3

Maintaining Security by Implementing, Managing, and Troubleshooting Service Packs and Security Updates

Terms you'll need to understand:

- ✓ Codec
- ✓ Certification Authority (CA)
- ✓ Trusted CA
- ✓ Systems Management Server (SMS)
- ✓ **hfnetchk**
- ✓ **qchain**
- ✓ Windows Update
- ✓ Windows XP Dynamic Update
- ✓ Certificate revocation list (CRL)
- ✓ Secure Sockets Layer (SSL)
- ✓ Microsoft Baseline Security Analyzer (MBSA)
- ✓ Software Update Services (SUS)
- ✓ Remote Installation Services (RIS)
- ✓ Slipstream

Concepts and techniques you'll need to master:

- ✓ Understanding the need for software updates, including the problems that are caused by updating or not updating
- ✓ Using the Microsoft tools (**hfnetchk**, SUS, and MBSA) to determine patching status
- ✓ Selecting and using Microsoft tools to update servers and clients
- ✓ Knowing how to install updated systems (by using slipstreaming and RIS, for example)
- ✓ Troubleshooting and resolving problems with attempted updates such as application incompatibilities, permissions problems, and update failure

Not long ago, system administrators had a choice about whether to update their systems. In many cases, they were safe in assuming that internal systems were not at risk. In many cases it was more beneficial to not update than to update because updates were plagued with unsolvable problems. "If it's not broken, don't fix it" was the rule.

Today, this is just not the case. Emerging statistics show that the majority of successful attacks are successful because they take advantage of a known vulnerability—for which there is a patch. Nimda, Code Red, and many versions of Linux SSL took advantage of these types of weaknesses.

The question today is not should you patch, but how are you going to patch, and how fast are you going to do it? Fortunately, many Microsoft tools can assist in solving the logistics of patching. To conquer this topic, you must know the tools (`hfnetchk`, Windows Update, SUS, and the SMS feature pack) and methods necessary to keep systems patched, and you must know how to troubleshoot the problems the patches may cause, and you need to understand the reasons tools may not work correctly.

Getting Your Patching Program Started

There are actually four processes involved in updating systems:

- Determining when updates are available
- Evaluating whether the updates are necessary
- Testing updates for your environment
- Updating systems

The first step in managing service packs and hotfixes is to know when they are needed. Whereas service packs fix multiple issues and are infrequently published, hotfixes are published as the need arises to patch existing vulnerabilities. To find out when fixes are necessary, you should subscribe to a hotfix notification service. For example, you can subscribe to Microsoft's Hotfix and Security Bulletin Service at `www.microsoft.com/technet/security/current.asp`.

When a notification is received, it should be evaluated and then, if approved, applied using some mechanism. Evaluation may consist of two phases—determining whether the patch is necessary and determining whether the patch is safe. You need to know whether the patch will cause problems.

Evaluation methods may include the following:

- *Do no evaluation*—You can blindly accept every proffered patch.
- *Wait for a while to see if others have problems with the patch*—This approach is often adopted by small businesses that cannot afford the testing time and systems needed for every hotfix.
- *Read Microsoft discussions and other resources to determine whether a system should be patched*—Some choices are obvious. For example, if the patch is for Microsoft SQL Server and a system is not running this service, the patch should not be applied. Other choices are not as obvious, and you must determine if the patch is necessary. For example, you need to consider what the patch does and whether its activities will prevent critical software from running or critical operations from occurring.
- *Select a time for patching*—It's a good idea to apply patches during idle time, especially if a reboot is necessary. You should evaluate whether there is a situation in which a patch is so critical that you must suspend activity and install the patch regardless of the consequences. Only the administrators and users of the systems can determine this, although management may need to be involved when downtime affects revenue-generating systems such as e-commerce servers.

After you decide that the patch is necessary, you should thoroughly and exhaustively test it to ensure noninterference with existing operations or other hardware/software conflicts. You should install hotfixes on test systems whose configuration mirrors that of the production machines. You can then test the systems for functionality.

After the patch has been tested, you must choose the appropriate way to update systems.

Windows XP Dynamic Update and Windows Update

Windows XP Dynamic Update is a service that runs only at the beginning of a Windows XP installation. Dynamic Update can be configured to automatically connect the Windows XP computer to the Internet and download all fixes and driver updates during installation.

The Windows Update service is an online service that can be used to update Windows computers with new utilities, drivers, and critical security updates.

Windows XP Dynamic Update

Dynamic Update is meant to provide a convenient way to obtain the latest fixes and newest drivers. You can select the option to use Dynamic Update during the Windows XP installation process. Obviously, an Internet connection is necessary for this. Administrators should consider the security issue here: Connecting a computer to the Internet during installation is not an industry best practice. In fact, best practice states that you should never do this.

Dynamic Update is not available by default on a computer that is installed via an unattended installation with an answer file. However, administrators can configure an installation to use Dynamic Update to download Dynamic Update packages to the corporate network from the Windows Update Catalog site. Thus, the update can occur from a safe, local network location instead of the Internet.

Windows Update

Windows XP can beconfigured to automatically and periodically contact the Windows Update site and download critical patches. Windows 2000 with Service Pack 3 or later can also be configured to contact the update site periodically. All Windows computers can also manually access the public update site, request evaluation, and approve downloads and installations.

The first time you connect a Windows system to the Windows Update site, a Web service control is downloaded and then used to scan the computer for needed updates. You can download new versions of the Web service from the Windows Update site.

The following are options for automatic updates:

- Download automatically and notify the user when the updates are ready to be installed.
- Notify the user when downloading and notify the user when the updates are ready to be installed.
- Turn off automatic updating.

Group Policy Control of Windows Update Technologies

In order for users to take advantage of the Windows Update service, they must have administrative privileges to download and install updates. You can use group policy to disable Windows Update services for all XP users, including other administrators. To do this, you must set the following policies that affect Windows Update:

- *User Configuration\Administrative Templates\Windows Components\Windows Update\Remove Access to Use All Windows Update Features*—You can select Enabled to cause all access to Windows Update features to be removed.
- *User Configuration\Administrative Templates\System\Configure Driver Search Locations*—You should select Enabled to search Windows Update for updates and then select Don't Search Windows Update.
- *User Configuration\Administrative Templates\Windows Components\Windows Media Player\Playback\Prevent Codec Download*—You should select Enabled to prevent downloads of updates.
- *User Configuration\Administrative Templates\Windows Components\Windows Messenger or Computer Configuration\Administrative Templates\Windows Components\Windows Messenger*—You should set Do Not Allow Windows Messenger to Be Run to Enabled. Note that if both the user and computer configuration settings are configured, the computer configuration settings will take precedence.
- *Windows Settings\Security Settings\Public Key Policy*—You should right-click Trusted Root Certificate Authorities and select Properties. Then you select Enterprise Root Certificate Authorities and add the CAs that are to be trusted. Doing this removes any currently trusted CAs in the trusted authorities store.

NOTE

Setting group policy to enter approved trusted root CAs removes the root CAs initially configured during installation. This could affect the functionality of the Windows system. Before using this choice, you should determine which certificates are essential to the operation of the clients you control. To fully understand the implications of making these changes, you need to understand Public Key Infrastructure (PKI) and how it is used in Windows. For more information, see Chapter 7, "Implementing and Managing PKI and EFS," and the resources mentioned in that chapter.

- *User Configuration\Administrative Templates\System\Windows Automatic Updates*—You should select Disabled.

EXAM ALERT

Windows XP uses the Windows Update service to search for drivers for Plug and Play devices if a new Plug and Play device is plugged in to the computer and there is not a local driver available. Windows XP's Windows Update service can also be configured to automatically search for updated drivers for existing devices, including printers. This feature can also be controlled via group policy.

Other Windows Automatic Technology Updates

Many Windows components are designed to automatically update. Although this is considered by some to be a boon—because security fixes can automatically be delivered—others feel that this can cause more problems than it solves.

Nevertheless, you need to know about these automation capabilities and how to manage them. The following technologies are also updated automatically:

- Media Player updates
- MSN Explorer updates
- Windows Messenger updates
- The Windows Help and Support Center
- Microsoft Update Root Certificates

Determining the Status of Service Packs and Security Updates

Two Microsoft tools are available to help determine the status of the service packs and security updates on Windows computers: Microsoft Baseline Security Analyzer (MBSA) and `hfnetchk`.

MBSA

MBSA is a GUI tool that can report the status of several security settings and uses a version of the command-line tool `hfnetchk` to determine the patching status of a specific machine or an entire network of machines. Reports can be archived, and notes in the reports explain the missing patches or point to Web-based repositories for further information and download. Used on a single machine, MBSA can serve as a diagnostic tool and can update the system. In the version of the tool that is available at the time of this writing, multiple machine updates directly from the tool are not possible.

MBSA also has a command-line version that you execute by typing `mbsacli.exe` at the command prompt. Table 3.1 describes the command-line switches that can be used with this command.

Table 3.1 mbsacli.exe Command-line Switches

Switch and Parameters	Description
/c <*domainname*>\\<*computername*>	Scans the named computer
/i <*xxx.xxx.xxx.xxx*>	Scans the computer at this IP address
/r <*xxx.xxx.xxx.xxx*> - <*xxx.xxx.xxx.xxx*>	Scans computers at any IP address in this range

(continued)

Table 3.1 mbsacli.exe Command-line Switches *(continued)*

Switch and Parameters	Description
/d <*domainname*>	Scans the domain
/n IIS	Skips Internet Information Server (IIS) checks
/n OS	Skips operating system checks
/n password	Skips password checks
/n SQL	Skips SQL checks
/n hotfix	Skips hotfix checks
/o %*domain*% - %*computername*%(%*date*%)	Specifies a filename for the output file
/e	Lists errors from the latest scan
/l	Lists all reports available
/ls	Lists reports from the latest scan
/lr <*reportname*>	Displays an overview report
/ld <*reportname*>	Displays a detailed report
/?	Gets help
/qp	Does not display progress
/qe	Does not display a list of errors
/qr	Does not display a list of reports
/q	Does not display anything
/f	Redirects output to a file

EXAM ALERT

An update of the MBSA tool has been released; however, Exam 70-214, "Implementing and Administering Security in a Windows 2000 Network," was written before this release, so this book comments only on the original tool. You should download the current edition of the tool and explore it, but remember that the exam questions were created before the tool was upgraded.

MBSA can be freely downloaded from Microsoft's site. The following sections discuss the requirements for running MBSA, how MBSA works, and how to use the reports that it provides.

MBSA Requirements

In order for MBSA to run, it must be installed on a Windows 2000 or Windows XP computer. It can, however, scan Windows NT 4.0 Service Pack 4 and above, Windows XP, and Windows 2000 computers. (Only local scans can be executed against a Windows XP Home Edition computer or a Windows XP Professional Edition computer using simple file sharing.) In addition, MBSA scans for problems with SQL Server, Microsoft Office, Windows Media Player, Exchange Server 5.5 and 2000, Internet Explorer (5.01 or later), and IIS (4.0 or later) if these applications are present.

The following are additional requirements for running MBSA:

- Internet Explorer 5.01 or greater must be installed, or you must have the XML parser.
- An XML parser (such as MSXML version 3.0, Service Pack 2) is needed. If a system is not running Internet Explorer 5.01 or greater, you need to download and install an XML parser. You can do this during setup.
- IIS common files are needed on the computer on which the tool is installed, if MBSA will be used to scan IIS computers.

In order to use MBSA to scan a computer, the computer must meet the following requirements:

- Internet Explorer 5.01 or greater must be installed.
- The user doing the scanning must have administrative privileges on each computer being scanned, whether the scan is local or remote.
- The server service must be running and Remote Registry Service must be running on Windows 2000 and Windows XP computers.

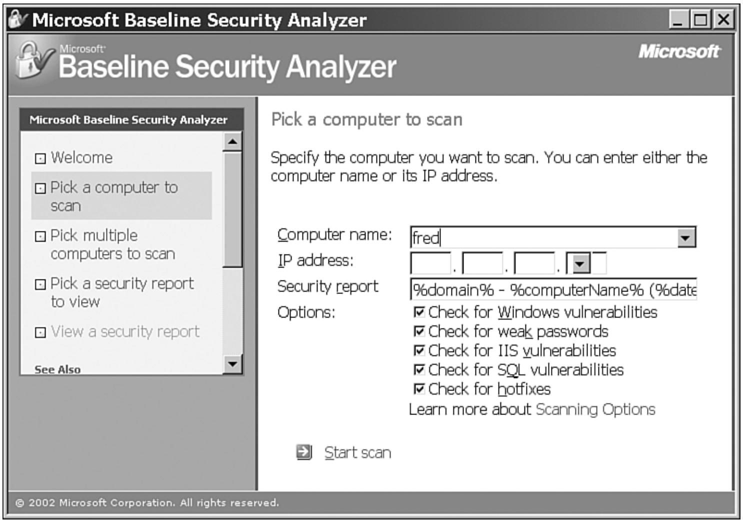
How MBSA Works

MBSA scans computers for common security misconfiguration problems and hotfix installations. It then reports the results. MBSA uses a custom version of `hfnetchk` for its hotfix analysis and downloads a current copy of the `mssecure.xml` file from Microsoft when it is run.

The following parts of the MBSA scan are optional and can be turned off in the interface prior to the scan:

- Windows operation system checks
- IIS checks
- SQL checks
- Hotfix checks
- Password checks

Figure 3.1 displays the MBSA options and shows how a computer can be selected for a scan.


Microsoft Baseline Security Analyzer
Microsoft
Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Start scan

Pick a computer to scan

Specify the computer you want to scan. You can enter either the computer name or its IP address.

Computer name: fred

IP address: . . .

Security report: %domain% - %computerName% (%date

Options:
☑ Check for Windows vulnerabilities
☑ Check for weak passwords
☑ Check for IIS vulnerabilities
☑ Check for SQL vulnerabilities
☑ Check for hotfixes

Learn more about Scanning Options

© 2002 Microsoft Corporation. All rights reserved.

Figure 3.1 MBSA options.

Scan reports are stored on the computer on which the tool is installed, in the `%userprofile%\Security Scans` folder. Each computer scanned produces its own report.

During the scan, vulnerability tests and security status checks are made (the items marked with asterisks (*) are critical checks):

- Tests for weak passwords by attempting to log on with a blank password, `password`, `PASSWORD`, the username, and the administrator name. This check notifies you of any locked out or disabled accounts.*
- Checks for missing service packs or hotfixes.*
- Checks for the number of members in the local Administrators group. If more than two are identified, this fact is listed.*
- Checks to see that all volumes use NT File System (NTFS).*
- Checks to see if autologon is enabled.*
- Tells you whether the guest account is disabled.*
- Checks the setting on restrict anonymous.*
- Checks to see if auditing is enabled.
- Checks the `services.txt` file (part of the MBSA program) and advises whether these potentially unnecessary services are running.

- Lists the shares available on the computer. It indicates that these shares exist even if file sharing has been disabled.
- Lists the Windows version.
- Checks Internet Explorer security zones and alerts to see if they differ from the defaults. (MBSA will note if your settings are different, even if your settings may be more secure.)
- Checks PowerPoint, Excel, Word, and Access for macros protection.
- Checks the version of Windows 2000 Server.
- Provides an overall security assessment in the form of a risk factor, such as Severe Risk or Low Risk.

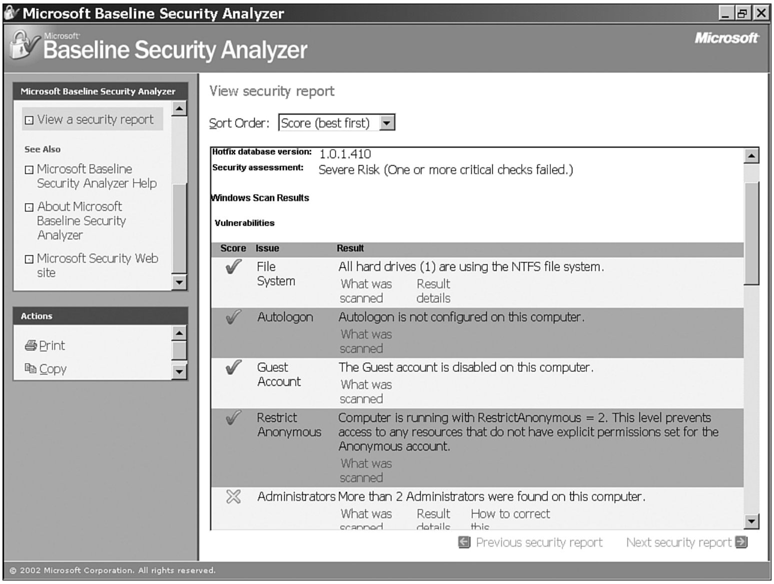
MBSA Reports

MBSA reports are used for several things, including the following:

- The overall rating may be used to identify systems that benefit most from security configuration. The higher the overall risk reported, the more work that needs to be done to secure them. You should use caution. You need to weigh the risk factor reported against the role of the computer. In most circumstances, a critical server should be dealt with before a user's desktop, even if MBSA gives the desktop a higher risk factor.
- Each vulnerability assessment can be explored for information on what was scanned, what the results were, and what to do to correct the problems that might show up in the reports. Often, explanations and pointers to further reading allow exploration of the topic. For a small business or for a user with a single desktop system, this might be the only exposure to security issues; therefore, the explanation and steps to improve security are valuable.
- Notification of missing hotfixes is a good indicator of the hotfixes that need to be downloaded and installed. The tool does not provide a way to automate hotfix application updates to multiple systems or to easily apply multiple hotfixes. However, you can use it to download and install one hotfix at a time. The tool identifies each missing hotfix and provides a link to the security bulletin and download path.
- Because scans can be run remotely and reports can be stored at a central location (they are stored on the computer the scan is run from), they can provide a picture of security across a domain or network without requiring a visit to each individual machine. This audit does not need to occur at the same time that the scan is run.

- ➤ If old reports are kept, improvement over time can be noted, although there is no automated way to compare report results.

Figure 3.2 displays a portion of a report that indicates the major security checks and the options available for discovering what was scanned and what to do about the results. In this example, the system failed one or more of the critical security checks, resulting in a rating of Severe Risk.


Microsoft Baseline Security Analyzer
Microsoft Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Actions
Print
Copy
© 2002 Microsoft Corporation. All rights reserved.
Previous security report
Next security report

View security report

Sort Order: Score (best first)

Hotfix database version: 1.0.1.410
Security assessment: Severe Risk (One or more critical checks failed.)

Windows Scan Results

Vulnerabilities

Score	Issue	Result
✓	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
✓	Autologon	Autologon is not configured on this computer. What was scanned
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict Anonymous	Computer is running with RestrictAnonymous = 2. This level prevents access to any resources that do not have explicit permissions set for the Anonymous account. What was scanned
✗	Administrators	More than 2 Administrators were found on this computer. What was scanned Result details How to correct this

Figure 3.2 An MBSA Severe Risk report.

hfnetchk

The Microsoft Network Security Hotfix Checker, `hfnetchk`, is a command-line utility that can be used to determine the patch status of a Windows computer. It can be used to examine Windows XP, Windows 2000, Windows NT 4.0, Microsoft SQL Server, and IIS 4.0 and 5.0. It does not display hotfix information for Exchange Server or other Microsoft products. The requirements for running `hfnetchk` are the same as those for running MBSA.

NOTE

hfnetchk was developed by Shavlik Technologies LLC (**www.shavlik.com**), which also produces a GUI version and an advanced command-line version of the tool. Documentation on the Shavlik site can help you understand how to use **hfnetchk**.

How hfnetchk Works

hfnetchk uses a combination of approaches to determine whether a security hotfix has been applied. It searches registry keys, checks file versions, and compares file checksums. If the information is missing or incorrect, hfnetchk reports the fix as not being installed. If there is a mismatch (for example, a registry key exists, a file checksum is incorrect), hfnetchk says that the hotfix is not installed and perhaps gives a warning status. In some cases, hfnetchk cannot determine whether a fix has been applied. The information may not be accessible, the fix may be a configuration, or there may be some other action that the tool cannot reliably check. These items are reported as note messages. In this case, a note explains the issue or points to a solution, which in most cases allows the administrator to determine patch status.

When you run hfnetchk, the tool automatically downloads the mssecure.xml file from Microsoft. This file is kept up-to-date and indicates the current hotfix requirements. The date on this file is displayed when you run hfnetchk.

You can run hfnetchk on isolated computer systems (those not connected to the Internet) or on systems that you do not want to access the Internet for this purpose by downloading a copy of the mssecure.xml file to another computer, placing a copy on the isolated computer, and using the -x switch. When hfnetchk is run using the -x switch, it does not attempt to access the file on Microsoft's site; it instead uses the local copy of mssecure.xml.

By default, hfnetchk requires access to the Internet in order to access information on the most recent updates. However, a copy of the update file can be downloaded from Microsoft from a computer that you use to access the Internet and then used on computers that do not have Internet access. The mssecure.xml file can reside on the local computer system, a network share, or an intranet Web site.

To use a local network share, you use this command:

```
hfnetchk -v -z -x s:\security\mssecure.xml
```

In this command, s:\security\mssecure.xml is the local path to the file.

To use an intranet site, you use this command line:

```
hfnetchk -v -z -x http://mysite.abc/mssecure.xml
```

In this command, http://mysite.abc/mssecure.xml is the URL where you have stored the mssecure.xml file.

Many other switches are available, as listed in Table 3.2.

Table 3.2 hfnetchk Switches

Switch	Action
-v	Views the specific reason the patch is considered not found
-z	Disables registry checks
-fh	Reads a list of computer names and performs a scan against multiple computers
-fip	Uses a list of IP addresses instead of computer names
-u	Supplies a username for remote computers
-p	Supplies a password
-x	Seeks the **mssecure.xml** file locally
-s 1	Stops note messages from being displayed
-s 2	Stops warning messages from being displayed
-f	Redirects the **hfnetchk** output to a file

The following command line, for example, uses a local copy of `mssecure.xml` and puts the output in tab-delimited form in the `scan.txt` file. It also disables registry checks and lists the specific reason for the failed check:

```
hfnetchk –v –z –x mssecure.xml –f scan.txt -otab
```

NOTE

You can download the signed **mssecure.xml** file from **http://download.Microsoft.com/download/xml/security/1.0/nt5/en-us/mssecure.cab**.

Or you can get the uncompressed form of the file from **www.microsoft.com/technet/security/search/mssecure.xml**.

A digitally signed, compressed **.cab** file is not decompressed by **hfnetchk** unless it is signed by Microsoft.

hfnetchk Requirements and Common Usage Mistakes

When `hfnetchk` was first released, a large number of problems were reported. Fortunately, most of them could be traced to two factors: Administrators were not accustomed to command-line tools, and administrators did not read the documentation. Using and troubleshooting `hfnetchk` is very simple if you understand these issues. First, the administrator must understand that clicking the executable in the GUI does not run the program. The administrator must use the command line and add switches and the appropriate values. Second, if the administrator reads the documentation, he or she will find that several requirements must be fulfilled. Understanding these requirements and making sure they are met will prevent most common problems from occurring. Finally, reading the report and the documentation it lists for further guidance will answer many common questions. Table 3.3 lists `hfnetchk` requirements and common problems as well as their resolution or where to find additional information.

Table 3.3 hfnetchk Problems and Requirements

Problem or Requirement	Notes or Resolution
hfnetchk might not run.	**hfnetchk** does not require Administrative privileges to run the command locally. However, use of the command on remote computers requires administrative privileges on each remote computer.
After you run **hfnetchk**, two entries on the report may include the same bulletin.	Bulletins can identify two or more patches to be installed. **hfnetchk** treats each patch separately and lists the relevant bulletin more than once if more than one bulletin-related patch is missing.
When **hfnetchk** is run against a pristine installation of Windows 2000 (with no service pack), many patches listed on Microsoft's Web site are not listed as missing.	A service pack must be installed before post–service pack patches are listed as not found.
If hotfixes are superceded by newer fixes, and the newer fix is installed, the old hotfixes do not show up as missing.	You can use the **–history 2** switch to display all hotfixes, even those that have been superceded.
hfnetchk may run locally, but it fails to scan a remote computer.	To scan a remote computer, **hfnetchk** must have NetBIOS access to the server service. On computers running Windows 2000 and later, NetBIOS access to Remote Registry Service is also necessary.

Installing Service Packs and Updates

There are several options for manually applying service packs and hotfixes. You can install service packs in the following ways:

- Through group policy
- By using Microsoft SMS
- By slipstreaming content to a network installation share of the I386 folder
- During a RIS installation
- Via custom scripts

You can also apply hotfixes by using most of these methods.

Security patches come with **hotfix.exe**, **hotfix.inf**, and the replacement files. **hotfix.exe** installs the patch, and **hotfix.inf** contains instructions for modifying registry settings and other files. You might need to delete the **hotfix.*** files when using nonmanual methods to perform an update. In addition, the manual installation checks for the service pack status of the local machine and the language it uses, and it warns the user. Automated installations may not perform these functions. You need to pay special attention to instructions for automated hotfix application.

A typical hotfix name is in the format **Q12345_w2k_sp2_x86_en.exe**, where:

- **12345** is the knowledge base article that describes the problem that the solution resolves.
- **w2k** is the operating system the fix is for.
- **sp2** is the service pack version in which the fix will be included.
- **x86** is the processor type on which the fix can be installed.
- **en** is the language version of the hotfix.

You should always examine and interpret the hotfix name before applying a hotfix. Applying or attempting to apply a hotfix to the wrong computer, with the service pack level, or with some other mismatch could result in undesirable effects. For more information, see the section “Troubleshooting the Deployment of Service Packs and Updates,” later in this chapter.

Using Group Policy to Install a Service Pack

Group policy software can be used to push service pack installations to existing client computers. An `update.msi` file is necessary for this. It was necessary to download the `update.msi` file for Service Pack 1; this file can be found in an expanded Service Pack 2 or Service Pack 3 executable. To expand the service pack, you use the following command:

```
win2kspx -x
```

In this command, *x* should be replaced by the number `2` or `3`, to indicate Service Pack 2 or Service Pack 3, respectively.

To create the group policy, you follow these steps:

1. Expand the service pack into a folder and share this folder.
2. In the Active Directory Users and Computers console, right-click the organizational unit (OU) where you want to create the group policy, and then click Properties.
3. Make a new group policy object (GPO) and edit it.
4. Select Computer Configuration, Software Settings, Software Installation and make a new package.
5. Browse to the `update.msi` file in your shared distribution folder. If the shared folder is on the domain controller, don’t browse to the local path. Make sure you locate it through its network path. (If you use a

local path on the domain controller, the workstation will not be able to find it.)

6. Modify the default method to enable the option Uninstall This Application when It Falls Out of the Scope of Management. This allows the uninstallation of the service pack by moving the computer from this OU.

Using SMS for Service Pack Installation

The creation of an SMS package to allow the installation of service packs is beyond the scope of Exam 70-214. However, you need to know that this is possible and that it involves the following steps:

1. *Importing the package definition file for the service pack*—A *package definition file* is a specially formatted file that contains the information necessary to create the SMS package. When you import this file, SMS creates the package automatically. The package file can then be modified for the specific installation.

2. *Providing the path to the service pack source files*—One of the modifications to the package file must be pointing SMS to the location for the intended installation files. Service pack files should be copied to their own network distribution share (for example, using `xcopy D:\ e:\w2ksp2.exe /x`) and then extracted (using `w2ksp2.exe /x`).

3. *Distributing the SMS package to the distribution point—Distribution points* are shared network folders where SMS clients can access the package.

4. *Creating the advertisement to notify SMS clients about the service pack*—The advertisement is the offer to the clients to let them know that the package is available. SMS allows you to select some or all clients to advertise the package to.

Slipstreaming

Slipstreaming is the process of adding service pack files to the contents of an accessible `I386` folder that contains the same contents as the `I386` folder from the original Windows installation CD-ROM. The updated `I386` folder can reside on the computer's hard disk (this is not recommended) or on a network distribution share, or it can be burned onto a bootable CD-ROM. Windows 2000 computers installed from the updated folder already have the service pack installed, provided that the updates are incorporated into the delivery point.

If the path to the service pack `update.exe` is `D:\I386\update\update.exe` (as it might be if you had the Windows 2000 installation CD-ROM in the `D:` drive) and the installation share is `C:\I386`, then this is the command you use for slipstreaming:

```
D:\I386\update\update.exe -S:C:\I386
```

Installing Hotfixes During Installation

Bringing up machines in a patched state is always desirable. To add Windows hotfixes during the installation process, two techniques are available: using `cmdlines.txt` and using `svcpack.inf`.

Using cmdlines.txt to Apply Hotfixes

To apply hotfixes during an unattended installation, you use the `cmdlines.txt` file. The following steps are necessary:

1. Create a distribution folder.
2. Create the answer file `unattend.txt` by using the Setup Manager tool. `unattend.txt` will contain any computer-specific information needed by the commands in the `cmdlines.txt` file.
3. Create the `cmdlines.txt` file by using the Setup Manager tool. `cmdlines.txt` is a file that contains the commands that would run during the GUI installation. These commands can be hotfix installation commands as well.
4. Add the `I386` folder from the Windows installation CD-ROM to the distribution folder.
5. Add the `unattend.txt` and `cmdlines.txt` files to the `\I386\$OEM$` subfolder.
6. Add hotfix executable files to the `\I386\$OEM$` subfolder. (Hotfix files are named *`six-digit-number`*`.exe`, where the six-digit number is the number assigned to the hotfix.) Hotfix files can be downloaded from Microsoft's Web site.
7. Add lines to the `cmdlines.txt` file, which is a file that must be available if a Windows automated installation requires the running of different code (for example, installation of applications or addition of hotfixes) after the operating system is installed. For example, to install the hotfix `Q123456.exe`, you use this line in the `[Commands]` section of the `cmdlines.txt` file:

   ```
   "Q123456 /q"
   ```

Using svcpack.inf to Install Hotfixes

When you use svcpack.inf to install hotfixes during Windows installation, you can use the Windows 2000 integrated (that is, Windows 2000 and service pack) installation CD-ROM to install the post–service pack hotfixes. To do so, you follow these steps:

1. Share the intended distribution drive folder.
2. Create an \I386 folder within this share.
3. Use xcopy to copy files and folders from the integrated Windows 2000/service pack CD-ROM to the I386 folder.
4. Open the I386\dosnet.inf file with Notepad or another text editor.
5. Locate the uniproc line in the [OptionalSRCDirs] section of the dosnet.inf file. After this line, create a new svcpack line. The section should look like this:

   ```
   [OptionalSRCDirs]
   uniproc
   svcpack
   ```

6. Save the changes and close dosnet.inf.
7. Create an I386\svcpack folder.
8. Copy each hotfix executable to the I386\svcpack folder. You must rename the hotfix files to use the 8.3 naming format (for example, Q*xxxxx*.exe).
9. Expand each hotfix to a unique temporary location by using the *filename -x* command. When you're prompted for a folder, enter the name of the hotfix (such as Q*xxxxx*).
10. Delete from the I386 folder the files that you want to replace with service pack or hotfix files.
11. Copy the sp3.cat catalog file to the network distribution folder if the sp3.cat file is a later version than the one that's already in the distribution folder. You can use the catver.exe tool to determine the version.
12. Copy the hotfix files from the temporary folders to the network distribution folder. (If hotfix files exist in a subfolder, you need to make sure to copy them to a folder of the same name that you have created as a subfolder of the I386 folder.) (Files in the symbols subfolder do not need to be copied, nor do the hotfix.exe, hotfix.inf, or spmsg.dll files.)
13. Repeat steps 11 and 12 for each hotfix.

14. Delete the `I386\svcpack.inf` file.

15. Create a new `svcpack.inf` file with a text editor and include the following lines:

```
[Version]
signature="Windows NT$"
MajorVersion=5
MinorVersion=0
BuildNumber=2195
[SetupData]
CatalogSubDir="I386\svcpack"
[ProductCatalogsToIinstall]
sp3.cat
[SetupHotfixesToRun]
```

16. For each hotfix, add a new line in the `[SetupHotfixesToRun]` section of the file, using the following format:

    ```
    Q##### /q /n /z
    ```

    Add the following line at the end of the file:

    ```
    qchain.exe
    ```

17. Download the free `qchain` utility from `www.microsoft.com/technet/security` and copy it to the `I386\svcpack` folder.

18. Run Windows 2000 Setup.

19. Test the installation. To determine whether hotfixes are installed, look for the hotfixes to appear in the Add/Remove Programs tool in the Control panel and an uninstallation folder to appear for each hotfix in the `%SYSTEMROOT%` folder. The `setupapi.log` file should also have entries.

Using RIS

You can use RIS to automatically install the Windows 2000 and XP operating systems. If they are appropriately configured, modern PCs can simply boot, locate a DHCP server to obtain an IP address, connect to the network, and contact a boot server to install the operating system.

Exam 70-214 does not cover RIS basics. You do need to thoroughly understand the RIS process, including how to set it up, make it work, and troubleshoot network and configuration issues. However, Exam 70-214 concentrates on how RIS can be used to install a Windows computer with the relevant service pack and hotfixes.

Adding Service Packs via RIS Installation

To automate the installation of service packs during a RIS installation, you follow these steps:

1. Edit the unattended installation file appropriately for unattended installation of the computer.

NOTE

When RIS is installed, all the default folders are created, as are the files needed for creating RIS installations. Templates are provided for files that you must build. **ristndrd.sif** is the name of a sample RIS template that could be used to create your own unattended installation file, but your file can have its own name, as long as the syntax is correct and the **.sif** extension is used. Details of this file can be found in the document "Remote Installation Services (RIS)," at **www.microsoft.com/technet/prodtechnol/windows200serv/deploy/depopt/remote.asp**.

2. Locate the `[GuiRunOnce]` section of the unattended installation file. Anything you list here is automatically placed in the installed computer's `RunOnce` registry key. A RIS Windows setup automatically performs an administrative logon after installation, and thus anything in the `RunOnce` registry key will run.
3. Copy the service pack's `update.exe` program to an accessible network share. In the example shown in step 4, this program exists in the `sp` folder beneath the *`server\share`* folder.
4. Call `update.exe` by placing the two commands in the following code in the `[GuiRunOnce]` section:

   ```
   net use n: \\server\share password /USER:username /persistent:no
   N: \sp\update.exe –u
   ```

   The `-u` switch allows the service pack to be installed in unattended mode. No user intervention is necessary; however, status messages will display onscreen.
5. Save the file.

Adding Hotfixes by Using RIS

You might want to evaluate whether the time needed to keep the unattended installation file up-to-date and the RIS server updated with current post–service pack fixes is necessary depending on your current patching strategy. Although it is desirable to have each newly installed computer join the production network thoroughly up-to-date, if your patching process automatically and regularly scans network computers, determines patch status, and applies patches, then this might be sufficient in your environment. You should carefully assess the risk and determine the best security practice for your organization.

To have RIS installations apply hotfixes, you must do the following:

- Ensure that patches reside on an accessible network share.
- Configure RIS to install the appropriate service pack.
- Add script lines to the `[GuiRunOnce]` section of the unattended installation file. Examples of appropriate lines can be found in the "Using Custom Scripts" section of this chapter.

Using Custom Scripts

In many environments, using existing tools to update computers is not possible. In very small environments, for example, use of SMS or even SUS would be overkill and would incur unwelcome expense. In other environments, where SUS is a welcome tool for patching maintenance, there are still other areas that require help. For example, SUS does not provide a way to patch Microsoft Exchange or to update user files, applications, scheduled jobs, and so on.

The solution, of course, is to script these tasks. Batch files, or scripts, require knowledge of the applicable switches. Switches for the `hotfix.exe` hotfix installation file, `hfnetchk`, `update.exe`, application-specific update programs, and other tools help you build appropriate scripts. In time, you might develop a library of appropriate scripts and batch files to automate their use via the AT utility or the Task Scheduler.

A tutorial on scripting is beyond the scope of Exam 70-214, but knowledge of how to use the `hotfix`, `qchain`, and `hfnetchk` commands is not. Switches and/or their use for the `hotfix`, `qchain`, and `hfnetchk` commands are described in the following sections. Other switches and command syntax are listed in other sections of this chapter where commands and tools are described.

The hotfix Command

The switches for the `hotfix` command are listed in Table 3.4. In addition to selecting switches appropriate to your needs, you need to remember to make sure you use the `hotfix -m` (unattended mode) switch in a script because installations might be scheduled to run unattended.

Table 3.4 hotfix Command Switches

Switch	Description
-y	Uninstalls the hotfix
-f	Forces applications to close at shutdown
-n	Does not create an uninstall directory
-z	Does not reboot when the update completes
-q	Uses quiet mode with no user interface
-m	Uses unattended mode
-l	Lists installed hotfixes

The qchain Command

Although you can install multiple hotfixes at once by running a prepared batch file, the probability for inappropriate installations of DLLs is possible. This is because of the way information about necessary files is managed by the update process. If an update that requires a reboot is installed and the system is rebooted before another update is applied, all is well. However, if updates are chained in a batch file with only a final reboot, it is possible that the incorrect versions of files are installed or that required updates will not occur.

NOTE

Use of **qchain** is not necessary after Windows 2000 Service Pack 3 or with Windows XP. This is because the hotfix process has been changed so that file versions cannot be incorrectly installed.

To resolve this issue and allow multiple updates to be installed, Microsoft supplies the `qchain` utility. The following is an example of a `qchain` batch file:

```
qxxxxx_w2k_sp2_x86_en.exe -z -m -q
qxxxxx_w2k_sp2_x86_en.exe -z -m -q
qxxxxx_w2k_sp2_x86_en.exe -z -m -q
qchain \\name\logs\%computername%_qchainlog_0x.txt
shutdown /l /r
```

The `qchain` command includes the network location of a logfile in which to log `qchain` results and includes a unique computer name (the computer name of the computer on which the updates occur). Thus, a centralized location for logs of updated systems can be managed. In the `qchain` statement, ***name*** indicates the name of the central computer, and *`logs`* indicates a share on that computer.

The `shutdown` command shown in this example is from the *Windows 2000 Server Resource Kit*, and the provided switches include `-l` (logoff) and `-r` (clean shutdown and restart).

> When a hotfix installation is run, information on the file to be updated is placed in the pending file rename queue, to be replaced after the restart. If the computer is not restarted, the pending file rename queue is overwritten by the next hotfix. If different versions of the file are listed, the wrong version might get updated. **qchain** cleans the pending file rename operations key in the registry; this guarantees that the latest version of the file is installed after a reboot. **qchain** is not necessary on machines that have Service Pack 3 or later installed.
>
> If you suspect that a version of an updated file is incorrect, you can use the **qfecheck.exe** utility to verify the installation of Windows 2000 hotfixes.

Using SUS

SUS is a new, free tool provided by Microsoft to assist in patch management. It is targeted at the environments that have 50–500 computers.

Using Windows Update services on corporate computers is not a valid option for most businesses. Users would require administrative privileges, or administrators would have to spend extra maintenance time with user desktops. In addition, there is no built-in way to approve some updates while disallowing others. There's no centralized control, and there is no way to pretest before updating. Windows SUS is designed to solve these problems.

SUS is installed on a server on the local network, and it downloads critical updates to a repository on the server. After administrator approval, the updates can be delivered to the user systems. User systems can be pointed to the SUS server, instead of to Windows Update, for updating.

Benefits of SUS include the following:

- *Administrator-controlled synchronization service on the local network*—You have a choice of manual or scheduled synchronization with Microsoft.
- *Intranet-hosted update server*—Multiple SUS servers can be used and can synchronize with intranet servers or a Microsoft server.
- *Administrator control over updates*—Until downloaded updates are approved on the SUS server, they are not available to users.
- *Email notification service*—The administrator is advised of new updates.
- *Statistics published to a log*—Statistics on updates that have been downloaded and whether they have been installed can be published to a preferred Web server (a server other than the SUS server) log.

- *Automatic updates*—You can automatically check for updates published on Microsoft's server. You can do this locally on a configured schedule.
- *Multiple SUS servers*—A SUS server can be pointed to another SUS server instead of to Windows Update.
- *Actual update downloads or client downloads of approved updates from the Internet*—Large networks with geographical spread might enjoy using Internet downloads, whereas systems on isolated networks might benefit from using downloads placed on the SUS server.
- *Administration via HTTP or HTTPS*—A browser can be used to administer SUS remotely. To improve security, the IIS can be appropriately configured for HTTPS.
- *Automated client updates*—Automated client updates can be done without administrative intervention on the client, or they can be set to require administrative intervention on the client.

SUS Requirements

In order to use SUS, both client and server software must be installed. Server and client software can be downloaded from Microsoft. Client software is a part of updated service packs.

In order to run SUS, a server must meet the following requirements:

- The server must be running Windows 2000 with Service Pack 2 or later.
- IIS must be enabled on the server.
- Internet Explorer 5.5 or later must be installed on the server.
- IIS should only host SUS because the security tool URLScan is used to lock down the server. Only the World Wide Web portion of IIS and its dependencies should be running. FrontPage Server extensions are not required. WebDAV, Internet printing, and the indexing service are turned off. Session state is disabled. Active Server Pages (ASPs) cannot create a session for each user who accesses an ASP program, and ASP scripts cannot store information in the session object or use the `session_onstart` or `session_onend` events.
- The server cannot be running Active Directory services or Microsoft Small Business Server (SBS).
- The server should be running most updated patches before SUS is installed.

- The minimum server requirements are Pentium III 733MHz with 512MB of RAM, a network adapter, and an NTFS partition with at least 100MB available for installing SUS and at least 6GB storage for the update if updates are to be stored locally. (This configuration can support 15,000 client machines.)

Client systems can run any of the following:

- Windows 2000 Professional Service Pack 2 or later.
- Windows XP Professional or Windows XP Home; Windows XP systems must update to Service Pack 1 in order to use automatic updates with SUS.
- Windows 2000 Server Service Pack 2 or later, Windows 2000 Advanced Server Service Pack 2 or later, or Windows 2000 Datacenter Server Service Pack 2 or later.

Windows NT is not a supported client for SUS. You cannot patch Windows NT by using SUS.

The SUS Setup Process

Installation of SUS on the server and configuration of clients to use it are straightforward. The following presetup process should be followed for the server installation:

1. Physically disconnect the server from the network.
2. Install Windows 2000. Do not install antivirus software, or make sure it is turned off during the installation of service packs, hotfixes, and SUS.
3. Install IIS. Also, run the IIS Lockdown tool before you reconnect the client to the network. IIS Lockdown helps to protect IIS by removing vulnerabilities.
4. Install the latest service packs, security rollup, and any security-related patches. There is no need to install the Microsoft Security toolkit because it is installed during SUS installation.

A local administrator can configure SUS. Configuration consists of setting the following:

- Whether update files are hosted on the SUS server or downloaded from the public Windows Update (Microsoft's) servers

- Proxy server information
- Options for handling approved content
- A list of client languages to support

In addition, if updates are not automatically synchronized, you should subscribe to the update alert service so that new updates can be manually downloaded. Finally, regular maintenance (which is restricted to local administrator access) includes the following:

- If synchronization is manual, maintenance should include downloading new updates as they are announced.
- Before updates can be made available for clients, an administrator must determine and approve the content to be published to computers running automatic updates.
- The server status and logs should be monitored.

The client software must also be installed (or obtained by installing the appropriate service pack: Windows 2000 Service Pack 3 or Windows XP Service Pack 1) on each client computer. Client installation and configuration consists of the following:

1. Installing the client. If Service Pack 3 has been loaded, the client is already available.
2. Restarting the computer.
3. Configuring the client to use SUS. Instructions for performing this step are detailed later in this chapter, in the section “Configuring Update Policies in SUS.”

NOTE

You can download the SUS client at **www.microsoft.com/downloads/details.aspx?FamilyId=A7AA96E4-6E41-4F54-972C-AE66A4E4BF6C&displaylang=en**.

How SUS Works

When updates are available, the following technology comes into play with SUS:

- SUS checks for a digital signature on files.
- Each client is scanned to determine the applicability of the update.

- The background intelligent transfer service (BITS) is used for background download. BITS, which is included with Windows XP, uses only idle bandwidth. The automatic update installer (or Service Pack 3) installs BITS for Windows 2000 systems.
- Windows Update technologies automatically batch updates so that if restarts are necessary, only one restart is required.
- The process can be configured via group policy, logon scripts, and registry keys.

Server processes include reliance on back-end technology used by the Microsoft Public Windows Update since mid-1998. In addition, the synchronization process validates the digital certificates; if the package is not from Microsoft, it is deleted. At all times, updates must be approved before they are made available for download by clients.

The following steps occur in the server synchronization process:

1. The SUS server connects to public Windows Update service and downloads content update *metadata* (that is, information on updates that are available for download).
2. SUS validates the metadata package for digital certificate.
3. SUS opens the metadata package.
4. SUS compares the metadata package information with its local copy and identifies new and duplicate files. The following actions are performed, depending on the differences found:
   - If a previous available update has been removed from public Windows Update service, it is revoked from the SUS server. Client machines are no longer offered the previously offered update.
   - If a previously available update has had files updated, files are automatically updated on the server. (Note that this type of update may be auto-approved or unapproved, depending on settings set by the administrator.)
   - If the server includes synchronization of update files (versus just metadata), new files are downloaded to a prespecified location.
   - If a previously downloaded file is missing from the intranet location, a new copy is downloaded.
   - If a file specified in the metadata cannot be downloaded, the associated metadata is removed from the list of *xxx* that can be approved for client downloads.

5. When changes are complete, if SUS is configured for manual synchronization, the success or failure is logged to a synchronization log.
6. If SUS is configured for automatic, scheduled synchronization and it fails, an attempt to resynchronize is made 30 minutes later. SUS tries three times by default. Administrators can configure the number of retries. Successful synchronization is logged.
7. Updates need to be approved before they are made available to computers running the automatic update client. If a fix is dependent on the installation of a previous fix, these dependencies are displayed, and all must be approved together, or none are available.

The synchronization logfile is always updated during synchronization, and all events are recorded. The following are some possible events:

- *Unable to connect*—The client can't connect to the update service.
- *Install ready—no recurring schedule*—Downloaded updates are listed. To install them, the administrator needs to log on and use the notification area.
- *Install ready—recurring schedule*—The download time and the date and time of projected installations are listed.
- *Install success*—Successfully installed updates are listed.
- *Install failure*—Updates that did not install are listed.
- *Restart required—no recurring schedule*—To complete the installation, the computer must be restarted.
- *Restart required—recurring schedule*—The computer will be restarted within 5 minutes. New downloads cannot be searched for until the system reboots.

EXAM ALERT

SUS cannot be installed on a domain controller or on Microsoft Small Business Server. SUS can only be used to install updates, not service packs, and you cannot add your own updates.

Configuring SSL to Secure SUS

Because administration on SUS can be performed via a browser, it's important to consider securing the communication between the administrator's browser and the SUS server. You can do so by configuring SUS to use SSL. The details for performing the actions listed here are described in Chapter 5, "Configuring and Troubleshooting Authentication for LANs, Internets, and Intranets," and in Chapter 7.

Configuring Update Policies in SUS

An automatic update policy can be written to perform a scheduled installation at a certain time every day. Automatic updates for servers are often scheduled for the weekend. Three possible responses can occur:

- If a local administrator is logged on, an update notice is displayed and they either allow the update or delay the update (which is then automatically rescheduled for the next day). The local administrator cannot deselect any updates; he or she can only delay them. The local administrator can delay the installation or resume the process at any time.
- If a user who is not an administrator is logged on, or if the computer is running but no one is logged on, the update is automatically installed. If a restart is necessary, a five-minute warning is given to allow a user to save files and log off.
- If the computer is turned off, the update is not installed.

The group policy settings for automatic updates are provided with the SUS installation package in the policy template file, `wuau.adm`. When the `wuau.adm` template file is added to the Group Policy Editor, settings are found under Computer Configuration, Administrative Templates, Windows Components, Windows Update. The installation behavior that can be specified is the same as that in the manual, computer-by-computer settings. In a non–Active Directory environment, the local group policy can be configured or registry settings can be set to configure automatic updates.

Using the SMS 2.0 SUS Feature Pack

Just as SMS can be used to deploy a service pack or install software, the SUS Feature Pack can be used to audit, distribute, track, and manage patching of Windows systems. The Feature Pack requires SMS 2.0 (Service Pack 4 is recommended, but the SMS SUS Feature Pack also supports Service Pack 3).

SMS provides computer and software inventory and scheduling of the deployment of updates. It also monitors the update process and targets updates according to system inventory (that is, in Active Directory or in manually created computer groups). Feature Pack tools, including the following, add software management features:

- *Security Update Inventory Installer*—This tool creates an inventory of applicable and installed security updates for client computers. It has three main components:
    - A Security Update Inventory Installer that builds the package, collection, and advertisement necessary to deploy
    - The Security Update Inventory tool, which uses MBSA and the Security Patch Bulletin catalog (`mssecure.xml`) to scan clients
    - A Security Update Synchronization tool that checks the Microsoft downloads site, looking for the new update bulletin catalog, and sends the latest version of the catalog to client computers
- *Office Update Inventory Tool*—This tool performs similar tasks (scans clients to determine necessary changes) for Office.
- *Distribute Software Updates Wizard Installer*—This tool performs software update distribution tasks such as analyzing update status for clients, providing a method for reviewing and authorizing updates, downloading updates, building packages and advertisements, distributing update advertisements, and deploying the Software Updates Installation Agent to clients. The Software Updates Installation Agent evaluates updates against missing and previously installed updates on clients.

Troubleshooting the Deployment of Service Packs and Updates

In a perfect world, the tools and methodologies discussed in this chapter are smoothly implemented and always work. Of course, in the real world, things do not always work as expected, and sometimes troubleshooting skills are necessary. Specific errors, issues, and steps to resolve issues are described in the sections that follow.

Troubleshooting SUS

Errors and issues related to SUS are outlined in Table 3.5. The associated cause and a possible resolution are provided for each issue.

Table 3.5 SUS Issues

Error or Issue	Cause	Resolution
Event ID 7024, server-specific error 2147944102. BITs does not start on Windows 2000 Server with Terminal Services (TS). After you install the automatic updates version 2.2 client on a Windows 2000 computer that has TS installed, BITS doesn't start and does not download the job that was passed to the service.	TS is set to start automatically. If this service is disabled, BITS does not start.	Remove the TS, or reset the service so that it starts automatically.
The automatic update client does not seem to have performed a detection cycle.	Unknown.	Force a detection by running **gpedit.msc** to configure the SUS server location. Configure the intranet Microsoft Update Service Location policy. Set the automatic updates policy to Not Configured. After setting the automatic updates policy to Not Configured, you can turn the service on and off by using the Control Panel. Start the tool in the Control Panel or use the Automatic Updates tab in Windows XP, set the option as desired, clear the Enable Automatic Updates check box, and then click Apply to apply the change. Within a few seconds, click to enable automatic updates and then click OK to force a detection cycle. Verify the changes by checking the registry key **HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUPdate\Autoupdate**.Verify that the **AUState** value is **2**; check the **DetectionStartTime** value, which should be approximately the time of the last used automatic updates. The value is deleted after the detection cycle occurs (5 to 10 minutes). Finally, view the logfile for entries.

(continued)

Table 3.5 SUS Issues *(continued)*

Error or Issue	Cause	Resolution
The automatic updates client does not detect approved updates from SUS.	The client is unable to resolve the name of the server and/or the client does not receive policy settings.	First, look for an entry like **2002/05/02 17:38:42:22:38I.42 Success IUENGINE Querying Software UpdateCatalog from http://*servername*/*autoupdate*/*getmanifest*.asp** in the **%SYSTEMROOT%windows Update.log** file. The date in this entry should be after the most recent update time. If it is not, update detection has not occurred. You can force detection by stopping the automatic update service and editing the registry key **HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUPdate\Autoupdate**.Then, you delete the **LastWaitTimeout** value and restart the service. After you do this, you should look for error codes in the Windows Update logfile.
Miscellaneous error codes are found in the update log file.These are codes generated when the client is trying to read the update information on the SUS server.	These may be due to various problems on the Web server side, and the error codes may lead you to a solution.	If a hexadecimal error code begins with 0x8019, convert the last three digits to decimal to get the HTTP status code. For example, 0x80190194 is status code 404.
The client is not getting updates, and the client was configured through manual editing of the registry.	Entries may not be in the correct place in the registry.	Use **gpedit.msc** to configure the client to make sure that registry entries are created in the correct location. In **gpedit**, under Computer Configuration, Administrative Template, select Action, Add/Remove Template. Click add and add the **wuau.adm** file. Then expand the Windows Components, Windows Update portion of Computer Configuration, Administrative Templates and configure the Windows Update policy.

(continued)

Table 3.5 SUS Issues *(continued)*

Error or Issue	Cause	Resolution
The client was configured using group policy, but does not detect updates.	The computer may not be getting the group policy.	Use the **gpresult** tool from the *Windows 2000 Resource Kit* to determine whether the client computer is receiving the policy settings.
An error occurs when you attempt to load **wuau.adm** with **poledit** in Windows NT 4.0: The error is "unexpected keyword; found garbled characters: the file cannot be loaded."	**wuau.adm** uses Unicode, but Windows NT 4.0 does not.	Open the **wuau.adm** file in Notepad and chose File, Save As. Then, disable the Save As Unicode check box.
Error 0x801900194 is logged in the Windows Update logfile when the client queries **autoupdatedrivers/getmanifest.asp**.	This is an expected error that does not indicate a problem. The client is checking for driver updates, and SUS can't synchronize them. (This is actually a 404, "file not found," error.)	
You are setting up SSL for accessing the IIS, and the IIS on the SUS server does not display the **Content\EULA** folder.	The **Content\EULA** folder does not appear until SUS has performed at least one successful synchronization.	Log on locally and manually synchronize the SUS server. Then set up SSL for remote administration.
The client cannot detect updates.	The client uses port 80 to detect updates. If the root of the Web site, the **/content** virtual root, or the **/selfupdate** virtual root is configured to use SSL, automatic update clients cannot detect updates.	Remove the SSL requirement from these folders.
SUS setup does not finish.	Many possibilities exist: The administrator is not logged on; SUS was installed through group policy with user settings; Internet Explorer 5.5 is not detected; an NTFS partition is not detected; Service Pack 2 or 3 is not detected; or there was an attempt to install SUS on a non-NTFS drive.	Modify the system to correct these errors. You might also need to turn off services that aren't required, such as antivirus software. Also, you should check the Event Viewer for messages. You need to be sure to upgrade to Windows Installer version 2.0 and turn on the Windows Installer logger. (More information can be found in knowledge base article 223300.)

Troubleshooting hfnetchk

As you learned earlier in this chapter, `hfnetchk` is a command-line hotfix assessment tool that you can use to determine the hotfix status of multiple Windows operating systems and products. `hfnetchk` reports the service pack status of the computer as well. It does not download patches nor provide any way to update systems.

The most common problem experienced when using `hfnetchk` is typos. When you're troubleshooting problems with `hfnetchk`, the first thing to check is the accuracy of the entered command line. Other common problems include the following:

➤ *False positives*—These problems occur when `hfnetchk` reports the need to apply a fix that is already applied. These reports should be considered suspect because there are a number of known issues where it is difficult for `hfnetchk` to determine whether a fix has been applied. These issues are documented in the notes. The report refers to a knowledge base article or to other information that either details how to determine whether the hotfix has been applied or why it might not be possible to determine. Known issues include MS01-022 and MS98-001.

➤ `hfnetchk` *displaying a message that the checksum is invalid and the file version is equal to or less than what is expected*—If you have this problem, most likely the file is old and the patch has not been installed.

➤ `hfnetchk` *displaying a message that the checksum is invalid and the file version is greater than expected*—If you have this problem, most likely you have installed a nonsecurity-related patch that just happens to install a file that is also in the hotfix. You might be protected from the vulnerability because the later version of the file might also include the fix.

➤ *After you install required patches, checksums still noted as bad*—Another patch can sometimes install an even newer version of the file replaced by a hotfix. You should check file versions against those in knowledge base articles to verify that the correct files are present. You can use `sigverif.exe` (a Windows 2000 command-line tool) to verify that the Microsoft signature is on system files. This eliminates the possibility that a Trojan Horse version of the file was installed on the system.

➤ *Inability to read the XML file*—The computer may not be able to access the XML file from the Microsoft site or cannot locate the one listed by using the `-x` switch. In this case, you need to verify the Internet connection or verify the alternate location and its accessibility. You can test to see that the local network or local copy of the file is not corrupt by attempting to open it in your browser. A good file will be readable in the browser.

Troubleshooting MBSA

The use of MBSA is straightforward and usually does not generate many errors. However, even though mistakes can occur with proper use, requirements and common problems in MBSA's configuration are detailed in the documentation that is downloaded with the tool. Administrators and users often choose to ignore these items, and therefore errors occur. Common errors or omissions and their resolution are detailed in Table 3.6.

Table 3.6 Common MBSA Problems and Solutions

Error or Problem	Cause	Solution
Unable to determine the computer file system type in Windows NT.	A registry check cannot verify that drives are hard disks. There may be a missing registry key in Windows NT.	There is currently no solution to this problem.
Different results occur between MBSA and Windows Update.	Windows Update carries critical updates only for Windows operating systems. MBSA security updates are missing for Windows and other applications, such as SQL Server. MBSA always looks for the latest hotfix. Windows Update may not because its scope is different.	There is currently no solution to this problem. Microsoft indicates that it is working to make scans consistent between products.
Can't install on Windows NT.	MBSA is not designed to be installed on Windows NT. MBSA can scan Windows NT from the Windows 2000 installation; it just cannot run on Windows NT.	Install MBSA on Windows 2000.
Can't find systems on the network.	The DNS server is unreachable.	Make sure DNS services are running and reachable.
MBSA cannot read or locate the XML file.	Another application may have unregistered the XML parser.	Reregister the parser by using **regsvr32 mscml.dll**.

Troubleshooting Installation Problems

Problems can occur when you attempt to add service packs and/or hotfixes during installation. Table 3.7 lists known problems and their resolution.

Table 3.7 MBSA Installation Problems

Product and Problem	Cause	Solution
RIS client cannot join the domain.	A prestaged computer account is disabled in Active Directory.	Enable (or reset) the account.
A stop 0x0000006b error is received, or setup stops when installing a Windows XP Service Pack 1 client via RIS.	NT LAN Manager (NTLM) version 2 is used during the client-logon phase of RIS installation of Windows XP Service Pack 1 and later. The problem is with SMB signing not always occurring.	Obtain a fix from Microsoft.
Using RIS, you get an error message saying that you have entered an invalid password and that you can continue the installation and attempt to join the domain later.	You might have this problem during a RIS installation including Windows 2000 Service Pack 2. This is a problem with Kerberos, which substituted the computer name for the username that is necessary to join a domain.	As a workaround, you can shut off the computer if you have this problem. You can then restart the computer, and Setup will restart and successfully complete. To solve this problem, you must obtain a fix from Microsoft and change RIS to install Service Pack 3.
You get Error 86, “The specified network password is not correct,” when attempting to map a drive using **net use** during an unattended installation of Service Pack 2.	The unattended installation is slipstreamed. Or The **net use** command is run directly from the **cmdlines.txt** file as **net use [*driveletter*:] [*computername*\ *sharename*\][*password*] [/*user*:[*domainname*\ *username*]** In this case, ***domainname*** is the name of the domain the computer is a member of.	Allow the GUI portion of Windows to complete and then reboot the computer. The installation will continue. Or Use a nonexistent domain name.

(continued)

Table 3.7 MBSA Installation Problems *(continued)*

Product and Problem	Cause	Solution
You cannot use a combination installation of Windows 2000, Service Pack 2, and post–Service Pack 2 hotfixes from a network share.	Hotfixes already included in Service Pack 2 are inadvertently added to the share. Service Pack 2 fixes (that is, post–Service Pack 1 fixes) have an **sp2.cat** file that contains the necessary signatures to allow Windows file protection to properly function. If the fix is slipstreamed into the share point, the new **sp2.cat** file overwrites the old and breaks Windows file protection.	You should slipstream only Windows Service Pack 3 and later fixes into a combination (Service Pack 2, Windows 2000, and hotfix) installation share.
You get the message "The BINL service cannot locate a flat image with a version that matches the version of the riprep image" or the message "An error occurred on the server. Please notify your administrator" or the message "Missing CD image."	This might occur when you're using RIS to install Windows 2000 Professional from an image created with **riprep.exe** or when attempting to create the riprep image. If a riprep image is used, a RIS server must find a CD-ROM–based image that matches the riprep image that is selected from the Client Installation Wizard. When no CD-ROM–based image is available, installation fails. The error also occurs when you run **riprep.exe** on a computer that has a hotfix that updates **ntoskrnl.exe** or you attempt to run **riprep.exe** on a computer that has a service pack installed but no image with the same service pack exists on the computer.	Make sure the proper CD-ROM–based images are available.

(continued)

Table 3.7 MBSA Installation Problems *(continued)*

Product and Problem	Cause	Solution
Hotfixes in the **[SetupHotfixesToRun]** section of the **svcpack.inf** file are not installed.	This technique does not work until Service Pack 2.	Update installation to include a more current service pack.
During an attempt to slipstream a Windows 2000 service pack into a CD-ROM–based image on a RIS server using the **update –s** switch, the following error occurs, "An error has occurred copying files from the service pack share to the distribution folder."	The slipstream switch for **update.exe** does not support slipstreaming to a CD-ROM–based RIS image.	Use **risetup.exe** to create the CD-ROM–based RIS image that has a slipstreamed service pack. You can create the slipstreamed installation folder on another server, share the folder, and then use **risetup.exe**. When you're prompted for the location of the files, type the path to the share.
RIS clients stop responding at the Setup Is Starting Windows 2000 screen.	If a slipstreamed CD-ROM–based image is attempted, the error "An error has occurred copying files from the service pack share to the distribution folder" occurs. The slipstream switch does not support this.	Use **risetup.exe** to create the CD-ROM–based RIS image that has a slipstreamed service pack. You can create the slipstreamed installation folder on another server, share the folder, and then use **risetup.exe**. When you're prompted for the location of the files, type the path to the share.

Troubleshooting qchain

`qchain` works to ensure that hotfixes are installed in the proper order for Windows NT and to ensure that hotfixes chained without a reboot do not install the wrong updated version of a file. However, qchain may not work correctly if hotfixes contain binary files, as listed in the `HKLM\System\CurrentControlSet\Control\Session Manager\KnownDLLs` registry key. The reason appears to be the code used to identify the version of these files. Post–Service Pack 2 hotfixes have been corrected to identify correct file versions and eliminate this problem.

Troubleshooting Windows Update

Errors can occur during use or attempted use of the Windows Update site. Table 3.8 enumerates the error conditions and explains possible causes and solutions. Many of these errors and problems are caused by failed installations or damaged scripting engines. Thus, removing and then reinstalling the Windows Update script engine often resolves Windows Update problems.

Table 3.8 Problems with Windows Update

Error or Problem	Cause	Solution
You are prompted to install the March 4 security update, even though you have already done so or have installed Service Pack 3 for Windows 2000 (which includes the update).	The Java Runtime Environment (JRE) from Sun Microsystems is installed. This sets the **HKEY_LOCAL_machine\Software\Microsoft\Active Setup\Components\{08b0e5co-4fcb-11cf-aaa5-00401c608500}** key to **3802**, which triggers the prompt.	If Windows 2000 (Service Pack 3) or Windows XP Service Pack 1 and Microsoft Virtual Machine 5.00.3805 are installed, this may not apply. Removing the JRE does not change the key. You need to reinstall the update to update the registry value to **3805**.
The error "JavaScript:void(0)" appears in the Internet Explorer status bar, and no downloadable file is received.	The scripting engine is damaged.	Download and install a new engine.
The Download button appears dimmed after components are chosen.	The Internet Explorer cache/history needs to be cleared or the control is damaged.	Clear the Internet Explorer cache and history, remove Windows Update controls, and install a new Windows script.
The Download button does not work.	There's a problem with the Visual Basic scripting engine.	Clear the Internet Explorer cache, install a new script engine, and disable antivirus software or Internet filter software.

(continued)

Table 3.8 Problems with Windows Update *(continued)*

Error or Problem	Cause	Solution
You get Error 403, "Access denied/forbidden."	There may be interference from ATGuard personal firewall or other security, Ad removal, download assistant, or Web accelerator software. The Windows update control may be damaged or missing. The host file may be damaged or contains incorrect information. There may be missing or damaged Internet Explorer files.	Remove suspect software and try using Windows Update again. If it still does not work, remove Windows Update controls and install a new scripting engine.
The WINUP-Blank Page is displayed. You might get the message "Done, but with errors on page" in the Internet Explorer status bar.	The Visual Basic Scripting support (VBScript) component failed to install properly or became corrupted after installation.	Remove the Windows Update controls and then reinstall them.
You are accessing through a proxy server or firewall and receive one of the following messages: "Cannot display page" or "Download and installation failed." The site hangs on the "Please Wait" window as it starts to initialize the product catalog.	Possible software incompatibility could involve WinProxy by Otis Software, WinGate by Deerfield.com, or Internet Gate from MaccaSoft. Possible caching of the Windows Update page might interfere with installation and initialization; port 80 or 443 may be disabled (both of these are used by Windows Update); and client machines may not be configured to allow active scripting or download and initialization of ActiveX controls.	Clear the proxy cache and configure it to exclude the Windows Update site; enable ports 80 and 443; set Internet Explorer security on the client to Medium or lower, with Active Scripting enabled and allowing download and initialization of ActiveX controls.
You get an error about installing a dependency.	The software control did not download or install properly.	Uninstall the control and then reinstall it.
An unknown error occurs.	The software control did not download or install properly.	Uninstall the control and then reinstall it.

(continued)

Table 3.8 Problems with Windows Update *(continued)*

Error or Problem	Cause	Solution
You chose not to download the software controls or there was a problem with downloading the controls, and much of the Windows Update site is unavailable to you. If you would like to download the controls, you need to click Try Again.	The software control did not download or install properly.	Uninstall the control and then reinstall it.
You get the error "Your Internet Explorer security settings are set too High. In order to use the Windows Update site, you need to set your security settings at Medium."	Windows Update requires Medium to Low security settings.	Set Internet Explorer security settings to Medium.
You get the error "Internet Explorer cannot open the Internet site address. A connection to the server cannot be established."	TCP/IP connectivity problems are occurring.	Troubleshoot TCP/IP connectivity.
The computer stops responding (hangs) when you attempt to download a file from the Windows Update site.	A script may be corrupt.	Install a new Windows Update script.
You encounter an error when loading the script (that is, when downloading critical update).	The Windows script is damaged.	Reinstall or remove and install the script.
You receive an "unknown error (-2147024770)" message when trying to install a Windows update.	Internet Explorer is corrupt or some system files are not registered correctly.	Repair the Internet Explorer installation by using Control Panel, Add/Remove Programs. If the Add/Remove Programs applet does not display Internet Explorer 5.5, use the command **rundll32 setupwbv.dll,ie5maintenance**.

The first problem in Table 3.8 is an interesting one. Not only does it reveal an interesting application conflict, which may result in an unnecessary warning, but the problem can actually prevent another advisory from occurring. Thus, it may mask a potential security vulnerability. The issue occurs because a third-party product modifies the registry key that is used by **hfnetchk** and the Windows Update site to determine whether a patch has been added. This results in a warning even if the patch has been installed. It also prevents a warning on another update (which requires the first to be installed). Fixing the first problem allows the Windows Update site or **hfnetchk** to give the correct warning if it affects the system. The two security bulletins to examine are MS02-013 and MS02-052. More information can be found in knowledge base article 329077.

You should use security zones to avoid the problem created when you lock down Internet Explorer and then try to use Windows Update. Windows Update requires that active scripting be enabled and the client be set to allow the download and initialization of ActiveX controls. You can put the Windows Update site address in the Trusted Sites zone and allow those activities there. You can then restrict them in the other security zones.

Exam Prep Questions

Question 1

Which of the following is the utility that allows automatic download and updating of Windows XP computers?

○ A. **qchain**

○ B. Dynamic Update

○ C. Windows Update

○ D. SUS

Answer C is correct because Windows Update is used to automatically download updates on Windows XP computers. Answer A is incorrect because `qchain` is a utility that can be used in scripts to apply multiple hotfixes with a single reboot. Answer B is incorrect because Dynamic Update is the ability of a Windows XP installation to connect to the Internet and download the latest drivers and updates during installation. Answer D is incorrect because SUS is the server software used to create an intranet version of Windows Update.

Question 2

Methods to perform operating systems installation that have service pack files include which of the following? (Choose all that apply.)

□ A. Dynamic Update and an Internet connection

□ B. Dynamic Update and an intranet connection

□ C. Slipstreaming

□ D. Windows Update

□ E. MBSA

□ F. SUS

Answers A, B, and C, are correct because dynamic updates can be done with an Internet connection and with an intranet connection and include service pack files, and because slipstreaming is a method that adds service pack files to an installation directory copy of Windows files. Answer D is incorrect because Windows Update cannot be used to install the operating system. Answer E is incorrect because MBSA is a tool for determining hotfix status and Answer F is incorrect because SUS is the server software used to create an intranet version of Windows Update.

Question 3

The simplest way to provide an automatic updating system for client systems that are used by nonadministrative users is to set up which of the following services?

❍ A. MBSA

❍ B. SUS

❍ C. Windows Update

❍ D. Dynamic Update

Answer B is correct because SUS clients can install updates even if an administrator is not logged on. Answer C is incorrect because Windows Update can be set to automatically download critical updates as they become available, but an administrator must install the updates. Answer A is incorrect because MBSA is a tool for determining hotfix status. Answer D is incorrect because Dynamic Update is the ability of an XP installation to connect to the Internet and download the latest drivers and updates during installation.

Question 4

Windows Update in Windows XP can be used to do which of following? (Choose all that apply.)

❑ A. Search for and download drivers for new hardware devices.

❑ B. Search for and download updated drivers for existing hardware.

❑ C. Search for and download updates to third-party software.

❑ D. Search for and download new Microsoft security tools.

Answers A and B are correct because Windows Update can search for and download drivers for new hardware devices and for updated drivers for existing hardware. Answer C is incorrect because third-party software may include its own update service, but Windows Update cannot be used. Answer D is incorrect because new Microsoft security tools are not made available via Windows Update.

Question 5

As the administrator in charge of your company's patching procedures, you want to implement MBSA. However, you are not able to get it to scan all systems in your network. You have a combination of Windows NT, Windows 98, Windows 2000, and Windows XP computers. Which of the following choices are possible causes for the scan failure? (Choose all that apply.)

❑ A. MBSA cannot run on Windows 2000 Professional; it must be installed on Windows 2000 Server.

❑ B. MBSA cannot be used to scan Windows 98.

❑ C. Remote Registry Service is disabled on some Windows NT computers.

❑ D. MBSA can be used to scan Windows XP home computers only if MBSA is installed on the Windows XP home computer.

❑ E. Windows XP Professional is using simple file sharing.

Answers B, D, and E are correct because MBSA cannot be used to scan Windows 98 and because Windows XP Home Edition must be locally scanned, and if Windows XP is using simple file sharing, it cannot be remotely scanned. Answer A is incorrect because MBSA can be installed and will run on Windows 2000 Professional. Answer C is incorrect because Remote Registry Service must be running on Windows 2000 computers, but it is not a service that is available in Windows NT.

Question 6

The first day on your job as administrator for the ABC Corporation, you are told to use **hfnetchk** to scan computers on your network for patching status and provide your boss with a report. All is going well until you must scan computers in the Finance Department. Because these computers (all Windows NT 4.0 Service Pack 6 computers) reside on their own LAN and by security policy and network configuration are not allowed access to the Internet or other parts of the network, you must go to the Finance Department to scan the computers. You install a copy of **hfnetchk** on a Windows 2000 Professional laptop and bring it along with you. You configure the laptop for network access on the Finance Department LAN and attempt to scan the systems, but the scan fails. You can **ping** the Finance Department computers. What are some possible reasons and what do you do to fix them? (Choose all that apply.)

❑ A. Windows NT computers cannot be scanned across the network; install **hfnetchk** on each computer and scan each computer.

❑ B. Because there is no Internet access, the **mssecure.xml** file cannot be reached; download a copy of the file to the laptop and use the **hfnetchk –x** command to do the scan.

❑ C. You do not have administrative privileges for every computer that you want to scan. Make sure you are using an administrative account in the same domain as the Finance Department or in a trusted domain and repeat the scan.

❑ D. Internet access is required in order to access the **mssecure.xml** file; temporarily connect the Finance Department network to the Internet, run the scans, and then disconnect the network from the Internet.

Answers B and C are correct because you must either have access to the Internet or a copy of the `mssecure.xml` file and you must have administrative privileges for every computer scanned. Answer A is incorrect because the Windows NT computer can be scanned across the network (and cannot be scanned locally because `hfnetchk` cannot be installed on Windows NT). Answer D is incorrect because security policy does not allow Internet access from these computers, so you should not connect them to the Internet.

Question 7

The command **hfnetchk –v –z –x mssecure.xml –f file.txt** does which of the following?

❍ A. **hfnetchk** reads in a list of computers in the **file.txt** file and scans them. It uses a local copy of the **mssecure.xml** file, disables the registry checks, and, if a patch is not found, displays the reason.

❍ B. **hfnetchk** redirects its output to the **file.txt** file. It uses a local copy of the **mssecure.xml** file and disables the registry checks. If a patch is not found, **hfnetchk** displays the reason.

❍ C. **hfnetchk** redirects the output to the **scan.txt** file and uses a local copy of the **mssecure.xml** file. It stops notes messages from being displayed, and, if a patch is not found, displays the reason.

❍ D. **hfnetchk** redirects the output to the **scan.txt** file, uses a local copy of the **mssecure.xml** file, disables the registry checks, and stops warning messages from being displayed.

Answer B is correct because the switches and entries listed cause `hfnetchk` to redirect its output to the `file.txt` file. It then uses a local copy of the `mssecure.xml` file and disables the registry checks. If a patch is not found, `hfnetchk` displays the reason. The remaining answers are incorrect because at least one thing they do is not listed in the answer: Answer D is incorrect because the `-s 2` switch would produce stop warning messages from being displayed. In Answer A, the `-fh` switch reads a list of computer names and performs a scan against multiple computers. In Answer C, the `-s 1` switch stops notes messages from being displayed.

Question 8

RIS can be used to provide network installation services for a Windows 2000 Professional computer. You can also use it to configure automatic application of the current service pack and relevant hotfixes. The best way to do this is by doing which of the following?

○ A. Add a GPO to the domain that includes a software installation policy.

○ B. Call the service pack **update.exe** from **[GuiRunOnce]** and add appropriate hotfix script lines to the **[GuiRunOnce]** section of the **unattended.txt** file.

○ C. Add to the RIS server a GPO that specifies automatic update. The GPO will be applied to the Windows computer after installation and reboot.

○ D. Add to the domain default security policy server a GPO that specifies automatic update. The GPO will be applied to the Windows computer after installation and reboot.

Answer B is correct because putting the command in this file causes the file to run after a reboot. Answer A is incorrect because it would affect all computers in the domain and not just the newly installed computers. Answer C is incorrect because a local GPO written for the RIS computer would not be applied to the newly installed Windows computers. Answer D is incorrect because automatic update is not available for Windows 2000 Professional computers prior to Service Pack 3.

Question 9

You are charged with recommending the best Microsoft solution to the patching problem. Money is not an issue, but reports and reduced administrative activity are problems. There are 4,000 computers in the organization. No computer management software has been installed. What product should you recommend?

○ A. SUS

○ B. MBSA

○ C. SMS

○ D. Windows Update

Answer C is correct because it is the recommended solution for companies with more than 500 computers to maintain. Answer A is incorrect because SUS is generally recommended for a much smaller network than this one; it cannot provide the management and reporting features that SMS can. Answer B is incorrect because MBSA is not a good patching solution (well, it might be okay for a very small company whose users act as administrators on their own computers). Answer D is incorrect because Windows Update is not a good solution for this many computers.

Question 10

What issues might limit the adoption of SUS by organizations with very small numbers (50 or fewer) of computers? (Choose all that apply.)

- ❑ A. There is a high cost associated with acquiring SUS.
- ❑ B. SUS is difficult to set up.
- ❑ C. SUS cannot be installed on a domain controller.
- ❑ D. A SUS server must have IIS loaded, but IIS will probably not be able to be used for most other Web applications.

Answers C and D are correct because a smaller company may not be able to afford another server for just this one service. Both of these options describe reasons that SUS cannot be used on other servers. Answer A is incorrect because SUS is a free download. Answer B is incorrect because installation and configuration require little administrator activity.

Need to Know More?

Alistair G. Lowe-Norris, “Scripting a Corporate Update System,” in *Windows Scripting Solutions*, October 2002, www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/maintain/optimize/SCRCUS.asp.

“Microsoft Windows 2000 Service Pack and Installation Guide,” www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/support/spdeploy.asp.

“Maintenance for Windows XP in Companies with More Than 5000 Computers,” www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/deskdeploy/wxpml/DEFAULT.asp.

“Maintenance for Windows XP in Companies with 500–5000 computers,” www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/deskdeploy/wxpmm/DEFAULT.asp.

“Maintenance for Windows XP in Companies with 50–500 Computers,” www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/deskdeploy/wxpms/DEFAULT.asp.

SUS home page, www.microsoft.com/windows2000/windowsupdate/sus/default.asp.

“Baseline Security Analyzer,” www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/mbsawp.asp.

“Scripting a Corporate Update System,” www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/maintain/optimize/SCRCUS.asp.

“Software Update Services Deployment Guide,” www.microsoft.com/windows2000/windowsupdate/sus/susdeployment.asp.

“Software Update Services Deployment White Paper,” www.microsoft.com/windows2000/windowsupdate/sus/susdeployment.asp.

“Patch Management Using Microsoft Software Update Services,” www.microsoft.com/technet/solutions/msm/swdist/PMSUSOG.asp.

“How to Turn on SSL Support for Your Software Update Services Administration Site,” http://support.Microsoft.com/default.aspx?scid=KB;en-use;326312&.

“Automatic Updates June 2002,” www.microsoft.com/windows2000/downloads/recommended/susclient/default.asp.