MCSE EXAM MATERIAL

▶ Professional
▶ Server
▶ Network

EXAM OBJECTIVES

Professional ▶

Exam 70-210

- Manage and troubleshoot Web server resources.

Server ▶

Exam 70-215

- Monitor, configure, troubleshoot, and control access to files and folders via Web services.
- Monitor, configure, troubleshoot, and control access to Web sites.

Network ▶

Exam 70-216

- Install and configure Certificate Authority (CA).
- Create certificates.
- Issue certificates.
- Revoke certificates.
- Remove the Encrypting File System (EFS) recovery keys.

CHAPTER

18

Managing Web and Certificate Services

This chapter focuses on several Windows 2000 Internet-related services. I'll begin by exploring Internet Information Services (IIS), Windows 2000's Web server service. In addition to showing you how to install the various components of IIS, I'll explain how to configure a Web site and how to publish Web content by using virtual directories and virtual servers. Because security is an ever-increasing concern for today's networks, I'll spell out several things you can do to increase Web server security. Finally, I'll explore how to monitor Web site access and how to troubleshoot Web services.

Next, I'll introduce you to the Indexing Service, a great feature of Windows 2000 that makes it possible for users to locate certain types of files by a word, phrase, or property of the document, such as the author's name.

The last half of this chapter is devoted to Certificate Services. I'll explain how to install this service on your Windows 2000 Server computer, and then how to use it to issue and manage certificates. I'll also show you how to revoke certificates, and how to manage Encrypting File System (EFS) recovery agents.

Chapter Pre-Test

1. List three commonly used components of Internet Information Services (IIS).
2. Which component of IIS provides Web server functionality to a Windows 2000 computer?
3. What is Personal Web Manager?
4. What is a virtual directory?
5. What is a virtual server?
6. List three things you can do to increase security of a Windows 2000 Web server.
7. The __________ __________ is a Windows 2000 service that indexes Web site content and other documents on a Windows 2000 computer so these items can be searched by users.
8. What is Certificate Services?
9. What term is used to refer to an organization that uses a computer to create, issue, and manage certificates, and is also used to refer to the actual server that performs the task of issuing and managing certificates?

Managing Web Services

In Windows 2000, *Web services* is an umbrella term that encompasses several Internet-related services that enable users to publish on and communicate over the Internet. With Web services, you can host Web sites, FTP sites, and newsgroups. In Windows 2000, Web services is synonymous with *Internet Information Services (IIS)*.

IIS is Windows 2000's Web server. IIS is actually a collection of several services. Some of the most commonly used components of IIS are:

- **World Wide Web Server:** This service enables a Windows 2000 computer to host one or more Web sites and function as a Web server.
- **File Transfer Protocol (FTP) Server:** This service enables a Windows 2000 computer to host FTP sites. Client computers can use these FTP sites to upload and download files.
- **FrontPage 2000 Server Extensions:** This service enables users of client computers that run Microsoft FrontPage to publish and manage Web sites on the Windows 2000 computer that has FrontPage 2000 Server Extensions installed.
- **SMTP Service:** SMTP stands for Simple Mail Transfer Protocol. This service enables a Windows 2000 computer to function as an outgoing mail server. The SMTP Service makes it possible for Web site clients to send e-mail messages directly from a Web site hosted by the Windows 2000 computer.
- **NNTP Service (Server only):** NNTP stands for Network News Transport Protocol. This service enables a Windows 2000 Server computer to host Internet newsgroups.

IIS 5.0 is an integral part of Windows 2000 Professional, Windows 2000 Server, and Windows 2000 Advanced Server. However, there are a few differences in IIS as it is implemented in Windows 2000 Professional. In Windows 2000 Professional, IIS is limited to a maximum of ten connections (versus unlimited connections in the Windows 2000 Server/Advanced Server implementations). In addition, Internet Services Manager (HTML) and the NNTP Service are not available on Windows 2000 Professional computers.

Windows 2000 Professional has one exclusive IIS component that Windows 2000 Server and Advanced Server don't have — Personal Web

Manager. This application is a simplified administrative tool that enables a novice user to manage and monitor a Web site on a Windows 2000 Professional computer.

IIS requires the use of TCP/IP, which is installed by default during the installation of Windows 2000 Professional, Windows 2000 Server, and Windows 2000 Advanced Server.

Installing IIS Components

Some, but not all, IIS components are installed by default during the installation of Windows 2000. If you chose not to install IIS during your installation of Windows 2000, or if you need additional IIS components, you can use the Add/Remove Programs application in Control Panel to install IIS components.

STEP BY STEP

ADDING IIS COMPONENTS

1. Select Start ➪ Settings ➪ Control Panel.
2. In the Control Panel dialog box, double-click Add/Remove Programs.
3. In the Add/Remove Programs dialog box, click Add/Remove Windows Components.
4. In the Windows Components Wizard dialog box, highlight Internet Information Services (IIS), and click Details.
5. The Internet Information Services (IIS) dialog box appears, as shown in Figure 18-1. Notice that the check box next to many IIS components is already selected — these components are already installed. The actual components installed on your Windows 2000 computer may differ from the ones shown in this figure.

   Select the check box next to each IIS component you want to add. Clear the check box next to any IIS component you want to remove. Click OK.
6. In the Windows Components Wizard dialog box, click Next.
7. If prompted, insert your Windows 2000 compact disc into your computer's CD-ROM drive and click OK. Close the Microsoft Windows 2000 CD dialog box. Windows 2000 configures components and installs the selected IIS components. In the Completing the Windows Components Wizard screen, click Finish.
8. Close Add/Remove Programs. Then close Control Panel.

STEP BY STEP *Continued*

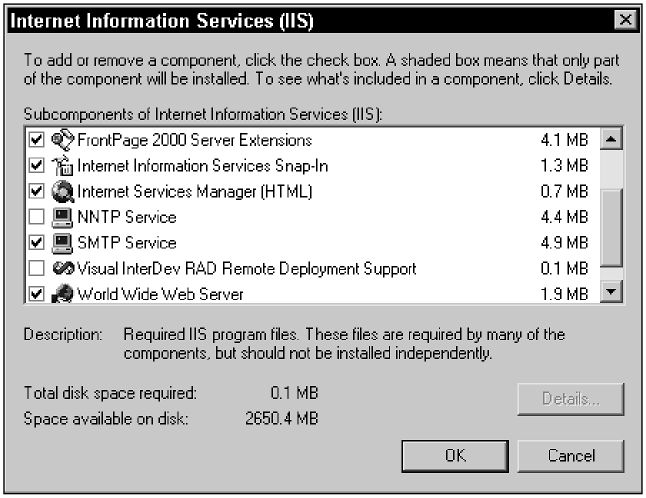

FIGURE 18-1 Selecting IIS components to install

Configuring a Web Site

Once the World Wide Web Server component of IIS is installed on your Windows 2000 computer, that computer functions as a Web server. When the World Wide Web Server is installed, it creates a Default Web Site on the Windows 2000 computer.

The Default Web Site is basically empty when it's first created. It does have a help file, which is configured to be the default home page, and some subfolders designed to support FrontPage 2000 Server Extensions. The contents of the Default Web Site are located, by default, in the `C:\Inetpub\wwwroot` folder on the Windows 2000 computer.

You can manage and configure the Default Web Site and any other Web sites on your computer by using the Internet Services Manager administrative tool. Internet Services Manager is an MMC console like many of the other administrative tools in Windows 2000. You can use this tool to manage IIS on the local computer, or you can connect to another computer on your network to manage IIS remotely.

In the steps that follow, I'll show you the basics of configuring the Default Web Site. You can also use these same steps to configure any other Web site on your Windows 2000 Web server.

STEP BY STEP

CONFIGURING THE DEFAULT WEB SITE

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Internet Services Manager.
2. In the left pane of the Internet Information Services dialog box, click the + next to the server that contains the Web site you want to configure. Right-click Default Web Site, and select Properties from the menu that appears.
3. The Default Web Site Properties dialog box appears, as shown in Figure 18-2. Notice the Description text box. You can change the name of the Default Web Site by typing in a new name in this text box.

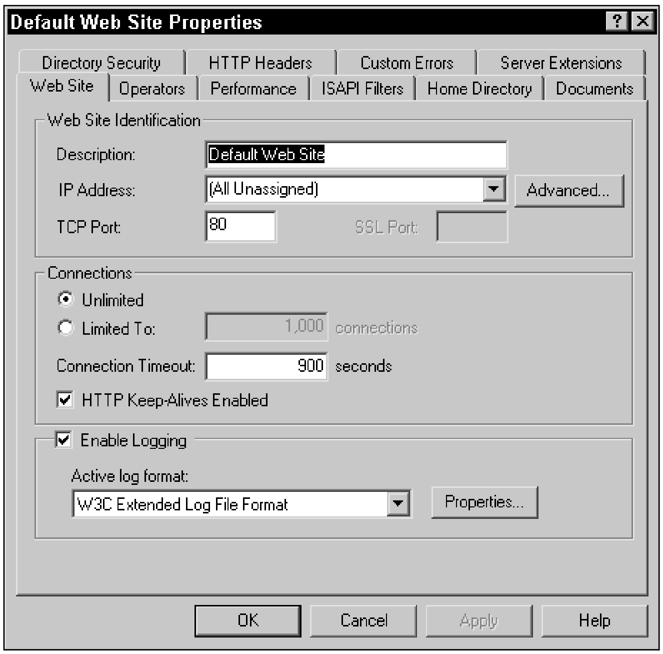

FIGURE 18-2 Configuring the Default Web Site

Configure the settings on the various tabs to meet your needs. (I'll discuss each of these tabs in the rest of this section.) Click OK.

4. Close the Internet Information Services dialog box.

There are numerous tabs in a Web site's Properties dialog box. On the Web Site tab, which is shown in Figure 18-2, you can assign one of the computer's IP addresses to this Web site. You can also configure the TCP port number that will be used by Web clients to access this Web site. The default port number of 80 is used for most Web sites. You can also configure connection limits and connection time-outs on this tab. Windows 2000 Professional computers have a maximum limit of ten connections. You can also enable logging and select a log file format on this tab.

On the Operators tab, you can specify which user accounts in the domain can manage this Web site. This tab is not available on Windows 2000 Professional computers.

On the Performance tab, you can configure three performance options for your Windows 2000 Web server. Figure 18-3 shows the Performance tab.

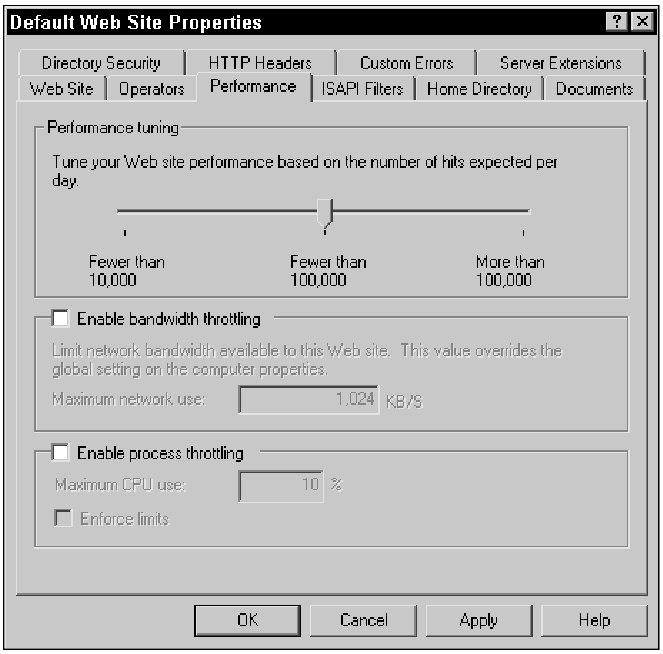

FIGURE 18-3 Configuring performance options

Use the Performance tuning slider to tune the performance of your Web server, based on the number of anticipated hits the site will receive each day. This slider configures the amount of the computer's RAM that is reserved for this Web site. If you want to prevent your Web server from using all of the available bandwidth on its network segment, select the check box next to "Enable bandwidth throttling" and specify the maximum amount of bandwidth you want the Web server to use, in kilobytes per second. Finally, if you want to limit the amount of processor time used by this Web site, you can select the "Enable process throttling" check box and specify a maximum percentage of CPU usage. You must also select the check box next to "Enforce limits," or the CPU limitation you specified won't be enforced—Windows 2000 will simply write an event to the Event log when the limit is exceeded.

On the ISAPI Filters tab, you can add and order ISAPI filters for the Web site. An ISAPI filter is a custom Web server application that extends the capabilities of a Web server.

On the Home Directory tab, you can manage and configure the home folder for this Web site. Figure 18-4 shows the Home Directory tab. Notice the path in the Local Path text box. This path specifies the location of the Web site's home folder. By default, for the Default Web Site, this is `C:\Inetpub\wwwroot`.

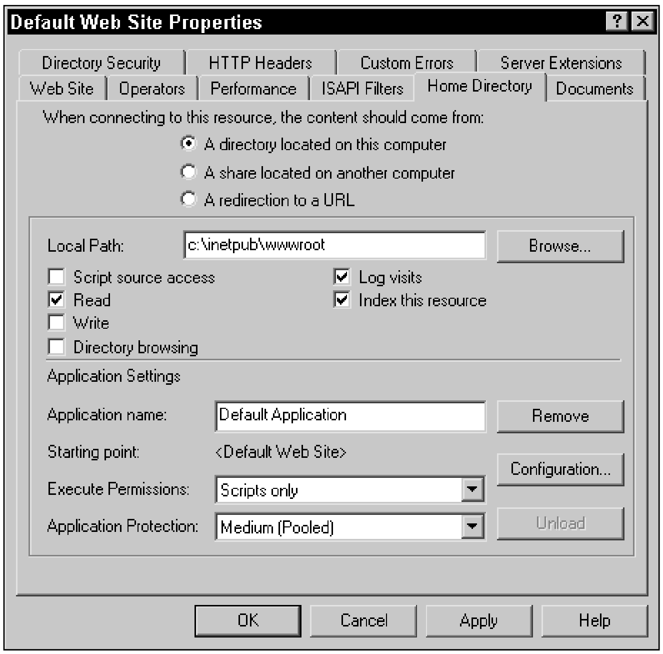

FIGURE 18-4 Configuring home directory options

On this tab you can configure the location of the home directory. The home directory for the Web site can be either a folder located on this computer or a shared folder or URL on another computer. You can also specify Web permissions and application settings for the home directory.

On the Documents tab, you can specify which document will be displayed as the Web site's home page to Web clients. Figure 18-5 shows the Documents tab.

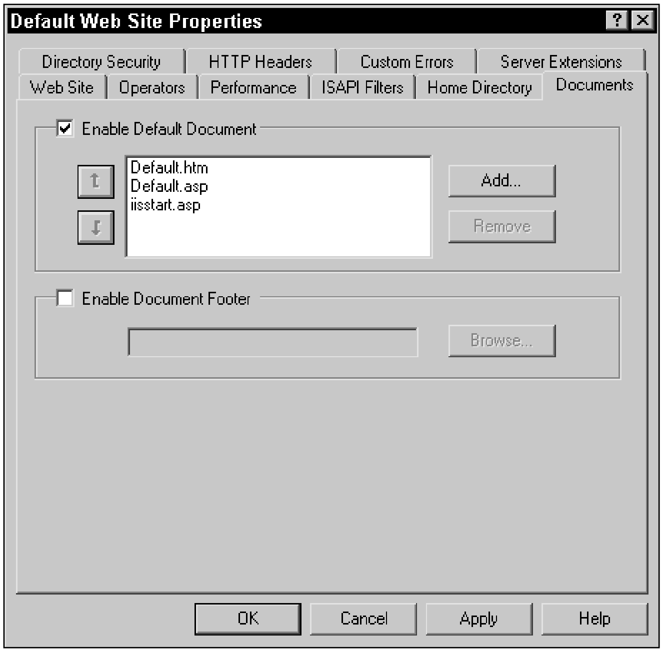

FIGURE 18-5 Configuring the default document

Notice that you can add and remove documents, and configure the order of documents on this tab. The document at the top of the list becomes the default document. If the check box next to "Enable Default Document" is not selected, Web clients will have to specify the name of the document they want to access in the URL they type in their browser—if they don't specify a document, an error message is displayed.

On the Directory Security tab, you can configure anonymous access and authentication methods. You can also configure IP address and domain name restrictions. Finally, you can assign a certificate to the Web site, and configure secure, encrypted communications between the Web server and Web clients. I'll discuss this tab in greater detail in the "Managing Web Server Security" section later in this chapter.

On the HTTP Headers tab, you can configure content expiration settings, custom HTTP headers, and content ratings for the Web site. An HTTP header is a value that is appended to all responses from the Web server to the Web client. Content ratings are used to identify the level of violence, sex, nudity, and offensive language in the Web site's content. These levels range from 0 (least offensive) to 4 (most offensive) for each category. If you don't assign content ratings to your Web site, Web clients who have configured content ratings in their Web browsers won't be able to access your Web site.

On the Custom Errors tab, you can specify a custom HTML document that will be displayed to Web clients when the associated HTTP error occurs on your Web server. Instead of using the default documents supplied by Microsoft, you can associate a custom document (that perhaps has a better explanation of the error) with a specific HTTP error number. For most situations, the default documents are adequate.

The Server Extensions tab is not operational until you configure your Windows 2000 Web server to use FrontPage Server Extensions. To accomplish this task, in the left pane of the Internet Information Services dialog box, right-click the Default Web Site and select All Tasks ➪ Configure Server Extensions. Then complete the Server Extensions Configuration wizard. Once the server is configured to use FrontPage Server Extensions, you can use the Server Extensions tab to configure Web content authoring options and security settings.

Using Personal Web Manager

Personal Web Manager is an easy-to-use Windows 2000 Professional tool that enables a novice user to manage and monitor a Web site on the local Windows 2000 Professional computer. Personal Web Manager enables you to stop and start the Default Web Site, view connection statistics, and manage Web site properties.

Personal Web Manager is an administrative tool. You can access it from the `Administrative Tools` folder in Control Panel, or from the Administrative Tools menu if you have configured the Administrative Tools menu to be displayed in the Start Menu.

STEP BY STEP

WORKING WITH PERSONAL WEB MANAGER

1. On your Windows 2000 Professional computer, select Start ➪ Settings ➪ Control Panel.
2. In Control Panel, double-click the `Administrative Tools` folder.

STEP BY STEP *Continued*

3. In the `Administrative Tools` folder, double-click Personal Web Manager.
4. When the "Tip of the day" appears, click Close. The Personal Web Manager main dialog box is displayed, as shown in Figure 18-6. Notice the statistics displayed in the Monitoring section of this dialog box.

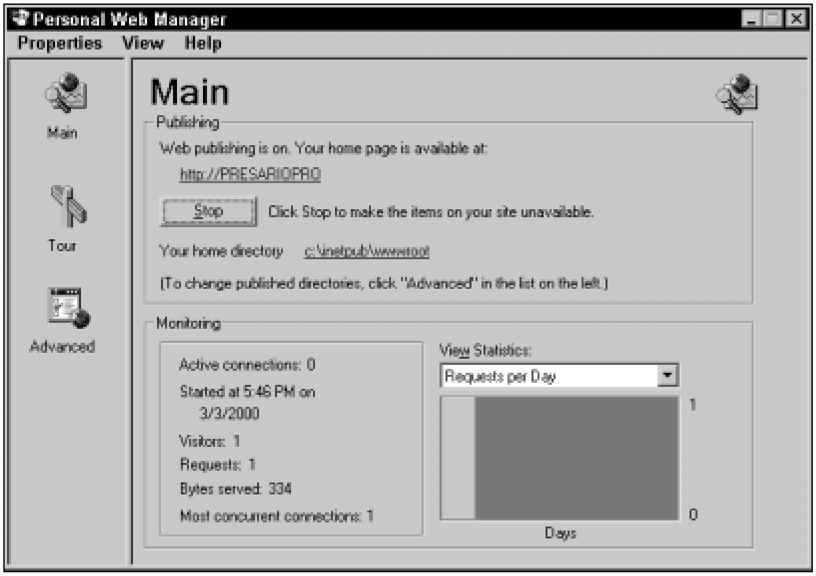

FIGURE 18-6 Personal Web Manager

To stop the Default Web Site, click Stop.

To view a product tour of IIS, click Tour.

To manage advanced Web site properties, such as enabling and configuring the default document, configuring access and application permissions, and creating virtual directories, click Advanced.

5. Close Personal Web Manager.

Publishing Web Content

At this point, you may be anxious to start publishing Web content on your Windows 2000 Web server. You might want to begin by using a Web page development tool to create your Web server's home page. Once you've created your home page, you'll need to copy the home page (which consists of an HTML file that should be named `Default.htm`, and any supporting graphics files) to the `C:\Inetpub\wwwroot` folder on your Windows 2000 Web server.

Anyone on your network (and, if your network is connected to the Internet, any Internet user) can access the home page by typing `http://` *`FQDN_of_your_Windows_2000_Web_server`* in their browser. For example, if your Windows 2000 Web server is named WWW and is located in a domain called domain1.mcse, you would type `http://www.domain1.mcse` in Internet Explorer to access your Web server's home page.

There are basically three ways to publish additional Web content on your Windows 2000 Web server:

- You can publish additional Web pages in the home folder of your Default Web site. To do this, copy the additional Web pages into this Web site's home folder.
- You can create a virtual directory and place Web pages in the folder to which the virtual directory points. A virtual directory is accessed by Web clients as though it were a subfolder of your Default Web site or another Web site on the Web server.
- You can create a virtual server and place Web pages in the virtual server's home folder. A virtual server appears to Web clients as a separate server with its own FQDN, although it exists on the same computer as the Default Web Site. You can only create virtual servers on Windows 2000 Server and Advanced Server computers.

In the next two sections, I'll show you how to create a virtual directory and a virtual server.

Creating a Virtual Directory

A *virtual directory* is a child Web site that doesn't contain Web content. Rather, it is a pointer to an actual folder that contains its Web content. A virtual directory is created on a Windows 2000 Web server. The folder containing the Web content can be located either on the Windows 2000 Web server or on any other computer on the network that is a member of the domain to which the Web server belongs.

The primary purpose of virtual directories is to organize the content of a large Web site into manageable-sized chunks, in much the same way you would use folders to organize the contents of a volume.

Web clients access a virtual directory as though it were a subfolder of a Web site. For example, the `Windows2000` virtual directory in the `www.microsoft.com` Web site is accessed as `www.microsoft.com/windows2000`. A virtual directory can be a child of a Web site or a child of another virtual directory on the Web server.

There is one drawback to using virtual directories: if the folder that contains the Web content is stored on computer *other* than the Windows 2000 Web server, network traffic is increased because the content must cross the network twice — once from the remote computer to the Web server, and again from the Web server to the Web client that requested the document.

There are two different ways you can create a virtual directory. You can use Internet Services Manager (or Personal Web Manager) to create a virtual directory on the Web server. You can also use Windows Explorer (on the Windows 2000 Web server) to designate a folder on a local drive as a virtual directory for one of the Web sites on this computer.

STEP BY STEP

USING INTERNET SERVICES MANAGER TO CREATE A VIRTUAL DIRECTORY

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Internet Services Manager.
2. In the left pane of the Internet Information Services dialog box, click the + next to the server that contains the Web site in which you want to create a virtual directory. Right-click the Web site, and select New ➪ Virtual Directory.
3. The Virtual Directory Creation wizard starts. Click Next.
4. In the Virtual Directory Alias screen, type in the user-friendly name that Web clients will use to access this virtual directory. Click Next.
5. In the Web Site Content Directory screen, either enter the local path to the folder that contains the Web content for this virtual directory, or enter a UNC path to the shared folder on another server that contains the Web content for this virtual directory. You can browse for this folder if you need to. Click Next.
6. The Access Permissions screen appears, as shown in Figure 18-7. Notice the permissions listed in this dialog box.

   Select the appropriateaccess permissions for the virtual directory. The selected permissions are granted to all users who access the virtual directory. The “Read” and “Run scripts” check boxes are selected by default. Click Next.

STEP BY STEP *Continued*

FIGURE 18-7 Setting access permissions for the virtual directory

7. In the "You have successfully completed the Virtual Directory Creation Wizard" screen, click Finish.
8. Internet Services Manager creates the virtual directory and displays it in the left pane of the Internet Information Services dialog box under the Web site in which you created it.
9. If you want to configure the properties of the virtual directory, right-click the virtual directory and select Properties from the menu that appears. Configuring a virtual directory is similar to configuring a Web site.
10. Close the Internet Information Services dialog box.

STEP BY STEP

USING WINDOWS EXPLORER TO CREATE A VIRTUAL DIRECTORY

1. On the Windows 2000 Web server, right-click My Computer, and select Explore from the menu that appears.
2. In the left pane, click the + next to the local drive that contains the folder you want to designate as a virtual directory. Expand folders until the folder you want to designate is displayed in the left pane. Right-click this folder, and select Properties from the menu that appears.
3. In the folder's Properties dialog box, click the Web Sharing tab.

STEP BY STEP *Continued*

4. On the Web Sharing tab, select the Web site on the local computer that will contain the virtual directory from the "Share on" drop-down list box. Then select the "Share this folder" option.
5. In the Edit Alias dialog box, enter the user-friendly name that Web clients will use to access this virtual directory in the Alias text box. Then select the appropriate access permissions for the virtual directory. The selected permissions are granted to all users who access the virtual directory. Click OK.
6. In the folder's Properties dialog box, click OK.
7. Windows 2000 creates the virtual directory. Close Windows Explorer. (If you want to configure the properties of the virtual directory, use Internet Services Manager to do so.)

Creating a Virtual Server

A *virtual server* is a pseudo WWW server with its own unique fully qualified domain name (FQDN), and often its own IP address. In Microsoft documentation, a virtual server is also called a Web site. To the Internet user accessing the virtual server, a virtual server appears to be a separate server; but in reality, a virtual server is *not* a separate server, but more like a shared folder on the Windows 2000 Server Web server that is accessed by specifying a different FQDN. A Windows 2000 Server Web server can be configured to accommodate multiple virtual servers. Each virtual server is assigned a separate home folder.

For example, an ISP could use one Windows 2000 Server Web Server to host virtual servers for several customers. Each customer could have its own FQDN for its Web site, such as `www.company_a.com`, `www.company_b.com`, `www.company_c.com`, and so on. To Internet users accessing these Web sites, each FQDN appears to be located on a different server.

You can only create virtual servers on Windows 2000 Server and Advanced Server computers—Windows 2000 Professional doesn't support this feature.

Because not all Web browsers can access Web sites that don't have unique IP addresses, you may need to assign IP addresses to any virtual servers you create. If you want to create a virtual server that will have its own IP address, you should configure an additional IP address for the network adapter card in your computer before you create the virtual server. To configure an additional IP address, in the `Network and Dial-up Connections` folder, configure the advanced TCP/IP settings for the connection that Web clients will use to access the virtual server.

STEP BY STEP

CREATING A VIRTUAL SERVER

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Internet Services Manager.
2. In the left pane of the Internet Information Services dialog box, right-click the server on which you want to create a virtual server, and select New ➪ Web Site.
3. The Web Site Creation wizard starts. Click Next.
4. In the Web Site Description screen, type in a description for the Web site. Click Next.
5. The IP Address and Port Settings dialog box appears, as shown in Figure 18-8.

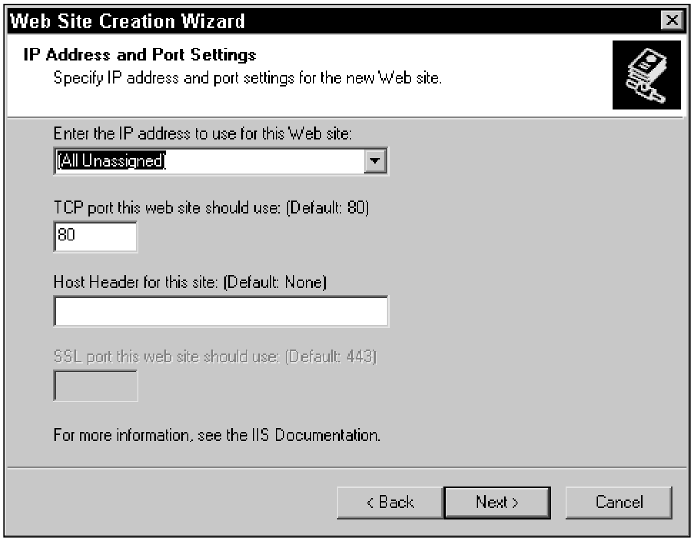

FIGURE 18-8 Configuring IP address and port settings for a virtual server

Configure *at least one* of the following options:

- **If you want to assign the virtual server an IP address,** select one from the “Enter the IP address to use for this Web site” drop-down list box.
- **If you need to change the TCP port number this virtual server will use,** specify this number in the “TCP port this web site should use” text box.
- **If you want to specify the FQDN that Web clients will use to access this virtual server** (such as `www.companyB.com`), enter it in the “Host Header for this site” text box.

STEP BY STEP *Continued*

TIP

You *must* specify either an IP address, a port number other than 80, or a host header in this dialog box to differentiate the virtual server from all other Web sites on this Windows 2000 Web server. Otherwise, the virtual server won't work. The most common item used to differentiate the virtual server from other Web sites is an IP address.

Click Next.

6. In the Web Site Home Directory screen, enter the path to the home folder you want to assign to the virtual server. This can be either a local path to the home folder for this virtual server, or a UNC path to the shared folder on another server that will function as the home folder for this virtual server. You can browse for this folder if you need to. Click Next.
7. In the Web Site Access Permissions screen, select the appropriate access permissions for the virtual server's home folder. The selected permissions are granted to all users who access this home folder. The "Read" and "Run scripts" check boxes are selected by default. Click Next.
8. In the "You have successfully completed the Web Site Creation Wizard" screen, click Finish.
9. Internet Services Manager creates the virtual server, and displays it in the left pane of the Internet Information Services dialog box. If you need to configure your new virtual server, right-click the virtual server and select Properties from the menu that appears. Configuring a virtual server is the same as configuring any other Web site. Close Internet Information Services.

Managing Web Server Security

When it comes to managing a Web server, security is of paramount concern. You're concerned about protecting the resources on your Windows 2000 Web server. You also want to make sure only authorized users gain access to your Web content. In addition, you may want to ensure that communications to and from the Web server are secure and protected from interception. In fact, there are so many things to be concerned about that you could lose a lot of sleep at night worrying about Web security issues.

EXAM TIP

The Server exam has two objectives on controlling access to Web sites and the files and folders they contain. Be sure you have Web server security down cold when you take this exam.

There are several things you can do to enhance your Windows 2000 Web server's security. You can:

- Specify the authentication methods a particular Web site (or virtual directory) will permit, including whether that site will permit anonymous access.
- Grant or deny access to a particular Web site (or virtual directory) based on the Web client's IP address or Internet domain name.
- Configure encrypted communications to and from the Web server by obtaining a certificate for the Web server.
- Configure home directory security settings for a particular Web site (or virtual directory).
- Place all Web content on NTFS volumes.
- Use physical and network security methods to protect the Web server.

You can perform the first four items in this list by configuring the Properties of the Web site. (For details on how to access this dialog box, see the step-by-step section titled "Configuring the Default Web Site" earlier in this chapter.) If you have more than one Web site on your Web server, you must configure these security options for each Web site. Figure 18-9 shows the Directory Security tab in a Web site's Properties dialog box (in this case, the Default Web Site). Notice the three types of security that can be configured on this tab.

To configure authentication methods, in the "Anonymous access and authentication control" section on the Directory Security tab, click Edit. The Authentication Methods dialog box appears, as shown in Figure 18-10. Notice that, by default, anonymous access to the Web site is allowed. This means that users are not required to provide a user name and password to access this Web site.

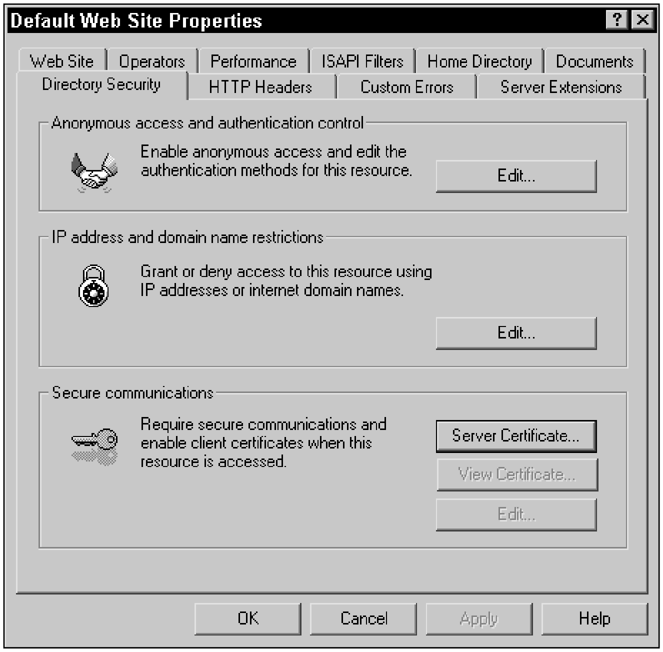

FIGURE 18-9 Configuring Web site security

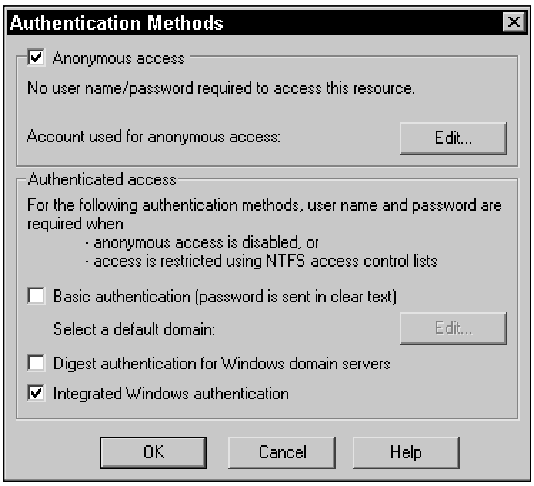

FIGURE 18-10 Configuring authentication methods for a Web site

You can configure several authentication options in this dialog box:

- **Anonymous access:** This option, which is selected by default, permits users to access the Web site without providing a user name and password. If Web content for this Web site is stored on an NTFS volume, Windows 2000 maps anonymous accesses to a specified user account. If that user account doesn't have the appropriate NTFS permissions to the Web content, the anonymous user is prompted to authenticate to the Windows 2000 Web server by using one of the authentication methods selected in the lower portion of the dialog box. By default, anonymous users are mapped to the IUSR_*Server_name* user account, which is a member of the Guests group. To change the account used for anonymous access, click Edit in the "Anonymous access" section. If you don't want to permit anonymous access to the Web site, clear this check box.
- **Basic authentication:** If you select this method, users who authenticate to the Windows 2000 Web server hosting this Web site are permitted to send their user names and passwords in clear text (without any encryption). If you select this option, you can optionally specify the Windows 2000 domain that will authenticate these users. This method is not recommended because it exposes your user names and passwords to anyone using a protocol analyzer to capture packets sent over the Internet.
- **Digest authentication for Windows domain servers:** If you select this method, users who authenticate to the Windows 2000 Web server hosting this Web site are permitted to use digest authentication. This method of authentication, which encrypts user names and passwords, and which can be used through a proxy server or a firewall, is currently only supported on Windows 2000 computers. If you select this method, you must configure all user accounts that will access this Web site to store their password using reversible encryption. Digest authentication can only be used on Windows 2000 Web servers that are members of a Windows 2000 domain.
- **Integrated Windows authentication:** This method, which is selected by default, permits users who authenticate to the Windows 2000 Web server hosting this Web site to use their normal Windows 2000 logon authentication. This is the most secure method of authentication, because, by default, it uses the Kerberos version 5 authentication protocol.

To grant or deny access to the Web site based on the Web client's IP address or Internet domain name, in the "IP address and domain name restrictions" section on the Directory Security tab, click Edit. The IP Address and Domain Name Restrictions dialog box appears, as shown in Figure 18-11.

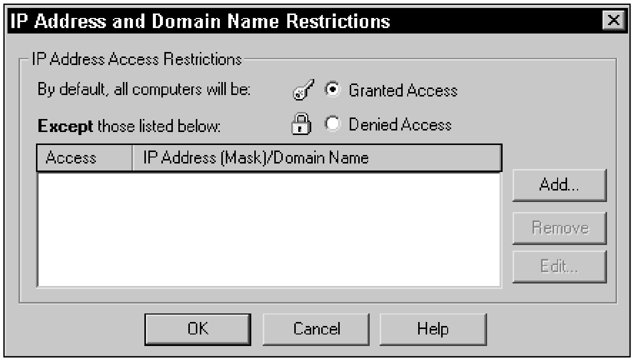

FIGURE 18-11 Configuring IP address and domain name restrictions

If you select the "Granted Access" option, all Web clients will be granted access to this Web site except those whose IP addresses or domain names are explicitly listed in this dialog box. If you select the "Denied Access" option, all Web clients will be denied access to this Web site except those whose IP addresses or domain names are explicitly listed in this dialog box. To add IP addresses (or domain names) to this dialog box, click Add.

To configure encrypted communications to and from the Web server by obtaining a certificate for the Web server, in the "Secure communications" section on the Directory Security tab, click Server Certificate. Then follow the directions presented on-screen in the IIS Certificate Wizard to obtain a certificate for this Web server. Once you've installed a certificate, you can use Web server applications that use Secure Sockets Layer (SSL) encryption on traffic to and from the Web server. In addition, you can configure the Web server to authenticate Web clients by using certificates (such as those contained on smart cards) instead of user names and passwords. (I'll cover how to use certificates in more detail later in this chapter.)

To configure home directory security settings for a Web site, you'll need to access the Home Directory tab in the Web site's Properties dialog box. Figure 18-12 shows the Home Directory tab.

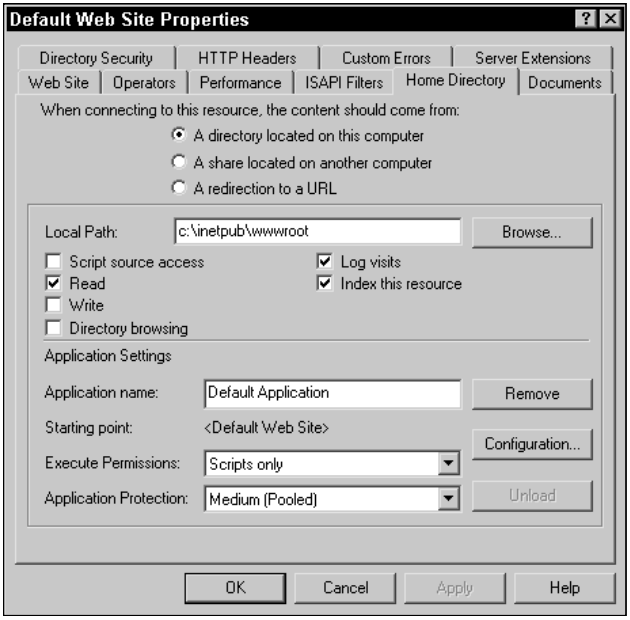

FIGURE 18-12 Configuring home directory security options

There are several settings that affect your Web site's security on this tab:

- **Script source access:** If you select this option, Web clients will be permitted to view the source code for scripts that run on this Web site. This practice is normally not recommended if security is a concern.
- **Read:** This option, which is selected by default, enables Web clients to access this Web site. You must ensure this option is selected or else Web clients will be unable to open this Web site's Web pages.
- **Write:** If you select this option, Web clients will be able to upload files to this Web site. This practice is normally not recommended if security is a concern.
- **Directory browsing:** If you select this option, Web clients will be able to use their Web browser to view a list of subfolders and files contained in this Web site. This practice is normally not recommended if security is a concern.
- **Log visits:** This option, which is selected by default, causes the Windows 2000 Web server to log each access to the Web site. This option is recommended if you want to monitor Web site usage.

- **Index this resource:** This option, which is selected by default, causes the Indexing service to include this Web site's contents in its Index. The Indexing service is covered later in this chapter.
- **Execute Permissions:** The setting determines whether Web clients can run scripts and executables in this Web site. There are three options in this drop-down list box: None, Scripts only, and Scripts and Executables. Select the option that corresponds to the type of content in the Web site. For example, if your Web site contains executables, you should select the Scripts and Executables option. If your Web site doesn't contain any scripts or executables, select None.

CAUTION

If you select Scripts and Executables, *and* you enable the Write permission to the Web site, you may end up exposing data in the Web site, and potentially the entire Web server, to hackers, who could upload a file containing a damaging executable (such as a virus).

You can also increase your Web server's security by only placing Web content on NTFS volumes, and configuring NTFS permissions for the Web content.

CROSS-REFERENCE

See Chapter 11 for detailed information on assigning NTFS permissions to files and folders.

Finally, you can use physical and network security to safeguard your Windows 2000 Web server. Physical security usually involves placing the server in a locked room that only administrators have access to. Network security often involves the use of firewalls to protect the Web server (and the network to which it is attached) from unauthorized access.

Monitoring Access to Files and Folders in Web Sites

Web sites are frequently monitored to determine how much the Web site is being utilized, which Web pages are being accessed most frequently, and who is accessing the Web site. In addition, the Windows 2000 Web server may be monitored periodically to ensure that its resources (memory, processor, disk, and so on) are adequate for its Web server tasks.

Logging is enabled on all Web sites created on a Windows 2000 Web server, by default. To view log files of Web site activity, including accesses to the files and folders in the Web site, you can use Notepad or any other text editor. By default, a Web site's log file is stored in the `SystemRoot\system32\LogFiles` folder.

Another way to manage logging is to select the ODBC Logging option and configure the logging data to be exported directly to a database. Then you can use the database's report tool to generate a report of Web site activity. This option is easier, from an administrator's standpoint, than wading through voluminous text files.

If you store your Web content on NTFS volumes, and if you disable anonymous access to the Web site, you can use Windows 2000 auditing to track accesses (and attempted accesses) to files and folders in a Web site.

CROSS-REFERENCE

Auditing of files and folders was covered in Chapter 13.

You can also use System Monitor, a Performance tool, to monitor the Web Service object and its many counters. The Web Service object and its counters are available in System Monitor when the World Wide Web Server component of IIS is installed on a Windows 2000 computer. You can also use System Monitor to determine if your Web server has adequate memory, processor, and disk resources.

CROSS-REFERENCE

I'll cover how to use System Monitor in Chapter 21.

Troubleshooting Web Services

Typically, Windows 2000 Web servers don't require much troubleshooting. Once the Web server is up and running, it normally just works.

However, it's not uncommon to experience difficulties when implementing Web services on your corporate intranet or on the Internet. Most often these problems are the result of an incorrectly configured option on the Windows 2000 Web server or Web site. Table 18-1 lists some common Web services problems and suggested solutions to those problems.

TABLE 18-1 Common Web Services Problems and Solutions

Problem	Recommended Solution
Users report that they can't access a Web site on your Windows 2000 Web server by typing the FQDN of the Web server in their Web browser.	Try to access the Web site by typing the IP address of the Web server instead of its FQDN in your Web browser. If this works, ensure that the Web server, including all of its aliases, is correctly listed in your domain's DNS server, and that the DNS server is operating.
Users report that they are prompted to enter a user name and password to access a Web site even though you configured that Web site to permit anonymous access.	Verify that the anonymous user account (IUSR_*Server_name*) has the appropriate NTFS permissions to the files and folders in the Web site.
Your Web content developer reports that the executables he has included in your company's Web site don't run when he accesses this Web site from a Web browser.	Ensure that the properties of the Web site are configured so that the Execute Permissions (on the Home Directory tab) option specifies that both Scripts and Executables can be run in this Web site. (The default setting for this option is Scripts only.)
A user reports that she is able to access your company's Web site from her computer at the office, but is unable to access the Web site from her home computer.	If you have implemented IP address and domain name restrictions on this Web site, ensure that the user's home computer is *not* denied access to the Web site by IP address or domain name. Or, if you're using a firewall, configure the firewall so that the user can connect to the Web site through the firewall. Or, if security is critical to this Web site, you may need to instruct the user to only access the Web site from her computer at the office.
Users who use older versions of Internet Explorer and Netscape Navigator report that they are unable to access a virtual server on your Windows 2000 Web server.	Because older Web browsers require an IP address when accessing a virtual server, ensure that the virtual server is configured with its own IP address.

Using the Indexing Service

The *Indexing Service* is a Windows 2000 service that indexes Web site content and other documents on a Windows 2000 computer so these items can be searched by users. You can think of the Indexing Service as a Windows 2000 search engine.

The Indexing Service is installed on both Windows 2000 Professional and Windows 2000 Server/Advanced Server computers by default. However, the service is configured to start manually, which means the service isn't enabled until you start it.

When you first start the Indexing Service, it examines all HTML documents, plain-text documents, Microsoft Office 95 and later documents, Internet mail and news files, and any other type of document for which a document filter is available. Then the Indexing Service creates catalogs (indexes) of the words and phrases contained in these files, as well as the properties of these documents. The Indexing Service automatically creates two catalogs: one for HTML and other documents contained in Web sites on the computer (the Web catalog), and one for all other indexable documents on the computer (the System catalog).

After the catalogs are constructed, users can search all indexed documents by word, phrase, or other property of the file, such as the author's name. As existing files are modified and new files are added, the Indexing Service updates its catalogs, automatically, in the background.

By default, all files and folders on a Windows 2000 computer's local hard disk are configured with the advanced attribute "For fast searching, allow Indexing Service to index this file (folder)." In addition, by default, the local hard disk is also configured to "Allow the Indexing Service to index this disk for fast file searching." Finally, all Web sites on a Windows 2000 Web server, by default, are configured to "Index this resource."

CAUTION

The Indexing Service requires a fair amount of disk space (as much as 40 percent of the space used by indexable documents) for the catalogs it generates. If space on your hard disk is an issue, you may not want to enable this service.

Using the Index Service is as easy as starting the service (and changing its startup type to automatic), waiting for the service to create the catalog, and then performing searches. There are several search tools you can use:

- The Search tool in the Start menu
- The Search tool in Windows Explorer
- The Indexing Service's query tool in Computer Management

TIP

Depending on the amount of data on your computer's local hard disk, the Indexing Service may require from 1 to 24 hours, or sometimes even longer, to create the catalog.

STEP BY STEP

ENABLING THE INDEXING SERVICE

1. Right-click My Computer, and select Manager from the menu that appears.
2. In the left pane of the Computer Management dialog box, click the + next to Services and Applications. Highlight Services. Then, in the right pane, right-click the Indexing Service, and select Properties from the menu that appears.
3. In the Indexing Service Properties (Local Computer) dialog box, select Automatic from the "Startup type" drop-down list box. Then click Start. Click OK.
4. The Indexing Service is started, and is configured to automatically start every time the computer starts. Close Computer Management.

Because you're probably already familiar with the Windows Explorer Search tool (which is the same search tool found in the Start menu), I'll show you how to use the Indexing Service's query tool in Computer Management.

STEP BY STEP

USING THE INDEXING SERVICE TO QUERY THE CATALOG

1. Right-click My Computer, and select Manager from the menu that appears.
2. In the left pane of the Computer Management dialog box, click the + next to Services and Applications. Click the + next to Indexing Service. Click the + next to either Web or System, depending on whether you want to search the computer's Web sites or its other documents. Highlight Query the Catalog.
3. In the right pane, an Indexing Service Query Form appears, as shown in Figure 18-13.

STEP BY STEP *Continued*

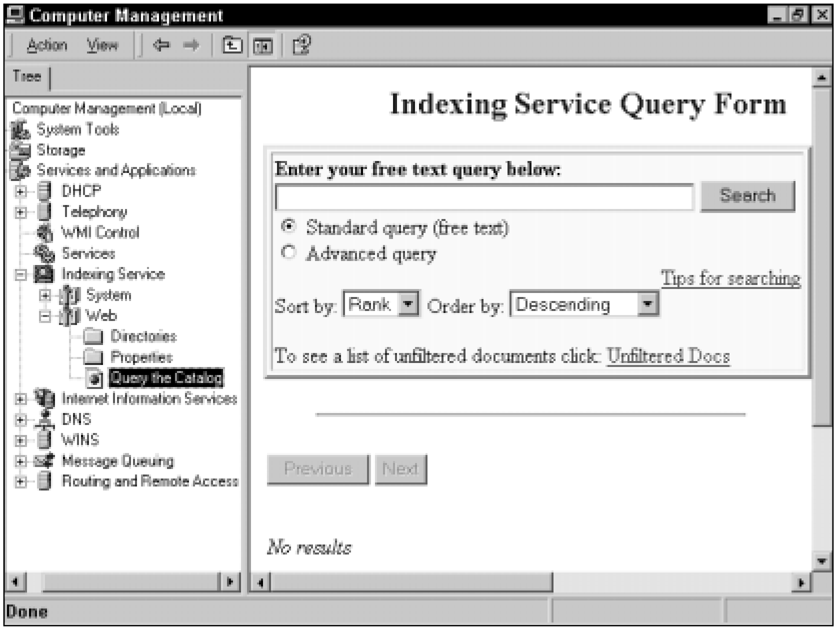

FIGURE 18-13 Querying a catalog

In the "Enter your free text query below" text box, type in the word or phrase you want to search for. For information on constructing better queries, click the "Tips for searching" link. Click Search.

4. The results of the search are returned in the right pane. Close Computer Management.

Managing Certificate Services

Certificate Services is a Windows 2000 Server service used to create, issue, and manage certificates on a Windows 2000 network. If your company's network isn't connected to the Internet, you probably don't have a need for Certificate Services. However, if your network is connected to the Internet, you may need the encryption and other security features that can be provided by certificates and Certificate Services. Certificate Services can be installed on any Windows 2000 Server computer, but can't be installed on Windows 2000 Professional computers.

An organization that uses a computer to create, issue, and manage certificates is called a *certification authority (CA)*. This term is also used to refer to the actual server that performs the task of issuing and managing certificates. In Windows 2000, the server on which Certificate Services is installed is a CA, and is also called a certificate server. The CA receives requests for certificates from other computers on the network, then verifies the credentials in the request, and finally creates and issues the certificate.

A *certificate* is a cryptographic tool used for encrypting and decrypting data, digitally signing files and other data, and performing user authentication. A certificate consists of two parts: a public key and a private key. The public key is the part of the certificate that an organization makes available to anyone requesting it. It's not a secret. On the other hand, a private key is the part of the certificate that is kept private, and not disclosed to anyone other than the user (or computer) to which it was issued. When you use certificates and their associated public and private keys, you are said to be implementing a public key infrastructure (PKI).

Any data encrypted by using the public key can only be decrypted by using the private key. Likewise, any file digitally signed by using the private key can only be verified by using the public key. In addition, a certificate can be stored on a smart card, and when used in conjunction with a smart card reader and a PIN number, can be used for user authentication.

If you want to enable users to send encrypted e-mail messages, or enable Web servers to perform encrypted two-way communication with Web clients over the Internet, or you want to use certificates and smart cards to authenticate users, you can either obtain certificates from a public CA, such as Verisign, or you can create and issue your own certificates by using Certificate Services. Because purchasing certificates from a public CA can be costly, if you plan to use more than one or two certificates in your organization, you'll probably want to install Certificate Services to create and issue your own certificates.

EXAM TIP

The Network exam has five objectives on using Certificate Services. If you don't use this feature regularly on your network, spend some time learning how to issue and manage certificates before you take this exam.

In the following sections, I'll show you how to install and configure Certificate Services, how to create and issue certificates, how to revoke certificates, and finally, how to manage Encrypting File System (EFS) recovery agents.

Installing and Configuring Certificate Services

Certificate Services can be installed during the installation of Windows 2000 Server, but is not normally installed until later. Before you install Certificate Services, you should ensure that the World Wide Web Server and the Common Files components of IIS are installed. It probably goes without saying, but Certificate Services also requires TCP/IP.

You can use the Add/Remove Programs application in Control Panel to install and configure Certificate Services.

STEP BY STEP

INSTALLING CERTIFICATE SERVICES AND CONFIGURING A CA

1. Select Start ➪ Settings ➪ Control Panel.
2. In the Control Panel dialog box, double-click Add/Remove Programs.
3. In the Add/Remove Programs dialog box, click Add/Remove Windows Components.
4. In the Windows Components Wizard dialog box, select the check box next to Certificate Services.
5. A warning dialog box appears, indicating that after Certificate Services is installed, you will not be able to rename this computer, nor will you be able to join a domain or remove the computer from the domain. Click Yes to continue.
6. In the Windows Components Wizard dialog box, click Next.
7. The Certification Authority Type screen appears, as shown in Figure 18-14.

   Select the certification authority role this server will perform:

   - **Enterprise root CA:** Select this option if you're installing the first certificate server in the forest. This type of CA is the most trusted CA on the network. This CA signs its own CA certificate, and can issue certificates to subordinate CAs. An enterprise root CA requires the use of Active Directory. Only a member of the Domain Admins group can install an enterprise root CA.
   - **Enterprise subordinate CA:** Select this option if you have already installed an enterprise root CA in the forest, and you need an additional CA. This CA must obtain its CA certificate from another CA in the forest. This type of CA also requires the use of Active Directory.

STEP BY STEP *Continued*

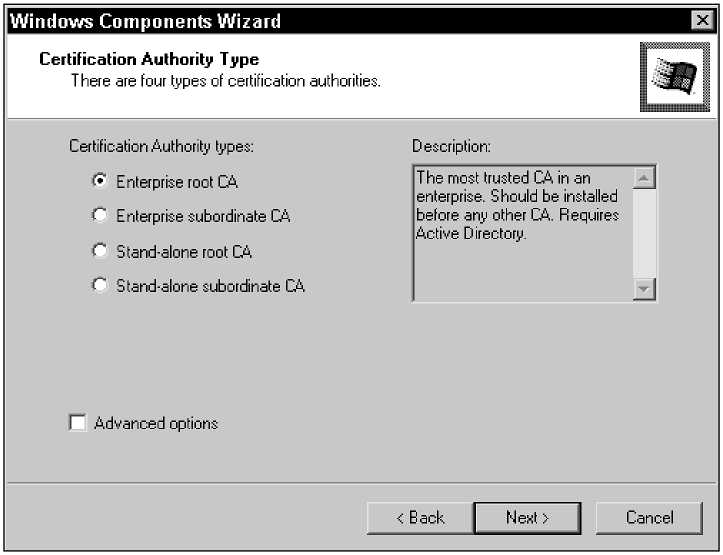

FIGURE 18-14 Selecting a certification authority (CA) type

- **Stand-alone root CA:** Select this option if you're installing the first certificate server that will become the root of a certificate authority hierarchy, and you want to be able to isolate the CA from your network for security reasons. This type of CA does not require the use of Active Directory.
- **Stand-alone subordinate CA:** Select this option if you have already installed a stand-alone root CA and you need an additional CA. This CA must obtain its CA certificate from another CA in the hierarchy. This type of CA does not require the use of Active Directory.

To configure advanced CA options, such as cryptographic service providers, hash algorithms, or key lengths, select the check box next to "Advanced options," and select the appropriate options on the following screen.

Click Next.

8. In the CA Identifying Information screen, enter the CA name, organization, city, state, description, and so on, to identify the CA. Click Next.
9. In the Data Storage Location screen, either accept the default database and log locations, or specify different locations. Click Next.
10. A warning dialog box appears, as shown in Figure 18-15. Notice that IIS must be stopped to complete the installation of Certificate Services. Click OK.

STEP BY STEP *Continued*

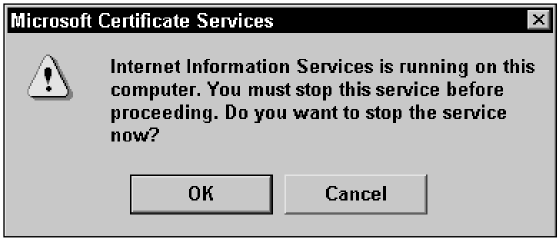

FIGURE 18-15 Certificate Services warning message

11. When prompted, insert your Windows 2000 Server compact disc into the computer's CD-ROM drive and click OK. When the Microsoft Windows 2000 CD dialog box appears, close it. Windows 2000 installs Certificate Services. In the Completing the Windows Components Wizard screen, click Finish.
12. Close Add/Remove Programs. Then close Control Panel.

Creating and Issuing Certificates

Now that you've installed Certificate Services and configured a CA, you're ready to specify the types of certificates your certificate server can issue. One CA can issue many different types of certificates, such as User, Computer, Web Server, Code Signing, Smartcard Logon, EFS Recovery Agent, and so on.

You can specify the types of certificates a CA can create and issue by using the Certification Authority administrative tool. This tool, like many other Windows 2000 administrative tools, is an MMC console.

STEP BY STEP

SPECIFYING THE TYPES OF CERTIFICATES A CA CAN CREATE AND ISSUE

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Certification Authority.
2. In the left pane of the Certification Authority dialog box, click the + next to the CA you want to configure. Highlight the `Policy Settings` folder. In the right pane, a list of certificate types this CA is currently permitted to issue is displayed, as shown in Figure 18-16.

STEP BY STEP *Continued*

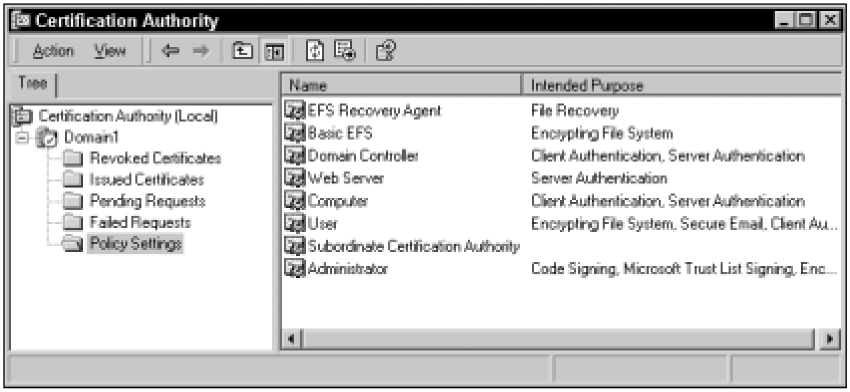

FIGURE 18-16 Viewing a CA's policy settings

3. To specify an additional certificate type, select Action ➪ New ➪ Certificate to Issue.
4. The Select Certificate Template dialog box appears. This dialog box doesn't display all possible types of certificates, but displays only the types of certificates this CA is not yet authorized to issue. Highlight the additional type of certificate you want this CA to be able to issue. For example, if you want this CA to be able to issue IPSec certificates, select IPSEC. Click OK.
5. Repeat Steps 3 and 4 until you have specified all desired certificate types. Close Certification Authority.

Once you've specified the types of certificates the CA can create and issue, users and client computers can request the certificates they need from the CA. When certificates are first implemented, the users and computers that require certificates request and receive them from the CA. Once issued, certificates are typically valid for one year. After certificates are implemented on a network, users and computers don't normally request certificates very often. Users and computers only request certificates when they need to perform a task, such as code signing, for which a certificate is required.

Users must manually request certificates for themselves. Users can also manually request certificates for their computers. There are two methods you can use to manually request certificates. Users of Windows 2000 computers can use the Certificate snap-in to the MMC. Users of all other computers can request certificates by using their Web browsers to access the CA's Web site at `http://`*`server_name_of_CA`*`/certsrv`.

In addition, an Administrator can use Group Policy to configure computers to automatically request certificates, when needed, from the CA.

STEP BY STEP

USING THE CERTIFICATE SNAP-IN TO REQUEST A CERTIFICATE

1. On the Windows 2000 client computer, select Start ➪ Run.
2. In the Run dialog box, type **mmc** and click OK.
3. In the Console1 dialog box, select Console ➪ Add Remove Snap-in.
4. In the Add/Remove Snap-in dialog box, click Add.
5. In the Add Standalone Snap-in dialog box, highlight Certificates. Click Add.
6. In the Certificates snap-in dialog box, select whether you want to manage certificates for your user account, for an account used by a Windows 2000 service, or for a computer account. Click Finish.
7. In the Add Standalone Snap-in dialog box, click Close.
8. In the Add/Remove Snap-in dialog box, click OK.
9. Maximize the Console Root dialog box.
10. In the left pane of the Console 1 – (Console Root) dialog box, click the + next to Certificates – Current User (or Service, or Local Computer). Click the + next to the `Personal` folder. Highlight the `Certificates` folder. Select Action ➪ All Tasks ➪ Request New Certificate.
11. The Certificate Request Wizard starts. Click Next.
12. In the Certificate Template screen, select the type of certificate you're requesting. Click Next.
13. In the Certificate Friendly Name and Description screen, enter a user-friendly name and description for the new certificate. Click Next.
14. In the Completing the Certificate Request Wizard screen, click Finish.
15. The Certificate Request Wizard displays a dialog box, indicating that the certificate request was successful. Click Install Certificate.
16. Another Certificate Request Wizard dialog box is displayed. Click OK.
17. The new certificate is displayed in the right pane. Close the MMC console.

If you don't want users to have to manually request certificates for their computers, you can use Group Policy to configure a computer, or all of the computers in an Active Directory container, such as a domain or OU, to automatically request certificates from the CA.

STEP BY STEP

CONFIGURING THE COMPUTERS IN AN OU TO AUTOMATICALLY REQUEST CERTIFICATES

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. In the left pane of the Active Directory Users and Computers dialog box, expand domains and OUs as necessary until the OU you want to configure is displayed in the left pane. Right-click the OU, and select Properties from the menu that appears.
3. In the OU's Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab, double-click the Group Policy object (GPO) you want to edit.
5. In the left pane of the Group Policy dialog box, click the + next to the `Windows Settings` folder in the Computer Configuration section. Click the + next to the Security Settings container. Click the + next to the `Public Key Policies` folder. Highlight the `Automatic Certificate Request Settings` folder.
6. Select Action ➪ New ➪ Automatic Certificate Request.
7. The Automatic Certificate Request Setup wizard starts. Click Next.
8. The Certificate Template screen appears, as shown in Figure 18-17.

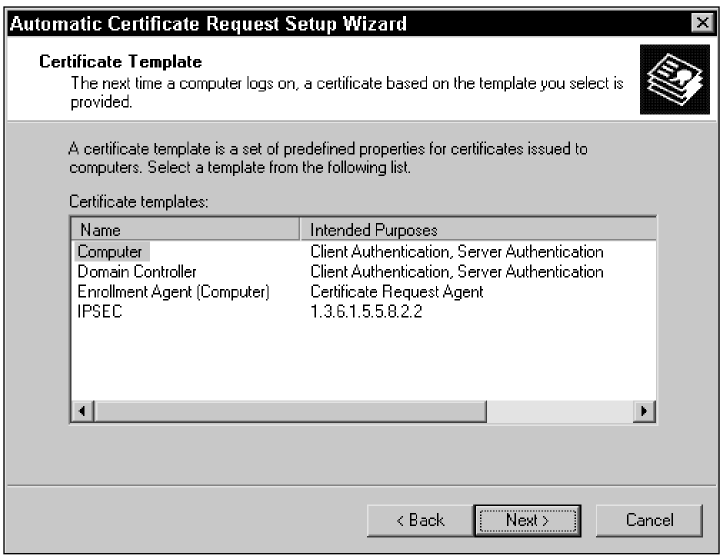

FIGURE 18-17 Selecting a certificate template

STEP BY STEP *Continued*

In this screen, highlight the type of certificate you want all of the computers in this OU to automatically request. Click Next.

9. In the Certification Authority screen, select one or more CAs from which the computers in this OU can automatically request certificates. Click Next.
10. In the Completing the Automatic Certificate Request Setup screen, click Finish.
11. The Automatic Certificate Request policy is displayed in the right pane. If you want all of the computers in this OU to automatically request more than one type of certificate, repeat Steps 6 through 10 as needed. Close the Group Policy dialog box.
12. In the OU's Properties dialog box, click OK.
13. Close Active Directory Users and Computers.

Revoking Certificates

Certificates should be revoked when the user (or computer) that uses the certificate no longer performs the task for which the certificate was requested. For example, if an employee leaves the company, you should revoke all of the user certificates assigned to that employee. Or, if an employee was issued a Code Signing certificate, but has recently been promoted to a management position and no longer performs code signing tasks, you should revoke that user's certificate.

You can use the Certification Authority administrative tool to revoke certificates.

STEP BY STEP

REVOKING A CERTIFICATE

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Certification Authority.
2. In the left pane of the Certification Authority dialog box, click the + next to the CA that issued the certificate you want to revoke. Highlight the `Issued Certificates` folder. In the right pane, right-click the certificate you want to revoke, and select All Tasks ➪ Revoke Certificate.
3. A Certificate Revocation dialog box appears, asking if you're sure you want to revoke the certificate.

   If you want to, you can specify a reason code for revoking this certificate, but this configuration is optional.

STEP BY STEP *Continued*

TIP

If you think you might want to reinstate this certificate at a later date, select a reason code of Certificate Hold. You can reinstate a held certificate by using the `certutil.exe` command-line utility.

Click Yes.

4. The certificate is revoked. The certificate is moved from the `Issued Certificates` folder to the `Revoked Certificates` folder. Close Certification Authority.

Managing Encrypting File System (EFS) Recovery Agents

As you may recall, the *Encrypting File System (EFS)* enables you to store files on an NTFS volume in an encrypted format, so that if an unauthorized user removes a hard disk from your computer, that user will be unable to access the data contained in the encrypted files. EFS is implemented in Windows 2000 by assigning the Encrypt attribute to folders and files. The Encrypt attribute is normally applied by a user to protect sensitive data that should only be accessed by that user.

But what happens when the user that assigned the Encrypt attribute is not available, or no longer works for the company, and you need to access the data contained in the encrypted files? That's when you need an EFS recovery agent. An EFS *recovery agent* is a user account that is assigned an EFS Recovery Agent certificate that permits the user to unencrypt (that is, recover) all encrypted files on a computer. By default, the Administrator account is a recovery agent.

However, depending on the sensitivity of your company's data, it may not always be desirable to grant any person — even an Administrator — the permissions to open any encrypted file at any time. So, what many companies do to safeguard their data is designate a user (probably an administrator) as a recovery agent, but then remove the user's EFS Recovery Agent certificate, so that the designated recovery agent can't casually open and view encrypted files.

The actual process of configuring a recovery agent in this manner is somewhat complicated:

1. The user who will function as the EFS recovery agent requests and receives an EFS Recovery Agent certificate from the CA.
2. The user exports the EFS Recovery Agent certificate to a file on a floppy disk.
3. The Administrator uses the floppy disk containing the certificate to designate the user as an EFS recovery agent (for a domain or OU) in Group Policy. Then the Administrator stores the floppy disk in a safe, vault, or other secure location.
4. Finally, the user removes his or her EFS recovery agent certificate.

EXAM TIP

One of the objectives for the Network exam mentions removing "the Encrypting File System (EFS) recovery keys." What this objective is really referring to is the entire process of designating a recovery agent, and then removing all EFS Recovery Agent certificates.

Later, if a recovery agent is needed to unencrypt data, the Administrator or designated user retrieves the floppy disk containing the EFS Recovery Agent certificate. Then the designated user imports that certificate onto the computer that will be used to recover the data. The designated user unencrypts the needed files. Lastly, the designated user deletes the EFS Recovery Agent certificate from the computer, and returns the floppy disk to the secure location.

In the following sections I'll show you how to designate a user as a recovery agent and how to remove the designated user's EFS Recovery Agent certificate.

TIP

Only the user that will receive a certificate can request a certificate. If someone other than yourself is designated as the recovery agent, that user should log on and request an EFS Recovery Agent certificate. That user should also export the certificate and later delete the certificate.

STEP BY STEP

REQUESTING AN EFS RECOVERY AGENT CERTIFICATE

1. Select Start ➪ Run.
2. In the Run dialog box, type **mmc** and click OK.
3. In the Console1 dialog box, select Console ➪ Add Remove Snap-in.
4. In the Add/Remove Snap-in dialog box, click Add.
5. In the Add Standalone Snap-in dialog box, highlight Certificates. Click Add.
6. In the Certificates snap-in dialog box, select the “My user account” option. Click Finish.
7. In the Add Standalone Snap-in dialog box, click Close.
8. In the Add/Remove Snap-in dialog box, click OK.
9. Maximize the Console Root dialog box.
10. In the left pane of the Console 1 – (Console Root) dialog box, click the + next to Certificates – Current User. Click the + next to the `Personal` folder. Highlight the `Certificates` folder. Select Action ➪ All Tasks ➪ Request New Certificate.
11. The Certificate Request Wizard starts. Click Next.
12. In the Certificate Template screen, select EFS Recovery Agent. Click Next.
13. In the Certificate Friendly Name and Description screen, enter a user-friendly name and description for the EFS Recovery Agent certificate. Click Next.
14. In the Completing the Certificate Request Wizard screen, click Finish.
15. The Certificate Request Wizard displays a dialog box, indicating that the certificate request was successful. Click Install Certificate.
16. Another Certificate Request Wizard dialog box is displayed. Click OK.
17. The EFS Recovery Agent certificate is displayed in the right pane. Leave the MMC console open and continue to the next set of steps.

After the designated user requests and receives an EFS Recovery Agent certificate, that user should export the certificate to a floppy disk.

STEP BY STEP

EXPORTING THE EFS RECOVERY AGENT CERTIFICATE

1. Insert a floppy disk that will contain the EFS Recovery Agent certificate into your computer’s `A:` drive.

STEP BY STEP *Continued*

2. In the right pane of the MMC console that you opened and configured in the previous section, right-click the EFS Recovery Agency certificate, and select All Tasks ➪ Export.
3. The Certificate Export wizard starts. Click Next.
4. In the Export Private Key screen, select the “No, do not export the private key” option. Click Next.
5. In the Export File Format screen, ensure that the “DER encoded binary X.509 (.CER)” format is selected. Click Next.
6. In the File to Export screen, type an appropriate name for the certificate, such as `a:\efscert`, and click Next.
7. In the Completing the Certificate Export Wizard screen, click Finish.
8. A Certificate Export Wizard message appears, indicating the export was successful. Click OK.
9. Close the MMC console.

The next step in the process is designating the user as a recovery agent by using Group Policy. An Administrator should perform this task.

TIP

Even if a user has requested and received an EFS Recovery Agent certificate, that user can’t unencrypt any files until they have been designated as a recovery agent in Group Policy.

STEP BY STEP

DESIGNATING A RECOVERY AGENT

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. In the left pane of the Active Directory Users and Computers dialog box, expand domains and OUs as necessary until the domain or OU for which you want to designate a recovery agent is displayed in the left pane. Right-click the domain or OU, and select Properties from the menu that appears.
3. In the domain or OU’s Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab, double-click the Group Policy object (GPO) you want to edit.

STEP BY STEP *Continued*

5. In the left pane of the Group Policy dialog box, click the + next to the `Windows Settings` folder in the Computer Configuration section. Click the + next to the Security Settings container. Click the + next to the `Public Key Policies` folder. Highlight the `Encrypted Data Recovery Agents` folder. Select Action ➪ Add.
6. The Add Recovery Agent Wizard starts. Click Next.
7. The Select Recovery Agents screen appears. The easiest way to add a user to the list of recovery agents is to retrieve the EFS Recovery Agent certificate from the floppy disk. To do this, click Browse Folders.
8. In the Open dialog box, in the "File name" text box, type the full path to the exported certificate file, for example, `a:\efscert`. Click Open.
9. In the Select Recovery Agents screen, click Next.
10. In the Completing the Add Recovery Agent Wizard screen, click Finish.
11. The newly designated recovery agent is displayed in the right pane. (If you have previously designated other recovery agents that you no longer wish to use, highlight them in the right pane, one at a time, and select Action ➪ Delete.) Close Group Policy.
12. In the domain or OU's Properties dialog box, click OK.
13. Close Active Directory Users and Computers.

The last part in the process is removing the designated user's EFS Recovery Agent certificate. The user who requested the EFS Recovery Agent certificate should perform this task (or you should be logged on as that user). You can use either the Internet Options application in Control Panel or the Certificates snap-in to the MMC to remove the certificate.

STEP BY STEP

DELETING EFS RECOVERY AGENT CERTIFICATES

1. Select Start ➪ Settings ➪ Control Panel.
2. In Control Panel, double-click Internet Options.
3. In the Internet Properties dialog box, click the Content tab.
4. On the Content tab, click Certificates.
5. The Certificates dialog box appears. Highlight the certificate you want to delete.

STEP BY STEP *Continued*

Before you delete the certificate, take special note of the "Certificate intended purposes" section in the lower portion of this dialog box. *Ensure that the intended purpose of the certificate you're deleting is "File Recovery."*

Click Remove.

6. A warning dialog box is displayed. Click Yes.
7. The certificate is deleted. In the Certificates dialog box, click Close.
8. In the Internet Properties dialog box, click OK.
9. Close Control Panel.

KEY POINT SUMMARY

This chapter introduced several important Web and Certificate Services topics:

- Internet Information Services (IIS) is Windows 2000's Web server. IIS is a collection of many services. Some of the most commonly used components are World Wide Web Server, File Transfer Protocol (FTP) Server, FrontPage 2000 Server Extensions, the SMTP Service, and the NNTP Service.
- Some IIS components are installed by default during the installation of Windows 2000. You can add additional components by using Add/Remove Programs.
- IIS requires the use of TCP/IP.
- You can manage and configure the Default Web Site and any other Web sites on your computer by using the Internet Services Manager administrative tool.
- Personal Web Manager is an easy-to-use Windows 2000 Professional tool that enables a novice user to manage and monitor a Web site on the local Windows 2000 Professional computer.
- A virtual directory is a child Web site that doesn't contain Web content. Rather, it is a pointer to an actual folder that contains its Web content.
- A virtual server is a pseudo WWW server with its own unique fully qualified domain name (FQDN), and often has its own IP address. To the Internet user accessing the virtual server, a virtual server appears to be a separate server; but in reality, a virtual server is *not* a separate server.

- You can do several things to increase security of your Windows 2000 Web server, including:
  - Specify the authentication methods a particular Web site (or virtual directory) will permit.
  - Grant or deny access to a particular Web site (or virtual directory) based on the Web client's IP address or Internet domain name.
  - Configure encrypted communications to and from the Web server by obtaining a certificate for the Web server.
  - Configure home directory security settings for a particular Web site (or virtual directory).
  - Place all Web content on NTFS volumes.
  - Use physical and network security methods to protect the Web server.
- Certificate Services is a Windows 2000 Server service used to create, issue, and manage certificates on a Windows 2000 network.
- An organization that uses a computer to create, issue, and manage certificates is called a certification authority (CA). This term is also used to refer to the actual server that performs the task of issuing and managing certificates.
- You can use the Certification Authority administrative tool to manage the CA, to specify the types of certificates the CA can issue, and to revoke certificates.

STUDY GUIDE

This section contains several exercises that are designed to solidify your knowledge about IIS and Certificate Services, and to help you prepare for the Professional, Server, and Network exams:

- **Assessment Questions:** These questions test your knowledge of the IIS and Certificate Services topics covered in this chapter. You'll find the answers to these questions at the end of this chapter.
- **Scenarios:** The situation-based questions in scenarios challenge you to apply your understanding of the material to solve a hypothetical problem. In this chapter's scenarios, you are asked to troubleshoot IIS problems and provide answers to the questions. You don't need to be at a computer to do scenarios. Answers to this chapter's scenarios are presented at the end of this chapter.
- **Lab Exercise:** These exercises are hands-on practice activities that you perform on a computer. The lab in this chapter gives you an opportunity to practice installing and configuring IIS and Certificate Services.

Assessment Questions

1. You want to install some additional Internet Information Services components that were not installed during the installation of Windows 2000 Server. Which tool should you use?

   A. Internet Services Manager

   B. Personal Web Server

   C. Add/Remove Programs

   D. `Networking and Dial-up Connections` folder

2. What protocol is required by Internet Information Services (IIS), the Indexing Service, and Certificate Services?

   A. TCP/IP

   B. NWLink IPX/SPX/NetBIOS Compatible Transport Protocol

   C. NetBEUI

   D. RIP Version 2 for Internet Protocol

3. You want to configure the Web site on your Windows 2000 Professional Web server computer. What tool can you use?
   A. Folder Options
   B. Internet Options
   C. Windows Explorer
   D. Personal Web Manager
4. You want to configure performance tuning for a Web site on your Windows 2000 Server computer on which Internet Information Services (IIS) is installed. What tool should you use to configure the Web site?
   A. Internet Options
   B. Internet Services Manager
   C. `Network and Dial-up Connections` folder
   D. Personal Web Manager
5. You work for an ISP that wants to host several Web sites for several of its customers on a single Windows 2000 Server computer on which Internet Information Services (IIS) is installed. Each of your customers wants their own Web site to appear as though it is located on a separate server. How can you accomplish this?
   A. Create a virtual directory for each of the Web sites.
   B. Create a virtual server for each of the Web sites.
   C. Assign a certificate to each of the Web sites.
   D. Use a third-party utility to give the appearance of each Web site being located on a separate server.
6. Which of the following actions can improve security on a Windows 2000 Web server? (Choose all that apply.)
   A. Place all Web content on FAT volumes.
   B. Use IP address or Internet domain name restrictions.
   C. Obtain a certificate for the Web server.
   D. Select Basic authentication for all Web sites on the Web server.
   E. Disable anonymous access to all Web sites on the Web server.

7. You are preparing to install Certificate Services for the first time on your Windows 2000 network. You plan to install Certificate Services on a Windows 2000 Server computer that is a member of the domain. You want the certification authority (CA) to be able to use Active Directory. Which CA type should you select when you install Certificate Services?
   A. Enterprise root CA
   B. Enterprise subordinate CA
   C. Stand-alone root CA
   D. Stand-alone subordinate CA
8. What must be true before a user can perform the role of an EFS recovery agent? (Choose all that apply.)
   A. The user must have an EFS Recovery Agent certificate.
   B. The user must be an Administrator.
   C. The user must be designated as an EFS recovery agent in Group Policy.
   D. The user must be logged on to a domain controller.

Scenarios

Troubleshooting access to Web servers and Web sites (and the files and folders they contain) can be a complex task. For each of the following situations, consider the given facts and answer the question or questions that follow.

1. Several users on your Windows 2000 network report that they are prompted to enter a user name and password each time they access an HTML file in a Web site on your company's Windows 2000 Web server, even though you configured that Web site to permit anonymous access.
   a. What is the most likely cause of this problem?
   b. What should you do to resolve the problem?

2. An employee of your company, John, just started telecommuting three days a week. John reports that he is unable to access the company's Web site when he is working at home, although he has no trouble accessing the Web site from his computer at the office.
   a. What is the most likely cause of this problem?
   b. What should you do to resolve the problem?

Lab Exercise

Lab 18-1 Managing Web and Certificate Services

MCSE EXAM MATERIAL

► Professional
► Server
► Network

The purpose of this lab is to provide you with an opportunity to practice the concepts you learned in this chapter by installing and configuring IIS and Certificate Services.

There are two parts to this lab:

- Part 1: Configuring, Securing, and Monitoring IIS
- Part 2: Installing, Configuring, and Using Certificate Services

Begin this lab by booting your computer to Windows 2000 Server and logging on as Administrator.

Part 1: Configuring, Securing, and Monitoring IIS

In this part, you use the `Network and Dial-up Connections` folder to assign an additional IP address to your network adapter card. Then you create a home folder, and use Internet Services Manager to create, configure, and secure a virtual Web server. Finally, you view one of the log files created by IIS to monitor access to the Web server.

1. Select Start ➪ Settings ➪ Network and Dial-up Connections.
2. In the `Network and Dial-up Connections` folder, right-click Local Area Connection, and select Properties from the menu that appears.

3. In the Local Area Connection Properties dialog box, highlight Internet Protocol (TCP/IP) and click Properties.
4. In the Internet Protocol (TCP/IP) Properties dialog box, click Advanced.
5. In the Advanced TCP/IP Settings dialog box, in the IP addresses section, click Add.
6. In the TCP/IP Address dialog box, enter an IP address of **192.168. 59.***xxx*, where *xxx* is a value that equals your current IP address plus 100. For example, if your IP address is currently 192.168.59.101, enter an IP address of 192.168.59.201. Then, enter a subnet mask of **255.255.255.0**.

   (Or, if you're on a live network, use the IP address and subnet mask provided to you by your administrator or instructor.)

   Click Add.
7. In the Advanced TCP/IP Settings dialog box, click OK.
8. In the Internet Protocol (TCP/IP) Properties dialog box, click OK.
9. In the Local Area Connection Properties dialog box, click OK.
10. Close the `Network and Dial-up Connections` folder.
11. Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.
12. In the left pane, click the + next to My Computer. Click the + next to Local Disk (C:). Highlight the `Inetpub` folder. Select File ➪ New ➪ Folder.
13. Type in a new name for the folder of **Virtualwww** and press Enter.
14. Close Windows Explorer.
15. Select Start ➪ Programs ➪ Administrative Tools ➪ Internet Services Manager.
16. In the left pane of the Internet Information Services dialog box, click the + next to server01. Then right-click server01, and select New ➪ Web Site.
17. The Web Site Creation wizard starts. Click Next.
18. In the Web Site Description screen, type in a description of **Virtual Server**. Click Next.
19. In the IP Address and Port Settings dialog box, select the IP address you just added from the "Enter the IP address to use for this Web site" drop-down list box. Click Next.

20. In the Web Site Home Directory screen, enter a path of **c:\inetpub\virtualwww** and click Next.
21. In the Web Site Access Permissions screen, select the check box next to Execute. Click Next.
22. In the "You have successfully completed the Web Site Creation Wizard" screen, click Finish.
23. Internet Services Manager creates the virtual server and displays it in the left pane of the Internet Information Services dialog box. To configure your new virtual server, right-click Virtual Server and select Properties from the menu that appears.
24. In the Virtual Server Properties dialog box, click the Directory Security tab.
25. On the Directory Security tab, in the "IP address and domain name restrictions" section, click Edit.
26. In the IP Address and Domain Name Restrictions dialog box, select the "Denied Access" option. Then click Add.
27. In the Grant Access On dialog box, select the "Group of computers" option. Type in a Network ID of **192.168.59.0** and enter a subnet mask of **255.255.255.0**. This setting enables all computers on the 192.168.59.0 subnet to access this Web site. Click OK.
28. In the IP Address and Domain Name Restrictions dialog box, click OK.
29. On the Directory Security tab, click OK. Close the Internet Information Services dialog box.
30. Right-click My Computer, and select Explore from the menu that appears.
31. In the left pane, click the + next to Local Disk (C:). Click the + next to the `WINNT` folder. Click the + next to the `system32` folder. Click the + next to the `LogFiles` folder. Highlight the `W3SVC1` folder. In the right pane, double-click the last log file listed.
32. Notepad opens the log file. Scroll down and view the contents of the log file. Notice that you can view the users who have accessed the Web site, and the IP addresses of the users' computers. Close Notepad.
33. Close Windows Explorer.

Part 2: Installing, Configuring, and Using Certificate Services

In this part, you install and configure Certificate Services and create a certificate authority (CA). Then you create and issue certificates, and export a certificate. You also remove an EFS Recovery Agent certificate. Then you designate an Encrypting File System (EFS) recovery agent in Group Policy. Finally, you revoke a certificate. You'll need a floppy disk to perform this part of the lab.

1. Select Start ➪ Settings ➪ Control Panel.
2. In the Control Panel dialog box, double-click Add/Remove Programs.
3. In the Add/Remove Programs dialog box, click Add/Remove Windows Components.
4. In the Windows Components Wizard dialog box, select the check box next to Certificate Services.
5. A warning dialog box appears, indicating that after Certificate Services is installed, you will not be able to rename this computer, nor will you be able to join a domain, or remove the computer from the domain. Click Yes.
6. In the Windows Components Wizard dialog box, click Next.
7. In the Certification Authority Type screen, select the "Enterprise root CA" option and click Next.
8. In the CA Identifying Information screen, enter a CA name of **domain1**, and an organization name of **domain1.mcse**. Then enter your city, state or province, e-mail address, and a CA description of **CA for domain1.mcse**. Click Next.
9. In the Data Storage Location screen, accept the defaults and click Next.
10. A warning dialog box appears. Click OK.
11. When prompted, insert your Windows 2000 Server compact disc into the computer's CD-ROM drive and click OK. When the Microsoft Windows 2000 CD dialog box appears, close it. Windows 2000 installs Certificate Services. In the Completing the Windows Components Wizard screen, click Finish.
12. Close Add/Remove Programs. Then close Control Panel.
13. Select Start ➪ Run.
14. In the Run dialog box, type **mmc** and click OK.
15. In the Console1 dialog box, select Console ➪ Add Remove Snap-in.

16. In the Add/Remove Snap-in dialog box, click Add.
17. In the Add Standalone Snap-in dialog box, highlight Certificates. Click Add.
18. In the Certificates snap-in dialog box, select the "My user account" option. Click Finish.
19. In the Add Standalone Snap-in dialog box, click Close.
20. In the Add/Remove Snap-in dialog box, click OK.
21. Maximize the Console Root dialog box.
22. In the left pane of the Console 1 – (Console Root) dialog box, click the + next to Certificates – Current User. Click the + next to the `Personal` folder. Highlight the `Certificates` folder.
23. Select Action ➪ All Tasks ➪ Request New Certificate.
24. The Certificate Request Wizard starts. Click Next.
25. In the Certificate Template screen, select EFS Recovery Agent. Click Next.
26. In the Certificate Friendly Name and Description screen, enter a Friendly name of **EFS Recovery** and click Next.
27. In the Completing the Certificate Request Wizard screen, click Finish.
28. The Certificate Request Wizard displays a dialog box, indicating that the certificate request was successful. Click Install Certificate.
29. Another Certificate Request Wizard dialog box is displayed. Click OK.
30. The EFS Recovery Agent certificate is displayed in the right pane. Repeat Steps 23 through 29 to request another certificate, except this time select a certificate template of User, and enter a Friendly name of **User Cert** when prompted.
31. Insert a floppy disk into your computer's `A:` drive. In the right pane, right-click the EFS Recovery Agency certificate that has a Friendly Name of EFS Recovery, and select All Tasks ➪ Export.
32. The Certificate Export wizard starts. Click Next.
33. In the Export Private Key screen, select the "No, do not export the private key" option. Click Next.
34. In the Export File Format screen, ensure that the "DER encoded binary X.509 (.CER)" format is selected. Click Next.
35. In the File to Export screen, type **a:\efscert** and click Next.

36. In the Completing the Certificate Export Wizard screen, click Finish.
37. A Certificate Export Wizard message appears, indicating the export was successful. Click OK.
38. In the right pane of the MMC console, right-click the EFS Recovery Agent certificate that has a Friendly Name of EFS Recovery, and select Delete from the menu that appears.
39. When a Certificates warning dialog box appears, click Yes.
40. Close the MMC console. When prompted to save console settings, click No.
41. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
42. In the left pane of the Active Directory Users and Computers dialog box, right-click domain1.mcse, and select Properties from the menu that appears.
43. In the domain1.mcse Properties dialog box, click the Group Policy tab.
44. On the Group Policy tab, double-click the Default Domain Policy.
45. In the left pane of the Group Policy dialog box, click the + next to the `Windows Settings` folder in the Computer Configuration section. Click the + next to the Security Settings container. Click the + next to the `Public Key Policies` folder. Highlight the `Encrypted Data Recovery Agents` folder. Select Action ➪ Add.
46. The Add Recovery Agent Wizard starts. Click Next.
47. The Select Recovery Agents screen appears. Click Browse Folders.
48. In the Open dialog box, type **a:\efscert.cer** in the File name text box. Click Open.
49. In the Select Recovery Agents screen, click Next.
50. In the Completing the Add Recovery Agent Wizard screen, click Finish.
51. The newly designated recovery agent is displayed in the right pane. Close Group Policy.
52. In the domain1.mcse Properties dialog box, click OK.
53. Close Active Directory Users and Computers.
54. Select Start ➪ Programs ➪ Administrative Tools ➪ Certification Authority.

55. In the left pane of the Certification Authority dialog box, click the + next to domain1. Highlight the `Issued Certificates` folder. In the right pane, there should be two certificates listed. Double-click the last certificate in the list to open it.
56. In the Certificate dialog box, verify that this certificate is intended to allow data on disk to be encrypted, protect e-mail messages, and prove your identity to a remote computer. Click OK. If the certificate you opened was intended for a different purpose, try double-clicking another certificate in the console until you find the one just described.
57. In the right pane of the console, right-click the certificate that met the criteria specified in Step 56, and select All Tasks ➪ Revoke Certificate.
58. A Certificate Revocation dialog box appears, asking if you're sure you want to revoke the certificate. Click Yes.
59. The certificate is revoked. The certificate is moved from the `Issued Certificates` folder to the `Revoked Certificates` folder. Close Certification Authority.

Answers to Chapter Questions

Chapter Pre-Test

1. The most commonly used components of IIS are World Wide Web Server, File Transfer Protocol (FTP) Server, FrontPage 2000 Server Extensions, the SMTP Service, and the NNTP Service.
2. World Wide Web Server
3. Personal Web Manager is an easy-to-use Windows 2000 Professional tool that enables a novice user to manage and monitor a Web site on the local computer.
4. A virtual directory is a child Web site that doesn't contain Web content. Rather, it is a pointer to an actual folder that contains its Web content.
5. A virtual server is a pseudo WWW server with its own unique fully qualified domain name (FQDN), and often has its own IP address. To the Internet user accessing the virtual server, a virtual server appears to be a separate server; but in reality, a virtual server is *not* a separate server, but more like a shared folder on the Windows 2000 Server Web server that is accessed by specifying a different FQDN.

6. You can do several things to increase security of your Web server, including:
   - Specify the authentication methods a particular Web site (or virtual directory) will permit, including whether that site will permit anonymous access.
   - Grant or deny access to a particular Web site (or virtual directory) based on the Web client's IP address or Internet domain name.
   - Configure encrypted communications to and from the Web server by obtaining a certificate for the Web server.
   - Configure home directory security settings for a particular Web site (or virtual directory).
   - Place all Web content on NTFS volumes.
   - Use physical and network security methods to protect the Web server.
7. The *Indexing Service* is a Windows 2000 service that indexes Web site content and other documents on a Windows 2000 computer so these items can be searched by users.
8. Certificate Services is a Windows 2000 Server service used to create, issue, and manage certificates on a Windows 2000 network. Certificate Services can be installed on any Windows 2000 Server computer, but can't be installed on Windows 2000 Professional computers.
9. Certification authority (CA)

Assessment Questions

1. **C.** Use the Add/Remove Programs application in Control Panel to install additional IIS components.
2. **A.** When you think Internet (or anything Internet-related), think TCP/IP.
3. **D.** Of the tools mentioned in the list, only Personal Web Manager can be used to configure a Web site.
4. **B**. Use Internet Services Manager to configure the Web site. You can't use Personal Web Services in this situation because Personal Web Services is a Windows 2000 Professional–only tool.

5. **B.** Virtual servers are just what you need in this situation. You can use Internet Services Manager to create them.
6. **B, C, E.** Placing Web content on FAT volumes doesn't provide security, but placing content on NTFS volumes does. Selecting Basic authentication also provides no security — user names and passwords are sent in clear text if this authentication method is selected.
7. **A.** Select Enterprise root CA if you're installing the first certificate server in the forest. This type of CA requires the use of Active Directory.
8. **A, C.** To perform the role of an EFS recovery agent, a user must have an EFS Recover Agent certificate, and must be designated as an EFS recovery agent in Group Policy.

Scenarios

1. The most likely cause of this problem is that you have configured NTFS permissions on the file, but have not granted the Web server's anonymous user account (`IUSR_`*`Server_name`*) permissions to access this file. To resolve this problem, assign the Web server's anonymous user account NTFS permissions to the file.
2. The most likely cause of this problem is that you have enabled IP address restrictions on the Web site. To resolve this problem, either remove the IP address restrictions, or add the IP address of John's home computer to the list of IP addresses explicitly granted access to the Web site.