Chapter 1

What's New in Windows Server 2012 R2

Windows Server 2012 R2 has over 300 new features, and it's the first Microsoft Server OS that has connectivity with the cloud. Explaining all of those features would take much more than a chapter (which is, of course, why we wrote a book!), but let's use these first few pages to give you the lay of the land. Now, we realize that some reading this book are just getting started with Windows Server, and so for them, *everything* is new, but many others of you reading this already know tons about Windows networking and would just like a summary of what's new in Server—this chapter summarizes that and where *to* find it in the book.

By now, we've sat through about a zillion Microsoft presentations on Windows Server, and they all start the same way, so apparently we're required by law (or at least by custom) to present the following as the first heading when doing an overview.

In this chapter, you'll learn about:

- The dramatic changes to the user interface
- New Active Directory features enhancing deployment and manageability
- Improvements to PowerShell
- New technology added to Hyper-V
- Enhancements to Windows networking, making it faster and more secure
- The new management tools
- The important features of IIS 8.0

Windows Server 2012 R2 Introduction

Well, with a slogan like, "Built from the cloud up," it doesn't take a mental heavyweight to figure out what was intended with Windows Server 2012 R2. So what is cloud technology? In a nutshell, it's the practice of using a network of remote servers to store, manage, and process data, rather than a local server. Windows Server 2012 R2 extends these technologies to corporations to be used in the same way for their employees. All corporate data using either virtual machines or individual workstations can be backed up directly to the cloud either on or off site. Cloud technologies are the driving force for the way the world conducts business today and in the near future.

From small business to some of the largest datacenters in the world, Windows Server 2012 R2 is one hot ticket. With virtually hundreds of new features from virtualization, networking, storage, usability, and much more, Windows Server 2012 R2 will not disappoint. The more we use it, the more we like it, and we think you will too!

The following sections offer a brief overview of what's new in this book and where to read more about those features.

Because this is an introductory chapter, all of the topics covered here will be talked about in depth elsewhere in the book.

Windows Server Editions

When Windows Server 2012 was released, you had the choice between Standard and Datacenter editions in both the Server Core and GUI versions. With the release of Windows Server 2012 R2, you have two more editions to choose from: Foundation and Essentials. Not only does each version have different features, but the price for each license reflects each version's features. Let's discuss the differences among all the editions.

Standard Edition

This is the enterprise-class cloud server and is the flagship OS. This chapter will cover in detail the changes affecting the Standard edition, because this is the most popular choice. This server is feature rich and will handle just about all your general networking needs. This server can be used for multipurpose or individual roles. It can be stripped down to its core for an even more secure and better-performing workhorse.

Datacenter Edition

This is Microsoft's "heavy-duty" virtualization server version. This is best used in highly virtualized environments because it sports unlimited virtual instance rights. That's right, I said unlimited! This is really the only difference between Datacenter and Standard, and of course this is reflected in the price; Datacenter costs about four times as much as Standard edition.

Foundation Edition

Foundation contains most core features found in the other editions, but there are some important limitations you should understand before you deploy it. Active Directory certificate service roles are limited to only certificate authorities. Here are some other limitations:

- The maximum number of users is 15.
- The maximum number of Server Message Block (SMB) connections is 30.
- The maximum number of Routing and Remote Access (RRAS) connections is 50.
- The maximum number of Internet Authentication Service (IAS) connections is 10.
- The maximum number of Remote Desktop Services (RDS) Gateway connections is 50.
- Only one CPU socket is allowed.
- It cannot host virtual machines or be used as a guest virtual machine.

Essentials Edition

This server is intended for very small companies with fewer than 25 users and 50 devices. This is a very cost-effective way to provide small business networking. Here are some but not all new features of Windows Server 2012 R2 Essentials:

- Improved client deployment
- Can be installed as virtual machine or on a server
- User group management
- Improved file history
- Includes BranchCache
- Uses the dashboard to manage mobile devices
- Includes System Restore

Desktop Changes

In Windows Server 2012, Microsoft removed the Start button from the lower left. In R2 the Start button has been put back so you can access your application menu. You can still hit the Windows key to access your menu if you've already gotten used to using it. If you're not familiar with where the Windows key is, it's to the left of the left Alt key on a standard keyboard. There is also a hotspot in the lower-right corner, which brings up a vertical menu bar. This dynamic menu contains these buttons: the Start menu, the Desktop settings, and Explorer search.

The new look and feel will take a bit of getting used to, but we think you will like the new UI changes. Server Manager has had a major overhaul also and grabs your attention with its colorful display warnings on the dashboard when a problem exists.

One user-requested feature that Server lacked was the ability to switch from the GUI version to Server Core. Often times requirements change that may require you to change over to Server Core. Previously you would have had to do a complete reinstall of Server Core. An administrator now has the ability to convert from the GUI version to Server Core and vice versa.

You can read more about this throughout the book starting in Chapter 2, "Installing and Upgrading to Windows Server 2012 R2."

Active Directory Changes

As you may know, Active Directory (AD) is in many ways the keystone piece of Windows networking, in other words, the central database of user and machine authentication data. Server 2012 R2 ADs include several useful new capabilities for Active Directory Certificate Services, Active Directory Rights Management Services, and Active Directory Domain Services. Collectively, the new features focus on deployment and manageability. The plan is to make it fast and easy to deploy Active Directory services and to have more flexibility accessing files while having better file security. Administration has also improved to make graphical and scripted management more consistent and user friendly.

You can read more about this in Chapter 7, "Active Directory in Windows Server 2012 R2."

Active Directory Domain Services Changes

Microsoft is always striving to make Active Directory Domain Services (AD DS) a more robust directory structure service. In the following sections we will explain what has been improved pertaining to Active Directory Domain Services.

Cloning Domain Controllers

Windows Server 2012 R2 gives you the ability to clone an existing domain controller to speed up deployment. Using the domain controller interface in Server Manager, you can promote a single virtual domain controller. You may then, within the same domain, deploy additional virtual domain controllers.

Cloning will reduce the number of repetitive steps in the deployment process. It will also let you deploy additional domain controllers configured and authorized by Active Directory. This is achieved by creating a copy of a virtual domain controller and then authorizing the source controller and running the appropriate Windows PowerShell cmdlets. Windows PowerShell will create a configuration file with promotion instructions. This file will contain Domain Name Server (DNS) information, name, IP address, and other pertinent information.

You can read more about this in Chapter 7.

Fine-Grained Password Policy Improvements

Active Directory does a lot of things besides just keeping a list of user account names and passwords, but if we had to choose the most important of its tasks, we think it'd be reasonable to say that protecting and maintaining passwords would be that task.

Prior to Windows Server 2008, the issue that we all faced was that everyone in the domain had to follow the same password rules. So, for example, the admin staff had to follow the same password rules as the sales team. Administrators should know how to protect their passwords better than salespeople. If not, you better find new administrators!

In Windows Server 2008, Microsoft introduced fine-grained password policies. This allows you to put separate password policies on separate groups. So now, the administrators can have their own policies and the salespeople can have their own.

In Windows Server 2012 R2, fine-grained password policies have been improved so that you now have the option to create and administer your password-settings objects (PSO) using the Active Directory Administrative Center. This new feature helps simplify your PSO management. Prior to Server 2012 R2, all PSOs had to be created using the Active Directory Schema Interface (ADSI Edit) tool.

You can read more about this in Chapter 7 also.

Active Directory Recycle Bin

We think the best way to explain the Active Directory Recycle Bin is to give you a real-world example and how this technology can save the day.

John is junior administrator for Wiley Books. It took him hours to add 20 new authors to Active Directory. Later when John was finished, he accidently deleted one of the company's Organizational Units (OU).

Wiley backs up all of their data on a nightly basis using Microsoft Windows Backup. Because of this, when restoring Active Directory, it is an all-or-nothing restore. Microsoft Windows

Backup does not give you the ability to restore just the OU. So now that we have to restore Active Directory, John would lose those hours of work because Active Directory's version would be from the previous night's tape backup. This is where the Active Directory Recycle Bin can help.

With Active Directory Recycle Bin, John can simply restore the OU without reverting to another location in time using backups.

Through the use of its new graphical user interface, administrators can now easily un-delete Active Directory objects without going through the tedious process that Windows Server 2008 offered. You can see it in action in Figure 1.1.

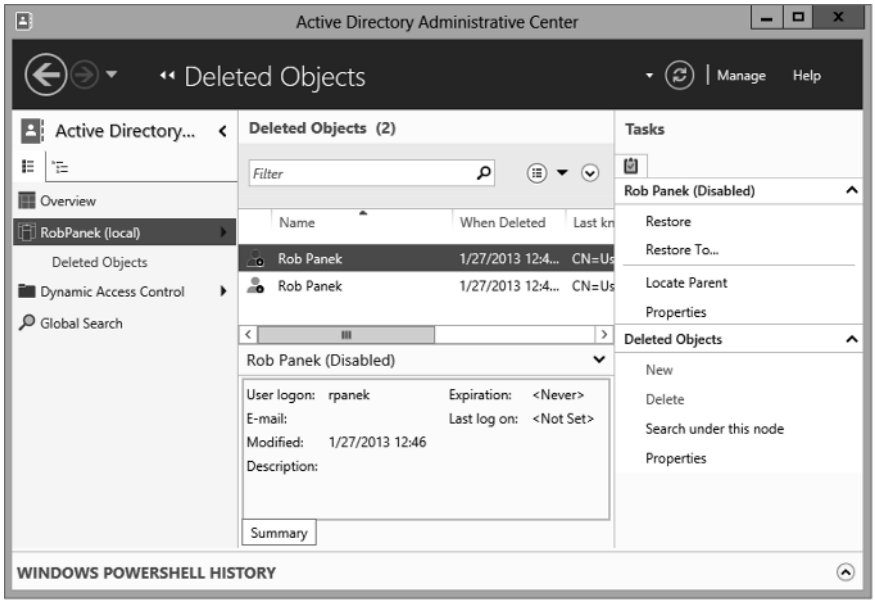

FIGURE 1.1 Sample Recycle Bin GUI

You can read more about Active Directory Recycle Bin in Chapter 7 as well.

PowerShell and AD Administrative Center

Ever since the advent of Windows, Microsoft has shipped operating systems whose administrative tools have, in the main, been graphically based tools; in fact, many Windows administrators can go weeks at a time without having to open a command line. That's good in that it means learning Windows administration is easier for new administrators than it would be for novices trying to learn Unix/Linux administration, because that latter group of operating systems is more heavily dependent on command-line administrative tools than GUI-based administrative tools.

What being command-line-centric does for the Unix/Linux world, however, is to make automating administrative tasks easier in Unix/Linux than it would be to automate many Windows administrative tasks. (You can put a command-line instruction into a batch file, which can then automate whatever task you're trying to accomplish. You can't put mouse clicks in a batch file.) So, Microsoft is trying to give Windows the "automate ability" that it lacks and that Unix and Linux have with a command shell called PowerShell. It's designed to let you take boring, repetitive tasks and automate them easily. Until now the learning curve to use PowerShell was quite steep.

Windows Server 2012 R2 introduces the PowerShell History Viewer, which allows administrators using Active Directory Administrative Center to view the Windows PowerShell commands that are executed. The PowerShell 3.0 improvements are as follows:

- Windows PowerShell workflow
- Windows PowerShell web access
- New Windows PowerShell ISE features
- Support for Microsoft .NET Framework 4.0
- Support for Windows' preinstallation environment
- Disconnected sessions
- Robust session connectivity
- Updatable help system
- Enhanced online help
- CIM integration
- Session configuration files
- Scheduled jobs and Task Scheduler integration
- Windows PowerShell language enhancements
- New core cmdlets
- Improvements to existing core cmdlets and providers
- Remote module import and discovery
- Enhanced tab completion
- Module autoloading
- Module experience improvements
- Simplified command discovery
- Improved logging, diagnostics, and Group Policy support
- Formatting and output improvements
- Enhanced console host experience

- New cmdlet and hosting APIs
- Performance improvements
- RunAs and shared host support
- Special character-handling improvements

As you can see by the long list of improvements, Microsoft intends to make PowerShell (see Figure 1.2) as important an administrative platform as the host of GUI tools that exist today.

You will read more about PowerShell throughout the entire book starting in Chapter 2, where you will use it to add roles and features.

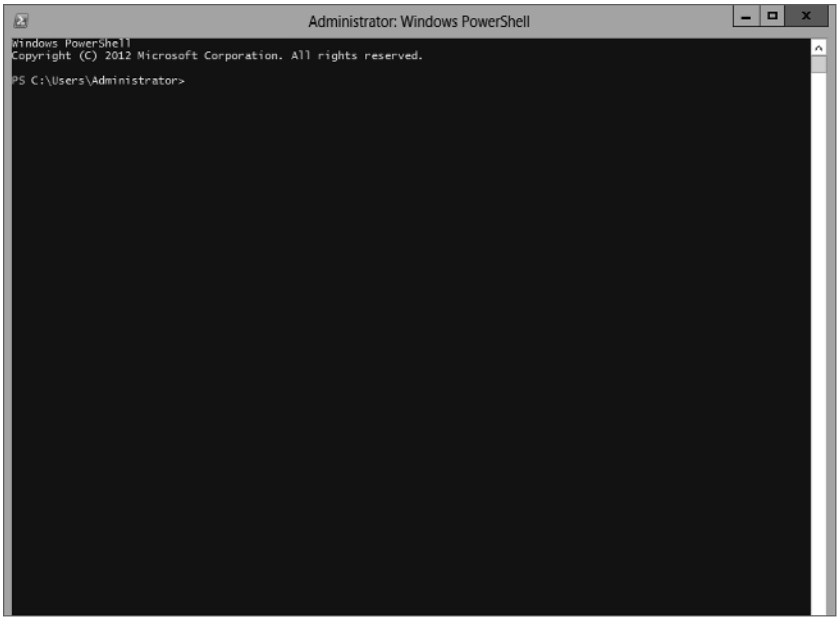

FIGURE 1.2 Using PowerShell to install a server role

Active Directory Rights Management Services

Passing secure documents and files within your company is vital to the company's information integrity. Your company's CFO, for example, may have a report listing the salaries of all the employees in the company. The CFO wants only other executives in the company to have access to the file. This is where Active Directory Rights Management Services (AD RMS) will be called on to secure the file. With AD RMS the CFO can encrypt or apply authentication to the file.

Prior to Windows Server 2012 R2, AD RMS setup required that only a user with local administrator privileges be allowed to install on the computer that hosted the SQL Server database. This was because AD RMS needed to read the SQL Server settings from the registry during installation. Microsoft implemented the following changes to deal with the AD RMS and how SQL Server is accessed:

- AD RMS now requires that the installer have sysadmin permissions in the SQL Server installation.
- The browser service for SQL Server must be running in order to locate any available SQL Server instances.
- Any ports used by AD RMS setup on the SQL Server computer should have Firewall exceptions enabled. You will need to enable TCP port (default port 1433) for the SQL instance and the UDP port (default port 1434) for the SQL Server Browser Service.

Another piece of AD RMS setup was upgraded. In previous server versions you would have to deploy from the computer where AD RMS was installed. In Windows Server 2012 R2 you are allowed to remotely deploy at targeted server computers.

You can read more about AD RMS starting in Chapter 7.

Active Directory Certificate Services

You can bind the identity of services, devices, and people to a private key using Active Directory Certificate Services (AD CS). This enhanced security feature allows access only to participating applications that support AD CS.

Listed here are some of the changes affecting Windows Server 2012 R2:

- Server Manager integration.
- Deployment and management using Windows PowerShell.
- AD CS role services can be run on Server Core on any version of Windows Server 2012 R2.
- Automatic certificate renewal is now supported for joined computers not in a domain.
- Certificate renewal with same key is enforced.
- International domain name support.
- CA role service has increased security enabled by default.

You can read more about AD CS starting in Chapter 7.

Virtualization

Virtualization allows you to put multiple computer operating systems on one physical machine. In the past, you would have used four servers for your domain controller, Exchange Server, DNS server, and DHCP server. Now you can have one physical box and four virtual servers. This saves money (on hardware) and also saves space (four servers before/one server now). Virtualization in Windows Server 2012 R2 is continuing to improve.

Hyper-V

Server virtualization—breaking one physical server up into a bunch of *virtual machines*—is one of the most significant changes in server management in the past 10 years. We wrote "server management" in lowercase because it's used not just in Windows Server but in various flavors of Linux, Unix, Sun Solaris, and so on. Being able to buy one big, powerful, reliable piece of hardware and fool it into believing that it's actually 10 or 20 smaller separate pieces of computer hardware and then installing separate server OSes on those bits of "virtual server hardware"

has greatly simplified server management for operations big and small. Furthermore, it has solved a server management problem that has bedeviled server room planners for years: underutilized hardware. The tool that fools the computer into thinking that it is actually many separate computers is generically called a *virtual machine manager* (VMM).

You see, ever since the start of server computing, most organizations have preferred to put each server function—email, AD domain controller, file server, web server, database server—on its own separate physical server. Thus, if you needed a domain controller, a web server, and an email server for your domain, you would commonly buy three separate server computers, put a copy of Windows Server on each one, and make one a DC, one a web server (by enabling Internet Information Services, R2's built-in web server software, on the server), and one an Exchange Server. The downside of this was that each of those servers would probably run at fairly low load levels: it wouldn't be surprising to learn that the DC ran about 5 percent of the CPU's maximum capacity, the web server a bit more, and the email server a bit more than that. Running a bunch of pieces of physical server hardware below their capacity meant wasting electricity, and that's just not green thinking, y'know? In contrast, buying one big physical server and using a VMM to chop it up into (for example) three virtual servers would probably lead to a physical server that's working near capacity, saving electricity and cooling needs.

First, let's cover the new technology added in this version. Since there are so many improvements to Hyper-V, we're just going briefly touch on each one:

- Client Hyper-V gives desktop Windows Hyper-V technology without the need for installing a server OS.
- A Hyper-V module for Windows PowerShell provides more than 160 cmdlets to manage Hyper-V.
- Hyper-V Replica allows you to replicate virtual machines between storage systems, clusters, and datacenters in two sites. This helps provide business continuity and disaster recovery.
- Resource metering helps track and collect data about network usage and resources on specific virtual machines.
- Simplified authentication groups administrators as a local security group. By doing so, fewer users need to be created to access Hyper-V.
- Single-root I/O virtualization (SR-IOV) is a new feature that allows you to assign a network adapter directly to a virtual machine.
- Storage migration allows you to move the virtual hard disks to a different physical storage while a virtual machine is running.
- SMB 3.0 file share is a new feature that provides virtual machines with shared storage, without the use of a storage area network (SAN).
- The virtual Fibre Channel allows you to virtualize workloads and applications that require direct access to Fibre Channel-based storage. It also makes it possible to configure clustering directly within the guest operating system (sometimes referred to as guest clustering).
- Virtual Non-Uniform Memory Architecture (NUMA) allows certain high-performance applications running in the virtual machine to use NUMA topology to help optimize performance.

Now let's briefly talk about some of the enhancements made to existing Hyper-V technology that many administrators will find useful.

- Dynamic memory allows you to configure Smart Paging so your virtual machines can more efficiently restart. If a virtual machine has less startup memory, dynamic memory can be configured to support it.
- Importing virtual machines has received a tune-up to better handle configuration problems that would normally prevent an import. Until now the process included copying a virtual machine but never checked for configuration issues.
- Live migrations make it possible to complete a live migration in a nonclustered environment. This improvement will make moving a live virtual machine easier.
- Larger storage resources, increased scale, and better hardware error-handling are offered in this version. The intention is to help you configure large, high-performance virtual machines with the ability to scale.
- Virtual Hard Disk Format (VHDX) increases the maximum storage size of each virtual hard disk. The new format supports up to 64 terabytes of storage. It also comes with built-in hardware protection against power failures. This format will also prevent performance falloff on large-sector physical disks.
- You no longer need to shut down the live virtual machine to recover deleted storage space. Virtual machine snapshots will now free up the space the snapshot consumed once it is deleted.

You can read more about this in Chapter 27, "Virtualization with Hyper-V."

Removed or Deprecated Items in Windows Server 2012 R2

VM Chimney, also referred to as TCP offload, has been removed and will no longer be available to guest operating systems. The WMI root\virtualization namespace is changed to just root\virtualization\v2 and will eventually be taken out completely in future Server versions. Authorization Manager (AzMan) has also been deprecated in this version and will be phased out in future releases. The new management tools for virtual machines will be the new standard.

Virtual Desktop Infrastructure

In Windows Server 2012 R2, Microsoft has made vast improvements to the virtual desktop infrastructure (VDI), with simpler administration, increased value, and better overall user experience.

Supporting mobile devices is a must in today's market. Virtual desktop infrastructure helps bridge the compatibility gap between devices by virtualizing resources. VDI provides stronger security and higher efficiency that improves productivity with a UI that the user is familiar with. Windows Server 2012 R2 and VDI make it a snap to deploy virtual resources across devices.

Windows Server 2012 R2 VDI, if running in a datacenter, will allow access for mobile devices using Hyper-V and Remote Desktop Services. Microsoft offers three different deployment types in a single solution: pooled desktops, personal desktops, and remote desktop sessions.

You can read more about VDI in Chapter 27.

Networking Changes

Servers are no good without the ability to talk to one another, but—of course—the downside of being able to communicate with other systems means that *infected* systems can try to spread their malware joy. ("Want to secure your server? Easy...disconnect the Ethernet cable!") Server 2012 R2 offers some networking changes to make Windows networking a bit faster and a bit more secure.

EAP-TTLS

With Windows Server 2012 R2 an exclusive protocol is being introduced as an Extensible Authentication Protocol (EAP) type called Tunneled Transport Layer Security (TTLS). This protocol is used with 802.1X Authenticated Wired and Wireless access. This new standards-based protocol provides a secure tunnel for client authentication. 802.1X provides a security shield that prevents unauthorized access to your intranet.

DNS

Although DNS has been around forever, the process by which it translates names seems to get better with each version. Changes in Windows Server 2012 R2 affect both DNS Server and Client. Let's take a look at the changes for Windows Server 2012 R2.

In PowerShell, DNS management has received some improvements. The DNS Server role, for example, has had some improvements to installation and removal using PowerShell. Additional developments in PowerShell include user interface, client query, and server configuration on older operating systems. The LLMNR query time-out has been 300 msec, which was not enough time for computers in power save mode. With the new improvements to DNS Client, this time-out has been increased to 820 msec.

IP Address Management

The IP Address Management (IPAM) framework is a new set of technologies for managing, monitoring, and auditing IP address space. By monitoring DHCP and DNS, IPAM can locate IP address servers within your network and allows you to manage them from a single central UI.

NIC Teaming

NIC Teaming technology in Windows Server 2012 R2 can take multiple network interface cards and team them together to interface as one. Doing so helps with failover should one device become inoperative. Load balancing is also improved when NICs are teamed because the bandwidth is combined into a single larger bandwidth.

You can read more about these topics and new features in Chapter 4, "Windows Server 2012 R2 Networking Enhancements," and Chapter 5, "IP Address Management and DHCP Failover."

Management Tools

Any good networking operating system should offer ways to simplify the job of keeping one server or one thousand servers up and running. The server should also stay up and running with the smallest amount of effort possible on the part of the humans doing the server administration. No one operating system has *the* answer for server administration, but Windows Server has gotten a bit better in 2012 R2 with some useful new tools.

Server Manager

Prior to Windows Server 2008, when an administrator had to configure and maintain a server, the administrator would have to use *many* different tools. Windows Server 2008 changed all that by introducing Server Manager, a one-stop shop for all of your configuration and management tools.

In Windows Server 2012 R2 (Figure 1.3), Microsoft has expanded this functionality even further. Server Manager now lets administrators manage multiple servers (virtual or physical/local or remote) as long as they are no older than Windows Server 2003.

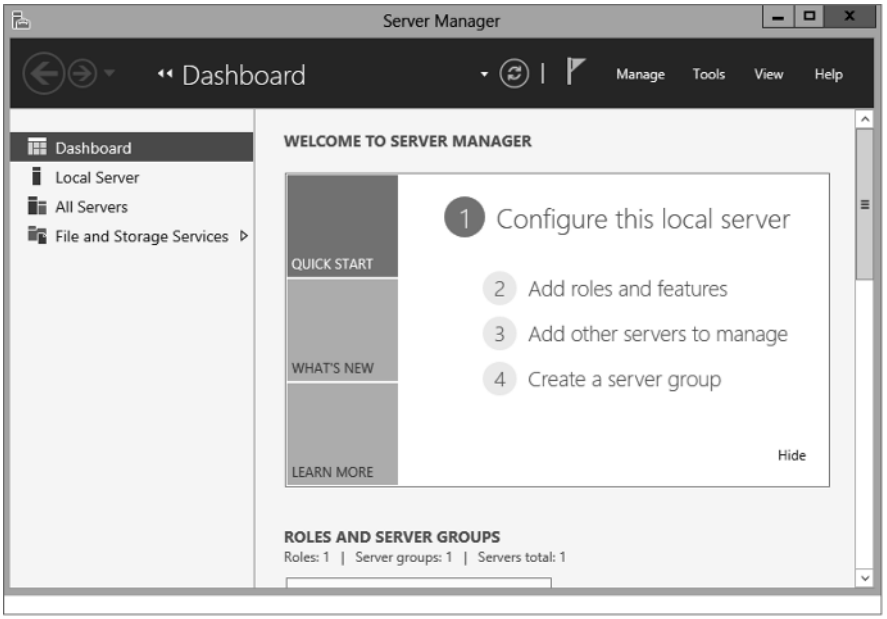

FIGURE 1.3 Server Manager

Adding roles and features in Server Manager has gotten even smarter. As you make your selections, the Add Roles and Features Wizard dynamically changes. The wizard assists you in deciding which subset of tools and features are needed for the requested role.

Server Manager has a new dashboard that can show you if problems exist using color-coded boxes. If, for example, an error occurred from within the DNS event log, the DNS box on the dashboard would turn red. This is an excellent tool for troubleshooting your server, and since the dashboard is the first thing you see when you log in, you can't miss it.

Speaking of troubleshooting your server, Server Manager has a host of new troubleshooting tools that we will show you more about in Chapter 2. These tools are all inside the role, inside Server Manager, so you do not have to open multiple applications like Event Viewer or Performance Analyzer to see the results—they're all in one spot!

You can read more about Server Manager in Chapter 2.

The Remote Tools: WinRM and WinRS

It's the case all too often that new operating systems include some really important and useful features that go largely unnoticed. Windows Server 2012 R2 contains one of those neat but largely unknown features in a new network protocol called Windows Remote Management (WinRM). To understand why WinRM is a great feature, let's consider what WinRM is intended to replace: a protocol known as the Remote Procedure Call (RPC).

Even if you've never heard of RPC, chances are that you've been using it for years. RPC's job is to allow one program to talk to another program, even if those programs are running on different computers. For example, if you've ever started up Outlook to read your email on an Exchange Server instance, then you've used RPC: it's how Outlook can tap Exchange on the shoulder and say, "Can I have my email, please?" Or if you've ever used an MMC snap-in like DNS, DHCP, or Computer Management to remotely control those functions on a remote computer from your desktop, you've used RPC.

RPC is a protocol that has provided much service over the years, but it has one big problem: it's hard to secure. Microsoft invented RPC back in the days when there was no Internet, and the vast majority of LANs extended no farther than the distance from the first floor to the top floor in an office building, so security wasn't all that big a concern. Years later, when security became a big concern, Microsoft tried to retrofit security onto RPC with some optional changes wrought first by XP SP2, but by that point the horse was out of the barn, and requiring RPC security would just end up breaking hundreds or perhaps thousands of RPC-dependent applications.

Clearly, the time had come for a change in how Windows programs talk to each other, so Microsoft decided to adopt a protocol that did the same sort of thing that RPC did, with a few changes:

- It's not proprietary but is standards-based and platform-independent—there are similar implementations popping up on Linux and Mac OS.
- It's a modified form of HTTPS.
- Its communications are encrypted.
- It requires authentication to use.

Components of Windows 2012 R2 that use WinRM include event log collection; the ability to use the new Server Manager snap-in on remote servers; and my personal favorite, a secure remote command shell called Windows Remote Shell, or `winrs`. If you need a secure, low-bandwidth remote-control tool, look to `winrs`. Read more about WinRM in Chapter 17, "Remote Server Administration."

Remote Desktop Services

In Windows Server 2012 R2 Microsoft has made large strides in improving the user and management experience. Microsoft intended to improve the user experience regardless of the

kind of device being used to connect. They wanted to make sure connecting through a WAN or LAN (to virtual desktops, RemoteApp programs, or session-based desktops) provides a rich experience to the user. Microsoft also wanted to make the remote desktop management experience better. We agree that they did make it better by adding a centralized console so administrators can manage Remote Desktop Services from a single location.

You can read more about Remote Desktop Services in Chapter 17.

Group Policy Object Improvements

What got better? Plenty. Managing Group Policy objects (GPOs) got easier with the built-in Group Policy Management Console. In previous Windows versions, one problem that administrators had was manually forcing a GPO to update. Even though GPOs automatically update every 90 minutes, there are times when you need a GPO to take effect immediately. Administrators had to remote in to the specific computer and run `gpupdate.exe` from the command line to manually update a GPO.

Now if an administrator wants to manually force a GPO update, the administrator can use the context menu for an OU in the Group Policy Management Console and schedule `gpupdate.exe` to run on multiple computers at the same time. Administrators can also achieve this by using the PowerShell utility and the new `Invoke-GPUpdate` cmdlet.

Here are some additional changes to Group Policy in Windows Server 2012 R2:

- When dealing with monitoring replication issues at the domain level, you no longer need to download and run separate tools.
- For devices running Windows RT, you can now configure local Group Policy. By default it is disabled, and the service must be started and set to automatic.
- Group Policy has been upgraded to support Internet Explorer 10.

You can read more about Group Policy in Chapter 9, "Group Policy: AD's Gauntlet and Active Directory Delegation."

File and Print Sharing

Back before we ran web or email services on our Windows servers, we only used Server to share two things: big hard drives and expensive printers. File and print are the oldest services offered by Microsoft networks, but apparently they're not too old to learn a few new tricks.

BranchCache

BranchCache is a technology that optimizes WAN bandwidth by copying content from either your main location or cloud server to your branch office. Once content is copied to the branch, users can access it locally rather than over the WAN. Having the ability to cache files will conserve bandwidth and improve security. BranchCache can support any size office and is not limited to how many it can service. BranchCache can be deployed with just a single Group Policy object (GPO). This technology uses the Windows file server to divide files into small encrypted pieces. The cool thing about dividing the files into smaller pieces is that client computers can download only the pieces that changed. BranchCache will also check for duplicate content and only download one instance of the content, saving disk space.

In Windows Server 2012 R2, BranchCache improvements include automatic client computer configuration and big performance and scalability increases. Client computers can be configured through the use of a Group Policy object. If a GPO has not been configured for BranchCache, then BranchCache will check the hosted cache server and use those settings by default.

One of the new advantages of BranchCache is the ability to preload specific content, like media and DVDs, on a hosted cached server and then have that content sent to the client cache.

Another very nice advantage is the improvements that have been made to allow for better database performance. BranchCache has done this by using the Extensible Storage Engine (ESE). This is the same database technology used by Microsoft Exchange Server. It allows scaling of a single hosted cache server to handle the increased demands of more people without having to increase hardware.

Hosted cache servers no longer need a server certificate issued by a certificate authority (CA). This will greatly reduce costs involved with deploying a public key with multiple CAs.

SMB 3.0

Windows' file server service bears the official name of SMB, which stands unhelpfully for Server Message Block. (Blame IBM, not Microsoft, because an IBM guy first designed it.) SMB has changed little over its roughly 25 years of life, with its biggest changes being support of somewhat bigger block sizes so as to be able to make use of networks faster than 100 Mbps (appeared in 2000), the ability to handle multiple paths, and the addition of digital signatures so as to foil man-in-the-middle attacks (appeared in 2001).

Windows Server 2012 R2 sports a somewhat reworked version of SMB that handles slow networks better, handles encryption more intelligently, cranks up throughput on file transfers, and supports PowerShell.

File Server Resource Manager

You can manage data stored on a file server using the tools in File Server Resource Manager. Some of the tools included help you to automate classification and reporting and manage files and quotas.

With Dynamic Access Control's File Classification Infrastructure you can control and audit access to files on the file server. You can now get more control on how your files are classified on your file servers. With the enhanced features, classifying files can be done manually or automatically.

You can read more about this topic starting in Chapter 13, "Files, Folders, and Basic Shares."

Web-based Services

Finally, there's the subset of the Internet that's become more important than all the rest of the Net put together: the Web and related services. They're important to Windows, and they saw some big changes in 2012 R2.

Web Server IIS

Windows' file services may not have changed much over the years, but that's not the case for Windows' *web* server. One key to hardening any server product is to keep the amount of

code exposed to the Internet to a bare minimum; if a web server can support, for example, something called FastCGI but your website doesn't *need* FastCGI, then why run FastCGI on an Internet-facing server and risk the possibility that someone discovers a way to use IIS's FastCGI to hack the server? Clearly you wouldn't, so it'd be nice to just strip your web server software of the things that you aren't going to need. (Security folks call this "minimizing the attack surface." Sometimes we think they play too much *Halo*.)

The perfect web server, then, would be composed of dozens of small modules, each of which could be removed or added as needed to allow the web administrator to build a web server that did exactly what she needed it to do...but no more. That was the guiding light for Windows Server 2008's IIS 7.0, a complete overhaul of IIS including some of the latest security technologies, including WinRM. (When you're doing remote administration of an IIS 7 box, you're using that protocol rather than RPC.)

Hacking IIS 7.0

No one has hacked IIS 7 yet to my knowledge, nor have they taken down IIS 7.5, which is the update shipped with Windows Server 2008 R2. Web admins also liked the cleaner, task-oriented interface of 7.x's IIS administration tools.

Knowing how companies live and breathe on the Internet in today's market, we would expect no less from Microsoft than for it to wave its technology wand across the web server. With the release of Windows Server 2012 R2 comes the newest version of the web server, IIS 8.0 (Figure 1.4). IIS 8.0 has also received a wealth of new rich features to administer and secure your website. Here are a few important changes made in IIS 8.0:

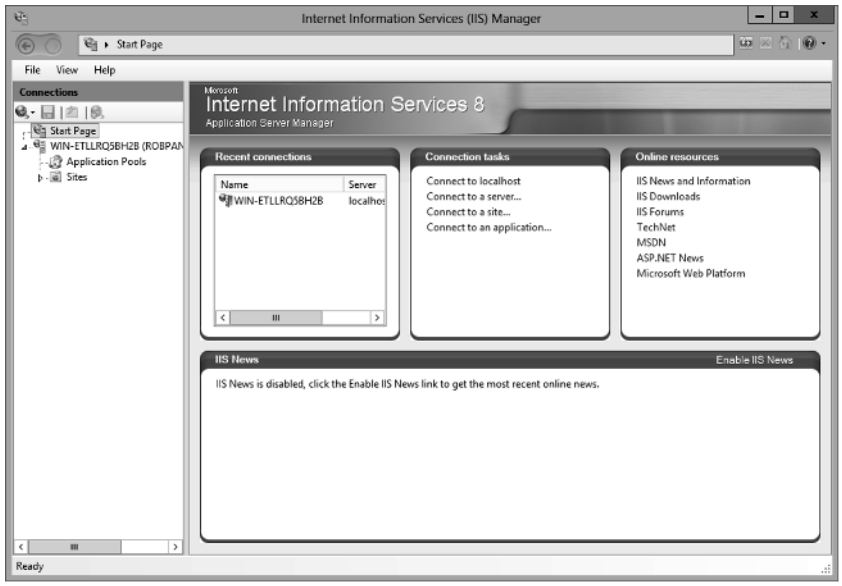

Figure 1.4 IIS's new management tool

- Application initialization
- Dynamic IP address restrictions
- Centralized SSL Certificate Support
- CPU throttling
- FTP logon attempt restrictions
- Server Name Indication (SNI) support
- Improved SSL and configuration scalability
- Support for multicore scaling on NUMA hardware

Even if you're not a webslinger by trade, it's never a bad idea to understand the current Windows web server—so don't skip Chapter 19, "Web Server Management with IIS."

Microsoft Management Console Gets the Ax!

In Windows Server 2012 R2 the Microsoft Management Console (MMC) snap-in is deprecated for Internet Information Services (IIS) Manager 6.0. In future releases of Windows Server, this will be removed.

FTP Server

Microsoft gets some things right and some things wrong. In a few cases, the company gets things terribly wrong, as was the case with the built-in File Transfer Protocol (FTP) server software that shipped with Windows for the past 15 years or so. It was so clunky, was so difficult to configure, and offered such minimally useful logs and an inability to configure things that *should* have been childishly easy to configure (such as user home directories) that just about everyone who needed a Windows FTP server ended up shelling out a few bucks for a third-party FTP server. Starting with Windows Server 2008 and R2, however, things changed considerably. As far as we can see, Microsoft tossed out all the FTP server code and rebuilt it from scratch. In Windows Server 2012 R2, they also added the ability to restrict the number of failed logon attempts that can be made to an FTP account in a certain period. So if you need a Windows-based FTP server, flip over to the IIS chapter (Chapter 19) to learn about the new changes to the FTP server.

You can read more about web server management in Chapter 19.