Tom Carpenter

Exam 98-365

Microsoft®

Windows Server® Administration ESSENTIALS

SYBEX SERIOUS SKILLS.

Introduction

Servers are important tools used on modern networks. They provide email support, file and print services, application functionality, and so much more. Server administrators are in high demand, and modern technologies such as virtualization and cloud computing have only increased the importance of the server administrator's job.

The Microsoft Technology Associate (MTA) certification is a certification provided for entry-level professionals and those with long careers in the industry who have never acquired a certification credential. It includes three separate tracks: Information Technology (IT) Professional, Developer, and Database. The IT Professional track is for individuals pursuing work as administrators. The Developer track is for individuals pursuing work as programmers and software engineers. The Database track is for individuals pursuing work as database administrators and database developers.

The IT Professional series includes three certifications:

Windows Server Administration Fundamentals This certification assumes no previous knowledge of Windows Server Administration and allows you to start from the beginning to learn how to administer Windows servers. The knowledge acquired through the Networking Fundamentals and Security Fundamentals certification programs will be helpful as you study Windows Server administration fundamentals, but it is important to remember that the MTA certification exams have no prerequisites. The Windows Server Administration Fundamentals exam and this book give you a solid foundation for working as a

server administrator in a Microsoft technology environment. You earn this certification by taking and passing exam 98-365. This book covers the objectives for the 98-365 exam.

Networking Fundamentals This is an important certification in the MTA IT Professional track. It provides the knowledge that lays a solid foundation of basic networking knowledge needed to administer modern networks and also helps you prepare for more advanced Microsoft Certified Technology Specialist (MCTS) and Microsoft Certified IT Professional (MCITP) tracks. You earn this certification by taking and passing exam 98-366.

Security Fundamentals Security Fundamentals is the another important certification in the MTA IT Professional track. It complements the knowledge learned in the Networking Fundamentals certification process and adds fundamental security knowledge needed by administrators. IT administrators in any environment need to be aware of the risks with IT systems. You earn this certification by taking and passing exam 98-367.

Each of these certifications can serve as a stepping-stone to Microsoft's next levels of certifications: Microsoft Certified Technology Specialist (MCTS) and Microsoft Certified IT Professional (MCITP).

Who Should Read This Book

This book is for current or aspiring professionals seeking a quick grounding in the fundamentals of administration in a Microsoft Windows Server environment. The goal is to provide quick, focused coverage of fundamental skills.

If you want to start a career in server administration or are already working in the field and want to fill in some gaps on fundamental topics, this book is for you. You can use the

knowledge gained from this book as a foundation for more advanced studies. Additionally, this book will act as an excellent reference for the day-to-day tasks you must perform as a Windows Server administrator.

This book is focused on the objectives of the Microsoft Technology Associates (MTA) Server Administration Fundamentals certification. This is the first numbered certification in the MTA IT Professional series (exam number 98-365), but you can take the three IT Professional series exams in any order you desire. You can read more about the MTA certifications and MTA exam certification paths at: www.microsoft.com/learning/en/us/certification/mta.aspx.

What You Will Learn

You will learn the essentials of server administration in a Microsoft environment. In addition, this book covers all the objectives of the Microsoft Technology Associates Windows Server Administration Fundamentals exam (exam 98-365).

What You Need

In order to perform the procedures provided throughout this book, you will need a Windows server. This server can be a virtual machine or a direct installation on computer hardware. The good news is that Windows Server 2008 R2 will run on practically any desktop computer that will run Windows 7. You can install the trial edition of Windows Server 2008 R2 and use it for up to 180 days. The trial edition can be downloaded from: http://www.microsoft.com/windowsserver2008/en/us/trial-software.aspx.

If you want to run Windows Server 2008 R2 in a virtual machine on top of Windows 7, you will need to have at least 4 GB of system memory in your Windows 7 computer, and

you will need to download the free VMware Player virtualization software. This software can run 64-bit operating systems, unlike Windows Virtual PC that Microsoft provides for Windows 7. You can download the VMware Player from this location: http://www.vmware.com/go/downloadplayer. Chapter 2, "Installing Windows Servers," provides instructions for performing an installation of Windows Server 2008 R2.

What Is Covered in This Book?

Microsoft Windows Server Administration Essentials is organized to provide you with the information you need to master the basics of administration in a Microsoft server environment.

Chapter 1: Windows Server Overview This chapter provides an overview of the Windows Server operating system and servers in general. It contrasts servers with clients and explains the benefits that servers provide. The concept of the server role is explained and the different server types are briefly discussed.

Chapter 2: Installing Windows Servers Chapter 2 explains the options you have for Windows Server installation and discusses the important considerations that must be made when upgrading servers. Server Core is introduced as well, and the concept of working with device drivers is also explained.

Chapter 3: Managing Windows Server Storage After installing Windows Server, you will need to configure the storage locations for file servers, application servers, and more. This chapter introduces data storage concepts and the technologies used for storage. You will also learn about fault tolerant storage through the use of RAID arrays and learn to identify storage technologies.

Chapter 4: Administering Services Chapter 4 defines the concept of a service and the important roles services play on modern networks. You will explore service configuration and management procedures. The chapter concludes with an explanation of service problem troubleshooting procedures.

Chapter 5: Active Directory Infrastructure Active Directory is Microsoft's directory service solution. This chapter introduces you to Active Directory concepts including the Domain Name System (DNS), sites, and replication. You will learn the information required to plan an Active Directory installation in this chapter.

Chapter 6: Configuring Active Directory While Chapter 5 introduces the concepts of Active Directory, this chapter steps you through the process of installing Active Directory from start-to-finish.

Chapter 7: Managing Active Directory Now that Active Directory is up and running, you will learn to manage it in this chapter. You will explore both the graphical user interface tools and the command-line tools available for Active Directory administration and management.

Chapter 8: Group Policy Management Group Policy is used to centrally configure, manage, secure, and control your Windows computers that participate in an Active Directory domain. This chapter introduces the concepts of Group Policy and provides you with instructions for creating and managing policy settings.

Chapter 9: Application Servers Application servers are implemented to support the applications that run on your network. This chapter introduces you to application servers in general and then explores specific server types, including database servers, mail servers, collaboration

servers, monitoring servers, and threat-management servers.

Chapter 10: Internet Information Services (IIS) Internet Information Servers (IIS) is the web server provided with Windows Server and even the Windows client operating systems. This chapter introduces you to the IIS components and management processes.

Chapter 11: File and Print Servers File and print servers are among the oldest server types. This chapter covers file and share permissions and the proper implementation procedures for printer sharing.

Chapter 12: Remote Access Technologies You cannot always go to a computer or server to manage it. This chapter introduces you to remote management tools that are available for administering Windows servers; it also addresses security through the use of virtual private networks (VPNs).

Chapter 13: Server Troubleshooting Troubleshooting skills are important for a Windows server administrator, and this chapter provides an essential overview of these skills. You will learn about troubleshooting methodologies and specific tools you can use in the troubleshooting process.

Chapter 14: Performance Tuning This chapter introduces you to performance analysis topics and then explores the different performance analysis tools in Windows Server. These tools include the Performance Monitor, the Resource Monitor, and the Task Manager.

Chapter 15: Server Maintenance In this final chapter, you will learn about important tasks and tools that help you maintain a stable server implementation. You will learn how to maintain hardware, plan for server downtime, use

Windows Update, automate using logs and alerts, and plan for business continuity.

Appendix A: Answers to Review Questions This appendix includes all of the answers to the review questions found in "The Essentials and Beyond" section at the end of every chapter.

Appendix B: Microsoft's Certification Program This appendix highlights the Microsoft certification program, and it lists the exam objectives for Exam 98-365 and how they map to this book's content.

In addition, we have created an online Glossary, the suggested or recommended answers to the additional exercises we have included at the end of each chapter, as well as additional exercises for instructors. You can download these at: www.sybex.com/go/winadminessentials.

Sybex strives to keep you supplied with the latest tools and information you need for your work. Please check their website at: www.sybex.com/go/winadminessentials, where we'll post additional content and updates that supplement this book if the need arises. Enter server administration essentials in the Search box (or type the book's ISBN: 978-1-118-01686-2), and click Go to get to the book's update page.

As the author, I would be glad to help you in your learning process. If you ever have questions along the way, feel free to email me at carpenter@sysedco.com. Thanks for reading.

CHAPTER 1
Windows Server Overview

Servers play a vital role on modern business computing networks. They provide such important services as e-mail, file storage, collaboration, and security. This chapter introduces you to servers in general and Microsoft Windows Server in specific. You will learn about the differences between servers and clients and the different designs of today's server hardware. Next, you will learn about the different roles servers play on modern computing networks and why these roles are important. Finally, you will explore the specifics of Windows Server. You will learn about the different interfaces it provides, networking features it offers, management features it supports, and the different editions of the product that are available. The following topics will provide coverage of this information:

- Introducing Servers
- Understanding Server Roles
- Microsoft Windows Server Features

Introducing Servers

If you want to understand Windows servers, you must begin by understanding servers in general. In this section, you will learn what servers are, how they differ from clients, and the various shapes and sizes in which they are manufactured. I will begin by defining what a server is so that you can keep this definition in mind as you read through the rest of this book.

Understanding Server Concepts

Computer networks are used to provide communications between computing devices. The computing devices include network infrastructure hardware devices, such as routers, switches, and firewalls. They also include clients and servers. Servers are used to provide services to the networked devices.

Servers must be connected to a network so that other devices (clients) can consume their services. These networks may include local area networks (LANs), wide area networks (WANs), and any other type of network on which the servers communicate. In the early days of computing, a server often sat on the other end of a telephone line allowing only one user to connect at a time. Even though this is not efficient, it still represents a network being used to access a server. The telephone line created the network connection between the client and the server.

> A *modem* is a modulator and demodulator that uses the telephone network to carry digital data as analog signals.

The services provided by a server include three primary categories of service:

Network Services Network services include any service that exists to provide network functionality. For example, the Dynamic Host Configuration Protocol (DHCP) is used to provide Internet Protocol (IP) configuration settings that allow client devices to communicate on the network. Another example is the Domain Name System (DNS) server service, which resolves Internet-like domain names to IP addresses. These Internet-like names are called *hostnames.*

DNS names look like *mypc.domain.name* or *yourpc.domain.name*. The leftmost portion is the host name and the rest is the domain name. Together they form a *fully qualified domain name* (FQDN).

Security Services Security services include those services that provide authentication, authorization, confidentiality, or some form of protection to the network and networked devices. An example of a security service is the Active Directory Domain Service (AD DS), which could also be partially categorized as a network service. AD DS provides the user accounts that are used to log on to Windows Server-based networks. When these accounts are used for logon processes, authentication is performed and authentication is a security service. An additional security service is the IPSec Policy Service, which enforces security settings for Internet Protocol (IP)-based communications.

Because they provide more than one type of service, some services can be placed in multiple categories of service.

Information Services Information services include any service that provides information access, information management, or information processing. For example, the Microsoft SQL Server service provides database access and database management. This functionality qualifies SQL Server as an information service. Microsoft SharePoint is another example of an information service. It provides for information storage and retrieval, as well as collaboration.

You will learn more about services in Chapter 4.

Understanding Client/Server Concepts

The term *client/server model* became very popular starting in the 1980s. The term simply indicates that an application is broken into two components: the *client* component—a computing device or application that consumes services—and the server component. Some of the processing is performed at the client and the rest is performed at the server. A modern example of this is a web-based application that depends on both the web server and the web browser (the client) to perform the required processing: The server retrieves and processes data that is then sent to the web browser. The browser reformats this data for the current screen resolution of the user's workstation. The point is that the two components work together.

> The first multiuser computer sharing method was developed by Fernando Corbató at Massachusetts Institute of Technology (MIT) in 1961.

It is not enough, however, to say that a server does part of the processing and the client does another part of the processing. In most client/server model systems, a single server can service many clients. You can define the relationship as a many-to-one relationship between the clients and the servers, as depicted in Figure 1.1: You can see that one file server provides file storage and retrieval services to multiple PC clients, a Mac client, and even a laptop computer. The clients are the many, and the server is the one in the many-to-one relationship.

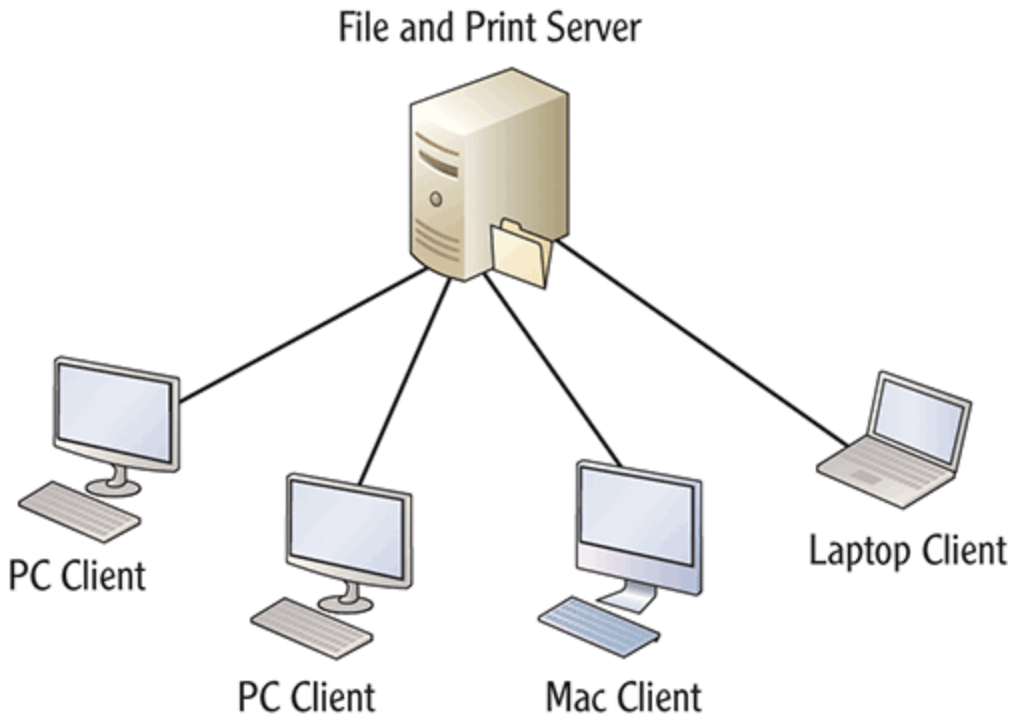

FIGURE 1.1 The many-to-one relationship of client/server computing

Additionally, the clients consume services from the network itself in that they utilize bandwidth made available by the network. *Bandwidth*, in this context, is defined as the maximum information that can be transmitted simultaneously across a communications channel. Each client consumes a portion of this bandwidth for network communications.

Table 1.1 provides a comparison of servers and clients.

TABLE 1.1 Comparing Servers and Clients

Typical Server Characteristics	Typical Client Characteristics
Used by many users	Used by one user at a time
Built from high-quality components	Built from average quality components
Optimized for background applications	Optimized for visual foreground applications
Provides services to the network	Consumes services from the network

In addition to the contrasting of servers and clients, you should understand the servers and clients available in the Microsoft product line. The following Microsoft server operating systems are still very popular today:

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2

The following Microsoft client operating systems are very popular:

- Windows XP
- Windows Vista
- Windows 7

Historically, Microsoft has released a new version of their client and server operating systems every two to four years. For example, Windows Vista was released in 2006 for business customers, although it wasn't released until January, 2007 for consumers. Windows 7 was released in

2009. Similarly, Windows Server 2003 was released in 2003 and Windows Server 2003 R2 was released in 2005.

Furthermore, a greater period exists between major version number releases of the operating systems. For example, Windows Vista was considered a major version number release that changed the major version number of the operating system from 5 to 6, whereas Windows 7, released very shortly thereafter, was considered an interim minor version release. To see this, access a Command Prompt on a Windows 7 system by clicking Start ➢ All Programs ➢ Accessories ➢ Command Prompt and then execute the `ver` command. You will see that it is version 6.1, as shown in Figure 1.2. Windows Vista was version 6.0.

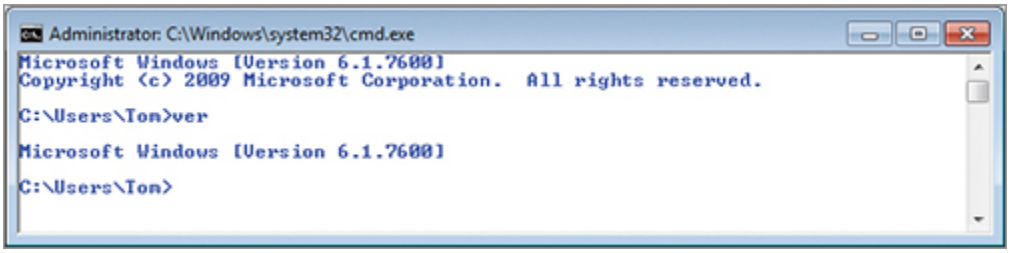

FIGURE 1.2 Viewing the version of Windows

The time between the release of Windows Vista and Windows 7 was approximately three years; however, the time between the release of Windows 2000 (a major version release at version 5.0) and Windows Vista (the next major version release) was six years. In most cases, the changes from a major version release to a minor version release are insignificant when compared to the changes made between major version releases, as is clearly seen when considering the minor differences between Windows 7 and Vista at the core operating system level and the major differences between Windows 2000 and Windows Vista. This is helpful to Information Technology (IT) professionals who must support these systems. In most cases, you will use the same or very similar operating system for a 4 to 6 year window of

time. Every 4 to 6 years, you should be prepared to learn many new things and unlearn many old things in relation to the operating systems you support.

> Many organizations plan upgrades for every other release. For example, they may have upgraded from Windows NT 4.0 to Windows XP, and their next upgrade will be to Windows 7, skipping Windows 2000 and Windows Vista.

Clients can also be used to perform server functions. We often call these clients *peer servers* because they are not intended primarily as a server. They are also sometimes called *logical servers* because the services they provide are logical services that run on the machine (just like a dedicated server). The main difference between a server that runs server services and a client that runs server services is that the server is dedicated to running those services and the client is typically not.

Understanding the Term “Logical”

In this context, the word “logical” simply means that the device is intended as one thing but it performs the logic of another. For example, a client computer is intended to be a workstation for a user; however, if it shares a folder onto the network, it is providing the same service as a file server. The logic of sharing is included in both operating systems, but it is implemented more frequently in server operating systems. The server operating system is optimized to provide file sharing functions and overcomes connection limits in client operating systems. Additionally, the server operating system offers advanced share management tools for quota management and file filtering, which is used to limit the file types that may be placed in the shares.

An example of a server service that may run on a client machine is file and printer sharing. You may have a printer connected to your Windows 7 machine that you want to make available to other users in your work area. You can do this, assuming it is allowed by network policies, using the Windows printer sharing capabilities. Technically, this makes your Windows 7 machine a print server, but we would not call the machine a server because it is still primarily used as a user’s workstation.

Logical Versus Dedicated Servers

If you browse around in the Services management tool on a Windows machine (accessed by clicking Start and typing **services.msc** into the Search field on a Windows Vista or later or Windows Server 2008 or later machine), you will notice that a service called Server exists. The existence of this service does not really classify the machine as a server in the traditional sense of the term. Technically, all network machines are servers in a logical sense, but they are not servers in a practical sense because they are not dedicated to server functions.

A Windows 7 machine may indeed respond to a network connection request and allow communications. Because the machine responded to a request and did not initiate the request, it is logically a server. However, we have traditionally considered a machine to be a server only when it is dedicated to server tasks. Therefore, a machine that sits in a special room and is rarely accessed at the console while being heavily accessed across the network is considered a server. But we would say it is impractical to consider a Windows 7 computer that is mostly used by a local user and rarely accessed as a logical server as a dedicated server.

While all of this might just seem like semantics, the reality is that we must clearly define servers versus clients so that we can plan our networks well. The placement of servers is very important because they are typically accessed by multiple users from multiple locations. The placement of desktop computing clients is typically fixed. We put them right in front of the users—at least, we do most of the time. This network location placement will impact security settings on routers and

switches related to the devices. For example, you will allow certain communications to pass through a switch port to a server that you would not allow to pass through to a client. Keep this in mind as you're planning your servers, clients, and networks.

Choosing Server Hardware

The actual computing device we call a server comes in several form factors. The *form factor* simply defines the design of the server's case and internal component access methods. For example, the case may be slim and provide limited component access or it may be large and bulky with easy component access. The form factor also dictates how the server may be installed or mounted in the environment.

> The form factor of a server is a reference to the design of the server's physical case and mounting methods.

Today, three major form factors exist and are available from many different vendors:

- Desktop
- Rack Mount
- Blade

The Desktop form factor looks just like a regular user's client computer. It may be slightly larger, but it will look much the same. The Desktop form factor includes those that stand upright (also known as a tower case) and those that lay horizontal (the traditional Desktop form factor). Figure 1.3 shows the IBM Power 780 desktop server. While it may appear a little fancier than a regular user's desktop

computer, it is essentially the same thing with extra monitoring features and higher quality components.

FIGURE 1.3 The IBM Power 780 Desktop form factor server

The rack mount servers are specially designed to mount in a rack cabinet. These cabinets typically have doors and are specially ventilated to provide cooling. Figure 1.4 shows the IBM Power 755 rack mount system. To make efficient use of space, you can mount more than one server in a

single rack cabinet. In many scenarios, you can also use a shared uninterruptible power supply (UPS) for all of the servers in the cabinet.

FIGURE 1.4 The IBM Power 755 Rack Mount form factor server

The final form factor is the server blade. In this case, the server is actually a removable blade that slides into a type of docking station used to house each blade. The docking station (called a BladeCenter by IBM, a Blade Enclosure by Dell, and by other names from other vendors) can house multiple blades. Because each blade is a server, you can store multiple servers in a single docking station. The blade docking station could be a desktop enclosure or it could mount in a rack cabinet, much like a rack server. Figure 1.5 shows the IBM BladeCenter PS701.

The form factor you choose will depend on the space in which it will be installed and the number of servers you require. For example, rack mount and blade servers are very popular when dozens or hundreds of servers are required. When only a few servers are required, the Desktop form factor is still quite common.

Understanding Server Roles

Now that you understand what a server is and how it differs from a client, it's important to grasp the concept of a *server role*. Much as you can play different roles in your life, the server can play different roles as well. In this section, you will first gain a clear understanding of what server roles are and then you will explore some common server roles.

FIGURE 1.5 The IBM BladeCenter PS701 Blade form factor server enclosure

A server role is defined as a collection of responsibilities provided to the network or networked devices by a specific server. A more detailed definition is that a server role is a set of software programs (services) that enable a server to perform specific functions for users or computers on the network. Servers are typically dedicated to a role, but in smaller organizations a server may play several roles at the same time. Server roles are based on role services and one or more role services is used to implement a given server

role. For example, the File Services role in Windows Server 2008 R2 includes the following role services:

> These role services are explained in detail in Chapter 11.

- Share and Storage Management
- Distributed File System (DFS)
- File Server Resource Manager (FSRM)
- Services for Network File System (NFS)
- Windows Search Service
- Windows Server 2003 File Services (for backward compatibility)
- BranchCache for network files

In addition to server roles, features may be added to a Windows server installation. A *feature* is much smaller than a role and may be defined as a software program that can support or add to the functionality of one or more server roles or the general functionality of the server. Features may require a server role be installed before they can be installed. As an example, the Windows Server Backup tools are installed as a feature on Windows Server 2008 R2. If you want to use the Windows Server Backup tools to schedule backups for your server's data, the feature must first be installed.

Deploying Applications on Your Network

The Application Server role, in Windows servers, provides an integrated environment for the deployment of custom business applications. The applications can be built using the Microsoft .NET Framework, which is a special software

framework for application development. The Application Server role provides the ability to run services and applications that are built on COM+, Message Queuing, Web Services and Distributed Transactions:

> A software framework is a collection or prebuilt code and other functions that can be used to quickly develop complex business applications.

COM+ COM+ allows for the remote invocation of applications. You can execute application code that is stored on remote servers rather than require that the code be installed on the local machine.

Message Queuing Message Queuing allows for asymmetric network communications, which means that a request can come into an application and be processed when the application has the available resources rather than requiring instant processing.

Web Services The Web Services allow your application to communicate using the Hypertext Transfer Protocol (HTTP) that is common to web-based communications.

Distributed Transactions The Distributed Transactions component allows for applications to complete transactions against multiple databases stored on multiple computers that participate in the network.

The Application Server role can be installed using the Server Manager on Windows Server 2008 and later. When you add the Application Server role, the following role services may be installed:

> You will learn more about the Application Server role in Chapter 9.

- Web Server (IIS)
- COM+ Network Access
- TCP Port Sharing
- Windows Process Activation Services Support
- Distributed Transactions

Providing Internet Access and Collaboration on Your Network

Web servers are some of the most common types of servers used on modern networks. Web servers are used to provide content to client computers and applications using HTTP for communications. HTTPS, which is the encrypted and secured version of HTTP, may also be used. Windows servers provide web server role functionality using the Internet Information Services (IIS) application and several other supporting services for authentication, logging, and application development.

With a web server, you can provide many different services to your users, including:

- Provide information to Internet users through your public website
- Allow for uploading and downloading of files through HTTP or FTP
- Host servers that contain business logic for multi-tier applications.
- Implement collaboration servers such as Microsoft SharePoint Server

Multi-tier applications are applications that reside on more than one machine and perform different processes or functions, such as display, data access, and data retrieval, on each machine.

Like any other role in Windows servers, you can add the Web Server role in the Server Manager. When you add the role, it is called the Web Server (IIS) role. Once installed, you can add components to the web server as needed. For example, you can add support for PHP as a programming language or you can add PERL support. Like most web servers, Microsoft's IIS is modular and extensible, allowing you to add features and components as needed. Additionally, a management tool called the IIS Manager is provided; it allows you to easily manage the web server using a GUI interface. The IIS Manager for IIS 7.5 running on Windows Server 2008 R2 is shown in Figure 1.6.

You will learn more about the Web Server (IIS) role in Chapter 10. You can also learn more at **www.iis.net/overview**.

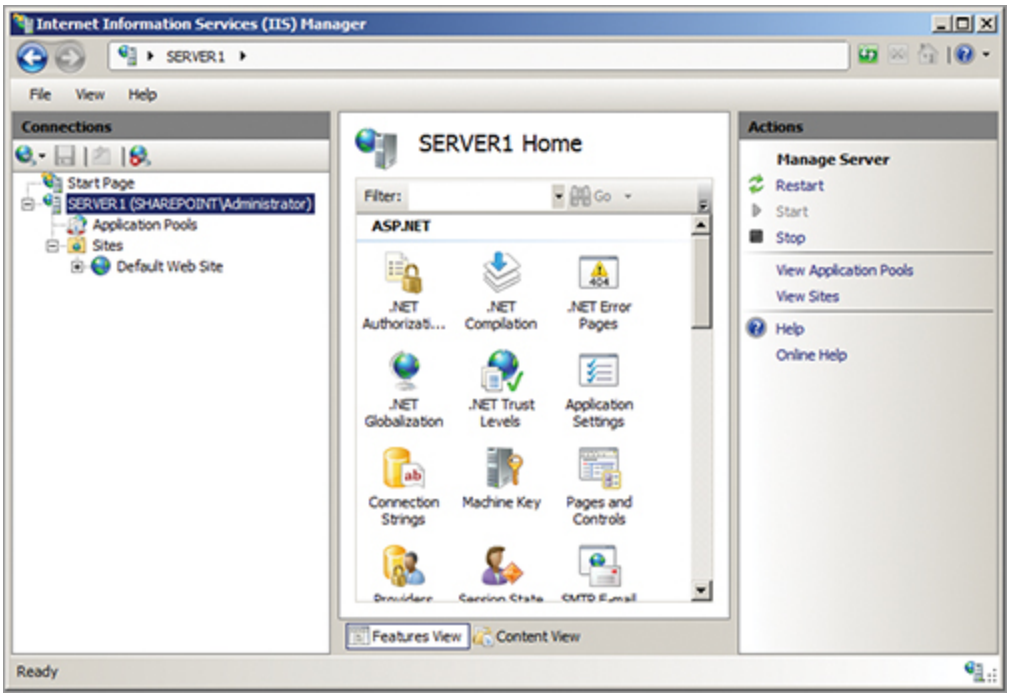

FIGURE 1.6 The IIS Manager used to manage the web server on Windows Server 2008 R2

Managing Files and Printers on Your Network

In the past, File and Print Services were referenced as a single role. In Windows Server 2008 R2 installations, the File Services role and the Print and Document Services role are now separate.

The File Services role provides features such as share management, storage management, file replication, and search services. Additionally, a collection of tools called the File Server Resource Manager (FSRM) provide simplified management of quotas, file screening (restricting the file types allowed on the server), storage reports generation, file management tasks (such as searching for files on the server), and management of remote storage resources.

The Print and Document Services role allows you to share printers and scanners on the network. You can centralize both printer and scanner management through this role.

Management tools called the Print Management console and Scan Management console are provided for centralized management. Additionally, you can install the management tools on Windows 7 clients so that administrators can run them remotely from the client computers.

> You will learn more about the File Services role and the Print and Document Services role in Chapter 11.

Providing Network Access for Remote Users

In earlier versions of Windows servers, the remote access capabilities are easier to locate because they were simpler. You installed Routing and Remote Access Services (RRAS), and you had a remote access server. In Windows Server 2008 and later, RRAS is part of the Network Policy and Access Services role. This role provides several functions to your network:

Network Access Protection (NAP) NAP provides a client health policy service to your network. NAP ensures that a connecting client meets a minimum set of requirements before allowing the client to communicate on the network. For example, it may require that the client have antivirus software installed and updated or that specific security updates have been applied to the operating system.

When a client is not incompliance with the NAP requirements, the client may be denied access to the network or granted restricted access. The restricted access option is typically used to allow the client to download antivirus updates or other updates that will allow it to come into compliance with the NAP policies.

IEEE 802.1X Authentication The IEEE developed an authentication mechanism that is used to ensure that devices are authenticated before they are allowed to

communicate on a network. This mechanism is known as 802.1X authentication. When a device first connects to the network, it is allowed to communicate only with an authentication server. Once authenticated, it is permitted to communicate with the rest of the network.

> The IEEE is the Institute of Electrical and Electronics Engineers, and they are responsible for many of the standards used on modern computer networks.

RADIUS Server The Remote Authentication Dial-In User Service (RADIUS) was originally developed to authenticate users dialing in on modem lines. Today, it is used for authentication of Virtual Private Network (VPN) traffic and wireless clients, as well as wired clients that authenticate using 802.1X authentication. The Microsoft RADIUS server component is included in the Network Policy and Access Services role.

> A VPN is a secured and encrypted link between two computers. It allows for secure communications across public networks.

Routing and Remote Access Services (RRAS) RRAS provides for both VPN server functionality and dial-up access to your network. As a VPN server, it allows client computers to connect across the Internet, or another network, and establish secured and encrypted communications. As a dial-up server, it allows client computers to connect using a modem, which is a communications device that allows network connections to be established across traditional telephone lines.

You will learn more about the Network Policy and Access Services role in Chapter 12.

Adding More Roles as Needed

Windows servers can support several additional roles. In addition to the roles mentioned in the preceding sections, the following roles are also supported:

Active Directory Certificate Services This role provides certificates for users and computers to use in authentication and encryption processes.

Active Directory Domain Services This role provides the Active Directory services to the network, which include user and group provisioning as well as computer and server management.

Active Directory Federation Services This role allows for two different authentication realms to share credentials so that users can use single sign-on procedures and not be required to sign on individually to each network.

Active Directory Lightweight Directory Services This role enables a minimal version of the Active Directory services for application use. It is used when Active Directory is not your primary network directory service.

Active Directory Rights Management Services This role is used to control access to and distribution of digital assets, such as documents and media. The assets are signed and secured so that only authorized users can access them.

You will learn more about the Active Directory role in Chapters 5, 6, and 7.