Planning and Implementing Server Roles and Security

ITINERARY

- **Objective 1.01** Evaluate and Select the Operating System to Install on Computers in an Enterprise
- **Objective 1.02** Plan a Secure Baseline Installation
- **Objective 1.03** Plan Security for Servers That Are Assigned Specific Roles
- **Objective 1.04** Configure Security for Servers That Are Assigned Specific Roles
- **Objective 1.05** Plan a Security Update Infrastructure

<table>
<thead>
<tr>
<th>NEWBIE</th>
<th>SOME EXPERIENCE</th>
<th>EXPERT</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 hours</td>
<td>3 hours</td>
<td>2 hours</td>
</tr>
</tbody>
</table>
Planning is one of those skills that is gained through a combination of knowledge and experience. In this chapter, we’re going to teach you the ins and outs of planning for a Windows Server 2003 deployment. This is a brand new type of exam for Microsoft: it’s the first planning exam they have ever had, and it’s a new type of exam that has been developed with a number of key improvements over previous exams. Specifically, Microsoft has extended the question types from simple multiple choice to include hotspot and drag-and-drop-style answers.

Microsoft has also changed the way questions are introduced in the exam. Previous exams used a suite of questions that made up the exam. In order to combat the growing number of sites that provide a list of the questions and answers, the new exams consist of hundreds of questions, only a selection of which you will answer. That means to pass the exam, you’ll actually need the knowledge provided in this book, rather than simply memorizing the right answers.

Finally, this is also one of the first exams designed from the start to address a common complaint of some of the earlier exams from the Windows 2000 MCSE, which was that it should test you on events and knowledge that will be required in the field. Therefore, by reading this book, not only should you be able to pass the exam, but you should also be able to apply many of the techniques and use much of your knowledge when you start your IT management job for real.

Throughout the exam, the primary concern is security, so throughout the book, we’ll concentrate on planning different aspects of your Windows Server 2003 installation and how it affects the overall security of your installation. Although this will seem tiresome at times, our aim is to make it as entertaining and interesting as possible.

We’ll also spend some time explaining why the security is so important. You might think it’s obvious, but others won’t. Technical and computer crime is on the rise, websites are broken into, industrial secrets are stolen, and in some cases criminal damage takes place. The meteoric rise of the Internet is in some small way responsible because it’s opened up the borders of various companies in ways they never expected. It’s also enabled unscrupulous individuals to study packets and information as it’s transferred between companies over what is a public network.

In this chapter, we’ll start with the basics of the operating systems, starting with the various editions, the security features of each version, and how this affects which edition you choose. We’ll also cover how to use different core security systems to enforce and apply security settings on your servers and clients.
Exam Tip

These tips should help you identify what elements of each section will actually be tested on within the exam. Although all of the material in the book is potentially included, sometimes you need specific information about how the questions are structured and how a particular system is tested upon. Remember, in this exam Microsoft is looking for planning and analytical skills, rather than experience or knowledge of individual wizards, configuration, and administration tools. That means knowing the abilities, limitations, and technical architecture of the operating system and having the ability to apply that to build a plan for your network’s infrastructure.

Objective 1.01

Evaluate and Select the Operating System to Install on Computers in an Enterprise

Windows Server 2003 is, like Windows 2000, split into a number of editions, each designed and targeted for a specific market and type of installation. As you plan your network, you’ll need to know how to translate your organization’s needs into a map of requirements for the operating system that will support your network.

In essence, these kinds of decisions are no different from any other you might make, from choosing dinner to choosing a new car. Okay, perhaps it’s a bit different. When choosing dinner it’s a question of likes and dislikes. When choosing a car, though, you need to think about a number of parameters, such as the type, the size, or the engine, before you get to the more human-like choices of colors, upholstery types, and whether you want a pair of dice dangling from the rearview mirror.

In this section, we’ll look at the basic functionality and abilities of each operating system edition—it won’t be an extensive summary and comparison, but it should be enough to enable you to differentiate between the versions and understand their key points. We’ll also look at how to evaluate the needs of your organization and match one of the versions to your needs. Armed with this information, you should be able to make some decisions about the security implications of choosing the different versions.
Windows Server 2003 Editions

The Windows Server 2003 family consists of four distinct products:

- **Windows Server 2003, Standard Edition**  The basic edition, which supports the majority of features. This replaces the Windows 2000 Server and Windows NT 4 Server products.

We’ll have a closer look at some of the specific features of each edition before comparing features across all editions.

**Standard Edition**

Standard Edition (SE) supports the entire basic set of Windows Server 2003 features. It can act as a domain controller or public key infrastructure (PKI) server and provide core network services like Domain Name Serving (DNS), Dynamic Host Configuration Protocol (DHCP), and WINS.

The Standard Edition is aimed at the broadest range of applications, in particular file servicing, print serving, and low-demand application serving (such as Microsoft Exchange Server, SQL Server, or similar application-led tasks). It can also support basic terminal services, although its memory and processor limitations may make it less than ideal for larger terminal services roles. It’s not capable of full clustering capabilities, but it does support network load balancing.

It should be clear that Standard Edition is ideal as an all-purpose platform for smaller environments, or as a server built into a group providing services in a larger network.

Technically, Standard Edition supports up to four CPUs in a Symmetric Multi-Processor (SMP) environment and up to 4GB of RAM. It can also address up to 4TB of disk space.
Enterprise Edition

The Enterprise Edition (EE) is intended for use in many of the same roles as Standard Edition, but it includes features designed to improve the reliability and scalability of these services. In particular, Enterprise Edition doubles the number of CPUs it can support to eight and the maximum RAM to 32GB. Enterprise Edition is also the first edition to support 64-bit processors.

Local Lingo

32-bit and 64-bit

Processors access memory and process instructions according to the width of the address that references the memory location. 32-bit processors can directly access up to 4GB of memory (tricks are used for values above this). A 64-bit processor can access a staggering 1.67 million terabytes of memory. 64-bit processors are not necessarily faster than their 32-bit counterparts, but the ability to address such large amounts of memory can increase the overall speed of an application by allowing more of the information to be directly available in memory.

Enterprise Edition supports Address Windows Extensions (AWE) that enable the operating system to reserve as little as 1GB for use by Windows, allowing the applications to use the remaining 3GB of the remaining memory. EE also allows memory to be added while the machine is running (hot-memory) on hardware systems that support it, and it allows non-uniform memory access (NUMA). Some systems use separate memory busses for separate processes; NUMA enables Windows to access these separate memory areas as one complete memory range (hence the support for 32GB of memory on 32-bit processor systems, 4GB for each of eight CPUs).

However, the primary improvements of this edition relate to additional functionality. Enterprise Edition supports clustering technology, allowing multiple servers to appear as one machine and automatically take over in the event of a failure. This works with clustered applications such as SQL Server Enterprise Edition and Exchange Server Enterprise Edition, as well as many applications and systems that do not directly include support for clustering technology.

Finally, EE extends the terminal services system with the Terminal Server Session Directory, which allows clients to reconnect to a terminal services system supported by a number of terminal services servers. For example, with eight terminal services servers, if one server fails, the Terminal Server Session Directory will allow clients to automatically reconnect to one of the remaining servers.
The Enterprise Edition is obviously all about maintaining the stability and reliability of your network services and should be used in situations where these parameters are most critical to your business needs.

**Datacenter Edition**

Datacenter is one of two editions of the operating system that are slightly different from the other versions. You cannot buy Datacenter Edition as a stand-alone product. Instead, it must be purchased as part of a combination of hardware and software from a supplier. The reason for this is that Datacenter Edition is sold only on hardware that has been specifically designed to work with the Datacenter Edition. Rules are much more strict about which hardware is supported, and specific solutions have to go through a huge range of tests. The aim is to provide you with a server that can remain up and running for 99.999 percent of the time—that’s about 9 hours of unplanned downtime each year.

**Travel Assistance**

Downtime is classed as a problem that makes the machine unusable. It doesn’t include the times when you take down the machine to perform some maintenance, install a patch, or change the hardware configuration.

The Datacenter program is 100 percent focused on reliability:

- All hardware included in a Datacenter server must meet rigid Microsoft standards and pass hundreds of compatibility and reliability tests, including everything from the processors and memory to the network cards, disk drives, and other components.
- All the device drivers must be certified and digitally signed by Microsoft. They must also have gone through similar testing procedures to the hardware—it can take months for a new piece of hardware to be certified for Datacenter Edition use.
- Customers cannot make unauthorized changes to the server hardware. All changes must pass the same suite of tests. Even when upgrading a four-CPU system to an eight-CPU system, you can only do so if the hardware has been certified in its eight-CPU configuration.

These rigid requirements, combined with the typical expense of a server that would make Datacenter Edition worthwhile to install, means that the Datacenter Edition is the least likely to be installed. It’s possible you’ll never ever come across a Datacenter Edition server in your entire career.
Web Edition

The Web Edition exists to fill a technological and price-related gap. The modern web server datacenter is not made up of single machines with a vast number of CPUs and memory. Instead, it’s made up of stacks and stacks of smaller, one- or two-CPU processors with comparatively low amounts of RAM.

In this instance, using the Standard Edition would just be too expensive—in many cases more expensive than the hardware on which the OS is running. Some companies have instead switched to Linux and Apache, rather than Windows and IIS, to support their websites.

Microsoft has responded by producing the Web Edition. It provides enough of the operating system, IIS, and web application platform (ASP, ASP.NET) to allow it to serve websites and applications. It also includes the network load balancing, so that it can be used in a quasi-clustered environment.

However, it’s also had a lot of technology removed, including Routing and Remote Access, terminal services, remote installation services, services for Macintosh, and Active Directory hosting. You can still connect to an Active Directory from Web Edition, but a Web Edition server cannot act as a domain controller.

Server Edition Comparison

To help you make decisions about which version you want to employ in your organization, we need to take a closer look at the specific differences, individual features, services, and abilities of each system. The basic requirements of each edition are listed in Table 1.1.

<table>
<thead>
<tr>
<th>Requirement/Edition</th>
<th>Standard</th>
<th>Enterprise</th>
<th>Datacenter</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU (32-bit)</td>
<td>133MHz</td>
<td>133MHz</td>
<td>400MHz</td>
<td>133MHz</td>
</tr>
<tr>
<td>CPU (64-bit)</td>
<td>N/A</td>
<td>733MHz</td>
<td>733MHz</td>
<td>N/A</td>
</tr>
<tr>
<td>Recommended CPU</td>
<td>P3 550MHz</td>
<td>P3 733MHz</td>
<td>P3 733MHz</td>
<td>P3 550MHz</td>
</tr>
<tr>
<td>RAM</td>
<td>128MB</td>
<td>128MB</td>
<td>512MB</td>
<td>128MB</td>
</tr>
<tr>
<td>Recommended RAM</td>
<td>256MB</td>
<td>256MB</td>
<td>1GB</td>
<td>256MB</td>
</tr>
<tr>
<td>Disk Space (32-bit)</td>
<td>1.5GB</td>
<td>1.5GB</td>
<td>1.5GB</td>
<td>1.5GB</td>
</tr>
<tr>
<td>Disk Space (64-bit)</td>
<td>N/A</td>
<td>2GB</td>
<td>2GB</td>
<td>N/A</td>
</tr>
</tbody>
</table>

TABLE 1.1 Windows Server 2003 Requirements for Different Editions
Of course, the reality is that if you are installing Windows Server 2003, you’ll probably also take the opportunity to convince management to buy you a new piece of hardware on which to install and run the new operating system, and it’s getting increasingly difficult to find machines with processors running at less than 2GHz, let alone as slow as 550MHz. Memory and hard disk will be the issue here, but again, specifications of these parameters are also typically high, with most servers coming with 256MB and 40GB hard drives at a minimum. At the time of writing, both RAM and hard disk storage are cheap, with 256MB available for less than $100 and hard disks at an unprecedented 1GB/$ rate.

However, if you want to take advantage of Windows Server 2003 features and upgrade your existing hardware, you need to keep the figures in Table 1.1 in mind. I’ve successfully deployed Windows Server 2003 Standard Edition on a P3 700MHz machine. This operates as the domain controller, installation server, file server, and software update server for a relatively small network.

**Exam Tip**

Microsoft is likely to test you on the specifics of Table 1.1 so it’s worth taking some time to remember the details. In particular, questions like “You have 10 Windows 2000 Servers that use Pentium III 600MHz processors. Which versions of Windows Server 2003 can you install on these machines?” may appear and then proceed to list the various editions to choose from.

When choosing a machine on which to install Windows Server 2003, you need to consider not only the current requirements, but also the future requirements and expandability. For example, if you know that you could support your company’s e-mail facilities on 4-CPU server but expect to double your staff over the next two years, Standard Edition on a 4-way SMP box may be a limitation.

A full summary of the hardware requirements of the various editions of Windows Server 2003 is given in Table 1.2.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Max RAM (32-bit)</td>
<td>4GB</td>
<td>32GB</td>
<td>64GB</td>
<td>2GB</td>
</tr>
<tr>
<td>Max RAM (64-bit)</td>
<td>N/A</td>
<td>32GB</td>
<td>512GB</td>
<td>N/A</td>
</tr>
<tr>
<td>Max CPUs (32-bit)</td>
<td>4</td>
<td>8</td>
<td>32</td>
<td>2</td>
</tr>
</tbody>
</table>
CHAPTER 1  Planning and Implementing Server Roles and Security

For more specific service-level features, you need to consult Table 1.3.

**TABLE 1.2  Features and Hardware Limits for Different Editions (continued)**

<table>
<thead>
<tr>
<th>Feature/Edition</th>
<th>Standard</th>
<th>Enterprise</th>
<th>Datacenter</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max CPUs (64-bit)</td>
<td>N/A</td>
<td>8</td>
<td>64</td>
<td>N/A</td>
</tr>
<tr>
<td>64-bit (Itanium) Support</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Hot memory</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Non-uniform memory access (NUMA)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

**TABLE 1.3  Service Support Matrix for Different Editions**

<table>
<thead>
<tr>
<th>Service/Edition</th>
<th>Standard</th>
<th>Enterprise</th>
<th>Datacenter</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory (Domain Controller)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Active Directory (Member Server)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Identity Integration Server 2003 Support</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Security Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet Connection Firewall</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Key Infrastructure, Certificate Services, and Smart Cards</td>
<td>Partial</td>
<td>X</td>
<td>X</td>
<td>Partial</td>
</tr>
<tr>
<td>Terminal Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Desktop for Administration</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Terminal Server</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terminal Server Session Directory</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Clustering Technology</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Load Balancing</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cluster Service</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
### TABLE 1.3 Service Support Matrix for Different Editions (continued)

<table>
<thead>
<tr>
<th>Service/Edition</th>
<th>Standard</th>
<th>Enterprise</th>
<th>Datacenter</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Communications and Networking Services</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual Private Network (VPN) support</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Partial</td>
</tr>
<tr>
<td>Internet Authorization Services (IAS)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Network Bridge</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Internet Connection Sharing (ICS)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>File and Print Services</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed File System (DFS)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Encrypting File System (EFS)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Shadow Copy Restore</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Removable and Remote Storage</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Fax service</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Services for Macintosh</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Management Services</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IntelliMirror</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Partial</td>
</tr>
<tr>
<td>Group Policy Results</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Partial</td>
</tr>
<tr>
<td>Windows Management Instrumentation (WMI) Command Line</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Remote OS installation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Remote Installation Services (RIS)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Windows System Resource Manager (WSRM)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Choosing the right edition or editions is therefore a case of matching your requirements to the list of available features. Within an enterprise environment, it’s likely that you will use a combination of editions to build up your network infrastructure. For example, in a medium-sized network with 250 clients, you may use a number of Standard Edition solutions to provide basic domain controller, file, and printer server functionality.

In a larger network with 1000 machines, Enterprise Edition might be used to support an Exchange installation, with further Standard Editions to support the remaining file and print services. If you have an Internet connection and are supporting a number of websites, you might use Web Editions to support your web presence. In a vast enterprise class network, you might employ Enterprise Editions in a clustered environment for Terminal Services or Exchange and SQL Server.

The results of your choice should be a combination of the expected loading, the support for specific features—including CPU and memory support if you need a beefy machine to run a particular service—and the need for extended functionality such as clustering. In all other situations, Standard Edition is going to be adequate for most needs.

### Identifying Minimum Configurations for Satisfying Security Requirements

Security is not just about making sure the sales department cannot see the files accounting is keeping on them. It’s also about ensuring the security and stability of your network services and environment for your users. This means that not

---

**TABLE 1.3** Service Support Matrix for Different Editions (continued)

<table>
<thead>
<tr>
<th>Service/Edition</th>
<th>Standard</th>
<th>Enterprise</th>
<th>Datacenter</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>.NET Application Services</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>.NET Framework</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Internet Information Services (IIS 6)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>ASP.NET</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Enterprise UDDI services</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Multimedia Services</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Windows Media Services</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
only do you need to take traditional security measures such as using passwords and considering file/folder security, but you also need to consider the stability of the system, its support for clustering technology, and its ability to withstand and, if necessary, recover from errors and problems that will affect your network.

With this in mind, you need to identify the minimum level of security required in your network, and you need to do it in such a way that it doesn’t affect the running and operation of your network. For example, it’s tempting to enforce the highest security for all your servers and services, but while this would be ultimately very secure, it would probably block or otherwise restrict the available options.

What you need is some sort of middle ground between no security at all and the maximum level of security. That mid-point will be the area where you get the best security while still supporting the services that you need to support. To find that mid-point, you need to create a basic level of security that can be applied to all your servers and services, and then create security templates that can be used to secure specific server types and the services that they support.

We’ll be covering the specifics of the process in this chapter, but you should know the five specific steps within the process:

- **Secure an initial installation** When you first create and install a new Windows Server 2003 computer, you need to secure the installation before you build onto that installation with additional security.

- **Create a secure baseline installation** The baseline installation is the core security settings that will be used across all your servers. With the baseline settings in place, you can specify additional settings for additional servers.

- **Design security for specific server roles** With the baseline in place, you can assign security settings for servers that provide file, print, IIS, and other services and tailor them accordingly.

- **Develop methods for updating systems** Keeping up to date with the latest patches should help keep your systems secure by plugging holes and faults in your OS. You need to apply these as carefully and efficiently as possible.

- **Test security** Once all the necessary systems are in place, you need to be able to test your security settings to make sure your systems are secure.
CHAPTER 1  Planning and Implementing Server Roles and Security

Objective 1.02  Plan a Secure Baseline Installation

You can plan the first two steps—securing an initial installation and planning a secure baseline installation—in one go. First, though, you must define the security policy that you are going to use on the servers and clients in your network.

Windows Server 2003 provides this functionality with security templates. The templates define specific security parameters that you can use to enforce basic security settings on new systems. The security templates are wide ranging, from configuring the basics of password policy through enforcing nightly back-ups and even network security settings.

In this section, we’ll look first at how you can use templates to enforce the default security settings on new systems. Then we’ll take a closer look at the specific client and server OS default security settings so that you know how to change these default parameters to match your own needs.

Travel Assistance

It’s impossible to list all of the possible security settings and parameters that can be configured through the security template system. Although you shouldn’t need it for the exam, you should be familiar with the various settings. Check the Windows Server 2003 site (www.Microsoft.com/windows2003) for more information.

Enforcing System Default Security Settings

There are a number of ways you can force a system to use and apply the default security settings. As it stands, Windows Server 2003 is already fairly secure during a standard installation. Most of the additional role-specific functionality, such as IIS, the DHCP service, and others, are not installed by default. Other simpler elements are also more secure. For example, the administrator password that you set during installation must adhere to the strictest settings (that is, it must be at least two nonalpha characters and at least six characters in length).
From a purely theoretical perspective, the easiest way to enforce the default security settings is to specify strict procedures to be used when installing the operating system, including:

- Install from the original CD-ROM media or install from updated media that incorporates the latest service packs and security updates.
- Install only from verified installation files, either from a CD or network share. If using a network share, ensure that it can be accessed only by suitably trained and qualified staff.
- Configure only those roles and services that need to be supported by the server. Windows Server 2003 doesn’t install most services by default. You can help maintain the security of the system by limiting those that are installed.
- Disable services that aren’t needed, including those services that are installed by default that you do not need.
- Allow only trusted staff to install the system.

Not all of these suggested procedures can be followed, of course. In a distributed environment where servers may be installed across the company, it can sometimes be a nonadministrator or tech support specialist who performs the installation.

In this case, there are a number of alternative solutions:

- Use the scripting facilities of the Windows installer to automatically configure and control the server installation. All the user has to do is start or boot the server for the installation to take place. All the other elements are provided by the installation scripts.
- Use an isolated network for installation. Make the installation files available on a network share, and then provide secure access to this network share (read-only) to the user performing the installation.
- Create customized media that include the scripts and patches for automated installation.
- Use Remote Installation Services to control the elements that can be installed after the initial server software installation.
- Use disk imaging techniques to create an image of each type of server. Installation can then take place by simply applying the image to the server disk. The image can include all the necessary software, updates, and security settings.
One other tool that you can employ is the Group Policy system to apply security templates to the server. These are applied when the server joins an active directory domain—probably a required step for all server installations. Because the template is applied at a central level, it’s impossible to override it. We’ll be looking more closely at Group Policy and security templates in Objective 1.03, “Plan Security for Servers That Are Assigned Specific Roles.”

**Security Settings, Templates, and Default Security**

Security settings can be applied across a network through the use of the Group Policy system and/or the security template system. The security templates are exactly that—a group of settings that specify basic security parameters. Windows Server 2003 comes with a number of default security templates designed for clients and servers, including specialized templates for specific server types and roles.

### Local Lingo

**Group policies** Settings that can be applied to computers in your network through the active directory system are group policies. The information is distributed to the clients automatically when the computer initially logs on to the domain, or it can be forced by using the gpupdate tool.

You can also create your own templates, either by using the supplied templates as a guide or creating brand new templates to suit your needs. These templates can be applied on an individual basis to machines with the secedit tool, or they can be applied through the Group Policy system. You can also set individual security parameters through the Group Policy system with or without a template as a base.

The security areas that can be configured through this system include:

- **Account policies** These are the computer security settings for accounts, including password policy (length, complexity, renewals), lockout policy, and Kerberos policy in domains on Windows 2000 and Windows Server 2003.
- **Local policies** These allow you to configure who has local or network access to the computer and whether or how local events are audited, including security settings for audit policy, user rights assignment, and security options.
Event logs These control security settings for the Application, Security, and System event logs. Event logs can be accessed using the Event Viewer.

Restricted groups These allow membership control of restricted groups. Administrators are able to enforce security policy settings regarding sensitive groups, such as Administrators or Payroll.

System services These control startup mode and security options (security descriptors) for system services such as DNS, DHCP, IIS, and others. You can use this to limit services on clients and servers even if the service has already been installed.

Registry This is used to configure permissions for existing registry keys, including auditing information and the access permissions.

File system This is used to configure security settings for file-system objects, including access control, audit, and ownership.

External Security
We once visited a company that was demonstrating the security of their systems. It was quite impressive. Users needed a smartcard to gain access to their computer, in addition to their login and password. Passwords were strict too, and rotated on a weekly basis, and their network used secure transmission. When we got to the server room, however, the door was propped open because the lock, an electronic one, had broken. It had been like this for months.

Despite all their security at the system level, just about anybody could walk into the server room and switch off, take down, or remove the servers.

This underpins a very basic principle: always start with the most basic security. In the case of your servers, that means making sure only authorized people can get to them. When it comes to the technical side of the security settings, the same basic rules apply: make sure the basics of the security system are in place and that the other security settings build on those basics.

Exam Tip
To be honest, Microsoft is unlikely to test you on this particular aspect of security, but we think it’s an important concept to understand—technical security is only any good if the systems are also physically secure. It’s a bit like your credit card security—having PIN numbers and a signature is all very well, but if somebody steals your card, you’re in for trouble.
Default Templates
A number of default templates are included with Windows Server 2003. They serve two purposes. First, they enable you to apply default security settings for different systems. This can be useful in situations where you want to return a system or group back to the initial security settings applied when the OS was first installed. Second, they enable to apply specific security settings for different environments.

Travel Assistance
Templates are stored within the %SystemRoot%\Security\Templates directory as a series of .inf files. You should make sure that only administrators have access to this directory.

The list of templates and their effect on the various security parameters is shown in Table 1.4.

<table>
<thead>
<tr>
<th>Title</th>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Security</td>
<td>Basicwk.inf, Basicsv.inf, Basicdc.inf</td>
<td>These are basic security templates, the contents of which match the default settings on Windows 2000 and Windows Server 2003 installations on NTFS partitions. The templates can be used to apply the settings to workstations (Basicwk.inf), member servers (Basicsv.inf), and domain controllers (Basicdc.inf).</td>
</tr>
<tr>
<td>Domain Controller</td>
<td>DC security.inf</td>
<td>When a server is promoted to a domain controller, this template is created and reflects the file, registry, and system service default security settings.</td>
</tr>
</tbody>
</table>
### TABLE 1.4 Security Templates for Servers and Clients (continued)

<table>
<thead>
<tr>
<th>Title</th>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Setup security.inf</td>
<td>This is dynamically generated by the operating system when it is installed. It contains the default security settings, including file permissions for the operating system files, that are applied during the operating system installation. You should never apply this template through Group Policy as it will update all machines within the domain or OU with the default settings of the machine from which it was applied. For example, applying the template from a Windows Server 2003 machine across a Windows XP network would render the clients unusable.</td>
</tr>
<tr>
<td>Compatible</td>
<td>Compatws.inf</td>
<td>This contains the settings that will apply default permissions for workstations and servers for three specific user groups: Administrators, Power Users, and Users. Administrators are given the most power, Users the least. You should use this template when you want to secure your systems but also provide members of the Users group with the ability to run certified applications on the machine in question. This template should not be applied to domain controllers.</td>
</tr>
</tbody>
</table>
### TABLE 1.4 Security Templates for Servers and Clients (continued)

<table>
<thead>
<tr>
<th>Title</th>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure</td>
<td>Securews.inf and Securedc.inf</td>
<td>This templates applies increased security settings for the operating system in a manner that should not affect the way applications can be executed or how users interact with the system. In particular, it increases the security on Account Policy, auditing, and some registry elements. It also disables LAN Manager and NTLMv1 for authentication, which will limit the interoperability of operating systems; specifically, Windows NT 3.51, Windows 95, and Windows 98 should not have this applied.</td>
</tr>
<tr>
<td>Highly Secure</td>
<td>hisecws.inf and hisecdc.inf</td>
<td>A superset of the Secure templates, these apply additional levels of security and restrictions, particularly with respect to encryption and signing during authentication with servers and file shares. The result is a configuration that is only compatible with operating systems of Windows 2000 vintage or later. The Highly Secure configuration is provided for Windows 2000, Windows XP, or Windows Server 2003–based computers that operate in native (or pure) Windows 2000 or Windows Server 2003 environments only.</td>
</tr>
<tr>
<td>System Root Security</td>
<td>Rootsec.inf</td>
<td>Rootsec.inf specifies the root permissions; that is, it defines the default permissions for the root of the system drive. This template can be used to restore the root directory permissions if they are somehow modified.</td>
</tr>
</tbody>
</table>
Plan Security for Servers That Are Assigned Specific Roles

When setting security parameters, you must have a method for applying them to your systems. You can use secedit on a machine-by-machine basis, but this is obviously quite a larger process if you have to apply the changes to a number of machines.

The easiest way to achieve the same results is to use group policies. Group Policy is a configuration system that is integrated and required with Active Directory and allows you to set specific parameters on all of the computers and/or users to whom it was assigned. Group policy can be applied at any or all of these levels, so you can define a domain-wide policy for basic settings and additional security settings for specific groups, such as domain controllers, member servers, and clients (Windows 2000 or later only).

The actual security settings either can be defined directly within Group Policy, or you can use one of the many security templates that we’ve already discussed. You can also create your own security templates to apply settings to your own groups of servers.

Taken together, you can use this system to apply security settings to specific server roles. Server roles actually have new meaning in Windows Server 2003: specific services are configured by enabling specific roles on each machine. Applying security to these roles is just a matter of creating a suitable template and applying that template at the right organizational level within the Group Policy system so that it is applied to the servers in question.

<table>
<thead>
<tr>
<th>Title</th>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Terminal Server User SID</td>
<td>Notssid.inf</td>
<td>The default file system and registry access control lists that are on servers grant permissions to a Terminal Server security identifier (SID). The Terminal Server SID is used only when Terminal Server is running in application compatibility mode. If Terminal Server is not being used, this template can be applied to remove the necessary Terminal Server SIDs from the file system and registry locations.</td>
</tr>
</tbody>
</table>
In this section, we're going to look at two areas: the effects of the Group Policy system and how it can be used, and how you can create your own specialized security templates for your server roles and specifications of your network.

**Deploying Security Configurations**

Now that you know what security settings to build and apply to your servers, we need to look at how you can apply those settings. In a well-managed network, you will almost certainly be employing Active Directory to provide authentication systems for your network.

Aside from the obvious finger-saving properties of only needing one password to access the network, Active Directory also provides a number of other facilities, including centralized information on the structure, design, and content of your network. It stores this structure and member information, so wouldn’t it be nice to be able to configure settings across all of the computers that are, for example, a member of the web server group?

That’s what Group Policy does. It creates a structure of settings for your computer that can be applied to groups of machines. Group Policy assigns these settings according to the members of a specific part of the Active Directory structure, such as an organizational unit (OU), domain, or subdomain. By default, these policies are inherited and cumulative across the network structure.

So, if you apply password security settings to an entire domain, all the computers within that domain will inherit those settings. If you apply the same policy only to members of the Sales OU, then only that OU’s members will have the policy applied. Group Policy can be applied either on a computer or a user basis. This enables you to create a user-led policy that will be applied to the machine when a user logs in, a computer-led policy that applies to all the machines in a group irrespective of who logs in, or a combination of the two.

A group policy is made up of a number of Group Policy Objects (GPOs), and each GPO is a suite of settings applied to a computer or user. Multiple policies may be applied to the same user or computer at each level, except the local policy (which is only controlled by the local machine). There are a number of policies, and they are processed into the final group policy in the following order:

1. **Local policy**  Each computer has exactly one GPO that is stored locally and shared by all users of that computer for both computer and user Group Policy processing. The local GPO is stored on each system in the `%SystemRoot%\System32\GroupPolicy` directory.

2. **Site policy**  Any GPOs that have been linked to the site that the computer belongs to are processed next.
3. **Domain policy**  
Domain-wide policies are processed in the order specified by the administrator. The order is important because individual GPOs may alter previous settings.

4. **Organizational unit policy**  
These are the GPOs that apply at an OU level.

---

### Travel Assistance

Additional information on Group Policy can be found on the Microsoft website at www.Microsoft.com/gp.

---

### Creating Custom Security Templates

To enable you to apply security settings to specific server roles, you need to be able to create different templates that specify the security settings for specific groups of servers, according to their role and purpose within the organization.

To do this, you can create security templates or modify one of the existing templates to create a template specific to a server role. These templates can then be applied to the servers by importing the template into the Group Policy Objects that you create, which in turn will propagate the security settings to the servers.

### Security Template Format

Security templates are text-based files. You can create templates either manually by creating a text file with Notepad, or, and this is the best method, using the Security Templates MMC snap-in.

Security Template Sections in the text file and the corresponding Group Policy area are listed in Table 1.5.

### Account Security

There are some additional considerations you need to give to the different accounts that are configured in all client and server systems, such as the Local System account and the built-in user accounts. Some can be quite dangerous—the local Administrator built-in account, for example, has all the rights on the local machine (same as a domain administrator), including the ability to create local accounts and detach itself from the domain.

The local Administrator account cannot be deleted, but you can change its name, making it more difficult for a user to guess the account and break into it. You should also change the password of the local Administrator to something...
suitably complex,—definitely different from the domain administrator passwords. It’s probably a good idea to also use different passwords on every server for the local Administrator accounts, or at the very minimum use different passwords for domain controllers and member servers.

Also ensure that the local administrator is not a member of the Domain Admins group. All these changes can be made through Group Policy, but it’s a much better idea to do this on a local, individual basis so that you can adjust the information based on each server.

The Guest account, also created by default, is automatically disabled on both member servers and domain controllers, so you shouldn’t need to give it any further thought. If it’s been enabled, you should disable it because it presents a security risk.

Finally, consider the impact of service accounts. Your server’s services are executed within the security context of its assigned service account. By default,
most services use the Local System account, which has relatively low security clearance and abilities. Occasionally, services need to be installed with alternative account security—make sure you choose the account carefully and avoid using the local administrator or any domain accounts for services.

**Objective 1.04**

**Configure Security for Servers That Are Assigned Specific Roles**

Now that you know how you can apply security settings and policies to your servers and clients, you need to know how to apply them to individual servers. How do you choose what security settings to set for your web server, domain controller, or file server?

You can get some ideas and summary information by looking at the specific role of the server and then developing and applying a suitable policy. Before you apply these individual policies, however, you should install one of the two baseline policies:

- **Domain Controllers Baseline Policy (BaselineDC.inf)** Required to set the baseline security policy for domain controllers.
- **Member Server Baseline Policy (Baseline.inf)** Required to set the baseline security policy for member servers of a domain.

To apply further security settings, you need to understand the needs and potential problems with specific server roles.

**Evaluating Security for Individual Roles**

One of the new features of Windows Server 2003 is that many of the systems that were previously installed and enabled by default in Windows 2000 are not installed or configured in Windows Server 2003. This increases security by forcing administrators to specifically enable the functionality they need.

To enable different functionalities, you must configure Windows Server 2003 with one or more server roles. This installs and enables specific elements of functionality according to the role. Any server can have more than one role—it’s a bit like giving a computer a number of personalities.

For example, IIS, a frequent source of security breaches and problems, is not installed by default into the Windows Server 2003 operating system; it must be installed after you install Windows Server 2003.
The roles are as follows:

- **File server**  Allows a server to share files and data across a network and sets up network shares.
- **Print server**  Enables you to share printers and use the printer spool mechanisms to provide centralized management of printers and print jobs.
- **Application server**  Installs Internet Information Services (IIS) 6 and related technologies such as COM+ and ASP.NET. Provides the basic functionality required to support websites and web applications, including XML and web services.
- **Mail server**  Enables the Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP3) protocols to support basic e-mail distribution. POP3 and SMP provide a simple, Internet-compatible e-mail service that can be used for low volume e-mail-only communication within an organization.
- **Terminal services**  Enables the terminal services system to allow remote users to run applications on a central server but display the virtual desktop and interface on a local machine.
- **Remote Access/VPN server**  Enables the routing and remote access system to allow a server to route network packets (including to create a VPN) and allows clients to dial in to a server.
- **Domain controller**  Installs the Active Directory service as a server, making the machine responsible for storing and distributing Active Directory information and the authorization of user account information.
- **DNS server**  Enables the Domain Name Service for translating friendly network names into IP addresses and vice versa.
- **DHCP server**  Installs the Dynamic Host Configuration Protocol (DHCP) service that can distribute IP addresses to clients dynamically, eliminating the need to set TCP/IP parameters manually.
- **Streaming media server**  Allows you to manage and deliver Windows Media content to clients, including streaming video and audio over the Internet or an intranet.
- **WINS server**  Installs the Windows Internet Name Service (WINS), which maps IP addresses to NetBIOS computer names and vice versa.
The security requirements of your server will depend entirely on the roles configured. IIS provides support for providing websites to clients, typically over the Internet. Obviously, this means that its security requirements are more extensive than those for a DNS or DHCP server, which is accessible only to your internal LAN.

For security purposes, you need to group the service-specific server roles as defined within Windows Server 2003 into more generic roles. You can then create a security policy based on these generic roles that will apply to a server that has one of the service-specific roles. For example, DNS, DHCP, and WINS are all examples of a network infrastructure role that has different security requirements from a server running IIS.

Table 1.6 lists the various service-oriented roles and matches them to one of the member server roles. Domain controllers obviously have special needs and cannot be pigeonholed into one of the group role definitions, so you wont find it in the table. Also note that technically IIS is an application server role, but it also has special needs as a primarily public rather than private service.

### Travel Assistance

Microsoft always advises that a domain controller should be kept separate from any type of application or IIS server because it becomes difficult to secure both the application and domain controller elements.

### Securing Server Roles

Now that you know how service roles are allotted into their different roles, you can apply different security settings and facilities to them. We cover the specific issues of each role group in the next sections.

<table>
<thead>
<tr>
<th>Service Role/Server Role</th>
<th>Application Server</th>
<th>File and Print Server</th>
<th>Infrastructure Server</th>
<th>IIS Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>File server</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Print server</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application server</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
 CHAPTER 1 Planning and Implementing Server Roles and Security

TABLE 1.6 Service Roles and Their Security Group Role Affiliations (continued)

<table>
<thead>
<tr>
<th>Service Role/Server Role</th>
<th>Application Server</th>
<th>File and Print Server</th>
<th>Infrastructure Server</th>
<th>IIS Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail server X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terminal services X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Access/VPN Server</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>DNS server X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP server X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Streaming media server X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WINS server X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Application Server Roles
Application servers are used to provide application-led services such as SQL Server and Exchange. Both these systems, and many of the others that will also be installed on an application server, have their own security systems and requirements.

This makes it difficult to suggest any specific security requirements for servers supporting this service without also covering the specifics of the application server security. Using the baseline security policy for member servers provides the best basis on which to work.

IIS Server Role
IIS is an application and therefore should be part of the application server role, but it has special needs. IIS can be used for both internal (intranet) and external (Internet) application serving. Therefore, a server supporting IIS needs to protect itself from the client computers that can connect to them.

Windows Server 2003 installs IIS in a highly secure locked mode that should make it impervious from many of the most basic attacks. However, as you enable more features, particularly Web Distributed Authoring and Versioning (WebDAV) and the Active Server Pages (ASP and ASP.NET) components, you start to weaken the security by opening up more potential for break-ins and security breaches.

The baseline security policy for member servers should be sufficient for the main server components, but you will also want to use the IIS Lockdown tool
and the Microsoft Baseline Security Analyzer to check the specific security of the IIS system and websites.

Note that there is also a Group Policy setting that can be used to disable the ability to install IIS. You can use this group policy on roles other than the IIS Server role to prevent these servers from enabling IIS. It does not affect existing installations, though, so if you have a specific server that needs IIS functionality but is part of another server role group, install IIS first, then apply the group policy to the OU for the group.

**File and Printer Server Roles**

File and print services provide a way of directly accessing and updating files on your server. This means that it can be difficult to secure servers supporting these roles without also limiting or disabling legitimate access to your server. A File and Print Server group policy is available that will secure your server without affecting services. The group policy also performs the following actions:

- Enables the Spooler service, which is used for printing.
- Disables the security policy setting Digitally Sign Client Communication (Always). If this is not disabled, clients will be able to print but not view the print queue. When attempting to view the print queue, they will receive the message, “Unable to connect. Access denied.”

The file server element is the most difficult to secure effectively. You can disable the protocols that support the file service, Server Message Block (SMB) and Common Internet File System (CIFS) high-security environments, but this will effectively disable the service, even for legitimate users.

Irrespective of the Group Policy settings, you should also consider the effects of securing individual files and folders within the shared directories and ensuring that the various folders and directories are correctly configured with permissions and ownership.

**Infrastructure Server Roles**

Infrastructure servers have relatively simple security requirements. The main services that they provide are not particularly well known for their security
exploits. They also do not normally compromise security through being enabled. In general, the baseline security template should be more than adequate.

**Creating an Active Directory Structure and Deploying the Security Configuration**

Apart from the overall makeup of your Active Directory structure, such as your choices for organizational and geographical elements within the directory, you need to be able to apply the various settings and policies at a server role level. This means creating a structure that enables you to apply the settings according to the different group roles that you defined in the previous section.

In addition, you need to consider subdivision of the roles and to differentiate between public and private IIS roles, specific application server implementations, and other subdivisions in the other roles, such as the sample shown in Figure 1.1.

**Objective 1.05 Plan a Security Update Infrastructure**

They used to have these adverts for car batteries that extolled the virtues of this new make of battery that you “could fit and forget,” the implication being that you’d never ever need to worry about it again. Well, some people treat
their security in the same way. They set up their group policies, install their firewalls, and configure all their servers with the various security templates and think they are covered for every eventuality.

The truth, of course, is very different. Those car batteries weren’t fit and forget, but they did last long enough that most people probably replaced their car before they had to think about the battery again. Your security’s time lag isn’t ten years like the battery, however. You really shouldn’t go more than ten minutes without considering your system’s security—at every point, each configuration change, new user, application, or system, the security should be right there at the top of the page of things to do.

The problem with computers is that they change. You don’t set up a computer and hope that nobody uses it. More to the point, you don’t ever believe that the computer is 100 percent guaranteed secure in the first place, no matter what it said on the box. You need to constantly review your security needs as well as your security settings and the effects of any newly discovered chinks in the security armor.

Doing this by hand would take ages, especially if you factor in all of your desktop and server machines. Microsoft provides two tools that will make your life significantly easier: Microsoft Baseline Security Analyzer and Windows Update. These deserve closer attention, so we’ll look at the specific of these two below.

Microsoft Baseline Security Analyzer

Keeping your systems secure and safe from attack, malicious access, and unscrupulous individuals as well as protecting the files in the accounts department from those troublemakers in sales can be a full time job. In fact, in large companies it’s fairly common to have someone whose sole responsibility is the security of your systems.

There are ways you can make your life easier when it comes to the security of your systems, including group policies and many of the simpler, nontechnological solutions covered in the “External Security” section of this chapter. Sometimes, however, you want to be able to run a quick test and make sure that everything is safe enough to use.

Microsoft provides a tool for exactly this purpose, called the Microsoft Baseline Security Analyzer (MBSA). The MBSA checks one or more machines and the security settings for the core operating system and a number of other systems, such as IIS and SQL Server. You can use it on clients (Windows XP only) and servers (Windows NT 4, Windows 2000, and Windows Server 2003). In all cases, its purpose is to identify misconfiguration errors that led to a security compromise.
Travel Assistance

All Microsoft downloads, including MBSA, can be obtained through the main Microsoft downloads page at www.Microsoft.com/downloads.

The specific areas that MBSA checks are

- **Windows operating system** Including guest account status, file system types, file shares, administrator group privileges, members, and many others.

- **Internet Information Server** Including virtual server directory configurations, sample applications (which should be removed in most instances), and general security settings on areas like the remote administration interface. It also checks if the IIS Lockdown tool has been used to check and secure the IIS installation.

Travel Advisory

The IIS Lockdown tool checks that default website settings and features have been switched off in versions of IIS prior to 5.1. It's not required for IIS 6, part of Windows Server 2003, because all of these features arrive already disabled.

- **Microsoft SQL Server** (SQL Server 7 and 2000 only) Including authentication mode, system administration account password status, and service account memberships.

- **Desktop application checks** Including checking IIS 5.01 and later security zone settings for each local user account and macro settings for Office 2000 and XP.

- **Security updates** Including checking the installed updates on each machine against the list either on the Windows Update site or with your local Software Update Services (SUS) server, if you have one installed. This checks for patches and updates against the core OS (for the platforms supported), Internet Explorer, Windows Media Player, IIS, SQL Server, and Microsoft Exchange.

MBSA can be used either through a GUI interface or a command-line interface, and you can run full blown MBSA scans or security update scans through the HFNetChk system. You can also scan a single machine or a group of machines,
either by their Active Directory domain or by IP address range. It doesn’t matter whether you are using a client OS or a server to run and originate the tests—the only requirement is that you must have Administrator authority for each machine that you want to test.

Through the GUI, once the tool has been used to test one or more machines, you’ll get a list of the tests that were executed and an idea of the seriousness of each problem on a machine-by-machine basis. You can see a sample of the output, executed on a Windows XP machine, in Figure 1.2.

If you click the Result Details link, you’ll be taken to web pages that give more detailed information, such as the list of missing updates or settings and information that were found to be suspect. Click the How To Correct This link to get information on how to fix the problem or where to download the patches in question.

![Microsoft Baseline Security Analyzer in action](image)
Exam Tip

Make sure you know how to use MBSA and what elements it does and doesn’t check before you go into the exam. You can get a full idea of the individual elements tested through the MBSA documentation page at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/mbsawp.asp.

You should use MBSA regularly on your network to check for potential problems. Theoretically, there is no limit to the number of machines that you can check at any one time, but the checks do take some time to resolve. You should assume that the checks will take about 2 minutes per client and 5 minutes per server, although it could easily increase to 20–30 minutes on a web server with a large number of configured websites. That means you could check about ten servers and 120 machines in one 8-hour period.

Using MBSA once a month is not a bad idea, but you might want to use it more frequently on your servers or critical desktop machines. Remember that if you are using Automatic Updates, especially in combination with SUS, the most important aspect—security updates—will have already been covered. That’s what we’re going to be looking at next.

Patches and Updates

Security is not just about restricting users, setting file permissions, and employing network level tools like Active Directory. It’s also about keeping your machine up to date with the latest patches and updates. With the best will in the world, it would be impossible for Microsoft to create such a complex and advanced system as Windows Server 2003 without there being a few problems.

These problems take a number of forms, but they basically fall into two categories: stability bugs and security bugs. Stability bugs affect the stability of your server that may, in turn, affect the stability and security of your network. For example, a stability bug could cause your server to fall over when an application tries to allocate itself a specific amount of memory, even if your server is technically able honor the request.

Security bugs are potentially more serious. Recent years have seen an increase in publicity about a number of worms and viruses to hit the Internet and be spread through Windows servers, particularly IIS. Most of these used an exploit in the operating system (particularly IIS) that allowed them to propagate across thousands of computers through the Internet in a relatively short space of time.
Local Lingo

Worms and viruses  A worm is a program that propagates itself over a network, while a virus is one that may propagate itself through a number of means, including a network, by copying itself to removable disks or spreading itself through e-mails. Not all worms and viruses are malicious or cause any serious damage, but even the relatively benign versions can be problematic.

Local Lingo

Exploit  Exploits are ways of attacking or bypassing the security of an operating system or application through a previously unknown or undocumented part of the system. The problem with exploits is that traditional security mechanisms, such as firewalls, frequently can't protect you because the exploit uses an otherwise legitimate method to contact your server.

The way to protect yourself from these, or recover from them if they have already happened to you, is to keep your systems up to date with the latest patches and security fixes.

Patch/Update Installation

Microsoft makes security and critical (stability) updates available on their website (www.Microsoft.com/downloads), which you can download and install as necessary. To keep up with the updates and patches though, you need to regularly check the site for updates. For a more automated solution, use the Windows Update or Automatic Update service. Alternative, more extensive sites and configuration can make use of a localized Software Update Service.

Whichever solution you choose, you should always test the patches and updates that are supplied. This is not because they may cause more problems than they solve (although this has happened) but because it may upset some part of your system or configuration in a way that neither you nor Microsoft can predict.

To give a good example, one of our clients used an undocumented feature (read that as “bug”—it’s all about classification), which should have been removed, to provide a particular suite of functionality to their clients. Everything was working fine until a security patched “fixed” (read that as “eliminated”) the feature and thereby rendered their software and solution unworkable. The client didn’t realize this until the users complained that things had stopped working, and it took a little while to work out what had actually happened.

If they had tested the patch before blindly applying it to all of their servers, they would have been able to spot the problem and prevent the patch from being
applied. This would have given them the necessary time to redevelop their application using the correct systems rather than a backdoor approach.

The same rules and restrictions should apply to your network—however much you do or don’t trust a software supplier, you must test what they provide to you before blindly applying it to all your systems.

**Windows Update**

Windows Update was a feature of Windows 98 that has since been extended and expanded upon in more recent editions of Windows operating systems. Essentially, Windows Update is a website that enables you to check, select, download, and install specific updates to your machine.

To use it, visit the Windows Update site, which uses an ActiveX application to determine what is installed on your machine and what is available from Microsoft, thereby building a list of potential patches—as shown in Figure 1.3.

The problem with Windows Update is that it requires manual intervention to operate. Although this means you can exercise a level of control over which patches are installed, the downside is that as the number of servers and clients increases in your organization, it becomes more and more time-consuming to use Windows Update to keep your systems up to date.
Automatic Updates

Automatic Update is a new feature built directly into Windows Server 2003 and Windows XP. Windows 2000 gained the ability to interface to the Automatic Update system with Service Pack 3, and it’s also available as an installable patch on all previous editions of Windows down to Windows 95.

The Automatic Update system makes use of Windows Update technology to enable critical updates and security patches to be automatically downloaded to your machine. In its basic format, it doesn’t automatically install them, but it notifies you that they are ready to be installed.

Travel Assistance

Automatic Update is disabled by default, but it’s automatically enabled into the notification system after you have installed the OS and rebooted the machine once.

You can change this behavior by using the Automatic Updates control panel for pre-Windows XP systems or the System Control Panel for Windows XP and Windows Server 2003 machines. The configurable properties are:

- How to download/install changes. There are three options: just notify that updates are available, download and notify that updates are read to install, or download and install the patches automatically.
- Download/check frequency and time of day.

You can either change these parameters manually on each machine (not recommended for those with full-time jobs), or you can use Group Policy to set these parameters throughout specific machines and organization units. The Group Policy location for this is Computer Configuration | Administrative Templates | Windows Components | Windows Update.

Through Group Policy you can also set how patches that require a restart should be handled: either automatically reboot the machine after the patches are installed, or notify the user that a restart is required after the patches are installed.

Which option you choose should depend on the machine and its role. Clients can normally be restarted automatically—providing the updates are downloaded and installed outside of normal working hours. For servers, you may want to avoid automatically restarting servers that are required to support your infrastructure. Mail servers (particularly those running Microsoft Exchange...
Server), web servers, and domain controllers should be probably not be automatically rebooted.

**Microsoft Software Update Services**

The problem with Windows Update is that the system is entirely client driven. To select and install updates requires human intervention to visit the initial site, select the packages, and download the various components. Automatic Updates solve this by automating the download and installation of the vital updates that will keep your servers and clients stable.

In a relatively small network this is not an issue, but in a larger network with hundreds or thousands of servers and clients, the updating process can have a significant effect on your Internet connectivity and the overall stability of the network. The Automatic Update system also eliminates an element of control—the system downloads all updates that Microsoft has released, without giving you the opportunity to test the effects or even approve the installation unless you resort back to a human-driven interface. Again, this is time consuming and something that should be avoided. What, then, is the solution?

Software Update Services (SUS) enables you to create one or more servers within a network that download the critical and security updates. Your other servers and clients can then be configured (through Group Policy) to use your local server as their source for the updates. This means that updates are downloaded once and then distributed through to the rest of your network using your LAN, rather than tying up the Internet connection with multiple downloads of the same update.

**Travel Advisory**

SUS handles only the critical and security updates. Additional updates and software releases that are not deemed to present a potential stability or security risk are not included. You’ll need to use other methods to distribute these updates to your clients and servers.

SUS also allows you to approve individual updates so that you can test an update and approve it for distribution to your servers and clients after you are satisfied that it will not affect your existing systems. You can see a sample of the approval window in Figure 1.4.
You can get more information on Microsoft Software Update Services at http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp.

If you use SUS, however, you need to consider the impact of SUS on your network and your network design, as well as how updates should be distributed across your network. Taking the first issue in hand, SUS has the same basic issues as Automatic Updates—that means you need to choose when updates are downloaded and installed and whether machines automatically reboot without human intervention after the updates have been controlled.

Unlike the user-controlled automatic update system, the group policy that controls automatic updates also enables you to specify the name of the machine from which updates are downloaded. Because Group Policy is based on the organization structure of your Active Directory installation, you can specify different servers for different OUs. This leads to a number of network-oriented benefits of the SUS system.
The effect of SUS on your network depends entirely on the size and design of the network. It’s tempting to install one server to provide SUS for the rest of your network, but in a large network this can create huge amounts of traffic and bottlenecks that will ultimately affect the performance of your network and your user’s perception of the effectiveness of the IT department.

**Travel Advisory**

Our theory about system administration and users is that your users’ perception of the system administrator and the IT department have more of an effect than hard data. For example, if your users complain about slow network speeds, you will be perceived as doing a bad job, even if you know that the network is running at 100 percent efficiency. Remember this when you prioritize jobs and plan your network—I guarantee it will make a difference!

You can do this through SUS because SUS appears to outside clients to be the same as the Automatic Update portion of Windows Update. If it didn’t, clients wouldn’t be able to use SUS just as readily as they use Microsoft’s servers for Automatic Updates. The advantage of this design is that you can stack SUS servers within a network environment, reproducing the effect of caching the updates from the Internet, which will reduce the load on the network.

For example, Figure 1.5 shows a distributed SUS network using localized SUS servers for each department. This method reduces the potential load of 500 clients from each department (a total of over 1500 machines) from requesting updates from a single server, which would almost certainly saturate the network and have a significant effect on the performance of the server itself.

The secondary benefit of a structure layout is that the approvals system also works through the structure. If you have one server, called Bear, contacting Microsoft for updates, and all the other servers are contacting Bear for their updates, you can still manage which updates are approved for your network by using the approvals system on Bear. The SUS servers that contact Bear will only download updates that have been approved on Bear. The updates will also need to be approved on these servers, but this is a minor task once the main download and approval has taken place.

This last feature also enables you to control the way updates are distributed to different collections of machines. In Figure 1.6, for example, there’s one central SUS server and two SUS servers downstream, one for clients and one for the web servers.
By approving updates on the central server, the two servers downstream receive all the updates. However, updates to the web servers and updates to the clients can be independently controlled by approving individual updates on each of the downstream servers. This allows you, for example, to install patches for known exploits on the web servers immediately, as these are public facing, while waiting until further tests have been completed before approving the same update for your clients.

To summarize, when planning for using SUS you need to consider all of the issues pertaining to automatic updates:

- Your network size
- Your network layout
- Your update and patching policy on a departmental and/or role basis

FIGURE 1.5 Localized SUS servers in a larger organization
Objective 1.01: Evaluate and Select the Operating System to Install on Computers in an Enterprise

There are effectively four new versions of Windows Server 2003: Standard Edition, Enterprise Edition, Datacenter Edition, and Web Edition. You should be able to identify the differences between the versions and pick the one with the appropriate features and capabilities according to your needs.

Objective 1.02: Plan a Secure Baseline Installation

Before computers are deployed in the organization, a baseline security configuration for computers needs to be defined. A baseline can be implemented either during or after the initial installation of the operating system, applying security templates to computers that have similar security requirements. The default Security Templates can be used, or they can be a starting point for modifying a template specific to the environment.
Objective 1.03: Plan Security for Servers That Are Assigned Specific Roles
The services and applications that are installed on a computer depend on the role that was selected when the Windows Server 2003 was installed. Computers use different threat models dependent on their defined role. Designing security for computers with specific roles requires detailed knowledge and experience with the services or applications that run on the computers. The goal of security policies is to define procedures for configuring and managing security in the network environment. Group Policy can help implement the security policy for all workstations and servers in the Active Directory domains. Group Policy used with the OU structure can be used to define specific security settings for certain server roles.

Objective 1.04: Configure Security for Servers That Are Assigned Specific Roles
Once baseline policies have been installed, the servers will be significantly more secure. From this state, more specific settings may need to be enabled, adding additional security to the baseline policy.

Objective 1.05: Plan a Security Update Infrastructure
Updating your machines with the latest patches and updates is at least as important as defining the original, as it ensures that your system is kept up to date. There are a number of tools that can help you in this task. The Microsoft Baseline Security Analyzer (MBSA) can identify outstanding patches that need to be applied to different systems. Windows Update can be configured on individual machines to automatically update a system with the latest patches and updates. If you want to centralize this service, either to reduce your Internet load or place a central point of control, you can use Software Update Services to download and distribute updates to your clients.

REVIEW QUESTIONS

1. You are the network administrator for a business that has 100 employees. You are responsible for implementing file and print services using Windows Server 2003. You want to implement a cost-effective solution with the possibility of growth, such as shared Internet connectivity. What version should you use?
   A. Windows Server 2003, Standard Edition
   C. Windows Server 2003, Datacenter Edition
2. You are the network administrator for a healthcare facility. You are responsible for installing a server to run a database using Windows Server 2003. This is a very important database that needs to be as reliable and stable as possible. Your facility has a variety of hardware and software, and you don’t want to get locked into a proprietary solution. What edition of Windows Server 2003 should you choose?
   A. Windows Server 2003, Standard Edition
   C. Windows Server 2003, Datacenter Edition

3. You are designing a plan to create a secure baseline for your network. What is the first step for creating a secure baseline?
   A. Create security policy
   B. Create custom security templates
   C. Test security templates
   D. Deploy security templates

4. You are the network administrator for a magazine company that has 300 employees. You are responsible for the implementation of a secure DNS server. You have taken the steps for a secure installation and are using Group Policy to secure your servers. What type of server role template would you apply to the DNS server to ensure the appropriate Group Policy will be applied?
   A. Domain Controller
   B. Application Servers
   C. File and Print Servers
   D. IIS Servers
   E. Infrastructure Servers

5. You are the network administrator for a magazine company that has 300 employees. You are responsible for the implementation of securing domain accounts. To what location in the Active Directory structure does this group policy need to be imported to apply to all Domain Accounts?
   A. Site
   B. Domain
   C. Domain controller OU
   D. Member server OU
   E. User OU
6. You are the network administrator for a magazine company that has 300 employees. You have created a member server baseline security template that you want to apply specifically to the member servers in your Active Directory structure. What is the next step?
   A. Use secedit to import the policy to the Primary Domain Controller.
   B. Use secedit to import the policy to the primary member server.
   C. Import the template to the Group Policy Object at the Domain.
   D. Import the template to the Group Policy Object at the Member Servers OU.
   E. Import the template to the Group Policy Object at the Domain Controllers OU.

7. You are the network administrator for a magazine company that has 300 employees. You are tasked with the implementation of a Member Server Security Baseline. A security policy for the domain controllers has already been implemented. What would be the best location in the Active Directory structure for this Group Policy to be imported into to apply to member servers?
   A. Site
   B. Domain
   C. Domain controller OU
   D. Member server OU
   E. User OU

REVIEW ANSWERS

1. A It’s designed for small organizations and departments and provides file and print services and secure Internet connectivity.
2. B Customers seeking higher levels of availability should choose Enterprise or Datacenter Editions, but because the Datacenter Edition offers a proprietary solution, the Enterprise Edition should be selected.
3. A This policy contains all business and technical requirements for the computer, operating system, and applications.
4. E Designed to increase security of servers acting as DNS, DHCP, and WINS servers.
5. This level is to address the common security requirements such as account policies and audit policies that must be enforced on all servers. Password and account policies will only affect domain accounts if the policies are set at the domain level.

6. After creating the template, it needs to be imported into a Group Policy Object using Active Directory Users and Computers.

7. Having all member servers in OUs by server roles is a good way to organize servers by function. If all member servers are contained in OUs under the Members Servers OU, that OU is the logical choice for placing this group policy.