Introduction

Windows Server 2008 R2 is the latest release of the Windows Server operating system. Over the years, it has evolved quite dramatically from the early days of Windows NT Server, Windows 2000, Windows 2003, or even Windows 2008. With the release of Windows Server 2008 R2, Microsoft again has introduced a number of new technologies intended to help IT professionals improve their ability to provide network services to the clients they serve.

We’ve had the opportunity to write a book on every version of Windows Server over the past two decades, and when we set out to write this book, we wanted to once again provide you, the reader, with a lot of really valuable information. Instead of just marketing fluff that talks about features and functions, we wanted to really dig down into the product and share with you best practices on planning, preparing, implementing, migrating, and supporting a Windows Server 2008 R2 environment.

Even though the original Windows Server 2008 released in early 2008 and Windows 2008 R2 released late in the summer of 2009, we’ve been fortunate enough to work with these operating system releases for more than 2 years in priority early adopter programs. The thing about being involved with a product so early on is that our first experiences with these products were without any documentation, Help files that provided guidance, or any shared experiences from others. We had to learn Windows Server 2008 R2 from experience, usually the hard way, but that has given us a distinct advantage of knowing the product forward and backward better than anyone could ever imagine. And we started to implement Windows Server 2008 R2 in production environments for a select group of our enterprise customers more than a year before the product release—where organizations were depending on the server operating system to run key areas of their business.

So the pages of this book are filled with years of experience with Windows Server 2008 and 2008 R2, live production environment best practices, and fully updated with RTM code specifics that will hopefully help you design, plan, prototype, implement, migrate, administer, and support your Windows Server 2008 R2 environment!

This book is organized into 11 parts, each part focusing on core Windows Server 2008 R2 areas, with several chapters making up each part. The parts of the book are as follows:

- **Part I: Windows Server 2008 R2 Overview**—This part provides an introduction to Windows Server 2008 R2 not only to give a general technology overview, but also to note what is truly new in Windows Server 2008 R2 that made it compelling enough for organizations to implement the technology in beta in production environments. We also cover basic planning, prototype testing, and migration techniques, as well as provide a full chapter on the installation of Windows Server 2008 R2 as well as the GUI-less Windows Server Core.
Part II: Windows Server 2008 R2 Active Directory—This part covers Active Directory planning and design. If you have already designed and implemented your Active Directory, you will likely not read through this section of the book in detail. However, you might want to look through the Notes and Tips throughout the chapter, and the best practices at the end of each chapter because we highlight some of the tips and tricks new to Windows Server 2008 R2 that are different from Windows 2000, 2003, and 2008. You might find that limitations or restrictions you faced when designing and implementing Active Directory 2003 and 2008 have now been revised. Topics such as federated forests, lightweight directory services, and identity lifecycle management capabilities might be of interest.

Part III: Networking Services—This part covers DNS, DHCP, domain controllers, IPv6, and IIS from the perspective of planning, integrating, migrating, and coexisting. Again, just like in Part II, you might find the Notes, Tips, and best practices to have valuable information on features that are new in Windows Server 2008 R2; you might find yourself perusing these chapters to understand what's new and different that you can leverage after a migration to Windows Server 2008 R2.

Part IV: Security—Security is on everyone’s mind these days, so it was a major enhancement to Windows Server 2008 R2. We actually dedicated three chapters of the book to security, breaking the information into server-level security such as Public Key Infrastructure (PKI) certificate services; transport-level security such as IPSec and NAT traversal; and security policies, Network Access Protection (NAP), and Network Policy Server (NPS) that have been updated in Windows Server 2008 R2.

Part V: Migrating to Windows Server 2008 R2—This part is dedicated to the migrations from Windows 2003 and 2008 to Windows Server 2008 R2. We provide a chapter specifically on tips, tricks, best practices, and lessons learned on the planning and migration process to Windows Server 2008 R2. We also have a chapter on application-compatibility testing of applications currently running on earlier versions of Windows Server and how to test and migrate applications to a Windows Server 2008 R2 platform.

Part VI: Windows Server 2008 R2 Administration and Management—After you get Windows Server 2008 R2 in place, you end up spending the rest of your time managing and administering the new operating system platform, so we’ve dedicated six chapters to administration and management. This section covers the administration and management of users, sites, organizational units, domains, and forests typical of a Windows Server 2008 R2 environment. Although you can continue to perform tasks the way you did in Windows 2000, 2003, and 2008, because of significant changes in replication, background transaction processing, secured communications, Group Policy management, and Windows PowerShell management tools, there are better ways to work with Windows Server 2008 R2. These chapters drill down into specialty areas helpful to administrators of varying levels of responsibility. This part of the book also has a chapter on managing Windows Server 2008 R2 using System Center Operations Manager 2007.
Part VII: Remote and Mobile Technologies—Mobility is a key improvement in Windows Server 2008 R2, so this part focuses on enhancements made to Routing and Remote Access Service (RRAS), significant improvements in Remote Desktop Services (formerly Terminal Services), and the introduction of a new remote access technology called DirectAccess. Instead of just providing a remote node connection, Windows Server 2008 R2 provides true end-to-end secured anytime/anywhere access functionality. The chapters in this part highlight best practices on implementing and leveraging these technologies.

Part VIII: Desktop Administration—Another major enhancement in Windows Server 2008 R2 is the variety of new tools provided to support better desktop administration, so this part is focused on desktop administration. The chapters in this part go in depth on client-specific group policies, the Group Policy Management Console, Active Directory Administrative Center, Windows PowerShell-based group policies, Windows Deployment Services (WDS), and desktop administration tools in Windows Server 2008 R2.

Part IX: Fault-Tolerance Technologies—As networks have become the backbone for information and communications, Windows Server 2008 R2 needed to be reliable and more manageable, and sure enough, Microsoft included several new enhancements in fault-tolerant technologies. The four chapters in this part address file system management and file-level fault tolerance in Distributed File System (DFS), clustering, Network Load Balancing, and backup and restore procedures. When these new technologies are implemented in a networking environment, an organization can truly achieve enterprise-level reliability and recoverability.

Part X: Optimizing, Tuning, Debugging, and Problem Solving—This part of the book covers performance optimization, capacity analysis, logging, and debugging to help optimize and solve problems in a Windows Server 2008 R2 networking environment.

Part XI: Integrated Windows Application Services—The last part of this book covers core application services integrated in Windows Server 2008 R2, including updates to Windows SharePoint Services and the Windows Media Services component.

It is our hope that the real-world experience we have had in working with Windows Server 2008 R2 and our commitment to relaying to you information that will be valuable in your planning, implementation, and migration to a Windows Server 2008 R2 environment will help you get up to speed on the latest in the Windows Server operating system software!
Windows Server 2008 R2 became available in the summer of 2009. In many ways, it is just the next-generation server operating system update to Windows Server 2008, but in other ways, it is more than just a service pack type update with significant feature enhancements introduced in the version release. To the authors of this book, we see the similarities that Windows Server 2008 R2 has in terms of usability and common graphical user interfaces (GUIs) with previous versions of Windows Server that make it easy to jump in and start implementing the new technologies. However, after over two years of early adopter experience with Windows Server 2008 R2 and the Windows 7 client operating system, when properly implemented, the new features and technologies built in to Windows Server 2008 R2 really address shortcomings of previous versions of Windows Server and truly allow IT organizations to help organizations meet their business initiatives through the implementation of key technologies now included in Windows Server 2008 R2.

This chapter provides an overview of what’s in Windows Server 2008 R2, explains how IT professionals have leveraged the technologies to improve IT services to their organization, and acts as a guide on where to find more information on these core technology solutions in the various chapters of this book.

**Windows Server 2008 R2 Defined**

Windows Server 2008 R2 is effectively the seventh generation of the Windows Server operating system. Upon initial boot, shown in Figure 1.1, Windows Server 2008 R2 looks
like Windows 7 relative to icons, toolbars, and menus. However, because Windows Server 2008 R2 is more of a business functional operating system than a consumer or user operating system, things like the cute Windows Aero 3D interface are not installed by default, and the multimedia features found in the Windows 7 Home or Ultimate versions of the operating system are also not installed and enabled by default.

Under the surface, though, and covered through the pages of this chapter are the new technologies and capabilities built in to Windows Server 2008 R2.

**Windows Server 2008 and Windows Server 2008 R2 Under the Hood**

Although there are a lot of new features and functions added in to Windows Server 2008 and Windows Server 2008 R2 that are covered in chapters throughout this book, one of the first places I like to start is around the things in Windows Server 2008/2008 R2 that you don’t see that make up some of the core capabilities of the new operating system. These are technologies that make the new operating system faster, more reliable, and do more things—but they aren’t features that you have to install or configure.

**Self-Healing NTFS**

One of the new embedded technologies in Windows Server 2008 and Windows Server 2008 R2 is self-healing NTFS. Effectively, the operating system has a worker thread that runs in the background, which makes corrections to the file system when NTFS detects a
corrupt file or directory. In the past when there was a file system problem, you typically had to reboot the server for chkdsk to run and clean up file and directory corrupt errors.

This self-healing function is not something you will ever see running; however, it is an added capability under the hood in Windows Server 2008 R2 that keeps the operating system running reliably and with fewer system problems.

**Server Message Block 2.0**

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

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

Most users on a high-speed local area network (LAN) won’t notice the improvements when opening and saving files out of something like Microsoft Office against a Windows Server 2008/2008 R2 server; however, for users who might be copying up large image files or data sets between systems will find the information copying 10 to 30 times faster. The performance improvement is very noticeable in wide area network (WAN) situations on networks with high latency. Because a typical transfer of files requires short read and write segments of data, a file could take minutes to transfer across a WAN that can transfer in seconds between SMB2-connected systems because the round-trip chatter is drastically reduced.

For SMB2 to work effectively, the systems on both ends need to be Windows Server 2008/2008 R2 systems, Windows Vista or Windows 7 systems, or a combination of the two. A Windows XP client to a Windows Server 2008/2008 R2 server will communicate over SMB 1.0 for backward compatibility and will not gain from this new technology.

SMB2 and the benefits of this embedded technology are discussed in more detail in Chapter 32, “Optimizing Windows Server 2008 R2 for Branch Office Communications.”

**Hyper-V**

Hyper-V is a technology built in to the core of the operating system in Windows Server 2008 and expanded in Windows Server 2008 R2 that greatly enhances the performance and capabilities of server virtualization in a Windows environment. In the past, virtual server software sat on top of the network operating system and each guest session was dependent on many shared components of the operating system.

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

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

**Core Parking**
A technology enhanced in the core Windows Server 2008 R2 operating system is a power-management technology called core parking. Normally, when a multicore server runs, all cores on all processors run at the highest speed possible, regardless of whether the server is being utilized. For organizations that need high capacity during the weekdays when employees are working, that means their systems are effectively idle during evenings and weekends, or more than two thirds of the time, yet consuming power and expending heat. With core parking, servers with the latest processors that recognize core parking protocols will shut down cores on a system when not in use. So, on a 16-core server, if only 2 cores are needed, the other 14 cores are powered off automatically. This dramatically improves power management and decreases the cost of operations of server systems.

**Windows Server 2008 R2 as an Application Server**
As much as there have been significant improvements in Windows Server 2008 R2 under the hood that greatly enhance the performance, reliability, and scalability of Windows Server 2008 R2 in the enterprise, Windows servers have always been exceptional application servers hosting critical business applications for organizations. Windows Server 2008 R2 continues the tradition of the operating system being an application server with common server roles being included in the operating system. When installing Windows Server 2008 R2, the Server Manager Add Roles Wizard provides a list of server roles that can be added to a system, as shown in Figure 1.2.

The various server roles in Windows Server 2008 R2 typically fall into three categories, as follows:

- **File and print services**—As a file and print server, Windows Server 2008 R2 provides the basic services leveraged by users in the storage of data and the printing of information off the network. Several improvements have been made in Windows Server 2008 R2 for file security (covered in Chapter 13, “Server-Level Security”) and file server fault tolerance (covered in Chapter 28, “File System Management and Fault Tolerance”).

- **Domain services**—In enterprise environments running Windows networking, typically the organization is running Active Directory to provide centralized logon authentication. Active Directory continues to be a key component in Windows Server 2008 R2, with several extensions to the basic internal forest concept of an organization to expanded federated forests that allow Active Directories to interconnect with one another. There are several chapters in Part II, “Windows Server 2008 R2 Active Directory,” that address Active Directory, federated forests, lightweight directories, and so on.
FIGURE 1.2 Server roles in Windows Server 2008 R2.

- **Application services**—Windows Server 2008 R2 provides the basis for the installation of business applications such as Microsoft Exchange, Microsoft Office SharePoint Services, SQL Server, and so on. These applications are initially made to be compatible with Windows Server 2008 R2, and later are updated to leverage and take full advantage of the new technologies built into the Windows Server 2008 R2 operating system. Some of the applications that come with Windows Server 2008 R2 include Remote Desktop Services for thin client computing access (covered in Chapter 25, “Remote Desktop Services”), Windows Media Services for video and audio hosting and broadcasting (covered in Chapter 36, “Windows Media Services”), utility server services such as DNS and DHCP (covered in Chapter 11, “DHCP/WINS/Domain Controllers,” and Chapter 10, “Domain Name System and IPv6”), SharePoint document sharing and collaboration technologies (covered in Chapter 35, “Windows SharePoint Services”), and virtual server hosting (covered in Chapter 37).

This book focuses on the Windows Server 2008 R2 operating system and the planning, migration, security, administration, and support of the operating system. Windows Server 2008 R2 is also the base network operating system on top of which all future Windows Server applications will be built.

**Windows Server 2008 R2 Active Directory**

Although Windows Server 2008 R2 provides a number of new server roles for application services, the release of Windows Server 2008 R2 also brings with it an update to Active Directory. Unlike the shift from Windows NT to Active Directory a decade ago that required a major restructuring of domain functions, Active Directory 2008 R2 is more
evolutionary than revolutionary. AD 2008 R2 adds a handful of new features that organizations might or might not choose to upgrade to AD 2008 R2 immediately; however, many organizations have found that the new enhancements in Active Directory 2008 R2 were the primary reason for their migration.

The new features in Active Directory 2008 R2 are as follows:

- **Active Directory Recycle Bin**—The AD Recycle Bin provides administrators an easy way to undelete objects in Active Directory. In the past, when an administrator inadvertently deleted an Active Directory object like a user, group, organizational unit container, or the like, the object was effectively gone and the administrator would have to create the object from scratch, which would create a whole new series of security principles for the new/unique object. The AD Recycle Bin now enables an administrator to simply run the recovery tool and undelete objects.

- **Managed Service Accounts**—Applications in a network frequently use service accounts associated with the security to start a database, conduct data searches and indexing, or launch background tasks. However, when an organization changes the password of a service account, all servers with applications using the service account need to be updated with the new password, which is an administration nightmare. With Active Directory 2008 R2 mode, service accounts can be identified and then managed so that a password change to a service account will initiate a process of updating the service account changes to application servers throughout the organization.

- **Authentication Mechanism Assurance**—Another Active Directory 2008 R2 feature is the enhancement of claims-based authentication in Active Directory. With authentication mechanism assurance, information in a token can be extracted whenever a user attempts to access a claims-aware application to determine authorization based on the user’s logon method. This extension will be leveraged by future applications to improve claims-based authentication in the enterprise.

- **Offline Domain Join**—For desktop administrators who create system images, the challenge of creating images is that a system needs to be physically connected to the network before the system can be joined to the domain. With Offline Domain Join, a system can be prejoined with a file created with a unique system credential written to a file. When a Windows 7 client system or Windows Server 2008 R2 server system needs to be joined, rather than physically connecting the system to the network and joining the system to the domain, this exported file can be used offline to join the system to the Active Directory domain.

**When Is the Right Time to Migrate?**

When Windows Server 2008 R2 first shipped in the summer of 2009, many organizations wondered about the right time to migrate to the new operating system. It used to be that you waited until the first service pack shipped before installing any Microsoft product; however, Windows Server 2008 R2 is effectively an update to Windows Server 2008 that is post–Service Pack 2. And early adopter beta participants found Windows Server 2008 R2
(and Windows 7) to be extremely stable and reliable and, thus, began implementation of the operating systems in production environments six+ months before the operating systems were released. So, the decision of when to implement Windows Server 2008 R2 comes down to the same decision on migration to any new technology—identify the value received by implementing Windows Server 2008 R2, test the solution in a limited environment, and roll out Windows Server 2008 R2 when you are comfortable that the product meets the needs of your organization.

This introductory chapter notes the many features and functions built in to Windows Server 2008 R2 that have helped other organizations make the decision that Windows Server 2008 R2 has significant value to plan a migration and new server implementation. Improvements in security, performance, and manageability provide benefits to organizations looking to minimize administration costs, while providing more functionality to users.

The cost and effort to migrate to Windows Server 2008 R2 vary based on the current state of an organization’s networking environment, as well as the Windows Server 2008 R2 features and functions the organization wants to implement. Some organizations begin their migration process to Windows Server 2008 R2 by adding a Windows Server 2008 R2 member server into an existing Windows 2000/2003/2008 network. Others choose to migrate their Active Directory to Windows Server 2008 R2 as their introduction to the new operating system.

### Adding a Windows Server 2008 R2 System to a Windows 2003/2008 Environment

Many organizations want to add in a specific Windows Server 2008 R2 function such as Windows Server 2008 R2 Remote Desktop Services (previously called Terminal Services), Hyper-V R2 virtualization, DirectAccess, or BranchCache. Such functions can be installed on Windows Server 2008 R2 member servers in an existing Active Directory 2003 networking environment. This allows an organization to get Windows Server 2008 R2 application capabilities fairly quickly and easily without having to do a full migration to Active Directory 2008 R2. In many cases, a Windows Server 2008 R2 member server can simply be added to an existing network without ever affecting the existing network. This addition provides extremely low network impact but enables an organization to prototype and test the new technology, pilot it for a handful of users, and slowly roll out the technology to the client base as part of a regular system replacement or upgrade process.

Some organizations have replaced all their member servers with Windows Server 2008 R2 systems over a period of weeks or months as a preparatory step to eventually migrate to a Windows Server 2008 R2 Active Directory structure.

### Migrating from Windows 2003 and Windows 2008 Active Directory to Windows Server 2008 R2 Active Directory

For organizations that already have a Windows 2003 or Windows 2008 Active Directory environment, migrating to Windows Server 2008 R2 for Active Directory functionality can provide access to several additional capabilities that require a Windows network to be running on Windows Server 2008 R2. Some of the Windows Server 2008 R2 technologies
that require implementation of the Windows Server 2008 R2 Active Directory include Active Directory Recycle Bin, Managed Service Accounts, PowerShell Administration, and Offline Domain Join capabilities as the most popular solutions.

Fortunately, organizations that already have Windows 2003 or 2008 Active Directory in place have completed the hard part of the Active Directory implementation process. Effectively, Windows Server 2008 R2 uses the same Active Directory organizational structure that was created with Windows 2003 or 2008, so forests, domain trees, domains, organizational units, sites, groups, and users all transfer directly into Windows Server 2008 R2 Active Directory. If the organizational structure in Windows 2003 or 2008 meets the needs of the organization, the migration to Windows Server 2008 R2 is predominantly just the insertion of a Windows Server 2008 R2 global catalog server into the existing Windows 2003 or 2008 Active Directory domain to perform a global catalog update to Windows Server 2008 R2 Active Directory.

Of course, planning, system backup, and prototype testing—covered in Chapter 16, “Migrating from Windows 2003/2008 to Windows Server 2008 R2”—help minimize migration risks and errors and lead to a more successful migration process. However, the migration process from Windows 2003 and Windows Server 2008 to Windows Server 2008 R2 is a relatively easy migration path for organizations to follow.

**Versions of Windows Server 2008 R2**

Windows Server 2008 R2 comes in the same release versions as the more recent server version releases from Microsoft with the addition of a Server Core version that provides a lighter GUI-less version of Windows Server 2008 R2. The main versions of Windows Server 2008 R2 include Windows Server 2008 R2, Standard Edition; Windows Server 2008 R2, Enterprise Edition; Windows Server 2008 R2, Datacenter Edition; Windows Web Server 2008 R2; and Windows Server 2008 R2 Server Core.

**Windows Server 2008 R2, Standard Edition**

The Windows Server 2008 R2, Standard Edition is the most common server version of the operating system. Unlike previous versions of Windows Server where basic functions and scalability for memory and processor support was limited to only the Enterprise or Datacenter Editions of the operating system, Windows Server 2008 R2, Standard Edition is now the default version deployed by organizations.

A basic Windows Server 2008 R2 x64-bit Standard Edition system supports up to four x64 professor sockets and 32GB of memory and supports all of the server roles available in Windows Server 2008 R2, with the exception of clustering, cross-file replication (DFS-R technology), and Active Directory Federation Services.

The Standard Edition is a good version of the operating system to support domain controllers, utility servers (such as DNS or DHCP), file servers, print servers, media servers, SharePoint servers, and so on. Most organizations, large and small, find the capabilities of the Standard Edition sufficient for most network services. See Chapter 34, “Capacity
One of the first things an organization becomes aware of is that Windows Server 2008 R2 ONLY comes in 64-bit (x64 or IA64) versions. 32-bit hardware and a 32-bit installation is no longer supported. The last version of the Windows Server operating system that supported 32-bit is Windows Server 2008.

**Windows Server 2008 R2, Enterprise Edition**

With the Windows Server 2008 R2, Standard Edition taking on the bulk of network services, the Windows Server 2008 R2, Enterprise Edition is really focused on server systems that require extremely large-scale processing and memory capabilities as well as clustering or Active Directory Federation Services. From the basis of scalability of processing and memory capacity, applications like Windows virtualization or enterprise-class Exchange 2010 or SQL 2008 servers would benefit from the capabilities of the Enterprise Edition of Windows Server 2008 R2.

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

For organizations leveraging the capabilities of Windows Server 2008 R2 for Thin Client Remote Desktop Services that require access to large sets of RAM (up to 2TB) and multiple processors (up to eight sockets), the Enterprise Edition can handle hundreds of users on a single server. Remote Desktop Services are covered in more detail in Chapter 25.

The Enterprise Edition, with support for server clustering, can provide organizations with the nonstop networking demands of true 24/7, 99.999% uptime capabilities required in high-availability environments. Windows Server 2008 R2, Enterprise Edition supports a wide variety of regularly available server systems, thus allowing an organization its choice of hardware vendor systems to host its Windows Server 2008 R2 application needs.

**Windows Server 2008 R2, Datacenter Edition**

Windows Server 2008 R2, Datacenter Edition is a high-end datacenter class version of the operating system that supports very large-scale server operations. The Datacenter Edition supports organizations that need more than eight core processors. The Datacenter Edition is focused at organizations that need scale-up server technology to support a large centralized data warehouse on one or limited numbers of server clusters.

As noted in Chapter 34 on performance and capacity analysis, an organization can scale-out or scale-up its server applications. Scale-out refers to an application that performs better when it is distributed across multiple servers, whereas scale-up refers to an application that performs better when more processors are added to a single system. Typical scale-out applications include web server services, electronic messaging systems, and file and
print servers. In those cases, organizations are better off distributing the application server functions to multiple Windows Server 2008 R2, Standard Edition or Enterprise Edition systems, or even Windows Web Server 2008 R2 systems. However, applications that scale-up, such as e-commerce or data warehousing applications, benefit from having all the data and processing on a single server cluster. For these applications, Windows Server 2008 R2, Datacenter Edition provides better centralized scaled performance as well as the added benefit of fault tolerance and failover capabilities.

**NOTE**
The Windows Server 2008 R2, Datacenter Edition used to be sold only with proprietary hardware systems; however, Windows Server 2008 R2, Datacenter Edition can now be run on “off-the-shelf” servers with extensive core, processor, and memory expansion capabilities. This update now allows organizations to purchase nonproprietary servers and get the scalability of the Datacenter Edition of the operating system for enterprise-class performance, reliability, and supportability.

**Windows Web Server 2008 R2 Edition**
The Windows Web Server 2008 R2 Edition is a web front-end server version of the operating system focused on application server needs that are dedicated to web services requirements. Many organizations are setting up simple web servers as front ends to database servers, messaging servers, or data application server systems. Windows Web Server 2008 R2 Edition can be used as a simple web server to host application development environments or can be integrated as part of a more sophisticated web farm and web services environment that scales to multiple load-balanced systems. The Windows Server 2008 R2 operating system has significant improvements in scalability over previous versions of the Windows operating system, and an organization can license multiple web services systems at a lower cost per server to provide the scalability and redundancy desired in large web farm environments.

**NOTE**
For organizations looking to purchase a low-cost Windows Web Server Edition to set up a simple file and print server or utility server (DNS, DHCP, domain controller), the Web Server Edition does not provide traditional multiuser file or print access or utility services. You need to purchase the Windows Server 2008 R2, Standard Edition to get capabilities other than web services.

**Windows Server 2008 R2 Server Core**
New to Windows Server 2008 and continued support with Windows Server 2008 R2 is a Server Core version of the operating system. Windows Server 2008 R2 Server Core, shown in Figure 1.3, is a GUI-less version of the Windows Server 2008 R2 operating system.
When a system boots up with Server Core installed on it, the system does not load up the normal Windows graphical user interface. Instead, the Server Core system boots to a logon prompt, and from the logon prompt, the system drops to a DOS command prompt. There is no Start button, no menu—no GUI at all.

Server Core is not sold as a separate edition, but rather as an install option that comes with the Standard, Enterprise, Datacenter, and Web Server Editions of the operating system. So, when you purchase a license of Windows Server 2008 R2, the DVD has both the normal GUI Edition code plus a Windows Server 2008 R2 Server Core version.

The operating system capabilities are limited to the edition of Server Core being installed, so a Windows Server 2008 R2, Enterprise Edition Server Core server has the same memory and processor limits as the regular Enterprise Edition of Windows Server 2008 R2.

Server Core has been a great version of Windows for utility servers such as domain controllers, DHCP servers, DNS servers, IIS web servers, or Windows virtualization servers being that the limited overhead provides more resources to the applications running on the server, and by removing the GUI and associated applications, there’s less of a security attack footprint on the Server Core system. Being that most administrators don’t play Solitaire or use Media Player on a domain controller, those are applications that don’t need to be patched, updated, or maintained on the GUI-less version of Windows. With fewer applications to be patched, the system requires less maintenance and management to keep operational.
NOTE
With the new remote administration capabilities of Windows Server 2008 R2, covered in Chapter 20, “Windows Server 2008 R2 Management and Maintenance Practices,” administrators can now remotely manage a Server Core system from the Server Manager GUI interface on another server. This greatly enhances the management of Server Core hosts so that administrators can use a GUI console to manage the otherwise GUI-less version of Windows Server.

What’s New and What’s the Same About Windows Server 2008 R2?

From a Microsoft marketing perspective, Windows Server 2008 R2 could be said to be faster, more secure, more reliable, and easier to manage. And it is true that the Windows Server 2008 R2 operating system has all these capabilities. However, this section notes specifically which changes are cosmetic changes compared with previous Windows operating systems and which changes truly improve the overall administrative and end-user experience due to improvements in the operating system.

Visual Changes in Windows Server 2008 R2

The first thing you notice when Windows Server 2008 R2 boots up is the new Windows 7-like graphical user interface (GUI). This is obviously a simple cosmetic change to standardize the current look and feel of the Windows operating systems. Interestingly, with the release of Windows Server 2008 R2, Microsoft did away with the “Classic View” of the administrator Control Panel. For all the network administrators who always switched their server Control Panel to the Classic View, that is now gone, and you will need to figure out the “updated” Control Panel that was the standard starting with Windows XP.

Continuation of the Forest and Domain Model

Windows Server 2008 R2 also uses the exact same Active Directory forest, domain, site, organizational unit, group, and user model as Windows 2000/2003/2008. So if you liked how Active Directory was set up before, it doesn’t change with Windows Server 2008 R2 Active Directory. Even the Active Directory Sites and Services, Active Directory Users and Computers (shown in Figure 1.4), and Active Directory Domains and Trusts administrative tools work exactly the same.

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

Windows Server 2008 R2 has added several new capabilities that simplify tasks. These capabilities could appear to be simply cosmetic changes; however, they actually provide significant benefits for administrative management.

New Server Manager Tool

A tool that was added in Windows Server 2008 is the Server Manager console, shown in Figure 1.5. Server Manager consolidates all of the administrative management consoles from Windows 2000/2003 into a single management tool. Now instead of having to open up the Active Directory Users and Computers console, Control Panel system properties, the DNS management console, and so on, and then toggle to the appropriate console you want, all of the information is now available in one screen.

Updated in Windows Server 2008 R2 is the ability for an administrator to use the Server Manager tool to access not only the server resources on the current server system, but also to remotely access server resources through the Server Manager tool on remote server systems. This remote capability of Server Manager minimizes the need of the administrator to remotely log on to systems to manage them; it allows the administrator to sit at a single Server Manager console and gain access to other servers in the organization.
Additionally, other tools like the Group Policy Management Console (GPMC) show up in Server Manager under the Features node and provide an administrator with the ability to edit group policies, change policies, and apply policies from the same console to which the administrator can make DNS changes, add users, and change IP configuration changes to site configuration settings.

**PowerShell for Administrative Tasks**

Another updated server feature in Windows Server 2008 R2 is the extension of PowerShell for server administration and management. PowerShell has now been extended to be a full scripting language for administration tasks in Windows Server 2008 R2. PowerShell was first introduced in Exchange 2007 as the Exchange Management Shell (EMS) that underlies all functions of Exchange 2007 administration. PowerShell (version 2.0) is now installed by default in Windows Server 2008 R2, as opposed to being an add-in feature in Windows Server 2008. As a built-in component, all administrative tasks are now fully PowerShell enabled.

PowerShell in Windows Server 2008 R2 provides the ability for administrators to script processes, such as adding users, adding computers, or even more complicated tasks such as querying a database, extracting usernames, and then creating Active Directory users, and to provision Exchange mailboxes all from a PowerShell script. Additionally, PowerShell in Windows Server 2008 R2 allows an administrator to script installation processes so that if, for example, the administrator creates a Remote Desktop server or web server with specific settings, the administrator can use a PowerShell script and deploy additional servers all identically configured using the same script over and over.
And with PowerShell 2.0 built in to Windows Server 2008 R2, PowerShell scripts and commands can be run against remote servers. This enables an administrator to sit at one server and remotely execute scripts on other servers in the environment. Using secured server-to-server session communications, an administrator can configure a group of servers, manage a group of servers, and reboot a group of servers all from a series of PowerShell commands.

All future server products released from Microsoft will have the PowerShell foundation built in to the core Windows Server 2008 R2 operating system, thus making it easier for products running on Windows Server 2008 R2 to use the same administrative scripting language. PowerShell is covered in detail in Chapter 21, “Automating Tasks Using PowerShell Scripting.”

**Active Directory Administrative Center**

New to Windows Server 2008 R2 and built on PowerShell v2.0, the Active Directory Administrative Center is a customizable console that an organization can create for specific administrators in the organization. As an example, an organization might have an administrator who only needs to reset passwords, or another administrator who only needs or manage print queues. Rather than giving the administrator access to the full Active Directory Users and Computers or Print Management consoles, an Active Directory Administrative console can be created with just a task or two specific to the administrator’s responsibilities.

The console is built on PowerShell, so underlying the GUI are simple PowerShell scripts. Anything that can be done in PowerShell on a Windows Server 2008 R2 server can be front-ended by the administration console. An example of the console is shown in Figure 1.6, and the tool is covered in detail in Chapter 18, “Windows Server 2008 R2 Administration.”

**Increased Support for Standards**

The release of Windows Server 2008 introduced several industry standards built in to the Windows operating system that have since been updated in Windows Server 2008 R2. These changes continue a trend of the Windows operating system supporting industry standards rather than proprietary Microsoft standards. One of the key standards built in to Windows Server 2008 and Windows Server 2008 R2 is IPv6.

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

Additionally, IPv6 supports new standards in dynamic addressing and Internet Protocol Security (IPSec). Part of IPv6 is to have support for the current IPv4 standards so that dual addressing is possible. With Windows Server 2008 R2 supporting IPv6, an organization can choose to implement a dual IPv6 and IPv4 standard to prepare for Internet communications support in the future. IPv6 is covered in detail in Chapter 10.
Changes in Active Directory

As noted earlier in this chapter, Active Directory in Windows Server 2008 R2 hasn’t changed to the point where organizations with solid Active Directory structures have to make changes to their directory environment. Forests, domains, sites, organizational units, groups, and users all remain the same. There are several improvements made in Active Directory and the breadth of functionality provided by directory services in Windows Server 2008 R2.

The changes made in Active Directory are captured in the name changes of directory services as well as the introduction of a Read-Only Domain Controller service introduced in Windows Server 2008.

Renaming Active Directory to Active Directory Domain Services

In Windows Server 2008, Active Directory was renamed to Active Directory Domain Services (AD DS), and Windows Server 2008 R2 continues with that new name. Active Directory Domain Services refers to what used to be just called Active Directory with the same tools, architectural design, and structure that Microsoft introduced with Windows 2000 and Windows 2003.

The designation of Domain Services identifies this directory as the service that provides authentication and policy management internal to an organization where an organization’s internal domain controls network services.
For the first time, AD DS can be stopped and started as any other true service. This facilitates AD DS maintenance without having to restart the domain controller in Directory Services Restore Mode.

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

Another name change in the directory services components with Windows Server 2008 from Microsoft is the renaming of Active Directory in Application (ADAM) to Active Directory Lightweight Directory Services (AD LDS). ADAM has been a downloadable add-in to Windows 2003 Active Directory that provides a directory typically used in organizations for nonemployees who need access to network services. Rather than putting nonemployees into the Active Directory, these individuals—such as contractors, temporary workers, or even external contacts, such as outside legal counsel, marketing firms, and so on—have been put in ADAM and given rights to access network resources such as SharePoint file libraries, extranet content, or web services.

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

**Expansion of the Active Directory Federation Services**

That leads to the third Active Directory service called Active Directory Federation Services, or AD FS. Active Directory Federation Services was introduced with Windows 2003 R2 edition and continues to provide the linking, or federation, between multiple Active Directory forests, or now with Windows Server 2008 R2 Active Directory Federation Services, the ability to federate between multiple Active Directory Domain Services systems.

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

Active Directory Federation Services is covered in detail in Chapter 8.
Introducing the Read-Only Domain Controller

Another change in Active Directory in Windows Server 2008 that was continued in Windows 2008 R2 was the addition of a Read-Only Domain Controller, or RODC. The RODC is just like a global catalog server in Active Directory used to authenticate users and as a resource to look up objects in the directory; however, instead of being a read/write copy of the directory, an RODC only maintains a read-only copy of Active Directory and forwards all write and authentication requests to a read/write domain controller.

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

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

Windows Server 2008 R2 Benefits for Administration

Windows Server 2008 R2 provides several new benefits that help organizations better administer their networking environment. These new features provide better file and data management, better performance monitoring and reliability tracking tools to identify system problems and proactively address issues, a new image deployment tool, and a whole new set of Group Policy Objects that help administrators better manage users, computers, and other Active Directory objects.

Improvements in the Group Policy Management

Windows Server 2008 R2 introduces over 1,000 new Group Policy Objects specific to Windows Server 2008 R2 and Windows 7, along with several new components that expand on the core capabilities of Group Policy management that have been part of Windows 2000/2003 Active Directory. The basic functions of Group Policy haven’t changed, so the Group Policy Object Editor (gpedit) and the Group Policy Management Console (GPMC) are the same, but with more options and settings available.

As mentioned earlier, the Group Policy Management Console can either be run as a separate MMC tool, or it can be launched off the Features branch of the Server Manager console tree, as shown in Figure 1.7. Group policies in Windows Server 2008 R2 provide more granular management of local machines, specifically having policies that push down to a client that are different for administrator and non-administrator users.
Additionally, applications can now query or register with a network location awareness service within Group Policy management, which provides the identity where a user or computer object resides. As an example, a policy can be written that allows users to have access to applications and files if they are on a local network segment, but blocks users from accessing the same content when they are on a remote segment for security and privacy reasons. This addition to group policies adds a third dimension to policies so that now administrators can not only define who and what someone has access to, but also limit their access based on where they are.


**NOTE**

When running the Group Policy Management Console to manage a Windows Server 2008 R2 Active Directory environment, run the GPMC tool from a Windows Server 2008 R2 server or a Windows 7 client system to have access to all the editable objects available. If you run the GPMC tool from a Windows 2003 server or Windows XP client, you will not see all the features nor have full access to edit all objects available.

This is because Windows Server 2008 R2 now supports new template file formats (ADMX and ADML) that are only accessible from Windows Server 2008, Windows Server 2008 R2, Windows Vista, and Windows 7 systems.
Introducing Performance and Reliability Monitoring Tools

Windows Server 2008 R2 introduces new and revised performance and reliability monitoring tools intended to help network administrators better understand the health and operations of Windows Server 2008 R2 systems. Just like with the Group Policy Management Console, the new Reliability and Performance Monitor shows up as a feature in the Server Manager console. By clicking on the Performance Diagnostic Console, the tool shows up in the right pane, as shown in Figure 1.8.

![Performance Monitor](image)

**FIGURE 1.8** Windows Reliability and Performance Monitor.

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

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

Leveraging File Server Resource Manager

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

FSRM, shown in Figure 1.9, in Windows Server 2008 R2 has been improved to allow the nesting of quotas to ensure the most restrictive policy is applied. Quotas can also transcend subfolders, so as new folders are created, or as policies are applied at different levels in a folder hierarchy, the policies still apply, and the rules are combined to provide varying levels of quota allocation to user data. Additionally, quotas are now based on actual storage, so if a file is compressed when stored, the user will be able to store more files within their allocated quota.

![File Server Resource Manager](image)

**FIGURE 1.9** File Server Resource Manager.

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

**Leveraging the Best Practice Analyzer**

Included in Windows Server 2008 R2 is a built-in Best Practice Analyzer. Found in the Server Manager console tool, the Best Practice Analyzer runs a series of tests against Active Directory roles, such as the Hyper-V role, the DNS role, and the Remote Desktop Services role, to assess whether the role has been installed and configured properly and to compare the installation with tested best practices.
Some of the results from the Best Practice Analyzer could tell an administrator they need to add more memory to a server, to move a role to a separate server to improve role optimization, or to shift a database to a different drive on the server to distribute disk performance demands on the system. More details on the Best Practice Analyzer are covered in Chapter 20.

**Introduction of Windows Deployment Services**

Windows Server 2008 introduced a new tool called Windows Deployment Services (WDS), which was effectively an updated version of the Remote Installation Services (RIS) that has been available for the past several years. Unlike RIS, which was focused on primarily scripted installations and client images, WDS in Windows Server 2008 R2 can distribute images of Windows 7 clients or Windows Server 2008 R2 servers in a significantly more flexible and modifiable deployment process.

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

With Windows Server 2008 R2 and Windows 7, the image can be created in Windows Imaging (WIM) format, which allows for the injection of patches, updates, or even new code to a WIM file without even booting the image file. This provides the organization with more than just static images that get pushed out like in RIS, but rather a tool that provides ongoing and manageable updates to image files.

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


**Improvements in Security in Windows Server 2008 R2**

Significantly more than just cosmetic updates are the security enhancements added to Windows Server 2008 R2. As organizations are struggling to ensure that their environments are secure, employees can depend on information privacy, and content is protected for regulatory compliance reasons; having the tools to secure the environment is critical.

**Enhancing the Windows Server 2008 R2 Security Subsystem**

Part IV of this book, “Security,” is focused on security in the different core areas. Chapter 13 addresses core security subsystems of Windows Server 2008 R2 as it relates to server systems. This includes the basics of server hardening, patching, and updating but also extends into new server security areas added to Windows Server 2008 R2, such as device control level security, wireless access security, and Active Directory Rights Management Services (RMS). Windows Server 2008 R2 has continued the “secure by default” theme at
Microsoft and no longer installs components like Internet Information Services (IIS) by default. The good part about it is that components that are not core to the operation of a server are not installed on the system; however, it means every time you install software, you need to add basic components and features. Getting to remember what has to be installed, configured, or made operational is important as servers are being built and added to a Windows Active Directory environment.

**Transport Security Using IPSec and Certificate Services**

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

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

Completely new to Windows Server 2008, updated in Windows Server 2008 R2, and a major focus for organizations are security policies and policy management around security systems. It used to be we would just lock down systems, make sure they were secure by default, and use our best judgment and best effort to secure a network. However, with laws and regulations, or even human resource departments getting involved in information security, the root of all IT security practices fall on having set security policies defined so that IT can implement technologies to address the organization policies around information security. This is covered in detail in Chapter 15, “Security Policies, Network Policy Server, and Network Access Protection.”

Chapter 15 goes beyond the policies and common best practices around policy management in an enterprise, and also digs into the underlying technologies that help organizations turn security policies into IT-managed technology services. Tools like the Network Policy Server in Windows Server 2008 R2 allow policies to be defined, and the Network Policy Server enforces those policies, specifically around remote logon access, access over wireless network connections, or the integration of Network Access Protection (NAP) in querying a device and making sure the device (desktop, laptop, or mobile device) has the latest patches, updates, and antivirus software dictated by management to ensure a device is secure.
Improvements in Mobile Computing in Windows Server 2008 R2

As organizations find their workforce becoming more and more mobile, Microsoft has made significant improvements to mobility in Windows Server 2008 R2. New technologies provide a more seamless experience for users with laptops to move from office, to home, to Internet Wi-Fi hot spots and maintain connectivity to network resources. These improvements do require mobile users to run the latest Windows 7 client operating system on their laptop system to gain access to these new services; however, once implemented, users find the functionality to greatly support easier access to network resources no matter where the user resides.

Windows Server 2008 R2 DirectAccess

One of the significant remote access enhancements in Windows Server 2008 R2 is the DirectAccess technology. DirectAccess provides a remote user the ability to access network resources such as file shares, SharePoint shares, and the like without having to launch a virtual private network (VPN) to gain access into the network.

DirectAccess is an amazing technology that combines sophisticated security technology and policy-based access technology to provide remote access to a network; however, organizations do find it challenging to get up to speed with all the technology components necessary to make DirectAccess work. So, although many organizations will seek to achieve DirectAccess capabilities, it might be months or a couple of years before all the technologies are in place for the organization to easily enable DirectAccess in their enterprise environment.

Some of the technologies required to make DirectAccess work include the following:

- **PKI certificates**—DirectAccess leverages PKI certificates as a method of identification of the remote device as well as the basis for encrypted communications from the remote device and the network. Thus, an organization needs to have a good certificate infrastructure in place for server and client certificate-based encrypted communications.

- **Windows 7 clients**—DirectAccess only works with clients that are running Windows 7. The client component for encryption, encapsulation, and policy control depend on Windows 7 to make all the components work together.

- **IPSec**—The policy control used in DirectAccess leverages IPSec to identify the destination resources that a remote user should have access to. IPSec can be endpoint to endpoint (that is, from the client system all the way to the application server) or IPSec can be simplified from the client system to a DirectAccess proxy server where the actual endpoint application servers do not need to be IPSec enabled. In any case, IPSec is a part of the security and policy structure that ensures the remote client system is only accessing server resources that by policy the remote client should have access to as part of the DirectAccess session connection.
IPv6—Lastly, DirectAccess uses IPv6 as the IP session identifier. Although most organizations have not implemented IPv6 yet and most on-ramps to the Internet are still IPv4, tunneling of IPv6 is fully supported in Windows 7 and Windows Server 2008 R2 and can be used in the interim until IPv6 is fully adopted. For now, IPv6 is a requirement of DirectAccess and is used as part of the remote access solution.

More details on DirectAccess are provided in Chapter 24, “Server-to-Client Remote Access and DirectAccess.”

Windows 7 VPN Reconnect

VPN Reconnect is not a Windows Server 2008 R2–specific feature but rather a Windows 7 client feature; however, with the simultaneous release of the Windows 7 client and Windows Server 2008 R2, it is worth noting this feature because Microsoft will be touting the technology and network administrators will want to know what they need to do to implement the technology. VPN Reconnect is simply an update to the VPN client in Windows 7 that reestablishes a VPN session on a client system in the event that the client system’s VPN session is disconnected.

VPN Reconnect effectively acknowledges that a client VPN session has been disconnected and reestablishes the session. Many longtime administrators might wonder why this is new because client systems in the past (Windows XP, Vista, and so forth) have always had the ability to retry a VPN session upon disconnect. However, the difference is that instead of simply retrying the VPN session and establishing a new VPN session, the VPN Reconnect feature of Windows 7 reestablishes a VPN session with the exact same session identification, effectively allowing a session to pick up exactly where it left off.

For example, a Windows 7 client user can be transferring a file on a wired VPN connected session and then switch midstream to a Wi-Fi VPN-connected session, and the file transfer will continue uninterrupted.

VPN Reconnect utilizes the IKE v2 protocol on the client and on the Windows Server 2008 R2 side with an established session identification so that upon reconnect, the session ID remains the same.

Chapter 24 provides more details on VPN Reconnect.

Windows 7 Mobile Broadband

Another Windows 7–specific technology for mobile users is Windows 7 Mobile Broadband. Again, something that has nothing to do specifically with Windows Server 2008 R2, Windows 7 Mobile Broadband is an update to the carrier-based (for example, AT&T, Sprint, Verizon) mobile connection devices and services in Windows 7.

In the past, a user plugged in a Mobile Broadband card to their Windows XP or Vista system and then had to launch an application such as the AT&T Connection Manager. With Windows 7 and the latest Mobile Broadband drivers for the device and for Windows 7, the insertion of the Mobile Broadband card into a mobile system automatically connects the user to the Internet. Just like if the user turns on a Wi-Fi adapter in a system
and automatically establishes a connection to a Wi-Fi access point, Mobile Broadband automatically connects the user to the Internet.

When the Windows 7 Mobile Broadband adapter is disconnected from the user’s system, the Mobile Broadband session disconnects, and if the system has a Wi-Fi or wired Ethernet connection available, the user’s system automatically connects to an alternate connection point. Combine Mobile Broadband with VPN Reconnect or with DirectAccess and a mobile user has seamless connection access back into their organization’s network.

**Improvements in Windows Server 2008 R2 for Better Branch Office Support**

Windows Server 2008 R2 has greatly enhanced the technology offerings that provide better IT services to organizations with remote offices or branch offices. Typically, a remote or branch office has limited IT support or at least the site needs to have the same functionality and reliability as the main corporate or business office, but without the budget, to have lots of redundant hardware and devices for full operational support. With the new Windows Server 2008 R2 branch office resources, a remote location can now have high security, high performance, access to data without significant latency, and operational capabilities, even if the remote site is dropped off the network due to a WAN or Internet connection problem.

The tools and technologies new or improved in Windows Server 2008 R2 include Read-Only Domain Controllers, BitLocker Drive Encryption, distributed file server data replication, and distributed administration.

Details on the new technologies built in to Windows Server 2008 R2 that better support remote and branch offices are covered in Chapter 32.

**Read-Only Domain Controllers for the Branch Office**

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

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

New to Windows Server 2008 R2 is a role called BranchCache. BranchCache is a technology that provides users with better access to files across a wide area network (WAN). Normally, if one user accesses a file, the file is transferred across the WAN for the user, and then when another user accesses the same file, the same file is again transferred across the WAN for the other user. BranchCache acknowledges that a file has been transferred across the WAN by a previous user, and instead of retrieving the file across the WAN, the file is accessed locally by the subsequent user.

BranchCache requires Windows 7 on the client side and can be set up so that the file is effectively retrieved in a peer-to-peer manner from another Windows 7 client that had previously accessed a file. Or, a Windows Server 2008 R2 server with the BranchCache server role can be set up in the remote location where remotely accessed files are temporarily cached for other Windows 7 client users to seamlessly access the files locally instead of being downloaded across the WAN.

BranchCache does not require the user to do anything differently. Users simply accesses files as they normally do (either off a Windows file system or from a SharePoint document library), and the combination of Windows 7 and Windows Server 2008 R2 does all the caching automatically. BranchCache has proven to improve access time on average 30%–45% for remote users, thus increasing user experience and potentially user productivity by having faster access to information in remote locations.

BitLocker for Server Security

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

So, BitLocker provides encryption of the volume of a Windows Server 2008 R2 server; for organizations that are concerned that the server might be physically compromised by the theft of the server or physical attack of the system, BitLocker is a great component to implement on the server system.

Distributed File System Replication

Introduced in Windows 2000, improved in Windows 2003, and now a core component of the branch office offerings in Windows Server 2008 R2, Distributed File System Replication (DFSR) allows files to be replicated between servers, effectively providing duplicate information in multiple locations. Windows Server 2008 R2 has a much improved Distributed File System than what was available in Windows 2000/2003. In most organizations, files
are distributed across multiple servers throughout the enterprise. Users access file shares that are geographically distributed but also can access file shares sitting on several servers in a site within the organization. In many organizations, when file shares were originally created years ago, server performance, server disk capacity, and the workgroup nature of file and print server distribution created environments in which those organizations had a file share for every department and every site. Thus, files have typically been distributed throughout an entire organization across multiple servers.

Windows Server 2008 R2 Distributed File System Replication enables an organization to combine file shares to fewer servers and create a file directory tree not based on a server-by-server or share-by-share basis, but rather an enterprisewide directory tree. This allows an organization to have a single directory spanning files from multiple servers throughout the enterprise.

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

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

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

One of the enhancements made in Windows Server 2008 R2 specific to DFS-R is the ability for an administrator to set a DFS replica to be read-only. In the past, DFS replicas were all read/write replicas so that a user in a remote location could accidentally overwrite files that then replicate to all replicas in the environment. Administrators have compensated for this potential issue by setting file-level permissions across files and folders; however, for many remote branch offices, if the administrator could simply make the entire replica read-only, it would simplify the security task dramatically. Thus, read-only replicas can now be set so that an entire server or branch of a DFS tree can be set to replicate to a remote server on a read-only basis.

Distributed File System Replication is covered in detail in Chapter 28.
**Improvements in Distributed Administration**

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

Windows Server 2008 R2 Active Directory has now defined a set of rights specific to branch office and remote site administrators. Very similar to site administrators back in the old Exchange Server 5.5 days—where an administrator was able to add users, contacts, and administer local Exchange servers—now network administrators in Active Directory can be delegated rights based on a branch or remote site role. This provides those administrators with the ability to make changes specific to their branch location. This, along with all the other tools in Windows Server 2008 R2 specific to branch office and remote office locations, now provides better IT services to organizations with multiple offices in the enterprise.

**Improvements for Thin Client Remote Desktop Services**

Windows Server 2008 R2 has seen significant improvements in the Terminal Services (now called Remote Desktop Services [RDS]) capabilities for thin client access for remote users and managed users in the enterprise. What used to require third-party add-ons to make the basic Windows 2000 or 2003 Terminal Services functional, Microsoft included those technologies into Windows Server 2008 and further enhanced them in Windows Server 2008 R2. These technologies include things such as the ability to access Remote Desktop Services using a standard Port 443 SSL port rather than the proprietary Port 3389, or the ability to publish just specific programs instead of the entire desktop, and improvements in allowing a client to have a larger remote access screen, multiple screens, or to more easily print to remote print devices.

These improvements in Windows Server 2008 R2 Remote Desktop Services have made RDS one of the easiest components to add to an existing Windows 2003 Active Directory to test out the new Windows Server 2008 R2 capabilities, especially because the installation of a Windows Server 2008 R2 Remote Desktop Services system is just the addition of a member server to the domain and can easily be removed at any time.

All of these new improvements in Windows Server 2008 R2 Remote Desktop Services are covered in Chapter 25.

**Improvements in RDP v6.x for Better Client Capabilities**

The first area of significant improvement in Windows Server 2008 Terminal Services was addressed in the update to the Remote Desktop Protocol (RDP) v6.x client, shown in Figure 1.10.
The RDP client with Windows Server 2008 provided the following:

- **Video support up to 4,096 x 2,048**—Users can now use very large monitors across an RDP connection to view data off a Windows Server 2008 Terminal Services system. With Windows Server 2008 R2 Remote Desktop Services, the latest support has been extended to support DirectX 9, 10, and 11 redirection.

- **Multimonitor support**—Users can also have multiple (up to 10) monitors supported off a single RDP connection. For applications like computer-aided design (CAD), graphical arts, or publishing, users can view graphical information on one screen and text information on another screen at the same time.

- **Secured connections**—The new RDP client now provides for a highly encrypted remote connection to a Remote Desktop Services system through the use of Windows Server 2008 R2 security. Organizations that need to ensure their data is protected and employee privacy is ensured can implement a highly secured encrypted connection between a Windows Server 2008 R2 Remote Desktop Services system and the remote client.

**Remote Desktop Services Web Access**

Also new to Windows Server 2008 and extended in Windows Server 2008 R2 Remote Desktop Services is a new role called Remote Desktop Services Web Access. Remote Desktop Services Web Access allows a remote client to access a Remote Desktop Services session without having to launch the RDP 6.x client, but instead connect to a web page that then allows the user to log on and access their session off the web page.
This simplifies the access method for users where they can just set a browser favorite to link them to a web URL that provides them with Terminal Services access.

**NOTE**

Remote Desktop Services Web Access still requires the client system to be a Windows XP, Windows Vista, Windows 7, Windows 2003, Windows Server 2008, or Windows Server 2008 R2 server system to connect to a Remote Desktop Services session. A browser user cannot be running from an Apple Macintosh or Linux system and access Remote Desktop Services Web Access. For non-Windows-based web clients, third-party vendors like Citrix Systems provide connector support for these types of devices.

**Remote Desktop Services Gateway**

Remote Desktop Services Gateway is an update to Windows Server 2008 R2 Remote Desktop Services and provides the connectivity to a Remote Desktop Services session over a standard Port 443 SSL connection. In the past, users could only connect to Windows Remote Desktop Services using a proprietary Port 3389 connection. Unfortunately, most organizations block nonstandard port connections for security purposes, and, thus, if a user was connected to an Internet connection at a hotel, airport, coffee shop, or other location that blocked nonstandard ports, the user could not access Terminal Services.

Now with Remote Desktop Services Gateway, the remote user to the Remote Desktop Services Gateway connection goes over Port 443 just like surfing a secured web page. Because of the use of SSL in web page access (anytime someone accesses a web page with https://), effectively now a user can access Windows Server 2008 R2 Remote Desktop Services from any location.

**Remote Desktop Services RemoteApps**

Another new server role added to Windows Server 2008 and updated in Windows Server 2008 R2 is called Remote Desktop Services RemoteApps. Remote Desktop Services RemoteApps allows administrators to “publish” certain applications for users to access. These applications could be things like Microsoft Outlook, Microsoft Word, the company’s time sheet tracking software, or a customer relationship management (CRM) program. Instead of giving users full access to a full desktop session complete with a Start button and access to all applications on the session, an organization can just publish a handful of applications that it allows for access.

Leveraging group policies and Network Policy Server, along with Remote Desktop Services RemoteApps, the administrators of a network can publish different groups of applications for different users. So, some users might get just Outlook and Word, whereas other users would get Outlook, Word, and the CRM application. Add in to the policy component the ability to leverage network location awareness (new to Windows Server 2008 R2 covered in the earlier section “Improvements in the Group Policy Management”), the administrators of the network can allow different applications to be available to users depending on whether the user is logging on to the network on the LAN or from a remote location.
Beyond just limiting users to only the programs they should have access to by policy, Remote Desktop Services RemoteApps minimizes the overhead for each user connection because the user no longer has a full desktop running, but only a handful of applications deemed necessary for the remote user’s access.

**Remote Desktop Services Connection Broker**

Formerly called the Session Broker in Windows Terminal Services, the Remote Desktop Services Connection Broker is a system that manages Remote Desktop sessions to ensure that if users are disconnected from a Remote Desktop server, the users can reestablish a connection to their session without loss of the session state. Without a Connection Broker, users who attempt to reconnect to Remote Desktop Services after a session disconnect might end up logging on to a completely different Remote Desktop server and have to go back to where they last saved data to pick up where they left off.

Other than the name change from Session Broker to Connection Broker, new to Windows Server 2008 R2 Connection Broker is the ability to cluster this role. In the past, this role was a single server instance. In the event that this server session was down, the connection states would not be preserved and the Session Broker would not do its job. By clustering the Connection Broker role, an organization can now add redundancy to a critical role for an organization that has several Remote Desktop servers and wants to provide users with the ability to reconnect back to their session after a temporary disconnect.

**Virtual Desktop Infrastructure (VDI)**

Lastly, a completely new role added to Windows Server 2008 R2 is the Virtual Desktop Infrastructure, or VDI role. Instead of Remote Desktop Services that provides a one-to-many experience, where effectively a single server instance is shared across multiple users, VDI provides a one-to-one virtual guest session relationship between the server and remote client. When a VDI client user logs on to a guest session, a dedicated guest session is made available to the user with a separate client boot-up shell, separate memory pool allocated, and complete isolation of the guest session from other guest sessions on the host server.

Windows Server 2008 R2 VDI provides two different VDI modes. One mode is a personalized desktop and the other is a pooled desktop. The personalized desktop is a dedicated guest session that users have access to each and every time they log on to the VDI server. It is basically a dedicated guest session where the image the guest uses is the same every time. A pooled desktop is a guest session where the user settings (favorites, background, and application configuration settings) are saved and reloaded on logon to a standard template. Actual guest session resources are not permanently allocated but rather allocated and dedicated at the time of logon.

VDI is covered in more detail in Chapter 25.
Improvements in Clustering and Storage Area Network Support

Although clustering of servers has been around for a long time in Windows (dating back to Windows NT 4.0, when it was available, but really didn’t work), clustering in Windows Server 2008 R2 now not only works, but also provides a series of significant improvements that actually make clustering work a whole lot better.

As IT administrators are tasked with the responsibility of keeping the network operational 24 hours a day, 7 days a week, it becomes even more important that clustering works. Fortunately, the cost of hardware that supports clustering has gotten significantly less expensive; in fact, any server that meets the required specifications to run Windows Server 2008 R2, Enterprise Edition can typically support Windows clustering. The basic standard for a server that is used for enterprise networking has the technologies built in to the system for high availability. Windows Server 2008 R2, Enterprise Edition or Datacenter Edition is required to run Windows Server 2008 R2 clustering services.

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

No Single Point of Failure in Clustering

Clustering by definition should provide redundancy and high availability of server systems; however, in previous versions of Windows clustering, a “quorum drive” was required for the cluster systems to connect to as the point of validation for cluster operations. If at any point the quorum drive failed, the cluster would not be able to failover from one system to another. Windows Server 2008 and Windows Server 2008 R2 clustering removed this requirement of a static quorum drive. Two major technologies facilitate this elimination of a single or central point of failure, which include majority-based cluster membership verification and witness-based quorum validation.

The majority-based cluster membership enables the IT administrator to define what devices in the cluster get a vote to determine whether a cluster node is in a failed state and the cluster needs to failover to another node. Rather than assuming that the disk will always be available as in the previous quorum disk model, now nodes of the cluster and shared storage devices participate in the new enhanced quorum model in Windows Server 2008 R2. Effectively, Windows Server 2008 R2 server clusters have better information to determine whether it is appropriate to failover a cluster in the event of a system or device failure.

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

**Stretched Clusters**

Windows Server 2008 R2 also introduced the concept of stretched clusters to provide better server and site server redundancy. Effectively, Microsoft has eliminated the need to have cluster servers remain on the same subnet, as has been the case in Windows clustering in the past. Although organizations have used virtual local area networks (VLANs) to stretch a subnet across multiple locations, this was not always easy to do and, in many cases, technologically not the right thing to do in IP networking design.

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

**Improved Support for Storage Area Networks**

Windows Server 2008 R2 also has improved its support for storage area networks (SANs) by providing enhanced mechanisms for connecting to SANs as well as switching between SAN nodes. In the past, a connection to a SAN was a static connection, meaning that a server was connected to a SAN just as if the server was physically connected to a direct attached storage system. However, the concept of a SAN is that if a SAN fails, the server should reconnect to a SAN device that is now online. This could not be easily done with Windows 2003 or prior. SCSI bus resets were required to disconnect a server from one SAN device to another.

With Windows Server 2008 R2, a server can be associated with a SAN with a persistent reservation to access a specific shared disk; however, in the event that the SAN fails, the server session can be logically connected to another SAN target system without having to script device resets that have been complicated and disruptive in disaster recovery scenarios.

**Addition of Migration Tools**

Beyond the standard migration tools that help administrators migrate from one version of Active Directory to another, or to perform an in-place upgrade from one version of Windows to another, Windows Server 2008 R2 has migration tools to help administrators move entire server roles from one system to another. These new tools provide migration paths from physical servers to virtual servers, or from virtual servers to physical servers. Other tools allow for the migration of DHCP configuration and lease information from one server to another. These tools and the prescriptive guidance help administrators migrate servers more easily than ever before.
### Operating System Migration Tools

Windows Server 2008 R2 provides tools that help administrators migrate from older versions of the Windows Server operating system to Windows Server 2008 R2. The supported migration paths are as follows:

- **Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2**—These operating systems can be migrated to Windows Server 2008 R2 using the operating system migration tools and guidance documentation.

- **x86 and x64**—Servers can be migrated from x86 to x64 and from x64 to x64 with limitations. Because Windows Server 2008 R2 is an x64 operating system only, there is no in-place upgrade support from x86 to x64, so the upgrade path is a server-to-server transition, not in-place. However, x64 to x64 in-place is supported as long as any applications sitting on the server can be upgraded from one x64 platform to the Windows Server 2008 R2 x64 platform.

- **Full Server and ServerCore**—Operating system migration from Full Server to ServerCore and from ServerCore to Full Server are supported typically as a server-to-server migration because in-place migrations between Full Server and ServerCore have limitations. The GUI needs to be added or removed and, thus, applications are typically migrated rather than complete operating system migrations between the platforms.

- **Physical and virtual**—Virtualization of guest sessions is the de facto standard in data centers these days and the implementation of applications on virtual guest sessions is the norm. As such, organizations wanting to migrate from physical server configurations to virtual guest sessions can leverage the migration tools and guidance available in performing server and application migrations to virtual server roles.

### Server Role Migrations

Included in Windows Server 2008 R2 are tools and guidance that help administrators migrate server roles to Windows Server 2008 R2 server systems. The supported migration paths are as follows:

- **Active Directory Domain Services**—The migration from Active Directory 2003 and Active Directory 2008 to Active Directory 2008 R2 is fully supported and covered in Chapter 16 of this book.

- **DNS and DHCP migrations**—New migration tools are available that help administrators migrate their DNS and DHCP servers from running on previous versions of Windows to servers running Windows Server 2008 R2, and not only just the service configurations but also DNS and DHCP data. In the past, the migration of DHCP to a new server usually meant the loss of DHCP lease information. With the new migration tools in Windows Server 2008 R2, an administrator can now migrate the server configuration as well as the lease data, including lease expiration data, as part
of the migration process. These migration tools are covered in Chapters 10 and 11 of this book.

- **File and print migrations**—Included in the migration tools for Windows Server 2008 R2 are features that migrate file data, included file permissions, and the migration of print server configurations and settings from older servers to new Windows Server 2008 R2 configurations. These migration tools help simplify the process of updating servers from old server systems to new systems with the least amount of impact on the organization and drastically simplify the process of migration for domain administrators.

### Improvements in Server Roles in Windows Server 2008 R2

The introduction of Windows Server 2008 R2 added new server roles to Windows as well as enhanced existing roles based on feedback Microsoft received from organizations on features and function wish lists. Server roles are no longer installed by default on a Windows Server 2008 R2 server and have to be selected for installation after the initial installation of the Windows operating system.

Some of the new or improved server roles in Windows Server 2008 R2 include Internet Information Services 7.5, SharePoint Services, Rights Management Service, and Windows virtualization.

### Introducing Internet Information Services 7.5

Internet Information Services 7.5 (IIS) is the seventh-generation web server service from Microsoft. Microsoft completely redesigned IIS 7.0 in Windows Server 2008 rather than just adding more functions and capabilities to the exact same IIS infrastructure as they have done for the past several years. The good part of the new IIS 7.x is that it now provides organizations with the ability to manage multiple web servers from a single console, rather than having to install components and configure each web server individually. This requires organizations to rethink and redesign their web management tasks from pushing the same content to dozens of servers individually to a process where information is pushed to a Shared Configuration store, where common information is posted and shared across all IIS 7.x servers. Organizations can continue to post information the old way by pushing information individually to each server; however, to gain the advantage of the new IIS 7.x services, redesigning how information gets posted should be changed to meet the new model.

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

IIS 7.5 is covered in detail in Chapter 12, “Internet Information Services.”

**Windows SharePoint Services**

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

Windows SharePoint Services is covered in detail in Chapter 35.

**Windows Rights Management Services**

Windows Rights Management Services (RMS) was available as a downloadable feature pack in Windows 2003 and is now included as an installable server role in Windows Server 2008 R2. Windows Rights Management Services sets the framework for secured information sharing of data by encrypting content and setting a policy on the content that protects the file and the information stored in the file.

Organizations have been shifting to RMS rather than the old secured file folder primarily because users who should be saving sensitive information into a file folder frequently forget to save files in the folder, and thus sensitive information becomes public information. By encrypting the content of the file itself, even if a file with sensitive information is stored in the wrong place, the file cannot be opened, and the information in the file cannot be accessed without proper security credentials to access the file.

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

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

Rights Management Services is covered in Chapter 13.
Windows Server Virtualization

A new technology that wasn’t quite available at the time Windows Server 2008 shipped in 2008, but has since been released and available on the original Windows Server 2008 R2 DVD, is Windows server virtualization known as Hyper-V. Hyper-V provides an organization with the ability to create guest operating system sessions, like those shown in Figure 1.11, on a Windows Server 2008 R2 server to get rid of physical servers, and instead make the servers available as virtual server sessions.

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

Virtualization in Windows Server 2008 R2 supports 64-bit and 32-bit guest sessions; has a built-in tool that allows a snapshot of a virtual session so that the session can be protected or rolled back in the event of a guest image failure or corruption; and has virtual sessions that can span terabytes of disk storage and use 16GB, 32GB, or more of memory per guest session. Windows Server 2008 R2 Hyper-V supports “live migrations,” which allows for a faster failover and recovery of a virtual guest session across host servers.

More details on Windows Server 2008 R2 virtualization are covered in Chapter 37.
Identifying Which Windows Server 2008 R2 Service to Install or Migrate to First

With the release of Windows Server 2008 R2, organizations need to create a plan to install or migrate to Windows Server 2008 R2 in a logical manner. Covered so far in this chapter have been all the top features, functions, and technologies built in to Windows Server 2008 R2 that organizations have found as key technologies they implemented to improve technology-driven business processes.

Because Windows Server 2008 R2 provides many different functions, each organization has to choose how to best implement Windows Server 2008 R2 and the various networking features that meet its own needs. In small network environments with fewer than 20 to 30 users, an organization might choose to implement all the Windows Server 2008 R2 features on a single server. However, in larger environments, multiple servers might be implemented to improve system performance, as well as provide fault tolerance and redundancy; thus, a more staged implementation of core services needs to be taken.

Windows Server 2008 R2 Core to an Active Directory Environment

For an organization that does not have Windows Active Directory already in place, that is one place to start because Active Directory Domain Services is key to application and user authentication. For organizations that already have a fully operational Active Directory running on Windows 2003 or Windows 2008, upgrading to Active Directory Domain Services on Windows Server 2008 R2 might be something that is addressed a little later in the upgrade cycle when AD DS 2008 R2 functionality is needed. To get a lot of the Windows Server 2008 R2 server functionality like 2008 R2 DFS, SharePoint Services, Hyper-V virtualization, and so on, an organization can still run on an older Active Directory environment (typically Active Directory 2003 native mode). However, the point is that Active Directory 2008 R2 is not a prerequisite to get Windows Server 2008 R2 server role functionality.

Because Active Directory is more than a simple list of users and passwords for authentication into a network, but rather a directory that Microsoft has embedded into the policy-based security, remote access security, and certificate-based security enhancements in Windows Server 2008 R2, AD DS 2008 implementation does occur earlier in the migration cycle for organizations wanting to implement many of the new Active Directory 2008 R2 technologies, such as Active Directory Recycle Bin, Offline Domain Join, Managed Service Accounts, and the ability to use PowerShell cmdlets within a Group Policy Object.

Windows Server 2008 R2 extends the capabilities of the Active Directory by creating better management tools, provides for more robust directory replication across a global enterprise, and allows for better scalability and redundancy to improve directory operations. Windows Server 2008 R2 effectively adds in more reliability, faster performance, and better management tools to a system that can be leveraged as a true enterprise directory provisioning, resource tracking, and resource management tool. Because of the importance of Active Directory to the Windows Server 2008 R2 operating system, plus the breadth of
capabilities that Active Directory can facilitate, six chapters in Part II of this book are dedicated to Active Directory.

**Windows Server 2008 R2 Running Built-in Application Server Functions**

As much as many administrators think of Active Directory as one of the key areas to upgrade when a new release of the operating system becomes available, in reality, Active Directory tends to not be the first thing updated. Instead, the real business drivers for migrating to Windows Server 2008 R2 typically come from the built-in application server programs that are available on Windows Server 2008 R2.

Windows Server 2008 R2 comes with several programs and utilities to provide robust networking capabilities. In addition to the basic file and print capabilities covered earlier in this chapter, Windows Server 2008 R2 can provide name resolution for the network and enable high availability through clustering and fault tolerance, connectivity for mobile users, web services functions, and dozens of other application server functions.

When convincing management that an upgrade to Windows Server 2008 R2 is important, the IT professional needs to sift through the technologies built in to Windows Server 2008 R2 and pick those services that help an organization use technology to achieve its business initiatives. When planning the implementation of Windows Server 2008 R2, a network architect needs to consider which of the server services are desired, how they will be combined on servers, and how they will be made redundant across multiple servers for business continuity failover.

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

Some of the built-in application server functions in Windows Server 2008 R2 include the following:

- **Domain controller**—Like in previous versions of the Windows operating system, the domain controller enables users to authenticate to the domain for access to network resources.

- **Global catalog server**—The global catalog server is a domain controller that also stores a subset of AD DS objects from other domains in the forest. When an internal or external user with appropriate security rights wants to look at a list of Active Directory users in the forest, the global catalog server provides the list.

- **DNS server**—The domain name system (DNS) maintains a list of network servers and systems and their associated IP addresses, so a DNS server provides information about the devices connected to the network.
Identifying Which Windows Server 2008 R2 Service to Install or Migrate to First

- **DHCP server**—The Dynamic Host Configuration Protocol (DHCP) assigns IPv4 and/or IPv6 network addresses to devices on the network. Windows Server 2008 R2 provides the service function to facilitate DHCP addresses to network devices.

- **Cluster server**—When fault tolerance is important to an organization, clustering provides failover from one system to another. Windows Server 2008 R2 provides the ability to link systems together so that when one system fails, another system takes over.

- **Network Policy Server**—NPS is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy. NPS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless and virtual private network (VPN) connections. NPS routes authentication and accounting messages to other RADIUS servers. It also acts as a health evaluation server for Network Access Protection (NAP).

- **Remote Desktop server**—Instead of having a full desktop or laptop computer for each user on the network, organizations have the option of setting up simple, low-cost thin terminals for users to gain access to network resources. Windows Server 2008 R2 Remote Desktop Services allows a single server to host network system access for dozens of users.

- **Remote access server**—When a remote user has a desktop or laptop system and needs access to network services, Windows Server 2008 R2 provides remote access services that allow the remote systems to establish a secure remote connection.

- **Web server**—As more and more technologies become web-aware and are hosted on web servers, Windows Server 2008 R2 provides the technology to host these applications for browser-based access.

- **Media server**—With information extending beyond text-based word processing documents and spreadsheets into rich media such as video and audio, Windows Server 2008 R2 provides a source for hosting and publishing video and audio content.

- **Virtualization server**—Windows Server 2008 R2 provides the core capabilities to do server virtualization, providing the capability for an organization to consolidate physical servers into fewer host server systems, thus decreasing the total cost of IT operations.

- **Distributed File System (DFS) server**—For the past decade, data files have been stored on file servers all around an organization. Windows Server 2008 R2 provides Distributed File Systems that allow an organization to take control of distributed files into a common unified namespace.

These plus several other functions provide robust networking services that help organizations leverage the Windows Server 2008 R2 technologies into solutions that solve business needs.
Windows Server 2008 R2 Running Add-in Applications Server Functions

Although some of the newer, built-in server application functions in Windows Server 2008 R2—such as Network Policy Server, server virtualization, Remote Desktop Services Web Access, Media Server, and so on—provide key areas for organizations to select as initial areas to implement Windows Server 2008 R2 technologies, other organizations might find add-in applications as being the key areas that drive an initial implementation of Windows Server 2008 R2. Some of the add-in applications come from Microsoft, such as the Microsoft Exchange Server 2010 messaging system or Microsoft SQL Server 2008 database system. Other add-ins to Windows Server 2008 R2 are provided by companies that provide human resource management applications; accounting software; document management tools; fax or voicemail add-ins; or other business, industry, or user productivity capabilities.

In earlier Windows Server operating systems, the core operating system provided simple logon and network connectivity functions; however, with Windows Server 2008 R2, the operating system includes many core capabilities built in to the Windows Server 2008 R2 operating environment. With integrated fault tolerance, data recovery, server security, remote access connectivity, web access technologies, and similar capabilities, organizations creating add-ins to Windows Server 2008 R2 can focus on business functions and capabilities, not on core infrastructure reliability, security, and mobile access functionality. This off-loading of the requirement of third-party add-in organizations to implement basic networking technologies into their applications enables these developers to focus on improving the business productivity and functionality of their applications. Additionally, consolidating information routing, security, remote management, and so on into the core operating system provides a common method of communication, authentication, and access to users without having to load up special drivers, add-ins, or tools to support each and every new application.

Much of the shift from application-focused infrastructure components to core operating system-focused functionality was built in to Windows 2000 and then later enhanced in Windows 2003 and Windows Server 2008. There were many challenges to earlier versions of the Windows operating system; however, after being on the market for many years now, Windows Server 2008 R2 add-ins have had several revisions to work through system functionality and component reliability between application and operating system. Fortunately, Windows Server 2008 R2 uses the same application/operating system technology used in Windows 2003 and Windows Server 2008, so applications written for Windows 2003 and Windows Server 2008 typically need just a simple service pack update to be able to run on Windows Server 2008 R2, if anything at all.

Summary

This introductory chapter was intended to highlight the new features, functions, migration tools, and management utilities in Windows Server 2008 R2 that will help administrators take advantage of the capabilities of the new operating system. If Windows Server 2008 R2 is seen as just a simple upgrade to Windows 2000/2003/2008, an organization
Best Practices

The following are best practices from this chapter:

- When implementing Windows Server 2008 R2 for the first time, or migrating to Windows Server 2008 R2 from a previous version of Windows, choose to implement the technologies in Windows Server 2008 R2 that will provide the organization with the most value in terms of employee productivity enhancements or regulatory compliance security improvements first.

- When considering adding a Windows Server 2008 R2 server to an existing Windows 2000/2003/2008 Active Directory environment, consider implementing things like Remote Desktop Services Web Access, SharePoint Services, or Windows virtualization, which have proven to be pretty easy to implement and provide a lot of value to organizations.

- To ultimately improve Windows security, tune and optimize Windows Server 2008 R2 for a secured networking environment.

- Use Remote Desktop Services in Windows Server 2008 R2 to provide users with access to local hard drives, as well as to redirect the audio from a centralized Terminal Server to a remote system.

- Use Windows Deployment Services (WDS) to create client system images that can be quickly and easily rolled back through Group Policy.

- Windows Server 2008 R2 virtualization can help organizations deploy clustering and add in disaster recovery data centers without having to add additional physical servers to the network.

- Remote and branch office locations greatly benefit from the use of Read-Only Domain Controllers, Distributed File System Replication, BitLocker security, and distributed administration tools built in to Windows Server 2008 R2.

- Using the new Windows Server 2008 R2 Server Manager can simplify the task of a network administrator trying to access information residing on different servers and in different server roles in the environment.
It is best to run the Group Policy Management Console on a Windows Server 2008 R2 or Windows 7 system to have access to all the policy features available (compared with running GPMC on a Windows XP or Windows Server 2003 system).
SYMBOLS

$Errors variable, 741
$Procs object collection, 712
$Sessions variable, 761

A

accelerators
  types, 713-714
  WMI, 749
accepting terms, 91, 101
access, 8
  access-based enumeration, 1122, 1162
  applications, troubleshooting, 1282
  BranchCache, 31
  CALs, 1435
  control policies, 790
  DFS, 1101
  DHCP activity logs, 350
  DirectAccess, 28-29, 863-872
  disaster recovery, 1277-1282
  empty-root domain model, 165
  file systems, 1102-1104
  files, auditing, 431-433
  Group Policy, 585-586
  groups, RDS, 958
  limitations, 460
  logon
    restrictions, 421
    smart cards, 423
    management, 1122-1128
  MMC management, 1075-1076
  mount points, 1107
  NAP, 349-350, 459-461
  networks, troubleshooting, 1278
  offline files, 1123
OUs, delegating administration, 184-186
Performance Options window, 1418
permissions, 471
physical restrictions, 421
physical site failures, 1274
PowerShell, 705
Registry, 745
remote, 847-850. See also remote access
removable storage, 1075
resources, auditing, 671-674
Routing and Remote Access dialog box, 479
RRAS, 462
Unmapped UNIX User Access, 247
Windows Server Backup, 1285-1287
access-based enumeration, 1122-1123,
1162-1163
access control entries (ACEs), 178
Access Permission section, 479
accidental deletion protection, 1254-1255
accounting improvements in NPS, 461
accounts
computer migration, 513-515
disaster recovery documentation, 1234
FIM, provisioning, 238, 241-243
Group Account Migration Wizard, 511
Krbtgt, 1306
lockout settings, 1077
preformatting AD computer, 1013
RMS Service, 453
security, 814
Service Account Migration Wizard, 515
UAC, 1046-1048
user migration, 512-513
ACEs (access control entries), 178
actions, 658
preferences, 1039
tasks, 1386
Actions menu, 1457
Actions pane, 380
activation
RD Licensing servers, 978
Windows operating systems, 94
Windows Server Core, 108
Active Directory. See AD
Active Directory Administrative Center, 19
Active Directory Certificate Services. See AD CS
Active Directory Domain Services. See AD DS
Active Directory Federation Services. See AD FS
Active Directory in Application Mode (ADAM),
21, 228
See AD LDS
Active Directory Rights Management Services.
See AD RMS
Active Directory Users and Computers tool, 17
active nodes, 1179
active/active clusters, 1180
active/passive clusters, 1179
ActivePerl scripts, 257
activity logs, DHCP access, 350
activity, monitoring users, 1349
AD (Active Directory)
authentication, 10
authoritative restores, 1297
backups, 1251-1256
Certificate Services, 1257-1259
changes in, 20-22
clients, monitoring configuration, 823-824
computer accounts, preformatting, 1013
containers, delegating GPO administrative
tasks, 636-637
design, 147-149
DNS zones
integration, 132
moving, 505
Federation Services, expansion in, 21
global catalog roles, 370
special-purpose domain model, 169-170
structures, 116-119, 154-155
TCP/IP compatibility, 115
tools, 675

AD DS Service Interfaces (ADSI), 121

AD FS (Active Directory Federation Services), 227, 232-236
applying, 235-236
components, 233
installation, 233-235
MMC administrative tools, viewing, 233

AD LDS (Active Directory Lightweight Directory Services), 227-232
configuration, 231
features, 229
installation, 229-232
instances, connections, 232
need for, 228
tools, 675

AD RMS (Active Directory Rights Management Services), 451-454
installation, 452-454
need for, 451
prerequisites, 451-452
tools, 675

AD-integrated zones, 285-286

ADAM (Active Directory in Application Mode), 21, 228

adapters
HBAs, 1187
networks, 1176

Add Account Partner Wizard, 235
Add Applications Wizard, 236
Add Cell to Display Filter, 1401
Add Features Wizard, 364
Add Image Wizard, 999
Add Publishing Point Wizard, 1498
Add Resource Partner Wizard, 235
Add Roles Wizard, 235, 248, 263-266, 334, 1444, 1522

Add Site Binding dialog box, 412
Add Web Site page, 390
add-on application server functions, running, 46
adding
boot images to WDS servers, 998-999
counters with Performance Monitor, 1362
disks, 1110-1112
domain controllers to sites, 557-558
domains, 107, 158-159
drivers to images, 1008
exclusions, 315
features, 97-98
File Services roles, 1120-1121
health policies to NPS, 471
Hyper-V roles, 1522-1524
install images to WDS servers, 999-1000
IPv6 hosts, 315-36
media to playlists, 1494
namespaces, 1157-1158
nodes
clusters, 1199-1200
NLB, 1221-1222
printers, 578-580
RAM to guest operating system sessions, 1533
roles, 97, 647
servers, 1157-1158
SMTP to servers, 1450
storage, 1200-1201, 1544-1545
users to NIS, 255-256
Windows Server 2008 R2, 11
additional tasks, upgrading, 99-100
addresses
APIPA
disabling, 344
IP, 330-332
Global Address List, 1393
IP, 88
IPv6, 215, 299-301, 311-313
ISATAP, 303-305
MAC, 1528
networks, 326
static IPv4 IP, assigning, 106-107
unique, 328
ADM
files, 603
subfolders, 593
administration, 548-549. See also management
AD, 551-553. See also AD (Active Directory)
administrative models, 550-551
benefits for, 22-26
Central Administration console, 1449
CMAK, 917-919
Computer Configuration Administrative Templates node, 1032
desktops, 985-988, 1020-1021
DFSR, 31-32
DHCP, 351, 358. See also DHCP (Dynamic Host Configuration Protocol)
distributed administration, optimizing, 33
documentation, 780-784
domains
decentralized, 158
forests, 565
single, 564
ease of, AD DS, 115
encryption, 1099
file system quotas, 1098-1099
GPOs, 619-637, 1043-1045
Group Policy, 585-586, 634. See also Group Policy
IIS delegation, 379
manuals, 783
models
centralized, 550
distributed, 550-551
mixed, 551
NFS, 249-250
optimization, 256-257
OU delegation, 184-185
passwords
configuration, 94
Directory Services Restore Mode, 1316
modification, 695
modifying, 106
RDS, 923
enabling, 953-955
planning, 948
remote
support, 989
Telnet Server, 256-257
Remote Server Administration Tools, 675-677
Role Administration Tool, 982
roles, separation at branch offices, 1307
RRAS servers, 479
security, 117, 412-414
Server Manager. See also Server Manager
Windows Media Services, 1489
WSS site collection, 1475-1479
Administrative console, Hyper-V, 1524-1529
administrative templates
customization, 606
for operating systems, 604-606
Group Policy, 594, 603-606
types of, 603
administrators
local, 1034-1036
local user policies, 589
policies, 1025

How can we make this index more useful? Email us at indexes@samspublishing.com
Run As Administrator command, 422-423 templates, Group Policy, 594
ADML files, 603
ADMT
installation, 507-508
lab environments, applying, 507
migration prerequisites, 508
v3.1 functionality, 506-507
ADMX
files, 603
Migrator tool, 613
ADOs (Active Directory Objects), exporting PowerShell, 1253
adprep utility, 496-497
ADSI (AD DS Service Interfaces), 121
ADSIEdit, 228
Advanced Encryption Standard (AES), 852
advanced functions, PowerShell, 709-710
advanced security, Windows Firewall integration, 424-428
advanced settings, triggers, 1385-1386
Advanced Tools section, 650
AES (Advanced Encryption Standard), 852
agentless exception monitoring, 800
agents
certificate configuration, 836
DMZ installation, 835
domain members, 820
downloading, 822
DRA, 1324, 1425
DSAs, 120
MA, 237, 239-240
management, 800
Nontrusted Domain Agents, monitoring, 811
OpsMgr
deployment, 820-822
security, 812
proxy configuration, 822-823
relay, DHCP 332-333
restarting, recovery, 822-828
roles, monitoring, 801
SHA, 461
aging DNS, 280-281
AGPM (Microsoft Advanced Group Policy Management), 612
agreeing on designs, 66-67
Alert Priority parameter, 838
Alert Severity parameter, 828
alerts
customization, 798
disabling, 838
document libraries, 1455
generating, 798-799
OpsMgr, tuning, 837-845
WSS, 1458
aliases
cmdlet, 723
PowerShell, 722-723
All Setting Disabled option, 573
All Users Host-Specific Profile, 728
All Users Profile, 728
all-in-one servers, 807
Allitems.aspx view, 1456
allocation
hardware, 544
Windows Server 2008 R2, 544
alternate network capabilities, DHCP clients, 344
analysis. See also troubleshooting
Best Practice Analyzer (BPA), 25-26, 1371-1372
capacity, 1389-1391
benefits of, 1392-1393
defining, 1391-1395
MBSA, 1394
processor usage, 1419-1420
Announcement File (.asx), 1494
anti-replay capability, 455
antivirus, 433
  configurations, 790
  RDS, 948
  upgrading, 54
APIPA (Automatic Private IP Addressing), 88, 330-332
  disabling, 344
APIs (application programming interfaces), 379, 459
Apple Mac
  file systems, 1104
  services, 1104
Application log, 1353
application programming interfaces (APIs), 379, 459
application service providers (ASP), 922, 924-925
applications
  access, troubleshooting, 1282
  AD LDS configuration, 231
  antivirus, 433
  assessments, 54
  availability, 1177
  compatibility
    RDS, 948-949
    testing, 541
  directory services, 114
  failover clusters, 1186-1187, 1203-1205
  failures, 1275
  Group Policy, troubleshooting, 575-577
  installation, 958
  lab-testing existing, 543-545
  loading, 544-545
  management, 988
  Microsoft Desktop Optimization Pack for Software Assurance, 612-613
  monitoring, 1347
NLB, 1215
  partitions, 286-287
  pools, 381, 390
  prioritizing, 537
  readiness verification, 488-489
  researching, 534-537
  servers
    add-on functions, running, 46
    running built-in functions, 44-45
    Windows Server 2008 R2 as, 8-10
  services, 9, 535-536
  site links, 553
  testing, 526, 527-529, 1206
WSS, 1441-1442, 1469. See also WSS (Windows SharePoint Services)
Applications and Services Logs folder, 1354-1355
AppLocker, creating, 1052-1055
applying
  6to4 tunneling protocol, 305-308
  AD FS, 235-236
  ADMT lab environments, 507
  background jobs, 720
  BranchCache, 1124-1125
  external disk subsystems, 1109
  filters, 1400
  FSRM, 1130-1131
  GPOs, 599
  IPSec encryption, 454-456
  ISATAP, 303-305
  manual backups, 1247-1249
  NFS, 249-250
  OpsMgr, 802-805
  patches, 644
  PowerShell, 703, 732-762
    modules, 755-757
    New-Object cmdlet, 757-762
    remoting, 757-761
assignment
client sites, 201
permissions to IIS user accounts, 414-415
static IPv4 IP addresses, 106-107
tasks
during disaster recovery, 1273
to backup teams, 1235
associating subnets with sites, 201-202, 209
assumptions, migration documentation, 71
asynchronous full zone transfers (AXFR), 276, 1427
AT&T, 29
attaching VHDs, 1117, 1118
attributes, 237
SID History, 506
audio, capturing, 1508-1510
Audit Collection Services, 800
auditing
AppLocker enforcement, 1053
DLL event log audit events, 1054
evironments, 665-674
file access, 431-433
granular, 493
NTFS folders, 1279
policies, 665-670, 1438
printing, 674
resource access, 671-674
Web services, 409
Auditing Entry window, 672
AUDITPOL command, 670
Authenticated Users group permissions, 1312
authentication
XXXX802.1X, NPS 462
Active Directory, 10
AD DS, 118, 246
background sessions, 933
BitLocker, 1330
EAP, 857
FTP, 396-403
IIS, 408-409
IPSec, 857
Kerberos, 133, 420
  support, 247
L2TP, 857
Network Level Authentication, RDS, 981
PEAP, 857
placeholder domain model, 169
PPTP, 857
RODCs, 22
RRAS, 856-858
selecting, 858-859
SSL, 410
Authentication feature page, 394
Authentication Rules feature page, 395
AuthenticationLevel property, 751
authoritative restores
  Active Directory, 1297
  backlinks, 1298
authorization
  background sessions, 933
  DHCP, 360
  HCAP, 462
Authorize DHCP Server page, 335
autoenrollment, certificates, 879-880, 904-905
Automated Deployment Services, 991
Automatic Private IP Addressing. See APIPA
automatic updates, 682-684
Automatic Updates clients, deployment, 434
automation
  DHCP database backup and restore, 337-338
  DNS, creating zones, 287
  guest sessions, launching, 1536-1537
  PowerShell, 697-699. See also PowerShell
  replication, 1147
  Task Scheduler, 1383
  updating, enabling, 96-97
  WAIK, 1007, 1018
AutoStart, broadcasts, 1485
autouninstall of software packages, 1089
availability
  applications, 1177
  High Availability Wizard, 1548
  services, 1177
Available section, 1113
avoiding full AD synchronization, 213
awareness, NLA, 587
AXFR (asynchronous full zone transfers), 276, 1427
back-end enterprise messaging systems, 1178
Background Intelligent Transfer Service (BITS), 98, 435
backgrounds
  jobs, 720
  migration documentation, 70
  section, documentation, 65
  session authentication, 933
  work, reducing, 640
backlinks, authoritative restores, 1298
Backup Domain Controller (BDC), 1306
backups, 1226-1227
  accidental deletion protection, 1254-1255
  Active Directory, 1251-1256
  Big Bang migration, 489
  command line, 1252
  databases, DHCP automation, 337-338
  DFS, 1166-1167, 1261
  DFSR, 32
  DHCP 1260
  disaster recovery documentation, 787-788

How can we make this index more useful? Email us at indexes@samspublishing.com
DNS, 1259
documentation, 1234
DVDs, 1245-1246, 1286
failover clusters, 1211-1215
files, 89
GPOs, 633-634
history, viewing, 1247
IIS, 1261
items, excluding, 1250-1251
media files, 1237
NLB nodes, 1223
OpsMgr, 807
options, 1228-1232, 1237-1238
preparedness, 1267-1271
procedures, 1235
roles, 1248
security deployment, 434
selecting, 1284
servers, 98
starter GPOs, 625-627
strategies, 1234-1235
System State, 1249-1250, 1394
upgrading, 54
validation, 694
verification, 686
VSS, 1100, 1167, 1262-1264
wbadmin.exe, 1246-1249
Windows Server Backup, 662-663, 1167, 1235-1238
WINS, 1259-1260
WSS, 1261-1262
baselines
benchmarks, 1394-1395
documentation, 789
MBSA, 1394
metric, 1393-1394
performance values, 789
policies, 1393-1394
value configuration, 1369-1371
Bash (Bourne Again shell), 700
basic disks, 1105-1106
dynamic disks, converting, 1112
basic features of WSS, 1436-1437
basic firewalls, 476
batteries, 1174. See also power
BDC (Backup Domain Controller), 1306
BDC (Business Data Catalog), 1438
behavior, memory, 1417
benchmarks, baselines, 1394-1395
benefits
of administration, 22-26
of BitLocker Drive Encryption, 1324
of capacity analysis, 1392-1393
of document libraries, 1464
of documentation, 764-765
of performance optimization, 1392-1393
of RDS, 922-923
Best Practice Analyzer, 25-26, 379, 1371-1372
best practices
DFS replication, 1161-1162, 1161-1162
failover cluster node backups, 1212
groups, 186-187
permissions, sharing, 1128
Big Bang migration, 487-491
backups, 489
hardware compatibility verification, 488
prerequisites, 487-488
recovery, 489
single domain controller servers, 489-491
virtual domain controller rollback option, 489
binding
SSL sites, adding, 412
verification, 334
Bindings button, 342
bit rates, selecting, 1507
BitLocker Drive Encryption, 31, 450, 790, 1323-1326
authentication, 1330
benefits of, 1324
configuration, 1326-1333
deleting, 1333
deployment, 1326
enabling, 1327-1332
hardware requirements, 1325
installation, 1326-1327
overview of, 1324-1325
partitions, 1327
recovery passwords, 1332-1333
tools, 676
volumes, enabling, 1331-1332
BITS (Background Intelligent Transfer Service), 98, 435
BITS Server Extensions Tools, 676
blackouts, rolling, 1229
block inheritance, Group Policy, 598
Block Policy Inheritance option, 573
blocks, 1131. See also screening files
BMC Patrol, 788
BMC Performance Manager, 1414
booting
discover images, creating, 1006
Diskpart.exe command-line utility, 1110
from SANs, 1109
images
adding drivers, 1008
manual driver injection, 1010
WDS, 992-993
BOOTP (Bootstrap Protocol), 329
bottlenecks, 1400, 1415-1416
Bourne Again shell (Bash), 700
Bourne shell, 700
BPA (Best Practice Analyzer), 379, 1371-1372
branch offices, 1303-1306
concerns and dilemmas, 1307-1308
DFS, 1340-1341
Group Policy, 1341
Next Generation TCP/IP stacks, 1339-1340
physical security, 1303
replication, 1339-1342
RODCs, 30, 1306-1310, 1339
SMB, 1341-1342
support, 30-33
WANs, 1339-1342
BranchCache, 31, 1124-1125
client configuration, 1334-1336
server configuration, 1334-1335
troubleshooting, 1338
breach identification procedures, security, 790
breadth, geographical, 61-62
bridgeheads, links, 129
bridging
IPv4, 301
site links, 204
broadband, 29
broadcasts, 1484. See also Windows Media Services
AutoStart, 1485
live events, 1506-1508
publishing, 1496-1504
stored single files, 1495-1497
budgets
compatibility testing, 531
estimates, 66
migration documentation, 72
power, 640

How can we make this index more useful? Email us at indexes@samspublishing.com
build procedures, server documentation, 781-782
building
  labs, 73-74
  system-level fault tolerance, 1174-1177
built-in
  functions, application servers, 44-45
  PowerShell providers, viewing, 727
  security tools, 420
Business Data Catalog (BDC), 1438
business goals, 50-53, 52-53
business-function OU designs, 188-191

c
C
  C shell, 700
CA (Certificate Authority), 210, 444, 445-446
cabinet files, starter GPOs, 625
caches
  BranchCache, 31, 1124-1125, 1333-1338
  client-side, 294, 1123-1124
  credentials, 22, 1306, 1309
  disabling, 1127
  limitations, 373
  management, 1484
  universal groups, 211-212, 371, 492
CAD (computer-aided design), 34
calendar.aspx page, 1465
calendars
  editing, 1466
  events, 1468
CALs (client access licenses), 41, 1435
  installation, 978
Canonical Name (CNAME) records, 270
capabilities that simplify tasks, 17-20
capacity analysis, 1389-1391
  benefits of, 1392-1393
  defining, 1391-1395
  Network Monitor, 1398-1404
  OpsMgr limitations, 809-810
  Performance Monitor, 1405-1408
  SCCP, 1413
  Task Manager, 1396-1398
tools, 1395-1415
Capture Filter pane, 1401
capturing
  audio, 1508-1510
  images, 993, 1016-1020
  screen content, 1510-1511
  video, 1508-1510
cards, networks, 1218
CD (connected delivery), 237
CD-ROM updates, 681
CD/DVD images, mounting, 1534-1535
CDs
  access, 1075
  Windows Server Backup, 1236
CEIP (Customer Experience Improvement Program), 97
Central Administration console, 1449, 1479
Central Administration console tools, 1437
Central Details pane, 380
central stores, GPOs, 594
  creating, 620-621
  verification, 621-622
centralized administration model, 550
Certificate Authority (CA), 210, 444, 445-446
Certificate Enrollment Web Service, 446
certificate revocation lists (CRLs), 446
Certificate Services, AD, 1257-1259
certificates, 790
  AD CS, 444-450
  agent configuration, 836
autoenrollment, 879-880, 904-905
digital, 444
DMZs, monitoring, 831-837
IP-HTTP, 905-906
requests, 411
root CA server requests, 832-835
servers, 856, 878-879
SSL, 409-413, 1337
templates for IP-HTTPS customization, 903-904
templates, formatting, 831-832
certification, 545
CGI feature page, 395
change. See also modification
control, 790-791, 1269-1270
functionality, password configuration, 255
management procedures documentation, 788
characters, Unicode support, 286
checklists, documentation, 776, 781
CHKDSK, 694
CIFS (Common Internet File System), 250
CIR (Committed Information Rate), 785
classes
  ManagementObject, 749
  ManagementObjectSearcher, 750
static, 712
classification
  FCI, 1099-1101, 1130, 1140-1141
  files, 1131, 1140-1141
  properties, 1141-1142
  rules, 1143-1144
clean version installation, 89-98
cleanup tasks, domain rename, 173
CLI (command-line interface), 700
  navigation, 706-707
  PowerShell, 705
client access licenses. See CALs
Client Access Point, 1179
Client Experience Configuration page, 929
client-side caching, 1123-1124
clients
  AD, monitoring configuration, 823-824
  ADMT impact, 506
  Automatic Updates deployment, 434
  BranchCache configuration, 1334-1336
caches
  client-side, 1123
  troubleshooting, 294
connection restrictions, 1166
DHCP
  alternate network capabilities, 344
  configuration, 472-473
  services, 330
dialers, Connection Manager, 917
DNS, 318
EC, 461, 618
Group Policy. See also Group Policy
  Group Policy management, 1022-1024
  lease restrictions, 472-473
NetBIOS resolution, 368
NFS, customizing, 250-251
RDP, 33-34
RDS, 927
sites, assigning, 201
SSLF, 622
UNIX
  configuration, 250-251
  installing Telnet servers, 257
VPNs, 854
  configuration, 888-891
  gateways, 476
  troubleshooting, 890-898
WSUS configuration, 437-439

clocks, configuration, 95

How can we make this index more useful? Email us at indexes@samspublishing.com
cloning, 990
   BitLocker, 1326
Cluster Shared Volumes. See CSV
clustering, 50
   building, 1174-1177
   Create Cluster Wizard, 1195
   DHCP servers, 357-358
   disk majority clusters, creating, 1543-1544
   failover, 1177, 1182, 1183
      backups, 1211-1215
      creating, 1195-1196
      deleting nodes, 1210-1211
      deploying services or applications, 1203-1205
      deploying virtual machines, 1546-1548
      deployment, 1191-1192
   geographically dispersed, 1213-1215
   installation, 1541-1542
   maintenance, 1208-1210
   operating systems, 1190
   overview of, 1184-1190
   testing, 1206-1208
Failover Clustering
   installation, 1193
   tools, 676
   heartbeats, 1180, 1215
   migration, 1211
   network configuration, 1196-1199
NLB, 379, 1178, 1184
   creating, 1218-1221
   deployment, 1215-1222
   maintenance, 1223-1225
   management, 1223-1225
No Majority: Disk Only Quorum model, 1185-1186
Node and Disk Majority Quorum model, 1185
Node and File Share Majority Quorum model, 1185
Node Majority Quorum model, 1184-1185
   nodes, adding, 1199-1200
   operation mode, 1217
   optimizing, 37-38
   quorums, 1180
      configuration, 1201-1202
      witness disk configuration, 1541
   resources, 1179
   servers, 45
   shared volumes, enabling, 1202-1203
   single points of failure in, 37-38
   storage, adding, 1200-1201
   stretched clusters, 38
   system-level fault tolerance, 1171
   technologies, 1177-1184
   terminology, 1179-1182
   test criteria, 529
   upgrading, 1211
   witness files, 1180
CMAK (Connection Manager Administration Kit), 852, 917-919
cmdlets, 707-708
   aliases, 723
   Copy-Item, 744
   debugging, 704
   Get-Alias, 723
   Get-Content, 744
   Get-EventLog, 739-741
   Get-Help, 733-734
   Get-ItemProperty, 745
   Get-Process, 746
   Get-WmiObject, 747, 751
   Import-Module, 757
   Invoke-Command, 759
   Invoke-WMIObject, 747, 751
   manual backups, 1247-1249
   Move-Item, 744
   New-Item, 743
New-Object, 757-762
New-PSSession, 760
Out-Default, 715
PowerShell, Windows Server Backup, 1238
Remote-Item, 743
Remove-WMIObject, 753
Rename-Item, 744
Set-ItemProperty, 745
Set-WMIInstance, 751
Sort-Object, 747
CNAME (Canonical Name) records, 270

collaboration
benefits of documentation, 764
sessions, 63-64
WSS, 1439
collisions, replication, 197
Color Filters, 1401
columns, logs, 1356
COM (Component Object Model), 702
combining files, Windows Media Services, 1501-1503
command line
backups, 1252
BitLocker installation, 1327
Diskpart.exe, 1110, 1114-1116
DNSCMD, 296-297
interface. See CLI
IPCONFIG, 295
Netsh, 358-359
NSLOOKUP, 294-295
RDS management, 982
scripts, 1489
TRACERT, 295-296
Web Server (IIS) role, installing, 387-388
command prompt, launching, 105-106
commands
AUDITPOL, 670
Get-Command, 734-736
netsh branchcache show status, 1338
oobe.exe, 643
PowerShell, 18, 707-711
Run As Administrator, 422-423
shells, 800
xcopy, 7
Committed Information Rate (CIR), 785
Common Internet File System (CIFS), 250
common language runtime, 420
communication
during disaster recovery, 1272
planning, documentation, 771-772
ports, 813
skills, 59
comparisons, baselining records for
documentation, 789
compatibility
applications, RDS, 948-949
HCL, 1109
RDS, Windows Installer, 929
TCP/IP AD DS, 115
testing, 523-526
applications, 541
defining goals for, 530-533
documentation, 533-534
lab-testing existing applications, 543-545
MAP toolkit, 542-543
need for, 526-527
preparing for, 527-534
Prototype phase, 546-547
requirements, 532-533
results, 542, 546
states, 538-541
tracking sheets for application
compatibility research, 538
upgrading, 542
vendor verification, 537-542
verification, 99

How can we make this index more useful? Email us at indexes@samspublishing.com
Compatibility Report page, 102

competent PC restores, 1291

completion documentation, 780

compliance, 1438

health policies, creating, 466-467

health policy, 460

Component Object Model (COM), 702

components

AD DS, outlining, 119-124

AD FS, 233

DirectAccess, 869-871

DNS, 278-285

DNSSEC, 317-318

enterprise networks, 326-328

file systems, 1097-1102

NAP, outlining, 460

needed for guest operating system sessions, 1529-1530

OpsMgr, 798-802, 805-807

UNIX

integration, 245-252

interoperability, 247-248

VPNs, 853-925

Windows Media Services, 1484-1489

compression

data, 1099

NTFS volumes, 1099

RDC, 1102, 1150

replication, disabling, 212

Compression feature page, 395

Computer Configuration Administrative Templates node, 1032

Computer Configuration node

Group Policy, 1029-1032

Computer Measurement Group, 1395

computer-aided design (CAD), 34

computername parameter, 752

computers

account migration, 513-515

competent PC restores, 1291

default local computer policy, 589

discovery, 820

fair share CPU scheduling, 929

GPOs

Computer Configuration node, 590

processing, 586-587

Group Policy management, 1045-1069

names, 87, 96, 642

policies, processing, 1027

powering, 1174-1175

conditions, 658, 1386-1387

configuration

AD

clients, 823-824

LDS, 231

lookups, 250

replication, 824-826

administration passwords, 94

agent proxy, 822-823

AppLocker, 1052-1055

as-built documentation, 782-783

autouninstall of software packages, 1089

baseline values, 1369-1371

BitLocker Drive Encryption, 1326-1333

BranchCache

clients, 1334-1336

servers, 1334-1335

certificates, servers, 878-879

clocks, 95

clustering

networks, 1196-1199

quorums, 1201-1202

witness disks, 1541

Computer Configuration Administrative Templates node, 1032
connection objects, 198-199
CSV, 1545-1546
customizing, 92-98
default settings, 642
Delay, 354
DHCP, 472-473
    reservations, 346-348
    scopes, 348
DHCPv6, 313-315
DirectAccess, 900-901, 906-910
disks, 1115
DNS servers, 266
DNSSEC zones, 318-323
domains, SIDs, 510-511
e-mail, WSS, 1449-1452
endpoints, 785
event subscriptions, 1354-1355
failback, 1204-1206
failover, 1204-1206
features, delegation, 415
files
    file system quotas, 1098-1099
    screens, 1135-1139
    shares, 1152
firewalls
    GPOs, 901-903
    Group Policy, 1062-1065
folder redirection, 1071-1075
FTP, 397-407
GPOs
    central stores, 620-621
    Computer Configuration node, 590
    links, 629, 1046
    reports, 632
    starter, 622-625
granular session control, 940-941
Group Policy, 569-575, 585-586, 1028-1033. See also Group Policy
domains, 628-629
    power, 1068-1069
    RDS, 1060-1062
groups, 564-568, 1080-1084
guest operating system sessions, 1533-1535
hardware, 544
    hardware-level RAID, 1176
    health policies, 466-472
    host servers, 1526-1529
IIS websites, 389-397
Initial Configuration Tasks, 95, 641-643
intersite replication intervals, 200
IP migration, 520-521
IPv6, 311-316
models, failover clusters, 1184-1190
networks, 95-96
New Configuration Wizard, 1529
NFS, shared network resources, 252
notification, 1146
NPS, 880-886
NTFS permissions, 1152
offline files, 1123
OprMgr, 822-831
options, FSRM, 1133
outgoing emails, 1451-1452
passwords, change functionality, 255
Performance Monitor management, 1363-1364
permissions, 32, 1128
planning, 54
policies, GPOE, 609
power sources, 640-641
preferences, item-level targeting, 1058-1060
Print Management console, 578
proxy, 790
push/pull partners, 365
quotas, 1129
  on file types, 24
  templates, 1134-1136
  with FSRM, 1133
real-time live broadcasts, 1492-1494
Remote Assistance, 955
Remote Desktop Session Host servers, 959-961
remoting, 718
reviewing, 1447
RODC administrator rights, 223
RRAS servers, 477, 886-887
SCCM, 1396
Scheduled Tasks, 1069
scopes, 333-336
SCW, 1026
security
  FTP sites, 400-401
  templates, 591
Server Manager, 657-661
servers
  for single on-demand video playback, 1496-1497
  playlists, 1501-1503
Sfc.exe, 1120
shadow copies, 1168
Share and Storage Management console, 1118-1128
Shared Configuration store, 40
shares, 1122-1128
SHV, 466
sites, 554-562, 1479
split-scope, 351
standalone local Group Policy, 1033-1036
System Center Configuration Manager 2007, 460, 990
System Configuration utility, 1295
tasks, 1387-1388
time zones, 95
triggers
  advanced settings, 1385-1386
  options, 1384-1385
tunnels, 303
UAC, 1046-1048
UNIX clients, 250-251
User Configuration node, 1032-1033
Validate a Configuration Wizard, 1193-1195, 1542-1543
VHDs, 1117
volumes, fault tolerance, 1112-1116
VPN clients, 888-891
WDS
  DHCP 997-998
  servers, 994-997
website properties, 392-397
Windows Firewall, 98
Windows Media Services, 1491-1492
Windows Server 2008 R2, 544
Windows Server Core, 105-111
Windows Update, 1065
WINS, 364-368
WSUS, 437-439
zone transfer servers, 275
Configuration Editor feature page, 397
Configuration Policy node, Group Policy, 1032-1033
Configure Your Server Wizard, 429
Confirm Installation Selections page, 335, 1121
conflicts, names, 512
connected delivery (CD), 237
Connection Broker, RDS (Remote Desktop Services), 36
Connection Manager, 852
  client dialers, 917
  CMAK, 917-919
  VPNs, 916-919
Connection Manager Administration Kit (CMAK), 852, 917-919
connection objects, creating, 198-199
Connection Security rules, 660
connections. See also mobile computing, optimizing
AD LDS instances, 232
client restrictions, 1166
DFS, 1147
DirectAccess, 872
failures, 61
ISPs, 152
limitations, 1165-1166
networks, 642
one-to-one network, 1217
RDP, 34
RDS, 925-927
RemoteApp, 940
replication, 558
SCP, 454
security, 34
SSTP, prevention, 898
types, 784
upgrading, 54
VPNs, 462, 852. See also VPNs
ports, 875-876
testing, 891-892
Connections pane, 380
Connections Strings feature page, 393
Connectix, 1516
Connector Framework, 800
connector namespace (CS), 237
consolidation
distributed data, 1147
servers, 54
consumption, power, 640-641
contacts, disaster recovery documentation, 1234
containers, AD, 636-637
content
defining, 1145
distribution, 1509-1510
screen, capturing, 1510-1511
Content Directory section, 390
content sources (SharePoint Server 2007), 1438
Control Wizard, 185
control, site delegation, 561-562
controllers. See domain controllers
conversion
6to4 IP addresses, 306
basic disks to dynamic disks, 1112
ISATAP IP addresses, 305
numbers, 299
parsing of captured data, 1404
replicated folders to read-only, 1162
video to Windows Media video formats, 1511-1512
Copy-Item cmdlet, 744
copying files, 744
cores
installation, 82-83. See also installation
parking, 8
Server Core, 14-16. See also Server Core
corruption
data, 1276
disaster recovery, 1282-1285
software, 1230
costs. See also budgets
benefits of documentation, 764-765
compatibility testing, 531
design and deployment teams, 58
disaster recovery, 765
domain models, 167
licenses, 56
links, 209
migration, 11

How can we make this index more useful? Email us at indexes@samspublishing.com
SharePoint implementations, 1435
sites, 205-206

counters
  BranchCache, 1338
  DNS, 1427
  memory, 1417
  network-based service, 1423
  performance, 1425-1426
Create and Attach Virtual Hard Disk window, 1117
Create Certificate Request, 396
Create Cluster Wizard, 1195
Create Domain Certificate Request, 410
Create Self-Signed Certificate Request, 410
creation rights, delegating GPO, 635
credentials
  caches, 22, 1306, 1309
  HCAP, 462
  Hyper-V, 1526
critical servers, 1175
CRLs (certificate revocation lists), 446
CRM (customer relationship management), 35, 52, 533
cross-forest transitive trusts, 151, 153-154, 492
cross-platform support, OpsMgr, 796
CS (connector namespace), 237
Cscript.exe, 701
CSV (Cluster Shared Volumes), 1540
  configuration, 1545-1546
  virtual machine deployment, 1546-1548
csvde.exe tool, 1252
currency, customizing, 90
Current User's Host-Specific Profile, 728
Current User's Profile, 728
Custom Views folder, 1352-1353
Customer Experience Improvement Program (CEIP), 97
Customer Experience Improvement Program Configuration screen, 1382
customer relationship management (CRM), 35, 533
customization, 90. See also configuration
  administrative templates, 606
  alerts, 798
  capture images, 1016-1020
  certificate templates for IP-HTTPS, 903-904
  configuration, 92-98
  document libraries, 1455
  events, logging, 1358-1359
  GPOs, 622-625, 1037-1039
  images, 989
  lists, 1468
  NDS clients, 250-251
  pages, 1477-1479
  permissions, 1128
  printers, 582
  resolution, 946
  topology, 1154
  views, 1353
  Windows Server Core, 105
  WSS, 1440
Customize This Server configuration category, 642

D
DACLs (discretionary access control lists), 120
daily maintenance, 685-688
data
  compression, 1099
  corruption, 1276
  disaster recovery, 1282-1285
  shadow copies, 1169-1170
Data Collector Sets, 1364-1366, 1406-1407
Data Recovery Agent (DRA), 1324
databases
backups, DHCP automation, 337-338
operations, 799
OpsMgr, sizing, 809
performance, 796
reporting, 799
services, failover clustering, 1178
WSS, 1104
Datacenter Edition, 13-14
Datasheet view, editing, 1457
Date-time property, 1141
DCDiag (Domain Controller Diagnosis), 690, 1378-1379
DCL (Digital Command Language), 701
DDNS (Dynamic DNS), 132
updating, 286
deadlines for projects, 57
Debug Logging tab, 293-294
debugging, 1343-1345
cmdlets, 704
Event Viewer, 1350-1359
Task Manager, 1345-1349
tools, 1371-1382
DEC (Digital Equipment Corporation), 701
decentralization
administration, domains, 158
replication designs, 218-220
Default Central Administration console, 1446
default configuration settings, 642
Default Document feature page, 395
defaults
domain password policy settings, 1077
local computer policy, 589
module locations, 755
RRAS servers, 479
site collection, WSS, 1452-1453
defining
addresses, DHCP 335
capacity analysis, 1391-1395
content, 1145
folders, 1159
goals, compatibility testing, 530-533
groups, Active Directory, 178-181
groups, management, 801-802
IPv6 structures, 214-215
LDAP, 121-122
names, masters, 123
OUs, 126-127, 176-178
PowerShell variables, 722
private/public key encryption, 443
scope of projects, 54-56
security, 419-420
server roles, 429
site link bridging, 204
teams, 58-59
Windows Server 2008 R2, 5-10
Definition property, 736
Delay configuration, 354
delegation
administration
DHCP, 358
GPOs, 1043-1045
IIS, 379
OUs, 184-185
control at the site level, 561-562
feature configuration, 415
GPO results, 1095
Group Policy, 634
of responsibilities, disaster recovery, 1270-1271
permissions, 185
RODC installation, 223, 374, 1315
Delegation Signer (DS) record, 317

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

BitLocker Drive Encryption, 1333
directories, 743
files, 743
groups, 182
lingering objects, 212
modules, 757
nodes from failover clusters, 1210-1211
roles, 647
demilitarized zones. See DMZs
departmental goals, 52-53
Deployed Printers node, 1030
deployment

AD DS domain controllers on Server Core, 206-207
applications, failover clusters, 1203-1205
Automated Deployment Services, 991
Automatic Updates clients, 434
BitLocker Drive Encryption, 1326
DFS, planning, 1152-1155
existing virtual machines, 1549
failover clusters, 1191-1211
geographic-based configuration groups, 808
install images, 1001-497
multiple tree domain models, 161
NAP, 460
NLB clustering, 1215-1222
NPS, 462-464
operating systems
  bare-metal systems, 988
  options, 989-991
OpsMgr, 807, 820-822
PKI, 443
printers, 1055-1058
RDS, 953-979
Remote Desktop Connection Broker, 964-967
Remote Desktop Gateway, 972-975
Remote Desktop Licensing, 977-979
Remote Desktop Web Access, 961-964
RemoteApp, 967-972
RODCs, 220-224, 372-374, 1311
security
  backups, 434
  patches, WSUS, 439
  physical, 420-424
  security-based configuration groups, 808
  through multiple layers of defense, 442
services, failover clusters, 1203-1205
software packages, 1087-1090
System Center Configuration Manager 2007 R2, 990
teams, defining, 58-59
virtual desktops, 975-977
virtual machines, 1546-1548
VPNs, 473-479
WDS, 988. See also WDS (Windows Deployment Services)
Windows Deployment Services Tools, 676
Windows Server Migration Tools, 339-340
deprovisioning accounts, 241-243. See also provisioning
depth, geographical, 61-62
design. See also configuration
  Active Directory, 147-149
  agreeing on, 66-67
  decisions, 63
  documentation, 767, 768-771
domains, overuse of OUs, 183
Group Policy
  AD, 616-617
  infrastructure, 616-619
groups, 182, 186-188
IIS, 382-383
networks, mapping, 207-208
OUs, 182
  group policies, 186-187
  models, 188-193
  starting, 182-184
phases, 63-67
replication, 216-220
  decentralized, 218-220
  hub-and-spoke, 217-218
servers, 66
sites, mapping, 207-208
structured design documents, 64-66
teams, defining, 58-59
Design phase, migration, 484
Desktop Experience feature, 946
desktops
  administration, 985-988, 1020-1021
  management, 988-989
  Microsoft Desktop Optimization Pack for Software Assurance, 612-613
  RDP, 33-34
  screens, 6
  VDI, 36
  virtual deployment, 975-977
Destination Usage box, 663
detection
  failures, 1175
  slow links, Group Policy, 602-603
  zombies, 493
determining scope of projects, 50
development
  AD DS, 115-116
  backup and recovery, 787-788
  questionnaires, 60
  UNIX integration components, 246-247
  WSUS, 435
Device Manager, 656-657
devices
  IPv6, 301
  NAT-PT, 311
  network documentation, 785
  non-Windows, OpsMgr integration, 804-805
  powering, 1174-1175
  redirection enforcement, 933
  synchronization, 27
  Windows Server Backup, 1237
DFS (Distributed File System), 3, 45, 50, 1101, 1147-1152
AD site administration, 551, 552
backups, 1166-1167, 1261
branch offices, 1340-1341
deployment, planning, 1152-1155
domain namespaces, 1149, 1153
file systems, 1101
folders, 1158-1161
Group Policy management, 615
hierarchies, backups, 1166
installation, 1155-1163
limitations of connections, 1165-1166
management, 1163-1166
Namespace Publishing page, 1127
namespaces, 1103, 1147-1149, 1155-1157
  creating roots, 1155-1157
  roots, 1152
referrals, disabling, 1164
replication, 1103, 1149-1150
  best practices, 1161-1162
  disabling, 1165
  planning, 1153-1154
  read-only, 1162
root, 1155-1157
targets, limiting connections to site, 1165-1166
terminology, 1122-1152

How can we make this index more useful? Email us at indexes@samspublishing.com
tools, 1163
troubleshooting, 1163-1166
types, 1152-1153
DFS Management console, 1152. See also DFS (Distributed File System); management
DfsCmd, 1163
DFSR (Distributed File System Replication), 31-32, 592, 1102
phased migration, 493
DfsrAdmin, 1163
DfsrDiag, 1163
DfsUtil, 1163
DHCP (Dynamic Host Configuration Protocol), 45, 258-325, 328-336, 459
access, activity logs, 350
administration, delegation, 358
authorization, 360
backups, 1260
changes in Windows Server 2008 R2, 336-344
clients
alternate network capabilities, 344
services, 330
database backup and restore automation, 337-338
disaster recovery, 1298-1299
distributed administration models, 551
dynamic DNS, 333
Group Policy, sites, 553
installation, 333-336
migration, 519-520
migrations, 39
multicast scopes, 358
name protection, 348-349
NAP
enabling, 473
integration, 349-350
need for, 328-329
NPS, 463
relay agents, 332-333
reliability, 345-350
reservations, 346-348
roles, selecting, 313
scope configuration, 348
secure updates, 279-280
security, 359-361
servers, 45
clustering, 357-358
migration, 338-341
services, 329-330
services
migration, 341-344
redundant implementation, 350-358
split scope, 351-357
superscopes, 358
testing, 336
tools, 675
WDS configuration, 997-998
DHCP Split-Scope Configuration Wizard, 354-357
DHCPv6, configuration, 313-315
diagnostics, 24
Best Practice Analyzer, 25-26
DNS, Event Viewer, 292-294
IIS, 378
Network Diagnostics Framework, 852
Server Manager, 652-657
Windows Memory Diagnostics Tool, 99, 1381
dialers, clients, 917
dialog boxes
Add Site Binding, 412
Routing and Remote Access, 479
Run As, 422
Share Properties, 1124
Web Site Bindings, 412
Windows Security Health Validator, 466
dial-up SAS servers, 476
Diffie-Hellman 2048-bit key support, 455
digital certificates, 444
Digital Command Language (DCL), 701
Digital Equipment Corporation (DEC), 701
Digital Rights Management (DRM), 451
DirectAccess, 3, 28-29, 863-872
    advantages of, 874
    components, 869-871
    configuration, 906-910
    connections, 872
    end-to-end model, 868
    end-to-end model, 868
    infrastructure configuration, 900-901
    installation, 906
IPv6, 865-866
monitoring, 914-916
selecting, 873-876
testing, 910-914
traffic separation, 869
tunnels, 867-868
directories
    AD LDS configuration, 231
    creating, 742-743
    deleting, 743
    integration, 327-328
    listing, 741-742
    management, 741-745
    Microsoft, reviewing original, 114
    moving, 744
    renaming, 744
    video for on-demand playback, 1498-1500
    WWW directory publishing, 1103
Directory Browsing feature page, 396
Directory Information Tree (DIT), 119
Directory Management Service, 1451
Directory Replication Agent (DRA), 1425
Directory Services Performance Monitor object, 1424
Directory Services Restore Mode (DSRM), 1254-1256
Directory Services Restore Mode administration password, 1316
directory services, evolution of, 114-115
Directory System Agents (DSAs), 120
disabling
    alerts, 838
    All Setting Disabled option, 573
    APIPA, 344
    caches, 1127
    DFS referrals, 1164
    functionality, starter GPOs, 628
    replication, 212, 1165
disaster recovery, 76
    access
        issues, 1277-1282
        Windows Server Backup, 1285-1287
    Active Directory Recycle Bin, 1292-1294
    compete PC restores, 1291
costs, 765
data corruption, 1282-1285
deblegation of responsibilities, 1270-1271
DHCP 1298-1299
documentation, 766, 785-788, 1234
domain controllers, 1294-1298
DVD backups, 1286
network shared folders, 1286
planning, 787, 1229-1230, 1265-1267
preparedness, 1267-1271
priorities, validation, 1272
RDS, 984
roles, services, 1291-1302
scenarios, 1274-1277
SLAs, 1231-1232
solutions, 1232-1233
System State, 1292
task assignment, 1273
troubleshooting, 1271-1274
Windows Server Backup, 1287-1291
WSS, 1299-1302
disconnections, 38. See also connections
Discover Image Metadata and Location page, 1005
discover images
adding drivers, 1008
WDS, 993, 1005-1016
discovery
computers, 820
migration, 484
phase, 59-62
Discovery Wizard, 820
discretionary access control lists (DACLs), 120
Disk Defragmenter, running, 689
disk majority clusters, creating, 1543-1544
Disk Management console, 1110
Server Manager, 664-657
Disk Manager, scanning, 1111
disk space, checking, 688
Diskpart.exe, 1110
fault tolerance, 1114-1116
disks
adding, 1110-1112
basic, 1105-1106
configuration, 1115
converting, 1112
dynamic, 1106
external subsystems, 1109
FDE, 1323
GPT, 1105
hardware-based arrays, 1109
hardware-based disk arrays, 1109
initialization, 1111
management, 1109-1118
MMC, 1110
quotas, 1134. See also quotas
rescanning, 1111
SANs, 1109
selecting, 1113
servers, fault tolerance, 1176
status, 1115
storage for host servers, 1520
subsystems, evaluating, 1421-1422
VHDs, 1106
VHDs, applying, 1116-1118
Windows Server 2008 R2, 1105-1109
Windows Server Backup management, 1236, 1286
Display Data Prioritization, 947
displays. See also viewing
filters, 1401
RDS, 945-947
distinguished name (DN), 1252
AD DS, 121
distributed administration model, 550-551
distributed administration, optimizing, 33
Distributed Cache mode, 1334-1337
distributed data consolidation, 1147
distributed environment synchronization, 227-232
Distributed File System. See DFS
Distributed File System Replication. See DFSR
distribution
content, 1509-1510
groups, 178, 179, 188, 562
OUs, 126
Distribution Group Management, 670
DIT (Directory Information Tree), 120
DLL event log audit events, 1054
DMZs (demilitarized zones), 424, 477
agent installation, 835
monitoring, 831-837
DN (distinguished name), 1252
AD DS, 121

DNS (Domain Name System), 44
AD DS, 288-290
roles, 131-133
support, 115
aging, 280-281
automation, creating zones, 287
backups, 1259
clients, 318
components, 278-285
distributed administration models, 551
DNSCMD, 296-297
Dynamic DNS, 278
Event Viewer, 292-294
evolution of, 285-286
forwarders, roles, 284-285
functionality, 278
GlobalNames zone, 291-292
Group Policy, sites, 553
hierarchies, 261-263
history, 260-261
implementation, 87
installation, 263-266
IPCONFIG, 295
IPv6, 259
migration, 39, 517-519
monitoring, 294, 1426-1428
namespaces, 131-132, 151-152, 159, 263
need for, 260-263
NSLOOKUP, 294-295
queries, 276-278
read-only, 1310
registration, 1214
root hints, 281-284
RRs, 266-270
scavenging, 280-281
security, updating, 279-280
servers, 44, 266
SRV records, 289-291
structures, 261
tools, 675
TRACERT, 295-296
troubleshooting, 292-297
Windows Server 2008 R2, 286-288
WINS
integration, 362-364
lookups, 285
zones, 132, 270-274
creating, 171
moving, 505
phased migration, 493
transfers, 264-277

DNSSEC (DNS Security), 316-323
components, 317-318
requirements, 318
zone configuration, 318-323

DNSUpdateProxy group, 361

documentation, 60, 762-763. See also WSS (Windows SharePoint Services)
AD infrastructure, 781
administration, 780-784
as built, 782-783
backups, 1234
baseline records, 789
benefits of, 764-765
change management procedures, 788
checklists, 781
communication plans, 771-772
compatibility testing, 533-534
completion, 780
design, 767, 768-771
disaster recovery, 766, 785-788, 1234, 1265-1267. See also disaster recovery
backup, 787-788
solution overview, 1232-1233
inventory, 536-537
knowledge sharing and management, 766-767
libraries, 1436, 1455
maintenance, 780-784
manuals, 783
migration, 69-73, 772-776
monitoring, 788
network infrastructure, 784-785
performance, 788-789
pilot test phase, 779
planning, 766
policies, 780-781
procedures, 784
projects, 767-780
reviewing, 767
routine reports, 789-790
security, 790-791
server build procedures, 781-782
structured design documents, 64-66
testing, 777-779
topology, 783
tracking sheets for application comparability research, 538
training, 776-777
troubleshooting, 783-784
types of, 765
updating, 694, 767
vision and plan, 63-67
WAIC, 1019
Windows system failover, 788
WSS, 1104

domain local groups, 563

Domain Name System. See DNS

Domain System Volume. See SYSVOL

Domain System Volume replication schedule, 592

domains

access-based enumeration, enabling, 1162-1163
AD DS. See AD DS (Active Directory Domain Services)
adding, 158-159
adprep utility, 496-497
controllers. See domain controllers
decentralized administration, 158
design, overuse of OUs, 183
DFS namespaces, 1148, 1149, 1153, 1155
forest administration, 565
FQDN, 820
functional levels, 503-504, 565-566
functionality, migration, 515-522
geographic limitations, 159
GPOs

creating, 1045-1046
planning, 1036-1045
restoring, 633-634
Group Policy, 1026
  creating, 628-629
  links, 617
hops, minimizing, 151
local groups, 128, 180-181
members, agents, 820
memberships, 642
models, 16, 154-155
multiple domain consolidation migration, 487
namespaces
  adding, 1157-1158
  adding additional namespace servers, 1157-1158
  enabling access-based enumeration, 1162
naming, 88, 96
Nontrusted Domain Agents, 811
PES installation, 509
power, Group Policy configuration, 1068-1069
renaming, 153, 492
RODC, 22
security, 159
services, 8
SIDs configuration, 510-511
single, administration, 564
software package deployment, 1087-1090
structures, AD DS, 149-151
trusts, 124-125, 150-151
usage, 126
Windows Server Core, adding, 107
DOSShell syntax, 701
downloading
  agents, 822
  updates, 97
  Windows Media Services source files, 1490
downtime
  planning, 1394
  replication, disabling, 1165
DRA (Data Recovery Agent), 1324
DRA (Directory Replication Agent), 1425
drivers
  images, adding, 1008
  manual driver injection, 1010
  signing, 99
drives
  BitLocker Drive Encryption, 1323-1326
    configuration, 1326-1333
    deleting, 1333
    partitions, 1327
    recovery passwords, 1332-1333
    volumes, 1331-1332
  PowerShell, 726-727
  Preferences User Drive Maps extension, 1058
DRM (Digital Rights Management), 451
DS (Delegation Signer) record, 317
DSAs (Directory System Agents), 120
DSRM (Directory Services Restore mode) passwords, 1254-1256
duration for compatibility testing, 530-531
DVDs
  access, 1075
  backups, 1245-1246, 1286
  Windows Server Backup, 1236
dynamic disks, 1106
  basic disks, converting to, 1112
Dynamic DNS. See DDNS
Dynamic Host Configuration Protocol. See DHCP
dynamic IP addresses, 88
dynamic updates, DNS, 265
Dynamic VHD performance, 1531

How can we make this index more useful? Email us at indexes@samspublishing.com
EAP (Extensible Authentication Protocol), 857

ease of administration, AD DS, 115

EC (Enforcement Client), 461

EC (Enterprise Client), 618

Edit Disk option, Virtual Network Manager, 1528

Edit Page interface, 1477-1479

editing

calendars, 1466
Datasheet view, 1457
PowerShell, 706
video, 1504

editors. See also tools

GPME, 609
GPOE, 608-609
Group Policy Starter GPO Editor, 609-610

EFI (Extensible Firmware Interface) support, 991

EFS (Encrypting File System), 27, 433, 450

BitLocker, differences between, 1324

elements

GPOs, 591
Group Policy, 591-603

e-mail

encryption, 27
WSS configuration, 1449-1452

Emergency Management Services (EMS), 1264

empty-root domain model, 165-168

EMS (Emergency Management Services), 1264

EMS (Exchange Management Shell), 18

emulators, PDCs, 123

Enable Unicast Rollover option, 1496

enabling

access-based enumeration, 1162-1163
auditing for NTFS folders, 1279
automatic updating, 96-97
BitLocker Drive Encryption, 1327-1332

BranchCache, 1124-1125
cluster shared volumes, 1202-1203
DHCP reservations, 346
feedback, 96-97
link layer filtering, 347
NAP 473
NTFS volume quotas, 1129
quotas, 1129
RDS administration, 953-955
Remote Assistance, 955
Remote Desktop, 98
shadow copies, 1263-1264
SIDHistory-filtering, 163
starter GPOs, 623-624

encapsulation, IPv6, 302

Encrypting File System. See EFS

encryption, 1099

AES, 852
BitLocker Drive Encryption, 31, 1323-1326
configuration, 1326-1333
deleting, 1333
partitions, 1327
recovery passwords, 1332-1333
tools, 676
volumes, 1331-1332

EFA, 433
e-mail, 27
FDE, 1323
files, 433
IPSec, 454-456
NTFS volumes, 1099
private/public key, defining, 443
SSL, 409-413
transport-level, 443
WEP 424
zones, records, 321

end state, 59, 65. See also scopes
end users
  satisfaction, verification, 78
  support, 989
end-to-edge model, DirectAccess, 868
end-to-end
  model, DirectAccess, 868
  service monitoring, 798
endpoint configuration, 785
enforcement
  AppLocker, 1053
  GPO links, 596-597
  NPS policy settings, 465-473
  redirection of devices, 933
  remote desktop policy settings, 1038
  storage policies, 1131
Enforcement Client (EC), 461
Enforcement Server (ES), 461
engines, PPM, 640
Enhanced Type System (ETS), 711-712
enhancements, PowerShell, 704
entering stub master servers, 274
Enterprise Admins group, 370
Enterprise Client (EC), 618
Enterprise Edition, 13
enterprise network components, 326-328
Enterprise Read-Only Domain Controller (ERODC), 1312
treatment resource planning (ERP), 531
enterprise root certification authority, 445
enterprise subordinate certification authority, 445
enumeration, access-based, 1122-1123, 1162-1163
environments, 58
  auditing, 665-674
  baselines, 1393
  distributed, synchronization, 227-232
documentation. See documentation
  EC, 618
  existing, 59-62
  ISE, 704
  SSLF, 622
  support, 78
  UNIX, 246
ERODC (Enterprise Read-Only Domain Controller), 1312
ERP (enterprise resource planning), 531
errors, 1422. See also troubleshooting
Errors feature page, 396
ES (Enforcement Server), 461
establishing site links, 558-561
estimates, budgets, 66
ETS (Enhanced Type System), 711-712
evaluation of subsystems, 1421-1422
Event Viewer
  debugging and logging, 1350-1359
  DNS, 292-294
  Group Policy, 614-615
  interfaces, 1351-1355
  management, 1355-1359
  monitoring, 686
  security, 673
  Server Manager, 649, 652-653
events
  archives, 1357
  BranchCache, 1338
  calendars, 1468
  DLL event log audit, 1054
  filtering, 687
  Get-EventLog cmdlet, 739-741
  live, broadcasting, 1506-1508
  logging, customization, 1358-1359
  rules, monitoring, 797
  subscription configuration, 1354-1355
  Wecsvc services, 653

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

BITS Server Extensions Tools, 676
Preferences User Drive Maps, 1058

extent of compatibility testing, 532

external (published) namespaces, 131, 151-152

external disks

subsystems, 1109
Windows Server Backup, 1236

external SANs, 1109. See also SANs (storage area networks)

external storage

management, 1109
support, 1109

F

failback, 1181, 1204-1206

Failed Request Tracing Rules feature page, 396

failover, 1175, 1181

clustering, 1177, 1182, 1183
backups, 1211-1215
creating, 1195-1196
deleting nodes, 1210-1211
deploying services or applications, 1203-1205
deploying virtual machines, 1546-1548
deployment, 1191-1211
geographically dispersed, 1213-1215
installation, 1541-1542
maintenance, 1208-1210
operating systems, 1190
overview of, 1184-1190
configuration, 1204-1206
split-scope configuration, 352
testing, 1206-1208

Failover Cluster Manager console, 1195, 1196
Failover Clustering
  feature installation, 1193
  tools, 676
failures. See troubleshooting
  cluster resource simulation, 1207
  connections, 61
  detection, 1175
  hard drives, 1230
fair share CPU scheduling, 929
fan-in remoting, 758
fan-out remoting, 758
farms, servers, 379
FAT (file allocation table), 1098. See also file systems
fault tolerance, 1096-1097
  Diskpart.exe, 1114-1116
  IIS, 383
  IP, 1175-1176
  servers, disks, 1176
  snapshots for guest sessions, 1538
  split-scope, 352
  system-level. See system-level fault tolerance
  volumes, 1108
    applying Disk Management snap-in, 1112-1114
    creating, 1112-1116
faults, soft and hard, 1418
Fax Server Tools, 675
FCI (File Classification Infrastructure), 1099-1101, 1130, 1140-1141
FDE (Full Disk Encryption), 1323
Feature Summary window, 648
features, 643-647
  AD CS, 445
  AD DS, 115, 153-154
  AD LDS, 229
  Add Features Wizard, 364
  adding, 97-98
  Desktop Experience, 946
  FTP configuration, 401-407
  Group Policy, 1028-1033
  OpsMgr, 796
  PowerShell, 703
  RDS, 928-947
  RODCs, 221
  RRAS, 851-852
  Server Manager, 651
  Windows Media services, 1484
  Windows Server Core, 108-110
Features View tab, 392
federated forests model, 155, 162-164
Federation Services, Active Directory expansion in, 21
feedback, enabling, 96-97
Fibre Channel, 1187
  storage arrays, 1188-1189
file allocation table (FAT), 1098. See also file systems
File Classification Infrastructure (FCI), 1099-1101, 1130, 1140-1141
File Replication Service (FRS), 1150
File Screen Properties section, 1137
File Server Resource Manager. See FSRM
File Services
  roles, 644, 1120-1121
  Tools, 675
File Signature Verification (Sigverif.exe), 1119
file systems
  access, 1102-1104
  DFS, 1101
  DFSR, 592, 1102
  EFS, 450
  fault tolerance, 1097-1102. See also fault tolerance
  FCI, 1099
  infrastructure, 1097-1102
  integrity, 694

How can we make this index more useful? Email us at indexes@samspublishing.com
management, 1096-1097
FSRM, 1130-1147
tools, 1102
MBR, 1105
monitoring, 1102
overview of, 1097-1102
partitions, 1107
quotas, 1098-1099
reliability, 1118-1120
reporting, 1102
RSS, 1101
VSS, 1100
Windows Server 2008 R2 disks, 1105-1109
WSS, 1104

File Transfer Protocol. See FTP

files
access, auditing, 431-433
ADM, 603
ADML, 603
ADMX, 603
backups, 89
cabinets, creating starter GPOs, 625
classification, 1131
creating, 742-743
deleting, 743
DFSR (Distributed File System Replication), 31-32
encryption, 433, 1099
expiration, 1101
gpt.ini, 593
install.wim image, 1000
LDIF, importing, 231
listing, 741-742
LMHOSTS, 368
management, 741-745, 1101
classification, 1140-1141
tasks, 1144-1147
media, backups, 1237
moving, 744
offline, 1123-1124
offline access, 1123
policies
screening, 1131
screens, 1131
reading information from, 744-745
recovery, 1282-1285
registry.pol, 593
renaming, 744
saving, 41
screening, 1099, 1130, 1136-1139
creating, 1135-1139
exceptions, 1139
security, 429-433
servers, 8
services, failover clustering, 1177
shares, 28, 1152
sharing, enabling BranchCache, 1125
System File Checker (Sfc.exe), 1119
transferring, 7
unattended answer, 1018-1019
video, formatting, 1475-1512
WIM, 26
Windows Media Services, combining, 1501-1503

filtering
events, 687
GPOs, 599-602
management, 631
security, 599-600
WMI, 600-601
link layers, 345-347
logs, 1356
Network Monitor, 1401
object collection, 746
per-user RemoteApp, 929
port rules, 1216-1217
printers, 582
WMI, 587

FIM (Forefront Identity Manager), 227, 233, 256
accounts, provisioning, 238, 241-243
group management, 240
identities, 240-241
installation, 240
roles, 239-240
synchronization, 236-240
finalizing installation, 92-98
financial benefits of documentation, 764-765
fine-grained password policies, 153, 493, 1077-1080
firewalls, 790
basic, 476
GPOs configuration, 901-903
Group Policy configuration, 1062-1065
OpsMgr, 812-813
profiles, 660
rules, 425-428
security, 424
Windows Firewall, 642
with Advanced Security feature, 659-660
configuration, 98
integration, 424-428
firmware, EFI, 991
flexibility, OUs, 183-184
Flexible Single Master Operations (FSMO), 374, 485, 1312, 1424
floppy disks, Hyper-V, 1529
Folder Redirection, 1123
folders. See also files
Applications and Services Logs, 1354-1355
Custom Views, 1352-1353
defining, 1159
DFS, 1158-1161
encryption, 1099
network shared, disaster recovery, 1286
NTFS
auditing, 1279
permissions, 1281
OUs, 182
recovery, 1282-1285
redirection, configuration, 1071-1075
remote shared, Windows Server Backup, 1236
shared network, Windows Server Backup, 1244-1245
shares, management, 1118-1128
staging, 1154
Subscriptions, 1354
sysvol policies, 592
SYSVOL, restoring, 1298
targets, 1152, 1159
backups, 1166
removing for maintenance, 1164-1165
tools, 650-651
Windows
Logs, 1353-1354
sharing, 1103
fonts, smoothing, 947
Forefront Identity Manager. See FIM
foreign DNS, AD DS and, 133
forests
AD DS, 118
adprep utility, 496-497
domain administration, 565
functional levels, upgrading, 503-504
models, 16
root zones, for _msdcs, 287-288
Format Volume page, 1113
formatting
answer files, 1019
AppLocker, 1052-1055
certificate templates, 831-832
connection objects, 198-199

How can we make this index more useful? Email us at indexes@samspublishing.com
directories, 742-743
files, 742-743
folders, DFS, 1158-1161
GPO domains, 1045-1046
Group Policy, 569-571
groups, 564-568
multicast images, 1019-1020
nodes, 1543-1544
partitions, volumes, 1098
port rules, 1216
RAID-5 volumes, 1114
reports, 632, 1408
Scheduled Tasks, 1069
scopes, 333-336
secure FTP sites, 400-401
user accounts, 414-415
VHDs, 1117
video conversion, 1511-1512
volumes, fault tolerance, 1112-1116
forms
   browser-based, 1438
   libraries, 1455
   management, 580
forward lookup zones, 271-272
Forwarded Events log, 1354
forwarders, DNS roles, 284-285
FQDN (fully qualified domain name), 820
frames, L2TP, 862
Free Software Foundation, 700
FreeBSD, 701
freshtastic snap-in, 754
FRS (File Replication Service), 1150
FSMO (Flexible Single Master Operations), 374, 485, 1312, 1424
FSRM (File Server Resource Manager), 24-25, 1099, 1127, 1130-1147
   configuration
      options, 1133
      quotas, 1133
file system management, 1130-1147
global options, 1133
installation, 1131-1132
shares, creating, 1127
storage
   generating reports with, 1139-1140
   reports, 1139-1140
FTP (File Transfer Protocol), 377
   file system access, 1103
   installing, 397-407
   modular-based IIS installation, 386
   servers, 378
FTPS (Secure File Transfer Protocol), 1104
Full Disk Encryption (FDE), 1323
full mesh topology, 1154
full zone transfers, 276
functional levels
   domains, 565-566
   upgrading, 503-504
functionality
   ADMT v3.1, 506-507
   BranchCache, 1124-1125
   DNS, 278
   domain migration, 515-522
   file screening, 1099
   Group Policy, 586, 1085-1087
   IPSec, 455
   keys, 455
   LOB, 1308
   mail-enabled group, 178
   OpsMgr, 797-802
   quotas, 1098
   RODCs, 1306
   Share and Storage Management console, 1118-1128
   SSLF, 622
   starter GPOs, disabling, 628
   universal groups, 181
   VPNs, enabling, 476-479
functions. See also commands
domains, renaming, 153
GPOs, separation of, 617-618
PowerShell, 708-709
future broadcasts, capturing sessions, 1509-1510

G
Gates, Bill, 420
Gateway, RDS (Remote Desktop Services), 35
gateways
   RD Gateway role service, 931
   Remote Desktop Gateway deployment, 972-975
   servers, 800
   VPNs, 476
gathering information, 87-89
GC (global catalogs), 1424
   AD DS, 122
   domain controllers, placement of, 370-374
   roles, 370
   servers, 44
Generate Resultant Set of Policy, 1094
generating
   alerts, 798-799
   FSRM storage reports, 1139-1140
   responses, 798-799
generic cluster resources, 1180
generic top-level domain names, 262
geography
   geographic limitations, domains, 159
   geographic-based configuration group deployment, 808
   geographical breadth and depth, 61-62
   geographical-based OU designs, 191-193
   geographically dispersed clusters, 1182
   geographically dispersed failover clusters, 1213-1215
Get() method, 750
Get-Alias cmdlet, 723
Get-Command, 734-736
Get-Content cmdlet, 744
Get-Help cmdlet, 733-734
Get-ItemProperty cmdlet, 745
Get-Process cmdlet, 746
Get-WmiObject cmdlet, 747, 751
Global Address List, 1393
global catalogs. See GC
global groups, 128, 181
global options, FSRM, 1133
globally unique identifier. See GUID
GlobalNames zone, 327
   DNS, 291-292
goals, 65
   business unit, 52-53
   compatibility testing, 530-533
   high-level business, 51
   migration documentation, 70
   technical, identifying, 53-59
GPMC (Group Policy Management Console), 18, 22-23, 607-608
   policies, viewing, 569
   results, 1091-1094
GPME (Group Policy Management Editor), 609
GPOE (Group Policy Object Editor), 608-609
GPOs (Group Policy Objects), 586
   Active Directory sites, 1042
   administration, 619-637
   backups, 633-634
   central stores, 594
   creating, 620-621
   verification, 621-622
   Computer Configuration node, 590

How can we make this index more useful? Email us at indexes@samspublishing.com
customization, 622-625
delegation, 1043-1045
domain controllers, 1041-1042
domains, creating, 1045-1046
elements, 591
filtering, 599-602
firewall configuration, 901-903
functions, separation of, 617-618
Group Policy Starter GPO Editor, 609-610
links, 596
configuration, 629, 1046
enforcement, 596-597
managing order of processing, 631-632
logon performance, 572-573
management, delegating rights, 635-636
models, 1091-1094
planning, 1036-1045
policies, 1037-1039
preferences, 595
processing, 586-588
RDS security, 980
replication, 591-593
reports, creating, 632
restoring, 633-634
security
filtering, 599-600, 631
policies, 790
templates, 590
Security Settings node, 1030-1032
settings, 595, 632
small businesses, 1042-1043
software package deployment, 1087-1090
starter, 594-607
backups, 625-627
creating, 622-625, 624-625
disabling functionality, 628
enabling, 623-624
policies, 623
restoring, 625-627
status, 601-602, 629-630
storage, 591-593
verification, 1036
WMI
filtering, 600-601
linking filters, 630-631
gpresult report, 1036
GPT (GUID Partition Table), 1105
gpt.ini files, 593
gpupdate.exe tool, 611
granular
auditing, 493
ccontrol, 1098
session configuration control, 940-941
graphical user interfaces (GUIs), 5, 700
graphs, Performance Monitor, 1362
Group Account Migration Wizard, 511
Group Policy, 585-586
AD management, 1076-1095
administrative templates, 594, 603-606
applications, troubleshooting, 575-577
block inheritance, 598
branch offices, 1341
clients, management, 1022-1024
Computer Configuration node, 1029-1032
computers, management, 1045-1069
configuration, 571-575
Configuration Policy node, 1032-1033
creating, 569-571
delegation, 634
DFS, management, 615
domains, 628-629, 1026
elements, 591-603
Event Viewer, 614-615
features, 1028-535
firewall configuration, 1062-1065
Folder Redirection, 1123
functionality, extending, 1085-1087
infrastructure design, 616-619
inheritance, 597
links
  domains, 617
  OUs, 617
  sites, 616-617
local, 588-590
loopback processing, 602
management, 568-569
need for, 1024
optimization, 571-575
order of processing, 598-599, 1027
power configuration, 1068-1069
PowerShell management, 612
Preferences User Drive Maps extension, 1058
processing, 586-588
RDS, 983-984, 1060-1062
remote workstation management, 1094-1095
restoring, 1298
results, 634
SCW, 1026
Sfc.exe configuration, 1120
sites, 553
slow link detection, 602-603
standalone local configuration, 1033-1036
System File Checker (Sfc.exe), 1120
tools, 607-615
  User Configuration node, 1032-1033
user management, 1070-1076
  wireless networks, 1065-1068
Group Policy Log View (GPLogView), 613
Group Policy Management Console. See GPMC
Group Policy Management Editor (GPME), 609
Group Policy Management Tools installation, 619-630
Group Policy Modeling tool, 575, 634
Group Policy Modeling Wizard, 1092
Group Policy Object Editor (GPOE), 608-609
Group Policy Starter GPO Editor, 609-610
groups
  AD, 562-564
    defining, 178-181
    scopes, 563-564
  AD DS roles, 127-129
  best practices, 186-187
  creating, 564-568
  deleting, 182
  design, 182, 186-188
  distribution, 179, 188, 562
  DNSUpdateProxy, 361
  Domain Admins, 370
  Enterprise Admins, 370
  FIM management, 240
  global, 128, 181
  local domains, 180-181
  logs, 1356
  machine local, 127, 180
  mail-enabled, 178, 180
  management, 567-568, 801-802
  membership, 178
  migration, 511-512
  multiple configuration, 808
  naming, 187
  nesting, 188
  New Replication Group Wizard, 1153
  option settings, 512
  OUs, selecting, 129
  permissions, ERODC, 1312
  policies, 186-187
  populating, 567
  RDS, 958
  replication, 1158-1161

How can we make this index more useful? Email us at indexes@samspublishing.com
restrictions, configuration, 1080-1084
scope, 180-181
security, 178, 563
structures, 174-176
types, 178-180, 562
types of, 128
universal, 128, 181
caches, 371, 492
memberships, 211-212
WSUS configuration, 437-439
guest images
rollbacks, 1539
snapshots, 1538-1539
guest operating system sessions
Hyper-V, launching, 1535-1537
installation, 1529-1533
modifying, 1533-1535
RAM, adding, 1533
snapshots, 1538-1540
GUID (globally unique identifier), 592, 612
WDS, 1014
GUID Partition Table (GPT), 1105
GUIs (graphical user interfaces), 5, 700

H
hacking, 424
Handler Mappings feature page, 396
hard disks
applying, 1116-1118
VHDs, 1106
hard drives
failures, 1230
partitions, 85
hard faults, 1418
hard limits, 1134
hardening server security, 427-430
hardware
allocation, 544
Big Bang migration compatibility verification, 488
configuration, 544
failures, 1229, 1277
hardware-based disk arrays, 1109
IHV, testing, 1118
migration, 485-486
minimum requirements, 84
NLB devices, 1175
powering, 1174-1175
procurement, 58
requirements
BitLocker Drive Encryption, 1325
OpsMgr, 805-806
verification, 689
virtualization, 1517
WSS, 1441-1442
Hardware Compatibility List (HCL), 1109, 1189
hardware-based disk arrays, 1109
hardware-level RAID, 1176
HBAs (host bus adapters), 1187
HCAP (Host Credential Authorization Protocol), 462
HCL (Hardware Compatibility List), 1109, 1189
health policies
compliance, 460
creating, 466-472
Health Registration Authority (HRA), 462
health state validation, 460
heartbeats, clustering, 1180, 1215
help, Get-Help cmdlet, 733-734
hierarchies
DFS backups, 1166
DNS, 261-263
text, 183
High Availability Wizard, 1548
high-level business goals, 51
historical records, benefits of documentation, 764
history
backups, viewing, 1247
of DNS, 260-261
of SharePoint, 1434-1436
of shells, 700-701
of Windows virtualization, 1516-1517
SID History attributes, 506
tasks, 1388
holes, security, 420
hops, minimizing, 151
host bus adapters (HBAs), 1187
Host Credential Authorization Protocol (HCAP), 462
host operating systems, Windows Server 2008 R2 installation, 1522
HOST resolution, troubleshooting, 294
host servers
configuration, 1526-1529
navigation, 1526-1529
Hosted Cache mode, 1334, 1337-1338
hosts
IPv6, adding, 315-316
RD Virtualization Host, 930
records, 267-268
Remote Desktop Session Host servers, 949-951
servers, directory of videos for playback, 1498-1500
WSH, 701
HP BTO Software, 1414
HRA (Health Registration Authority), 462
HTTP Redirect feature page, 396
hub-and-spoke topology, 1154
replication designs, 217-218
selecting, 1160
Hyper-V, 7-8. See also virtualization
Administrative console, 1524-1529
failover clustering, 1178
guest operating system sessions, 1535-1537
implementation, planning, 1519-1521
integration, 1517-1519
Live Migration, 1181, 1540-1550
new features, 1518-1519
Quick Migration, 1181, 1540-1550
roles, 1519, 1522-1524
services, 1521
settings, 1526
snapshots, 1521, 1537
tools, 676
VHD, 1118
Virtual Network Manager, 1526-1528
virtualization, 166
Windows Media Services, 1485

IANA (Internet Assigned Numbers Authority), 261-262
ICANN (Internet Corporation for Assigned Names and Numbers), 261-262
ICMP (Internet Control Message Protocol), 762
identification
of bare minimum services, 1231
of business goals, 50-53
of migration objectives, 484
of RAID-5 volumes, 1116
of security risks, 679
of services, 1228
of single points of failure, 1228
of technical goals, 53-59
of technologies, 1228

How can we make this index more useful? Email us at indexes@samspublishing.com
identities, FIM management, 240-241
Identity Lifecycle Manager (ILM), 236
Identity Management for UNIX, 254
    installing, 254
idle sessions, 932
IGMP Multicast, 1217
IHVs (independent hardware vendors), 1118
    hardware, testing, 1118
IIS (Internet Information Services), 26, 375-377
    administration, delegating, 379
    ASP.NET, 392
    authentication, 408-409
    backups, 1261
    design, 382-383
    diagnostics, 378
    fault tolerance, 383
    FTP installation, 397-407
    installation, 383-389
    logging, 415-416
    management, 378
Manager, 379
    navigating, 380
        Permissions feature page, 397
    modular-based IIS installation, 384-386
    optimization, 378-379
    planning, 382-383
    security, 407-416
    server requirements for, 382-383
    server role optimization, 40-41
    troubleshooting, 378
    upgrading, 383-389
    user accounts, creating, 414-415
    virtual directories, modifying, 391
    Web sites, 382, 389-397
    Windows PowerShell Provider, 379
    WSS, reviewing configurations, 1447
ILM (Identity Lifecycle Manager), 236
IM (instant messaging), 798
images
    boot, manual driver injection, 1010
    capture, 1016-1020
    discover, WDS, 1005-1016
    drivers, adding, 1008
    install
        deployment, 1001-1007
        troubleshooting, 1003-1005
    metadata, 999
    multicast, formatting, 1019-1020
    RIPREP, 1016
    RIS, upgrading, 1016
    RISETUP, 1016
    rollbacks, 1538
    WDS, 989
        boot, 992-993
        capture, 993
        discover, 993
        installation, 993
        types, 992
imaging systems, 990
Immediate Task preference setting, 1069
implementation
    Active Directory, 12
    DHCP redundant services, 350-358
    DNS, 87
    Exchange, 55
    hardware-level RAID, 1176
    Hyper-V, planning, 1519-1521
    migration, 78
    non-Microsoft DNS, 289
    phases, 57
    policies, 1393
    RDS, 922-925
    servers, identifying technical goals, 53-59
    time frames, 56-58
Implementation phase, migration, 485
Import-Module cmdlet, 757
importing
    DHCP server settings, 343-344
    LDIF files, 231
    management packs, 818-820
    security templates, 591
Importing LDIF Files page, 231
Improved Maintenance Pack, 796
in-band power metering, 640
inbound rules, 660
    Windows Firewall, 425
incoming email, configuration, 1449-1450
increasing service and application availability, 1177
incremental zone transfers (IXFR), 276, 1427
independent hardware vendors. See IHVs
independent software vendors (ISVs), 606
information overload management, 62
Information Rights Management (IRM), 1438
infrastructure
    Active Directory, 194-195
    AD documentation, 781
    branch offices, 1305. See also branch offices
    DirectAccess configuration, 900-901
    FCI, 1099-1101, 1130, 1140-1141
    file system, 1097-1102
    Group Policy, 585-586. See also Group Policy
        design, 616-619
    masters, 123
    network documentation, 784-785
    powering, 1174-1175
    recovery, 1273
    VDI, 36
inheritance
    Block Policy Inheritance option, 573
    Group Policy, 597, 598
Initial Configuration Tasks tool, 641-643
Initial Configuration Tasks Wizard, 95
initial master, 1153
initial replication, 1153
initialization
    disks, 1111
    IXFR, 276
    live broadcasts, 1506-1508
    new Windows disks, 1111
in-place upgrade migration, 485-486
Inspect Disk option, Virtual Network Manager, 1528
Install Now page, 90
install.wim image file, 1000
installation, 8, 43-46, 82-83
    Active Directory Domain Services, 110-111
    AD CS, 446-450
    AD FS, 233-235
    AD LDS, 229-232
    AD RMS, 452-454
    ADMT, 507-508
    applications, 958
    autouninstall of software packages, 1089
    BitLocker Drive Encryption, 1326-1327
    BranchCache, 1124-1125
    CAL, 978
    capture images, 1016-1020
    clean versions, 89-98
    clustering, failover, 1541-1542
    DFS, 1155-1163
    DHCP 333-336
    DirectAccess, 906
    DMZs, agents, 835
    DNS, 263-266
    Failover Clustering feature, 1193
    file backups, 89
    File Services roles, 1120
    FIM, 240
    finalizing, 92-98
How can we make this index more useful? Email us at indexes@samspublishing.com
FSRM, 1131-1132
FTP, 397-407
Group Policy Management Tools, 619-630
guest operating system sessions, 1529-1533
Hyper-V roles, 1522-1524
Identity Management for UNIX, 254
IIS, 383-397
images, WDS, 993
locations, selecting, 92
modular-based IIS, 378, 384-386
modules, 755-757
Network Monitor, 1400
Network Printer Installation Wizard, 579
NFS services, 248-249
NLB, 1216
NPS, 463-464
operating systems
  manual, 989
  manufacturer-assisted, 990
  unattended, 990
OpsMgr, 814-822
Password Synchronization roles, 254
PES, 509
preplanning, 83-89
Print Management console, 577-578
RD Licensing role services, 978
Remote Server Administration Tools, 676-677
RIS, 991
RODCs, 222, 1310-1323
deblegation, 374
  Server Core, 1318-1319
staged, 1319-1323
roles, 248, 642
Server Core, 1484
servers, SMTP 1450
single-server OpsMgr 2007 R2, 815-818
SUA, 253
telnet servers, UNIX, 257
types, selecting, 91-92
unattended servers, 111
updating, 97
WAIX, 1007, 1018
WDS, 994-1005
Web Server (IIS) roles, 386-388
Windows Installer, RDS compatibility, 929
Windows Media Encoder, 1505
Windows Media Services, 1489-1492
Windows Server 2008 R2 as host operating system, 1522
Windows Server Backup, 1239-1241
Windows Server Core, 103-105
Windows Server Migration Tools, 339
WINS, 364-368
WSS, 1440-1454
WSUS, 436-437
instances, 1361
  AD LDS connections, 232
  instant messaging (IM), 798
  .NET objects, 761
Integrated Scripting Environment. See ISE
integration
  components, UNIX, 245-252
directories, 327-328
DNS zones, AD, 132
Hyper-V, 1517-1519
NAP, 349-350
OpsMgr, 792-794
  AD, 804
  non-Windows devices, 804-805
PKI, Kerberos authentication, 450
single sign-on, 1438
UNIX prerequisites, 248
Windows Firewall, 424-428
WINS, DNS, 362-364
WSS, Office 2007, 1469-1475
integrity, 455
  file systems, 694
  VSS, 1100
Intelligent Timer Tick Distribution, 640
interactive remoting, 757
interfaces
  ADSI, 121
  APIs, 379
  CLI, 700, 705
  Edit Page, 1477-1479
  EFI, 991
  Event Viewer, 1351-1355
  GUIs, 5, 700
  new features, 16
  shells, 700-701
  Task Scheduler, 1384
Interix, 246. See also SUA (Subsystem for UNIX-based Applications)
internal (hidden) namespaces, 131
internal namespaces, selecting, 152
international languages, 246
Internet Assigned Numbers Authority (IANA), 261-262
Internet Control Message Protocol (ICMP), 762
Internet Corporation for Assigned Names and Numbers (ICANN), 261-262
Internet Information Services. See IIS
Internet Protocol. See IP
Internet Protocol version 4 (IPv4), 19
Internet Protocol version 6. See IPv6
Internet Security and Acceleration (ISA), 424
Internet service provider (ISP), 152, 784
Internet standards, 116
InterNIC standard namespaces, 152
interoperability, UNIX components, 247-248
intersite replication interval configuration, 200
intersite topology generator (ISTG), 204, 213, 493, 558
intervals, intersite replication configuration, 200
intranets, 1440
Intrasite Automatic Tunnel Addressing Protocol (ISATAP), 216, 303-305
Introduction to File Services page, 248
inventory
documentation, 536-537
networks, 534-535
resources, 58
servers, 535
Invoke-Command cmdlet, 759
Invoke-WMI Method cmdlet, 752
IP (Internet Protocol)
  addresses, 88
  APIPA, 330-332
  configuration, migration, 520-521
  fault tolerance, 1175-1176
  replication, 210
  virtualization, RDS, 930
IP Address and Domain Restrictions feature page, 396
IP Address Assignment page, 467
IP Security. See IPSec
IP-HTTP certificates, 905-906
IP-HTTPS, custom certificate templates for, 903-904
Ipconfig, 295, 1375-1376
IPSec (IP Security), 27, 862
  advantages of, 873
  authentication, 857
  encryption, 454-456
  functionality, 455
  L2TP, 475-476
  NPS, 462
IPv4 (Internet Protocol version 4), 19

How can we make this index more useful? Email us at indexes@samspublishing.com
IPv6 (Internet Protocol version 6), 19
  addresses, 215, 299-301
  settings, 311-313
  configuration, 311-316
DirectAccess, 865-866
DNS, 259
encapsulation, 302
hosts, adding, 315-316
importance of network addressing, 326
migration, 216
overview of, 297-311
structures, defining, 214-215
support, 213-216
transition technologies, 301-303
IRM (Information Rights Management), 1438
ISA (Internet Security and Acceleration), 424
ISAPI Filters feature page, 396
ISATAP (Intrasite Automatic Tunnel Addressing Protocol), 216, 303-305
iSCSI
  software, 1188
  storage, 1189-1190
ISE (Integrated Scripting Environment), 704
  PowerShell, 720-721
job, backgrounds, 720
JScript, 701
KCC (Knowledge Consistency Checker), 198, 204
  site links, 552
Kerberos, 198
  authentication, 133, 420
  PKI integration, 450
  support, 247
Key Signing Key (KSK), 317
keyboards
  customizing, 90
  Hyper-V, 1526
keys, functionality, 455
Kixstart, 701
Knowledge Consistency Checker. See KCC
knowledge, sharing and management, 766-767
Krbtgt accounts, 1306
KSK (Key Signing Key), 317
L
L2TP (Layer 2 Tunneling Protocol), 475, 852
  advantages of, 873
  authentication, 857
  IPSec, 475-476
labor, 58
labs
  building, 73-74
  environments, applying ADMT, 507
  lab-testing existing applications, 543-545
  results, 74-75
languages
  common language runtime, 420
  customizing, 90
international, 246
programming, SUA, 253
LANs (local area networks), 7
NTLM (NT LAN Manager), 118
wireless security, 424
latency, replication, 199-200
launching
command prompts, 105-106
DNS scavenging, 280-281
Hyper-V
  Administrative consoles, 1524-1526
guest operating system sessions,
  1535-1537
real-time live broadcasts, 1495
Layer 2 Tunneling Protocol (L2TP), 475
layers
  links, filtering, 345-347
  security, 420
LDAP (Lightweight Directory Access Protocol), 114
  defining, 121-122
  viewing, 177
LDIF files, importing, 231
Ldifde.exe tool, 1252
LDP.exe, 228
learning curves, 56
leases
  client restrictions, 472-473
  DHCP IP addresses, 351
legacy Microsoft NetBIOS resolution, need for, 362
length of prefixes, 554
levels
  AD DS, outlining, 118-119
  compatibility testing, 532
  functional
domains, 565-566
  upgrading, 503-504
item-level targeting, 1039
site delegation, 561-562
leveraging
  BitLocker, 1323
  RODCs, 1308-1310
Windows Media Services, 1489
LGPOs (Local Group Policy Objects), 1025
libraries
  documents, 1436, 1455
  forms, 1455
  pictures, 1455
  searching, 1455
  Wiki page, 1455
  WSS, 1104, 1453-1469
licenses
  accepting terms, 101
  CALs, 978, 1435
  costs, 56
  OEM, 1026
  Remote Desktop Licensing, 937-940, 977-979
  terms, accepting, 91
  See LDAP
limitations
  access, 460
caches, 373
capacity, OpsMgr, 809-810
connections, 1165-1166
data compression, 1099
DFS, 1165-1166
domain rename, 171
hard limits, 1134
RAM, 1418, 1533
RODCs, 1311-1312
soft limits, 1134
storage, 695, 1131
users, 75-78

How can we make this index more useful? Email us at indexes@samspublishing.com
line-of-business (LOB) functionality, 1308
lingering objects, 493
deleting, 212

links
AD sites, 552-553
GPOs, 587, 596
configuration, 629, 1046
enforcement, 596-597
managing order of processing, 631-632

Group Policy
domains, 617
OUs, 617
sites, 616-617
layers, filtering, 345-347
sites, 129, 209
applying, 202-204
establishing, 558-561
slow link detection, Group Policy, 602-603
speed, 785
WMI filters, GPOs, 630-631

Linux, 701
Lionbridge (Veritest), 1395
lists, 1437
calendars, 1465
directories, 741-742
Tasks, 1468-1469
WSS, 1453-1469

live broadcasts, 1506-1508
Live Migration, 1181
executing, 1549-1550
Hyper-V, 1518, 1540-1550

LMHOSTS files, 368
load, reducing, 157
loading
applications, 544-545
modules, 757

LOB (line-of-business) functionality, 1308
local administrators, 1034-1036
local area network. See LANs
local group domains, 128, 180-181
local Group Policies, 588-590
Local Group Policy Objects (LGPOs), 1025
local resource redirection, RDS, 942-945
local scopes, PowerShell, 724
local security
policies, 1025
user management, 569
local volumes, Windows Server Backup, 1236
locations
default module, 755
documentation, 766
installation, selecting, 92
NLA, 587
physical placement of RDS, 952
lockdown procedures, 790
lockout, account settings, 1077
logging, 1343-1345
Event Viewer, 1350-1359
events, customization, 1358-1359
IIS, 415-416
security, 1359
Task Manager, 1345-1349
viewing, 1357
Windows Logs folder, 1353-1354
Logging feature page, 397
logical cores, Hyper-V, 1518
Logical Unit Number (LUN), 1181
logon
access
restrictions, 421
smart cards, 423
messages, 933
performance, GPOs, 572-573
logs
activity, DHCP access, 350
DLL event log audit events, 1054
events, Get-EventLog cmdlet, 739-741
Group Policy Log View (GPLogView), 613
lookups
  Active Directory configuration, 250
  forward zones, 271-272
  NSLOOKUP, 294-295
  reverse zones, 265, 272
  WINS, 285
loopback processing, 1028
  Group Policy, 602
looping video, 1499
losses, data, 1276
LUN (Logical Unit Number), 1181

M
MA (management agent), 237, 239-240
Mac (Apple) services, 1104
MAC (Media Access Control) addresses, 1528
Machine Key feature page, 393
machine local groups, 127, 180
machine names, modifying, 106
Machine subfolder, 593
Mail Exchanger (MX) records, 269-270
mail-enabled groups, 178, 180
maintenance, 638-639. See also troubleshooting
  BitLocker, 1326
daily, 685-688
documentation, 780-784
failover clusters, 1208-1210
file system integrity, 694
Improved Maintenance Pack, 796
monthly, 694-695
NLB clusters, 1223-1225
optimization, 680
power sources, 640-641
quarterly, 695
reports, 842-845
routine, 1394
schedules, 685-695
targets, 1164-1165
weekly, 688-694
WINS, 368
malicious programs, 701
Manage NFS Sharing button, 252
managed service accounts, Active Directory, 10
management, 638-639
  access, 1122-1128
AD RMS, 451-454
agents, 800
applications, 988
benefits for administration, 22-26
caches, 1484
change management procedures
documentation, 788
CMAK, 917-919
Connection Manager, 852
CRM, 52
desktops, 988-989
Device Manager, 656-657
DFS, 1163-1166
DFSR, 31-32
directories, 741-745
Directory Management Service, 1451
disaster recovery solution overview,
  1232-1233
Disk Management console, 1110
Diskpart.exe command-line utility, 1110
disks, 1109-1118
documentation. See also WSS (Windows SharePoint Services)
DRM, 451
encryption, 1099
Event Viewer, 1355-1359
external storage, 1109
Failover Cluster Manager console, 1196

How can we make this index more useful? Email us at indexes@samspublishing.com
file systems, 1096-1097
  FSRM, 1130-1147
  quotas, 1098-1099
  tools, 1102
files, 741-745
  classification, 1140-1141
  tasks, 1144-1147
FIM identities, 240-241
folders
  shares, 1118-1128
  sharing, 1125-1128
forms, 580
FSRM, 24-25, 1130-1147
GPMC, 22-23, 607-608
  results, 1091-1094
GPME, 609
GPOs, 588, 619-637
  delegating rights, 635-636
  link order of processing, 631-632
  security filtering, 631
  status, 629-630
Group Policy, 568-569, 615-400
  AD, 1076-1095
  clients, 1022-1024
  computers, 1045-1069
  PowerShell, 612
  remote workstations, 1094-1095
  users, 1070-1076
Group Policy Management Tools installation, 619-630
groups, 567-568
  defining, 801-802
  FIM, 240
IIS, 378
information overload, 62
knowledge, 766-767
management-level reporting, 789
MMC access, 1075-1076
multiple tree domain models, 161-162
New Server Manager tool, 17-18
NLB, clustering, 1223-1225
NTLM, 118
OpsMgr, 802
  packs, 797
    importing, 818-820
    OpsMgr, 794-795
packs, third-party, 805
Performance Monitor, 1363-1364
PMOs, 1268-1269
policies, 583-585
power sources, 640-641
PowerShell, 18
  processes, 746-747
  Registry, 745-746
Print Management console, 610-611, 678-679
printing, 576-582
projects, 50
proxy, 1484
quotas, NTFS volumes, 1128-1129
RDS, 982-983
remote, 674-679
  Server Manager, 674-675
  WinRM, 653, 677-678
RMS, 41
roaming profile cache, 930
roles, 647
root management server, 799
RRAS servers, 479
Run As Administrator command, 422-423
SCCM, 1396
security, 27, 679-680
Server Manager, 647-651. See also Server Manager
servers, 800, 807, 988-989
services, PowerShell, 737-739
Share and Storage Management console, 1118-1128
site tools, WSS, 1437
System Center Configuration Manager 2007, 460, 990
Task Manager, 1345. See also Task Manager updating, 988
users, 568-569
Virtual Network Manager, 1526-1528
Windows Server Backup, 1235-1237, 1285-1287
Windows Server Core, 105-111
WMI, 587
WSRM, 925, 1408-1413
WSS site collection, 1475-1479
management agent (MA), 237, 239-240
Management Studio Express, 1448
ManagementObject class, 749
ManagementObjectSearcher class, 750
Manager, IIS, 379
navigating, 380
Managing Multiple Remote Access Servers page, 478
manual backups, wbadmin.exe, 1247-1249
manual driver injection, 1010
manual failover, 1206. See also failover
manual installation, operating systems, 989
manual settings, IPv6 addresses, 311-313
manual updates, 681
manually launching guest sessions, 1536-1537
manuals, administration documentation, 783
manufacturer-assisted installation, operating systems, 990
MAP (Microsoft Assessment and Planning), 542-543, 1396, 1413
mapping
Preferences User Drive Maps extension, 1058
site design into network design, 207-208
masks, subnets, 554
Master Boot Record (MBR), 1105
masters
infrastructure, 123
names, defining, 123
RIDs, 123
roles, moving, 500-501
schemas, 123
MBR (Master Boot Record), 1105
MBSA (Microsoft Baseline Security Analyzer), 1394
mean time between failures (MTBF), 689
mean time to repair (MTTR), 689
media
file backups, 1237
Windows Server Backup, 1235-1237
Media Access Control (MAC) addresses, 1528
members
domains, agents, 820
nondomain, monitoring, 811
memberships
domains, 642
groups, 178, 568
teams, backups, 1235
universal group caches, 211-212
memory
behavior, 1417
counters, 1417
guest sessions, adding, 1533
monitoring, 1416-1419
RAM, 1416
Resource Monitor, 1417
Windows Memory Diagnostics Tool, 99, 1381
menus
Actions, 1457
New, 1457
Settings, 1458

How can we make this index more useful? Email us at indexes@samspublishing.com
messages
logon, 933
system, 933
metadata, 1437
boot images, 1006
Discover Image Metadata and Location page, 1005
document libraries, 1455
images, 999
metadirectory, 237
metaverse namespace (MV), 237
methods
distribution, content, 1509-1510
Get(), 750
.NET Framework, 712
metric baselines, 1393-1394
Microsoft
Advanced Group Policy Management (AGPM), 612
Assessment and Planning, 542-543, 1396, 1413
Baseline Security Analyzer, 1394
Desktop Optimization Pack for Software Assurance, 612-613
directories, reviewing original, 114
Forefront Threat Management Gateway 2010, 298
Identity Integration Server (MIIS), 236
Management Console. See MMC
Metadirectory Services (MMS), 236
Office SharePoint Services 2007 (MOSS), 41
Operations Manager (MOM), 1413
Update Standalone (MUS) packages, 1490
Virtual Server, 1516
migration, 10-12, 43-46
Active Directory, 43-44
AD, 517-519
ADMT prerequisites, 508
ADMX Migrator tool, 613
adprep utility, 496-497
Big Bang, 487-491
application readiness verification, 488-489
backups, 489
hardware compatibility verification, 488
prerequisites, 487-488
recovery, 489
single domain controller servers, 489-491
virtual domain controller rollback option, 489
clustering, 1211
computer accounts, 513-515
DHCP, 519-520
servers, 338-341
services, 341-344
DNS, 517-519
documentation, 63, 69-73, 772-776
domains
collectors, 495-496
functionality, 515-522
Group Account Migration Wizard, 511
groups, 511-512
implementation, 78
in-place upgrades, 485-486
IP configuration, 520-521
IPv6, 216
Live Migration, 1181
executing, 1549-1550
Hyper-V, 1540-1550
multiple domain consolidation, 487, 505-522
objectives, identifying, 484
options, 486-487
Password Migration Wizard, 515
phases, 487, 491-505
planning, 67-73
Printer Migration Wizard, 522
printer settings, 521-522
processes, 484-487
projects
    phases, 484-485
    planning, 50
Quick Migration, 1181, 1540-1550
server roles, 515-516
Service Account Migration Wizard, 515
strategies, 486
testing, 545
time frames, 56-58
tools, 38-40
    operating systems, 39
    server roles, 39-40
user accounts, 512-513
WDS, 1015-1016
Window Server 2003, 481-483
Windows 2003, 11-12
Windows Server Migration Tools, 338-341, 516-517
WINS, 368
MIIS (Microsoft Identity Integration Server), 236
milestones, 57
    migration documentation, 71
MIME Types feature page, 397
minimizing hops, domains, 151
minimum hardware requirements, 84
minor updates, 540
mirrored volumes, 1108
mitigation, security, 374
mixed administration model, 551
MMC (Microsoft Management Console)
    access management, 1075-1076
    AD FS, viewing, 233
disk management, 1110
    Disk Management console, 1110
Event Viewer interfaces, 1351
Network Policy tool, 466
RDS, 925
Run As dialog box, 422
Windows Server Backup, 1238
MMS (Microsoft Metadirectory Services), 236
MOBILE, 852
Mobile Broadband (Windows 7), 29-30
mobile computing, optimizing, 28-30
models
    administration, 550-551
    centralized, 550
    distributed, 550-551
    mixed, 551
    COM, 702
domains, 16, 154-155
failover cluster configuration, 1184-1190
    GPOs, 1091-1094
Group Policy Modeling tool, 575, 634
Group Policy Modeling Wizard, 1092
No Majority: Disk Only Quorum, 1185-1186
Node and Disk Majority Quorum, 1185
Node and File Share Majority Quorum, 1185
Node Majority Quorum, 1184-1185
OU design, 188-193
    quorum disk, 37
modes
    RDS, 925-927
    remoting, 757
modification
    Active Directory, changes in, 20-22
    alerts, 838
group membership, 568
guest operating system sessions, 1533-1535
    IIS virtual directories, 391
    machine names, 106
    parsing, 1404
How can we make this index more useful? Email us at indexes@samspublishing.com
passwords, 106, 695
quotas, 1134-1135
RDP ports, 981
RRAS network policies, 479
schedules, 199
schemas, 120
services, 739
modular-based IIS installation, 378, 384-386
modules
deleting, 757
installation, 755-757
PowerShell, 715-716, 755-757
Modules feature page, 397
MOM (Microsoft Operations Manager), 1413
monitoring
AD
  clients, 823-824
  replication, 824-826
AD DS, 1424-1426
agent roles, 801
agentless exception, 800
applications, 1347
bottlenecks, 1415-1416
DirectAccess, 914-916
DMZs, 831-837
DNS, 294, 1426-1428
documentation, 788
directories, 744
dns zones, 505
files, 744
files, 1102
memory, 1416-1419
Network Monitor, 1398-1404
network subsystems, 1422-1423
Nontrusted Domain Agents, 811
objects, 1370-1371
OpsMgr, 794-795, 802
pagefile usage, 1416-1419
performance, 1348, 1359-1360, 1415-1423
networks, 1348-1349
OpsMgr, 804
reducing overhead, 1369-1370
rules, 797
Performance Monitor, 653-656, 1360-1372
processes, 1347
RDS, 945-947
reliability, 1359-1360
Reliability Monitor, 1368
roles, 647
services, 796, 1347
states, 798
Task Manager, 1345. See also Task Manager
tools, 24
URLs, scaling, 796
user activity, 1349
monitors, spanning, 946
monthly maintenance, 694-695
morale of teams, maintaining, 1273
MOSS (Microsoft Office SharePoint Services 2007), 41
mount points, 1107
  volumes, 1107
mounting physical CD/DVD images, 1534-1535
mouse, Hyper-V, 1526
Move-Item cmdlet, 744
moving
directories, 744
DNS zones, 505
files, 744
roles, OM, 500-501
_msdc, forest root zones for, 287-288
MTBF (mean time between failures), 689
MTTR (mean time to repair), 689
multicasting, 1217, 1493
  images, formatting, 1019-1020
  scopes, DHCP 358
  Silverlight, 1485
  WS-Discovery, 1336
Multichoice property, 1141
Multiconfiguration Service HealthValidators, 461
multimaster replication, AD DS, 122
multimaster topology concepts, 196
multimonitor support
  RDP 34
multipage meeting workspaces, 1467
Multipath I/O (MPIO), 1189, 1190
multiple configuration groups, 808
multiple domains
  consolidation migration, 487, 505-522
  models, 147, 155-160
multiple files, Windows Media Services, 1501-1503
multiple group membership, 178
multiple local group policies, 589
multiple tree
  AD DS, 160-162
  single forest models, 155
multisite clusters, 1182
Multistring property, 1141
multivalued attribute replication, 493
MUS (Microsoft Update Standalone) packages, 1490
MV (metaverse namespace), 237
MX (Mail Exchanger) records, 269-270
My Sites (SharePoint Server 2007), 1438

N
Name Resolution Policy, 1029
Name Resolution Policy Table (NRPT), 321

Name Server (NS) records, 268
names
  Active Directory, 20-21
  capture images, 1017
  computers, 87, 96, 642
  conflicts, 512
  DHCP protection, 348-349
distinguished (DN), AD DS, 121
DN, 1252
domains, 88, 96
FQDN, 820
generic top-level domain, 262
GlobalNames zone, 291-292, 327
groups, 187
machine names, modifying, 106
masters, defining, 123
networks, 1196
playlists, 1502
publishing points, 1498
relative distinguished, outlining, 121
resolution, 322, 327
site links, 203
trees, 167
UNC, 88, 379, 1103
WINS, 361. See also WINS (Windows Internet Naming Service)
workgroups, 88
namespaces
  access-based enumeration, enabling, 1162-1163
  AD DS, selecting, 151-152
  adding, 1157-1158
  DFS, 1101, 1103, 1147-1149, 1155-1157
    creating roots, 1155-1157
    domains, 1149, 1153
    roots, 1152
  DNS, 131-132, 159, 263

How can we make this index more useful? Email us at indexes@samspublishing.com
domains, enabling access-based enumeration, 1162
servers, adding, 1157-1158
standalone DFS, 1153
NAP (Network Access Protection), 2, 27, 459-461
changes in Windows Server 2008 R2, 461
components, outlining, 460
deployment, 460
DHCP integration, 349-350
enabling, 473
terminology, 461
NAT (Network Address Translation), 455
between networks, 476
NAT-PT devices, 311
native commands, PowerShell, 710
navigation
CLI, 706-707
document libraries, 1456-1464
Event Viewer, 1351-1355
host servers, 1526-1529
Manager, IIS, 380
NPS, 462-463
PowerShell, 732-736
NDS (Novell Directory Services), 114
need
for AD LDS, 228
for AD RMS, 451
for compatibility testing, 526-527
for DHCP, 328-329
for DNS, 260-263
for Group Policy, 1024
for legacy Microsoft NetBIOS resolution, 362
for OUs (organizational units), 177
for RODCs, 221
for SharePoint 2007 products, 1435-1436
for transport-level security, 442
for WSS, 1439-1440
nesting groups, 188
.NET
Application Settings feature page, 393
Authorization Rules feature page, 392
Compilation feature page, 392
Error Pages feature page, 392
Globalization feature page, 392
objects, instances, 761
Profile feature page, 392
Roles feature page, 393
Server Core, 379
Trust Levels feature page, 393
Users feature page, 393
.NET Framework, 702
methods, 712
PowerShell, 711-714
NetBIOS, 170
client resolution, 368
need for legacy Microsoft resolution, 362
Netgroup support, 247
NetMon, 1338
netsh branchcache show status command, 1338
Netsh command-line utility, 358-359
Netstat, 1377
Network Access Protection. See NAP
Network Address Translation. See NAT
Network Device Enrollment Service, 446
Network Diagnostics Framework, 852
network file system. See NTFS (NT File System)
Network Information Service. See NIS
network interface cards (NICs), 454, 1416
Network Level Authentication, RDS, 981
Network Load Balancing. See NLB
Network Location Awareness. See NLA
Network Location Service (NLS), 871
Network Monitor Parser Language (NPL), 1404
Network Monitor, capacity analysis, 1398-1404
Virtual Network Manager, 1526-1528
VPNs, 850-856. See also VPNs (virtual private networks)
wireless
   Group Policy, 1065-1068
   security, 424
New Configuration Wizard, 1529
new features, 6, 16-19
   Hyper-V, 1518-1519
New Folder window, 1159
new installations. See also installation selecting, 85-86
New-Item cmdlet, 743
New menu, 1457
New-Object cmdlet, 757-762
New-PSSession cmdlet, 760
New Replication Group Wizard, 1153
New Scope Wizard, 333
New Server Manager tool, 17-18
Next Generation TCP/IP stacks, 1339-1340
Next Secure (NSEC) record, 317
NFS (Network File Service)
   administration, 249-250
   clients, customizing, 250-251
   file systems, 1104
   services, 248-249, 1104
   shared network resource configuration, 252
NFTS (Network File System), self-healing NFTS, 6-7
NICs (network interface cards), 454, 1416
   specifying, 478
NIS (Network Information Service), 247
   users, adding, 255-256
NLA (Network Location Awareness), 587
   Group Policy, 602-603
NLB (Network Load Balancing), 379, 1171
   applications, 1215
   backups, nodes, 1223

network operating system. See NOS
Network Policy and Access Services Tools, 676
Network Policy MMC tool, 466
Network Policy Server, 45
Network Printer Installation Wizard, 579
networks
   6to4 tunneling protocol, 305-308
   access, troubleshooting, 1278
   adapters, 1176
   addresses, 326
   alternate capabilities, DHCP clients, 344
   card configuration, 1218
   clustering, 1196-1199
   configuration, 95-96
   connections, 642
   design, mapping, 207-208
   disaster recovery documentation, 1234
   enterprise components, 326-328
   infrastructure documentation, 784-785
   inventory, 534-535
   IP, 1175. See also IP (Internet Protocol)
   location awareness services, 23
   naming, 1196
   outage, 1229, 1274
   performance, monitoring, 1348-1349
   policies, RRAS modification, 479
   protocols, 88
   RDS requirements, 952
   resources, sharing, 252
   services, changes in Windows Server 2008 R2, 328
   settings, modifying for guest sessions, 1533-1534
   shared folders
      disaster recovery, 1286
      Windows Server Backup, 1244-1245
   stability, 60
   subsystems, monitoring, 1422-1423

How can we make this index more useful? Email us at indexes@samspublishing.com
clustering, 1178, 1184
  creating, 1218-1221
  deployment, 1215-1222
  maintenance, 1223-1225
  management, 1223-1225
IIS fault tolerance, 383
installation, 1216
network card configuration, 1218
  nodes, adding, 1221-1222
  services, 1215
tools, 676
NLS (Network Location Service), 871
No Majority: Disk Only Quorum model, 1185-1186
  no topologies, 1154
Node and Disk Majority Quorum model, 1185
Node and File Share Majority Quorum model, 1185
Node Majority Quorum model, 1184-1185
nodes, 1179
  active, 1179
  clustering, adding, 1199-1200
  Configuration, Server Manager, 657-661
    creating, 1543-1544
  failover clusters, deleting, 1210-1211
  GPO Computer Configuration, 590
  NLB
    adding, 1221-1222
    backups, 1223
  passive, 1179
  SANs, 38
nonadministrators
  local user policies, 589
  policies, 1025, 1034-536
non-compliant clients, creating health policies, 467
non-Microsoft DNS implementations, 289
non-Windows devices, OpsMgr integration, 804-805
Nontrusted Domain Agents, monitoring, 811
NOS (network operating system), 52, 326
  upgrading, 54
notifications
  configuration, 1146
  OpsMgr, 796, 828-831, 838
  thresholds, 1135
Novell Directory Services (NDS), 114
NPL (Network Monitor Parser Language), 1404
NPS (Network Policy Server), 2, 360, 459, 852
  xxxx802.1x authentication 462
  changes in Windows Server 2008 R2, 461
  configuration, 880-886
  deployment, 462-464
  DHCP, 463, 472-473
  installation, 463-464
  IPSec, 462
  navigation, 462-463
  policy settings enforcement, 465-473
  RADIUS, 463
  VPNs, 854-856
NRPT (Name Resolution Policy Table), 321
NS (Name Server) records, 268
NSEC (Next Secure) record, 317
Nslookup, 294-295, 1378
NSM, 1414
NT File System (NTFS). See NTFS
NT LAN Manager (NTLM), 118
Ntbackup.exe, 1236
ntdsutil, 123, 1295
NTFS (NT File System), 1098. See also file systems
  folders
    auditing, 1279
    permissions, 1281
  partitions, 1098
permissions
  configuration, 1152
  troubleshooting, 1278
security, 430-431
volumes
  data compression, 1099
  encryption, 1099
  quota management, 1128-1129
  quotas, 1098-1099
NTLM (NT LAN Manager), 118
Number property, 1141
numbers
  conversion, 299
  OM roles 122-124
  version properties, 197-198

O
object identifier (OID), 857
Object REXX, 701
objectives, migration, 65. See also goals
  documentation, 70
  identifying, 484
objects, 1361
  COM, 702
  connections, creating, 198-199
  Directory Services Performance Monitor, 1424
  GPOE, 608-609
  GPOs, 586
  lingering, 212, 493
  monitoring, 1370-1371
  .NET instances, 761
  schemas, 120
  WshShell, 745
OEM (original equipment manufacturer), 990
off-the-shelf software applications, 60
Office 2007, WSS integration, 1469-1475
Office Domain Join, Active Directory, 10
offline files, 1123-1124
  access, 1123
OID (object identifier), 857
OM (Operations Master), 122-124, 500-501
on-demand video playback
  configuration, 1496-1497
  directories, 1498-1500
one-to-one network connections, 1217
ongoing preparedness, disaster recovery, 1267-1271
ooBE.exe command, 643
Open Server Manager, 248
Open System Interconnection (OSI), 475
operating systems
  administrative templates for, 604-606
  bare-metal systems deployment, 988
  failover clusters, 1190
  Group Policy, 1025-1028
  guest sessions
    installation, 1529-1533
    launching Hyper-V, 1535-1537
    modifying, 1533-1535
    snapshots, 1538-1540
  installation
    manual, 989
    manufacturer-assisted, 990
    unattended, 990
  migration tools, 39
  NOS, 52, 326. See also operating systems
  options, deployment, 989-991
  selecting, 91
operational data, processing, 798
Operations Console, 800
operations database, 799
Operations Master (OM), 122-124, 500-501

OpsMgr (System Center Operations Manager) 2007

- AD integration, 804
- agent deployment, 820-822
- alerts, tuning, 837-845
- applying, 802-805
- architecture, 796-802
- backups, 807
- capacity, limitations, 809-810
- component requirements, 805-807
- configuration, 822-831
- databases, sizing, 809
- deployment, 807
- DMZs, monitoring, 831-837
- features, 796
- firewalls, 812-813
- functionality, 797-798
- installation, 814-822
- integration, 792-794
- management, 802
- monitoring, 794-795, 802
- non-Windows device integration, 804-805
- notifications, 828-831
- performance, 804
- redundancy, 810-811
- reports, 798, 803, 839-845
- security, 811-814
- stores, capturing data, 800-801
- subscriptions, 828-831
- third-party management packs, 805

optimization

- administration, 256-257
- branch office replication, 1339-1342
- clustering, 37-38
- distributed administration, 33
- Group Policy, 571-575
- IIS, 378-379

maintenance, 680
mobile computing, 28-30
performance, 1389-1391
benefits of, 1392-1393
by server roles, 1423-1429
Performance monitor, Server Manager, 653-656
RDS, 33-36
Remote Desktop Session Host servers, 949-951
replication, 210
SANs, 37-38
security subsystems, 26-27
server roles, 40-42
uptime, 1271

options. See also customization

- All Settings Disabled option, 573
- backups, 1228-1232, 1237-1238
- binding, verification, 334
- Block Policy Inheritance, 573
- Enable Unicast Rollover, 1496
- global, FSRM, 1133
- group settings, 512
- operating system deployment, 989-991
- power, Group Policy configuration, 1068-1069
- RODCs, 1315
- startup, 1264-1265
- triggers, 1384-1385
- upgrades, 102
- Windows Media Encoder, 1510-1512

order of processing, Group Policy, 598-599

Ordered List property, 1141

organizational benefits of documentation, 764
organizational unit. See OUs
original equipment manufacturer (OEM), 990

Originating Writes, 130

OSI (Open System Interconnection), 475
OUs (organizational units), 62, 167, 174-176
  AD DS, defining, 176-178
  administration, delegating, 184-185
  defining, 126-127
  design, 182
    group policies, 186-187
    models, 188-193
  starting, 182-184
  Group Policy links, 617
  groups, selecting, 129
  usage, 126
Out-Default cmdlet, 715
Out-Of-Box Experience, 643
out-of-the-box
  policy settings, 589
  workflows, WSS, 1438
outages
  networks, 1229, 1274
  power, 1229
outbound rules, 660
  Windows Firewall, 425
outcome, Group Policy Modeling, 634
outgoing email, configuration, 1451-1452
outlining
  AD DS
    components, 119-124
    levels, 118-119
  AD LDS features, 229
  NAP components, 460
  OpsMgr architecture, 798-802
  relative distinguished names, 121
  service account security, 814
Outlook 2007, WSS, 1458
Output Caching feature page, 397
outsourcing BitLocker, 1326
overhead, reducing, 1369-1370
Overrides view, 796
Overview of Performance Monitor screen, 1360

P

packages
  MUS, 1490
    software, deployment, 1087-1090
packet errors, 1422
packs
  Improved Maintenance Pack, 796
    management, 797
    importing, 818-820
    OpsMgr, 794-795
    third-party, OpsMgr, 805
    service, 681-685
Page Faults/sec counter, 1418
pagefile usage, monitoring, 1416-1419
Pages and Controls feature page, 393
pages, customization, 1477-1479
Pages/sec counter, 1418
panes, IIS, 380-381
parameters
  Alert Priority, 838
  Alert Severity, 828
  argumentList, 753
  AsJob, 760
  computername, 752
  Invoke-Command cmdlet, 760
  ThrottleLimit, 760
  Win32_WMISetting, 752
parity stripes, 1108
parking cores, 8
parsers, Network Monitor, 1404
parsing LMHOSTS files, 368
partitions, 1107
  AD LDS configuration, 231
  applications, 286-287
  BitLocker Drive Encryption, 1327
  GPT, 1105
  hard drives, 85

How can we make this index more useful? Email us at indexes@samspublishing.com
NTFS, 1098
volumes, 1098

partners, WINS replication, 365

passive nodes, 1179

Password Export Server (PES) service, 508
installation, 509

Password Migration Wizard, 515

passwords
administration
configuration, 94
Directory Services Restore Mode, 1316
BitLocker Drive Encryption, 1332-1333
change functionality configuration, 255
DSRM, 1254-1256
fine-grained password policies, 153
fine-grained policies, 1077-1080
key information, exporting, 508-509
modifying, 106, 695
policies, 493, 791
recovery, 1331
replication, 223
synchronization, 254
UNIX, 246

patches
applying, 644
security, WSUS, 439

Pathping, 1375

PDCs (Primary Domain Controllers), 123, 198, 1306

PEAP (Protected EAP), 852, 857
peer-root domain models, 155, 165
per-packet authenticity, 455
per-user RemoteApp filtering, 929

PerfMon, 788

performance
backups, VSS, 1100
BranchCache, 1338
counters, 1425-1426
databases, 796
DirectAccess, monitoring, 914-916
documentation, 788-789
Dynamic VHD, 1531
Group Policy, 586
Hyper-V, 7-8
logon, GPOs, 572-573
monitoring, 1348, 1359-1360, 1415-1423
reducing overhead, 1369-1370
networks, 60, 1348-1349
OpsMgr, 804
optimization, 1389-1391
benefits of, 1392-1393
by server roles, 1423-1429
Remote Desktop Services Server, 1427
reports, 795, 839-842
RODCs, 1316
rules, monitoring, 797
synchronization, 1341
tools, 24
virtual servers, 1429

Performance Monitor, 1360-1372
capacity analysis, 1405-1408
Data Collector Sets, 1364-1366
DNS, 294
management, 1363-1364
reports, 1366-1367
Server Manager, 653-656

Performance Options window, accessing, 1418

Performance Resource and Optimization (PRO) Tips, 796

Perl, 701

permissions, 182
access, 471, 479
configuration, 32, 1128
delegating, 185
groups
   ERODC, 1312
   modification, 568
IIS, assigning to user accounts, 414-415
NTFS
   configuration, 1152
   folders, 1281
   troubleshooting, 1278
Registry settings, 509-510
shares, validation, 1279
sharing, 1128
SMB, 1127
PES (Password Export Server) service, 508
   installation, 509
phantom domain controllers, retiring, 502-503
phases
   design, 63-67
   discovery, 59-62
   documentation, 779
   implementation, 57. See also implementation
   migration, 487, 491-505
   pilot, 75-78
   planning, 67-73
   project migration, 484-485
   Prototype, compatibility testing, 546-547
   prototypes, 73-75
physical access restrictions, 421
physical CD/DVD images, mounting, 1534-1535
physical disasters, 1229. See also disaster recovery
physical host memory, Hyper-V, 1518
physical locations, centralized administration models, 550
physical placement of RDS, 952
physical security
   branch offices, 1303
   deployment, 420-424
physical site failures, 1274
physical-to-virtual image creation, 1519
pictures, libraries, 1455
PID (process identifier), 1347
Pilot phase, migration, 485
pilot phases, 75-78, 779
Ping, 762, 1372-1374
pipelines, PowerShell, 715
PKI (Public Key Infrastructure), 27, 443
   Kerberos authentication integration, 450
   smart cards, using in, 450
placeholder domain model, 155, 167-169
placement of global catalog domain controllers, 370-374
planning, 50
   compatibility testing, 542
   configuration, 54
   DFS
      deployment, 1152-1155
      replication, 1153-1154
   disaster recovery, 787, 1229-1230, 1265-1267. See also disaster recovery
   documentation, 63-67, 766
downtime, 1394
GPOs, 599, 1036-1045
Hyper-V implementation, 1519-1521
IIS, 382-383
installation, 83-89
MAP, 1396
migration phases, 67-73
projects, 768
RDS, 947-953
recovery, 1228
Remote Desktop Session Host servers tolerance, 953
SCCP, 1413
testing, 73-75
tools, 1408-1414

How can we make this index more useful? Email us at indexes@samspublishing.com
validation, 75-78
WINS, 368
playback, video on demand, 1496-1497, 1498-1500
playlists
server configuration, 1501-1503
starting, 1503
wrappers, 1494
pluggable authentication and authorization feature, 933
PMOs (Project Management Offices), 1268-1269
Point-to-Point Protocol (PPP), 475
Point-to-Point Tunneling Protocol (PPTP), 475
Pointer (PTR) records, 270
points
Add Publishing Point Wizard, 1498
mount, 1107
publishing, starting, 1495
policies
administrators, 1025
AppLocker, 1052-1055
auditing, 665-670, 1438
baselines, 1393-1394
Block Policy Inheritance option, 573
default local computer, 589
documentation, 780-781
execution, 732
files
screening, 1131
screens, 1131
fine-grained password, 153, 1077-1080
GPMC, viewing, 569
GPOs, 1037-1039
Group Policy, 585-586. See also Group Policy
groups, 186-187
health, 460, 466-472
implementation, 1393
management, 583-585
name resolution, 322
Name Resolution Policy, 1029
Network Policy Server, 45
networks, RRAS modification, 479
nonadministrator, 1034-1036
NRPT, 321
passwords, 493, 791
Preferences User Drive Maps extension, 1058
processing, 1027-1028
security, 27, 1025
settings, NPS enforcement, 465-473
software restrictions, 1049-1051
starter GPOs, 623
storage, 1131
trust, AD FS, 235
Policy-base QoS node, 1030
pools, applications, 381, 390
populating groups, 567
Portal Site Connection, 1477
portals, creation of, 1440
porting scripts, 247
ports
communication, 813
RDP modification, 981
rules
filtering, 1216-1217
formatting, 1216
VPN connections, 875-876
postmortem meetings, disaster recovery, 1273
power
Group Policy configuration, 1068-1069
outages, 1229
UPS, testing, 694
Power Management AQ, 641
power sources, 640-641, 1174-1175
PowerShell, 18-19, 678
access, 705
ADOs, exporting, 1253
advanced functions, 709-710
aliases, 722-723
applying, 703
CLI, 705
cmdlets, Windows Server Backup, 1238
commands, 707-711
drives, 726-727
editing, 706
enhancements, 704
features, 703
functions, 708-709
Get-Command, 734-736
Get-EventLog cmdlet, 739-741
Group Policy management, 612, 620
ISE, 720-721
manual backups, 1247-1249
modules, 715-716, 755-757
native commands, 710
navigation, 732-762
.NET Framework, 711-714
New-Object cmdlet, 757-762
overview of, 702-704
pipelines, 715
process management, 746-747
profiles, 728-729
providers, 726-727
RDS management, 983
Registry management, 745-746
remoting, 398-720, 757-761
scopes, 724-726
scripts, 710-711
security, 729-732
service management, 737-739
shells, 700-701. See also shells
snap-ins, 715-716, 754-755
variables, 722
windows, 342
WMI, 747-754
PPM (Processor Power Management) engines, 640
PPP (Point-to-Point Protocol), 475, 852
PPTP (Point-to-Point Tunneling Protocol), 475, 871
advantages of, 873
authentication, 857
preformatting AD computer accounts, 1013
Preboot Execution Environment (PXE), 26
precedence, Group Policy, 597
preferences, 90
actions, 1039
GPOs, 595, 1037-1039
Immediate Task setting, 1069
item-level targeting configuration, 1058-1060
Preferences User Drive Maps extension, 1058
preferred bridgehead servers, 206
prefixes, length, 554
preparation
for compatibility testing, 527-534
live broadcasts, 1506
server installations, 83-89
preparedness, backups, 1267-1271
preplanning installation, 83-89
prerequisites, 59. See also requirements
AD RMS, 451-452
ADMT migration, 508
Big Bang migration, 487-488
domain rename, 171
RODC deployment, 1311
UNIX integration, 248
WSUS, 435
prevention, SSTP connections, 898
How can we make this index more useful? Email us at indexes@samspublishing.com
previous state, restoring clusters to, 1212
Primary Domain Controllers (PDCs), 123, 198, 1306
primary zones, 272
Print Management console, 576, 610-611, 678-679. See also printing
  applying, 580-582
  configuration, 578
  installation, 577-578
Print Services Tools, 676
Printer Migration Wizard, 522
printers
  adding, 578-580
  deployment, 1055-1058
  filtering, 582
  settings, migration, 521-522
printing
  auditing, 674
  management, 576-582
  Network Printer Installation Wizard, 579
  servers, 8
  services, failover clustering, 1177
prioritization
  applications, 537
  disaster recovery, 1272
  recovery, 1230
privacy, 455
private scopes, 725
private/public key encryption, defining, 443
privileges, Run As Administrator command, 422-423
PRO (Performance Resource and Optimization) Tips, 796
procedures
  backups, 1235
  change management documentation, 788
  documentation, 784
process identifier (PID), 1347
processes
  group migration, 512
  migration, 71, 484-487
  monitoring, 1347
  PowerShell management, 746-747
  termination, 753
processing
  Group Policy, 586-588
    loopback, 602
    order of, 598-599
  loopback, 1028
  operational data, 798
  outcome, Group Policy Modeling, 634
  policies, 1027-1028
Processor Power Management (PPM) engines, 640
processors
  host servers, 1520
  Hyper-V, 1518
  usage analysis, 1419-1420
procurement
  hardware, 58
  software, 58
products, researching, 534-537
profiles
  firewalls, 660
  PowerShell, 728-729
ProgID (programmatic identifier), 762
programming languages, SUA, 253
Programs and Features tool, reviewing, 1448
Project Management Offices (PMOs), 1268-1269
projects
  deadlines for, 57
  defining scope of, 54-56
  determining scope of, 50
  documentation, 767-780
  migration phases, 484-485
  planning, 768
Proof-of-Concept phase, migration, 485
properties
  AuthenticationLevel, 751
classification, 1141-1142
Definition, 736
File Screen Properties section, 1137
FTP configuration, 401-407
site link creation, 203
SSL configuration, 413
version numbers, 197-198
WDS, 1013
Web site configuration, 392-397
Protected EAP (PEAP), 852, 857
protection
  accidental deletion, 1254-1255
names, DHCP, 348-349
NAP, 349-350, 459-461
protocols
  6to4 tunneling, 305-308
BOOTP, 329
DHCP, 328-336
  backups, 1260
  migrations, 39
  servers, 45
FTP, 377
  configuration, 397-407
  file system access, 1103
HCAP, 462
ICMP, 762
IP addresses, 88
IPSec, 862
ISATAP, 216, 303-305
L2TP, 475, 852
LDAP, 114, 121-122
networks, 88
PPP, 475, 852
PPTP, 475, 871
RARP, 329
RDC, 1150
RDP, 33-34
SMTP, 179
SNMP, 798
SOAP, 718
SSTP, 852, 863
TCP/IP, 326
Teredo tunneling, 308-311
tunnels, 475
VPNs, 858-863
WEP, 424
Prototype phase
  compatibility testing, 546-547
  migration, 484
prototypes, 73-75
Provide Computer Information configuration
category, 642
Providers feature page, 393
providers, PowerShell, 726-727
Provision a Shared Folder Wizard, 1126
provisioning
  accounts, 238, 241-243
domain controllers, 224
proxies
  agent configuration, 822-823
  configurations, 790
  management, 1484
Web, 424
PSSnapins, 716
PTR (Pointer) records, 270
Public Key Infrastructure. See PKI
publishing
  Add Publishing Point Wizard, 1498
  broadcasts, 1504-1496
  namespaces, selecting 151-152
  on-demand, 1504-1496
  points, starting, 1495
  WWW directory, 1103

How can we make this index more useful? Email us at indexes@samspublishing.com
push/pull partner configuration, 365
PXE (Preboot Execution Environment), 26
Python, 701

Q
QoS (Quality of Service), 1422
qualification, disasters, 1271
Quality of Service (QoS), 1422
Quarantine Policy Check, 852
queries
DNS, 276-278
iterative, executing, 278
recursive, executing, 276-277
questionnaires, 60
Quick Migration, 1181
Hyper-V, 1540-1550
quorums
clustering, 1180, 1201-1202
disk models, 37
witness disks, 1541
Quota Policy, 1127
quotas
enabling, 1129
file systems, 1098-1099
file types, configuration, 24
FSRM configuration, 1133
modification, 1134
modifying, 1134-1135
NTFS volumes, 1128-1129
standard sizes, 1130
templates, 1134-1136

RAID (redundant array of inexpensive disks), 1176
fault-tolerance disk arrays, 1112
RAID-5 volumes, 1108-1109, 1113
raising domain functional levels, 504
RAM (random access memory), 1416
for host servers, 1520
guest operating system sessions, adding, 1533
limitations, 1418
random access memory. See RAM
RARP (Reverse Address Resolution Protocol), 329
rates, bit, 1507
RD Gateway (Remote Desktop Gateway) role service, 931
RD Session Host (Remote Desktop Session Host), 928-930
RD Virtualization Host (Remote Desktop Virtualization Host), 930
RDC (Remote Differential Compression), 1102, 1150
RDP (Remote Desktop Protocol), 33-34
port modification, 981
RDS (Remote Desktop Services), 919-922
administration, 923, 953-955
antivirus, 948
application compatibility, 948-949
ASP, 924-925
clients, 927
Connection Broker, 36
connections, 925-927
deployment, 953-979
disaster recovery, 984
features, 928-947
Gateway, 35
Group Policy, 983-984, 1060-1062
groups, 958
implementation, 922-925
IP virtualization, 930
local resource redirection, 942-945
management, 982
MMC, 925
modes, 925-927
monitoring, 945-947
Network Level Authentication, 981
network requirements, 952
optimizing, 33-36
physical placement of, 952
planning, 947-953
PowerShell management, 983
reasons for renaming of, 928
RemoteApps, 35-36, 940
Role Administration Tool, 982
security, 979-981
service packs, applying, 984
sessions, remote management of, 982
Single Sign-On, 945
support, 924, 981-984
tools, 676
users, 923-924
viewing, 945-947
Web Access, 34-35
Windows Installer compatibility, 929

**read-only**

AD DS, 1308
DFS replication, 1162
DNS, 1310
SYSVOL, 1310

**Read-Only Domain Controllers. See RODCs**

**Read-Only Global Catalog (ROGC) servers, 122**

**read/write replicas, 32**

dreadiness, application verification, 488-489
reading information from files, 744-745
real-time live broadcasts, 1484
    Windows Media Services, 1492-1495

**records**

baseline documentation, 789
CNAME, 270
DS, 317
hosts, 267-268, 315-316
MX, 269-270
NS, 268
NSEC, 317
PTR, 270
RRs, 266-270
RRSIG, 317
SOA (Start of Authority), 267
SRV, 269, 289-291
TTL values, 279-280
types of, 270
zones, encryption, 321

**recovery, 1228-1232**

agents, restarting, 822-828
Big Bang migration, 489
BitLocker Drive Encryption, 1332-1333
DFSR, 32
disaster, 76, 1229-1230
Diskpart.exe command-line utility, 1110
DRA, 1324
files, 1282-1285
folders, 1282-1285
infrastructure, 1273
passwords, 1331
prioritization, 1230
RDS, 984
RODCs, 1316
shadow copies, 1169-1170
System Startup and Recovery tool, 1380-1382
recursive queries, executing, 276-277
Recycle Bin, 1256-1257, 1477
    AD, 10, 153
disaster recovery, 1292-1294

*How can we make this index more useful? Email us at indexes@samspublishing.com*
redirection
   EMS, 1264
   enforcement, devices, 933
   folder configuration, 1071-1075
   local resources, RDS, 942-945
reducing
   background work, 640
   load, 157
   overhead, performance monitoring, 1369-1370
   power consumption, 640-641
   replication, workloads, 1308
redundancy, 76, 1147
   implementation, DHCP services, 350-358
   OpsMgr, 810-811
   power, 1175
redundant array of inexpensive disks. See RAID
referrals, disabling DFS, 1164
reflection, 711
refresh, synchronous foreground, 1090-1091
registery.pol files, 593
registration
   DNS, 1214
   Dynamic DNS, 361
   snap-ins, 754
Registry
   permission settings, 509-510
   PowerShell management, 745-746
   security, 790
   values, 745
RegularExpression, 1143
relationships, transitive trust, 117
relative distinguished names, outlining, 121
relative identifiers (RIDs), 123
relay agents, DHCP, 332-333
reliability
   DHCP, 345-350
   file systems, 1118-1120
   Group Policy, 586
   monitoring, 1359-1360
   system file, 1118-1120
Reliability and Performance Monitor tool, 24
Reliability Monitor, 1368
remote access, 847-850
   reviewing, 61
   Routing and Remote Access dialog box, 479
   servers, 45
   upgrading, 54
remote administration
   support, 989
   Telnet server, 256-257
Remote Assistance configuration, 955
Remote Authentication Dial-in User Service. See RADIUS
Remote Desktop
   enabling, 98
   servers, 45
Remote Desktop connection authorization policy (RD CAP), 933
Remote Desktop Connection Broker (RD CB), 935-937
   deployment, 964-967
Remote Desktop Gateway (RD Gateway)
   deployment, 972-975
   role services, 931
Remote Desktop Licensing (RD Licensing), 937-940
   deployment, 977-979
Remote Desktop Protocol. See RDP
Remote Desktop Services. See RDS
Remote Desktop Services Manager (tsadmin.msc), 982
Remote Desktop Services Server performance, 1427
Remote Desktop Session Host (RD Session Host), 928-930, 949-951
   configuration, 959-961
   roles, 956-959
tolerance, planning, 953
upgrading, 952
Remote Desktop Virtualization Host (RD Virtualization Host), 930
Remote Desktop Web Access
deployment, 961-964
role, 934-935
Remote Differential Compression (RDC), 1102, 1150
Remote Installation Services. See RIS
remote installation, IIS, 379
remote management, 674-679
  power policies, 640
  Server Manager, 674-675
  WinRM, 653, 677-678
Remote Server Administration Tools, 675-677
  installation, 676-677
remote servers
  BranchCache, 1124-1125
  logging, viewing, 1357
remote shared folders, Windows Server Backup, 1236
Remote Storage Service. See RSS (Remote Storage Service)
remote workstations, Group Policy management, 1094-1095
Remote-Item cmdlet, 743
RemoteApps
deployment, 967-972
  RDS, 35-36, 940
remoting PowerShell, 716-720, 757-761
removable storage access, 1075
Remove-WMIObject cmdlet, 753
removing. See deleting
Rename-Item cmdlet, 744
renaming
  Active Directory, 20-21
  AD DS, 170-173
domains, 153, 492
  files, 744
Rendom tools, 172
replacing
domain controllers, 498-500
  system files, 1119
replicas, read/write, 32
replication
  AD DS, 129-131, 195-200
  AD, monitoring configuration, 824-826
  automation, 1147
  branch offices, 1339-1342
  collisions, 197
  compression, disabling, 212
  connections, 558
design, 216-220
  decentralized, 218-220
  hub-and-spoke, 217-218
  DFS, 1103, 1149-1150
  best practices, 1161-1162
  disabling, 1165
  planning, 1153-1154
  read-only, 1162
  DFSR, 31-32, 592, 1102
  disabling, 1165
  DRA, 1425
  File Replication Service, 592
  FRS, 1150
  GPOs, 591-593
  groups, 1158-1161
  IP, 210
  latency, 199-200
  multimaster, AD DS, 122
  multivalued attribute, 493
  New Replication Group Wizard, 1153
  optimization, 210
  passwords, 223
How can we make this index more useful? Email us at indexes@samspublishing.com
RDC, 1102
RODCs, 373, 1306
schedules, 209, 1155
SMTP, 210
synchronization, 197
topologies, 207-213, 1154-1155
WINS, 365-367
workloads, reducing, 1308

Reporting Wizard, 515
reports
  databases, 799, 807
  file systems, 1102
  FSRM storage, 1139-1140
  GPOs, creating, 632
  gpresult, 1036
  Group Policy Modeling, 577
  maintenance, 842-845
  OpsMgr, 798, 803
  performance, 795, 839-842
  Performance Monitor, 1366-1367, 1406
  reviewing, 791
  routines, documentation, 789-790
  schedules, OpsMgr, 839-845
  storage, FSRM, 1139-1140
  System Performance, 1367
  User Defined, 1366

Request Filtering feature page, 397
requests
  certificates, 411
  root CA server certificates, 832-835
requirements
  capacity analysis. See capacity analysis
  DirectAccess, 864
  DNSSEC, 318
  documentation, 766
  during compatibility testing, 532-533
  external storage support, 1109

firewalls, OpsMgr, 812-813
hardware
  BitLocker Drive Encryption, 1325
  OpsMgr, 805-806
IIS
  fault tolerance, 383
  servers, 382-383
  minimum hardware, 84
OpsMgr components, 805-807
RDS
  networks, 952
  planning, 948-949
remoting, 718
scope of application testing, 529
software, OpsMgr, 806
support, external storage, 1109
Windows Media Encoder, 1504-1505
Windows Media Services, 1486
WSS, 1441-1442
rescanning disks, 1111
researching
  applications, 534-537
  products, 534-537
  tracking sheets for application compatibility research, 538
reservations, DHCP, 346-348
resolution
  clients, NetBIOS, 368
  customization, 946
  HOST, troubleshooting, 294
  Name Resolution Policy, 1029
  names, 322, 327
  need for legacy Microsoft NetBIOS, 362
  NRPT, 321

Resource Monitor, memory, 1417
Resource Record Signature (RRSIG) record, 317
resource records (RRs), 266-270
resources
  access, auditing, 671-674
  capacity analysis. See capacity analysis
  clustering, 1179
  compatibility testing, 531-532
  FSRM, 1130-1147
  generic cluster, 1180
  local redirection, RDS, 942-945
  networks, sharing, 252
  schedules, during disaster recovery, 1273
  segmenting, 980
  sharing, 163, 578
  tools, 1382
  WSRM, 925, 1408-1413

Results and Support section, 650

responses, generating, 798-799

responsibilities
  disaster recovery, delegation of, 1270-1271
  migration documentation, 71

restarting agents, recovery, 822-828

restoring. See also disaster recovery
  databases, DHCP automation, 337-338
  failover clusters, 1211-1215
  GPOs, 633-634
  Group Policy, 1298
  NLB nodes, 1223
  starter GPOs, 625-627
  SYSVOL folders, 1298

restrictions
  access, logon, 421
  clients
    connections, 1166
    leases, 472-473
  group configuration, 1080-1084
  physical access, 421
  software policies, 1049-1051
  write access to removable storage, 1075

results
  compatibility testing, 542, 546
  GPMC, 1091-1094
  Group Policy, 634
  lab testing, 74-75
  pilot phases, 77

retention policies, 1438

retiring domain controllers, 501-503

Retry Task Wizard, 515

return on investment (ROI), 765

Reverse Address Resolution Protocol (RARP), 329

reverse lookup zones, 265, 272

reverting to snapshot sessions, 1540

reviewing
  configuration, IIS, 1447
  documentation, 767
  GPO models, 1093
  original Microsoft directories, 114
  Programs and Features tool, 1448
  remote access, 61
  reports, 791
  WAN (wide area network), 62

RIDs (relative identifiers), 123

rights
  AD RMS, 451-454
  DRM, 451
  RMS, 41

Rights Management Services (RMS), 26, 41

RIPREP images, 1016

RIS (Remote Installation Services), 26, 991
  upgrading, 1016

RISETUP image, 1016

risks
  migration documentation, 71
  security, identifying, 679
  speed versus, 69
RMS (Rights Management Services), 26, 41
roaming profile cache management, 930
Robomon/Logitude, 1414
RODCs (Read-Only Domain Controllers), 22, 372-374
branch offices, 30, 1306-1310, 1339
deploying, 220-224, 372-374, 1311
functionality, 1306
installation, 1310-1323, 1319-1323
leveraging, 1308-1310
limitations, 1311-1312
options, 1315
phased migration, 493
replication, 196, 373, 1306
Server Core, 1318-1319
ROGC (Read-Only Global Catalog) servers, 122
ROI (return on investment), 765
Role Administration Tool, 982
Role Services section, 649
roles, 643-647
AD CS, 446
AD DS, 644
DNS, 131-133
groups, 127-129
AD FS installation, 234
Add Roles Wizard, 334, 1522
adding, 97, 647
administration, separation at branch offices, 1307
agents, monitoring, 801
backups, 1248
BranchCache, 31
CAs, 445-446
deleting, 647
DHCP, selecting, 313
DNS, 264, 284-285
File Services, 644, 1120-1121
FIM, 239-240
FSMO, 485
global catalogs, 370
Hyper-V, 1519, 1522-1524
installation, 248, 642
management, 647
migration documentation, 71
monitoring, 647
OM, 122-124, 500-501
Remote Desktop Session Host servers, 956-959
replication in AD DS, 196
Server Manager, 648-651
servers
defining, 429
migration, 39-40, 515-516
optimizing, 40-42
performance optimization by, 1423-1429
services
AD CS, 446
disaster recovery, 1291-1302
Web Servers, 386-388, 644
Windows Server 2008 R2, 8-9
Windows Server Core, 108-110
Windows Server Updates Services, 989
Roles node, 248
Roles Summary window, 648
rollbacks
guest images, 1539
images, 1538
strategies, 76
rolling blackouts, 1229
rollouts, pilot phases, 76-77
roots
CA server certificate requests, 832-835
DFS, 1155-1157
DFS namespaces, 1152, 1155-1157
hints, DNS, 281-284
management server, 799
zones, forest for _msdcs, 287-288
Route, 1377-1378
routers, 1175
equivalent, 1175
endpoint configuration, 785
routes, tunneling, 303
routines
documentation, 789-790
maintenance, 1394
Routing and Remote Access dialog box, 479
Routing and Remote Access Service. See RRAS
routing between networks, 476
RPCSEC_GSS, 247
RRAS (Routing and Remote Access Service), 3, 462, 847-850
authentication, 856-858
features, 851-852
network policy modification, 479
servers, 854, 886-887
services, 851-852
VPNs
deployment, 473-480
enabling functionality, 476-479
RRs (resource records), 266-270
RRSIG (Resource Record Signature) record, 317
RSCA (Runtime Status and Control API), 378
RSS (really simple syndication) feeds, WSS, 1458
RSS (Remote Storage Service), 1101
file systems, 1101
rules
classification, 1143-1144
Connection Security, 660
events, monitoring, 797
firewalls, 425-428
inbound, 425, 660
outbound, 425, 660
performance, monitoring, 797
ports
filtering, 1216-1217
formatting, 1216
Run As Administrator command, 422-423
Run As dialog box, 422
running
add-on application server functions, 46
built-in functions on application servers, 44-45
Disk Defragmenter, 689
Live Migration, 1549-1550
manual backups, 1247-1249
Validate a Configuration Wizard, 1193-1195, 1542-1543
runspaces, 761
Runtime Status and Control API (RSCA), 378
runtime, common language, 420
S
Safe E-Mail Servers section, 1451
SANs (storage area networks), 1109
booting from, 1109
disaster recovery documentation, 1234
disk storage for host servers, 1520
optimizing, 37-38
SAS (Serial Attached SCSI), 1188
satisfaction, end-user, 78
saving
files, 41
power, 640-641
state, 1537
scalability
servers, 1342
URLs, monitoring, 796

How can we make this index more useful? Email us at indexes@samspublishing.com
scanning
  CHKDSK, 694
disks, 1111
Sfc.exe, 1119
scavenging DNS, 280-281
SCCM (System Center Configuration Manager), 1396
  AD site administration, 552
SCCP (System Center Capacity Planner), 1413
Scheduled Tasks, creating, 1069
ScheduledDefrag task, 658
schedules
  backups, 663, 1238
documentation, 766
Domain System Volume replication, 592
fair share CPU scheduling, 929
maintenance, 685-695
migration documentation, 73
modification, 199
replication, 209, 1155
reports, OpsMgr, 839-845
resources during disaster recovery, 1273
site link replication, 203
Task Scheduler, 1382-1388
Windows Server Backup, 1241-1244
schemas
  AD DS, 120-121
  extending, 120
global catalog, avoiding full AD synchronization, 213
masters, 123
modification, 120
objects, 120
placeholder domain model, 168
security, 168
updating, 490
SCOM (System Center Operations Manager), 788
scopess
  AD groups, 563-564
  applications, testing, 527-529
  creating, 333-336
DHCP
  configuration, 348, 472-473
  Delay configuration, 354
  enabling NAP 473
  multicast scopes, 358
  superscopes, 358
DHCPv6 configuration, 314-315
groups, 180-181
PowerShell, 724-726
private, 725
projects, defining, 54-56
scripts, 408
  split, DHCP 351-357
SCP (Service Connection Point), 454
screening files, 1099, 1130, 1136-1139
  policies, 1131
screens
  content, capturing, 1510-1511
desktops, 6
files
  creating, 1135-1139
  exceptions, 1139
  policies, 1131
scripts
  ActivePerl, 257
  command line, 1489
  ISE, 704
  porting, 247
  PowerShell, 18, 699, 710-711
  scopes, 408
  SUA, 253
  WSH, 701
Scripts node, 1030
SCW (Security Configuration Wizard), 1026
SD DS, X.500, 119
SDK (software development kit), 799
SDM (System Definition Model), 798
search engines, WSS, 1440
searching
  libraries, 1455
  servers, sites, 557
secondary zones, 289-290
Secure File Transfer Protocol (FTPS), 1104
Secure Socket Tunneling Protocol (SSTP), 852
Secure Sockets Layer. See SSL
security, 679-680. See also access
  AD DS, 115, 133-134
  administration, 117, 412-414
  antivirus, 433
  assessments, 791
  backup deployment, 434
  BitLocker Drive Encryption, 31, 1323-1326
    configuration, 1326-1333
    deleting, 1333
    partitions, 1327
    recovery passwords, 1332-1333
    volumes, 1331-1332
  connecting, 34
  Connection Security rules, 660
  defining, 419-420
  DHCP, 359-361
  DNS, updating, 279-280
  DNSSEC, 316-323
documentation, 790-791
domain controllers, DHCP, 361
domains, 159
encryption, IPSec, 454-456
Event Viewer, 673
FDE, 1323
files, 429-433
firewalls, 424, 812-813
GPOE, 609
GPOs
  filtering, 599-600
  management, 631
Group Policy, 585-586, 1030
  groups, 178, 563
  IIS, 407-416
  improvements to, 26
  IPSec, 862
  layers, 420
  logging, 1359
MBSA, 1394
mitigation, 374
multiple layers of defense, deployment, 442
NTFS, 430-431
OpsMgr, 811-814
patches, WSUS, 439
physical
  branch offices, 1303
  deployment, 420-424
  policies, 27, 1025
PowerShell, 729-732
RDS, 979-981
risks, identifying, 679
schemas, 168
Server Manager, 429-430
servers, 418-419, 427-430
service accounts, 814
shares, comparing to NTFS security, 431
SSL, 622
subsystems, optimizing, 26-27
templates, GPOs, 590
transport, 27, 440-441, 444
universal groups, 563
user management, 569

How can we make this index more useful? Email us at indexes@samspublishing.com
Windows Firewall
configuration, 98
integration, 424-428
Windows Server 2008 R2, 408
wireless networks, 424
WSUS, 434-439
Security Configuration Wizard (SCW), 1026
Security Filtering settings, 186
security identifiers. See SIDs
Security log, 1354
Security Settings node, GPOs, 1030-1032
Security Translation Wizard, 515
security-based configuration group deployment, 808
segmenting resources, 980
Select Role Services page, 248
selecting
AD DS, domain structures, 154-155
authentication, 858-859
backups, 1284
bit rates, 1507
DFS types, 1152-1153
DHCP roles, 313
DirectAccess, 873-876
disks, 1113
File Services roles, 1121
hub-and-spoke topology, 1160
installation types, 91-92
internal namespaces, 152
license programs, 979
local Group Policy for administrators, 1035
locations, installation, 92
namespaces, AD DS, 151-152
new installations, 85-86
operating system installation options, 1532
operating systems, 91
OUs and groups, 129
server types, 86-87
single domain models, 155-156
sites, 208-209
System State only backups, 1250
versions, 84-85
volumes, 1288
VPN, 873-876
self-healing NFTS, 6-7
separation
of GPO functions, 617-618
of traffic, DirectAccess, 869
Serial Attached SCSI (SAS), 1188
Serial Port Console Redirection (SPCR), 1265
Server Core
AD DS domain controllers, deployment, 206-207
installation, 1484
.NET, 379
RODC installation, 1318-1319
versions, 14-16
Server for Network Information Services (SNIS), 254
Server Manager, 647-651
Add Features Wizard, 364
Add Roles Wizard, 8
BitLocker, installation with, 1326
configuration, 657-661
diagnostics, 652-657
Disk Management, 664-665
Event Viewer, 652-653
features, 651
Hyper-V, adding roles, 1522-1524
Performance Monitor, 653-656
remote management, 674-675
roles, 648-651
security, 429-430
services, 660-661
storage, 661-665
Task Scheduler, 657-659
Windows Firewall
integration, 424
   with Advanced Security feature, 659-660
Windows Server Backup, 662-663
WMI Control tool, 661
Server Message Block 2.0, 7
Servermanagercmd.exe command-line utility, 994
servers
   access-based enumeration, enabling, 1162-1163
   AD, 856
   add-on application server functions, running, 46
   all-in-one, 807
   APIs, 379
   applications, Windows Server 2008 R2 as, 8-10
   backups, 98
   BITS Server Extensions Tools, 676
   BranchCache configuration, 1334-1335
   build procedure documentation, 781-782
   certificates, 856, 878-879
   clustering, 45
   consolidating, 54
   critical, 1175
   design decisions, 66
   DHCP, 45
      authorization, 360
      clustering, 357-358
      configuration, 472-473
      migration, 338-341
      services, 329-330
   DHCPv6 configuration, 313-315
   disaster recovery documentation, 1234
   disks, fault tolerance, 1176
   DMZs, monitoring, 831-837
   DNS, 44, 266
   ES, 461
   failures, 1275-1277
   farms, support, 379
   files, 8
   FSRM, 1130-1147
   FTP, 378. See also FTP (File Transfer Protocol)
   gateways, 800
   global catalog, 44
   Group Policy, 553. See also Group Policy
   hosts
      configuration, 1526-1529
      directory of videos for playback, 1498-1500
      navigation, 1526-1529
   IIS, requirements for, 382-383
   implementation, identifying technical goals, 53-59
   installation, 82-83. See also installation inventory, 535
   management, 800, 807, 988-989
   namespaces, adding, 1157-1158
   Network Policy Server, 45
   PES, 508
   pilot phases, 76
   playlist configuration, 1501-1503
   preferred bridgehead, applying, 206
   printers, adding, 579
   printing, 8
   RADIUS, 45
   Remediation Servers, 461
   remote access, 45
   Remote Desktop Session Host, 949-951
   Remote Server Administration Tools, 675-677
   remote servers, BranchCache, 1124-1125
   RIS, upgrading, 1016
   RODCs, configuration as, 223

How can we make this index more useful? Email us at indexes@samspublishing.com
services
accounts, security, 814
AD CS, 444-450
AD RMS, 451-454
Apple Mac, 1104
applications, 9, 535-536
Automated Deployment Services, 991
availability, 1177
bare minimum, identifying, 1231
databases, failover clustering, 1178
DHCP
clients, 330
migration, 341-344
redundant implementation, 350-358
servers, 329-330
Directory Management Service, 1451
directory, evolution of, 114-115
disaster recovery documentation, 1234
domains, 8
failover clusters, 1203-1205
File Replication Service, 592
File Services roles, adding, 1120-1121
file systems, 1102-1104
access, 1102-1104
quotas, 1098-1099
files, failover clustering, 1177
FSRM, 1099. See also FSRM (File Server Resource Manager)
FTP 398. See also FTP (File Transfer Protocol)
Hyper-V, running other on, 1521
identifying, 1228
modification, 739
monitoring, 796, 1347
networks, changes in Windows Server 2008 R2, 328
NFS, 248-249, 1104
NLA, 587

Service Account Migration Wizard, 515
Service Connection Point (SCP), 454
service packs (SPs), 681-685
Service (SRV) records, 269
DNS, 289-291
service-level agreements (SLAs), 61, 788, 795, 1231-1232

ROGC, 122
roles
defining, 429
migration, 39-40, 515-516
optimizing, 40-42
performance optimization by, 1423-1429
root management, 799
RRAS, 854, 886-887
scalability, 1342
security, 418-419
hardening, 427-430
layers, 420
shares, 1122
single on-demand video playback, 1496-1497
sites, searching, 557
SMTP installation, 1450
stub master, entering, 274
telnet server, 247
types, selecting, 86-87
unattended, installation, 111
Virtual Server, 748
virtualization, 42, 45, 1429, 1513, 1519-1520
WDS
adding install images, 999-1000
configuration, 994-997
Web, 45
Windows Server Backup, 1167, 1235-1238
Windows Server Migration Tools, 338-341, 516-517
WSUS, 434-439
zone transfer configuration, 275

Service Account Migration Wizard, 515
Service Connection Point (SCP), 454
service packs (SPs), 681-685
Service (SRV) records, 269
DNS, 289-291
service-level agreements (SLAs), 61, 788, 795, 1231-1232
NLB, 1215
PES, 508
PowerShell, management of, 737-739
printing, failover clustering, 1177
Remote Desktop Session Host servers, 956-959
RIS, 991
roles
  AD CS, 446
    backups, 1248
    disaster recovery, 1291-1302
RRAS, 462, 851-852
Server Manager, 660-661
status, management, 738
testing, 1206
VSS, 1100
Web, auditing, 409
Windows Deployment Services Tools, 676
Windows Media Services. See Windows Media Services
WSUS, 434-439, 684-685
Services and Applications group, 1179
Session 0 isolation, 941-942
Session State feature page, 393
sessions
  background authentication, 933
  captured broadcasts, 1509
  collaboration, 63-64
  granular configuration control, 940-941
  RDS, remote management of, 982
  Remote Desktop Session Host servers, 949-951
  timeouts, 932
Set-ItemProperty cmdlet, 745
Set-WMIInstance cmdlet, 751
settings
  All Settings Disabled option, 573
  baseline values, 1369-1371
default configuration, 642
execution policies, 732
GPOs, 588, 595, 632
Group Policy, 1028-1033
groups, options, 512
Hyper-V, 1526
Immediate Task, 1069
IPv6 addresses, 311-313
lockout accounts, 1077
networks, modifying for guest sessions, 1533-1534
Performance Monitor, management, 1363-1364
policies, NPS enforcement, 465-473
printers, migration, 521-522
Registry permissions, 509-510
Task Scheduler, 658
tasks, 1387-1388
trigger options, 1384-1385
UAC, 1046-1048
Windows Settings node, 1029-1030
Windows Update configuration, 1065
Settings menu, 1458
Setup log, 1354
SFU (Windows Services for UNIX), 245
SHA (System Health Agent), 461
shadow copies
  configuration, 1168
data recovery, 1169-1170
enabling, 1263-1264
files, 1283
recovery, 1169-1170
volumes, 1190
VSS, 1100
Share and Storage Management console, 1118-1128
Share Properties dialog box, 1124
Shared Configuration store, 40

How can we make this index more useful? Email us at indexes@samspublishing.com
shared networks
  folders, Windows Server Backup, 1244-1245
  resources, NFS configuration, 252
shared storage, 1181
  failover clusters, 1187-1188
shared volumes, clustering, 1202-1203
SharePoint, 28. See also WSS (Windows SharePoint Services)
shares
  access, management, 1122-1128
  creating, 1119
  DFS. See DFS (Distributed File System)
files, 28, 1152
folder management, 1118-1128
permissions, validation, 1279
security, comparing to NTFS security, 431
servers, 1122
troubleshooting, 1278
sharing, 1122
  CSC, 1123-1124
  CSV, 1540, 1545-1546
  fair share CPU scheduling, 929
files, enabling BranchCache, 1125
folders
  management, 1125-1128
  VSS, 1100
  Windows Server Backup, 1236
knowledge, 766-767
network resources, 252
permissions, 1128
resources, 163, 578
Windows folders, 1103
shells
  Bourne, 700
  C, 700
commands, 800
history of, 700-701
overview of, 700-701
PowerShell, 678
short message service (SMS), 798
shortcuts
  relationships, 171
  Run As Administrator command, 422-423
  trusts, 150
shuffling video, 1499
SHV (System Health Validator), 461
  configuration, 466
SID History attributes, 506
  filtering, 163
SIDs (security identifiers), 123, 178, 182
  domain configuration, 510-511
signatures
  File Signature Verification (Sigverif.exe), 1119
  RRSIG records, 317
signing, drivers, 99
Silverlight, 1485
Simple Mail Transfer Protocol. See SMTP
simple volumes, 1107
simplifying tasks, capabilities, 17-20
simulation, cluster resource failures, 1207
single broadcasts, 1484
single domains
  administration, 564
  controller servers, 489-491
  models, 155-157
single-forest models, 160-162
single on-demand video playback configuration, 1496-1497
single points of failure
  identifying, 1228
  in clustering, 37-38
Single Sign-On (SSO), 254
  integration, 1438
  RDS, 945
single-server OpsMgr 2007 R2 installation, 815-818
Site Directory (SharePoint Server 2007), 1438
Site Hierarchy, 1477
Site Settings page (settings.aspx), 1475
site-to-site VPNs, 476
sites, 129
  AD, 200-207
    administration, 551-553
    GPOs, 1042
    links, 552-553
    clients, assigning, 201
  collection, WSS management, 1475-1479
  configuration, 554-562
  costs, 205-206
  creating, 554-556
  delegation, 561-562
  design, mapping, 207-208
  domain controllers, adding, 557-558
  establishing, 207
  Group Policy, 553, 616-617
  links, 209
    applying, 202-204
    establishing, 558-561
    selecting, 208-209
  servers, searching, 557
  subnets
    associating, 201-202, 209
    creating, 556-557
  WSS, 1437
sizing
  databases, OpsMgr, 809
  servers to support virtualization, 1519-1520
skills, communication, 59
SLAs (service-level agreements), 61, 788, 795, 1231-1232
slow link detection, Group Policy, 602-603
small businesses, GPOs, 1042-1043
smart cards
  logon access, 423
  PKI, using in, 450
SMB (server message block), 55, 1103
  branch offices, 1341-1342
  permissions, 1127
smoothing fonts, 947
SMS (short message service), 798
SMTP (Simple Mail Transfer Protocol), 179
  installation, 1450
  replication, 210
  tools, 676
SMTP E-Mail feature page, 394
snap-ins
  Disk Management console, 1110
  disk management MMC, 1110
  GPMC, 607-608
  MMC, Windows Server Backup, 1238
  PowerShell, 715-716, 754-755
  Windows Media Service, 1489
snapshots
  guest images, 1538-1539
  guest operating system sessions, 1538-1540
  Hyper-V, 1521, 1537
  image rollbacks, 1538
  reverting to, 1540
SNIS (Server for Network Information Services), 254
SNMP (Simple Network Management Protocol), 798
Snover, Jeffrey, 702
SOA (Start of Authority) record, 267
SOAP, 718
  soft faults, 1418
  soft limits, 1134
  soft skills, 59

How can we make this index more useful? Email us at indexes@samspublishing.com
software. See also applications
  antivirus, 433
  corruption, 1230
  disaster recovery documentation, 1234
  Microsoft Desktop Optimization Pack for Software Assurance, 612-613
  package deployment, 1087-1090
  procurement, 58
  requirements, OpsMgr, 806
  restriction policies, 1049-1051
  upgrading, 54
  WSS, 1441-1442
software development kit (SDK), 799
solutions, disaster recovery, 1232-1233
Sort-Object cmdlet, 747
sorting logs, 1356
source domains, PES installation, 509
source files, downloading Windows Media Services, 1490
SP (service patch) compatibility, 540
spanned volumes, 1107-1108, 1113
spanning monitors, 946
SPCR (Serial Port Console Redirection), 1266
special-purpose domain model, 155, 169-170
Specialized Security Limited Functionality (SSLF), 622
specifying
  NICs, 478
  RADIUS settings for VPNs, 478
specifying languages, 90
speed
  links, 785
  versus risk, 69
split scope, DHCP, 351-357
spreadsheets, 1471-1475. See also Excel 2007
Sprint, 29
SPs (service packs), 681-685
SQL (Structured Query Language)
  Database Space report, 845
  FIM installation, 240
  WSS, 1104
SQL Server, Management Studio Express, 1448
SRV (Service) records, 269
  DNS, 289-291
SSL (Secure Sockets Layer), 1447
  authentication, 410
  certificates, 409-413, 1337
SSL Settings feature page, 397
SSLF (Specialized Security Limited Functionality), 622
SSO. See Single-Sign On
SSTP (Secure Socket Tunneling Protocol), 852, 863
  advantages of, 874
  connection prevention, 898
  troubleshooting, 895
stability
  networks, 60
  system files, 1118-1120
staged RODC installations, 1319-1323
staging folders, 1154
stakeholders, migration planning phase, 67
standalone
  CAs, 444
  DFS namespaces, 1149, 1153
  local configuration, Group Policy, 1033-1036
  root certification authority, 445
  subordinate certification authority, 445
  systems, security templates, 591
Standard Edition, 12-13
standard questionnaires, 60
standard quota sizes, 1130
standardization, Group Policy, 1033
standards
  Internet, 116
  support for, 19
Start of Authority (SOA) record, 267

starter GPOs, 594-607
- backups, 625-627
- creating, 622-625
- enabling, 623-624
- functionality, disabling, 628
- policies, 623
- restoring, 625-627

starting
- DNS scavenging, 280-281
- OU designs, 182-184
- playlists, 1503
- publishing points, 1495
- real-time live broadcasts, 1495
- single file publishing points, 1497

startup
- options, 1264-1265
- System Startup and Recovery tool, 1380-1382

states
- clusters, restoring to previous, 1212
- domain controllers, disaster recovery, 1294-1298
- health state validation, 460
- monitoring, 798
- of compatibility, 538-541
- saving, 1537
- System State
  - backups, 1249-1250
  - disaster recovery, 1292

static classes, 712
static IP addresses, 88

status
- disks, 1115
- GPOs, 601-602, 629-630
- service management, 738

step-by-step procedure documents, 780

Stop Service option, Hyper-V, 1528

storage
- adding, 1544-1545
- arrays, Fibre Channel, 1188-1189
- backups on DVDs, 1245-1246
- capacity analysis. See capacity analysis clustering, adding, 1200-1201
- disks for host servers, 1520
- documentation, 766
- external, management, 1109
- failover clusters, 1187-1188
- file system quotas, 1098-1099
- FSRM
  - generating reports with, 1139-1140
  - reports, 1139-1140
- GPOs, 591-593
- iSCSI, 1189-1190
- limitations, 695, 1131
- policies, 1131
- power management, 640
- quotas, 1098-1099
- removable access, 1075
- RSS, 1101
- Server Manager, 661-665
- Share and Storage Management console, 1118-1128
- shared, 1181
- upgrading, 54

storage area networks. See SANs

stored single files, broadcasting, 1495-1497

stores, OpsMgr, 800-801

strategies
- backups, 1234-1235
  - for determining implementation timelines, 56
  - migration, 486
  - rollback, 76
  - virtualization, 1515-1517

stretch clusters, 1182

How can we make this index more useful? Email us at indexes@samspublishing.com
stretched clusters, 38
String property, 1141
String type, 1143
StringCaseSensitive, 1143
striped volumes, 1108-557, 1113
structured design documents, 64-66
Structured Query Language. See SQL
structures
  AD CS, 446
  AD DS, 116-119, 154-155
  DNS, 261
domains, 149-151
groups, 174-176
IPv6, defining, 214-215
OUs, 126
stub zones, 272-274
SUA (Subsystem for UNIX-based Applications), 245, 247, 252-253
  installing, 253
  programming languages, 253
  scripts, 253
subdomains, 160. See also domains
  trees, viewing, 117
subfolders
  ADM, 593
  Machine, 593
  User, 593
subnets
  AD site administration, 552
  mask to prefix length, 554
  sites
    associating, 201-202, 209
    creating, 556-557
subscriptions
  event configuration, 1354-1355
  OpsMgr, 828-831
Subscriptions folder, 1354

subsites, 1475
Subsystem for UNIX-based Applications. See SUA
subsystems
  disks, evaluating, 1421-1422
  external disks, 1109
  networks, monitoring, 1422-1423
  security, optimizing, 26-27
summary documents, compatibility testing, 534
superscopes, DHCP, 358
support
  AD DS
    DNS, 115
    security, 115
  BlitLocker authentication, 1330
  branch offices, 30-33
  disaster recovery documentation, 1234
  EFI, 991
  end users, 989
  environments, 78
  external storage, 1109
  for standards, 19
  international languages, 246
  IPv6, 213-216
  Kerberos, 247
  multimonitor, RDP, 34
  Netgroups, 247
  phase, migration, 485
  RDS, 924, 981-984
  requirements, external storage, 1109
  SANs, 38
  server farms, 379
  technical, 1394
  template file formats, 23
  tools, 1382
  Unicode characters, 286
  UNIX updates, 247
  video, RDP, 34
Windows Server Backup, 1235-1237
WMI Management, 247
switches, 1175
synchronization, 1123-1124
AD, avoiding full, 213
cross-forest trusts, 162
devices, 27
distributed environments, 227-232
FIM, 236-240
multiple identities with FIM, 242
passwords, 254
performance, 1341
replication, 197
sharing, 1123
synchronous foreground refresh, 1090-1091
syntax, DOSShell, 701
Sysprep, 1016
System Center Capacity Planner (SCCP), 1413
System Center Configuration Manager. See SCCM
System Center Operations Manager. See OpsMgr
System Center Virtual Machine Manager (VMM), 1519
system compatibility, verification, 99
System Configuration utility, 1295
System Definition Model (SDM), 798
system failures, 1275-1277
System File Checker (Sfc.exe), 1119-1120
system files
reliability, 1118-1120
stability, 1118-1120
System Health Agent (SHA), 461
System Health Validator (SHV), 461
configuration, 466
System log, 1354
system messages, 933
System Performance report, 1367

System Services section, 649
System Startup and Recovery tool, 1380-1382
System State
backups, 1249-1250, 1394
disaster recovery, 1292
domain controllers, disaster recovery, 1294-1298
system-level fault tolerance, 1171-1174
building, 1174-1177
clustering, 1177-1182
SYSVOL, 1150
folders, restoring, 1298
policies folder, 592
read-only, 1310

T

tables
GPT, 1105
NRPT, 321
tape devices, Windows Server Backup, 1237
targets
DFS, limiting connections to site, 1165-1166
folders, 1152, 1159, 1166
item-level targeting, 1039, 1058-1060
maintenance, 1164-1165
Task Manager
capacity analysis, 1396-1398
debugging and logging, 1345-1349
Task Scheduler, 1382-1388
Server Manager, 657-659
Summary window, 659
tasks
actions, 1386
backups, 1235
conditions, 1386-1387

How can we make this index more useful? Email us at indexes@samspublishing.com
delegating, 184
desktop administration, 1020-1021
disaster recovery, assignment, 1273
Event Viewer, 1356
file management, 1144-1147
GPOs, 619-637
history, 1388
Immediate Task setting, 1069
Initial Configuration Tasks tool, 641-643
ScheduledDefrag, 658
ServerManager, 658
settings, 1387-1388
Tasks list, 1468-1469
TCP/IP (Transmission Control Protocol/Internet Protocol), 326
AD DS compatibility, 115
branch offices, 1339-1340
tools, 1372-1379
teams
backups, 1235
defining, 58-59
morale, 1273
technical goals, identifying, 53-59
technical reporting, 790
technical support, 1394
technologies
file systems, 1097-1104
identifying, 1228
transition, IPv6, 301-303
Telnet servers, 247
remote administration, 256-257
UNIX, installing, 257
templates
administrative. See also administrative templates
certificates, formatting, 831-832
Computer Configuration Administrative Templates node, 1032
document libraries, 1455
file screens, 1137-1139
Group Policy, administrative, 603-606
NPS, 461
quotas, 1134-1136
screening, 1099
security, 590
Teredo tunneling protocol, 308-311
Terminal Services. See RDS (Remote Desktop Services)
termination processes, 753
terminology
clustering, 1179-1182
DFS, 1150-1152
NAP 461
terms of use, accepting, 91, 101
testing
applications, 526, 527-529
Best Practice Analyzer, 25-26
compatibility, 523-526. See also compatibility applications, 541
defining goals for, 530-533
lab-testing existing applications, 543-545
MAP toolkit, 542-543
need for, 526-527
preparing for, 527-534
Prototype phase, 546-547
results, 542, 546
states, 538-541
tracking sheets for application compatibility research, 538
upgrading, 542
vendor verification, 537-542
DCDIAG, 693
DHCP, 336
DirectAccess, 910-914
Distributed Cache mode, 1336-1337
documentation, 777-779
failover, 1206-1208
Group Policy Modeling, 634
hardware, IHV, 1118
lab results, 74-75
migration, 545
mount points, 1107
planning, 73-75
upgrading, 545
UPS, 694
VPN connections, 891-892
text hierarchies, 183
theft of domain controllers, 1307
third-party
  applications, 1177
capacity planning tools, 1414-1415
management packs, OpsMgr, 805
snap-ins, registering, 755
thresholds
  file system quotas, 1098-1099
  notification, 1135
  quotas, 1098-1099
ThrottleLimit parameter, 760
throttling bandwidth, 1155
time
  customizing, 90
  frame for compatibility testing, 530-531
  zones, 642
  zones, configuration, 95
Time to Live (TTL), 279-280
timelines
  migration documentation, 71
  project plans, 67-68
timeouts, sessions, 932
tolerance, Remote Desktop Session Host servers, 953
Tolly Group, The, 1395
toolkits, MAP, 542-543

tools
  Active Directory Users and Computers, 17
  AD, 228
  AD DS, 675
  AD LDS, 675
  AD RMS, 675
  ADMX Migrator, 613
  adprep utility, 496-497
  Advanced Tools section, 650
  Arp, 1376-1377
  assessment, 1408-1414
  BitLocker, 31
  BitLocker Drive Encryption Tools, 676
  BITS Server Extensions Tools, 676
  BPA, 1371-1372
  built-in security, 420
  capacity analysis, 1395-1415
  Central Administration console, 1479
  command-line, Diskpart.exe, 1110
csvde.exe, 1252
  DCDiag, 1378-1379
desktop administration, 985-988
diskpart.exe, 1110, 1114-1116
dns, 675
  DSCMD, 296-297
  Disk Defragmenter, running, 689
diskpart.exe, 1110, 1114-1116
  DNS, 675
  FCI, 1140-1141. See also FCI (File Classification Infrastructure)
  File Services Tools, 675
  File Signature Verification (Sigverif.exe), 1119

How can we make this index more useful? Email us at indexes@samspublishing.com
file system management, 1102
folders, 650-651
FSRM, 1130. See also FSRM (File Server Resource Manager)
GPMC, 22, 607-608. See also GPMC (Group Policy Management Console)
GPME, 609
GPOE, 608-609
gpupdate.exe, 611
Group Policy, 607-615
   Log View (GPLogView), 613
   Management Tools, installation, 619-630
   Modeling, 575
   Starter GPO Editor, 609-610
Hyper-V, 676
IIS, 378, 379-380
Initial Configuration Tasks, 641-643
Ipconfig, 295, 1375-1376
Ldifde.exe, 1252
Microsoft Desktop Optimization Pack for Software Assurance, 612-613
migration, 38-40
   operating systems, 39
   server roles, 39-40
monitoring, 24
Netstat, 1377
Network Policy
   and Access Services Tools, 676
   MMC, 466
New Server Manager, 17-18
NLB, 676
Nslookup, 294-295, 1378
Ntbackup.exe, 1236
ntdsutil, 123
NTDSUTIL utility, 1295
Pathping, 1375
performance, 24
Performance Monitor, 1360-1372
Ping, 762, 1372-1374
planning, 1408-1414
Print Services Tools, 676
Programs and Features, 1448
RDS, 676
Reliability
   and Performance Monitor, 24
   Monitor, 1368
Remote Desktop Services Manager
   (tsadmin.msc), 982
Remote Server Administration Tools, 675-677
Rendom, 172
resources, 1382
Role Administration Tool, 982
Route, 1377-1378
security, optimizing policies, 27
Servermanagercmd.exe command-line utility, 994
site management, 1437
SMTP, 676
SUA, 245
support, 1382
Sysprep, 1016
System Configuration utility, 1295
System File Checker (Sfc.exe), 1119-1120
System Startup and Recovery, 1380-1382
Task Manager, 1345. See also Task Manager
Task Scheduler, 1382-1388
TCP/IP 1372-1379
third-party capacity planning, 1414-1415
TRACERT, 295-296
Tracert, 1374-1375
video, editing, 1504
wbadmin.exe, 1246-1249
wdsutil.exe command-line, 676
Web Server, 676
Windows Deployment Services Tools, 676
Window Memory Diagnostics Tool, 99, 1381
Windows Server Migration Tools, 338-341, 516-517
WINS, 676
WMI Control, Server Manager, 661
top-level sites, 1477. See also sites
topologies
customization, 1154
documentation, 783
full mesh, 1154
hub-and-spoke, 1154, 1160
ISTG, 204, 213, 558
multimaster concepts, 196
replication, 207-213, 1154-1155
WINS push/pull, 365
TPM (Trusted Platform Module), 1324
BitLocker Drive Encryption, 1328-1329
Tracert, 1374-1375
tracking
PMOs, 1269
sheets for application compatibility research, 538
traditional scenarios
DirectAccess, 898-916
VPNs, 876-878
traffic
QoS, 1422
separation, DirectAccess, 869
training
benefits of documentation, 764
documentation, 776-777
migration documentation, 71
prototype phase, 73-75
requirements during compatibility testing, 532-533
Training phase, migration, 485
Transaction Processing, 1395
transfers
files, 7
zones, 264-277, 1428
transition technologies, IPv6, 301-303
transitive trusts, 124, 150
cross-forest, 492
relationships, 117
Transmission Control Protocol/Internet Protocol. See TCP/IP
transmission types, 1020
transport security, 27
transport-level security, 440-441
digital certificates, 444
equachment, 443
need for, 442
traps, SNMP, 798
traversal, NAT, 455-456
trees
AD DS
domains, 117-118
multiple, 160-162
DIT, 120
naming, 167
triggers, 657
advanced settings, 1385-1386
options, 1384-1385
replication, 1153
troubleshooting
antivirus, RDS, 948
applications, access, 1282
Best Practice Analyzer, 25-26
bottlenecks, monitoring, 1415-1416
BranchCache, 1338
compete PC restores, 1291
DFS, 1163-1166
diagnostics, 24
disaster recovery, 1271-1274

How can we make this index more useful? Email us at indexes@samspublishing.com
Diskpart.exe command-line utility, 1110
DNS, 292-297
DNSCMD, 296-297
documentation, 783-784
Event Viewer. See Event Viewer
Get-Help cmdlet, 733-734
Group Policy applications, 575-577
hardware failures, 1229
“island” problem, 287
IIS, 378
install images, 1003-1005
IPCONFIG, 295
network access, 1278
Network Diagnostics Framework, 852
pilot phases, 77
RAID-5, 1108-1109
RDS, 981-984
server failures, 1275-1277
single points of failure, identifying, 1228
SSTRP 895
System File Checker (Sfc.exe), 1119
TRACERT, 295-296
VPN clients, 890-898
Windows Memory Diagnostics Tool, 99, 1381

Trusted Platform Module. See TPM

trusts

cross-forest transitive, 153-154, 492
domains, 124-125, 150-151
explicit, 124
policies, AD FS, 235
transitive, 117, 124
two-way transitive, 158

Trustworthy Computing initiative, 420
TTL (Time to Live), 279-280
tuning alerts, OpsMgr, 837-845
tunnels, 860
6to4 protocol, 305-308
automatic, 303
configuration, 303
DirectAccess, 867-868
ISATAP, 216, 303-305
protocols, 475
Teredo protocol, 308-311
VPNs, 474-475
two-way transitive trusts, 158
types

of accelerators, 713-710, 749
of administrative templates, 603
of CAs, 445-446
of connections, 784
of DFS, 1152-1153
of documentation, 765
of Group Policies, 588
of groups, 128, 178-180, 562
of images, WDS, 992
of installation, selecting, 91-92
of operating systems, installation, 91
of records, 270
of servers, selecting, 86-87
of single domain models, 157
of transmissions, 1020
of triggers, 1384

U

UAC (User Account Control), 1046-1048
unattended answer files, 1018-1019
unattended installation, operating systems, 990
unattended server installation, 111
UNC (Universal Naming Convention), 379, 1103
Unicast, 1217, 1493
Unicode character support, 286
uniform resource locators. See URLs
uninstallation, autouninstall of software packages, 1089
uninterruptible power supply. See UPS
unique addresses, 328
universal groups, 128, 181, 563
   caches, 371, 492
   memberships, caches, 211-212
Universal Naming Convention (UNC), 379, 1103
UNIX, 244-245
   Active Directory, configuration lookups, 250
   client configuration, 250-251
   integration
      components, 245-252
      prerequisites, 248
   interoperability components, 247-248
   shells, 700
   SUA. See SUA
   Telnet servers, installing, 257
Unmapped UNIX User Access, 247
Update Sequence Numbers. See USNs
Update This Server configuration category, 642
updating, 681-685
   automatic updates, 96-97, 682-684
   Automatic Updates client deployment, 434
   CD-ROM updates, 681
   DDNS, 286
   DNS security, 279-280
   documentation, 694, 767
   dynamic updates, DNS, 265
   installing, 97
   management, 988
   manual updates, 681
   MUS, 1490
   printer filters, 580
RDS, applying, 984
Reliability Monitor, 24
schemas, 490
Windows Media Services, 1488-1489
Windows Update, 642, 1065
WSUS, 434-439, 684-685
upgrading
   additional tasks, 99-100
   Big Bang migration, 491
   clustering, 1211
   compatibility testing, 542
   domain controllers, 497-498
   executing, 100-102
   functional levels, 503-504
   IIS, 383-389
   in-place upgrades, migration, 485-486
   NOS (network operating system), 54
   Remote Desktop Session Host servers, 952
   RIS, 1016
   selecting over new installations, 85-86
   testing, 545
   versions, 540
   Windows Server 2008 R2, 98-102
   WINS, 368-369
Upload menu, 1457
uploading rename scripts, 172
UPS (uninterruptible power supply), 1174
   testing, 694
uptime, optimization, 1271
URLs (uniform resource locators), 1456
   scaling, monitoring, 796
usage, domains, 126
User Account Control (UAC), 1046-1048
User Configuration node, 1032-1033
User Defined report, 1366
User subfolder, 593

How can we make this index more useful? Email us at indexes@samspublishing.com
users
access, RDS, 958
accounts
  creating, 414-415
  migration, 512-513
  UNIX, 246
activity, monitoring, 1349
GPOs, processing, 587
Group Policy management, 1070-1076
limiting, 75-78
management, 568-569
NIS, adding, 255-256
nonadministrators policies, 1025
policies, processing, 1027
Preferences User Drive Maps extension, 1058
profiles (SharePoint Server 2007), 1438
RDS, 923-924
USNs (Update Sequence Numbers), 196
  applying, 196-197
utilities. See tools

V
Validate a Configuration Wizard, 1542-1543
  running, 1193-1195
validation
  backups, 694
  DNSSEC, 317
  health state, 460
  permissions on NTFS folders, 1281
  planning, 75-78
  priorities, disaster recovery, 1272
  shares, permissions, 1279
  SHV, 461
values
  baseline configuration, 1369-1371
  baseline performance, 789
  Registry, 745
  TTL, 279-280
variables
  $Errors, 741
  $Sessions, 761
  PowerShell, 722
VBScript, 701
VDI (Virtual Desktop Infrastructure), 36
VDS (Virtual Disk Service), 1106
vendors, compatibility testing, 537-542
verification
  application readiness, 488-489
  backups, 686
  Big Bang migration, 488
  binding options, 334
  end-user satisfaction, 78
  File Signature Verification (Sigverif.exe), 1119
  GPOs, 621-622, 1036
  hardware, 689
  minimum hardware requirements, 84
  namespace server additions, 1158
  system compatibility, 99
  vendors, compatibility testing, 537-542
Verizon, 29
versions
  clean installations, 89-98
  document libraries, 1455
  IIS, upgrading from, 388-389
  number properties, 197-198
  selecting, 84-85
  upgrading, 540
  Windows Media Services, 1486-1488
  Windows Server 2008 R2, 12-16
VHDs (virtual hard disks), 1106, 1529
applying, 1116-1118
Dynamic VHD performance, 1531

video
capturing, 1508-1510
directories for on-demand playback, 1498-1500
editing, 1504
formatting, conversions, 1511-1512
looping, 1499
playback, on-demand configuration, 1496-1497
shuffling, 1499
support, RDP, 34

View menu, 1460

viewing
AD FS MMC administrative tools, 233
AppLocker, 1054
backup histories, 1247
directory publishing points, 1500
Event Viewer. See Event Viewer
federated forest models, 164
GPOs settings, 632
Group Policy Log View (GPLogView), 613
LDAP, 177
logs, 1357
multiple-tree domain models, 161-162
OUs, 126
Performance Monitor, 1360
placeholder domain model, 169
policies, GPMC, 569
PowerShell providers, 727
RDS, 945-947
reports, 1408
rules, firewalls, 425-428
screens, 6
Server Manager, 429-430
single-domain models, 156-157

special-purpose domain models, 170
Task Scheduler, 1384
trees, 117

views
Allitems.aspx, 1456
customization, 1353
Datasheet, editing, 1457
document libraries, 1455
Overrides, 796

virtual cluster servers, 1179
virtual desktop deployment, 975-977
Virtual Desktop Infrastructure (VDI), 36
virtual directories, 391
Virtual Disk Service (VDS), 1106
virtual disks, 1517
virtual guest memory, Hyper-V, 1518
virtual hard disks. See VHDs
virtual LAN identification (VLAN ID), 1527
virtual local area networks (VLANs), 38
virtual machine deployment, 1546-1548
Virtual Machine Manager (VMM), 1519
Virtual Memory System (VMS), 701
Virtual Network Manager, 1526-1528
Virtual PC, 1516
virtual private networks. See VPNs
Virtual Server 2005, 748, 1516
Virtual Server 2005 R2, 1517
virtual server performance, 1429
virtual-to-virtual image copying, 1519

virtualization
history of, 1516-1517
Hyper-V, 7-8, 166, 1517-1519
IP, RDS, 930
RD Virtualization Host, 930
servers, 42, 45, 1519-1520
strategies, 1515-1517
viruses, 701

How can we make this index more useful? Email us at indexes@samspublishing.com
visibility, OU, 178
vision, documentation of, 63-67
visual changes in, 16
VLAN ID (virtual LAN identification), 1527
VLANs (virtual local area networks), 38
VMM (Virtual Machine Manager), 1519
VMS (Virtual Memory System), 701
Volume Shadow Copy Service. See VSS
volumes, 1107
  BitLocker Drive Encryption, enabling, 1331-1332
  clustering, enabling, 1202-1203
  CSV, configuration, 1540, 1545-1546
  data compression, 1099
  Domain System Volume replication, 592
  encryption, 1099
  fault tolerance, 1108
    applying Disk Management snap-in, 1112-1114
    creating, 1112-1116
  file system quotas, 1098-1099
  folders, sharing, 1125-1128
  mirrored, 1108
  mount points, 1107
NTFS
  data compression, 1099
  encryption, 1099
  quota management, 1098-1099, 1128-1129
partitions, 1098, 1107
RAID-5, 1108-1109, 1113
selecting, 1288
shadow copies, 1190
shares, creating, 1122
simple, 1107
spanned, 1107-1108, 1113
striped, 1108, 1113
Windows Server Backup, 1236, 1287-1291
VPNs (virtual private networks), 28, 459, 850-856, 1103, 1175
  clients, 854
    configuration, 888-891
    troubleshooting, 890-898
  components, 853-925
  Connection Manager, 916-919
  connections, 462
  connections, testing, 891-892
  deployment, 473-479
  functionality, enabling, 476-479
  gateways, 476
  NPS, 854-856
  port connections, 875-876
  protocols, 858-863
  selecting, 873-876
  site-to-site, 476
  traditional scenarios, 876-878
  tunnels, 474-475
  VPN Reconnect (Windows 7), 29
VSS (Volume Shadow Copy Service), 1100, 1190
  applying, 1167-1170
  backups, 1167, 1262-1264
  file systems, 1100
  Hyper-V snapshots, 1521
  Windows Server Backup, 1167
W
WAIK (Windows Automated Installation Kit), 1007, 1018
WANs (wide area networks), 7
  branch offices, 1339-1342
  domain controller promotion from media, 154
  replication, 196
  reviewing, 62
wbadmin.exe, 1246-1249
   manual backups, 1247-1249
WDS (Windows Deployment Services), 26, 988, 991-994
   AD, preformatting computer accounts, 1013
   DHCP configuration, 997-998
   drivers, adding, 1008
   GUID, 1014
   images, 989
      boot, 992-993
      capture, 993, 1016-1020
      discover, 993, 1005-1016
      installation, 993
      types, 992
   installation, 994-1005
   migration, 1015-1016
   properties, 1013
   RIS, upgrading, 1016
   servers
      adding boot images to, 998-999
      adding install images, 999-1000
      configuration, 994-997
wdsutil.exe command-line tool, 676
Web Access, RDS, 34-35
Web console, 800
Web pages
   .htm files, 1494
   WSS, 1437
web proxying, 424
Web Servers, 45
   IIS roles, installing, 386-388
   modular-based IIS installation, 384
   roles, 644
   tools, 676
Web services, auditing, 409
websites
   Bindings dialog box, 412
   IIS, 382, 389-397
   properties, configuration, 392-397
   secure FTP, creating, 400-401
WebDav Authoring Rules feature page, 397
Wecsvc (Windows Event Collector), 653
weekly maintenance, 688-694
WEP (Wireless Encryption Protocol), 424
white pages, 114-115
wide area networks. See WANs
Wiki page library, 1455
WIM (Windows Imaging), 26, 999
Win32_WMISetting parameter, 752
windows
   Auditing Entry, 672
   Feature Summary, 648
   New Folder, 1159
   Performance Options, accessing, 1418
   PowerShell, 342
   Roles Summary, 648
   Server Manager Server Summary, 648
   Task Scheduler Summary, 659
Windows 2000 administrative templates, 604-605
Windows 2003, migration from, 11-12
Windows 7
   activation, 94
   administrative templates, 605-606
   folders, sharing, 1103
   Group Policy, 1025-1028
   Group Policy Management Tools, 619-620
   Mobile Broadband, 29-30
   VPN Reconnect, 29
Windows Automated Installation Kit (WAIK), 1007, 1018
Windows Clustering feature, 50
Windows Deployment Services. See WDS
Windows Deployment Services Tools, 676
Windows Error Reporting, 97
Windows Event Collector (WecsVC), 653

How can we make this index more useful? Email us at indexes@samspublishing.com
Windows Explorer, WSS, 1458
Windows Firewall, 642
   Advanced Security feature, 659-660
   configuration, 98
   integration, 424-428
Windows Imaging (WIM), 26, 999
Windows Installer, RDS compatibility, 929
Windows Internet Naming Service. See WINS
Windows Logs folder, 1353-1354
Windows Management Instrumentation. See WMI
Windows Media Encoder, 1504
   installation, 1505
   options, 1510-1512
   requirements, 1504-1505
Windows Media Services, 1481-1484
   audio/video, capturing, 1508-1510
   configuration, 1491-1492
   files, combining, 1501-1503
   installation, 1489-1492
   leveraging, 1489
   live events, broadcasting, 1506-1508
   overview of, 1484-1489
   real-time live broadcasts, 1492-1495
   requirements, 1486
   source files, downloading, 1490
   stored single files, broadcasting, 1495-1497
   updating, 1488-1489
   versions, 1486-1488
   video directories for on-demand playback, 1498-1500
   Windows Media Encoder, 1504, 1510-1512
Windows Memory Diagnostics Tool, 99, 1381
Windows PowerShell Provider, 379. See also PowerShell
Windows Registry. See Registry
Windows Remote Management (WinRM), 653, 677-678, 717
Windows Rights Management Services (RMS), 41
Windows Script Host (WSH), 701
Windows Search Service, 1121
Windows Security Health Validator dialog box, 466
Windows Server 2003, 144
   administrative templates, 604-605
   migration. See migration
Windows Server 2003 migration, 481-483
Windows Server 2008 R2. See also servers
   Active Directory, 9-10
   adding, 11
   administrative templates, 605-606
   allocation, 544
   application servers, 8-10
   changes
      in AD DS, 134-146
      in DHCP 336-344
      in network services, 328
      in WINS, 364
   configuration, 544
   defining, 5-10
   Delay configuration, 354
   disks, 1105-1109
   DNS in, 286-288
documentation. See documentation
Group Policy, 1025-1028
Group Policy Management Tools, 619
host operating system installation, 1522
overview of, 5-6
security, 408
unattended installation, 111
upgrading to, 98-102
versions, 12-16
Windows Server Backup, 662-663, 1167, 1235-1238. See also backups
access, 1285-1287
applying, 1239-1246
file recovery, 1283
installation, 1239-1241
management, 1285-1287
MMC, 1238
PowerShell cmdlets, 1238
schedules, 1241-1244
support, 1235-1237
volumes, disaster recovery, 1287-1291

Windows Server Core
activation, 108
domains, adding, 107
features, 108-110
installing, 103-105
managing, 105-111
roles, 108-110

Windows Server Migration Tools, 338-341, 516-517
deployment, 339-340
installation, 339

Windows Server Update Services. See WSUS

Windows Services for UNIX (SFU), 245
Windows Settings node, 1029-1030
Windows SharePoint Services. See WSS
Windows system failover documentation, 788
Windows System Resource Manager (WSRM), 925, 1408-1413

Windows Time, 198
Windows Update, 642
configuration, 1065
Windows Update console, 684. See also updating
Windows virtualization, 1513-1515. See also virtualization
Windows Vista administrative templates, 605-606

Windows XP administrative templates, 604-605
WinRM (Windows Remote Management), 653, 677-678, 717
WINS (Windows Internet Naming Service), 258-325, 361-364
backups, 1259-1260
configuration, 364-368
DNS integration, 362-364
Group Policy, sites, 553
installation, 364-368
lookups, 285
maintenance, 368
migration, 368
planning, 368
replication, 365-367
tools, 676
upgrading, 368-369
Windows Server 2008 R2, changes in, 364

Wireless Encryption Protocol (WEP), 424
wireless networks
  Group Policy, 1065-1068
  security, 424

witness files, clustering, 1180

wizards
  Add Account Partner Wizard, 235
  Add Applications Wizard, 236
  Add Features Wizard, 364
  Add Publishing Point Wizard, 1498
  Add Resource Partner Wizard, 235
  Add Roles Wizard, 235, 248, 263-266, 334, 1444, 1522
  ADMT migration, 506
  Configure Your Server Wizard, 429
  Control Wizard, 185
  Create Cluster Wizard, 1195
  DHCP Split-Scope Configuration Wizard, 354-357
  Discovery Wizard, 820

How can we make this index more useful? Email us at indexes@samspublishing.com
Exchange 5.5 Mailbox Translation Wizard, 515
Group Account Migration Wizard, 511
Group Policy Modeling Wizard, 1092
High Availability Wizard, 1548
Initial Configuration Tasks Wizard, 95
Network Printer Installation Wizard, 579
New Configuration Wizard, 1529
New Replication Group Wizard, 1153
New Scope Wizard, 333
Password Migration Wizard, 515
Printer Migration Wizard, 522
Provision a Shared Folder Wizard, 1126
Reporting Wizard, 515
Retry Task Wizard, 515
SCW, 1026
Security Translation Wizard, 515
Server Manager Add Roles Wizard, 8
Service Account Migration Wizard, 515
Validate a Configuration Wizard, 1193-1195, 1542-1543
WMI (Windows Management Instrumentation), 587
Control tool, Server Manager, 661
GPOs
  filtering, 600-601
  linking filters, 630-631
Management, support, 247
PowerShell, applying, 747-754
remoting, 717
Word 2007, WSS, 1469-1471
workgroups, 642
  local user policies, 590
  naming, 88
  security templates, 591
workloads
  characterization, 1394
  replication, reducing, 1308
workspaces
  multipage meeting, 1467
  WSS, 1437
workstations, local user policies, 590
World Wide Port Number (WWPN), 1189
worms, 701
Wrapper Playlist (.wsx), 1494
WS-Discovery, 1336
Wscript.exe, 701
WSH (Windows Script Host), 701
WshShell object, 745
WSRM (Windows System Resource Manager), 925, 1408-1413
WSS (Windows SharePoint Services), 41, 1104, 1431-1433
  backups, 1261-1262
  basic features of, 1436-1437
  benefits, 1464
  Central Administration console, 1449
  customization, 1440
  default site collection, 1452-1453
  disaster recovery, 1299-1302
  email configuration, 1449-1452
  Excel 2007, 1471-1475
  file systems, 1104
  IIS, reviewing configurations, 1447
  installation, 1440-1454
  libraries, 1453-1469
  lists, 1453-1469
  needs for, 1439-1440
  Office 2007 integration, 1469-1475
  out-of-the-box workflows, 1438
  requirements, 1441-1442
  SharePoint, past versions, 1434-1439
  site collection management, 1475-1479
  Word 2007, 1469-1471
WSUS (Windows Server Update Services), 434-439, 460, 684-685
  configuration, 437-439
  installation, 436-437
  prerequisites, 435
  security patches, 439
WWPN (World Wide Port Number), 1189
WWW Directory Publishing, 1103
X-Y-Z
X.500, AD DS, 119
xcopy command, 7
XML (Extensible Markup Language), 399
  GPO administrative policies, 594
Yes/No property, 1141
zombie detection, 493
Zone Signing Key (ZSK), 317
zones
  DMZs, 424, 477
  DNS, 132, 270-274
    automatic creation of, 287
    creating, 171
    moving, 505
    phased migration, 493
    transfers, 264-277
  DNSSEC, configuration, 318-323
  forest root for _msdcs, 287-288
  forward lookup, 271-272
  GlobalNames, 291-292, 327
  primary, 272
  record encryption, 321
  reverse lookups, 265, 272
  secondary, 272, 289-290
  stub, 272-274
  time, 95, 642
  transfers, 1428
ZSK (Zone Signing Key), 317