch or the `-dlv` switch to get detailed info.

```
C:\Windows\System32>cscript slmgr.vbs -dli
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.

Name: Windows(TM) Server code name "Longhorn",
ServerEnterpriseCore edition
Description: Windows Operating System - Server code name
"Longhorn", RETAIL channel
Partial Product Key: 2T9PJ
License Status: Initial grace period
Time remaining: 42000 minute(s) (29 day(s))
```

If you have a normal license key or Multiple Activation Key (MAK) that activates with Microsoft, you can go ahead and just activate. However, if you have a local Key Management Service (KMS), tell the activation to use it via the `-skms <KMS server>` switch. If you need to clear the configured KMS server, use the `-ckms` switch. If you are using an enterprise license key, use the `-ipk <key>` switch.

To activate, use the `-ato` switch as previously mentioned. Rerun the display of license information to see the status is now licensed with no time remaining.

```
C:\Windows\System32>cscript slmgr.vbs -ato
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
Activating Windows(TM) Server code name "Longhorn",
ServerEnterpriseCore edition
(f00d81ce-df2c-47cb-a359-36d652296e56) ...
Product activated successfully.
```

```
C:\Windows\System32>cscript slmgr.vbs -dli
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
Name: Windows(TM) Server code name "Longhorn",
ServerEnterpriseCore edition
Description: Windows Operating System - Server code name
"Longhorn", RETAIL channel
Partial Product Key: 2T9PJ
License Status: Licensed
```

Installing Patches and Configuring Auto-Update

You can use various methods to patch Server Core. You can push patches with Group Policy or System Center Configuration Manager or any other deployment-type product. You can use Windows Update, which is disabled by default. (You can confirm that with the `/au /v` switches with `scregedit.wsf`.) To enable Windows Update to perform the normal 3 a.m. checks, run the following commands. The `scregedit.wsf` script is Server Core-specific and was written to help perform the functions that are

otherwise difficult to do from the command line. The script is installed automatically on all Server Core installations.

```
C:\Windows\System32>cscript scregedit.wsf /au 4  
Microsoft (R) Windows Script Host Version 5.7  
Copyright (C) Microsoft Corporation. All rights reserved.
```

Registry has been updated.

```
C:\Windows\System32>net stop wuauserv  
The Windows Update service is stopping.  
The Windows Update service was stopped successfully.
```

```
C:\Windows\System32>net start wuauserv  
The Windows Update service is starting.  
The Windows Update service was started successfully.
```

You can force an update pass to run using the following command:

```
C:\Windows\System32>wuauclt /detectnow
```

You can't configure options to download patches and prompt for installation. You can either enable automatic download and application of patches or have automatic update turned off: There is no in-between configuration. You can always check the state of patch installations via the `wmic qfe list` command.

You can manually install patches using the `wusa` command, as in the following example:

```
wusa <patch name>.msu /quiet
```

Remember the patches all have applicability rules, so they won't install if the patch does not apply. If you want to check whether a patch applies, run the command without the `/quiet` switch. If you are prompted to install, it means the patch applies; if you are not prompted, it means the patch does not apply to Server Core and has been ignored. You learn more detail about patching in Chapter 17, "Managing and Maintaining Windows Server 2008."

Configuring the Pagefile

By default, the pagefile is set as managed by the system. This behavior can be modified by disabling the automatic pagefile management and manually configuring a specific pagefile size. For example, the following disables the automatic pagefile management and sets the pagefile to 1GB minimum, 2GB maximum. In general, the default Windows settings for the pagefile should not be changed—do so only if given specific guidance by an expert or vendor of an application being installed. Notice the code in the following listing is using the Windows Management Instrumentation Command-Line (WMIC) environment, which opens up a lot of functionality. Some of the other commands you performed could have been done with the WMIC. After running the commands in this listing, you must restart the server for the changes to take effect.

```
C:\Windows\System32>wmic computersystem set
➔AutomaticManagedPagefile=false
Updating property(s) of '\\SAVTSTCORE01\ROOT\CIMV2:Win32_
ComputerSystem.Name="SA
VTSTCORE01"'
Property(s) update successful.

C:\Windows\System32>wmic pagefileset where name="C:\\
➔pagefile.sys" set InitialSize=1000,MaximumSize=2000
Updating property(s) of '\\SAVTSTCORE01\ROOT\CIMV2:Win32_
PageFileSetting.Name="C
:\pagefile.sys"'
Property(s) update successful.
```

Configuring the Firewall

On a new Server Core installation, the firewall is enabled by default and blocking almost everything. You can turn off the firewall by using the following command, which opens up the ports and allows Remote Desktop, SNMP, and so forth. You can enable the firewall again by changing disable to enable.

```
Netsh firewall set opmode disable
```

You can configure the firewall elements using the `netsh` command and its various components. For example, to enable the Remote Desktop, use the following command:

```
C:\Windows\System32>netsh firewall set service
➔type=remotedesktop mode=enable
```

There is an easier way, however. The Windows Firewall MMC snap-in can connect to a remote machine, so let's try that approach as opposed to working out the hundreds of possible `netsh` commands. If you are configuring many servers, however, it would be worth creating a script with the `netsh` commands, or configuring the firewall using Group Policy. If you want to use Group Policy, the firewall is available as part of Computer Configuration, Windows Settings, Security Settings, Windows Firewall with Advanced Security. Right-click Inbound Rules (see Figure 14-8) and select a new rule, and you can use the predefined Remote Administration and Remote Desktop rules. It might not be practical to place the Server Core machines in their own OU for the application of the Group Policy, so you can use a WMI filter to check the `OperatingSystemSKU` of the server for the values 12, 13, and 14, which correspond to the Datacenter, Standard, and Enterprise Server Core installations, respectively. A sample WMI filter follows:

```
select * from Win32_OperatingSystem where OperatingSystemSKU=12
or OperatingSystemSKU=13 or OperatingSystemSKU=14
```

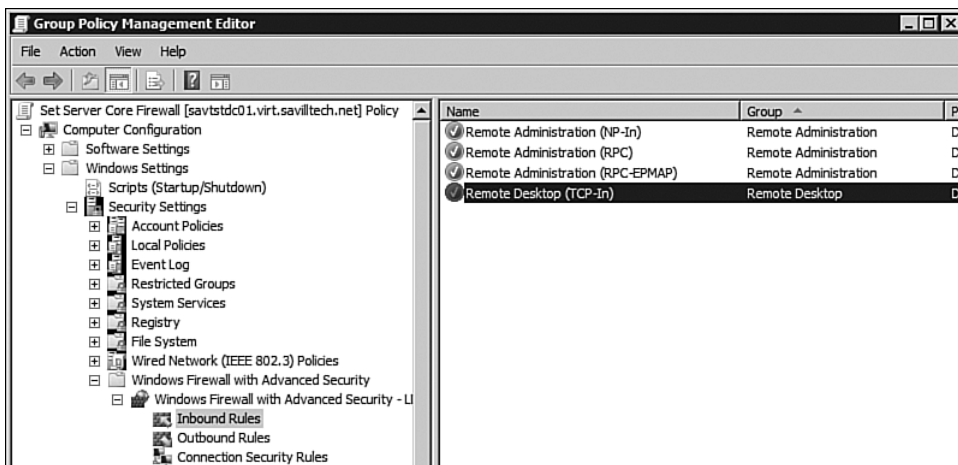


FIGURE 14-8 Using Group Policy to configure the firewall is a good option for larger deployments.

Before you try this, you get an error when you launch the remote firewall snap-in because the firewall you are trying to configure blocks remote management by default. So, you need one more `netsh` command to enable the remote management capability:

```
C:\Windows\System32>netsh firewall set service  
type=remoteadmin mode=enable
```

Now let's manage remotely:

1. Open a new MMC instance (Start, Run, MMC).
2. From the File menu, select Add/Remove Snap-In.
3. Select Windows Firewall with Advanced Security, and click the Add button (see Figure 14-9).

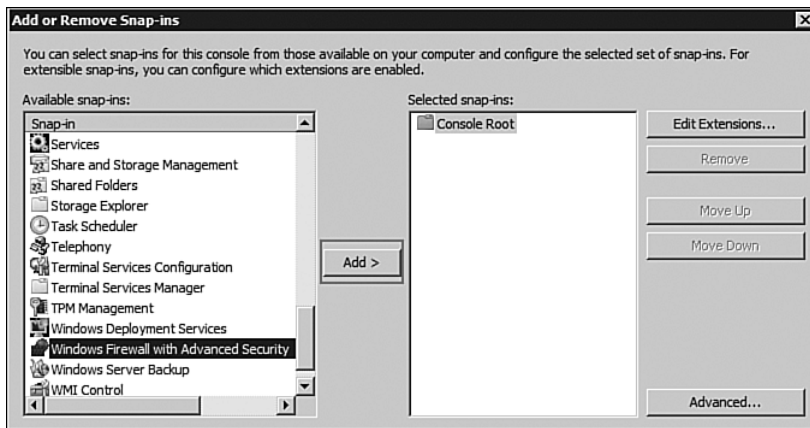


FIGURE 14-9 Select Windows Firewall with Advanced Security.

4. You are prompted to indicate whether the computer is the local computer or another computer. Check Another Computer (see Figure 14-10), specify the name of your Server Core computer, and click Finish.
5. Click OK to close the Add or Remove Snap-Ins dialog box.

Now configure the firewall remotely and enable exceptions as required.

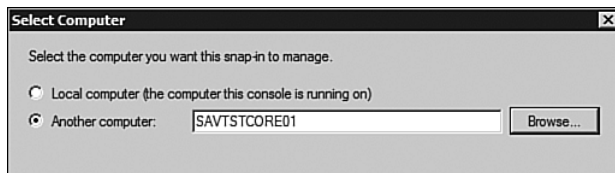


FIGURE 14-10 Check Another Computer.

Enabling Remote Desktop

Server Core contains the Remote Desktop component, which can be a useful way to manage a Server Core environment. But due to its mainly command prompt–based interface nature, there are less resource-greedy ways of managing a Server Core install.

To check the current state of Remote Desktop, use the `scregedit.wsf` script with the `/ar /v` switches, as shown in the following listing. In this case, by default, the Remote Desktop is disabled because the Deny Terminal Server Connections setting is set to true. You must be in the `Windows\System32` folder to run the script:

```
C:\Windows\System32>cscript scregedit.wsf /ar /v
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.

System\CurrentControlSet\Control\Terminal Server
fDenyTSConnections
View Registry setting.
1
```

To enable Remote Desktop, use the `/ar 0` switch:

```
C:\Windows\System32>cscript scregedit.wsf /ar 0
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.

Registry has been updated.
```

```
C:\Windows\System32>cscript scregedit.wsf /ar /v
Microsoft (R) Windows Script Host Version 5.7
```

Copyright (C) Microsoft Corporation. All rights reserved.

```
System\CurrentControlSet\Control\Terminal Server
    fDenyTSConnections
View Registry setting.
0
```

Additionally, by default, only connections from the newest Remote Desktop Protocol (RDP) clients that support the Credential Security Service Provider (CredSSP) are accepted, which allows the user's current credentials to be automatically passed to the target server. However, you can change this behavior using the /CS 0 switch with scregedit.wsf.

Configuring Hardware

Some things, such as screen resolution, are difficult to configure from Server Core. One of the few GUI tools provided is the Registry Editor, which means you can perform configurations; it's just a bit ugly. Normally, you are advised to use the Registry Editor only as a last resort, but for some things in Server Core it's your only option. Using the Registry Editor, navigate to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Video\<GUID of graphics card>\0000 key. Modify the DefaultSettings.XResolution (see Figure 14-11) and DefaultSettings.YResolution values to the desired values. Just make sure they are right.

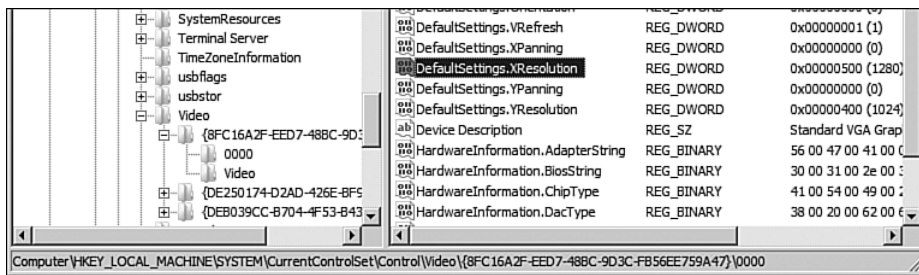


FIGURE 14-11 Setting the screen resolution for the system.

If you want to modify screen saver values, for example, do it in the Registry as well. By default, the screen saver kicks in after 10 minutes and uses the logon screen saver (logon.scr), requiring a password when the

screen saver is deactivated. To modify this, use the Registry Editor again and move to the `HKEY_CURRENT_USER\Control Panel\Desktop` key. The following values can be changed:

- **ScreenSaveActive.** 1 means screen saver is turned on, 0 disables.
- **ScreenSaverIsSecure.** 1 means password is required, 0 no password needed.
- **ScreenSaveTimeOut.** Time in seconds of inactivity before screen-saver starts.
- **SCRNSAVE.EXE.** The name of the screen saver. `Logon.scr` or `scrnsave.scr` for the blank screen saver.

You can also specify a background wallpaper by creating a string value named `WallPaper` under the same key with the full name and path of the image to use as the background.

In terms of adding hardware, if you need to install drivers, you are not prompted to install a driver for new hardware as in a normal Windows Server installation. Instead you need to manually install the driver and then, depending on the hardware, reboot the server for the new driver to be used with the hardware. Copy the driver files to a location on the server and then run the following command to load the driver:

```
Pnputil -i -a <driver>.inf
```

You can list all drivers on the system via the `sc query type=driver` command (note the space between `type=` and `driver`). When you have the service name of the driver, uninstall with the `sc delete <service_name>` command.

Adding Roles and Features

So far everything you have done configures the server. So far it does not do anything; it's not running any roles or features that are the cornerstone of Windows Server 2008.

You don't have access to the normal Server Manager interface to add roles and features, and all the features, except ADDS, are added via the

`Ocsetup` command. `Ocsetup` is a case-sensitive command and is part of all Windows Server 2008 installations. Active Directory installation is installed via the `dcpromo` command, which installs the binaries and configures things via an unattended answer file. You can't use DCPROMO GUI. You have to use an unattended answer file or command-line switches. See the Active Directory chapters for examples of unattended Active Directory installations.

To uninstall roles and features, use the same command but add `/uninstall` at the end. The exception again is ADDS, which once again uses DCPROMO.

Tables 14-2 and 14-3 list the names of the components and what they correspond to in features and roles. However, you can run `oclist` for a complete list; `oclist` is a Server Core-specific command. New roles and features will be added to Server Core in the future. For example, WDS support is expected in the Windows Server 2008 R2 timeframe.

Table 14-2 Server Roles and `Ocsetup` Names

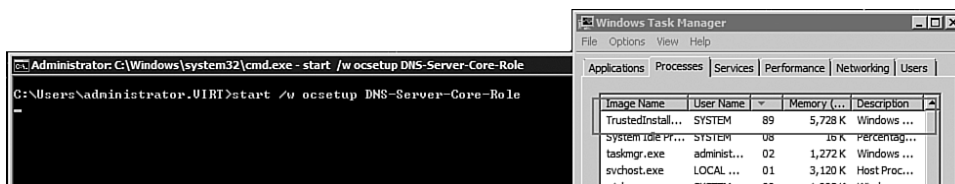
Server Role	Ocsetup Name
Active Directory Lightweight Directory Services (ADAM)	DirectoryServices-ADAM-ServerCore
DHCP	DHCPServerCore
DNS	DNS-Server-Core-Role
Distributed File System Service	DFSN-Server
Distributed File System Replication (DFSR)	DFSR-Infrastructure-ServerEdition
File Services	File-Server-Core-Role
File Replication Service (FRS)	FRS-Infrastructure
IIS (no ASP.NET)	IIS-WebServerRole (plus subcomponents visible via <code>oclist</code>)
Network File System (NFS)	ServerForNFS-Base
Media Server	MediaServer
Hyper-V	Microsoft-Hyper-V

Table 14-3 Server Features and Ocsetup Names

Server Feature	Ocsetup Name
Backup	WindowsServerBackup
BitLocker Drive Encryption	BitLocker
BitLocker Remote Admin Tool	BitLocker-RemoteAdminTool
Failover Cluster	FailoverCluster-Core
Multipath IO	Microsoft-Windows-MultipathIO
NFS Client	ClientForNFS-Base
Network Load Balancing	NetworkLoadBalancingHeadlessServer
Quality of Service	QWAVE
Removable Storage Management	Microsoft-Windows-RemovableStorageManagementCore
SNMP	SNMP-SC
Subsystem for UNIX-bases applications	SUACore
Telnet Client	TelnetClient
Windows Activation Service (WAS)	WAS-WindowsActivationService
WINS	WINS-SC

By default, if you execute Ocsetup with a package to install, the command prompt returns instantly while the installation happens in the background, and you will not know when the install has completed. To work around this, run the Ocsetup command after a `start /w` to tell the command to execute and to wait for the execution to complete.

Let's install the DNS Server role, as shown in Figure 14-12. During the install, the TrustedInstaller process is activated and responsible for the actual installation.

**FIGURE 14-12** Installing a role is a one-step process.

After you install the role, it is marked as installed in the Optional Component listing, as shown in the following:

```
C:\Users\administrator.VIRT>oclist
```

Use the listed update names with Ocsetup.exe to install/uninstall a server role or optional feature.

Adding or removing the Active Directory role with OCSetup.exe is not supported.

It can leave your server in an unstable state. Always use DCPromo to install or uninstall Active Directory.

```
=====
Microsoft-Windows-ServerCore-Package
Not Installed:BitLocker
Not Installed:BitLocker-RemoteAdminTool
Not Installed:ClientForNFS-Base
Not Installed:DFSN-Server
Not Installed:DFSR-Infrastructure-ServerEdition
Not Installed:DHCPServerCore
Not Installed:DirectoryServices-ADAM-ServerCore
Not Installed:DirectoryServices-DomainController-ServerFounda-
tion
Installed:DNS-Server-Core-Role
Not Installed:FailoverCluster-Core
Not Installed:FRS-Infrastructure
```

In the DNS case, the service could be managed locally via DNSCMD, which is a standard part of the DNS role to facilitate command-line management, or more likely you can run the DNS MMC snap-in on a Vista/2008 box and remotely connect and manage the DNS service on the core installation. For example, in Figure 14-13, the root of the DNS navigation node is right-clicked and the Server Core installation is added, which you can now manage with the GUI remotely.

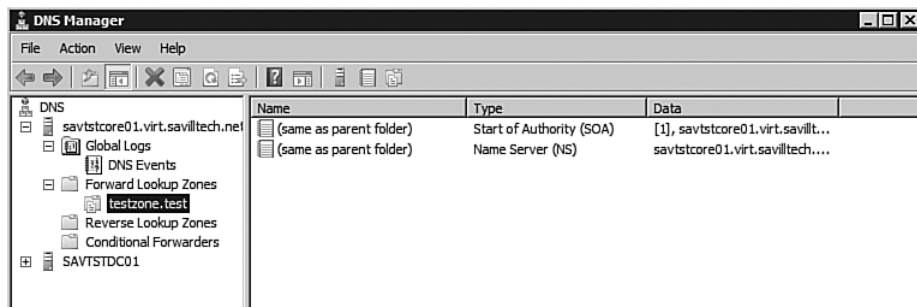


FIGURE 14-13 In reality, you remotely control most of the server core areas of functionality.

As with all the remote GUI tools, if you receive an Access Denied error, solve it by performing a `net use` to the machine before remotely connecting. The command establishes an authenticated session:

```
C:\Users\john>net use * \\savgstcore01.virt.savilltech.net\c$
➔/user:virt\administrator *
Type the password for \\savgstcore01.virt.savilltech.net\c$:
*****
Drive Z: is now connected to
\\savgstcore01.virt.savilltech.net\c$.
```

The command completed successfully.

A better way is to use `cmdkey`, which allows credentials to be set for various target systems:

```
C:\Users\john>cmdkey /add:savgstcore01.virt.savilltech.net
➔/user:virt\administrator /pass:*****
```

CMDKEY: Credential added successfully.

Installing Applications

For the Windows Server 2008 release, Server Core is designed to run in-the-box functions, that is, the supported server roles and features and not additional applications.

None of the major products are supported on Server Core; for example, Exchange, SharePoint, SQL, and so on. For additional applications, there is some planning for the future when managed code support is added to Server Core. However, there are limits to what can be added to Server Core; otherwise, it becomes a normal Windows installation.

Agents should be installable and supportable under Server Core, for example, backup agents, Microsoft Operations Manager (MOM), Systems Management Server (SMS) agents, and so on, which are managed via a remote administrative console function. You can install antivirus agents on Server Core installations and manage them remotely. For example, ForeFront runs on Server Core. Virtual machine additions can be installed and they run fine; in fact, they are recommended. The general rule of thumb is that agents have no shell or GUI dependencies and do not require managed code; if all these are true, the agent runs under Server Core.

To install additional software, execute the setup executables or manually install the MSI files using this command:

```
Msiexec /i <application>.msi
```

To check the installed applications, use the `wmic` command and the production function as shown in the following:

```
C:\Windows\System32>wmic
wmic:root\cli>product
AssignmentType  Caption                                Description
1               Virtual Machine Additions             Virtual Machine
Additions
```

This output is long, so you need to scroll to see everything.

To uninstall an application, use the `wmic` command by checking the name of the application and then calling `uninstall` for it, for example:

```
C:\Windows\System32>wmic product get name /value
Name=Virtual Machine Additions

C:\Windows\System32>wmic product where name="Virtual Machine
Additions" call uninstall
```

In the short term, the only installations you do will likely be agents and antivirus, but who knows what the future will bring?

Performing Common Actions Using Server Core

One quick way to get information about your environment is with the `systeminfo` command, as shown executing in the following listing:

```
C:\Windows\System32>systeminfo.exe
```

```
Host Name:                SAVTSTCORE01
OS Name:                  Microsoft Windows Server 2008
Enterprise
OS Version:              6.0.6001 Service Pack 1, v.222 Build
6001
OS Manufacturer:        Microsoft Corporation
OS Configuration:       Member Server
OS Build Type:           Multiprocessor Free
Registered Owner:        Windows User
Registered Organization:
Product ID:               78440-034-0066664-70918
Original Install Date:   9/4/2007, 4:05:28 PM
System Boot Time:        9/9/2007, 6:46:54 PM
System Manufacturer:     Microsoft Corporation
System Model:             Virtual Machine
System Type:             X86-based PC
Processor(s):             1 Processor(s) Installed.
                          [01]: x86 Family 6 Model 15 Stepping
6 GenuineIntel ~
4 Mhz
BIOS Version:             American Megatrends Inc. 080002 ,
2/22/2006
Windows Directory:       C:\Windows
System Directory:        C:\Windows\system32
Boot Device:             \Device\HarddiskVolume1
System Locale:            en-us;English (United States)
Input Locale:            en-us;English (United States)
Time Zone:               (GMT-06:00) Central Time (US &
Canada)
Total Physical Memory:    1,023 MB
Available Physical Memory: 778 MB
Page File: Max Size:     2,299 MB
Page File: Available:    2,092 MB
Page File: In Use:       207 MB
```

```
Page File Location(s):      C:\pagefile.sys
Domain:                     virt.savilltech.net
Logon Server:               \\SAVTSTDC01
Hotfix(s):                  N/A
Network Card(s):            N/A
```

One item many users struggle with is no system clock, which they get used to in the System Tray. You can update your prompt to include the time with the following prompt command:

```
C:\Windows\System32>prompt [%T] $S$P$G
```

```
[10:50:03.26] C:\Windows\System32>
```

```
[10:50:04.50] C:\Windows\System32>
```

What else do you normally use on a system? The Task Manager. Its keyboard shortcut still works in Server Core, so press Ctrl+Shift+Esc to open the Windows Task Manager or access it via the Windows Security Dialog by pressing Ctrl+Alt+Del. There is no Windows Task Manager help, however, because the help is based on HTML, which is not included in the Server Core.

What about rebooting, shutting down, and logging off? You can access the Windows Security dialog and elect to shut down or reboot, or you can use the Windows standard shutdown command. The key switches you use are as follows, but you can find full information by running `shutdown /?`.

- /s. Shutdown.
- /r. Reboot.
- /t 0. Wait 0 seconds to perform the action.
- /a. Abort a shutdown. This is usable only if you had a time other than 0, so you can type before the reboot/shutdown occurs.

For example, to reboot the computer immediately, use this command:

```
Shutdown /r /t 0
```

To log out, you can use the `logoff` command-line utility or the Windows Security dialog.

From a utility perspective, both Notepad and Regedit are included in Server Core, RegEdit because you need it and Notepad because customers demanded it. However, neither has help because the help has

dependencies on HTML. As noted previously, HTML is not included. However, the basic Copy, Paste, Find, and other commands all function. The Open and Save dialogs might look familiar, but not in a good way (see Figure 14-14).

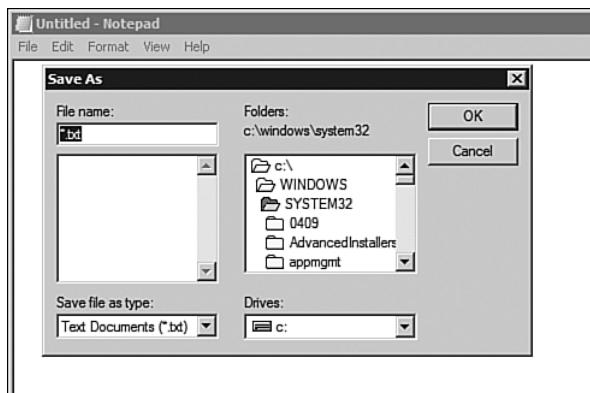


FIGURE 14-14 The days before the new operating system dialogs.

Remotely Managing Server Core

You have seen that you can use the command line for many configuration items, and nearly all Windows components come with command-line tools for management. So, you could manage Server Core locally. However, that is far from ideal, and you turned on the remote admin mode of Terminal Services so that you could remote to the box and access Server Core as if logged on locally. You have also seen how the MMC snap-ins can run on other computers and remotely manage the services on a Server Core installation. For example, the DNS MMC snap-in is probably the most-used remote management method. There are other options which give you the ability to remotely run commands on the Server Core installation—thanks to the inclusion of RPC and DCOM on Server Core, which facilitate the remote administration. Remember to enable the RemoteManage firewall rule.

Three of the MMC snap-ins require additional configuration on the Server Core installation:

- For Device Manager, enable the PnP policy. Even when enabled, Device Manager runs in a read-only mode, which is useful for checking hardware and device driver info. Load the local policy on the Server Core box (or create a Group Policy Object [GPO] that applies to Server Core) and enable the Allow Remote Access to the PnP Interface policy under Computer Configuration, Administrative Templates, System, Device Installation and reboot the Server Core computer, as shown in Figure 14-15.
- The Disk Management MMC snap-in requires two changes. Enable a firewall group on the server core installation and on the machine performing the remote management:


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

 In addition, run the Virtual Disk Service via this command:


```
net start VDS
```
- Enable Remote IPsec Monitor management using the SCRegEdit.wsf script:

```
C:\Windows\System32> cscript scregedit.wsf /IM 1
```

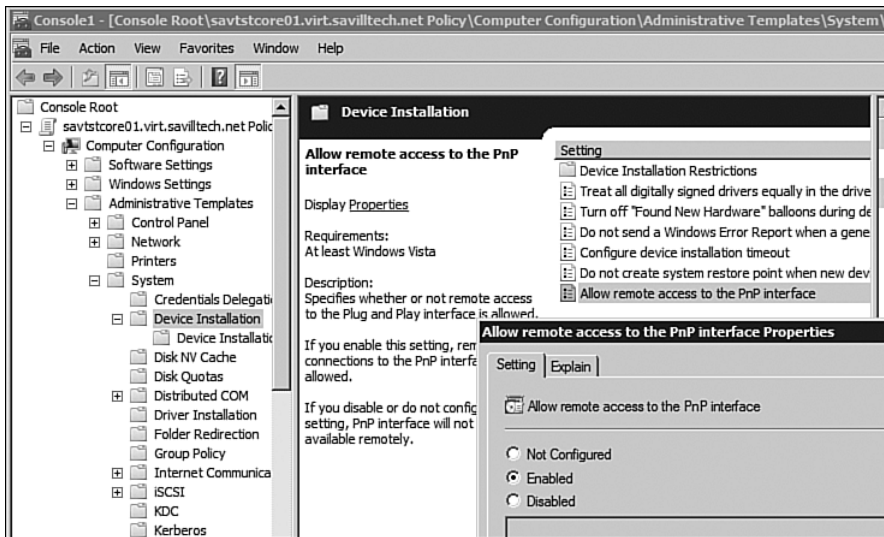


FIGURE 14-15 Enable the Allow Remote Access to the PnP Interface policy.

Another command-line option is the WS-Management and Windows Remote Shell. However, this runs the command, remotely catches the output, and sends it back. The advantage of WS-Management is that it operates over HyperText Transfer Protocol (HTTP) or HyperText Transfer Protocol over Secure Sockets Layer (HTTPS), so there are no additional port requirements for WS-Management to function because the HTTP ports are normally open by default. However, you can change this port if required.

When you enable WS-Management on the server using the quick configuration, the best security method available to the installation is used. For example, on a domain-joined machine, Kerberos is selected. Run the `winrm quickconfig` command as shown in the following listing:

```
C:\Users\administrator.VIRT>winrm quickconfig
WinRM is not set up to allow remote access to this machine for
management.
The following changes must be made:

Create a WinRM listener on HTTP://* to accept WS-Man requests
to any IP on this machine.
Enable the WinRM firewall exception.

Make these changes [y/n]? y

WinRM has been updated for remote management.

Created a WinRM listener on HTTP://* to accept WS-Man requests
to any IP on this machine.
WinRM firewall exception enabled.
```

This can be configured via Group Policy through Computer Configuration, Administrative Templates, Windows Components, Windows Remote Management, WinRM Service and enabling Allow Automatic Configuration of Listeners. There are other options in the same policy location regarding the use of Kerberos/Basic authentication.

On the client side, use the `WinRS` command in the following format:

```
WinRS -r:<remote system> command
```

For the remote system, type in the name of the remote computer or enter it in the form of a URL; for example, `http://ip address:port` or

<http://fqdn>; <http://192.168.1.232:80> or <http://savgstcore01.virt.savilltech.com>. By default, your existing credentials are used. Credentials are passed using the /domain, /userd and /password arguments. Some sample uses are shown in the following listing:

```
C:\Users\Administrator>winrs -r:savgstcore01 ipconfig
```

Windows IP Configuration

Ethernet adapter Local Area Connection:

```

Connection-specific DNS Suffix . . . :
Link-local IPv6 Address . . . . . :
fe80::c49a:b729:8c8b:471e%2
IPv4 Address. . . . . : 192.168.1.232
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

```

Tunnel adapter Local Area Connection*:

```

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . :

```

Tunnel adapter Local Area Connection* 2:

```

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . :

```

```
C:\Users\Administrator>winrs -r:savgstcore01 cscript
```

```
➔c:\windows\system32\scregedit.wsf /AR /v
```

Microsoft (R) Windows Script Host Version 5.7

Copyright (C) Microsoft Corporation. All rights reserved.

System\CurrentControlSet\Control\Terminal Server

fDenyTSConnections

View Registry setting.

0

You can use the Task Scheduler as in a normal Windows installation, as items such as event logging/forwarding and performance counters, which

you can fully access via the Computer Management MMC running remotely, as shown in Figure 14-16. You can use the reliability interface against Server Core. Note that you can access both the Task Scheduler and Event Viewer through the Computer Management MMC snap-in. You have full access to the local users and groups. (Although you could use the `net user` and `net localgroup` commands to perform user/group management locally.)

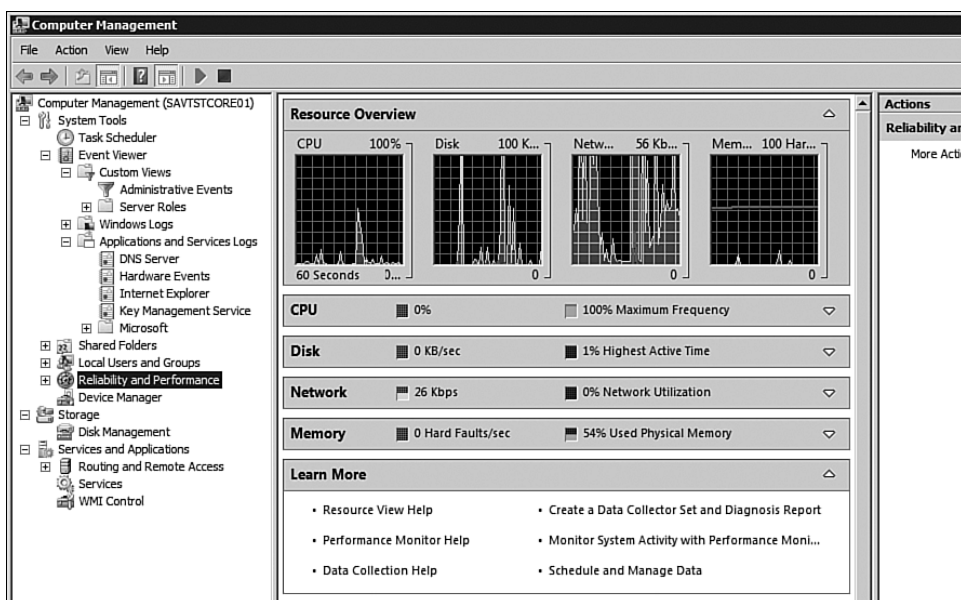


FIGURE 14-16 The remote capabilities of RPC and DCOM give the GUI-less Server Core a great remote GUI experience.

If you want to view the event log locally on a Server Core installation, use the `Wevtutil.exe` command. For example, to view the five most recent event logs in text format from the `SYSTEM` log, use the following command:

```
C:\Windows\System32>wevtutil qe system /rd:true /c:5 /f:text
Event[0]:
  Log Name: System
  Source: Virtual Disk Service
  Date: 2007-09-09T19:04:09.000
```

```
Event ID: 4
Task: N/A
Level: Information
Opcode: N/A
Keyword: Classic
User: N/A
User Name: N/A
Computer: savtstcore01.virt.savilltech.net
Description:
Service stopped.
```

You can also search for specific event IDs. For example, to search for reboots, which are event ID 1074, use the following command:

```
wevtutil ql system /q:*[System[(EventID=1074)]] /f:text
```

SNMP can be enabled on Server Core to allow management by your management tools if they are SNMP-based. SNMP is enabled by installing the SNMP feature. Both SNMPv1 and SNMPv2c are supported. Normal WMI scripting can be used both locally and, more likely, from a remote station.

Let's look back at the Remote Desktop option. Maybe you want a remote command prompt without a full session. With the new application publishing features of Windows Server 2008, you can publish a command prompt by performing the following actions.

You need to use the Terminal Services (TS) RemoteApp Manager, which is available on a full Windows 2008 installation with the Terminal Server Role installed. So, on a full Windows Server installation, add the Terminal Server role. Notice you need Terminal Server only because you want access to the RemoteApp Manager. Alternatively, you can add the Remote Server Administration Tools feature and select only the Terminal Server Tools option if you don't want to install the Terminal Server role on any server, as shown in Figure 14-17. This latter option avoids installing TS and allows configuration from any platform supporting Remote Server Administration Tools; for example, Windows Vista.

After the TS RemoteApp Manager is running, change the server that the client connects to so that the Server Core machine is selected via the Connect to Computer option in the Action menu of the Actions pane. In the Actions pane, click the Add RemoteApp Programs link, which starts the RemoteApp Wizard (covered in detail in Chapter 9, "Terminal Services"). After clicking Next at the Introduction screen of the wizard, a

list of programs that can be published is displayed. Click the Browse button, navigate to the Windows\System32 folder, and select cmd.exe. Click Next, as shown in Figure 14-18, and then click Finish.

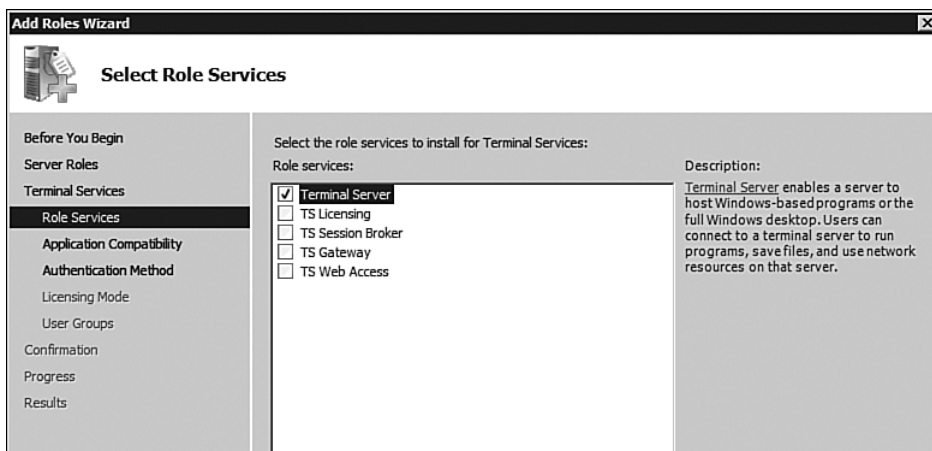


FIGURE 14-17 Adding the Terminal Server role to a server. There's no need for the other components.

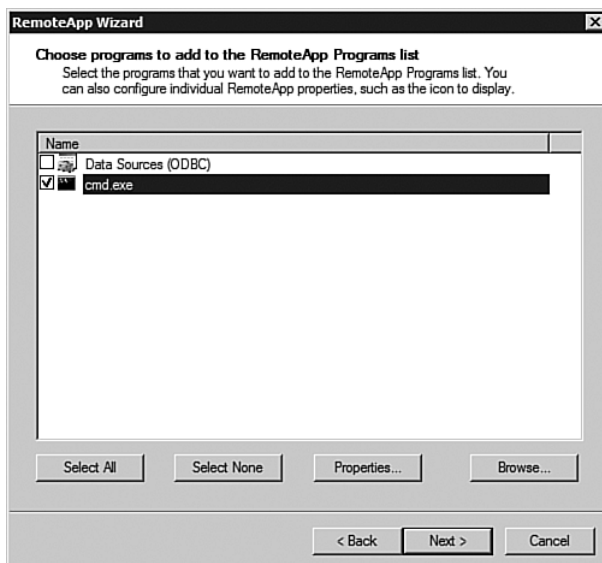


FIGURE 14-18 Publishing the cmd.exe application.

Finally, as shown in Figure 14-19, click the Create .rdp File link. Figure 14-19 shows the options for connecting to a computer and starting the Add RemoteApp Program Wizard.

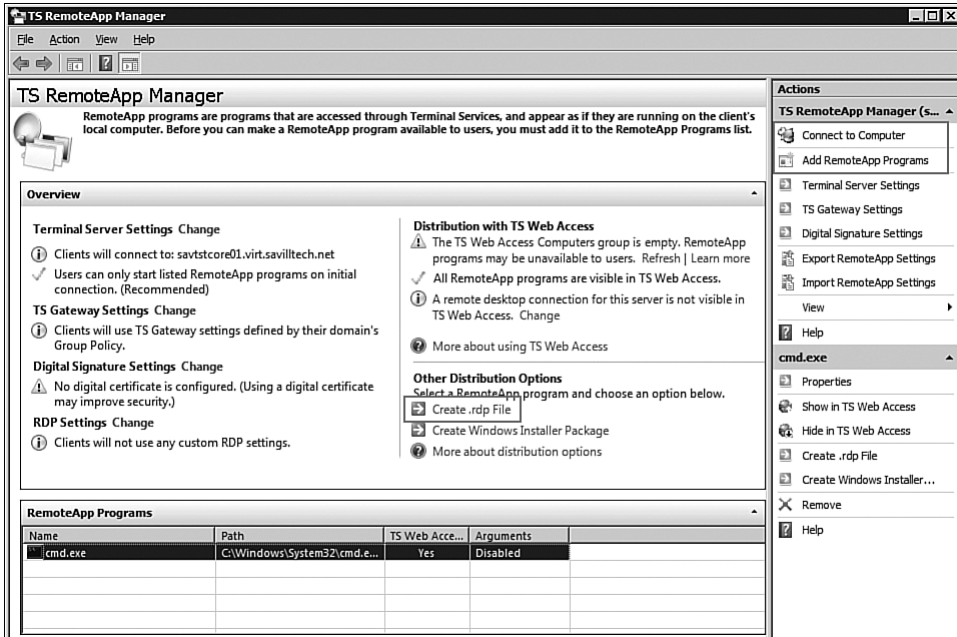


FIGURE 14-19 Creating a published application RDP for the cmd prompt.

You can take the generated RDP file and run it from any Vista/Windows Server 2008 client to open a seamless command window that is running on the Server Core installation. The following listing shows the content of the generated RDP that can be modified with an updated server name:

```
disableclipboardredirection:i:0
redirectposdevices:i:0
redirectprinters:i:1
redirectcomports:i:1
redirectsmartcards:i:1
devicestoredirect:s:*
drivestoredirect:s:*
redirectdrives:i:1
```

```
session bpp:i:32
span monitors:i:1
remoteapplicationmode:i:1
server port:i:3389
allow font smoothing:i:1
promptcredentialonce:i:0
authentication level:i:0
gatewayusagemethod:i:2
gatewayprofileusagemethod:i:0
gatewaycredentialssource:i:0
full address:s:savtstcore01.virt.savilltech.net
alternate shell:s:|cmd
gatewayhostname:s:
remoteapplicationname:s:cmd.exe
remoteapplicationcmdline:s:
screen mode id:i:2
winposstr:s:0,1,424,117,835,356
compression:i:1
smart sizing:i:1
keyboardhook:i:2
audiomode:i:0
redirectclipboard:i:1
displayconnectionbar:i:1
autoreconnection enabled:i:1
prompt for credentials:i:0
negotiate security layer:i:1
remoteapplicationicon:s:
shell working directory:s:
disable wallpaper:i:1
disable full window drag:i:1
allow desktop composition:i:0
disable menu anims:i:1
disable themes:i:0
disable cursor setting:i:0
bitmapcachepersistenable:i:1
```

When using a terminal server connection with the Terminal Server Client (mstsc), ensure that disk drives are available from the client machine by selecting the drives as available under the Local Resources tab (you have to click the More button) or as an option, as shown in Figure 14-20. The local client drives are accessible as \\tsclient\\<drive> on the remote system. You can then map to these drives to get full access as in the following example:

```
C:\Windows\System32>net use * \\tsclient\d
Drive Y: is now connected to \\tsclient\d.
```

The command completed successfully.

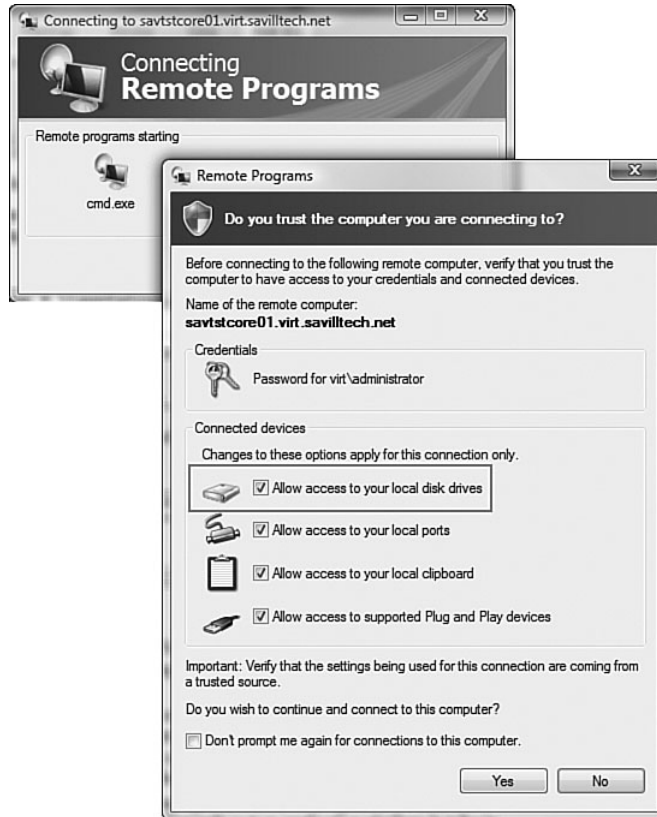


FIGURE 14-20 The Remote Programs client gives easy access to controlling the local resource access.

Summary

Server Core is a great addition to the Windows Server family. If the estimate of Server Core needing only one-third the patches required by a full Windows installation is accurate, Server Core will be much easier to manage. Resource usage is lower, with around two-thirds of the normal number of services both installed and running.

So far the top uses for Server Core are expected to be domain controllers (and Server Core also supports Read Only Domain Controllers [RODC]) making it ideal for branch office locations, IIS Web servers, and file/print servers.

The installation process for Server Core is the same as for a full installation, and you can use the same automated installation methods as for a full installation. To configure and manage a core installation, use a slightly different process than you use for a full installation, even though many of the methods you use for Server Core can be used on a full server installation. The command-line options in Server Core give you the ability to perform nearly all functions, and where they fall short you can remotely manage your server. But remember that Server Core is still a Windows installation. All the normal command-line tools and scripting capabilities are available, so just because this chapter didn't cover it does not mean it's not an option. For example, the `tasklist` command is great for seeing the processes running on the system, and `taskkill` is great for stopping them!

If you want a lower overhead Windows installation, Server Core might be the answer.

INDEX

Symbols

- : (colons) in variable
 - names, PowerShell response to, 1543
- 32-bit architectures, OS images for, 1043
- 64-bit architectures, OS images for, 1043
- 1231 error codes (NAP), 515

A

- ABE (access-based enumeration), 981
- access
 - access tokens, 1333
 - to NLB (Network Load Balancing) clusters, 1219-1220
 - UAC (User Access Control) administrator accounts, 50-52
 - benefits of, 50
 - elevation of privilege, 52-56
- Account is Disabled option (Active Directory Users and Computers MMC snap-in), 790
- Account Lockout Policy, 220-221
- Account tab (user objects), 790
 - Account Options area, 792
 - Logon Hours option, 791
 - Unlock Account option, 792
- accounting, WSRM (Windows System Resource Manager), 1327-1328
- accounts
 - administrator accounts, 50-52
 - computer accounts, 1036-1038
 - elevation of privilege, 52-56
 - locked out accounts, unlocking, 222
 - policies
 - Account Lockout Policy, 220-221
 - Kerberos Policy, 221-222
 - Password Policy, 219-220
- ACID (atomic, consistent, isolated, and durable) test, 228
- actions, triggering in response to disk quotas, 274
 - commands, 278-279
 - e-mail messages, 275-276
 - event logs, 277
 - reports, 279
- Actions pane (MMC), 90
- activating
 - servers in Server Core, 926-927
- Windows Server 2008
 - KMS, 120-122
 - MAK, 120-122
 - MSDN keys, 117
- Windows Vista,
 - reduced-functionality mode, 1078-1079
- Active Directory. *See* AD
- Active Directory Application Mode (ADAM). *See* AD LDS (Active Directory Lightweight Directory Services)
- Active Directory Certificate Services. *See* ADCS
- Active Directory Domain Services. *See* ADDS
- Active Directory Domain Services (ADDS) Installation Wizard, 639-651, 719
- Active Directory Federation Services. *See* AD FS
- Active Directory Lightweight Directory Services. *See* AD LDS
- Active Directory Rights Management Services. *See* AD RMS
- Active Directory Services Interface (ADSI), 636, 1529
- Active Directory Sites and Services MMC snap-in, 859
- Active Directory Users and Computers MMC snap-in, 799
- Account is Disabled option, 790
- computer objects, 802-804
 - Delegation tab, 803
 - General tab, 802

- Member Of tab, 803
- Operating System tab, 803
- contacts, 802
- Environment tab, 612
- OU
 - configuring, 781
 - creating, 780
 - delegating permissions, 782, 785-787
 - deleting, 782
 - naming, 780
 - nesting, 780
- Password Never Expires
 - option, 790
- Remote Control tab, 613
- Sessions tab, 612
- Terminal Services Profile tab, 613
- User Cannot Change
 - Password option, 789
- user groups
 - Attribute Editor tab, 801
 - creating, 799
 - distribution groups, 797
 - domain local groups, 797-799
 - global groups, 797
 - Managed By tab, 800
 - Member Of tab, 800
 - Members tab, 799
 - removing users from, 801
 - scope of, 798
 - security groups, 797
 - Security tab, 800
 - universal groups, 797-799
- User Must Change
 - Password at Next Logon option, 788
- user objects
 - Account tab, 790-791
 - Address tab, 790
 - COM+ tab, 794
 - General tab, 790
 - Member Of tab, 794
 - Organization tab, 794

- Profile tab, 792-793
- Telephones tab, 793
- active-active clusters, 1207
- active file screens, 285
- active-passive clusters, 1207
- Active X components, 597
- AD (Active Directory), 623
 - Active Directory Users and Computers MMC snap-in, 779
 - Account is Disabled
 - option, 790
 - computer objects, 802-804
 - configuring OU, 781
 - contacts, 802
 - creating OU, 780
 - delegating OU permissions, 782, 785-787
 - deleting OU, 782
 - Environment tab, 612
 - naming OU, 780
 - nesting OU, 780
 - Password Never Expires
 - option, 790
 - Remote Control tab, 613
 - Sessions tab, 612
 - Terminal Services Profile tab, 613
 - User Cannot Change
 - Password option, 789
 - user groups, 797-800
 - User Must Change
 - Password at Next Logon option, 788
 - user objects, 790-794
- AD FS, 891
 - authentication, 894
 - claim mappings, 903
 - claims-aware agent
 - installation, 897
 - FS, 892
 - FS-P, 893
 - installing, 895-906
 - operational overview, 893-895

- troubleshooting, 907-908
- Web Server SSO
 - Agent, 893
- AD LDS, 852-865
 - AD partition creation, 857
 - AD Sites and Services
 - MMC snap-in, 859
 - installing, 855
 - instance backups, 863
 - instance connections, 862
 - instance creation, 855, 859
 - instance management, 854
 - instance names, 856
 - instance removal, 863
 - instance restoration, 863
 - LDAP, 854-856
 - replication in, 860-861
 - SSL port
 - customization, 856
 - usage example, 853
- AD RMS, 865-891
 - CLC, 867
 - document access, 866
 - installing, 869-873
 - licensing, 887-890
 - operational overview, 875
 - RAC, 867
 - Reports node, 888
 - restricting access
 - via, 877-881
 - SQL database
 - backups, 889
 - Super User groups, 890
 - template access,
 - enabling, 885-886
 - template creation, 882-884
- ADCS (Active Directory Certificate Services), 156, 1102
- CA, 158-163
- certificate templates,
 - 164, 168
- installing, 158
- Network Device
 - Enrollment Service, 159

- Online Responder, 159
 - private key
 - cryptography, 159
 - stand-alone CA, 158
- ADDS (Active Directory Domain Services), 114, 1102, 1209
 - ADDS Installation Wizard, 639-651
 - DNS, 427
 - starting/stopping, 827
- Advanced Tools, 1099-1101
- auditing, 829-830, 834
- backups
 - deleted object
 - recovery, 825
 - Last Interactive Logon Information feature, 819-821
 - restartable directory service, 826-829
 - snapshots, 822-825
 - Windows Backup, 812-814
- command line, managing
 - from, 804-811
- DFSR, FRS migration to
 - for SYSVOL replication, 843-848
- discussed, 632
- DIT (directory information tree), 633
- DNS (domain name system), 636-637
- domain controllers
 - adding, 679-683
 - creating from
 - media, 715-718
 - demoting, 767, 770-776
 - FSMO roles, 679
 - moving, 707
 - RDOCs. *See* RDOCs (read-only domain controllers)
 - removing, 719-722
 - unattended installation, 683-684
 - verifying operation
 - of, 705-715
- domain modes
 - mixed mode, 672
 - Windows 2000 native mode, 672
 - Windows Server 2003 interim native mode, 673
 - Windows Server 2003 native mode, 673
 - Windows Server 2008 native mode, 673-674
- domains
 - BDC (backup domain controller), 625
 - creating, 639-651, 698-704
 - DNS delegation, 704-705
 - DNS names, 639
 - NetBIOS names, 628, 639
 - PDC (primary domain controller), 624
 - removing, 719-722
 - versus workgroups, 623-627
 - Windows OS domain compatibility, 627-630
- eDirectory
 - synchronization, 1594
- File Migration Utility, 1603-1604, 1607
- forest modes, 674-677
 - Windows 2000 mode, 675
 - Windows Server 2003 interim mode, 675
 - Windows Server 2003 mode, 675-676
 - Windows Server 2008 mode, 676-677
- forests, 653-656
- FRS, DFSR migration
 - for SYSVOL replication, 843-848
- FSMO (Flexible Single Master Operation) roles
 - best practices, 685-686
 - domain naming master
 - FSMO roles, 669-670, 687
 - GC (Global Catalog)
 - setting, 694,-698
 - infrastructure FSMO roles, 668, 686
 - moving from command line, 691-692
 - PDC emulator FSMO roles, 666-667, 686
 - potential problems, 686-687
 - RID master FSMO roles, 667, 686
 - schema master FSMO roles, 668, 687
 - seizing, 693-694
 - transferring graphically, 687-691
- GC (global catalog), 670-671
- LDAP (Lightweight Directory Access Protocol), 635
- listing printers in, 307-309
- management tools,
 - accessing, 778
- mapping, 1575
- MSDSS replication, 1597, 1602
- NDS synchronization, 1594
- NIS migration, 1581
- OUs (organizational units), 656-657
- passwords, 834-835
- prestaging computers in, 1029-1030
- prune and graft
 - functionality, 836
- replication
 - full replication, 626
 - partial replication, 627
 - urgent replication, 627

- restoring
 - authoritative restores, 814, 817
 - DFSR, 817
 - DSRM, 815
 - nonauthoritative restores, 814
 - NTFRS, 817
- schemas, 637-638
- site connectivity,
 - customizing, 657-666, 753
 - ADLB tool, 765
 - core site link attributes, 755-757
 - redundant connection mode, 766
 - site topology management, 758-764
- trees, 651-652
- trust relationships
 - discussed, 740-743
 - external trust, 747
 - forest trust, 744-745
 - managing, 747-751
 - parent-child trust, 743
 - realm trust, 747
 - shortcut trust, 745-746
 - tree-root trust, 744
- trusts
 - benefits of, 630-632
 - definition, 630
 - upgrading, 836-843
 - user objects, deleting, 815
 - X.500 model, 633-634
- AD FS (Active Directory Federated Services), 891, 1102
 - authentication, 894
 - claim mappings, 903
 - claims-aware agent installation, 897
 - FS, 892
 - FS-P, 893
 - installing, 895-906
 - operational overview, 893-895
 - troubleshooting, 907-908
 - Web Server SSO Agent, 893
- AD LDS (Active Directory Lightweight Directory Services), 852-865, 1103
 - AD Sites and Services MMC snap-in, 859
 - installing, 855
 - instances
 - backups, 863
 - connecting to, 862
 - creating, 855, 859
 - creating AD partitions, 857
 - managing, 854
 - naming, 856
 - removing, 863
 - restoring, 863
 - LDAP, 854-856
 - replication in, 860-861
 - Setup Wizard, 855
 - SSL ports, 856
 - troubleshooting, 861
 - usage example, 853
- AD RMS (Active Directory Rights Management Services), 865-868, 891, 1103
 - CLC, 867
 - documents, accessing, 866
 - installing, 869-873
 - licensing, 887-890
 - operational overview, 875
 - RAC, 867
 - Reports node, 888
 - restricting access via, 877-881
 - SQL database backups, 889
 - Super User groups, 890
 - templates
 - creating, 882-884
 - enabling client access, 885-886
- ADAM (Active Directory Application Mode). *See* AD LDS (Active Directory Lightweight Directory Services)
- ADCS (Active Directory Certificate Services), 156, 1102
 - CA
 - configuring domain client trust of, 160-161
 - enterprise CA, 158
 - managing, 162-163
 - stand-alone CA, 158
 - Web enrollment page, 159
 - certificate templates, 164, 168
 - installing, 158
 - Network Device Enrollment Service, 159
 - Online Responder, 159
 - private key cryptography, 159
- ADCS area (Server Manager) Certificate Templates MMC snap-in, 163
- Enterprise PKI (PKIView) MMC snap-in, 162
- Add Account Partner Wizard, 902
- Add Account Store Wizard, 899
- Add Features Wizard, 1117-1118
- Add Printer Wizard, 310-311
- Add Roles Wizard, 1107-1111
 - DHCP installation, 383
 - TS installation, 558
- Add/Remove Servers dialog, 293
- address bar (Windows Explorer), 79
- Address Leases leaf (Properties context menu, Advanced tab), 397

- Address Pool leaf (Properties context menu, Advanced tab), 397
- Address tab (user objects), 790
- addresses
 - IP addresses
 - automatic private IP addressing, 351-352
 - discussed, 29
 - gateway configuration, 349-350
 - global unicast addresses, 366
 - link-local addresses, 366
 - managing for NLB (Network Load Balancing), 1226
 - NAT (Network Address Translation), 352-355
 - setting, 345-349
 - site-local addresses, 367
 - unique local addresses, 367
 - MAC addresses, 337-339
- ADDS (Active Directory Domain Services), 114, 1102, 1209
- ADDS Installation Wizard, 639-651
- DNS, 427
- starting/stopping, 827
- ADLB (Active Directory Load Balancer) tool, 765
- Admin logs (Event Viewer), 1382
- Administration page (TS Web Access), 594
- Administrator accounts
 - authorization, 143
 - passwords
 - setting in Server Core, 920
 - Windows Server 2008 configurations, 109
 - when to use, 50-52
- ADMX files, customizing, 1480-1485
- adrestore command, 825
- ADS (Automated Deployment Services), 1015
- ADSI (Active Directory Scripting Interface), 636, 1529
- Advanced Group Policy Management (AGPM), 37, 1491
- Advanced Research Protocol Agency Network (ARPANET), 335
- Advanced tab
 - Properties menu, 301-303
 - Address Leases leaf, 397
 - Address Pool leaf, 397
 - Reservations leaf, 398
 - scope management, 396
 - RDC tool, 526, 543
- Advanced Tools (AD), 1099-1101
- advanced Windows Server 2008 installations, 130
- Aero effects, 67-70
- AGMP (Advanced Group Policy Management), 1491
- AH (Authentication Headers), 203
- aliases (PowerShell), 1544-1550
- allocating resources (WSRM), 1320-1326
- AllSigned script execution level (PowerShell), 1553
- Analytic logs (Event Viewer), 1382
- analyze feature (SCW), 185-186
- answer files
 - automated Windows Server 2008 installations, 133, 137-139
 - creating, 1050-1058
- antecedents, 1109
- Anytime Upgrade, 1016
- APIPA (Automatic Private IP addressing), 380
- appcmd utility, 1643-1645
- Appearance tab (Performance Monitor), 1363
- application data, recovering, 1168-1170
- Application logs (Event Viewer), 1382
- application partitions (DNS), 422-424
- Application Server, 1103
- applications
 - installing in Server Core, 938-939
 - in OS images, 1042
 - virtual applications
 - advantages of, 1272-1273, 1281-1283
 - application virtualization process, 1277-1278
 - caching, 1279
 - creating, 1276-1277
 - loading, 1279
 - memory use, 1280
 - patching, 1281
 - processor use, 1279
 - SoftGrid architecture, 1273-1276
- Applications and Services log area (Event Viewer), 1382
- Applications tab (Task Manager), 71-72
- AppStation Group Policy template, 1504
- architecture
 - of clusters, 1230-1232
 - of IIS (Internet Information Services) 7.0
 - configuring, 1619-1625
 - features and modules, 1612-1617

- IIS processing, 1617-1618
 - modules, 1616
- \$args arrays, 1554-1555, 1558
- arguments (VBScript), 1531
- arp command, 339
- ARPANET (Advanced
 - Research Protocol
 - Agency Network), 335
- ASP support (IIS), 1613
- ASP.NET support (IIS), 1613
- Asset Inventory Service, 37
- Assign Static IP Addresses
 - user property, 470
- assigned software, 1437
- assigning
 - disk quotas, 280-284
 - file screens to folders/
 - volumes, 285
- asynchronous application
 - (Group Policy),
 - 1421-1425
- AT command, 1124
- atomic, consistent, isolated,
 - and durable (ACID)
 - test, 228
- \$AttrDef file, 227
- Attribute Editor tab (user
 - groups), 801
- audits
 - AD, 829-830, 834
 - creating capture boot
 - images, 1067-1068
 - file screen audits, 265
 - SCW, 184
- authentication
 - AD FS, 894
 - basic authentication
 - (IIS), 1614
 - client certificate
 - mapping authentication
 - (IIS), 1615
 - digest authentication
 - (IIS), 1615
 - discussed, 32-33
 - domain methods,
 - configuring, 176-178

- IPsec, 207
- Kerberos, 173-176
- LDAP Authentication
 - servers, 1592
- NAP, 510
- NLA, 526-528
- NTLM, 172-173
- RADIUS, 482
- RRAS configuration, 463
- SCW, 183
- two-factor
 - authentication, 142
- VPN, 454, 463
- Windows authentication
 - (IIS), 1615
- Authentication Exemption
 - connection security
 - rule, 208
- authoritative DNS servers, 410
- authoritative restores, 814, 817
- authorization
 - administrator accounts, 143
 - best practices, 143
 - DHCP servers, 387
 - discussed, 32-33
 - TS Gateway
 - TS CAP, 570-571, 575
 - TS RAP, 572-575
 - unknown clients, 1030-1035
 - URL authorization,
 - 1634-1638
 - WDS, 1041
- auto-update, configuring in
 - Server Core, 927-928
- autocomplete feature
 - (CMD.EXE), 1516
- autoenrolling certificate
 - templates, 164, 168-170
- Automated Deployment
 - Services (ADS), 1015
- automated Windows Server
 - 2008 installations
 - answer files, 133, 137-139
 - autoattend.xml files,
 - 134-137

- OOBE, 137-138
- Windows Automated
 - Installation Kit, 133,
 - 138-139
- automatic image-based
 - deployment, 1049-1062
- automatic network print
 - addition, 326
- automatic private IP
 - addressing, 351-352
- automatic updates,
 - Windows Server 2008
 - configurations, 113
- AutoRun values (CMD.EXE),
 - 1510
- autoattend.xml files, 134-137

B

- b bar (RDC tool), 531
- B-node (Broadcast 0x1)
 - node type, 382
- Background Intelligent
 - Transfer Service (BITS)
 - Server Extensions, 1113
- backup domain controller
 - (BDC), 625
- backups
 - AD, 811
 - AD LDS instances, 863
 - deleted object
 - recovery, 825
 - Last Interactive Logon
 - Information feature,
 - 819-821
 - restartable directory
 - service, 826-829
 - snapshots, 822-825
 - Windows Backup, 812-814
 - data collector sets, 1375
 - distributed services, 956
 - Group Policy, 1487-1488
 - Last Interactive Logon
 - Information
 - feature, 819-821
 - RADIUS configurations, 486

- scopes (DHCP), 401
 - security, 144
 - snapshots
 - AD, 822-825
 - creating, 822-823
 - mounting, 823-825
 - SQL databases, 889
 - storing, 144
 - TS licensing, 557
 - with WSB (Windows Server Backup)
 - AD backups, 812-814
 - backup features, 1153-1156
 - discussed, 1152-1153
 - installing, 1158
 - recovery features, 1156-1158
 - scheduling backups, 1159-1160
 - single-time backups, 1161-1164
 - system state backups, 1164
 - bandwidth, Network-Current Bandwidth counter, 1364
 - \$BasClus file, 227
 - Base SDK option (SUA installations), 1570
 - Base Utilities option (SUA installations), 1570
 - basic authentication (IIS), 1614
 - Basic Task Wizard, 1127
 - batch files, CMD.EXE, 1528
 - BCD
 - BCDEdit (Boot Configuration Editor), 1353-1355
 - defining, 1349
 - troubleshooting, 1350
 - bcdedit /enum command, 1353
 - BDC (backup domain controller), 625
 - benchmarks (system), 1356
 - \$Bitmap file, 227
 - BitLocker, 144-147
 - command line, enabling from, 151-153
 - configuring, 149
 - Drive Encryption, 100-101, 149, 1113
 - Drive Encryption Control Panel applet, 149, 154
 - emergency recovery passwords, 154
 - FVEK, 145-146
 - manage-bde.wsf script, 149
 - turning off, 154
 - BITS (Background Intelligent Transfer Service) Server Extensions, 1113
 - blue screens of death (BSODs), 65
 - \$Boot file, 227
 - boot folders, 129
 - boot images
 - capture boot images, 1064-1074, 1077-1081
 - defined, 1044
 - Discover boot images, 1063-1064
 - installing, 1044-1045
 - boot menu (OS Loader)
 - accessing, 1335
 - Debugging Mode option, 1337
 - Directory Services Restore Mode option, 1337
 - Disable automatic restart on system failure option, 1337
 - Disable Driver Signature Enforcement option, 1337
 - Enable Boot Logging option, 1336
 - Enable low-resolution video (640-480) option, 1337
 - Last Known Good Configuration option, 1337
 - Repair Your Computer option, 1335
 - Safe Mode option, 1336
 - Safe Mode with Command Prompt option, 1336
 - Safe Mode with Networking option, 1336
 - Start Windows Normally option, 1337
 - boot process, 1039
 - boot programs, configuring for PXE clients, 1037
 - Boot Repair Your Computer option (Windows RE), 1346
 - Boot tab (MSConfig), 1400
 - bootrec command, 1349
 - bridgehead servers, 762-764
 - bridging site links, 760
 - BSODs (blue screens of death), 65
 - builtin containers, 779
- ## C
- /c <command> switches, 1510
 - C shells (SUA), 1572-1573
 - CA (Certificate Authorities), 156
 - certificate templates
 - autoenrollment, 164, 168-170
 - configuring, 165
 - converting, 163
 - issuing, 165-167
 - versions of, 163
 - certificates
 - manual certificate requests, 168
 - viewing, 169
 - domain client trust, 160-161
 - enterprise CA, 158
 - hierarchy of, 157-158
 - intermediate CA, 157
 - issuing CA, 157
 - names, changing, 159

- root CA, 156
- stand-alone CA, 158
- CA Web enrollment page (ADCS), 159
- cable modems (DHCP), 381
- caching
 - DNS, 443
 - universal group membership caching, 697-698
 - virtual applications, 1279
- Callback user property (RRAS), 469-470
- CAP (Connection Authorization Policy), 570-571, 575
- Capacity Planner (System Center), 1406
- capture boot images, 1064-1074, 1077-1081
- case sensitivity of UNIX, 1572
- catalogs
 - GC (global catalog), 670-671
 - Microsoft update catalog, 1181-1182
- CCR (Cluster Continuous Replication), 1210
- central store (Group Policy), 1485-1487
- certificate requests (manual), 168
- certificate templates
 - autoenrollment, 164, 168-170
 - configuring, 165
 - converting, 163
 - issuing, 165-167
 - versions of, 163
- Certificate Templates MMC
 - snap-in (Server Manager, ADCS area), 163
- Certificate Templates node (Certificates MMC snap-in), 170
- certificates, 1645-1647
 - CA (Certificate Authorities), 156
 - domain client
 - trust, 160-161
 - enterprise CA, 158
 - hierarchy of, 157-158
 - intermediate CA, 157
 - issuing CA, 157
 - names, changing, 159
 - root CA, 156
 - stand-alone CA, 158
- certificate templates
 - autoenrollment, 164, 168-170
 - configuring, 165
 - converting, 163
 - issuing, 165-167
 - versions of, 163
- credential roaming, 170
- TS Gateway, 576-577
- Certificates MMC snap-in, 168
- Certificate Templates
 - node, 170
 - Failed Request node, 169
 - Pending Requests node, 170
- CGI support (IIS), 1613
- chkdsk command, 1352
- claim mappings (AD FS), 903
- claims-aware agent (AD FS), 897
- Class A network addresses, 340
- Class B network addresses, 341
- Class C network addresses, 341
- Class D network addresses, 341
- Class E network addresses, 341
- CLC (Client Licensor Certificates), 867
- Client Services for NetWare, 1594
- Client Settings tab (Terminal Services Configuration MMC snap-in), 615
- clients
 - authorizing unknown, 1030-1035
 - client certificate
 - mapping authentication (IIS), 1615
 - client fallback (DFSN), 963
 - client management
 - in remote environments, 955
 - client notification (NAP), 514
 - Client Services for NetWare, 1594
 - Group Policy client support, 1499-1500
 - Internet Printing Client, 1114
 - managing Windows Server from, 1202-1203
 - PXE clients. *See* PXE clients
 - Telnet Client, 1116
 - TFTP (Trivial File Transfer Protocol) Client, 1116
- Clipboard sharing (RDC tool), 531
- Cluster Continuous Replication (CCR), 1210
- CLUSTER.EXE command, 1264-1266
- clusters. *See also* NLB (Network Load Balancing)
 - accessing, 1219-1220
 - architecture, 1230-1232
 - CCR (Cluster Continuous Replication), 1210
 - cluster modes, 1226
 - configuring, 1215
 - creating, 1248-1249
 - failover clustering
 - active-active clusters, 1207
 - active-passive clusters, 1207

- cluster architecture,
 - 1230-1232
 - cluster creation,
 - 1248-1249
 - Cluster Events, 1262
 - cluster failover, 1255-1258
 - cluster permissions, 1263
 - cluster validation,
 - 1245-1247
 - command-line
 - management, 1264-1266
 - dependency reports, 1262
 - discussed, 1206-1208,
 - 1229-1230
 - file share witnesses, 1208
 - high-availability services
 - and applications,
 - 1251-1254
 - iSCSI Initiator
 - configuration,
 - 1243-1245
 - network adapter
 - configuration, 1250
 - network and security
 - enhancements,
 - 1236-1237
 - node management,
 - 1261-1262
 - quorum model
 - modification, 1259-1260
 - quorum modes, 1232-1235
 - quorums, 1208
 - supported hardware, 1
 - 237-1242
 - upgrading from Windows Server 2003, 1266-1268
- SCC (single copy cluster), 1210
- validating, 1245-1247
- CMAK (Connection Manager Administration Kit), 1113
- CMD.EXE, 1508
- AutoRun values, 1510
 - /c <command>
 - switches, 1510
 - command prompt window
 - changing font size in, 1511
 - Colors tab, 1513
 - customizing, 1511-1513
 - Discard Old Duplicates
 - option, 1511
 - finding commands in,
 - 1517-1518
 - Font tab, 1511
 - Insert mode option, 1511
 - Layout tab, 1513
 - Options tab, 1511
 - QuickEdit mode
 - option, 1511
 - starting/stopping
 - output in, 1511
 - /d switches, 1511
 - DOSKEY, 1514
 - echo %path%
 - command, 1518
 - environment variables,
 - 1519, 1522
 - external commands, 1517
 - Hello World messages, 1516
 - input/output, redirecting,
 - 1523-1525
 - internal commands, 1515
 - /k <command>
 - switches, 1511
 - multiple commands
 - batch files, 1528
 - chaining, 1525-1526
 - scrolling through files/
 - folders, 1516
 - set command, 1519, 1522
 - starting, 1510
 - where command, 1518
- cmdlets (command-lets), 1537-1540
- Get-ChildItem, 1544
 - get-itemproperty, 1547
 - get-process, 1550
 - get-psdrive, 1545
 - get-psprovider, 1549
 - get-service, 1552
 - Invoke-Expression, 1552
 - Set-ExecutionPolicy, 1553
 - set-itemproperty, 1547
 - Set-Location, 1545
 - start-service, 1552
 - stop-process, 1551
- CNAME records, 413
- Co-owner access level, 248
- cold boot attacks, 155
- colons (:) in variable names,
 - PowerShell response to, 1543
- Colors tab (CMD.EXE), 1513
- command bar (Windows Explorer), 81
- command line. *See also specific commands*
- AD management, 804-811
 - advanced Windows Server 2008 installations, 130
 - BitLocker, enabling, 151-153
- CMD.EXE, 1508
- AutoRun values, 1510
 - /c <command>
 - switches, 1510
 - command prompt window,
 - 1511-1518
 - /d switches, 1511
 - DOSKEY, 1514
 - echo %path%
 - command, 1518
 - environment variables,
 - 1519, 1522
 - external commands, 1517
 - Hello World
 - messages, 1516
 - input/output, redirecting,
 - 1523-1525
 - internal commands, 1515

- /k <command>
 - switches, 1511
- multiple commands,
 - 1525-1528
- scrolling through files/
 - folders, 1516
- set command, 1519, 1522
- starting, 1510
- where command, 1518
- command.com
 - starting, 1508
 - Windows Server
 - availability, 1509-1510
- configuring WDS from, 1028
- failover clustering,
 - 1264-1266
- Monad, 1507
- MS-DOS, 1508
- NLB (Network Load Balancing) logs,
 - 1227-1228
- opening, 130
- PowerShell, 1536
 - aliases, 1544-1550
 - cmdlets (command-lets),
 - 1537-1540
 - confirm option,
 - 1551-1552
 - error handling, 1559-1563
 - exit statements, 1557
 - functions, 1544-1545,
 - 1557-1558
 - Hello World
 - messages, 1552
 - installing, 1537
 - listing running processes
 - in, 1550
 - param statements,
 - 1555-1556
 - Run dialog, 1557
 - scripts, 1552-1558
 - stopping processes, 1551
 - stopping WMP, 1552
 - variables, 1540-1544
 - whatif option, 1551-1552

- Registry, 1190-1192
- Server Manager, 1141-1146
- Task Scheduler, 1133-1135
- TS management, 619
- user management, 796
- Windows Firewall
 - configuration, 200-201
- Windows RE, 1348
- WSB (Windows Server Backup), 1170-1172
- WSH, 1528
 - ADSI, 1529
 - forcing scripts to run in
 - particular hosts, 1530
 - Hello World messages,
 - 1529-1530
 - setting command host run
 - commands, 1530
 - switching between scripts
 - in, 1531
 - WMI, 1529
 - WMI calls via VBScript,
 - 1532-1536
- command prompt window
 - (CMD.EXE)
 - customizing
 - Colors tab, 1513
 - Discard Old Duplicates
 - option, 1511
 - Font tab, 1511
 - Insert mode option, 1511
 - Layout tab, 1513
 - Options tab, 1511
 - QuickEdit mode
 - option, 1511
 - finding commands in,
 - 1517-1518
 - font size, changing, 1511
 - starting/stopping output
 - in, 1511
- command.com
 - starting, 1508
 - Windows Server availability,
 - 1509-1510
- commands. *See*
 - specific commands*

- comments
 - PowerShell scripts, 1554
 - VBScript, 1531
- commit size (virtual
 - memory), 1360
- communication
 - communication testing
 - with Network and Sharing Center, 373-376
 - with pathping command,
 - 372-373
 - with ping utility, 368-371
 - with tracert command,
 - 371-372
 - PXE clients with WDS, 1025
- compatibility reports,
 - Windows Server 2008
 - upgrades, 128-129
- computer accounts,
 - configuring, 1036-1038
- Computer Manager, 1151-1152
- computer objects, 802-804
 - Delegation tab, 803
 - General tab, 802
 - Member Of tab, 803
 - Operating System tab, 803
- computers containers, 779
- conditional forwarders (DNS),
 - 440-442
- Configuration Action page
 - (SCW), 180
- Configuration APIs (IIS), 1617
- Configuration data
 - collectors, 1373
- configuring. *See*
 - also* customizing
 - BitLocker, 149
 - boot programs for PXE
 - clients, 1037
 - C shells (SUA), 1572-1573
 - certificate templates, 165
 - computer accounts,
 - 1036-1038
 - data collector sets,
 - 1372-1373

- DFSN, 970-980
- DFSR, 981-990
- DHCP
 - DHCPv6 protocol, 386
 - DNS, 386
 - NAP configurations, 510-515
 - scope, 386-393
- disk quotas, 250-252
- DNS, 386
- domain authentication
 - methods, 176-178
- domain client trust of CA, 160-161
- e-mail notifications, 262
- enforcements (NAP), 500-519
- event logs (Event Viewer), 1384-1385, 1397
- gateways, 349-350
- GPOs (Group Policy Objects), 1180-1181
- Group Policy Preferences, 1494-1499
- health policies (NAP), 502-506
- Hyper-V, 1294-1295
- IdMU, 1576-1577
- IIS (Internet Information Services), 1619-1625
- IP addresses
 - MAC addresses, 398-399
 - for multicast transmissions, 1039-1040
- IPsec, 203, 209
- iSCSI Initiator, 1243-1245
- Korn shells (SUA), 1572-1573
- Licensing mode (TS), 548
 - per-device mode, 551, 554
 - per-user mode, 549
- NAP
 - authentication, 510
 - client configuration, 508-510
- DHCP configuration, 510-515
 - enforcements, 500-519
 - health policies, 502-506
 - NAP-incapable policy creation, 507
 - network policies, 504
 - SHV, 501
- network adapters, 1250
- network connections, 112
- network printer connections, 309-314
- NFS
 - servers, 1588-1590
 - shares, 1590
- NLB
 - additional nodes, 1218
 - clusters, 1215
 - DNS records, 1219
 - host-specific information, 1213
 - port rules, 1215-1217
- OU, 781
- partitions, 108
- Performance Monitor
 - (Reliability and Performance interface), 1361
- print servers, 327
- RADIUS, 478
 - backing up configurations, 486
 - defining policy order, 483-484
 - policy configuration, 479-482
- redundant connection
 - mode, 766
- RRAS, 459, 462
 - advanced logging, 472
 - Assign Static IP Addresses user property, 470
 - Callback user property, 469-470
 - connection request authentication, 463
- DHCP, 463-464
 - disabling VPN connectivity, 470
 - NAP, 469
 - passwords, 467
 - PPTP, 464, 471
 - RADIUS, 463
 - security, 467
 - SSL certificates, 474-476
 - SSTP, 473-477
 - troubleshooting, 468-469
 - Verify Caller-ID user property, 469-470
 - VPN connection selection, 466
 - VPN initialization, 468-469
- Server Core, 918-919
 - administrator password, 920
 - applications, 938-939
 - auto-update, 927-928
 - default scripting engine, 925-926
 - firewalls, 929-931
 - hardware, 933-934
 - international settings, 925
 - joining domains, 924-925
 - pagefiles, 929
 - patches, 927-928
 - Remote Desktop, 932-933
 - roles and features, 934-938
 - server activation, 926-927
 - server name, 920-921
 - static TCP/IP v4 information, 921-923
 - time zone, 923-924
- SHV, 501
- site links, 758
- SUA shells, 1572-1573
- SysKey, 218
- time zones, 110
- TS, 606-609, 615-616
- universal group membership
 - caching, 697-698
- URL authorization for
 - web sites, 1634-1638

- variable scope, 1543-1544
- virtual memory, 1194-1200
- visual effects, 1192-1193
- VMs, 1299-1306
- VSS, 256-257
- WDS, 1019-1026
 - authorizing unknown clients, 1030-1035
 - DHCP options, 1027-1028
 - from command line, 1028
 - prestaging computers in Active Directory, 1029-1030
 - server customization, 1035-1041
- Windows Firewall, 197-201
- Windows Server 2008 Administrator
 - accounts, 109
 - ICT interface, 110
 - naming domains/workgroups, 112
 - network connection configurations, 112
 - rebooting after, 112
 - Remote Desktop activation, 116
 - role/feature installation, 114-115, 123
 - time zone configurations, 110
 - update configurations, 113-114
 - Windows Firewall activation, 117
 - WSRM, 1328-1330
- confirm option (PowerShell), 1551-1552
- connection bar (RDC tool), 531
- Connection Manager
 - Administration Kit (CMAK), 1113
- connection request policies (NPS), 479
- Connection Request Policy Wizard, 484
- console tree (MMC), 89
- consolidating servers, 960
- contacts, 802
- containers, linking GPOs (Group Policy Objects) to, 1412-1417
- Content pane (Windows Explorer), 82
- contexting, 1282
- Contributor access level, 248
- Control Host menu commands, Drainstop, 1224
- Control Panel
 - discussed, 93
 - programs and features, 95-96
 - searching, 94
- Control Panel applet (Windows Firewall)
 - firewall configuration, 197-200
 - General tab, 197
 - Group Policy Preferences settings, 1493
 - Import Policy action, 200
 - Inbound Rules section, 198
 - New Rule action, 198
 - Outbound Rules section, 198
- converting
 - certificate templates, 163
 - file systems, 237-238
 - security policies to GPO, 184
- copy-on-write, 1174
- core changes to Windows Server 2008, 22-23
- core site links
 - cost attribute, 755-756, 759
 - replication interval attribute, 757-759
 - sites connected via link attribute, 755
- counters. *See also* data collector sets
 - Memory-Available Bytes counter, 1364
 - Memory-Page Faults/sec counter, 1364
 - Memory-Pages Input/sec counter, 1364
 - Memory-Pages Reads/sec counter, 1364
 - Memory-Pages/sec counter, 1364
 - Network-Bytes Total/Sec counter, 1364
 - Network-Current Bandwidth counter, 1364
 - Paging File-%Usage counter, 1364
 - Performance Monitor
 - adding to, 1363-1364
 - Create New Data Collector Set wizard, 1366
 - saving configured counter sets, 1365-1366
 - PhysicalDisk-% Disk Time counter, 1365
 - PhysicalDisk-current Disk Queue Length counter, 1365
 - Processor-% Processor Time counter, 1365
 - Processor-Interrupts per second counter, 1365
 - System-Processor Queue Length counter, 1365
- CPU detail (Reliability and Performance interface, Resource View), 1358
- Create New Data Collector Set wizard, 1366, 1373
- Create Quota dialog box, 280
- credential roaming, 170
- Credentials accounts (DNS), 425-427

cross-domain GPO
 linking, 1436
 cross-file RDC, 968
 cross-link trust, 745-746
 cryptography, 159
 cscript interpreter, 308
 currency format, 101-102
 Custom connection
 security rule, 208
 custom logging (IIS), 1614
 Custom RDP Settings tab
 (RemoteApp), 588
 Custom Views (Event Viewer),
 1386-1389
 customizing
 ADMX files, 1480-1485
 command prompt window
 (CMD.EXE), 1511-1513
 consoles (MMC), 90-93
 Event Viewer, 1385-1389
 LDAP ports, 856
 server properties, 1035-1041
 site connectivity, 753
 ADLB tool, 765
 core site link attributes,
 755-757
 managing site topology,
 758-764
 redundant connection
 mode, 766
 SSL ports, 856
 Cutler, David, 2

D

/d switches (CMD.EXE), 1511
 data collector sets, 1367. *See*
 also counters
 backups, 1375
 data collectors
 adding to, 1372-1373
 Configuration, 1373
 configuring, 1372-1373
 Event trace, 1373
 properties of, 1372

Data Manager, managing
 data via, 1371
 Directory tab, 1369
 General tab, 1368
 LAN Diagnostics, 1367
 operational overview,
 1375-1376
 properties of, 1368
 restoring, 1375
 Schedule tab, 1370
 Security tab, 1370
 Stop Condition tab, 1370
 System Diagnostics, 1367
 System Performance, 1367
 Task tab, 1371
 templates, saving as, 1375
 data encryption (VPN), 455
 Data Execution Prevention
 (DEP), 1200-1202
 Data Link layer (OSI model),
 337-339
 Data Manager, 1371
 data migration (DFSN), 959
 data storage, 23-26
 Data tab (Performance
 Monitor), 1362
 databases, LSA (Local Security
 Authority), 625
 Datacenter edition (Windows
 Server 2008), 21, 1310
 DataScrn (datascren.sys), 261
 dcdiag command, 711-714
 depromo command, 705-707,
 730-731, 935
 DDNS (dynamic DNS), 30
 Debug logs (Event
 Viewer), 1382
 Debugging Mode option
 (OS Loader, boot
 menu), 1337
 dedicated redirectors, 609
 default documents (IIS), 1613
 default scripting engine,
 configuring in Server
 Core, 925-926

deferred enforcement stage
 (NAP deployment), 499
 defrag utility, 239-240
 defragmenting disks, 238-240
 del command, 230
 delegation
 Delegation of Control
 Wizard, 782
 DNS, 434
 GPO, 1466-1470
 in Server Manager, 1151
 Delegation of Control
 Wizard, 782
 Delegation tab (computer
 objects), 803
 deleting
 AD LDS instances, 863
 event subscriptions, 1397
 OU, 782
 user objects, 825
 demoting domain
 controllers, 767
 DNS cleanups, 773
 removing defunct domain
 controllers, 770-772
 removing domains, 774-776
 server record cleanups, 774
 DEP (Data Execution
 Prevention), 1200-1202
 Deploy with Group Policy
 dialog, 314
 deployment
 discussed, 33-35
 image-based deployment
 automating, 1049-1062
 creating capture boot
 images, 1064-1074,
 1077-1081
 image management,
 1044-1048
 image requirements,
 1042-1043
 Microsoft Solution
 Accelerator for Business
 Desktop Deployment
 2007, 1081

- multicast transmission, 1079-1081
 - problems with, 1011-1013
 - SYSPREP tool, 1013-1017
 - System Center
 - Configuration Manager, 1082-1083
 - media-based deployment, 1063-1064
 - of printers, 314-317
 - of software, 1436
 - assigned software, 1437
 - Microsoft Software Installer, 1437-1440
 - network distribution
 - points, 1437
 - published software, 1437
 - ZAP files, 1440-1442
 - WDS. *See* WDS
 - Desktop Experience, 1113
 - Desktop Windows Manager (DWM), 64-67
 - desktops, remote, 956
 - detailed memory view (Reliability and Performance interface, Resource View), 1360
 - Details pane
 - MMC, 90
 - Windows Explorer, 82
 - detecting slow links, 1426-1427
 - Device Manager, 943, 1119
 - DFS (Distributed File Systems), 956
 - connection management, 990-992
 - DFSN, 957
 - ABE, 981
 - adding servers, 974
 - client failback, 963
 - client view, 959
 - configuring, 970-980
 - data migration, 959
 - delegating namespace management, 975
 - folder management, 977
 - folder creation, 961, 978
 - folder management, 977
 - folder targets, 961-963, 978
 - installing, 969
 - namespace creation, 971
 - namespace servers, 960
 - NetWare
 - interoperability, 960
 - searches in, 977
 - server consolidation, 960
 - upgrading to Windows Server 2008 mode DFSN, 998
 - usage example, 957
 - Windows Server 2008
 - changes to, 963-964
 - DFSR, 13, 957, 965-967
 - AD restoration, 817
 - configuring, 981-990
 - folder replication, 982-984
 - FRS migration to for SYSVOL replication, 843-848
 - server eligibility, 983
 - topology replication, 984-986
 - folders, managing, 997
 - installing, 969
 - replica members, 992-995
 - troubleshooting, 999-1007
 - DFSN (Distributed File System Namespace), 957
 - ABE, 981
 - client failback, 963
 - client view, 959
 - configuring, 970-980
 - data migration, 959
 - delegating namespace management, 975
 - folder management, 977
 - folders
 - creating, 961, 978
 - targets, 961-963, 978
 - installing, 969
 - namespace creation, 971
 - namespace servers, 960
 - NetWare
 - interoperability, 960
 - searches in, 977
 - server consolidation, 960
 - servers, adding to, 974
 - usage example, 957
 - Windows Server 2008
 - changes to, 963-964
 - Windows Server 2008 mode DFSN, upgrading to, 998
- DFSR (Distributed File System Replication), 13, 957, 965-967
- AD restoration, 817
 - configuring, 981-990
 - folder replication, 982-984
 - FRS migration to for SYSVOL replication, 843-848
 - server eligibility, 983
 - topology replication, 984-986
- dfsrdiag command, 1005
- DHCP (Dynamic Host Configuration Protocol), 377, 1103
- address requests, 463
 - administration
 - scope backups, 401
 - scope configuration, 391-393
 - scope creation, 399
 - scope management, 393-394, 397
 - APIPA, 380
 - authorizing, 387
 - authorizing WDS in, 1041
 - cable modems, 381

- configuring for WDS, 1027-1028
 - DHCPv6, 386, 401-403
 - DNS
 - configuring, 386
 - DNS domain name
 - (option 015) option, 382
 - DNS server (option 006) option, 382
 - domain controller actions, 388-390
 - secure updates, 405-406
 - domain controller actions, 388-390
 - DSL modems, 381
 - four-packet structure of, 378
 - installing, 381-383
 - leases, 378-380, 396-397, 404
 - NAP
 - configuration, 510-515
 - deployment, 497
 - quarantine
 - enforcement, 492
 - networking services,
 - distributing, 954
 - redundancy, 404-405
 - RRAS configuration, 464
 - scopes
 - backups, 401
 - configuring, 386
 - creating, 388, 399
 - DHCPv6
 - configuration, 402
 - managing, 393-394, 397
 - option configuration, 391-393
 - redundant
 - configurations, 404
 - server activation, 390
 - WINS/NBNS servers (option 044) option, 382
 - WINS/NBT node type (option 046) option, 382
- DHCPv6, 386, 401-403
- Diagnostic Report Wizard, 1000
 - Diagnostic startup (MSConfig), 1400
 - Diagnostics and Recovery Toolset, 37
 - Diagnostics node (Server Manager), 1119
 - dialogs. *See specific dialogs*
 - digest authentication (IIS), 1615
 - Digital Signature tab (RemoteApp), 588
 - digital signatures, 588, 596
 - DIMS (Digital Identity Management Services), 170
 - directories. *See also* AD (Active Directory)
 - directory browsing (IIS), 1613
 - directory services, 632
 - Directory Synchronization Services (DSS), 1594
 - restartable directory service, 826-829
 - directory information tree (DIT), 633
 - Directory Services Restore Mode option (OS Loader, boot menu), 1337
 - Directory Synchronization Services (SFN), 1594
 - Directory tab (data collector set properties), 1369
 - dirquota.exe, 288
 - Disable automatic restart on system failure option (OS Loader, boot menu), 1337
 - Disable Driver Signature Enforcement option (OS Loader, boot menu), 1337
 - Disable the Service option (SCW), 182
 - disabled devices, 1122
 - Discard Old Duplicates option (CMD.EXE command prompt window), 1511
 - Discover boot images, 1063-1064
 - Discovery mode (TS licensing), 554-556
 - Disk Defragmenter, 238-240
 - Disk Management MMC
 - snap-in, 231-236, 943
 - disk-only model (quorum mode configuration), 1235
 - disk resource overview (Reliability and Performance interface, Resource View), 1359
 - disk space (hard drives)
 - BitLocker drive encryption, 100-101
 - Windows Server 2008 installation requirements, 100
 - disk wiping, 144
 - diskpart utility, 236-237
 - disks. *See* hard disks
 - Diskshadow, 1175-1178
 - Display tab (RDC tool), 537-539
 - distinguished name tags (DNTs), 633
 - distinguished names (DNs), 633
 - Distributed File System
 - Replication. *See* DFSR
 - distributed services
 - backups, 956
 - client management, 955
 - DFS, 956
 - adding/removing replica members, 992-995
 - connection management, 990-992

- folder management, 997
- installing, 969
- troubleshooting, 999-1007
- DFS, 957
 - ABE, 981
 - adding servers, 974
 - client failback, 963
 - client view, 959
 - configuring, 970-980
 - data migration, 959
 - delegating namespace management, 975
 - folder creation, 961, 978
 - folder management, 977
 - folder targets, 961-963, 978
 - installing, 969
 - namespace creation, 971
 - namespace servers, 960
 - NetWare
 - interoperability, 960
 - searches in, 977
 - server consolidation, 960
 - upgrading to Windows Server 2008 mode
 - DFS, 998
 - usage example, 957
 - Windows Server 2008
 - changes to, 963-964
- DFS, 13, 957, 965-967
 - AD restoration, 817
 - configuring, 981-990
 - folder replication, 982-984
 - FRS migration to for SYSVOL replication, 843-848
 - server eligibility, 983
 - topology replication, 984-986
- domain controllers, 954
- FRS, 964
- networking services, 954
- patches, 955
- print management, 955
- remote desktops, 956
- remote servers, 956
- security, 953-954
- server management, 955
- distributed storage, 26-28
- distribution groups, 797
- DIT (directory information tree), 633
- DMZ (demilitarized zones), 144
- DNs (distinguished names), 633
- DNS (Domain Name System)
 - ADDS, 427
 - authoritative DNS servers, 410
 - caching in, 443
 - cleanups, 773
 - CNAME records, 413
 - communication, 361
 - conditional forwarders, 440-442
 - delegation, 434, 704-705
 - DHCP servers
 - configuring for, 386
 - domain controller actions, 388-390
 - secure updates for, 405-406
 - discussed, 29, 407, 636-637, 1103-1104
 - forwarders, 439
 - hierarchy of, 407
 - installing, 411
 - IPv6 support for, 447
 - lookups, 407-409
 - managing, 412
 - application partitions, 422-424
 - domain creation, 416
 - domain-wide partitions, 423
 - forest-wide partitions, 423
 - record response behavior, 413
 - Round Robin functionality, 415-416
 - subnet prioritization, 415
 - zone creation, 417-420
 - _msdcs zones, 428
 - names, 639
 - networking services, distributing, 954
 - operational overview, 407-409
 - records, adding, 1219
 - scavenging in, 431
 - security, 425-427
 - TTL, 410
 - zones
 - GlobalNames zones, 444-445
 - reverse lookup zones, 432-434
 - scavenging in, 431
 - stub zones, 437
- DNS domain name (option 015) option, DHCP installation, 382
- DNS server (option 006) option, DHCP installation, 382
- DNS tab (Properties context menu), 395
- DNTs (distinguished name tags), 633
- Domain Controller Wizard, 683
- domain controllers, 779
 - adding, 679-683
 - creating from media, 715-718
 - demoting, 767, 770-776
 - DHCP actions, 388-390
 - directory partitions list, viewing, 423
 - distributed services, 954
 - FSMO roles, 679
 - best practices, 685-686
 - Domain Naming Master, 687
 - GC (Global Catalog) setting, 694-698

- Infrastructure Master, 686
- moving from command
 - line, 691-692
- PDC Emulator
 - Master, 686
- potential problems,
 - 686-687
- RID Master, 686
- Schema Master, 687
- seizing, 693-694
- transferring graphically,
 - 687-691
- moving, 707
- RDOCs (read-only domain controllers)
 - features, 722-725
 - installing, 729-740
 - prerequisites for
 - deployment, 729
 - restrictions, 726, 729
- removing, 719-722
- unattended installation,
 - 683-684
- verifying operation of,
 - 705-715
- Windows Server 2008
 - upgrades, 127
- domain local groups, 797-799
- domain modes (AD), 672-674
 - mixed mode, 672
 - Windows 2000 native
 - mode, 672
 - Windows Server 2003
 - interim mode, 673
 - Windows Server 2003
 - mode, 673
 - Windows Server 2008
 - mode, 673-674
- Domain Name System. *See* DNS
- domain naming master FSMO
 - roles, 669-670, 687
- domain-wide partitions,
 - creating DNS in, 423
- domains. *See also* DNS
 - (Domain Name System)
 - AD domain modes, 672-674
 - mixed mode, 672
 - Windows 2000 native
 - mode, 672
 - Windows Server 2003
 - interim mode, 673
 - Windows Server 2003
 - mode, 673
 - Windows Server 2008
 - mode, 673-674
 - ADDS, 114
 - BDC (backup domain controller), 625
 - builtin containers, 779
 - computers containers, 779
 - configuring in Server
 - Core, 924-925
 - creating, 416, 639-651, 698
 - advantages, 699-700
 - DNS delegation, 704-705
 - step by step process,
 - 700-704
 - Domain Controllers, 779
 - firewall exception
 - behaviors, 196
 - ForeignSecurityPrincipals
 - containers, 779
 - forests, 653-656
 - naming
 - DNS names, 639
 - NetBIOS names, 628, 639
 - Windows Server 2008
 - configurations, 112
 - PDC (primary domain controller), 624
 - prune and graft
 - functionality, 836
 - removing, 719-722, 774-776
 - replication
 - full replication, 626
 - partial replication, 627
 - urgent replication, 627
 - trees, 651-652
- trusts
 - benefits of, 630-632
 - definition, 630
 - users containers, 780
 - versus workgroups, 623-627
 - Windows OS domain
 - compatibility, 627-630
- DOS (Disk Operating System),
 - 1, 1508
- DOSKEY, 1514
- DPM (Data Protection Manager), 1405
- Drain mode (TS Session Broker), 610-611
- Drainstop command (Control Host menu), 1224
- Drive Encryption Control
 - Panel applet
 - (BitLocker), 149
- drivers
 - adding to driver store,
 - 1123-1124
 - adding to WIM files,
 - 1073-1074, 1077-1078
 - installing, 107
 - TS Easy Print, 559-561, 564
 - Windows RE, managing
 - in, 1351
- drives. *See* hard disks
- \$DRVLTR\$ files, 130
- DSC (Dynamic Suite Composition), 1282
- dsdbutil command, 863
- DSL modems, 381
- DSRM (Directory Services Restore Mode), 815
- DVDs, installing Windows
 - Server 2008 from,
 - 101-105
- DWM (Desktop Windows Manager), 64-67
- DWORD values, 698
- dynamic content compression
 - (IIS), 1615
- dynamic DNS (DDNS), 30

Dynamic Host Configuration Protocol. *See* DHCP
dynamic NAT (Network Address Translation), 353, 460
Dynamic Suite Composition (DSC), 1282
dynamic VLAN (Virtual Local Area Networks), 494

E

e-mail notifications
 configuring, 262
 notification limits, 263
 sending in event of print server failure, 331
 sending in response to disk quotas, 275-276
EAP quarantine, 494
echo %path% command (CMD.EXE), 1518
eDirectory, 1594
editing
 file screens, 287
 Registry, 1188-1190
 tasks, 1131-1132
EFS (Encrypted File System), 252-255
elevation of privilege, 52-56
emergency recovery
 passwords, 154
emulation, 1509
Enable Boot Logging option (OS Loader, boot menu), 1336
Enable low-resolution video (640-480) option (OS Loader, boot menu), 1337
enabling. *See* configuring
encapsulation, 454
Encrypted File System (EFS), 252-255

encryption, 1645-1647
 BitLocker drive encryption, 100-101
 IPsec, 204
 partitions, 144-154
 UNIX passwords, 1584
 VPN, 455
enforcements (NAP), 500-519
Enterprise Agreement, 15
enterprise CA (Certificate Authorities), 158
Enterprise edition (Windows Server 2008), 21, 1310
Enterprise PKI (PKIView)
 MMC snap-in (Server Manager, ADCS area), 162
enumdirectorypartitions
 command, 423
Environment tab (Active Directory Users and Computers MMC snap-in), 612
error handling. *See* WER
ESP (Encapsulating Security Payload) protocol, 203
event filtering, 1385-1389
event logs, 1383
 clearing, 1397
 configuring, 1384-1385, 1397
 NAP, 517-519
 querying, 1398-1400
 viewing, 1383, 1399
event subscriptions, 1389-1397
Event trace data
 collectors, 1373
Event Viewer
 accessing, 1381
 Admin logs, 1382
 Analytic logs, 1382
 Application logs, 1382
 Applications and Services log area, 1382

Custom Views, 1386-1389
 customizing, 1385-1389
Debug logs, 1382
event filtering, 1385-1389
event logs, 1383
 clearing, 1397
 configuring, 277, 1384-1385, 1397
 Forwarded Events logs, 1382
 Operational logs, 1382
 querying, 1398-1400
 Security logs, 1382
 Setup logs, 1382
 System logs, 1382
 viewing, 1383, 1399
event subscriptions, 1389-1397
 wevutil.exe command-line interface, 1397, 1399-1400
 Windows Logs node, 1382
Excel RMS-protected documents, 868
exceptions, 287
Exclusion Ranges (Address Pool leaf), 397
exit statements, 1557
expanding Server Manager, 1149-1150
Experience tab (RDC tool), 541-542
Explorer. *See* Windows Explorer
exporting
 disk quota information, 252
 file screens, 288-289
 tasks, 1132
external command (CMD.EXE), 1517
external networks, 1294
external trust, 747

F

F12 key (network boot), 1039

faAdmcConv command, 1486

Failed Request node

(Certificates MMC
snap-in), 169

failover clustering

active-active clusters, 1207

active-passive clusters, 1207

cluster architecture,

1230-1232

cluster creation, 1248-1249

Cluster Events, 1262

cluster failover, 1255-1258

cluster permissions, 1263

cluster validation, 1245-1247

command-line management,
1264-1266

dependency reports, 1262

discussed, 20, 1114,

1206-1208, 1229-1230

file share witnesses, 1208

high-availability services and
applications, 1251-1254

iSCSI Initiator configuration,
1243-1245

network adapter

configuration, 1250

network and security

enhancements,

1236-1237

node management,

1261-1262

quorum model modification,

1259-1260

quorum modes, 1208,

1232-1233

disk-only, 1235

node and disk

majority, 1234

node and file share

majority, 1235

node majority, 1233-1234

supported hardware,

1237-1242

upgrading from Windows

Server 2003, 1266-1268

failure pop-up (NAP), 513

FAT (File Allocation Table),

225-226

FAT32, 226

Fax server, 1104

feature delegation (IIS),

1640-1642

File Allocation Table (FAT),

225-226

File Migration Utility, 1594,

1603-1604, 1607

file screen audits, 265

File Server Resource Manager.

See FSRM

File Services, 1104

file share witnesses, 1208

file systems

comparison of, 230

converting, 237-238

DFS, 956

adding/removing replica

members, 992-995

connection management,

990-992

DFSN. *See* DFSN

DFSR. *See* DFSR

folder management, 997

installing, 969

troubleshooting, 999-1007

discussed, 225

disk defragmentation,

238-240

EFS (Encrypted File

System), 252-255

FAT (File Allocation

Table), 225-226

FAT32, 226

file screens

active versus passive, 285

assigning, 285

discussed, 284-285

editing, 287

exceptions, 287

exporting, 288-289

importing, 288-289

formatting and managing

with Disk Management

MMC snap-in, 231-236

with diskpart utility,

236-237

FSRM (File Server

Resource Manager)

discussed, 257-258

disk quotas. *See*

disk quotas

e-mail notifications, 262

file screen audits, 265

file screens, 284-289

installing, 258-262

notification limits, 263

report locations, 264-265

scripting, 290

storage reports, 264-273

NTFS (New Technology

File System)

\$AttrDef file, 227

\$BasClus file, 227

\$Bitmap file, 227

\$Boot file, 227

checking version of, 226

discussed, 226

disk quotas, 250-252,

273-284

file ownership, 240-243

file permissions, 243-247

\$LogFile file, 227

\$MFT file, 227

\$MFTMirr file, 227

\$Quota file, 227

self-healing NTFS,

228-229

shares, 248-250

symbolic links, 228-230

transaction NTFS, 228

- \$UpCase file, 227
- versions, 227
- \$Volume file, 227
- VSS (Volume Shadow Copy Service), 255-257
- permissions, updating, 1445
- files
 - ADMX files, 1480-1485
 - \$BasClus, 227
 - \$Bitmap, 227
 - \$Boot, 227
 - \$LogFile, 227
 - \$MFT, 227
 - \$MFTMirr, 227
 - ownership of, 240-243
 - paging files, 1194-1196
 - configuring in Server Core, 929
 - crash considerations, 1196-1197
 - moving, 1197-1199
 - viewing usage of, 1199-1200
 - permissions, 243-247
 - \$Quota, 227
 - recovering, 1168-1170
 - .reg files, 1188-1190
 - screens
 - active versus passive, 285
 - assigning, 285
 - discussed, 284-285
 - editing, 287
 - exceptions, 287
 - exporting, 288-289
 - importing, 288-289
 - scrolling through, 1516
 - shares, 248-250
 - unattend.xml files, 918
 - \$UpCase, 227
 - VHD format, 1154, 1303-1304
 - \$Volume, 227
 - ZAP files, 1440-1442
- filescrn.exe, 288
- filtering
 - events in Event Viewer, 1385-1389
 - GPO (Group Policy Object) application, 1453-1460
 - with Windows Explorer, 83
- finding
 - commands in CMD.EXE
 - command prompt window, 1517-1518
 - printers in Active Directory, 307-309
- firewalls
 - configuring in Server Core, 929-931
 - domain exception behaviors, 196
 - private network exception behaviors, 196
 - public network exception behaviors, 196
 - rules, editing in SCW, 182
 - Windows Firewall, 196, 528
 - configuring, 197-201
 - Control Panel applet, 197-200
 - enabling in Windows Server 2008 configurations, 117
 - Group Policy area, 201
 - Import Policy action, 200
 - Inbound Rules section, 198
 - monitoring section, 201
 - New Rule action, 198
 - Outbound Rules section, 198
 - turning off, 201
 - Windows Firewall with Advanced Security, 195
- Flexible Single Master Operation roles. *See* FSMO roles
- Flip, 68
- folders
 - DFS folder management, 997
 - DFSN
 - creating in, 961, 978
 - folder targets, 961-963, 978
 - managing in, 977
 - DFSR, replicating via, 982-984
 - recovering, 1168-1170
 - scrolling through, 1516
 - winsxs, 1106
- Font tab (CMD.EXE), 1511
- font size, changing in CMD.EXE command prompt window, 1511
- ForeignSecurityPrincipals containers, 779
- forests, 653-656
 - forest modes (AD), 674-677
 - Windows 2000 mode, 675
 - Windows Server 2003 interim mode, 675
 - Windows Server 2003 mode, 675-676
 - Windows Server 2008 mode, 676-677
 - forest trust, 744-745
 - forest-wide partitions, creating DNS in, 423
 - prune and graft functionality, 836
- format command, 1352
- formatting file systems
 - with Disk Management MMC snap-in, 231-236
 - with diskpart utility, 236-237
- forward replication (MSDSS), 1596-1597, 1602
- forward synchronization (MSDSS), 1595-1596
- Forwarded Events logs (Event Viewer), 1382

forwarders (DNS), 439
 FPNW (File and Print Services for NetWare), 1594
 FRS (File Replication Service), 964
 DFS, troubleshooting, 999
 DFSR migration for
 SYSVOL replication,
 843-848
 FS (Federation Service), 892
 FS-P (Federation Service Proxy), 893
 FSMO (Flexible Single Master Operation) roles, 679
 best practices, 685-686
 domain naming master
 FSMO roles, 669-670
 Domain Naming Master, 687
 GC (Global Catalog)
 setting, 694-698
 infrastructure FSMO roles,
 668, 686
 moving from command
 line, 691-692
 PDC emulator FSMO roles,
 666-667, 686
 potential problems, 686-687
 RID master FSMO roles,
 667, 686
 schema master FSMO
 roles, 668, 687
 seizing, 693-694
 transferring graphically,
 687-691
 FSRM (File Server Resource Manager)
 discussed, 257-258
 disk quotas. *See* disk quotas
 e-mail notifications, 262
 file screen audits, 265
 file screens
 active versus passive, 285
 assigning, 285
 discussed, 284-285

 editing, 287
 exceptions, 287
 exporting, 288-289
 importing, 288-289
 installing, 258-262
 notification limits, 263
 report locations, 264-265
 scripting, 290
 storage reports, 264-266
 scheduling, 267-273
 types of reports, 266-267
 FTP Management Console
 (IIS), 1616
 FTP Server, 1616
 full control permissions, 244
 full replication, 626
 functions
 PowerShell functions,
 creating, 1544-1545
 PowerShell scripts,
 1557-1558
 FVEK (Full-Volume
 Encryption Keys),
 145-146

G

Gates, Bill, 3
 gateways
 configuring, 349-350
 Gateway (TS), single
 sign-ons via, 603
 GC (global catalog), 670-671,
 694-698
 General tab
 computer objects, 802
 data collector set
 properties, 1368
 MSConfig, 1400
 Performance Monitor, 1361
 printer properties, 299
 Properties context
 menu, 395
 RDC tool, 537

Terminal Services
 Configuration MMC
 snap-in, 617-618
 user objects, 790
 Windows Firewall Control
 Panel applet, 197
 zone properties menu, 429
 Get-ChildItem cmdlet, 1544
 get-itemproperty cmdlet, 1547
 get-process cmdlet, 1550
 get-psdrive cmdlet, 1545
 get-psprovider cmdlet, 1549
 get-service cmdlet, 1552
 .GetType() method, 1542-1543
 Global Audit Policy, 830
 global catalog (GC),
 670-671, 694-698
 global unicast addresses, 366
 Globally Unique Identifier
 (GUID), 1012
 Globalnames zones (DNS),
 444-445
 GNU SDK option (SUA
 installations), 1570
 GNU Utilities option (SUA
 installations), 1570
 GPMC (Group Policy
 Management Console),
 11, 1427-1430. *See also*
 Group Policy
 GPOs (Group Policy Objects)
 applying to sites, 1436
 configuring, 1180-1181
 creating, 1430-1435
 cross-domain linking, 1436
 delegation, 1466-1470
 deploying printers
 with, 314-317
 discussed, 1411-1412
 filtering application of,
 1453-1460
 linking to containers,
 1412-1417

- modifying GPO application behavior, 1446-1451
- NAP client
 - configuration, 508
- reports, 1464-1465
- results, 1471-1476
- security policies,
 - converting to, 184
- Starter GPOs, 1460-1463
- GPOVault, 1491
- GPRESULT utility, 1474-1475
- GPUPDATE tool,
 - 1421, 1425-1426
- Graph tab (Performance Monitor), 1362
- Group Policy
 - application of, 1421-1425
 - backup of, 1487-1488
 - central store, 1485-1487
 - custom ADMX files, 1480-1485
 - discussed, 1409
 - features, 1410-1411
 - GPMC (Group Policy Management Console), 11, 1427-1430
 - GPOs (Group Policy Objects)
 - applying to sites, 1436
 - creating, 1430-1435
 - cross-domain linking, 1436
 - delegation, 1466-1470
 - discussed, 1411-1412
 - filtering application of, 1453-1460
 - linking to containers, 1412-1417
 - modifying GPO
 - application behavior, 1446-1451
 - reports, 1464-1465
 - results, 1471-1476
 - Starter GPOs, 1460-1463
 - group membership restrictions, 1445
 - Group Policy Modeling, 1476-1480
 - IPsec configuration, 209
 - local policy, viewing, 1417-1421
 - loopback processing, 1451-1452
 - Microsoft templates, 1503-1504
 - permissions updates, 1445
 - Preferences
 - client support, 1499-1500
 - configuring, 1494-1499
 - Control Panel
 - Settings, 1493
 - features, 1492-1493
 - history of, 1491-1492
 - reports, 1500
 - Windows Settings, 1493
 - refreshing, 1425-1426
 - restoring, 1488-1490
 - security template
 - integration, 192
 - slow link detection, 1426-1427
 - software deployment, 1436
 - assigned software, 1437
 - Microsoft Software Installer, 1437-1440
 - network distribution points, 1437
 - published software, 1437
 - ZAP files, 1440-1442
 - software restrictions, 1442-1444
 - structure, 1410
 - troubleshooting, 1501-1502
 - TS management, 620
 - viewing sites, 1436
 - Group Policy area (Windows Firewall), 201
 - Group Policy Editor, 188
 - Group Policy Management Console (GPMC), 11, 1427-1430
 - Group Policy Objects. *See* GPOs
 - Group Policy Results Wizard, 1471-1474
 - grouping items in Windows Explorer, 83
 - groups, restricting memberships to, 1445
 - GUID (Globally Unique Identifier), 1012

H

 - H-node (Hybrid 0x8) node type, 382
 - HAL (Hardware Abstraction Layer), 1043
 - handles (objects), 1334
 - hard disks
 - BitLocker drive encryption, 100-101
 - defragmentation, 238-240
 - disk quotas
 - actions, 274-279
 - assigning, 280-284
 - discussed, 273
 - enabling, 250
 - hard quotas, 274
 - importing quota information, 252
 - moving from one disk to another, 252
 - properties, 275
 - soft quotas, 274
 - file systems. *See* file systems
 - mirrored disks (RAID 1), 231
 - RAID
 - Windows Server 2008
 - installation, 100
 - RAID 0 (striped disks), 231
 - RAID 5, 231
 - spanned disks, 231

- wiping, 144
- Windows Server 2008
 - installation
 - requirements, 100
- hard quotas, 274
- Hardware Abstraction Layer (HAL), 1043
- headers
 - TCP headers, 356
 - UDP headers, 357
- health policies, 479
 - checks, enabling, 504
 - configuring, 502-503
- health reports, 1001
- health updates, 491
- Hello World messages
 - CMD.EXE, 1516
 - PowerShell, 1552
 - VBScript, 1529-1530
- high availability
 - choosing high-availability methods, 1209-1210
 - discussed, 1205
 - failover clustering
 - active-active clusters, 1207
 - active-passive clusters, 1207
 - cluster architecture, 1230-1232
 - cluster creation, 1248-1249
 - Cluster Events, 1262
 - cluster failover, 1255-1258
 - cluster permissions, 1263
 - cluster validation, 1245-1247
 - command-line management, 1264-1266
 - dependency reports, 1262
 - discussed, 1206-1208, 1229-1230
 - file share witnesses, 1208
 - high-availability services and applications, 1251-1254

- iSCSI Initiator
 - configuration, 1243-1245
- network adapter
 - configuration, 1250
- network and security enhancements, 1236-1237
- node management, 1261-1262
- quorum model
 - modification, 1259-1260
- quorum modes, 1232-1235
- quorums, 1208
- supported hardware, 1237-1242
- upgrading from Windows Server 2003, 1266-1268
- NLB (Network Load Balancing)
 - accessing NLB clusters, 1219-1220
 - cluster mode and IP address management, 1226
 - command-line management, 1227-1228
 - configuring, 1213-1219
 - discussed, 1205-1206, 1210-1212
 - installing, 1213
 - logging and credentials, 1227
 - migrating from Windows Server 2003, 1229
 - port rule management, 1220-1223
 - removing, 1228
 - server management, 1223-1226
- HiSecDC option (Security Templates MMC snap-in), 189

- HiSecWS option (Security Templates MMC snap-in), 189
- Home Edition (XP), 8
- hosted VMM (Virtual Machine Manager), 1284-1285
- hostname command, 412, 920-921
- HRA (health registration authorities), 493
- HTTP errors (IIS), 1613
- HTTP Logging (IIS), 1614
- HTTP redirection (IIS), 1613
- Hyper-V, 1104
 - advanced management, 1317-1318
 - command-line management, 1311-1313
 - configuration, 1294-1295
 - discussed, 1283-1284, 1289-1291
 - Hypervisor Virtualization technology, 1285-1287
 - installing, 1291-1292
 - on laptops, 1318-1319
 - licensing, 1309-1310
 - live migration, 1316-1317
 - network management, 1293
 - Physical-to-Virtual Migration, 1313
 - quick migration, 1313-1316
 - snapshots, 1310-1311
 - VM configuration, 1299-1306
 - VM controls, 1306-1309
 - VM creation, 1296-1299

I

- icacls utility, 247
- ICT (Initial Configuration Tasks)
 - definition, 18
 - DHCP installations, 381
 - Windows Server 2008 configuration, 110

- Identity Integration Feature Pack (IIFP), 11
- IdMU (Identity Management for UNIX), 1574-1577
- IE ESC (Internet Explorer Enhanced Security Configuration), 210-211
- IEEE 802.1x authenticated network connections.
See EAP quarantine
- IETF (Internet Engineering Task Force), 352
- ifconfig command, 347-348
- IIFP (Identity Integration Feature Pack), 11
- IIS (Internet Information Services)
 - and Windows Vista, 1648-1649
 - certificates, 1645-1647
 - configuring, 1619-1625
 - discussed, 18, 1611
 - encryption, 1645-1647
 - features and modules, 1612-1617
- IIS Manager
 - adding web sites, 1630-1633
 - appcmd utility, 1643-1645
 - command line, 1643-1645
 - configuring URL
 - authorization for web sites, 1634-1638
 - discussed, 1628-1630
 - feature delegation, 1640-1642
 - remote management, 1639-1640
- IIS processing, 1617-1618
- installing, 1625-1628
- Management
 - Compatibility, 1616
- Management Console, 1616
- Metabase
 - Compatibility, 1616
 - modules, 1616
 - Scripting Tools, 1616
 - Server Core support, 1648
 - Windows Media Services
 - 2008, 1650
 - Windows Web Server 2008, 1649-1650
 - WMI Compatibility, 1616
- image-based deployment
 - automating, 1049-1062
 - creating capture boot
 - images, 1064-1074, 1077-1081
- image management, 1044-1048
- image requirements, 1042-1043
- Microsoft Solution
 - Accelerator for Business Desktop Deployment 2007, 1081
- multicast transmission, 1079-1081
- problems with, 1011-1013
- SYSPREP tool, 1013-1017
- System Center Configuration Manager, 1082-1083
- WDS. *See* WDS
- WIM images, 1340-1345
- imagex /apply command, 1342-1343
- Import Policy action (Windows Firewall Control Panel applet), 200
- importing
 - disk quota information, 252
 - file screens, 288-289
 - tasks, 1132
- Inbound Rules section (Windows Firewall Control Panel applet), 198
- InfoPath, 868
- infrastructure FSMO roles, 668, 686
- Initial Configuration Tasks.
See ICT
- Insert mode option (CMD.EXE command prompt window), 1511
- install images
 - defined, 1044
 - installing, 1046
- Install Licenses Wizard, 546
- installing
 - AD FS, 895-906
 - AD LDS, 855
 - AD RMS, 869-873
 - ADCS, 158
 - applications
 - in Server Core, 938-939
 - on TS, 585
 - boot images, 1044-1045
 - claims-aware agent (AD FS), 897
 - DFS, 969
 - DFSN, 969
 - DHCP, 381-383
 - DNS, 411
 - domain controllers, 683-684
 - drivers, 107, 1123-1124
 - FSRM, 258-262
 - Hyper-V, 1291-1292
 - IdMU, 1576-1577
 - IIS, 1625-1628
- image-based deployment
 - automating, 1049-1062
 - creating capture boot
 - images, 1064-1074, 1077-1081
 - image management, 1044-1048
 - image requirements, 1042-1043

- Microsoft Solution
 - Accelerator for Business Desktop Deployment 2007, 1081
 - multicast transmission, 1079-1081
 - problems with, 1011-1013
 - SYSPREP tool, 1013-1017
 - System Center
 - Configuration Manager, 1082-1083
 - install images, 1046
 - media-based deployment, 1063-1064
 - NFS servers, 1587
 - NLB, 1213
 - Novell Client for Windows, 1594
 - PowerShell, 1537
 - Print Management
 - components, 291-292
 - printers, 317-318
 - RDOCs, 729-740
 - roles/features, 114-115, 123, 1106-1112, 1146-1149
 - Server Core, 915-916
 - Server Manager features, 1117-1118, 1146-1149
 - SUA, 1569
 - Base SDK option, 1570
 - Base Utilities option, 1570
 - GNU SDK option, 1570
 - GNU Utilities
 - option, 1570
 - Perl option, 1571
 - security, 1571
 - SVR-5 Utilities option, 1570
 - Visual Studio Debugger
 - Add-in option, 1571
 - TS
 - Gateway, 568-569
 - licenses, 545-547
- Session Broker, 605
- Web Access, 594
- VPN, 458
- WAIK, 1052
- WDS, 1017-1019
- Windows Server 2008
 - activating installations, 117, 120-122
 - advanced installations, 130
 - automated installations, 133-139
 - currency format selection, 101-102
 - driver installations, 107
 - DVD installations, 101-105
 - existing OS installations, 123-125
 - keyboard layout selection, 101-102
 - language selection, 101-102
 - license agreements, 105, 124
 - media installations, 101-105
 - NTFS volumes, 105
 - partition
 - configurations, 108
 - partitions, 125
 - product keys, 103-104, 124
 - RAID configurations, 100
 - requirements for, 100
 - troubleshooting, 131-133
 - viewing log files, 131-133
 - virtual installations, 99
 - WIM file installations, 101
- WINS, 448
- WSB, 1158
- intermediate CA (Certificate Authorities), 157
- internal command (CMD.EXE), 1515
- internal network
 - connections, 1294
- international settings,
 - configuring in Server Core, 925
- Internet connections, 144
- Internet Engineering Task Force (IETF), 352
- Internet Information Services. *See* IIS
- Internet printing, 331-332
- Internet Printing Client, 1114
- Internet Protocol. *See* IP
- Internet Storage Name Server (iSNS), 1114
- IntraSite Automatic Tunnel Addressing Protocol (ISATAP), 922
- Invoke-Expression
 - cmdlet, 1552
- IP (Internet Protocol)
 - discussed, 335-336
 - gateway configuration, 349-350
 - IP addresses
 - APIPA, 380
 - automatic private IP addressing, 351-352
 - configuring for multicast transmissions, 1039-1040
 - DHCP. *See* DHCP
 - discussed, 29
 - DNS. *See* DNS
 - gateway configuration, 349-350
 - global unicast
 - addresses, 366
 - link-local addresses, 366
 - MAC addresses, 398-399
 - managing for NLB (Network Load Balancing), 1226

- NAT (Network Address Translation), 352-355, 460-461
 - setting, 345-349
 - site-local addresses, 367
 - unique local addresses, 367
 - WINS, 447-448
 - IP filters, 506
 - IPv4 limitations, 350-351
 - IPv6, 20, 362-368, 447
 - IP and domain restrictions (IIS), 1615
 - MAC addresses, 337-339
 - subnet masks, 339-344
 - ipconfig command, 337-338, 365-366, 380, 921-922
 - IPsec (IP security), 202
 - AH, 203
 - authentication, 207
 - configuring, 203, 209
 - connection security rules, 208
 - encryption, 204
 - ESP protocol, 203
 - IPsec SA, 204
 - key exchange, 204
 - key exchange configuration, 206
 - NAP, 493
 - server configuration, 204-206
 - Transport mode, 203
 - Tunnel mode, 203
 - IPv6 (Internet Protocol, Version 6), 20, 362-368, 447
 - ISAKMP (Internet Security Association and Key Management Protocol), 204
 - ISAPI Extensions support (IIS), 1613
 - ISAPI Filters support (IIS), 1614
 - ISATAP (IntraSite Automatic Tunnel Addressing Protocol), 922
 - iSNS (Internet Storage Name Server), 11, 1114, 1243-1245
 - Isolation connection security rule, 208
 - issuing certificate templates, 165-167
 - issuing CA (Certificate Authorities), 157
 - Itanium edition (Windows Server 2008), 21
- J**
- jobs (processes), defining, 1334
 - joining domains, 924-925
 - junction points, 1021
- K**
- /k <command> switches (CMD.EXE), 1511
 - Kerberos authentication, 173-176
 - Kerberos Policy, 221-222
 - key exchange (IPsec), 204-206
 - keyboards layouts, 101-102
 - Kiosk Group Policy template, 1504
 - KMS (Key Management Service), 120-122
 - Korn shells (SUA), configuring, 1572-1573
- L**
- L2TP (Layer Two Tunneling Protocol), 456-457
 - LAN Diagnostics data collector sets, 1367
 - LAN Manager NOS (Network Operating System), 2
 - languages
 - in OS images, 1042
 - selecting for Windows Server 2008 installation, 101-102
 - laptops
 - Hyper-V on, 1318-1319
 - security, 145
 - Last Interactive Logon
 - Information feature, 819-821
 - Last Known Good
 - Configuration option (OS Loader, boot menu), 1337
 - Layout tab (CMD.EXE), 1513
 - LDAP (Lightweight Directory Access Protocol), 635
 - AD LDS, 854-856
 - Authentication servers, 1592
 - SCW, 182
 - leases (DHCP), 378-380, 396-397, 404
 - LFN (Long File Name) support, 225
 - licensing
 - AD RMS, 887-890
 - discussed, 35-38, 105, 124
 - Enterprise Agreement, 15
 - Software Assurance, 15
 - TS, 544
 - backups, 557
 - changing Discovery mode, 554-556
 - Install Licenses Wizard, 546
 - license installation, 547
 - Licensing mode
 - configuration, 548-554
 - managing, 546
 - troubleshooting, 556
 - TS Licensing
 - installation, 545
 - VMs (virtual machines) with Hyper-V, 1309-1310

- Lightly Managed Group Policy template, 1503
- Lightweight Directory Access Protocol (LDAP), 635
- limited access networks, creating via IP filters (NAP enforcement configuration), 506
- Line Printer Remote (LPR) Port Monitor, 1114
- link-local addresses, 366
- links
 - slow links. detecting, 1426-1427
 - symbolic links, 228-230
- Linux NFS servers, connecting to, 1591
- live migration (VMs with Hyper-V), 1316-1317
- load balancing, 765
- loading virtual applications, 1279
- local policy, 1417-1421
- Local Resources tab (RDC tool), 539-541
- Local Security Authority (LSA) database, 625
- Local Users and Groups snap-in, 1140-1141
- locations, report, 264-265
- locked-out user accounts, 791
- Log on Settings tab (Terminal Services Configuration MMC snap-in), 616
- \$LogFile file, 227
- logging off Server Core, 941-942
- logging tools (IIS), 1614
- Logon Hours option (user objects, Account tab), 791

- logons
 - Last Interactive Logon Information feature, 819-821
 - logon rights, granting to TS via TS Web Access, 600
 - Windows Server 2008, 48
 - Windows Vista, 47-48
 - Windows XP, 46-47
- logs, 131-133
 - Admin logs, 1382
 - Analytic logs, 1382
 - Application logs, 1382
 - Debug logs, 1382
 - event logs, 1383
 - clearing, 1397
 - configuring, 1384-1385, 1397
 - NAP, 517-519
 - querying, 1398-1400
 - viewing, 1383, 1399
 - Forwarded Events logs, 1382
 - migration logs, 1600-1601
 - NLB (Network Load Balancing) logs, 1227
 - Operational logs, 1382
 - performance logs, 1377
 - RADIUS logs, 485
 - Security logs, 1382
 - Setup logs, 1382
 - System logs, 1382
- Long File Name (LFN) support, 225
- lookups (DNS), 407-409
- loopback processing, 1451-1452
- LPR (Line Printer Remote) Port Monitor, 1114
- LSA (Local Security Authority) database, 625

M

- M-node (Mixed 0x4) node type, 382
- MAC addresses, 337-339, 398-399
- Macintosh, Windows Server integration, 1566
- MAK (Multiple Activation Keys), 120-122
- manage-bde.wsf script, 149
- Managed By tab (user groups), 800
- Management Console (IIS), 1616
- Management Scripts and Tools (IIS), 1616
- Management Service (IIS), 1616
- managing
 - failover clustering
 - Cluster Events, 1262
 - cluster failover, 1255-1258
 - cluster permissions, 1263
 - command-line
 - management, 1264-1266
 - dependency reports, 1262
 - nodes, 1261-1262
 - quorum model
 - modification, 1259-1260
 - file systems
 - with Disk Management MMC snap-in, 231-236
 - with diskpart utility, 236-237
- FSRM (File Server Resource Manager) from script, 290
- IIS (Internet Information Services) with IIS Manager
 - adding web sites, 1630-1633
 - appcmd utility, 1643-1645

- command line, 1643-1645
- configuring URL
 - authorization for
 - web sites, 1634-1638
- discussed, 1628-1630
- feature delegation, 1640-1642
- remote management, 1639-1640
- NLB (Network Load Balancing)
 - cluster mode and
 - IP address management, 1226
- command-line management, 1227-1228
- logging and credentials, 1227
- port rule management, 1220-1223
- server management, 1223-1226
- printing with Print Management
 - adding print servers, 293
 - adding printers, 294-297
 - allowing users to install printers, 317-318
 - automatic network print addition, 326
 - connecting users to network printers, 309-314
 - custom views, 328-330
 - deploying printers using group policy, 314-317
 - discussed, 290-293
 - installing, 291-292
 - Internet printing, 331-332
 - listing printers in Active Directory, 307-309
 - migrating printers, 319-325
 - notifications, 331
 - print server
 - configuration, 327
 - printer properties, 299-306
 - Server Core, 942-950
 - trust relationships, 747-751
 - Windows Server from
 - client, 1202-1203
- manual certificate requests, 168
- manual updates, 113
- mapping printers, 564-565
- MAV (Microsoft Application Virtualization), 585
- MBR (Master Boot Record), 1349
- media
 - creating domain controllers from, 715-718
 - media Windows Server 2008 installations, 101-105
- media-based deployment, 1063-1064
- Member Of tab
 - computer objects, 803
 - user groups, 800
 - user objects, 794
- Members tab (user groups), 799
- memory
 - counters, 1364
 - detailed memory view (Reliability and Performance interface, Resource View), 1360
- Memory overview (Reliability and Performance interface, Resource View), 1359
- shareable memory size, 1360
- virtual application use of, 1280
- virtual memory
 - commit size, 1360
 - paging files, 1194-1200
- Windows Server 2008
 - installation requirements, 100
 - working set size, 1360
- Memory-Available Bytes counter, 1364
- Memory overview (Reliability and Performance interface, Resource View), 1359
- Memory-Page Faults/sec counter, 1364
- Memory-Pages Input/sec counter, 1364
- Memory-Pages Reads/sec counter, 1364
- Memory-Pages/sec counter, 1364
- Message Queuing, 1114
- metadata cleanups, 770-776
- \$MFT file, 227
- \$MFTMirr file, 227
- Microsoft .NET Framework 3.0, 1113
- Microsoft Disk Operating System (MS-DOS), 1, 1508
- Microsoft Management Console. *See* MMC
- Microsoft Multipath I/O (MPIO), 1114
- Microsoft Network Monitor, 357-361
- Microsoft Software Installer, 1437-1440
- Microsoft Solution Accelerator for Business Desktop Deployment 2007, 1081
- Microsoft update catalog, 1181-1182
- migrating
 - DFS, 959
 - migration logs (MSDSS), 1600-1601
 - printers, 319-325

- VMs (virtual machines)
 - with Hyper-V
 - live migration, 1316-1317
 - Physical-to-Virtual Migration, 1313
 - quick migration, 1313-1316
- from Windows Server 2003
 - failover clustering, 1266-1268
 - NLB (Network Load Balancing), 1229
- migration logs (MSDSS), 1600-1601
- mirrored disks (RAID 1), 231
- mixed domain mode (AD), 672
- mixed mode (UNIX integration services), 1567
- mklink utility, 229
- MMC (Microsoft Management Console), 6
 - Actions pane, 90
 - console tree, 89
 - customized consoles, 90-93
 - Details pane, 90
 - discussed, 86-88
- mobile devices, 868
- Mobile Group Policy
 - template, 1504
- modeling, Group Policy
 - Modeling, 1476-1480
- modems, 381
- modes
 - AD (Active Directory) modes
 - domain modes, 672-674
 - forest modes, 674-677
 - Windows 2000 mode, 675
 - interim mode, 675
 - Windows Server 2003 mode, 675-676
 - Windows Server 2008 mode, 676-677

- cluster modes, 1226
- quorum modes, 1232-1233
 - disk-only, 1235
 - node and disk
 - majority, 1234
 - node and file share
 - majority, 1235
 - node majority, 1233-1234
- Modify permissions, 244
- modules (IIS), 1612-1617
- Monad, 1507
- monitoring networks, 357-361
- monitoring-only mode (NAP), 490
- monitoring section (Windows Firewall), 201
- monolithic hypervisors, 1286
- motherboard TPM chips, 145-146
 - BitLocker configuration, 149
 - enabling, 148
- mount command, 1342, 1590
- mounting WIM files, 1069-1070
- moving
 - disk quotas from one disk to another, 252
- domain controllers, 707
- FSMO roles
 - from command line, 691-692
 - graphically, 687-691
 - seizing roles, 693-694
- paging files, 1197-1199
- MPIO (Microsoft Multipath I/O), 1114
- MS-DOS, 1, 1508
- MSConfig, 1400-1401
- _msdcs zone (DNS), 428
- MSDN keys, 117
- MSDSS (Microsoft Directory Synchronization Services), 1594
 - forward replication, 1596-1597, 1602

- forward synchronization, 1595-1596
- logs
 - migration logs, 1600-1601
 - viewing, 1599
- passwords, 1601-1602
- reverse replication, 1596-1597, 1602
- reverse synchronization, 1595-1596
- msg command, 619
- mstsc.exe (Microsoft Terminal Services Client). *See* RDC (Remote Desktop Connection) tool
- multicast transmissions
 - configuring IP address for, 1039-1040
 - for image-based deployment, 1079-1081
- multithreading, 1509
- Multiuser Group Policy
 - template, 1504

N

- Name Servers tab (zone properties menu), 429
- names
 - conventions, 406
 - DNs (distinguished names), 633
 - DNS (Domain Name System) names, 639
- domains, Windows Server
 - 2008 configurations, 112
- NetBIOS names, 628, 639
- RDNs (relative distinguished names), 633
- server names, configuring in Server Core, 920-921
- workgroups, Windows Server
 - 2008 configurations, 112
- namespace servers, DFSN, 960

- NAP (Network Access Protection), 17, 488
 - architecture of, 491
 - authentication, 510
 - certificate requests, 500-501
 - clients
 - configuring, 508-510
 - notifying, 514
 - deploying, 497
 - deferred enforcement stage, 499
 - Enforcement mode, 500
 - Reporting mode, 499
 - design considerations for using, 498
 - DHCP (Dynamic Host Configuration Protocol)
 - configuring, 510-515
 - quarantine
 - enforcement, 492
 - dynamic VLAN (Virtual Local Area Networks), 494
 - EAP (Extensible Authentication Protocol)
 - quarantine, 494
 - enforcement, configuring, 500-519
 - event logs, 517-519
 - failure pop-up, 513
 - health policies
 - configuring, 502-503
 - enabling checks, 504
 - health updates, 491
 - HRA (Health Registration Authority), 493
 - IPsec (IP Security), 493
 - limited access networks, creating via IP filters, 506
 - monitoring-only mode, 490
 - NAP-incapable policy
 - creation, 507
 - network policies,
 - configuring, 504
 - operational overview, 495
 - PEAP (Protected Extensible Authentication Protocol), 495, 509-510
 - remote access
 - quarantine, 495
 - restrictions, viewing, 517
 - RRAS (Routing and Remote Access Services), configuring, 469
 - SHA (System Health Agents), 489-490, 496
 - SHV (System Health Validators), 489, 496, 501
 - SoH (Statement of Health)
 - messages, 488
 - SoHR (Statements of Health Response) messages, 496
 - troubleshooting, 516
 - 1231 error codes, 515
 - event logs, 517-519
 - TS Gateway
 - enforcement, 495
- napstat command, 513
- NAPT (Network Address Port Translation), 353
- NAT (Network Address Translation), 31, 352-355
 - dynamic NAT, 460
 - PAT, 461
 - static NAT, 460
- navigating
 - Remote Desktop
 - sessions, 536
 - Server Manager, 1087-1092
- Navigation pane (Windows Explorer), 82
- NBP (Network Boot Program), 1025
- NDS (Novell Directory Services)
 - AD synchronization, 1594
 - passwords, 1601-1602
- nesting OU, 780
- .NET Environment, 1617
- .NET Extensibility, 1613
- net share utility, 248
- net stop/start command, starting/stopping NTDS, 827
- net user command, 920
- NetBIOS
 - names, 336, 628, 639
 - WINDS/NBT node type (option 046), 382
- netdom command, 686, 920, 924-925
- netdom trust command, 751
- netsh client show state command, 517
- NETSH command, 477, 921
- netsh command, Windows Firewall configuration, 200-201
- netsh http show ssl command, 474
- netsh.exe command-line tool, 401
- NETSTAT command, 477
- NetWare
 - Client Services for NetWare, 1594
 - DFSN interoperability, 960
 - File Migration Utility, 1603-1604, 1607
 - FPNW (File and Print services for NetWare), 1594
 - MSDSS (Microsoft Directory Synchronization Services), 1594
 - forward replication, 1596-1597, 1602

- forward synchronization, 1595-1596
- reverse replication, 1596-1597, 1602
- reverse synchronization, 1595-1596
- SFU (Services for UNIX), 1593-1594
- Windows Server
 - integration, 1565
- Network Address Port Translation (NAPT), 353
- Network Access Protection (NAP), 17, 488
 - architecture of, 491
 - authentication, 510
 - certificate requests, 500-501
 - clients
 - configuring, 508-510
 - notifying, 514
 - deploying, 497
 - deferred enforcement stage, 499
 - Enforcement mode, 500
 - Reporting mode, 499
 - design considerations for using, 498
 - DHCP (Dynamic Host Configuration Protocol)
 - configuring, 510-512, 515
 - quarantine enforcement, 492
 - dynamic VLAN (Virtual Local Area Networks), 494
 - EAP (Extensible Authentication Protocol)
 - quarantine, 494
 - enforcement, configuring, 500-519
 - event logs, 517-519
 - failure pop-up, 513
 - health policies
 - configuring, 502-503
 - enabling checks, 504
 - health updates, 491
 - HRA (Health Registration Authority), 493
 - IPsec (IP Security), 493
 - limited access networks, creating via IP filters, 506
 - monitoring-only mode, 490
 - NAP-incapable policy creation, 507
 - network policies, configuring, 504
 - operational overview, 495
 - PEAP (Protected Extensible Authentication Protocol), 495, 509-510
 - remote access
 - quarantine, 495
 - restrictions, viewing, 517
 - RRAS (Routing and Remote Access Services), configuring, 469
 - SHA (System Health Agents), 489-490, 496
 - SHV (System Health Validators), 489, 496, 501
 - SoH (Statement of Health) messages, 488
 - SoHR (Statements of Health Response) messages, 496
 - troubleshooting, 516
 - 1231 error codes, 515
 - event logs, 517-519
 - TS Gateway
 - enforcement, 495
- Network Access Protection tab (Properties context menu), scope management, 396
- Network Adapter tab (Terminal Services Configuration MMC snap-in), 616
- network adapters, configuring, 1250
- Network Address Port Translation (NAPT), 353
- Network Address Translation (NAT), 31, 352-353, 355
 - dynamic NAT, 460
 - PAT, 461
 - static NAT, 460
- Network and Sharing Center, 373-376
- Network Boot Program (NBP), 1025
- Network-Bytes Total/Sec counter, 1364
- Network-Current Bandwidth counter, 1364
- Network Device Enrollment Service (ADCS), 159
- Network File System (NFS) servers
 - configuring, 1588-1590
 - file name conversion, 1591
 - installing, 1587
 - Linux connections, 1591
 - sharing, 1590
 - troubleshooting, 1591
- Network Information Service (NIS)
 - AD migration, 1581
 - domains, adding, 1578-1580
 - IdMU, 1574
 - NIS Data Migration Wizard, 1578-1580
 - services, adding, 1578-1580
 - structure of, 1575
 - Web resources, 1581
- Network Level Authentication (NLA), 526-528
- Network Load Balancing (NLB), 1114
 - cluster mode and IP address management, 1226
 - command-line management, 1227-1228

- configuring, 1213
 - additional nodes, 1218
 - clusters, 1215
 - DNS records, 1219
 - host-specific
 - information, 1213
 - port rules, 1215-1217
- discussed, 1205-1206, 1210-1212
- installing, 1213
- logging and credentials, 1227
- NLB clusters, accessing, 1219-1220
- port rule management, 1220-1223
- removing, 1228
- server management, 1223-1226
- Windows Server 2003, migrating from, 1229
- Network Monitor, 357, 359-361
- Network Operating System (NOS), 2
- network overview (Reliability and Performance interface, Resource View), 1359
- Network Policy and Access Services, 1104
- Network Policy Server (NPS)
 - connection request
 - policies, 479
 - health policies, 479
 - network policies, 479
- RADIUS
 - backing up
 - configurations, 486
 - configuring, 478-484
 - logging, 485
- networking
 - ARPANET (Advanced Research Protocol Agency Network), 335
 - boot, F12 key in, 1039
 - communication testing, 368
 - Network and Sharing Center, 373-376
 - pathping command, 372-373
 - ping utility, 368-371
 - tracert command, 371-372
 - connections
 - internal connections, 1294
 - Windows Server 2008
 - configurations, 112
 - DHCP, 377
 - administration, 391-394, 397-400
 - APIPA, 380
 - authorization, 387
 - cable modems, 381
 - DHCPv6 protocol, 386, 401-403
 - DNS configuration, 386
 - DNS domain name
 - (option 015) option, 382
 - DNS secure updates, 405-406
 - DNS server (option 006)
 - option, 382
 - domain controller
 - actions, 388-390
 - DSL modems, 381
 - four-packet structure
 - of, 378
 - installing, 381-383
 - leases, 378, 396-397, 404
 - redundancy, 404-405
 - releasing leases, 380
 - renewing leases, 380
 - scope backups, 401
 - scope configuration, 386, 391-393
 - scope creation, 388, 399
 - scope DHCPv6
 - configuration, 402
 - scope management, 393-394, 397
 - server activation, 390
 - WINS/NBNS servers
 - (option 044) option, 382
 - WINS/NBT node type
 - (option 046) option, 382
- discussed, 29-31
- distribution points, 1437
- DNS
 - ADDS, 427
 - application partitions, 422-424
 - authoritative DNS servers, 410
 - caching in, 443
 - CNAME records, 413
 - conditional forwarders, 440-442
 - Credentials accounts, 425-427
 - delegating in, 434
 - domain creation, 416
 - domain-wide
 - partitions, 423
 - forest-wide partitions, 423
 - forwarders, 439
 - GlobalNames
 - zones, 444-445
 - hierarchy of, 407
 - installing, 411
 - IPv6 support for, 447
 - lookups, 407, 409
 - managing, 412-424
 - _msdcs zones, 428
 - operational overview, 407-409
 - record response
 - behavior, 413, 416
 - reverse lookup zones, 432-434
 - Round Robin functionality, 415-416
 - scavenging, 431

- security, 425-427
- stub zones, 437
- subnet prioritization, 415
- TTL, 410
- zone creation, 417-420
- external networks, 1294
- failover clustering network-
 - ing enhancements,
 - 1236-1237
- Hyper-V network
 - management, 1293
- limited access networks,
 - creating via IP filters
 - (NAP enforcement
 - configuration), 506
- monitoring with Microsoft
Network Monitor,
 - 357-361
- NAT, 460
- NLB (Network Load
Balancing)
 - accessing NLB clusters,
 - 1219-1220
 - cluster mode and
 - IP address
 - management, 1226
- command-line
 - management, 1227-1228
- configuring, 1213-1219
- discussed, 1205-1206,
 - 1210-1212
- installing, 1213
- logging and
 - credentials, 1227
- migrating from Windows
Server 2003, 1229
- port rule management,
 - 1220-1223
- removing, 1228
- server management,
 - 1223-1226
- policies
 - NAP, 504
 - NPS, 479
- printers
 - automatic network print
 - addition, 326
 - connecting users to net-
work printers, 309-314
- private networks, 196, 1295
- public networks, firewall
 - exception behaviors, 196
- services
 - distributed services, 954
 - remote access, 955
- VPN
 - authentication, 454
 - data encryption, 455
 - encapsulation, 454
 - installing, 458
 - L2TP, 456-457
 - NAP, 495-519
 - PPTP, 455-457
 - Remote Access VPN, 452
 - security, 454
 - server configuration,
 - 462-477
 - site-to-site VPN, 453
 - SSTP, 456
- WINS, 447-448
- Networking tab (Task
Manager), 75
- New Replicated Folders
Wizard, 997
- New Rule action (Windows
Firewall Control Panel
applet), 198
- New Technology File System
(NTFS). *See also* File
Server Resource
Manager (FSRM)
 - \$AttrDef file, 227
 - \$BasClus file, 227
 - \$Bitmap file, 227
 - \$Boot file, 227
 - checking version of, 226
 - disk quotas, 273
 - actions, 274-279
 - assigning, 280-284
 - enabling, 250
 - hard quotas, 274
 - importing quota
 - information, 252
 - moving from one disk to
another, 252
 - properties, 275
 - soft quotas, 274
- file ownership, 240-243
- file permissions, 243-247
- file screens
 - active versus passive, 285
 - assigning, 285
 - discussed, 284-285
 - editing, 287
 - exceptions, 287
 - exporting, 288-289
 - importing, 288-289
- \$LogFile file, 227
- \$MFT file, 227
- \$MFTMirr file, 227
- new features of, 20
- \$Quota file, 227
- self-healing NTFS, 228-229
- shares, 248-250
- symbolic links, 228-230
- transaction NTFS, 228
- \$UpCase file, 227
- versions, 227
- \$Volume file, 227
- volumes, Windows Server
 - 2008 installations, 105
- VSS (Volume Shadow Copy
Service), 255-257
- NFS (Network File System)
 - servers
 - configuring, 1588-1590
 - file name conversion, 1591
 - installing, 1587
 - Linux connections, 1591
 - sharing, 1590
 - troubleshooting, 1591
 - nfsshare command, 1590

- NIS (Network Information Service)
 - AD migration, 1581
 - domains, adding, 1578-1580
 - IdMU, 1574
 - NIS Data Migration Wizard, 1578-1580
 - services, adding, 1578-1580
 - structure of, 1575
 - Web resources, 1581
- NLA (Network Level Authentication), 526-528
- NLB (Network Load Balancing), 1114
 - cluster mode and IP address management, 1226
 - command-line management, 1227-1228
 - configuring, 1213
 - additional nodes, 1218
 - clusters, 1215
 - DNS records, 1219
 - host-specific information, 1213
 - port rules, 1215-1217
 - discussed, 1205-1206, 1210-1212
 - installing, 1213
 - logging and credentials, 1227
 - NLB clusters, accessing, 1219-1220
 - port rule management, 1220-1223
 - removing, 1228
 - server management, 1223-1226
 - Windows Server 2003, migrating from, 1229
- nlb command, 1227-1228
- node and disk majority (quorum mode configuration), 1234
- node and file share majority (quorum mode configuration), 1235
- node majority (quorum mode configuration), 1233-1234
- nodes (NLB), adding/removing, 1218
- nonauthoritative restores, 814
- NOS (Network Operating System), 2
- notifications
 - configuring, 262
 - limits of, 263
 - print server failure, sending in event of, 331
- Novell Client for Windows, installing, 1594
- Novell Directory Services (NDS)
 - AD synchronization, 1594
 - passwords, 1601-1602
- NPS (Network Policy Server)
 - connection request policies, 479
 - health policies, 479
 - network policies, 479
- RADIUS
 - backing up configurations, 486
 - configuring, 478-484
 - logging, 485
- nslookup (Name Server Lookup)
 - command, DNS conditional forwarders, 443
 - lookups, 407-409
 - reverse record lookups, 434
- nslookup client, 361
- NT. *See* Windows NT
- NTDS (NT Directory Service)
 - metadata cleanups, 770
 - starting/stopping, 827
- ntdsutil command, 691-692
 - seize option, 693-694
 - snapshots, creating, 822-823
- NTFRS (NT File Replication Service), AD restoration, 817
- NTFS (New Technology File System). *See also* FSRM (File Server Resource Manager)
 - \$AttrDef file, 227
 - \$BasClus file, 227
 - \$Bitmap file, 227
 - \$Boot file, 227
 - checking version of, 226
 - disk quotas, 273
 - actions, 274-279
 - assigning, 280-284
 - enabling, 250
 - hard quotas, 274
 - importing quota information, 252
 - moving from one disk to another, 252
 - properties, 275
 - soft quotas, 274
 - file ownership, 240-243
 - file permissions, 243-247
 - file screens
 - active versus passive, 285
 - assigning, 285
 - discussed, 284-285
 - editing, 287
 - exceptions, 287
 - exporting, 288-289
 - importing, 288-289
 - \$LogFile file, 227
 - \$MFT file, 227
 - \$MFTMirr file, 227
 - new features of, 20
 - \$Quota file, 227
 - self-healing NTFS, 228-229
 - shares, 248-250
 - symbolic links, 228-230
 - transaction NTFS, 228
 - \$UpCase file, 227
 - versions, 227
 - \$Volume file, 227

- volumes, Windows Server
 - 2008 installations, 105
- VSS (Volume Shadow Copy Service), 255-257
- NTLM (NT LAN Manager)
 - authentication, 172-173
- \$null variable, 1544
- NWLink protocol, 1593

O

- OCI (Oracle Call Interface),
 - SUA support for, 1569
- oclist command, 935
- Ocsetup command, 935-936
- ODBC (Open Database Connectivity)
 - logging (IIS), 1614
 - SUA support for, 1569
- Office 2003, RMS-protected documents, 868
- Office 2007
 - RMS-protected documents, 868
 - Word, launching remotely, 590-591
- Online Responder (ADCS), 159
- OOBE (Out of Box Experience), automated Windows Server 2008 installations, 137-138
- Operating System tab (computer objects), 803
- Operational logs (Event Viewer), 1382
- Option Explicit command,
 - WMI calls via VBScript, 1534
- Options tab (CMD.EXE), 1511
- Organization tab (user objects), 794
- organizational units (OUs),
 - 656-657
 - configuring, 781
 - creating, 780
 - delegating permissions, 782, 785-787
 - deleting, 782
 - naming, 780
 - nesting, 780
- OS (Operating Systems)
 - handles, defining, 1334
 - jobs, defining, 1334
 - processes, defining, 1333
 - threads, defining, 1334
 - Windows Server 2008
 - installations, 123, 125
 - license agreements, 124
 - partitions, 125
 - product keys, 124
- OS Loader, boot menu
 - accessing, 1335
- Debugging Mode
 - option, 1337
- Directory Services Restore Mode option, 1337
- Disable automatic restart
 - on system failure option, 1337
- Disable Driver Signature Enforcement
 - option, 1337
- Enable Boot Logging
 - option, 1336
- Enable low-resolution video (640-480) option, 1337
- Last Known Good
 - Configuration option, 1337
- Repair Your Computer
 - option, 1335-1336
- Safe Mode option, 1336
- Safe Mode with Command Prompt option, 1336
- Start Windows Normally
 - option, 1337
- OSI model
 - Data Link layer, 337-339
 - illustration, 337
- OTS (Over the Shoulder)
 - elevation, 54
- OU (organizational units),
 - 656-657
 - configuring, 781
 - creating, 780
 - delegating permissions, 782, 785-787
 - deleting, 782
 - naming, 780
 - nesting, 780
- Out of Box Experience (OOBE), automated Windows Server 2008 installations, 137-138
- Outbound Rules section (Windows Firewall Control Panel applet), 198
- ownership of files, 240-243

P

- P-node (Point to point 0x2)
 - node type, NetBIOS resolution, 382
- PAE (Physical Address Extensions) option (BCDEdit), 1355
- paging files, 1194-1195
 - crash considerations, 1196-1197
 - moving, 1197-1199
 - Server Core, configuring in, 929
 - usage of, viewing, 1199-1200
- Paging File-%Usage
 - counter, 1364
- param statements, PowerShell scripts, 1555-1556
- parent partitions, 1287-1289
- parent-child trust, 743
- partial replication, 627

partitions

- AD partitions, creating in
 - AD LDS instances, 857
- application partitions (DNS), 422-424
- domain-wide partitions,
 - creating in DNS, 423
- encrypting, BitLocker, 144-149, 152-154
- extending, 108
- forest-wide partitions,
 - creating in DNS, 423
- parent partitions, 1287-1289
- Windows RE installations, 1342-1343
- Windows Server 2008 installations
 - configuring, 108
 - existing OS installations, 125
- passive file screens, 285
- passwords
 - Account Lockout Policy, 220-221
 - Administrator accounts,
 - Windows Server 2008 configurations, 109
 - administrator passwords, setting in Server Core, 920
 - Kerberos Policy, 221-222
 - MSDSS, 1601-1602
 - Novell directory services, 1601-1602
- password hashes, 172
- Password Never Expires
 - option (Active Directory Users and Computers MMC snap-in), 790
- Password Policy, 219-220
- Password Settings Container
 - object class, 834-835
- Password Settings object class, 834-835

recovery passwords,

- BitLocker, 154
- RRAS configuration, 467
- storing, RODC (Read-Only Domain Controllers), 144
- UNIX, 1579
 - encryption, 1584
 - synchronizing, 1583-1586
- PAT (Port Address Translation), 461
- patches
 - distributed services, 955
 - managing
 - discussed, 1178-1180
 - group policy configuration, 1180-1181
 - Microsoft update catalog, 1181-1182
 - update options, 1183-1184
 - remote servers, 955
 - Server Core, installing in, 927-928
 - virtual applications, 1281
- pathping command, 372-373
- PC Restores, 1165-1166
- PDC (Primary Domain Controllers), 624
- PDC Emulator
 - FSMO roles, 666-667
 - Master role, 686
- PEAP (Protected Extensible Authentication Protocol), 495, 509-510
- Peer Name Resolution Protocol (PNRP), 1115
- Pending Requests node (Certificates MMC snap-in), 170
- per-device mode (Licensing mode), 551, 554
- per-user mode (Licensing mode), 549

performance

- data collector sets
 - adding data collectors to, 1372-1373
 - backups, 1375
 - Configuration data collectors, 1373
 - configuring data collectors, 1372-1373
 - data collector
 - properties, 1372
 - Directory tab, 1369
 - Event trace data
 - collectors, 1373
 - General tab, 1368
 - LAN Diagnostics, 1367
 - managing data via Data Manager, 1371
 - operational overview, 1375-1376
 - properties of, 1368
 - restoring, 1375
 - saving as templates, 1375
 - Schedule tab, 1370
 - Security tab, 1370
 - Stop Condition tab, 1370
 - System Diagnostics, 1367
 - System Performance, 1367
 - Task tab, 1371
- logs, comparing multiple log files via Performance Monitor, 1377
- Reliability and Performance interface (Server Manager)
- Performance Monitor, 1360-1366, 1377
- Process Explorer, 1380
- Process Monitor, 1380
- Reliability Monitor, 1378
- Resource View, 1357-1358
- system performance
 - benchmarks, 1356
 - Performance tab (Task Manager), 1355

- Performance Log Users
 - security group (Performance Monitor), 1360
- Performance Monitor (Reliability and Performance interface), 1360
- Appearance tab, 1363
- configuring, 1361
- counters
 - adding to, 1363-1364
 - Create New Data Collector Set wizard, 1366
 - saving configured sets of, 1365-1366
- Data tab, 1362
- General tab, 1361
- Graph tab, 1362
- performance logs, comparing
 - multiple log files, 1377
- Source tab, 1361
- Users security group, 1361
- Performance tab (Task Manager), 74, 1355
- Perl option (SUA installations), 1571
- permissions
 - cluster permissions, 1263
 - file permissions, 243-247
 - OU permissions, delegating, 782, 785-787
 - Server Manager
 - permissions, 1151
 - updating, 1445
- physical security, servers, 155
- Physical-to-Virtual
 - Migration (VMs with Hyper-V), 1313
- PhysicalDisk-% Disk Time counter, 1365
- PhysicalDisk-Current Disk Queue Length counter, 1365
- ping utility, 368-371
- PnpUtil command, 1123
- PNRP (Peer Name Resolution Protocol), 1115
- PoC (proof of concept), NAP deployment, 497
- Point-to-Point Tunneling Protocol (PPTP), 455-457, 464, 471
- Policy Module tab (Properties dialog), 169
- Port Address Translation (PAT), 461
- port rules
 - configuring, 1215-1217
 - defined, 1213
 - management, 1220-1223
- Ports tab (printer properties), 300-301
- PowerPoint, RMS-protected documents, 868
- PowerShell, 19, 1536
 - aliases, 1544-1550
 - cmdlets (command-lets), 1537-1540
 - Get-ChildItem, 1544
 - get-itemproperty, 1547
 - get-process, 1550
 - get-psdrive, 1545
 - get-psprovider, 1549
 - get-service, 1552
 - Invoke-Expression, 1552
 - Set-ExecutionPolicy, 1553
 - set-itemproperty, 1547
 - Set-Location, 1545
 - start-service, 1552
 - stop-process, 1551
 - confirm option, 1551-1552
 - error handling, 1559-1563
 - functions, creating, 1544-1545
 - Hello World messages, 1552
 - installing, 1537
- listing running processes
 - in, 1550
- scripts
 - \$args arrays, 1554-1555, 1558
 - AllSigned execution level, 1553
 - comments in, 1554
 - exit statements, 1557
 - functions, 1557-1558
 - Hello World
 - messages, 1552
 - param statements, 1555-1556
 - RemoteSigned execution level, 1553
 - Restricted execution level, 1553
 - Run dialog, 1557
 - running, 1553-1555
 - Unrestricted execution level, 1553
- stopping processes, 1551
- variables, 1540
 - colons (:) in, 1543
 - configuring scope in, 1543-1544
 - .GetType() method, 1542-1543
 - \$null variable, 1544
 - ToUpper() method, 1541
- whatif option, 1551-1552
- WMP (Windows Media Player), stopping, 1552
- PPTP (Point-to-Point Tunneling Protocol), 455-457, 464, 471
- Preboot Execution Environment (PXE), clients, 1011
- boot programs, configuring, 1037
- server response settings, 1036
- WDS communication, 1025

- prestaging computers in Active Directory, 1029-1030
- Preview pane (Windows Explorer), 82
- primary domain controllers (PDC), 624
- Print Services, 1105
- printhrm utility, 320-324
- printing, 28
 - Active Directory, listing in, 307-309
 - adding printers, 294-297
 - allowing users to install, 317-318
 - automatic network print addition, 326
 - connecting users to network printers, 309-314
 - deploying using group policy, 314-317
 - distributed services, 955
 - Internet Printing Client, 1114
 - migrating, 319-325
 - Print Management, 290
 - adding print servers, 293
 - adding printers, 294-297
 - allowing users to install printers, 317-318
 - automatic network print addition, 326
 - configuring print servers, 327
 - connecting users to network printers, 309-314
 - custom views, 328-330
 - deploying printers using group policy, 314-317
 - installing, 291-292
 - Internet printing, 331-332
 - listing printers in Active Directory, 307-309
 - migrating printers, 319-325
 - notifications, 331
 - printer properties, 299-306
 - properties
 - Advanced tab, 301-303
 - General tab, 299
 - Ports tab, 300-301
 - Security tab, 303-306
 - Sharing tab, 299-300
 - remote print servers, managing, 955
 - TS Easy Print, 559
 - drivers, 559-564
 - printer mapping, 564-565
 - private key cryptography, ADCS, 159
 - private networks, 196, 1295
 - privileges, elevation of, 52-56
 - Process Explorer (Reliability and Performance interface), 1380
 - Process Model, 1617
 - Process Monitor (Reliability and Performance interface), 1380
 - processes
 - access tokens, 1333
 - jobs, defining, 1334
 - threads, defining, 1334
 - Processes tab
 - Task Manager, 73-74, 1355
 - TS Manager, 619
 - processor scheduling, 1193
 - Processor-% Processor Time counter, 1365
 - Processor-Interrupts per second counter, 1365
 - processors
 - virtual application use of, 1279
 - Windows Server 2008
 - installation requirements, 100
 - product keys, Windows Server
 - 2008 installations, 103-104, 124
 - Profile tab (user objects), 792-793
 - profiles (roaming), 792
 - Programs tab (RDC tool), 541
 - Promiscuous mode, 358
 - properties
 - disk quotas, 275
 - printer properties
 - Advanced tab, 301-303
 - General tab, 299
 - Ports tab, 300-301
 - Security tab, 303-306
 - Sharing tab, 299-300
 - server properties, customizing, 1035-1041
 - Properties context menu
 - Advanced tab
 - Address Leases leaf, 397
 - Address Pool leaf, 397
 - Reservations leaf, 398
 - scope management, 396
 - DNS tab, scope management, 395
 - General tab, scope management, 395
 - Network Access
 - Protection tab, scope management, 396
 - Properties dialog, Policy Module tab, 169
 - Properties tab (Terminal Services Configuration MMC snap-in), 615
 - Protected Extensible Authentication Protocol (PEAP), 495, 509-510
 - prune and graft
 - functionality, 836
 - public networks, firewall exception behaviors, 196
 - published software, 1437
 - PXE (Preboot Execution Environment)
 - clients, 1011
 - boot programs, configuring, 1037

server response
settings, 1036
WDS communication, 1025

Q

querying event logs (Event Viewer), 1398-1400
quick migration (VMs with Hyper-V), 1313-1316
QuickEdit mode option (CMD.EXE command prompt window), 1511
quorums, 1208
model modification, 1259-1260
modes, 1232
disk-only, 1235
node and disk majority, 1234
node and file share majority, 1235
node majority, 1233-1234
Quota (quota.sys), 261
\$Quota file, 227
quotas (disk)
actions, 274-279
assigning, 280-284
discussed, 273
enabling, 250
hard quotas, 274
importing quota information, 252
moving from one disk to another, 252
properties, 275
soft quotas, 274
qWave (Quality Windows Audio Video Experience), 1115

R

R2 release (Windows 2003), 12-15
RAC (Rights Account Certificates), 867

RADIUS (Remote Authentication Dial In User Service)
authentication, 482
configuring, 478
backing up configurations, 486
defining policy order, 483-484
policy configuration, 479-482
logging, 485
remote server groups, 478
RRAS (Routing and Remote Access Services)
configuration, 463
RAID (Redundant Array of Independent Disks)
RAID 0 (striped disks), 231
RAID 1 (mirrored disks), 231
RAID 5, 231
Windows Server 2008 installation, 100
RAP (Resource Authorization Policy), TS Gateway, 572-575
RDC (Remote Desktop Connection) tool, 529
Advanced tab, 526, 543
b bar, 531
Clipboard sharing, 531
closing sessions, 531-533
Display tab, 537-539
Experience tab, 541-542
full-screen mode, 531
General tab, 537
Local Resources tab, 539-541
Programs tab, 541
RDC (Remote Differential Compression), 1115
cross-file RDC, 968
DFS connection management, 991

RDNs (Relative Distinguished Names), 633
RDOCs (Read-Only Domain Controllers), 19
features, 722-725
installing, 729-740
prerequisites for deployment, 729
restrictions, 726, 729
RDP (Remote Desktop Protocol)
creating, 589
Custom RDP Settings tab (RemoteApp), 588
executing, 589
thin clients, defining, 525
RE (Recovery Environment)
accessing, 1338
BCDEdit, 1353-1355
Boot Repair Your Computer option, 1346
command prompt, 1348-1349
disk access, 1352
driver management, 1351
file access, 1352
installed instances to repair, selecting, 1339
installing, 1340-1345
local server installations, 1340-1345
partitions, installing to, 1342-1343
recovery options, selecting, 1340
services management, 1351
WIM image installations, 1340-1345
Read and execute permissions, 244
Read permissions, 244
Reader access level, 248
realm trust, 747

- rebooting
 - Server Core, 941-942
 - Windows Server 2008, 112
 - recovery
 - deleted user objects, 825
 - keys, BitLocker
 - configuration, 150
 - passwords, BitLocker, 154
 - WSB (Windows Server Backup), 1156-1158
 - PC Restores, 1165-1166
 - system state recovery, 1167-1168
 - Volume Shadow Copy Service (VSS), 1172-1178
 - volume/file/folder recovery, 1168-1170
 - reduced-functionality mode (Windows Vista), 1078-1079
 - redundancy in DHCP, 404-405
 - Redundant Array of Independent Disks (RAID)
 - RAID 0 (striped disks), 231
 - RAID 1 (mirrored disks), 231
 - RAID 5, 231
 - Windows Server 2008
 - installation, 100
 - redundant connection mode, configuring, 766
 - refreshing Group Policy, 1425-1426
 - REG command, 1191-1192
 - .reg files, 1188-1190
 - REG.EXE command, 1351
 - regedit.exe (Registry editor), 1351
 - Registry
 - command-line access, 1190-1192
 - discussed, 1185-1186
 - editing, 1188-1190
 - permissions, updating, 1445
 - .reg files, 1188-1190
 - relative distinguished names (RDNs), 633
 - Reliability and Performance interface (Server Manager)
 - Performance Monitor
 - adding counters to, 1363-1364
 - Appearance tab, 1363
 - comparing multiple performance log files, 1377
 - configuring, 1361
 - Create New Data Collector Set Wizard, 1366
 - Data tab, 1362
 - General tab, 1361
 - Graph tab, 1362
 - Performance Log users security group, 1360
 - Performance Monitor users security group, 1361
 - saving configured counter sets, 1365-1366
 - Source tab, 1361
 - Process Explorer, 1380
 - Process Monitor, 1380
 - Reliability Monitor, 1378
 - Resource View, 1357-1358
 - Remote Access VPN (Virtual Private Networks), 452
 - Remote Assistance, 1115
 - Remote Authentication Dial In User Service (RADIUS)
 - authentication, 482
 - configuring, 478
 - backing up
 - configurations, 486
 - defining policy order, 483-484
 - policy configuration, 479-482
 - logging, 485
 - remote server groups, 478
 - RRAS (Routing and Remote Access Services)
 - configuration, 463
 - Remote Control tab (Active Directory Users and Computers MMC snap-in), 613
 - Remote Desktop, 525
 - Administration mode, 534, 544
 - connections, initiating, 529-535
 - enabling, 529
 - NLA, 526-528
 - RDC tool, 529
 - Advanced tab, 543
 - b bar, 531
 - Clipboard sharing, 531
 - closing sessions, 531-533
 - Display tab, 537-539
 - Experience tab, 541-542
 - full-screen mode, 531
 - General tab, 537
 - Local Resources tab, 539-541
 - Programs tab, 541
 - rules, viewing details of, 528
 - Server Core, configuring in, 932-933
 - Session 0, 532, 536
 - session navigation, 536
 - Terminal Services
 - Configuration MMC, 534
 - Windows Server 2008
 - configurations, enabling in, 116
- Remote Desktop
 - Protocol (RDP)
 - creating, 589
 - Custom RDP Settings tab (RemoteApp), 588

- executing, 589
- thin clients, defining, 525
- Remote Differential
 - Compression (RDC), 1115
 - cross-file RDC, 968
 - DFS connection
 - management, 991
- remote environments
 - client management, 955
 - IIS (Internet Information Services), 1639-1640
 - patches, 955
 - remote access in networking services, 955
 - remote desktops, distributed services, 956
 - remote print servers,
 - managing, 955
 - remote RADIUS server groups, 478
 - remote servers, distributed services, 956
 - Server Core, 942-950
 - server management, 955
 - WinRM, 955
- Remote Installation Services (RIS), 1011
- Remote IPsec Monitor,
 - configuring in Server Core, 943
- Remote Procedure Calls (RPC)
 - over HTTP Proxy, 1115
- Remote Server Administration Tools (RSAT), 1115, 1202-1203
- remote sessions. *See* TS (Terminal Services)
- RemoteApp (Remote Applications), 584
 - Custom RDP Settings tab, 588
 - Digital Signature tab, 588
 - digital signatures, 596
 - distributing applications, 589-593
 - enabling, 585
 - managing, 586
 - Terminal Server tab, 587
 - TS Gateway tab, 587
- RemoteApp Wizard, 585
- RemoteSigned script execution level (PowerShell), 1553
- Removable Storage Manager (RSM), 1115
- Remove Role Wizard, 1112
- REMOVEMEMORY option (BCDEdit), 1355
- removing
 - domain controllers, 719-722, 767, 770-776
 - domains, 719-722, 774-776
 - NLB (Network Load Balancing), 1218, 1228
 - roles, 1112
 - Server Manager
 - features, 1118
 - users from user groups, 801
- renewing leases (DHCP), 380
- repadmin command, 709-710, 861
- Repair Your Computer option (OS Loader, boot menu), 1335
- replica domain controllers
 - adding, 679-683
 - unattended installations, 683-684
- replication
 - AD LDS, 860-861
 - full replication, 626
 - MSDSS, 1596-1597, 1602
 - partial replication, 627
 - urgent replication, 627
- Report and Histogram Data section (Performance Monitor, General tab), 1361
- Reporting mode (NAP deployment), 499
- reports
 - GPO (Group Policy Object) reports, 1464-1465
 - Group Policy Preferences reports, 1500
 - report locations, 264-265
 - running in response to disk quotas, 279
 - storage reports, 264
 - scheduling, 267-273
 - types of reports, 266-267
- Reports node (AD RMS), 888
- request filtering (IIS), 1615
- Request for Comment (RFC) documents, 352
- Request Monitor (IIS), 1614
- Reservations leaf (Properties context menu, Advanced tab), 398
- resource allocation, WSRM (Windows System Resource Manager), 1320-1326
- Resource Authorization Policy (RAP), TS Gateway, 572-575
- Resource View (Reliability and Performance interface), 1357-1358
- Resources and Support section (Server Manager, Terminal Server role page), 615
- restartable directory service, 826-829
- restoring
 - AD
 - authoritative restores, 814, 817
 - DFSR, 817
 - DSRM, 815
 - nonauthoritative restores, 814
 - NTFRS, 817

- AD LDS instances, 863
 - data collector sets, 1375
 - Group Policy, 1488-1490
- Restricted script execution
 - level (PowerShell), 1553
- restrictions
 - group membership
 - restrictions, 1445
 - software restrictions, 1442-1444
- reverse lookup zones (DNS), 432-434
- reverse replication (MSDSS), 1596-1597, 1602
- reverse synchronization (MSDSS), 1595-1596
- RFC (Request for Comment) documents, 352
- RFC 2307 standard, 1576
- RFC 2782, 636
- RID Master FSMO roles, 667, 686
- Rights Account Certificates (RAC), 867
- RIS (Remote Installation Services), 1011
- RMS (Right Management Services), 11
 - AD RMS, 865, 868, 891
 - CLC, 867
 - document access, 866
 - installing, 869-873
 - licensing, 887-890
 - operational overview, 875
 - RAC, 867
 - Reports node, 888
 - restricting access via, 877-881
 - SQL database
 - backups, 889
 - Super User groups, 890
 - template access, enabling, 885-886
 - template creation, 882-884
 - mobile device support, 868
 - Office support for, 868
 - Windows Mobile 6
 - support, 866
- roaming profiles, enabling, 792
- RODC (Read-Only Domain Controller)
 - definition, 19
 - password storage, 144
- Role Services section (Server Manager, Terminal Server role page), 615
- Role Summary, 1093-1099
- roles, 1092
 - AD FS (Active Directory Federation Services), 1102
 - AD LDS (Active Directory Lightweight Directory Services), 1103
 - AD RMS (Active Directory Rights Management Services), 1103
 - ADCS (Active Directory Certificate Services), 1102
 - ADDS (Active Directory Domain Services), 1102
 - Advanced Tools, 1099-1101
 - Application Server, 1103
 - DHCP (Dynamic Host Configuration Protocol) server, 1103
 - DNS server, 1103-1104
 - Fax server, 1104
 - File Services, 1104
 - FSMO (Flexible Single Master Operation) roles, 666
 - best practices, 685-686
 - Domain Naming Master, 669-670, 687
 - GC (Global Catalog) setting, 694-698
 - Infrastructure Master, 668, 686
 - moving from command line, 691-692
 - PDC Emulator Master, 666-667, 686
 - potential problems, 686-687
 - RID Master, 667, 686
 - Schema Master, 668, 687
 - seizing, 693-694
 - transferring graphically, 687-691
- Hyper-V, 1104
- installing, 1106-1112, 1146-1149
- Network Policy and Access Services, 1104
- Print Services, 1105
- removing, 1112
- Role Summary, 1093-1099
- Server Core, configuring in, 934-938
- TS (Terminal Services), 1105
- UDDI (Universal Description, Discovery, and Integration) services, 1105
- Web Server (IIS), 1105
- Windows Deployment Services, 1106
- Windows Server 2008
 - configurations, installing in, 114-115, 123
- root CA (Certificate Authorities), 156
- Round Robin functionality (DNS), 415-416
- route print command, 348
- RPC (Remote Procedure Calls) over HTTP Proxy, 1115
- RRAS (Routing and Remote Access Services)
 - configuring, 459, 462
 - advanced logging, 472
 - Assign Static IP Addresses user property, 470

- Callback user property, 469-470
- connection request
 - authentication, 463
- DHCP (Dynamic Host Configuration Protocol), 463-464
- disabling VPN
 - connectivity, 470
- NAP (Network Access Points), 469
- passwords, 467
- PPTP (Point-to-Point Tunneling Protocol), 464, 471
- RADIUS (Remote Authentication Dial-In Service), 463, 478-486
- security, 467
- SSL (Secure Socket Layer) certificates, 474-476
- SSTP (Secure Socket Tunneling Protocol), 473-477
- troubleshooting, 468-469
- Verify Caller-ID user property, 469-470
- VPN (Virtual Private Networks), 466-469
- NAP (Network Access Points), 488
- 1231 error codes, 515
- architecture of, 491
- authentication, 510
- certificate requests, 500-501
- client configuration, 508-510
- client notification, 514
- configuring, 469
- creating limited
 - access networks via IP filters, 506
- deploying, 497-500
- design considerations
 - for using, 498
- DHCP (Dynamic Host Configuration Protocol) configuration, 510-512, 515
- DHCP (Dynamic Host Configuration Protocol) quarantine enforcement, 492
- dynamic VLAN (Virtual Local Area Networks), 494
- EAP (Extensible Authentication Protocol) quarantine, 494
- enforcement
 - configuration, 500-501, 504-507, 510-512, 515-519
- event logs, 517-519
- failure pop-up, 513
- health policies, 502-504
- health updates, 491
- HRA (Health Registration Authority), 493
- IPsec, 493
- monitoring-only mode, 490
- NAP-incapable policy creation, 507
- network policies, 504
- operational overview, 495
- PEAP (Protected Extensible Authentication Protocol), 495, 509-510
- remote access
 - quarantine, 495
- SHA (Secure Hash Algorithm), 489-490, 496
- SHV (System Health Validators), 489, 496, 501
- SoH (Statement of Health) messages, 488
- SoHR (Statement of Health Request/Response) messages, 496
- troubleshooting, 515-519
- TS Gateway
 - enforcement, 495
 - viewing restrictions, 517
- NAT (Network Address Translation)
 - dynamic NAT, 460
 - PAT (Port Address Translation), 461
 - static NAT, 460
- RADIUS (Remote Authentication Dial-In Service)
 - configuring, 463, 478-486
 - logging, 485
- routing, 486-487
- VPN (Virtual Private Networks)
 - authentication, 454
 - configuring, 466-469
 - data encryption, 455
 - encapsulation, 454
 - installing, 458
 - L2TP (Layer 2 Tunneling Protocol), 456-457
 - PPTP (Point-to-Point Tunneling Protocol), 455-457
 - Remote Access VPN, 452
 - security, 454
 - server configuration, 462-477
 - site-to-site VPN, 453
 - SSTP (Secure Socket Tunneling Protocol), 456
- RSAT (Remote Server Administration Tools), 1115, 1202-1203

RSM (Removable Storage Manager), 1115

Run dialog, PowerShell scripts, 1557

Russinovich, Mark, 22

S

SA (Security Associations)
IPsec SA, 204

ISAKMP (Internet Security Association and Key Management Protocol), 204

SACL (System Access Control Lists), 830

Safe mode (DSRM), 815

Safe Mode with Command Prompt option (OS Loader, boot menu), 1336

Safe Mode with Networking option (OS Loader, boot menu), 1336

saving

counter sets, Performance Monitor (Reliability and Performance interface), 1365-1366

data collector sets as templates, 1375

security policies, SCW (Security Configuration Wizard), 184

sc command, 1138-1139

scaling, TS Gateway, 583

/scanos command, 1349

scavenging (DNS), 431

SCC (Single Copy Cluster), 1210

SCCM (System Center Configuration Manager), 1404, 1183

SCE (System Center Essentials), 1407

Schedule tab (data collector set properties), 1370

scheduling

backups, 1159-1160

processor scheduling, 1193 reports, 267-273

Schema Master FSMO roles, 668, 687

schemas (AD), 637-638

schtasks.exe, 1133-1135

SCOM (System Center Operations Manager), 1403

scope

delegated OU

permissions, 784

user groups, 798

scope (variables), configuring via PowerShell, 1543-1544

scopes (DHCP)

backups, 401

configuring, 386

creating, 388, 399

DHCPv6 configuration, 402

managing, 393-394, 397

option configuration, 391-393

redundant

configurations, 404

screens (file)

active versus passive, 285

assigning, 285

discussed, 284-285

editing, 287

exceptions, 287

exporting, 288-289

importing, 288-289

scregedit.wsf script, 932-933 scripts

FSRM (File Server Resource Manager), 290

PowerShell, 1556

AllSigned script execution level, 1553

\$args arrays, 1554-1555, 1558

comments in, 1554

exit statements, 1557

Hello World

messages, 1552

param statements, 1555-1556

RemoteSigned script execution level, 1553

Restricted script execution level, 1553

Run dialog, 1557

running in, 1553, 1555

Unrestricted script execution level, 1553

scregedit.wsf, 932-933

Slmgr.vbs, 926-927

scrolling through files/folders, CMD.EXE, 1516

SCW (Security Configuration Wizard), 179

analyze feature, 185-186

audit configuration, 184

Configuration Action page, 180

Disable the Service option, 182

firewalls, editing rules, 182

LDAP (Lightweight Data Access Protocol), 182

outbound resource access, 183

outgoing authentication, 183

Registry settings configuration, 182

role-based service configuration, 181

secedit.exe command-line tool, 187, 193-194

Security Configuration and Analysis MMC snap-in, 187-192

security policies, 184

- Security Templates MMC
 - snap-in, 187-189
- SMB (Server Message Block) option, 182
- Viewer, 180, 186
- scwcmd command, converting
 - security policies to GPO, 185
- SDK (software development kits), SUA, 1569
- searches
 - Control Panel, 94
 - DFSN, 977
 - Windows Explorer, 81
- secedit.exe command-line
 - tool, 187, 193-194
- Secure Socket Tunneling Protocol (SSTP), 456, 473-477
- SecureDC option (Security Templates MMC snap-in), 189
- SecureWS option (Security Templates MMC snap-in), 189
- security, 31-32
 - account policies
 - Account Lockout Policy, 220-221
 - Kerberos Policy, 221-222
 - Password Policy, 219-220
 - AD FS (Active Directory Federation Services), 891
 - authentication, 894
 - claim mappings, 903
 - claims-aware agent
 - installation, 897
 - FS (Federation Services), 892
 - FSP (Federation Service Providers), 893
 - installing, 895-901, 904-906
 - operational overview, 893-895
 - troubleshooting, 907-908
 - Web Server SSO Agent, 893
- ADCS (Active Directory Certificate Services), 156
 - autoenrolling certificate templates, 164, 168
 - CA Web enrollment page, 159
 - configuring domain client trust of CA (Certificate Authorities), 160-161
 - enterprise CA (Certificate Authorities), 158
 - installing, 158
 - managing, 162-163
 - NDES (Network Device Enrollment Service), 159
 - Online Responder, 159
 - private key
 - cryptography, 159
 - stand-alone CA (Certificate Authorities), 158
 - Administrator accounts, changing passwords, 109
 - authentication, 142
 - configuring domain methods, 176-178
 - discussed, 32-33
 - Kerberos, 173-176
 - NTLM (NT LAN Manager), 172-173
 - two-factor authentication, 142
- authorization
 - administrator
 - accounts, 143
 - best practices, 143
 - discussed, 32-33
- backups, offsite storage, 144
- CA (Certificate Authorities)
 - changing names of, 159
 - domain client trust, 160-161
 - enterprise CA, 158
 - hierarchy of, 157-158
 - intermediate CA, 157
 - issuing CA, 157
 - issuing certificate templates, 167
 - manual certificate requests, 168
 - root CA, 156
 - stand-alone CA, 158
 - viewing certificates, 169
- certificate templates
 - autoenrollment, 164, 168-170
 - configuring, 165
 - converting, 163
 - issuing, 165-167
 - versions of, 163
- certificates, 170, 1645-1647
- distributed services, 953-954
- DMZ (Demilitarized Zones), 144
- DNS (Domain Name Systems)
 - Credentials accounts, 425-427
 - updates, 405-406
- domain controllers, distributed services, 954
- encryption, 1645-1647
- failover clustering security
 - enhancements, 1236-1237
- firewalls
 - domain exception behaviors, 196
 - private network exception behaviors, 196
 - public network exception behaviors, 196

- Windows Firewall, 117, 196-201
- Windows Firewall with Advanced Security, 195
- groups, 797
- hard disks, wiping, 144
- IE ESC, 210-211
- Internet connections, 144
- IPsec
 - AH, 203
 - authentication, 207
 - Authentication Exemption
 - connection security rule, 208
 - configuring, 203, 209
 - connection security rule, 208
 - encryption, 204
 - ESP protocol, 203
 - IPsec SA, 204
 - Isolation connection
 - security rule, 208
 - key exchange, 204-206
 - server configuration, 204-206
 - Server-to-Server
 - connection security rule, 208
 - Transport mode, 203
 - Tunnel connection
 - security rule, 208
 - Tunnel mode, 203
- laptops, 145
- locked out accounts,
 - unlocking, 222
- partitions, BitLocker
 - encryption, 144-149, 152-154
- passwords
 - Account Lockout Policy, 220-221
 - hashes, 172
 - Kerberos Policy, 221-222
 - Password Policy, 219-220
- RODC (Read-Only Domain Controllers), 144
- policies (SCW), 184
- RMS (Rights Management Services)
 - AD RMS, 865-891
 - mobile device
 - support, 868
 - Office support for, 868
- RRAS (Routing and Remote Access Services)
 - configuration, 467
- SA (Security Association)
 - IPsec, 204
- ISAKMP (Internet Security Association and Key Management Protocol), 204
- SCW (Security Configuration Wizard), 179
 - analyze feature, 185-186
 - audit configuration, 184
 - Configuration Action
 - page, 180
 - Disable the Service
 - option, 182
 - editing firewall rules, 182
 - LDAP (Lightweight Data Access Protocol), 182
 - outbound resource
 - access, 183
 - outgoing
 - authentication, 183
 - policies, 184
 - Registry settings
 - configuration, 182
 - role-based service
 - configuration, 181
 - saving security
 - policies, 184
 - secedit.exe command-line
 - tool, 187, 193-194
- Security Configuration and Analysis MMC snap-in, 187, 190-192
- Security Templates MMC snap-in, 187-189
- SMB (Server Message Block) option, 182
- Viewer, 180, 186
- servers, cold boot
 - attacks, 155
- SUA (Single User Accounts), 1571
- SysKey, 218
- templates
 - GPO, 188
 - group policy
 - integration, 192
- TPM (Trusted Platform Module) chips, 145-146
- BitLocker
 - configuration, 149
 - enabling, 148
- UAC (User Access Control), 213-218
- user accounts, locked-out
 - accounts, 791
- VPN (Virtual Private Networks), 454
- Windows Defender, 209
- Security Identifier (SID), 1012
- Security Layer, Terminal Services Configuration MMC snap-in, General tab), 617-618
- Security logs (Event Viewer), 1382
- Security tab
 - data collector set
 - properties, 1370
 - printer properties, 303-306
 - user groups, 800
- Security Templates MMC snap-in (SCW), 187-189
- seize option (ntdsutil command), 693-694

- self-healing NTFS (New Technology File Systems), 228-229
- self-signed certificates,
 - exporting from TS Web Access, 598
- Server Core, 19, 911-915
 - benefits, 912-913
 - configuring, 918-919
 - administrator password, 920
 - applications, 938-939
 - auto-update, 927-928
 - default scripting engine, 925-926
 - firewalls, 929-931
 - hardware, 933-934
 - international settings, 925
 - joining domains, 924-925
 - pagefiles, 929
 - patches, 927-928
 - Remote Desktop, 932-933
 - roles and features, 934-938
 - server activation, 926-927
 - server name, 920-921
 - static TCP/IP v4
 - information, 921-923
 - time zone, 923-924
 - installing, 915-916
 - limitations, 913
 - logging off, 941-942
 - managing remotely, 942-950
 - rebooting, 941-942
 - systeminfo command, 940
 - tables of roles and features, 914
- Server Core support (IIS), 1648
- Server Manager, 1085-1086.
 - See also* servers
- AD (Active Directory)
 - management tools, accessing, 778
- AD RMS (Active Directory Rights Management Services) installation, 869-873
- ADCS (Active Directory Certificate Services) area
 - Certificate Templates MMC snap-in, 163
 - Enterprise PKI (PKIView) MMC snap-in, 162
- automated role/feature installation, 1146-1149
- command line, 1141-1146
- expanding, 1149-1150
- features
 - installing, 1117-1118
 - list of available features, 1113-1114
 - removing, 1118
 - summary of available features, 1114-1117
- Local Users and Groups snap-in, 1140-1141
- navigating, 1087-1092
- permissions, 1151
- Reliability and Performance interface
 - Performance Monitor, 1360-1366, 1377
 - Process Explorer, 1380
 - Process Monitor, 1380
 - Reliability Monitor, 1378
 - Resource View, 1357-1358
- roles, 1092
 - AD FS (Active Directory Federation Services), 1102
 - AD LDS (Active Directory Lightweight Directory Services), 1103
 - AD RMS (Active Directory Rights Management Services), 1103
- ADCS (Active Directory Certificate Services), 1102
- ADDS (Active Directory Domain Services), 1102
- Advanced Tools, 1099-1101
- Application Server, 1103
- DNS server, 1103-1104
- DHCP (Dynamic Host Configuration Protocol) server, 1103
- Fax server, 1104
- File Services, 1104
- Hyper-V, 1104
- installing, 1106-1112
- Network Policy and Access Services, 1104
- Print Services, 1105
- removing, 1112
- Role Summary, 1093-1099
- TS (Terminal Services), 1105
- UDDI (Universal Description, Discovery, and Integration) services, 1105
- Web Server (IIS), 1105
- Windows Deployment Services, 1106
- server information,
 - viewing, 1119-1123
- Server Summary, 1088
- Services node, 1135-1139
- storage management, 1141
- Task Scheduler
 - command-line access, 1133-1135
 - creating tasks, 1126-1131
 - discussed, 1124-1126
 - managing library, 1126
 - modifying tasks, 1131-1132
 - viewing task execution, 1132

- Terminal Server role
 - page, 615
- TS (Terminal Services)
 - management, 614
- WMI Control, 1139-1140
- Server Manager MMC
 - snap-in, 19
- Server Message Block (SMB)
 - 1.0, 283
- Server Message Block (SMB) 2.0, 284
- Server Side Includes (IIS), 1614
- Server Summary (Server Manager), 1088
- Server-to-Server connection
 - security rule, 208
- servermanagcmd.exe, 1141-1149, 1625
- servers. *See also*
 - Server Manager
 - Application Server, 1103
 - bridgehead servers, 762, 764
 - CA (Certificate Authorities), 156
 - configuring, 1328-1330
 - consolidating, 960
 - customizing properties, 1035-1041
 - DFSN (Distributed File System Namespace)
 - adding to, 974
 - consolidating via, 960
 - namespace servers, 960
 - DFSR (Distributed File System Replication)
 - eligibility, 983
 - DHCP (Dynamic Host Configuration Protocol), 1103
 - Fax server, 1104
 - IPsec configuration, 204-206
 - namespace servers, 960
 - NLB (Network Load Balancing), managing for, 1223-1226
 - patches, 955
 - physical security, cold boot attacks, 155
 - print servers
 - adding, 293
 - configuring, 327
 - records, cleaning up, 774
 - remote environments, managing in, 955
 - remote print servers, managing, 955
 - remote servers, distributed services, 956
 - Server Core, activating in, 926-927
 - server information, viewing, 1119-1123
 - server names, configuring in Server Core, 920-921
 - TCP/IP (Transfer Control Protocol/Internet Protocol), 1115
 - Telnet Server, 1116
 - WINS (Windows Internet Name Service)
 - server, 1117
 - WSRM (Windows System Resource Manager), configuring via, 1328-1330
 - Service Desk (System Center), 1406
 - services
 - directory services, 632.
 - See also* AD (Active Directory)
 - IIS. *See* IIS (Internet Information Services)
 - RMS (Rights Management Services), 11
 - Server Manager, managing with, 1135-1139
 - stateless services, 1205
 - SUS (Software Update Services), 11
 - TS (Terminal Services), 19
 - Windows Deployment Services, 20
 - Windows RE, managing in, 1351
 - WINS (Windows Internet Name Service), 29
 - WSS (Windows SharePoint Services), 12
 - Services for NetWare (SFN), 1593-1594
 - Services node (Server Manager), 1135-1139
 - Services tab
 - MSConfig, 1401
 - Task Manager, 74
 - Session 0, 532, 536
 - Session Broker (TS), 604
 - configuring, 606-609
 - dedicated redirectors, 609
 - deploying, 609
 - Drain mode, 610-611
 - installing, 605
 - Sessions tab (Active Directory Users and Computers MMC snap-in), 612
 - set command (CMD.EXE), 1519, 1522
 - Set-ExecutionPolicy cmdlet, 1553
 - set-itemproperty cmdlet, 1547
 - Set-Location cmdlet, 1545
 - Setup logs (Event Viewer), 1382
 - SFN (Services for NetWare), 1593-1594
 - SHA (System Health Agents), 489-490, 496
 - shadow copy feature, 255-257
 - shareable memory size (memory), 1360
 - shares, 248-250
 - Sharing tab (printer properties), 299-300
 - shortcut trust, 745-746

- showmount command, 1591
- shutdown command, 941
- SHV (System Health Validators),
 - 489, 496, 501
- SID (Security Identifier), 1012
- Sidebar, 61-64
- signatures (digital), 596
- Simple Network Management Protocol (SNMP), 1116
- single address NAT (Network Address Translation), 353
- single copy cluster (SCC), 1210
- single-time backups, 1161-1164
- SIS (Single Instance Storage), 1020-1021
- Site Bindings dialog, 1647
- site connectivity,
 - customizing, 753
 - ADLB tool, 765
 - core site link attributes, 755-757
 - redundant connection mode, 766
 - site topologies, managing, 758-764
- site links
 - bridgehead servers, 762-764
 - bridging, 760
 - configuring, 758
 - core site links
 - connected via link attribute, 755
 - cost attribute, 755-756, 759
 - replication interval attribute, 757-759
 - creating, 758
- site-local addresses, 367
- site-to-site VPN (Virtual Private Networks), 453
- site topologies, managing, 758-764
- sites (AD), 657-666
- Simgvbs script, 926-927
- slow links, detecting, 1426-1427
- SMB (Server Message Block) 1.0, 283
- SMB (Server Message Block) 2.0, 284
- SMB (Server Message Block) option (SCW), 182
- snapshots
 - AD, 822-825
 - creating, 822-823
 - mounting, 823-825
 - VMs (virtual machines) with Hyper-V, 1310-1311
- SNMP (Simple Network Management Protocol), 1116
- soft quotas, 274
- SoftGrid, 36
 - architecture of, 1273-1276
 - TS (Terminal Services), 585
- Software Assurance, 15
- software
 - deploying, 1436
 - assigned software, 1437
 - Microsoft Software Installer, 1437-1440
 - network distribution points, 1437
 - published software, 1437
 - ZAP files, 1440-1442
 - restrictions, 1442-1444
- Software Installer, 1437-1440
- Software Update Services (SUS), 11
- SoH (Statement of Health) messages, 488
- SoHR (Statement of Health Response) messages, 496
- Source tab (Performance Monitor), 1361
- spanned disks, 231
- SQL database backups, 889
- srmhost.exe (SrmReports), 261
- SrmReports (srmhost.exe), 261
- SrmSvc (srmsvc.dll), 261
- SSL (Secure Socket Layer) certificates, RRAS
 - configuration, 474-476
 - port customization, AD LDS, 856
- SSTP (Secure Socket Tunneling Protocol), 456, 473-477
- stacking in Windows Explorer, 84-85
- stand-alone CA (Certificate Authorities), 158
- Standard edition (Windows Server 2008), 21, 1309
- Start menu, 57-59
- Start of Authority tab (Zone Properties menu), 429
- Start Windows Normally option (OS Loader, boot menu), 1337
- start-service cmdlet, 1552
- Starter GPOs (Group Policy Objects) application, 1460-1463
- stateful mode (DHCPv6), 402
- stateless mode (DHCPv6), 402
- stateless services, 1205
- Statement of Health (SoH) messages, 488
- Statement of Health Response (SoHR) messages, 496
- static content (IIS), 1613
- static content compression (IIS), 1615
- static NAT (Network Address Translation), 353, 460
- static routing, RRAS (Routing and Remote Access Services), 487
- Stop Condition tab (data collector set properties), 1370
- stop-process cmdlet, 1551

- storage
 - data storage, 23-26
 - distributed storage, 26-28
 - managing, 1141
- Storage Manager for Storage Area Networks (SANs), 1116
- storage reports, 264
 - scheduling, 267-273
 - types of reports, 266-267
- storing
 - backups, security, 144
 - passwords, RODC (Read-Only Domain Controllers), 144
- storrep.exe, 288
- striped disks (RAID 0), 231
- stub zones (DNS), 437
- SUA (Subsystem for UNIX-based Applications), 1116
 - installing, 1569
 - Base SDK (Software Development Kit) option, 1570
 - Base Utilities option, 1570
 - GNU SDK option, 1570
 - GNU Utilities option, 1570
 - OCI (Oracle Call Interface) support, 1569
 - ODBC (Open Database Connectivity) support, 1569
 - Perl option, 1571
 - SVR-5 Utilities option, 1570
 - Visual Studio Debugger Add-in option, 1571
 - mixed mode, 1567
 - SDK (Software Development Kits), 1569
 - security, 1571

- shell configuration, 1572-1573
- subnet masks, 339-344
- subnet prioritization, DNS, 415
- subnet-calculator.com
 - web site, 342
- subscriptions (events), 1389-1392, 1395-1397
- Subsystem for UNIX-based Applications (SUA), 1116
- Summary section (Server Manager, Terminal Server role page), 615
- Super User groups, AD RMS, 890
- SUS (Software Update Services), 11
- SVR-5 Utilities option (SUA installations), 1570
- switching users, 77-78
- symbolic links, 228-230
- symmetric keys, certificate
 - template autoenrollment, 170
- symmetric multitasking, 1509
- synchronization
 - AD (Active Directory), 1594
 - MSDSS (Microsoft Directory Synchronization Services), 1594-1596
 - UNIX AD mapping, 1575
 - UNIX passwords, 1583-1586
- synchronous application (Group Policy), 1421-1425
- SysKey, 218
- SYSprep tool, 1013-1017
- System Access Control Lists (SACL), 830
- System Center
 - Capacity Planner, 1406
 - Desktop Error Monitoring, 37

- DPM (Data Protection Manager), 1405
- SCCM (System Center Configuration Manager), 1082-1083, 1183, 1404
- SCE (System Center Essentials), 1407
- SCOM (System Center Operations Manager), 1403
- Service Desk, 1406
- VMM (Virtual Machine Manager), 1406
- System Diagnostics data collector sets, 1367
- System Health Agents (SHA), 489-490, 496
- System Health reports (AD RMS), 888
- System Health Validators (SHV), 489, 496, 501
- System logs (Event Viewer), 1382
- System Management Server OS Deployment Feature Pack, 1016
- System Performance data collector sets, 1367
- system state
 - backing up, 1164
 - recovering, 1167-1168
- system tray, 61
- System-Processor Queue Length counter, 1365
- systeminfo command, 940
- SYSVOL (System Volume), replicating, 843-848

T

- Tab key, CMD.EXE
 - functions, 1516
- takeown utility, 242-243
- Task Manager
 - Applications tab, 71-72
 - discussed, 71

- Networking tab, 75
- Performance tab, 74, 1355
- Processes tab, 73-74, 1355
- Services tab, 74
- Users tab, 76-77
- Task Scheduler, 1124-1125
 - command-line access, 1133-1135
 - library management, 1126
 - tasks
 - creating, 1126-1131
 - exporting, 1132
 - importing, 1132
 - modifying, 1131-1132
 - stopping execution of, 1132
 - viewing execution of, 1132
- Task tab (data collector set properties), 1371
- Taskbar, 60-61
- TaskStation Group Policy template, 1504
- tattooing the system, 1409
- TCP (Transmission Control Protocol), 355-356
- TCP/IP (Transmission Control Protocol/Internet Protocol), 1115
 - IP (Internet Protocol), 335-336
 - automatic private IP addressing, 351-352
 - communication testing, 368-376
 - gateway configuration, 349-350
 - IP addresses, 345-349
 - IPv4 limitations, 350-351
 - IPv6, 362-368
 - MAC addresses, 337-339
 - NAT (Network Address Translation), 352-355
 - subnet masks, 339-344
 - network monitoring with
 - Microsoft Network Monitor, 357-361
 - Server Core, configuring in, 921-923
 - TCP (Transmission Control Protocol), 355-356
 - UDP (User Datagram Protocol), 356-357
- Telephones tab (user objects), 793
- Telnet Client, 1116
- Telnet Server, 1116
- templates
 - AD RMS (Active Directory Rights Management Services)
 - creating, 882-884
 - enabling client access, 885-886
 - Group Policy templates, 1503-1504
 - saving data collector sets as, 1375
- Terminal Server role page (Server Manager), 615
- Terminal Server tab (RemoteApp), 587
- Terminal Services (TS), 19, 1105
 - Active Directory Users and Computers
 - MMC snap-in
 - Environment tab, 612
 - Remote Control tab, 613
 - Sessions tab, 612
 - Terminal Services Profile tab, 613
 - application installations, 585
 - benefits of, 522-523
 - configuring, 615-616
 - installing, 558
 - licensing, 544
 - backups, 557
 - changing Discovery mode, 554-556
 - Install Licenses Wizard, 546
 - license installation, 547
 - Licensing mode
 - configuration, 548-554
 - managing, 546
 - troubleshooting, 556
 - TS Licensing
 - installation, 545
 - managing, 618
 - command-line, 619
 - group policies, 620
 - Processes tab, 619
 - Server Manager, 614
 - Users tab, 619
 - Remote Desktop, 525
 - enabling, 529
 - initiating connections, 529-535
 - NLA, 526-528
 - RDC tool, 529-533, 537-543
 - Remote Desktop for Administration mode, 534, 544
 - Session 0, 532, 536
 - session navigation, 536
 - Terminal Services
 - Configuration MMC, 534
 - viewing rule details, 528
 - RemoteApp, 584
 - Custom RDP Settings tab, 588
 - Digital Signature tab, 588
 - digital signatures, 596
 - distributing applications, 589-593
 - enabling, 585
 - managing, 586

- Terminal Server tab, 587
- TS Gateway tab, 587
- thin clients, defining, 525
- TS Easy Print
 - drivers, 559-561, 564
 - printer mapping, 564-565
- TS Gateway, 566-567
 - certificate management, 576-577
 - installing, 568-569
 - managing, 581-582
 - monitoring, 581-582
 - scaling, 583
 - server connections, 579-580
 - single sign-ons via, 603
 - TS CAP, 570-571, 575
 - TS RAP, 572- 575
- TS Session Broker, 604
 - configuring, 606-609
 - dedicated redirectors, 609
 - deploying, 609
 - Drain mode, 610-611
 - installing, 605
- TS Web Access, 597
 - Administration page, 594
 - digital signatures in, 596
 - exporting self-signed certificates, 598
 - granting user logon rights to TS, 600
 - installing, 594
 - secure access to, 598
 - single sign-ons via, 601-602
 - Web access, 597
- Terminal Services
 - Configuration MMC (Microsoft Management Console) snap-in, 534
 - Client Settings tab, 615
 - General tab, Security Layer, 617-618
 - Log on Settings tab, 616
 - Network Adapter tab, 616
 - Properties tab, 615
- Terminal Services Profile tab
 - (Active Directory Users and Computers MMC snap-in), 613
- text, changing font size in
 - CMD.EXE command prompt window, 1511
- TFTP (Trivial File Transfer Protocol) Client, 1116
- thin clients, defining, 525
- threads, defining, 1334
- thunking, 1509
- Time to Live (TTL), 355
- time zones, configuring
 - Server Core, 923-924
 - Windows Server 2008 configurations, 110
- Tools tab (MSConfig), 1401
- topologies, replicating via
 - DFSR (Distributed File System Replication)
- ToUpper() method, 1541
- TPM (Trusted Platform Module) chips, 145-146
 - BitLocker configuration, 149
 - enabling, 148
- tracert command, 371-372
- Tracing (IIS), 1614
- transaction NTFS, 228
- transfer command, 691
- transferring FSMO roles
 - command-line, 691-692
 - graphically, 687-691
- Transmission Control Protocol (TCP), 355-356
- Transmission Control Protocol/Internet Protocol (TCP/IP), 1115
 - IP (Internet Protocol), 335-336
 - automatic private IP addressing, 351-352
 - communication testing, 368-376
 - gateway configuration, 349-350
 - IP addresses, 345-349
 - IPv4 limitations, 350-351
 - IPv6, 362-368
 - MAC addresses, 337-339
 - NAT (Network Address Translation), 352-355
 - subnet masks, 339-344
 - network monitoring with Microsoft Network Monitor, 357-361
 - Server Core, configuring in, 921-923
 - TCP (Transmission Control Protocol), 355-356
 - UDP (User Datagram Protocol), 356-357
- Transport mode (IPsec), 203
- tree-root trust, 744
- trees (AD), 651-652
- Trivial File Transfer Protocol (TFTP) Client, 1116
- troubleshooting
 - AD FS (Active Directory Federation Services), 907-908
 - AD LDS (Active Directory Lightweight Directory Services), replication, 861
 - BCD (Boot Configuration Data), automatic repairs, 1350
 - boot menu (OS Loader)
 - accessing, 1335
 - Debugging Mode option, 1337
 - Directory Services Restore Mode option, 1337
 - Disable automatic restart on system failure option, 1337

- Disable Driver
 - Signature Enforcement option, 1337
- Enable Boot Logging option, 1336
- Enable low-resolution video (640-480) option, 1337
- Last Known Good
 - Configuration option, 1337
- Repair Your Computer option, 1335
- Safe Mode option, 1336
- Safe Mode with Command Prompt option, 1336
- Safe Mode with Networking option, 1336
- Start Windows Normally option, 1337
- data collector sets
 - adding data collectors to, 1372-1373
 - backups, 1375
 - Configuration data collectors, 1373
 - configuring data collectors, 1372-1373
 - data collector
 - properties, 1372
 - Directory tab, 1369
 - Event trace data collectors, 1373
 - General tab, 1368
 - LAN Diagnostics, 1367
 - managing data via Data Manager, 1371
 - operational overview, 1375-1376
 - properties of, 1368
 - restoring, 1375
 - saving as templates, 1375
 - Schedule tab, 1370
 - Security tab, 1370
 - Stop Condition tab, 1370
 - System Diagnostics, 1367
 - System Performance, 1367
 - Task tab, 1371
- DFS (Distributed File Systems), 999-1001, 1004-1007
- Event Viewer
 - accessing, 1381
 - Admin logs, 1382
 - Analytic logs, 1382
 - Application logs, 1382
 - Applications and Services log area, 1382
 - Custom Views, 1386-1389
 - customizing, 1385-1389
 - Debug logs, 1382
 - event filtering, 1385-1389
 - event logs, 1383-1385, 1397-1399
 - event subscriptions, 1389-1397
 - Forwarded Events logs, 1382
 - Operational logs, 1382
 - Security logs, 1382
 - Setup logs, 1382
 - System logs, 1382
 - wevutil.exe command-line interface, 1397-1400
 - Windows Logs node, 1382
- Group Policy, 1501-1502
- MSConfig, 1400-1401
- NAP (Network Access Protection), 516
 - 1231 error codes, 515
 - event logs, 517-519
- NFS (Network File System) servers, 1591
- performance
 - benchmarks, 1356
- Reliability and Performance interface (Server Manager)
 - Performance Monitor, 1360-1366, 1377
 - Process Explorer, 1380
 - Process Monitor, 1380
 - Reliability Monitor, 1378
 - Resource View, 1357-1358
- RRAS (Routing and Remote Access Services) configuration, 468-469
- System Center
 - Capacity Planner, 1406
 - DPM (Data Protection Manager), 1405
 - SCCM (System Center Configuration Manager), 1404
 - SCE (System Center Essentials), 1407
 - SCOM (System Center Operations Manager), 1403
 - Service Desk, 1406
 - VMM (Virtual Machine Manager), 1406
- Task Manager, Performance tab, 1355
- TS licensing, 556
- VPN (Virtual Private Network) server configuration, 468-469
- WER (Windows Error Reporting), 1401
- Windows RE
 - accessing, 1338
 - BCDEdit, 1353, 1355
 - Boot Repair Your Computer option, 1346
 - bootrec command, 1349
 - command prompt, 1348-1349
 - disk access, 1352

- driver management, 1351
- file access, 1352
- installing, 1340-1345
- local server installations, 1340-1345
- partition installations, 1342-1343
- selecting installed instances to repair, 1339
- selecting recovery options, 1340
- services management, 1351
- WIM image installations, 1340-1345
- Windows Server 2008
 - installations, viewing log files, 131-133
- Troubleshooting reports (AD RMS), 888
- trust relationships, 740-742
 - external trust, 747
 - forest trust, 744-745
 - managing, 747-751
 - parent-child trust, 743
 - realm trust, 747
 - shortcut trust, 745-746
 - tree-root trust, 744
- trusts, benefits of, 630-632
- TS (Terminal Services), 19, 1105
 - Active Directory Users and Computers
 - MMC snap-in
 - Environment tab, 612
 - Remote Control tab, 613
 - Sessions tab, 612
 - Terminal Services Profile tab, 613
 - application installations, 585
 - benefits of, 522-523
 - configuring, 615-616
 - installing, 558
 - licensing, 544
 - backups, 557
 - changing Discovery mode, 554-556
 - Install Licenses Wizard, 546
 - license installation, 547
 - Licensing mode configuration, 548-554
 - managing, 546
 - troubleshooting, 556
 - TS Licensing installation, 545
 - managing, 618
 - command-line, 619
 - group policies, 620
 - Processes tab, 619
 - Server Manager, 614
 - Users tab, 619
 - Remote Desktop, 525
 - enabling, 529
 - initiating connections, 529-535
 - NLA, 526-528
 - RDC tool, 529-533, 537-543
 - Remote Desktop for Administration mode, 534, 544
 - Session 0, 532, 536
 - session navigation, 536
 - Terminal Services
 - Configuration MMC, 534
 - viewing rule details, 528
 - RemoteApp, 584
 - Custom RDP Settings tab, 588
 - Digital Signature tab, 588
 - digital signatures, 596
 - distributing applications, 589-593
 - enabling, 585
 - managing, 586
 - Terminal Server tab, 587
 - TS Gateway tab, 587
 - thin clients, defining, 525
 - TS Easy Print
 - drivers, 559-561, 564
 - printer mapping, 564-565
 - TS Gateway, 566-567
 - certificate management, 576-577
 - installing, 568-569
 - managing, 581-582
 - monitoring, 581-582
 - scaling, 583
 - server connections, 579-580
 - single sign-ons via, 603
 - TS CAP, 570-571, 575
 - TS RAP, 572- 575
 - TS Session Broker, 604
 - configuring, 606-609
 - dedicated redirectors, 609
 - deploying, 609
 - Drain mode, 610-611
 - installing, 605
 - TS Web Access, 597
 - Administration page, 594
 - digital signatures in, 596
 - exporting self-signed certificates, 598
 - granting user logon rights to TS, 600
 - installing, 594
 - secure access to, 598
 - single sign-ons via, 601-602
 - Web access, 597
- TS CAP (Connection Authorization Policy), 570-571, 575
- TS RAP (Resource Authorization Policy), 572-573, 575

TTL (Time to Live), 355, 410
Tunnel connection security
 rule, 208
Tunnel mode (IPsec), 203
tunneling protocols
 L2TP (Layer 2 Tunneling
 Protocol), 456-457
 PPTP (Point-to-Point
 Tunneling Protocol),
 455-457, 464, 471
 SSTP (Secure Socket
 Tunneling Protocol),
 456, 473-477
turning on/off
 BitLocker, 204
 Windows Firewall, 201
two-factor authentication, 142

U

UAC (User Access Control),
 213-218
 administrator accounts
 elevation of privilege,
 52-56
 when to use, 50-52
 benefits of, 50
UDDI (Universal
 Description, Discovery,
 and Integration)
 services, 1105
UDP (User Datagram
 Protocol), 356-357
umount command, 1591
unattend.xml files, 918
unattended domain controller
 installations, 683-684
unique local addresses, 367
universal group membership
 caches, 697-698
UNIX
 AD mapping, 1575
 case sensitivity, 1572
 IdMU, 1574-1577
 integration services, 1566
 database
 connectivity, 1569
 mixed mode, 1567
 porting applications, 1568
 SUA, 1567-1573
 LDAP Authentication
 servers, 1592
 NFS servers
 configuring, 1588-1590
 installing, 1587
 share configuration, 1590
 troubleshooting, 1591
 NIS
 AD migration, 1581
 adding domains,
 1578-1580
 adding services, 1578-1580
 IdMU, 1574
 NIS Data Migration
 Wizard, 1578-1580
 structure of, 1575
 Web resources, 1581
 passwords, 1579
 encryption, 1584
 synchronizing, 1583-1586
 unknown clients, authorizing,
 1030-1035
 Unlock Account option
 (user objects, Account
 tab), 792
 unlocking locked out
 accounts, 222, 791
 Unrestricted script execution
 level (PowerShell), 1553
 \$UpCase file, 227
 updates
 DNS, secure updates,
 405-406
 health updates, NAP, 491
 patches, 1183-1184
 permissions, 1445
 WIM files, 1070-1073
 Windows Server 2008
 configurations, 113-114
 \$UPGRADE.~OS folders,
 Windows Server 2008
 upgrades, 129
 upgrades
 AD, 836-843
 Anytime Upgrade, 1016
 DFSN, Windows Server
 2008 mode, 998
 from Windows Server 2003.
 See migrating from
 Windows Server 2003
 Windows Server 2008, 126
 boot folders, 129
 compatibility reports,
 128-129
 domain controllers, 127
 \$DRVLTR\$ files, 130
 \$UPGRADE.~OS
 folders, 129
 \$WINDOWS.~BT
 folders, 129
 \$WINDOWS.~LS
 folders, 129
 \$WINDOWS.~Q
 folders, 130
 urgent replication, 627
 URL authorization, 1615,
 1634-1638
 USB keys, BitLocker
 configuration, 150
 User Access Control (UAC),
 213-218
 administrator accounts
 elevation of
 privilege, 52-56
 when to use, 50-52
 benefits of, 50
 user accounts
 creating, 788
 locked-out accounts, 791
 managing via command
 line, 796

- user authentication, 142
- User Cannot Change Password
 - option (Active Directory Users and Computers MMC snap-in), 789
- user containers, 780
- User Datagram Protocol (UDP), 356-357
- user groups
 - Attribute Editor tab, 801
 - creating, 799
 - distribution groups, 797
 - domain local groups, 797-799
 - global groups, 797
 - Managed By tab, 800
 - Member Of tab, 800
 - Members tab, 799
 - removing users from, 801
 - scope of, 798
 - security groups, 797
 - Security tab, 800
 - universal groups, 797-799
- user logon rights, granting
 - to TS via TS Web Access, 600
- User Must Change Password at Next Logon option (Active Directory Users and Computers MMC snap-in), 788
- user objects
 - Account tab, 790
 - Account Options area, 792
 - Logon Hours option, 791
 - Unlock Account option, 792
 - Address tab, 790
 - COM+ tab, 794
 - deleted objects, recovering, 825
 - deleting, 815
 - General tab, 790
 - Member Of tab, 794

- Organization tab, 794
- Profile tab, 792-793
- Telephones tab, 793

users

- elevation of privileges, 52-56
- printers
 - installing, 317-318
 - network connections, 309-314
- switching, 77-78

user containers, 780

Users tab

- Task Manager, 76-77
- TS Manager, 619

V

validating cluster configurations, 1245-1247

VAMT (Volume Activation Management Tool), MAK, 120

variables

- CMD.EXE environment variables, 1519, 1522
- PowerShell, 1540
 - colons (:) in, 1543
 - .GetType() method, 1542-1543
 - \$null variable, 1544
 - scope, configuring in, 1543-1544
 - ToUpper() method, 1541

VBScript

- arguments, 1531
- comments, 1531
- Hello World messages, 1529-1530
- WMI calls, 1532-1536
- Wscript.Arguments()
 - array, 1531
- Wscript.Quit()
 - function, 1531

Verify Caller-ID user property, RRAS configuration, 469-470

verifying domain controller operation, 705-715

VHD (Virtual Hard Disk) files, 1154, 1303-1304

vhdmount.exe, 1303

video, Enable low-resolution video (640-480) option (OS Loader, Boot menu), 1337

Viewer (SCW), 180, 186

viewing

- local policies, 1417-1421
- page file usage, 1199-1200
- server information, 1119-1123
- task execution, 1132

Virtual Machine Manager (VMM), 1284-1285, 1406

virtual machines. *See* virtualization; VMs (virtual machines) with Hyper-V

virtual memory

- commit size, 1360
- paging files, 1194-1195
 - crash considerations, 1196-1197
 - moving, 1197-1199
- viewing usage of, 1199-1200

virtualization. *See also* TS (Terminal Services)

- advantages, 1330
- discussed, 38-41, 1271-1272
- MAV, TS, 585
- virtual applications
 - advantages of, 1272-1273, 1281-1283
 - application virtualization process, 1277-1278
 - caching, 1279
 - creating, 1276-1277
 - loading, 1279

- memory use, 1280
 - patching, 1281
 - processor use, 1279
 - SoftGrid architecture, 1273-1276
 - VMs (virtual machines) with
 - Hyper-V, 1283
 - advanced management, 1317-1318
 - command-line
 - management, 1311-1313
 - hosted VMM (Virtual Machine Manager), 1284-1285
 - Hyper-V configuration, 1294-1295
 - Hyper-V installation, 1291-1292
 - Hyper-V on laptops, 1318-1319
 - Hyper-V overview, 1289-1291
 - Hypervisor Virtualization technology, 1285-1287
 - licensing, 1309-1310
 - live migration, 1316-1317
 - network
 - management, 1293
 - parent partitions, 1287-1289
 - Physical-to-Virtual Migration, 1313
 - quick migration, 1313-1316
 - snapshots, 1310-1311
 - VM configuration, 1299-11306
 - VM controls, 1306-1309
 - VM creation, 1296-1299
 - Windows Server 2008
 - installations, 99
 - WSRM (Windows System Resource Manager)
 - accounting, 1327-1328
 - conditions, 1327
 - discussed, 1319-1320
 - resource allocation
 - policies, 1320-1326
 - server configuration, 1328-1330
 - Vista. *See* Windows Vista
 - visual effects, 1192-1193
 - Visual Studio Debugger Add-in
 - option (SUA installations), 1571
 - VLAN (Virtual Local Area Networks), dynamic
 - VLAN, 494
 - VMM (Virtual Machine Manager), 1284-1285, 1406
 - \$Volume file, 227
 - Volume Shadow Copy
 - Service (VSS), 255-257, 1172-1178
 - volumes, recovering, 1168-1170
 - VPN (Virtual Private Networks)
 - authentication, 454
 - data encryption, 455
 - encapsulation, 454
 - installing, 458
 - L2TP, 456-457
 - NAP
 - certificate requests, 500-501
 - deploying, 497-500
 - design considerations for using, 498
 - enforcement configuration, 500-501, 504-507, 510-512, 515-519
 - operational overview, 495
 - PEAP, 495
 - PPTP, 455-457
 - Remote Access VPN, 452
 - security, 454
 - server configuration, 462
 - advanced logging, 472
 - Assign Static IP Addresses
 - user property, 470
 - Callback user property, 469-470
 - connection request
 - authentication, 463
 - connection selection, 466
 - DHCP address
 - requests, 463
 - disabling VPN
 - connectivity, 470
 - initialization, 468-469
 - NAP, 469
 - passwords, 467
 - PPTP, 464, 471
 - security, 467
 - SSL certificates, 474-476
 - SSTP, 473-477
 - troubleshooting, 468-469
 - Verify Caller-ID user
 - property, 469-470
 - site-to-site VPN, 453
 - SSTP, 456
 - VSS (Volume Shadow Copy Service), 255-257, 1172-1178
 - vssadmin utility, create shadow parameters, 256
- ## W
- WAIK (Windows Automated Installation Kit), 12, 133, 138-139, 1017
 - answer files, 1052-1058
 - installing, 1052
 - WAS (Windows Process Activation Service), 1116, 1616
 - WAS-Config-APIs module (IIS), 1617
 - WAS module (IIS), 1616

- WAS-NET-Environment module (IIS), 1617
- WAS-Process-Model module (IIS), 1617
- wbadmin command, 1160, 1164, 1167-1172
- WBB (Windows Server Backup), 1117
- WDS (Windows Deployment Services), 20, 1106. *See also* deployment
 - authorizing, 1041
 - configuring, 1019-1026
 - authorizing unknown clients, 1030-1035
 - DHCP options, 1027-1028
 - from command line, 1028
 - prestaging computers in Active Directory, 1029-1030
 - server customization, 1035-1041
- image management in, 1044-1048
- installing, 1017-1019
- PXE client communication with, 1025
- WDSUTIL tool, 1028, 1047
- Web Access (TS), 597
 - Administration page, 594
 - digital signatures in, 596
 - installing, 594
 - secure access to, 598
 - self-signed certificates, exporting, 598
 - single sign-ons via, 601-602
 - user logon rights to TS, granting, 600
- Web-App-Dev module (IIS), 1613
- Web-ASP module (IIS), 1613
- Web-ASP-NET module (IIS), 1613
- Web-Basic-Auth module (IIS), 1614
- Web-Cert-Auth module (IIS), 1615
- Web-CGI module (IIS), 1613
- Web-Client-Auth module (IIS), 1615
- Web-Common-Http module (IIS), 1612
- Web-Custom-Logging module (IIS), 1614
- Web-Default-Doc module (IIS), 1613
- Web-Digest-Auth module (IIS), 1615
- Web-Dir-Browsing module (IIS), 1613
- Web-Dyn-Compression module (IIS), 1615
- Web edition (Windows Server 2008), 21
- Web-Filtering module (IIS), 1615
- Web-Ftp-Mgmt-Console module (IIS), 1616
- Web-Ftp-Publishing module (IIS), 1616
- Web-Ftp-Server module (IIS), 1616
- Web-Health module (IIS), 1614
- Web-Http-Errors module (IIS), 1613
- Web-Http-Logging module (IIS), 1614
- Web-Http-Redirect module (IIS), 1613
- Web-Http-Tracing module (IIS), 1614
- Web-Includes module (IIS), 1614
- Web-IP-Security module (IIS), 1615
- Web-ISAPI-Ext module (IIS), 1613
- Web-ISAPI-Filter module (IIS), 1614
- Web-Lgcy-Mgmt-Console module (IIS), 1616
- Web-Lgcy-Scripting module (IIS), 1616
- Web-Log-Libraries module (IIS), 1614
- Web-Metabase module (IIS), 1616
- Web-Mgmt-Compat module (IIS), 1616
- Web-Mgmt-Console module (IIS), 1616
- Web-Mgmt-Tools module (IIS), 1616
- Web-NET-Ext module (IIS), 1613
- Web-ODBC-Logging module (IIS), 1614
- Web-Performance module (IIS), 1615
- Web-Request-Monitor module (IIS), 1614
- Web-Scripting-Tools module (IIS), 1616
- Web-Security module (IIS), 1614
- Web Server (IIS), 1105
- Web Server SSO Agent, 893
- Web-Stat-Compression module (IIS), 1615
- Web-Static-Content module (IIS), 1613
- Web-Url-Auth module (IIS), 1615
- Web-Windows-Auth module (IIS), 1615
- Web-WMI module (IIS), 1616

- ul style="list-style-type: none; padding-left: 0;">
- web sites
 - IIS (Internet Information Services), adding with, 1630-1633
 - URL authorization, configuring, 1634-1638
- WER (Windows Error Reporting), 1401
- wevtutil.exe command, 946-947
- wevutil.exe command-line interface (Event Viewer), 1397-1400
- WGA (Windows Genuine Advantage), 1078
- whatif option (PowerShell), 1551-1552
- where command (CMD.EXE), 1518
- wildcard certificates, 1646
- WIM (Windows Imaging Format), 1016
 - Windows RE installations, 1340-1345
 - WIM files
 - adding drivers to, 1073-1078
 - applying updates to, 1070-1073
 - mounting, 1069-1070
 - Windows Server 2008 installations, 101
- Win32_PageFileUsage pagefile object, 1199
- \$WINDOWS.~BT folders, Windows Server 2008 upgrades, 129
- \$WINDOWS.~LS folders, Windows Server 2008 upgrades, 129
- \$WINDOWS.~Q folders, Windows Server 2008 upgrades, 130
- Windows 3.0, 2-3
- Windows 98, 5-6
- Windows 2000, 6-7
 - forest mode (AD), 675
 - native domain mode (AD), 672
- Windows 2003 R2, 12-15
- Windows 2003 servers, list of modes, 1035-1036
- Windows Aero effects, 67-70
- Windows authentication (IIS), 1615
- Windows Automated Installation Kit (WAIK), 12, 133, 138-139, 1017
 - answer files, 1052-1058
 - installing, 1052
- Windows Backup, AD backups, 812-814
- Windows Defender, 209
- Windows Deployment Services (WDS), 20, 1106. *See also* deployment
 - authorizing, 1041
 - configuring, 1019-1026
 - authorizing unknown clients, 1030-1035
 - DHCP options, 1027-1028
 - from command line, 1028
 - prestaging computers
 - in Active Directory, 1029-1030
 - server customization, 1035-1041
 - image management in, 1044-1048
 - installing, 1017-1019
 - PXE client communication
 - with, 1025
- Windows Event Collector
 - service, event subscriptions, 1390
- Windows Explorer
 - address bar, 79
 - advanced features, 85-86
 - command bar, 81
 - Content pane, 82
 - Details pane, 82
 - discussed, 78-79
 - filtering, 83
 - grouping, 83
 - Navigation pane, 82
 - Preview pane, 82
 - searching, 81
 - stacking, 84-85
- Windows Firewall, 196, 528
 - configuring, 197-201
 - Control Panel applet
 - firewall configuration, 197-200
 - General tab, 197
 - Import Policy action, 200
 - Inbound Rules
 - section, 198
 - New Rule action, 198
 - Outbound Rules
 - section, 198
 - Group Policy area, 201
 - monitoring section, 201
 - turning off, 201
- Windows Server 2008
 - configurations, enabling in, 117
- Windows Firewall with Advanced Security, 195
- Windows Flip, 68
- Windows Genuine Advantage (WGA), 1078
- Windows Imaging Format (WIM), 1016
 - Windows RE installations, 1340-1345
 - WIM files
 - adding drivers to, 1073-1078
 - applying updates to, 1070-1073

- mounting, 1069-1070
- Windows Server 2008
 - installations, 101
- Windows Internal
 - Database, 1116
- Windows Internet Name
 - Service (WINS), 29, 447-448, 1117
- Windows Logs node (Event Viewer), 1382
- Windows Management
 - Instrumentation (WMI), 1529, 1532-1536
- Windows Media Services
 - 2008, 1650
- Windows Mobile 6,
 - RMS-protected documents, 866
- Windows NT
 - limitations of, 629
 - version 3.1, 3-4
 - version 3.5, 4-5
 - version 4.0, 5
- Windows PowerShell, 19, 1116
- Windows Process Activation
 - Service (WAS), 1116, 1616
- Windows RE (Recovery Environment)
 - accessing, 1338
 - BCDEdit, 1353-1355
 - Boot Repair Your Computer option, 1346
 - command prompt, 1348-1349
 - disk access, 1352
 - driver management, 1351
 - file access, 1352
 - installed instances to repair, selecting, 1339
 - installing, 1340-1345
 - local server installations, 1340-1345
 - partitions, installing to, 1342-1343
 - recovery options, selecting, 1340
 - services management, 1351
 - WIM image installations, 1340-1345
- Windows Remote Management (WinRM), 955, 1389
- Windows Script Host (WSH), 1528
- ADSI (Active Directory Service Interfaces), 1529
- command host run
 - commands, setting, 1530
- Hello World messages, 1529-1530
- scripts
 - forcing to run in particular hosts, 1530
 - switching between, 1531
- WMI (Windows Management Instrumentation), 1529, 1532-1536
- Windows Server 2003, 9-12
 - domain mode (AD), 673
 - interim domain mode (AD), 673
 - interim mode (AD), 675
 - migrating from
 - failover clustering, 1266-1268
 - NLB (Network Load Balancing), 1229
- Windows Server 2003 mode (AD), 675-676
- Windows Server 2008 mode (AD), 676-677
- Windows Server Backup (WSB), 1117
 - backups
 - backing up system state, 1164
 - features of, 1153-1156
 - scheduling, 1159-1160
 - single-time backups, 1161-1164
 - command-line interface, 1170-1172
 - discussed, 1152-1153
 - installing, 1158
 - recovery
 - PC Restores, 1165-1166
 - system state recovery, 1167-1168
 - volume/file/folder recovery, 1168-1170
 - recovery features, 1156-1158
 - VSS (Volume Shadow Copy Service), 1172-1178
- Windows Server Core
 - benefits of, 912-913
 - configuring, 918-919
 - administrator password, 920
 - applications, 938-939
 - auto-update, 927-928
 - default scripting engine, 925-926
 - firewalls, 929-931
 - hardware, 933-934
 - international settings, 925
 - joining domains, 924-925
 - pagefiles, 929
 - patches, 927-928
 - Remote Desktop, 932-933
 - roles and features, 934-938
 - server activation, 926-927
 - server name, 920-921
 - static TCP/IP v4 information, 921-923
 - time zone, 923-924
 - definition, 19
 - discussed, 911-915
 - installing, 915-916
 - limitations, 913
 - logging off, 941-942
 - managing remotely, 942-950
 - rebooting, 941-942
 - systeminfo command, 940

- tables of roles and features, 914
- Windows Server Update Services (WSUS), 1183
- Windows Services for NetWare/UNIX, 12
- Windows Settings (Group Policy Preferences), 1493
- Windows SharePoint Services (WSS), 12
- Windows System Image Manager, 1053
- Windows System Resource Manager (WSRM), 1117, 1319
 - accounting, 1327-1328
 - conditions of, 1327
 - resource allocation policies, 1320-1326
 - server configuration, 1328-1330
- Windows Vista, 17
 - activating, 1078-1079
 - feature comparison, 44-45
 - IIS (Internet Information Services), 1648-1649
 - logons, 47-48
 - reduced-functionality mode, 1078-1079
- Windows XP, 7-9, 46-47
- WinRM (Windows Remote Management), 955, 1389
- winrm quickconfig
 - command, event subscriptions, 1389
- winrm/config command, 1391
- WinRS command, 944-945
- WINS (Windows Internet Name Service), 29, 447-448, 1117
- WINS tab (zone properties menu), 430
- WINS/NBNS servers (option 044) option, DHCP installation, 382
- WINS/NBT node type (option 046) option, DHCP installation, 382
- winsxs folder, 1106
- wiping hard disks, 144
- wireless communication, 345
- Wireless LAN (WLAN) Service, 1117
- wizards
 - Active Directory Domain Services Installation Wizard, 719
 - AD LDS Setup Wizard, 855
 - Add Account Partner Wizard, AD FS installation, 902
 - Add Account Store Wizard, AD FS installation, 899
 - Add Features Wizard, 1117-1118
 - Add Printer Wizard, 310-311
 - Add Roles Wizard, 1107-1111
 - DHCP installation, 383
 - TS installation, 558
 - ADDS (Active Directory Domain Services) Installation Wizard, 639-651
 - Basic Task Wizard, 1127
 - Connection Request Policy Wizard, RADIUS policy configuration, 484
 - Create New Data Collector Set Wizard (Performance Monitor), 1366
 - Create New Data Collector Wizard, 1373
 - Delegation of Control Wizard, 782
 - Diagnostic Report Wizard, 1000
 - Domain Controller Wizard, 683
 - Group Policy Results Wizard, 1471-1474
 - Install Licenses Wizard, 546
 - New Replicated Folders Wizard, 997
 - NIS Data Migration Wizard, 1578-1580
 - RemoteApp Wizard, 585
 - Remove Role Wizard, 1112
 - SCW (Security Configuration Wizard), 179
 - analyze feature, 185-186
 - applying security policies, 184
 - audit configuration, 184
 - Configuration Action page, 180
 - converting security policies to GPO, 184
 - Disable the Service option, 182
 - editing firewall rules, 182
 - LDAP (Lightweight Data Access Protocol), 182
 - modifying security policies, 184
 - outbound resource access, 183
 - outgoing authentication, 183
 - Registry settings configuration, 182
 - role-based service configuration, 181
 - saving security policies, 184
 - secedit.exe command-line tool, 187, 193-194

- Security Configuration and Analysis MMC snap-in, 187, 190-192
 - Security Templates MMC snap-in, 187-189
 - SMB (Server Message Block) option, 182
 - Viewer, 180, 186
 - WLAN (Wireless LAN) Service, 1117
 - WMI (Windows Management Instrumentation), 1529, 1532-1536
 - WMI Control, 1139-1140
 - wmic command, 939
 - wmic qfe list command, 928
 - WMP (Windows Media Player), stopping via PowerShell, 1552
 - Word
 - launching remotely, 590-591
 - RMS-protected documents, 868, 878
 - workgroups
 - domains versus, 623-627
 - naming, Windows Server 2008 configurations, 112
 - working set size (memory), 1360
 - WOW (Windows On Windows), 1509
 - Write permissions, 244
 - WS-Management, configuring in Server Core, 944
 - WSB (Windows Server Backup), 1117
 - backups
 - backing up system state, 1164
 - features of, 1153-1156
 - scheduling, 1159-1160
 - single-time backups, 1161-1164
 - command-line interface, 1170-1172
 - discussed, 1152-1153
 - installing, 1158
 - recovery
 - PC Restores, 1165-1166
 - system state recovery, 1167-1168
 - volume/file/folder recovery, 1168-1170
 - recovery features, 1156-1158
 - Volume Shadow Copy Service (VSS), 1172-1178
 - Wscript.Arguments() array, VBScript, 1531
 - Wscript.Quit(0) function, VBScript, 1531
 - WSH (Windows Script Host), 1528
 - ADSI (Active Directory Service Interfaces), 1529
 - command host run
 - commands, setting, 1530
 - Hello World messages, 1529-1530
 - scripts
 - forcing to run in particular hosts, 1530
 - switching between, 1531
 - WMI (Windows Management Instrumentation), 1529, 1532-1536
 - WSRM (Windows System Resource Manager), 1117, 1319
 - accounting, 1327-1328
 - conditions of, 1327
 - resource allocation policies, 1320-1326
 - server configuration, 1328-1330
 - WSS (Windows SharePoint Services), 12
 - WSUS (Windows Server Update Services), 1183
 - wusa command, 928
- ## X - Y - Z
- X.500, 633-634
 - XP. *See* Windows XP
 - XPS (XML Paper Specification), 290
 - ZAP files, 1440-1442
 - zone properties menu
 - General tab, 429
 - Name Servers tab, 429
 - Start of Authority tab, 429
 - WINS tab, 430
 - Zone Transfers tab, 430
 - zones (DNS)
 - creating, 417-420
 - delegating, 434
 - GlobalNames zones, 444-445
 - _msdcs zones, 428_
 - reverse lookup zones, 432-434
 - scavenging in, 431
 - stub zones, 437