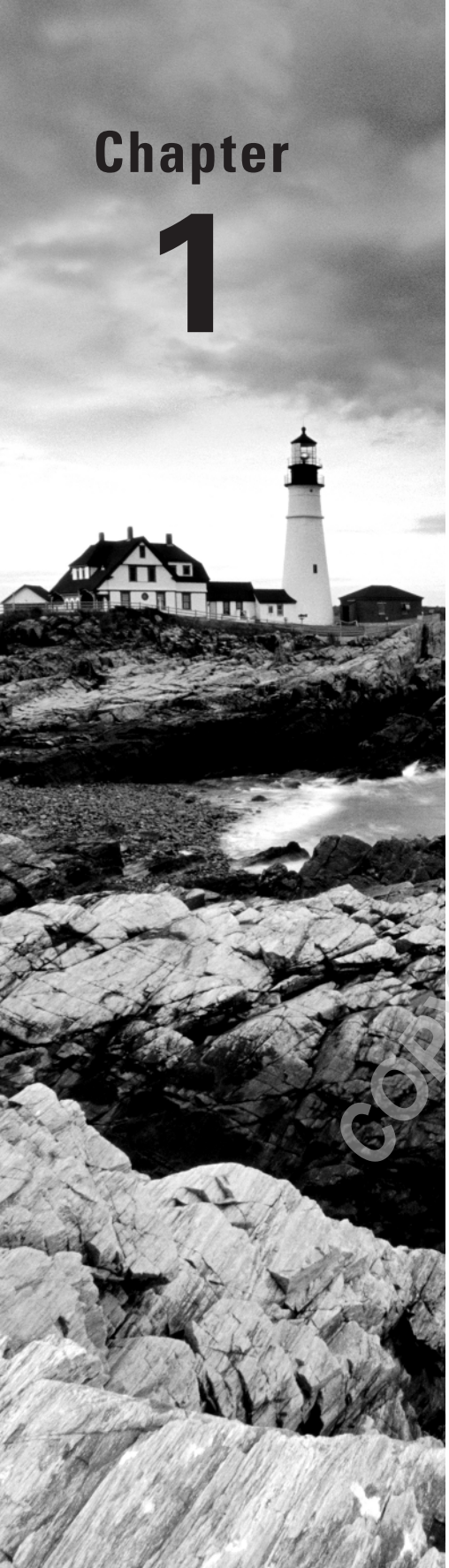


Chapter 1

Introducing Windows Server 2008

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Planning for Server Deployment**
  - Plan Server Installations and Upgrades. May include but is not limited to: Windows Server 2008 edition selection, rollback planning, Bitlocker implementation requirements.
- ✓ **Planning for Server Management**
  - Plan Server Management Strategies. May include but is not limited to: remote administration, remote desktop, server management technologies, Server Manager and ServerManagerCMD, delegation policies and procedures.

This chapter is designed to give you a short overview of many of the features of Windows Server 2008, especially as they relate to the 70-646 exam. Future chapters will delve a little deeper into the topics, but first we'll start with a foundation.

I fully expect you to want to install a copy of Windows Server 2008 on a system. After all, it's hard to learn something that you haven't seen and played with. One of the primary sections of this chapter will walk you through the steps of installing Server 2008 and configuring it as a domain controller.

You'll notice in the list of objectives that rollback planning, Bitlocker implementation requirements, remote administration, remote desktop, and delegation policies and procedures are listed. Rollback planning is covered in Chapter 2, "Planning Server Deployments." Remote administration and remote desktop are covered in Chapter 3, "Using Windows Server 2008 Server Management Tools." Chapter 5, "Monitoring and Maintaining Active Directory" covers delegation policies and procedures. Bitlocker implementation requirements are covered in Chapter 8, "Planning Windows Server 2008 Security."

Windows Server 2008 Editions

Microsoft has released multiple editions of Windows Server 2008. Most editions come in both 32-bit and 64-bit editions except for the Itanium edition, which comes only in the 64-bit edition.

Three include virtualization capabilities using the Hyper-V virtualization technology. Hyper-V is the virtual machine technology that allows multiple operating systems to run concurrently on the same system. Virtualization can be used for server consolidation where multiple servers can be combined onto a single server or to consolidate testing or development environments. Hyper-V will work only on 64-bit systems.

The editions that include Hyper-V are as follows. The most significant differences between these editions are related to how many virtual servers each edition can host.

Windows Server 2008 Standard with Hyper-V The Standard with Hyper-V edition is for small to medium-sized businesses. It includes support for a single virtual server.

Windows Server 2008 Enterprise with Hyper-V The Enterprise edition is for larger organizations and can support up to four virtual servers. It also includes support for clustering and hot-add memory capabilities.

Windows Server 2008 Datacenter with Hyper-V The Datacenter edition is for high-end applications and large-scale virtualization. It adds to the features of the Enterprise edition, including hot-add processor capabilities. An unlimited number of virtual servers can be hosted on the Datacenter edition.

The Enterprise and Datacenter editions both support hot-add capabilities. *Hot-add means you can add* physical processors or physical memory without shutting down the system. The system hardware must also support this capability.

The same three editions exist without Hyper-V:

Windows Server 2008 Standard without Hyper-V The Standard with Hyper-V edition is for small to medium-sized businesses.

Windows Server 2008 Enterprise without Hyper-V The Enterprise edition is for larger organizations.

Windows Server 2008 Datacenter without Hyper-V The Datacenter edition is for high-end applications, including very large databases.

Additionally, two editions are designed for specific workloads:

Windows Web Server 2008 This edition is designed to be a dedicated web server and hosts Internet Information Services (IIS) edition 7.0 and all the associated components such as ASP.NET and the Microsoft .NET Framework.

Windows Server 2008 for Itanium-based systems This is designed to work on systems using the high-end 64-bit Itanium processors. It is optimized for large databases.

Real World Scenario

Choosing the Correct Operating System

Consider this scenario: You are working as a network administrator, and the company is considering consolidating several servers onto a single server using Windows Virtualization. It will host three virtual servers. Which operating system would you use?

First, you would use one of the editions that includes Hyper-V. These are the Standard, Enterprise, and Datacenter editions. Second, you would need to choose an edition that supports five virtual servers. Standard supports one virtual server, Enterprise supports up to four virtual servers, and Datacenter supports an unlimited number of servers. Windows Server 2008 Enterprise edition with Hyper-V will meet your needs.

Table 1.1, Table 1.2, and Table 1.3 show the different server roles matched to the available Windows Server 2008 editions.

TABLE 1.1 Specialized Server Roles

Server Role	Web	Itanium	Standard	Enterprise	Datacenter
Web Services (IIS)	Yes	Yes	Yes	Yes	Yes
Application Server	No	Yes	Yes	Yes	Yes
Print Services	No	No	Yes	Yes	Yes
Hyper-V	No	No	Yes	Yes	Yes

Notice that the Web edition supports the Web Services role running IIS and nothing else. The Itanium edition supports high-end application server applications such as Microsoft's SQL Server with very large databases or Microsoft Exchange Server with a large number of users and mailboxes.

TABLE 1.2 Active Directory (AD) Server Roles

Server Role	Web	Itanium	Standard	Enterprise	Datacenter
AD Domain Services	No	No	Yes	Yes	Yes
AD Lightweight Directory Services	No	No	Yes	Yes	Yes
AD Rights Management Services	No	No	Yes	Yes	Yes
AD Certificate Services	No	No	Partial	Yes	Yes
AD Federation Services	No	No	No	Yes	Yes

The Standard edition supports creating certificate authorities but doesn't support all of the functionality of certificate services.

TABLE 1.3 Network Infrastructure and General Server Roles

Server Role	Web	Itanium	Standard	Enterprise	Datacenter
DHCP Server	No	No	Yes	Yes	Yes
DNS Server	No	No	Yes	Yes	Yes
Fax Server	No	No	Yes	Yes	Yes
UDDI Services	No	No	Yes	Yes	Yes
Windows Deployment Services	No	No	Yes	Yes	Yes
File Services	No	No	Partial	Yes	Yes
Network Policy and Access Services	No	No	Partial	Yes	Yes
Terminal Services	No	No	Partial	Yes	Yes

The Standard edition has limited support for some of these roles. For File Services, only one Distributed File System (DFS) root is supported. For Network Policy and Access Services, it is limited to 250 RRAS connections, 50 IAS connections, and 2 IAS Server Groups. For Terminal Services, it is limited to 250 connections.

Key Benefits of Windows Server 2008

When weighing the costs of upgrading from your current operating system to Windows Server 2008, IT professionals must consider what the benefits are and then determine whether the benefits are worth the costs.

Although the following benefits are extensive, they make a difference only if your environment will use the added benefits. Expect Microsoft to stress the benefits of new features in every way possible—including in exams.

IIS 7 and the .NET Framework

The Windows Server 2008 Web edition has been expressly created to support the Web role. It hosts IIS 7 and includes support for ASP.NET and the current versions of the .NET Framework. When released, the .NET Framework 3.0 was included. However, the .NET Framework 3.5 can be downloaded and installed if your web developers need it for their web applications.

As background, the most widely used web server on the Internet is Apache, which is a free product that can run on Unix—or one of the Unix derivatives (such as Linux)—which is also free. Microsoft has been steadily breaking into this market with its Web edition product in Windows Server 2003 and IIS 6. Windows Server 2008 offers additional capabilities with the Web edition and IIS 7.

However, IIS is not only for the Internet. Many companies use IIS on their intranet to serve Internet technologies to internal employees. IIS 7 supports web pages, websites, web applications, and web services. While the Web edition provides dedicated support for IIS 7, any edition can run IIS 7.

Microsoft has improved the security of IIS by ensuring that separate web applications are isolated from each other in a "sandboxed" configuration. Of significant value to server administrators, the IIS administration tool has been improved for many of the common administrative tasks.

Chapter 7, "Planning Terminal Services Servers," will cover the maintenance of IIS 7 in more depth.

Virtualization

The Windows Server virtualization role is one of the biggest additions in Windows Server 2008 and, arguably, one of the most exciting.

For years, there has been an ongoing trend of server consolidation. For example, instead of having one DHCP server, one file server, and one IIS server, it's possible to have one server running all of these roles. Individually, each of the servers might be using only 5 to 10 percent of the available processing power. With all of the roles on a single server, the server's resources are more fully being utilized. From a management perspective, spending $20,000 or so on a single server and using only about 5 percent of it just doesn't make fiscal sense.

However, consolidating roles onto a single server does have drawbacks. As a simple example, a patch applied for one service may have an unwanted side effect on another service. However, if each server is running within the host as an isolated system, then changes to one system do not affect another system.

Consider Figure 1.1. If you're running Windows Server 2008 Enterprise edition, you can have as many as four virtual servers. In the figure, three virtual servers are running: one is running Windows 2008, one is running Linux (Novell SUSE Linux Enterprise Server), and one is running Windows Server 2003. Each of these virtual servers is completely isolated from the others, but they are sharing the host's network interface card (NIC) and other hardware resources.

At this writing, the only Linux version supported in Hyper-V is Novell SUSE Linux Enterprise Server.

From the network perspective, the four servers (the host and the three virtual servers) would appear as shown in Figure 1.2. Even though the virtual servers are hosted within a single Windows Server 2008 system, they appear as separate individual servers. They have their own hostnames and their own IP addresses.

Virtualization solves many of the problems that occurred with traditional server consolidation. It allows multiple servers to be consolidated onto a single server, while still allowing each server to remain isolated from other servers hosted on the same machine.

FIGURE 1.1 Virtual server within a host

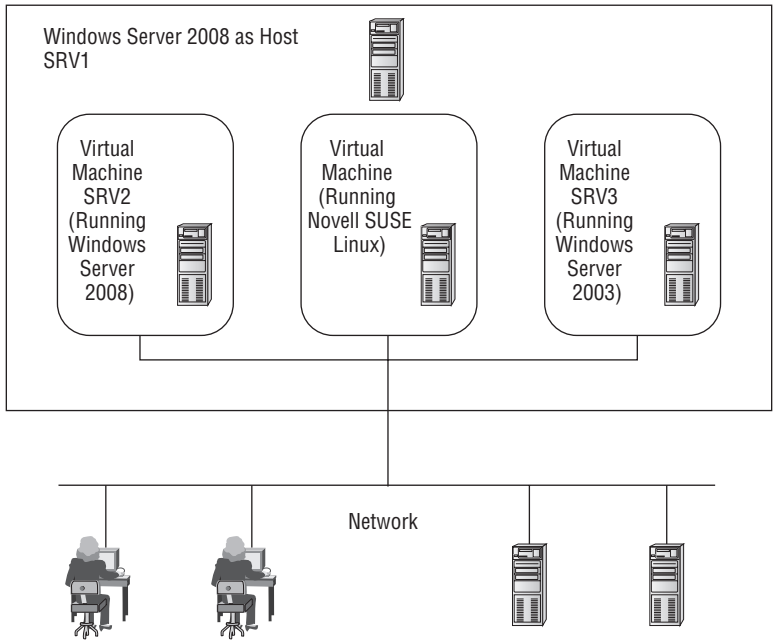
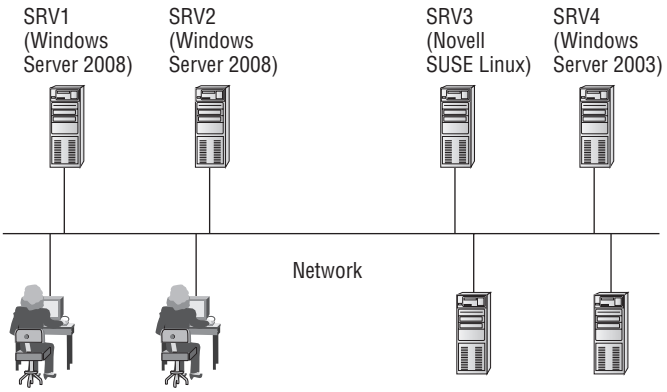


FIGURE 1.2 Virtual servers on a network



When planning for a Windows Server 2008 virtualization solution, remember a few key points:

- The host must be running a 64-bit edition of Windows Server 2008. (Virtual machines can run either 32-bit or 64-bit editions).
- Windows Server 2008 Standard edition supports one virtual server.
- Windows Server 2008 Enterprise edition supports as many as four virtual servers.
- Windows Server 2008 Datacenter edition supports an unlimited number of virtual servers.
- Hardware requirements of the host depend on the hardware requirements of the individual virtual machines. It wouldn't be uncommon to see a host designed to support many virtual servers with as many as 32 or more processors and 64GB or more of RAM.

Chapter 2, "Planning Server Deployments," will cover Windows Server virtualization in more depth.

Security

Security is intertwined in all aspects of the operating system. Since before the release of Windows XP SP2, Microsoft has developed products with the mantra of SD^3+C (Secure by Design, Secure by Default, Secure in Deployment and Communications).

In other words, security is considered in the entire life cycle of any of Microsoft's products. It wasn't always that way. In the past, Microsoft had usability as the most important aspect of the products, and the security was implemented toward the end of the development process. Inevitably, this caused problems.

Some of the security improvements include the following:

BitLocker Drive Encryption BitLocker Drive Encryption available on Server 2008 is the same feature available in Vista Enterprise and Vista Ultimate. It allows entire data volumes (any non-OS volume) to be protected with encryption. If a system is stolen, BitLocker makes it significantly more difficult to boot from another added volume and then access existing data. This can protect regular data and also operating system data such as the Active Directory database on a domain controller.

Network Access Protection (NAP) When clients access the network remotely (via dial-up or VPN remote access technologies), there is the risk that they aren't healthy. For example, they could be infected with viruses or not have the most recent updates and patches. NAP allows the system to check the health of these clients before they are allowed access. Unhealthy clients can be quarantined until the health problems are addressed.

Improved Security Log Many of the events recorded in the security log have been improved. For example, when audited data is changed, not only is the event listed, but also new and old values are included. Additional events have been added to show permission changes and IPSec activity.

Chapter 8, "Planning Windows Server 2008 Security," has a section dedicated to security, but you can expect security topics to come up throughout the book.

Interaction with Vista

Windows Server 2008 and Windows Vista are designed to work best together. Some of the features that are available when Windows Vista and Server 2008 are used on the same network are as follows:

Improved Group Policy Many additional Group Policy management settings are available to manage Vista clients. As one example, Group Policy can be used to limit bandwidth usage by individual applications.

Event subscription This allows you to configure computers to monitor for specific events and forward them to other computers. With event subscription, you can more easily centrally monitor computers on your network.

NAP features When Vista clients access a network access server (using either dial-in or VPN technologies), NAP features built into both Vista and Server 2008 protect the network. NAP will check the client to ensure it is compliant with predefined security requirements. If not, NAP can restrict the client from accessing the network until the security issues are addressed.

IPv6 support Both Vista and Server 2008 support the use of both of both IPv4 and IPv6. IPv6 is installed and active by default.

Windows XP and Windows Server 2003

What Microsoft did with Windows Vista and Windows Server 2008 is similar to how it released Windows XP and Windows Server 2003.

First, the desktop operating system was released. While consumers started trying the new operating system, the final development on the Server product was being finished.

I remember that when Windows XP came out, people were complaining about it. However, once Server 2003 came out and administrators realized how well Windows XP and Windows Server 2003 worked together, the migration to Windows XP began in earnest.

When Windows Vista was released, people were complaining about it. I fully expect that once administrators begin migrating to Windows Server 2008 and realize how well Windows Vista and Windows Server 2008 work together, the migration to Windows Vista will move into full swing.

History repeats itself. Even in the IT world.

New Features of Windows Server 2008

If you're coming to Windows Server 2008 from a Windows Server 2003 background, you're probably very interested in learning what's new. There's a lot that's similar, which will reduce your learning curve. There's also a lot that's new.

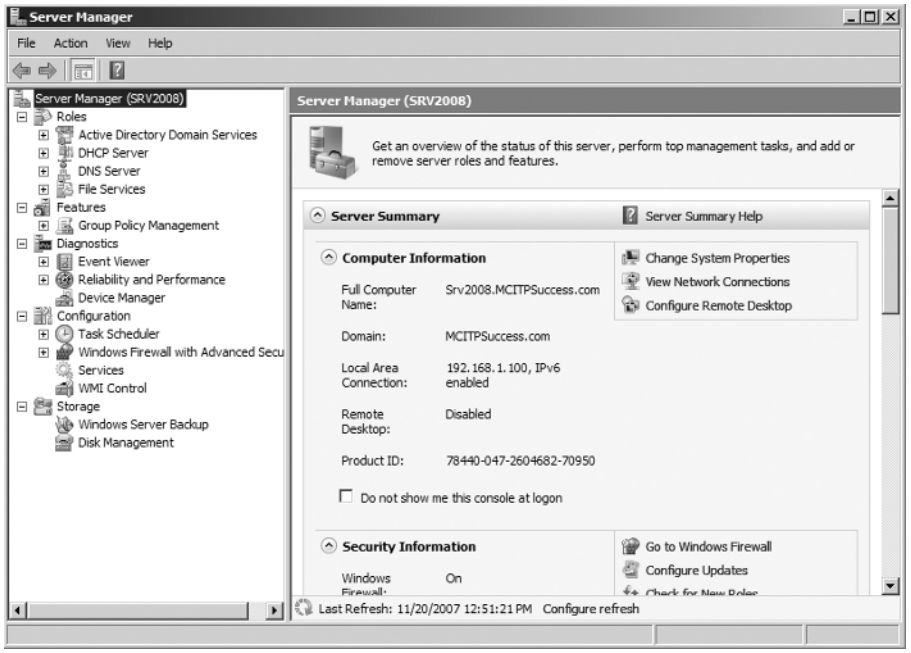
Server Manager

Server Manager is a new console designed to streamline the management of a Windows Server 2008 server. As an administrator, expect to use Server Manager for many different purposes.

The first time you looked at Event Viewer in an operating system, it was new and different. However, in time, Event Viewer became a common tool you used often that was very simple to use. Expect Server Manager to be as common to you as Event Viewer. As a matter of fact, it even includes some of Event Viewer's data.

Figure 1.3 shows Server Manager. It's actually a Microsoft Management Console (MMC) with several useful snap-ins added.

FIGURE 1.3 Server Manager



Server Manager includes many tools that can be used to do the following:

Manage a server's identity Here you can find basic computer information such the computer name, workgroup or domain name, local area connection data, and whether remote desktop is enabled. It also includes a link to system properties, so many of these items can be modified.

Display the current status of the server Server Manager queries the system logs and identifies the types of messages that have been listed. If warnings or errors are found in the logs for the role, an icon appears indicating the health of the server.

Easily identify problems with any installed roles Each role has a summary page that shows events for the role. This is a filtered view showing only the events for this role. The actual number of informational messages, warnings, and errors are listed, and you can double-click any of the events to view the message.

Manage server roles, including adding and removing roles As many as 17 roles can be installed on the server, and by clicking the Roles selection, each of the installed roles is listed. You can add roles by clicking the Add Roles link, which will launch the Add Roles Wizard. Similarly, you can remove roles by clicking the Remove Roles link.

Add and remove features Features (such as Windows PowerShell or BitLocker Encryption) can be added or removed using Server Manager.

Perform diagnostics Access to Event Viewer, the Reliability and Performance Monitor tools, and Device Manager are accessible here. These tools allow you to do some basic investigations when troubleshooting server problems.

Configure the server Four snap-ins are included: Task Scheduler, Windows Firewall, Services, and WMI Control.

Configure backups and disk store Windows Server Backup and Disk Management tools are included here.

You'll use the Server Manager tool in maintenance and management tasks covered throughout this book.

To launch Server Manager, you can select Start ➢ Administrative Tools ➢ Server Manager. Also, you can right-click Computer in the Start menu and select Manage.

Server Manager has a related command-line tool named `ServerManagerCmd.exe`. Many of the same tasks performed through the Server Manager GUI can be performed via the command-line tool.

The strength of any command-line tool is the ability to script the tasks required and then, when necessary, simply rerun the script. You no longer need to wade through the screens and hope you're remembering exactly what you clicked last time. Instead, you

simply run your verified script, and you're done. Additionally, you can schedule scripts to run at some future time.

You'll be using Server Manager throughout the book.

Server Core

Server Core is a completely new feature in Windows Server 2008. It allows you to install only what's needed on the server to support the specific role the server will assume.

For example, if you're planning on creating a server that will be a DHCP server and only a DHCP server, you can use Server Core. Instead of installing the full Windows Server 2008 operating system, Server Core will install only a subset of the executable files and supporting dynamic link libraries (DLLs) needed for the Role you select.

A significant difference between Server Core and the full operating system is that Server Core does not have a graphical user interface (GUI). Instead, all interaction with Server Core takes place through the command line.

Server Core provides several benefits:

- It requires less software so uses less disk space. Only about 1GB is used for the install.
- Since it is less software, it requires fewer updates.
- It minimizes the attack surface since fewer ports are opened by default.
- It's easier to manage.

Server Core cannot be used for all possible server roles, but it can be used with many. The following server roles are supported on Server Core:

- Active Directory Domain Services
- Active Directory Lightweight Directory Services (AD LDS)
- DHCP Server
- DNS Server
- File Services
- Print Services
- Web Services
- Hyper-V

Server Core does not include all the features available on other Server installations. For example, it does not include the .NET Framework or Internet Explorer.

Server Core will be explored in greater depth in Chapter 2, "Planning Server Deployments."

PowerShell

The difference between a good administrator and a great administrator is often determined by their ability to script.

PowerShell is scripting on steroids—in a good way. It combines the command-line shell with a scripting language and adds more than 130 command-line tools (called *cmdlets*).

As an administrator, expect to use PowerShell quite frequently for many administrative and management tasks. Currently, you can use PowerShell with the following:

- Exchange Server
- SQL Server
- Internet Information Services
- Terminal Services
- Active Directory Domain Services
- Managing services, processes, and the registry

Windows PowerShell isn't installed by default. However, you can easily install it using the Server Manager's Add Features selection.

Windows Deployment Services

One of the most time-consuming tasks involved with computers can be setting up new systems. To install the operating system alone, it may take 30 minutes. Add the time it takes to install current patches, updates, and additional applications, as well as set up baseline security, and your time for a single system can be three or more hours. And that's just one box!

If you have 20 computers to set up, it can take one-and-a-half workweeks (60 hours). In short, this is unacceptable.

Historically, administrators have used imaging technologies (such as Symantec's Ghost) to capture an image and then deploy this image to multiple computers.

Remote Installation Services (RIS) was Microsoft's previous foray into automating the installation of systems. Unfortunately, it had some issues that prevented it from becoming popular with a lot of administrators. Windows Deployment Services (WDS) is a significant redesign of RIS.

Windows Deployment Services uses the Windows Image (WIM) format. A significant improvement with WIM over RIS images is that it is file-based and works well across many different hardware platforms. Further, tools are available that allow the images to be modified without having to completely rebuild the image.

WDS includes three primary component categories:

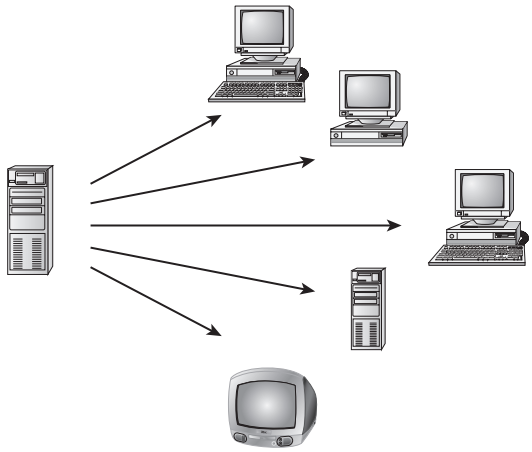
Server components The server components provide a method for a client to be able to boot with network access and load the operating system. It includes a Preboot Execution Environment (PXE, often called "pixie") server and Trivial File Transfer Protocol (TFTP) server. The server includes a shared folder with images and other files used to load an image onto a remote computer.

Client components The client components include a Windows Pre-Installation Environment (Windows PE) that allow the client to boot into a graphical user interface and select an appropriate image from the server.

Management components WDS includes tools used to manage server, images, and client computer accounts. For example, Sysprep is used to remove computer unique information (such as SIDs) before capturing images, and the WDS Capture utility is used to capture images and store them in the WIM format.

Figure 1.4 shows how WDS would work. The WDS server holds the images. PXE clients would boot and then connect to the WDS server. A Windows PE image would be downloaded to the client. This image includes a graphical user interface that could be used with user interaction or scripted to automate the process.

FIGURE 1.4 Windows Deployment Services



You'll explore Windows Deployment Services in greater depth in Chapter 2.

New Functionality in Terminal Services

Terminal Services provides two distinct capabilities:

For the administrator Allows the administrator to remotely administer systems using Remote Desktop Connection or Remote Desktops. With Windows Server 2008, Remote Desktop Connection 6.0 is available, which provides some security improvements, but generally, the remote desktop functionality is similar in Windows Server 2008 as it was in Windows Server 2003.

For end users Allows end users to run programs from Terminal Services servers. The significant change in Windows Server 2008 is the ability for multiple users to run programs centrally from a single server. From the user's perspective, it appears as though the programs are actually running on their system. Additionally, Terminal Services applications can more easily traverse firewalls allowing applications to be accessed without the need to create VPN connections.

You'll explore Windows Terminal Services in greater depth in Chapter 7.

Network Access Protection

Network Access Protection (NAP) is an added feature that can help protect your network from remote access clients. Yes, you read that correctly. NAP helps you protect the *network* from the *clients*.

Within a local area network (LAN), you can control client computers to ensure they're safe and healthy. You can use Group Policy to ensure that it's locked down from a security perspective and that it's getting the required updates. Antivirus and spyware software can be pushed out, regularly updated and run on clients. You can run scripts to ensure that all the corporate policies remain in place.

However, you can't control a client accessing your network from a hotel or someone's home. It's entirely possible for a virus-ridden computer to connect to your network and cause significant problems.

The solution is NAP, which is a set of technologies that can be used to check the health of a client. If the client is healthy, it's allowed access to the network. If unhealthy, it's quarantined and allowed access to remediation servers that can be used to bring the client into compliance with the requirements.

Health policies are determined and set by the administrator (that's you). For example, you may choose to require that all current and approved updates are installed on clients. In the network you use Windows Software Update Services (WSUS) to approve and install the updates on clients. Since the VPN client isn't in the network, they might not have the required updates. The client would be quarantined, and a WSUS server could be used as a remediation server to push the updates to the client. Once the updates are installed, the client could be rechecked and issued a health certificate and then granted access to the network.

You'll explore NAP in greater depth in Chapter 4, "Monitoring and Maintaining Network Infrastructure Servers."

Read-Only Domain Controllers

A *read-only domain controller* (RODC) hosts a read-only copy of the Active Directory database. This is somewhat of a misnomer, because changes *can* be made to the database. However, the changes can come only from other domain controllers, and the entire database isn't replicated; instead, only a few select objects are replicated.

Usually, domain controllers are considered peers where they are all equal (with a few exceptions). Any objects can be added or modified (such as adding a user or a user changing their password) on any domain controller. These changes are then replicated to other domain controllers. However, with RODCs, changes to the domain controller can come only from other domain controllers. Moreover, the changes are severely restricted to only a few select objects.

The huge benefit of the RODC is that credentials of all users and computers in Active Directory are not replicated to the RODC. This significantly improves the security of domain controllers that are placed at remote locations. If stolen, they hold the credentials of only a few objects.

As an example, when Sally logs on for the first time at the remote office, the RODC contacts a regular domain controller at the main office to verify the credentials of Sally. In

addition to verifying the credentials, the domain controller can replicate the credentials to the RODC; Sally's credentials are then cached on the RODC. The next time Sally logs on, the RODC checks her credentials against the cached credentials.

If the RODC is somehow stolen, the entire Active Directory database isn't compromised since the RODC would hold only a minimum number of accounts.

The one requirement to support read-only domain controllers is that the domain controller hosting the PDC Emulator FSMO role must be running Windows Server 2008.

FSMO roles (including the PDC Emulator) are covered in the "Review of Active Directory" section later in this chapter.

Real World Scenario

Authentication at a Remote Office

Consider a remote office connected that has only 10 users and little physical security. The office is connected to the main office via a low-bandwidth wide area network (WAN) link. The challenge you face is allowing the users to log in and authenticate.

In past versions, you had one of two choices: place a domain controller (DC) in the remote office or allow the users to authenticate over the WAN link to a DC at the main office.

With little physical security, the DC could get stolen, and suddenly your entire domain could be compromised. Remember, the DC holds information for all users and computers. A solution would be to implement physical security, but with only 10 users, it's likely that you don't have the budget or staff to do this for a single server.

If the bandwidth is low (say a demand-dial 56K connection), then authentication could be very time-consuming for users. Additionally, depending on the usage of the connection, it may already be close to maximum usage or, worse, unreliable.

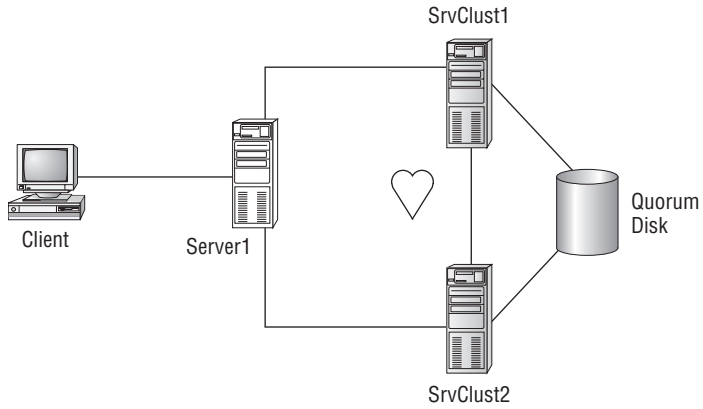
With Windows Server 2008, you have a third option. Place an RODC at the remote location. Users can log on to the DC using credentials cached on the RODC. This allows the users to quickly log on even if the WAN connection is slow or unreliable. If the DC is stolen, you still have some problems to deal with, but you won't need to consider rebuilding your entire domain. Instead, you need to deal only with the accounts at the remote office.

Improvements in Failover Clustering

Before discussing the improvements in failover clustering, let's review the big picture of clustering.

In Figure 1.5, the client connects to a virtual server (named Server1) that is configured as part of a two-node cluster. The nodes are SrvClust1 and SrvClust2. Both the cluster nodes have connections to the network, to each other, and to a shared quorum disk. Only one node is active in a cluster at a time.

FIGURE 1.5 A two-node failover cluster



As an example, you could be running SQL Server 2008 on both servers within a cluster configuration. SrvClust1 would be active, and SrvClust2 would be inactive. In other words, even though both servers are running, only SrvClust1 is responding to requests. SrvClust2's primary job at this point is to monitor the heartbeat of SrvClust1. If SrvClust1 goes down or services stop running, SrvClust2 recognizes the failure and is able to cover the load. From the client's perspective, there may be a momentary delay, but the actual outage is significantly limited.

Not all Windows Server 2008 editions support clustering. The only editions that do support clustering are these three:

- Windows Server 2008 Enterprise edition
- Windows Server 2008 Datacenter edition
- Windows Server 2008 Itanium edition

The two editions that do *not* support clustering are Windows Server 2008 Standard edition and Web edition.

Some of the improvements that Windows Server 2008 brings to failover clustering are as follows:

- Eliminates the quorum disk as a single point of failure with a new quorum model.
- Provides a tool for validating your hardware for cluster support before it's deployed.
- Provides enhanced support for storage area networks.
- Provides improved management tools that make setting up clusters easier.
- The quorum disk is now referred to as a *witness disk*.

Failover clustering will be covered in more depth in Chapter 9, "Planning Business Continuity and High Availability."

Installing Windows Server 2008

If you don't have an instance of Windows Server 2008 installed, you'll want to do that as quickly as possible. Server administration is a participation sport. You can't hope to get good at this without digging in and getting your hands into the operating system.

In this section, you'll learn how to get a free evaluation copy of Windows Server 2008 (if you don't already have one) and how to install it on Virtual PC. This will allow you to do your regular work on Windows Vista or Windows XP and then, when desired, launch Windows Server 2008 on the same system.

Hardware Requirements

Table 1.4 lists the basic system requirements for Windows Server 2008 editions.

TABLE 1.4 Hardware Requirements for Windows Server 2008 Editions

	Standard	Enterprise	Datacenter
Processor (min)	1GHz (x86) 1.4GHz (x64)	1GHz (x86 1.4GHz (x64)	1GHz (x86) 1.4GHz (x64)
Processor (recommended)	2GHz or faster	2GHz or faster	2GHz or faster
Memory (min)	512MB	512MB	512MB
Memory (recommended)	2GB or more	2GB or more	2GB or more
Memory (max)	4GB (32 bit) 32GB (64 bit)	64GB (32 bit) 2TB (64 bit)	64GB (32 bit) 2TB (64 bit)
Disk space (min)	10GB	10GB	10GB
Disk space (recommended)	40GB	40GB	40GB

Hardware resources would need to be increased for any systems using Hyper-V technology and running virtual machines. For example, if you're running three virtual servers within a Windows Server 2008 Enterprise edition, you would need additional processing power, more memory, and more disk space.

Running Windows Server 2008 on Your System

To get the most out of the book and your studies, it's best to have a Windows Server 2008 operating system installed. This allows you to see and apply the concepts. I strongly

encourage you to get a copy of Windows Server 2008 and install it on a system that you can access regularly.

In the sidebar "How to Obtain a Copy of Windows Server 2008," I explain how you can get evaluation copies of Windows Server 2008. If your budget allows, you might consider investing in a subscription to TechNet (`http://technet.microsoft.com`). In addition to providing you with copies of all the current operating systems and current applications (such as Microsoft Office and Visio), it also provides you with a wealth of technical resources such as videos and TechNet articles.

How to Obtain a Copy of Windows Server 2008

It's common for Microsoft to provide free evaluation copies of Server operating systems for your use. Currently, you can download Windows Server 2008 30-day and 180-day evaluation editions free of charges here:

`http://www.microsoft.com/windowsserver2008/en/us/trial-software.aspx`

Beware, though. These files are quite large. If you're using a slower dial-up link, you might want to see whether Microsoft is currently offering an evaluation DVD via regular mail. Purchasing an evaluation DVD isn't an available option at this writing, but Microsoft has often included this as an option with other Server products. There's a nominal cost involved with this option, but it's better than trying to download more than 2GB at 56KB.

The download is an `.iso` image of the actual DVD. Search with your favorite search engine for *Download Windows Server 2008,* and you'll find the link.

Once you download the .iso image, you can burn it to a DVD. If you don't have the software needed to burn it to DVD, you can use one of the many freeware utilities (such as ImgBurn) to burn the .iso image to your DVD.

Using Virtual PC 2007

Virtual PC is an excellent tool that will allow you to install multiple instances of Windows Server 2008 on a single operating system. For example, you may be running Windows XP or Windows Vista on your primary computer. Instead of making this system a dual-boot or multiboot operating system, you can use Virtual PC to install all of these operating systems and make them easily accessible within your primary operating system.

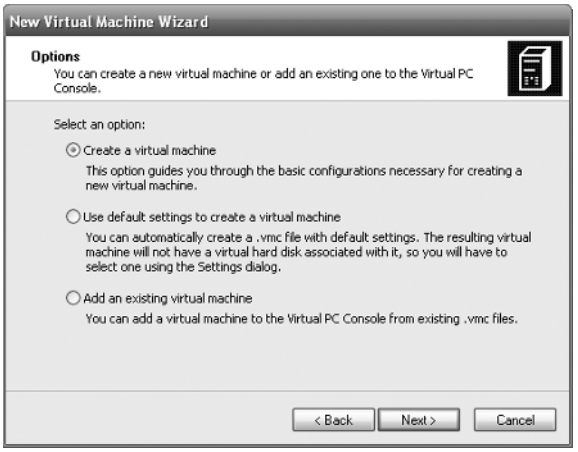
Exercise 1.1 will show you how you can download and install Virtual PC and begin installing any operating system within Virtual PC.

EXERCISE 1.1

Installing Virtual PC 2007

1. Use your favorite search engine, and enter Download Virtual PC. At this writing, the current version is Virtual PC 2007, and you can find information on it at `http://www.microsoft.com/windows/products/winfamily/virtualpc/default.mspx`.
2. Save the file to somewhere on your hard drive (such as `c:\downloads`).
3. Once the download completes, click Run to run the Setup file. Click Run or Continue (on Windows Vista) again in the Security Warning box.
4. Follow the installation wizard to finish installing Virtual PC.
5. Click Start ➢ All Programs ➢ Microsoft Virtual PC to launch Virtual PC.
6. On the Welcome to the New Virtual Machine Wizard page, click Next.

   If you already have at least one virtual machine installed on Virtual PC, the New Virtual Machine Wizard won't start automatically. Instead, you need to click the New button in Virtual PC to launch the wizard.
7. On the Options page, ensure that Create a Virtual Machine is selected, as shown in the following graphic. Click Next.



8. On the Virtual Machine Name and Location page, enter Server2008 in the Name and Location box. Click Browse. Notice that this defaults to the `My Documents\My Virtual Machines` location. You can leave this as the default or browse to another location if desired. Click Next.

EXERCISE 1.1 *(continued)*

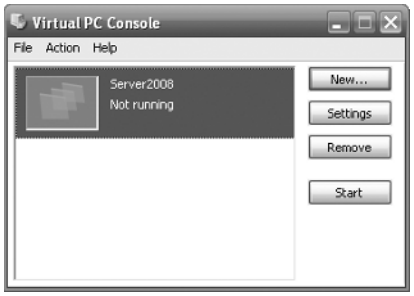
9. On the Operating System page, select Windows Vista. This will select a memory size of 512MB and a virtual disk size of 65GB. Click Next.

10. On the Memory page, accept the default of Using the Recommended RAM, and click Next.

11. On the Virtual Hard Disk Options page, select A New Virtual Hard Disk, and click Next.

12. On the Virtual hard Disk Location, accept the defaults, and click Next.

13. On the Completing the New Virtual Machine Wizard page, click Finish. The Virtual PC Console will open with the new virtual PC, as shown in the following graphic.



Note that while you've created the virtual PC instance, it's just an empty shell at this point. Windows Server 2008 still needs to be installed.

14. With the virtual machine selected, click Start in the Virtual PC Console to launch it.

15. Select the CD menu, and select Capture ISO Image. On the Select CD Image to Capture page, browse to where your ISO image is located, select it, and click Open.

    Alternatively, you can insert the Windows Server 2008 operating system DVD into your system DVD player. If the AutoPlay feature starts the DVD on the host operating system, close the window. Within Virtual PC, on the CD Menu, select Use Physical Drive X:\, where X: is the drive.

16. With the bootable DVD image captured, you can reset your Virtual PC either by selecting the Action menu and clicking Reset or by pressing Right Alt+Del keys to force a reboot to the DVD. At this point, the installation of Windows Server 2008 will start.

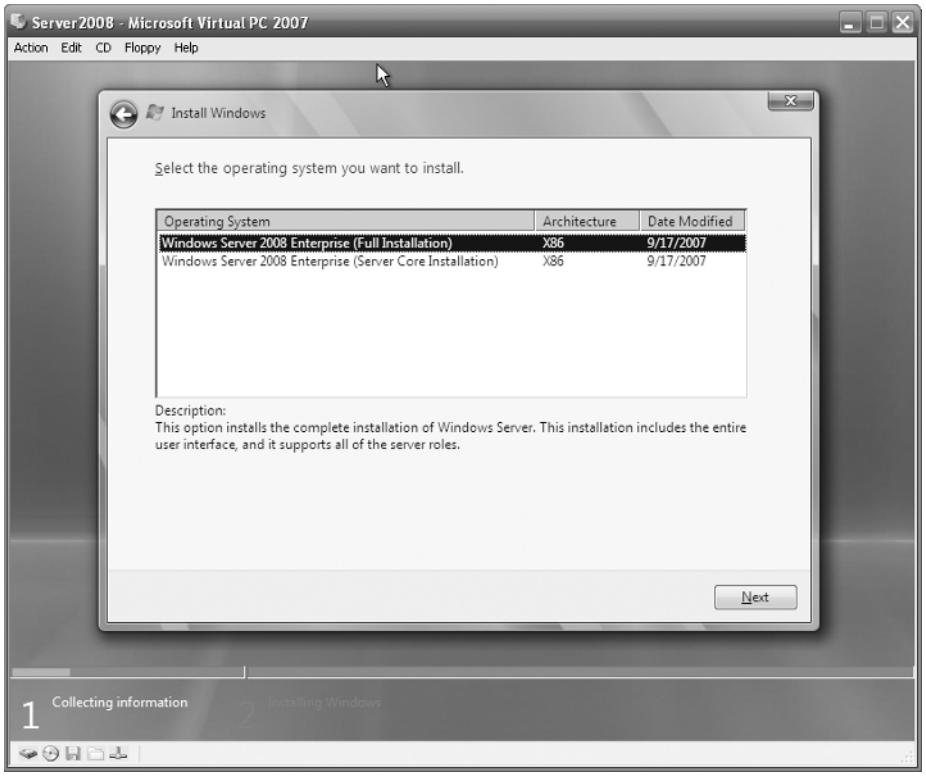
From this point on, the installation will work the same whether it is on Virtual PC or on a clean system. If you did Exercise 1.1 ("Installing Virtual PC 2007"), continue from step 2 in Exercise 1.2. If you chose not to use Virtual PC, begin Exercise 1.2 at step 1.

In Exercise 1.2, you will install Windows Server 2008.

EXERCISE 1.2

Installing Windows Server 2008

1. Insert the Windows Server 2008 operating system DVD. If the AutoPlay feature doesn't start the installation, use Windows Explorer to browse to the DVD drive, and double-click Setup.
2. If the Language Choice screen appears, accept the default language, time, currency, and keyboard. Click Next.
3. On the installation screen, click Install Now.
4. On the Product Key page, enter the product key. Click Next.
5. On the Select the Operating System page, select Windows Server 2008 (Full Installation), as shown in the following graphic. I'll cover how to install the Server Core installation in Chapter 2. Click Next.

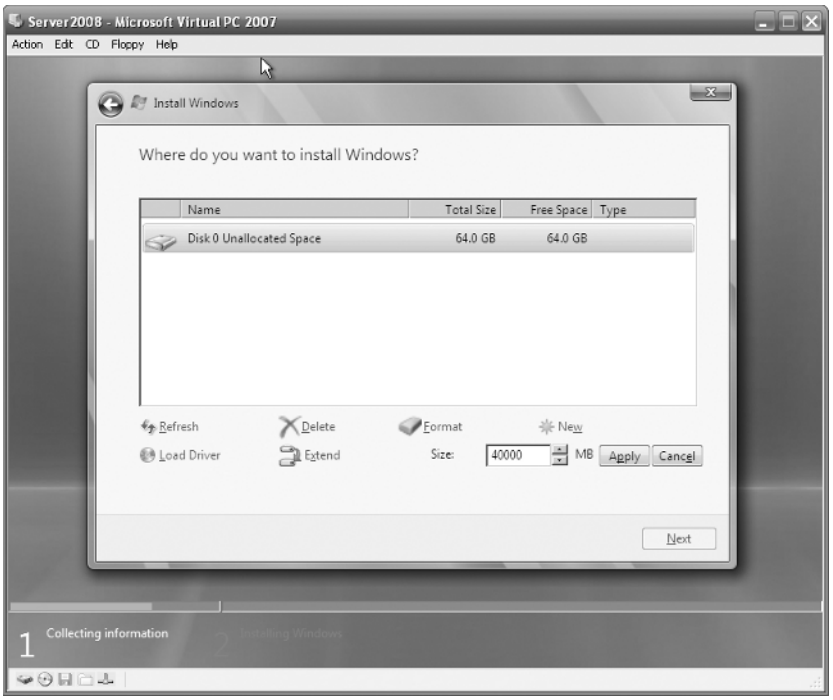


EXERCISE 1.2 *(continued)*

6. On the License Terms page, review the license terms, and click the I Accept the License Terms box. Click Next.

7. On the Type of Installation page, click Custom (Advanced).

8. On the Where Do You Want to Install Windows page, click Drive Options (Advanced). Click New. Change the size to 40,000MB, as shown in the following graphic. Click Apply.



9. Select Disk 0 Partition 1, and click Next. The partition will be formatted with NTFS as part of the installation. At this point, take a break. The installation will continue on its own.

10. When complete, the Password Change screen will complete. Click OK.

11. Enter a new password in the two text boxes. I enter P@ssw0rd on test installations. It meets complexity requirements and doesn't require me to remember multiple passwords. I don't recommend using this password on a production server. Hit Enter after the passwords are entered.

12. Once the password has been changed, the screen indicates success. Click OK.

EXERCISE 1.2 *(continued)*

13. If you've installed this on Virtual PC, follow the remaining steps to finalize the installation:

    a. Install the Virtual Machine Additions by selecting the Action menu and then clicking Install or Update Virtual Machine Additions. In the dialog box that appears, click Continue.

    b. In the AutoPlay dialog box, click Run setup.exe.

    c. On the Welcome page, click Next.

    d. On the Setup Completed page, click Finish. When the Virtual Machine Additions completes the installation, it will indicate you must restart the computer. Click Yes.

    e. Once it reboots, select Action, and then click Close. Select Save State. This will save all the changes you've made to the installation and close the Virtual PC.

What I've done when learning Windows Server 2008 is to make a copy of the virtual hard drive image after I've activated it and use it as a baseline. Then if anything goes wrong, I simply make another copy of the baseline and start over.

When working with Virtual PC, the Right Alt key (the Alt key to the right of the spacebar) is referred to as the Host key. To log on, instead of pressing Ctrl+Alt+Del, press the Right Alt+Del keys. To change the display to full-screen mode, press Right Alt+Enter. When in full-screen mode, press Right Alt+Enter to change back to Windows mode. If the cursor ever seems to be "stuck" in Virtual PC, press the Right Alt key to allow you to move it out of the Virtual PC window. Last, when turning off Virtual PC, you will be prompted to save your changes. This commits all the changes you've made during the session to the virtual hard disk. If you choose not to save your changes, the next time you reboot, none of your changes will apply.

Activating Windows Server 2008

Just as any Windows operating system today, Windows Server 2008 must be activated. Typically a computer will connect with a Microsoft server over the Internet. Data is transferred and back and forth and the computer is activated. You may have computers that connect with the Internet but still need to be activated. This can be done with the Key Management Service (KMS)

If a computer can't be activated, you'll lose all functionality when the activation period expires. The only thing the computer can do is access the tools used to activate it.

In larger companies, volume license keys are purchased for multiple servers instead of purchasing licenses individually. When using volume license keys you have two choices of how to activate your servers: Multiple Activation Key (MAK) and Key Management Service (KMS).

Multiple Activation Key With a Multiple Activation Key (MAK), a company purchases a fixed number of licenses and any servers installed with this key can be activated over the Internet with Microsoft. If the computers have Internet access, this is an automated process. It's also possible to activate a MAK by phone for systems without Internet access.

Key Management Service The Key Management Service (KMS) can be used instead of MAK if you want to eliminate the need to connect directly to Microsoft computers. For example, you may have servers in a secure network without Internet access. Instead of manually activating each server over the phone, you can use the KMS.

First, you would install the KMS on a server and activate it using traditional means (via the Internet or phone). The KMS can then be used to activate other systems within your network.

Systems activated by the KMS must contact the KMS at least once every 6 months to renew their activation. All contact with the KMS is automated without any user intervention.

Review of Active Directory

Active Directory is Microsoft's implementation of a directory service. A *directory service* holds information about resources within the domain. Resources are stored as objects and include users, computers, groups, printers, and more.

In Windows Server 2008, five different server roles support Active Directory:

- Active Directory Domain Services
- Active Directory Certificate Services
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services

The primary role is Active Directory Domain Services. The other roles add to the capabilities of Active Directory.

Objects include users, computers, groups, and more. The Active Directory database is stored only on servers holding the role of domain controllers.

A significant benefit of using Active Directory Domain Services is that it enables you as an administrator to manage desktops, network servers, and applications all from a centralized location.

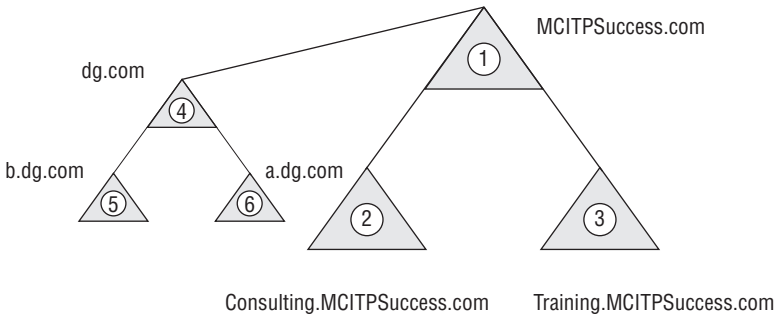
Active Directory Elements

Active Directory can spread beyond a single domain, though. Take a look at Figure 1.6. This figure shows the logical structure of Active Directory in a multiple-domain, multiple-tree forest.

Active Directory has several elements you should know for the exam:

Root domain The MCITPSuccess.com domain (labeled 1) is the root domain. The root domain is the very first domain created in a forest. This domain would also be considered a parent domain to both the Consulting.MCITPSuccess.com domain (labeled 2) and the Training.MCITPSuccess.com domain (labeled 3).

FIGURE 1.6 Logical structure of Active Directory



If nothing were added other than the root domain, the root domain would also be called a *tree* and a *forest*.

Child domain Both the Consulting.MCITPSuccess.com and Training.MCITPSuccess.com domains are considered child domains of the MCITPSuccess.com. A child domain has the same namespace (in this case MCITPSuccess.com) as the parent.

Tree A tree is a group of domains that share the same namespace. In the figure, there are two trees. The domains labeled 1, 2, and 3 all share the same namespace of MCITPSuccess.com and so compose one tree. The second tree is composed of the domains labeled 4, 5, and 6; these domains share the same namespace of dg.com. Even though the second tree has a different namespace, it is associated with the first namespace, as shown with the connecting line.

Forest A forest is all of the domains in all the trees in the same logical structure as the root domain. In other words, all the trees in the world aren't part of a single forest. Instead, only trees created off the root domain are part of the forest to which the root domain belongs.

Trusts Each of these domains is connected with a line with another domain in the forest. The line implies a two-way trust. A trust allows users in one domain to be able to access resources in another domain (if permissions are granted). Two-way means that users in domain 1 can access resources in domain 2, and users in domain 2 can access resources in domain 1.

Additionally, trusts within a forest are transitive. Since domain 2 trusts domain 1, and domain 1 trusts domain 3, then domain 1 also trusts domain 3.

Active Directory Domain Services Schema The Active Directory Domain Services schema contains definitions of all the objects that can be contained in Active Directory Domain Services and also lists the attributes or properties of those objects.

A real-world example of the schema is the white pages of a phone book. No matter what city you're in, you expect to find names, addresses, and phone numbers in the white pages. The schema of the white pages defines a single object (a phone listing) with three attributes or properties (name, address, and phone number). Of course, a phone book would have multiple listings. If I called up the phone company and asked them to publish my birthday in their next phone book, they'd probably laugh. Or a tech geek might tell me, "Sorry, that property is not in our schema."

In Active Directory Domain Services, you can add objects such as users, computers, groups, and more. You can't add a kitchen sink object because it's not in the schema. Further, you can't add birthday attributes to the user object because it's not in the schema.

There is only one Active Directory Domain Services schema for the entire forest. Other schemas exist for other Active Directory roles. For example, the Active Directory Lightweight Directory Services role contains its own schema.

Global catalog The global catalog is a listing of all objects in the forest. It holds a full listing (including all attributes) of objects in the domain and a partial (only some of the attributes) read-only copy of the objects from other domains. The global catalog is held on a domain controller configured as a global catalog server. The first domain controller in a domain is automatically configured as a global catalog server, and replica domain controllers can be configured as global catalog servers if desired.

Many processes and applications regularly use the global catalog to identify objects and attributes. For example, when a user logs on, the global catalog is queried to identify the Universal Group membership.

Consider a forest of six domains. The global catalog could be quite huge if it held all the attributes of all the objects. To make the size of the global catalog more manageable in large forests, the global catalog includes only some of the more often used attributes of objects. For example, a user object may have as many as 100 different attributes such as name, user logon name, universal principal name, SAM account name, password, street address, post office box, city, state, ZIP, and much more. Clearly some of these attributes are more important than others. The schema defines which attributes are replicated to the global catalog.

FSMO roles In a Windows Server 2008, domain controllers can hold additional flexible single master operations (FSMO) roles. Five FSMO roles exist. Two (the Schema Master and the Domain Naming Master) are unique to the forest. The other three (RID Master, PDC Emulator, and Infrastructure Master) are contained in each domain in the forest.

It's common for all of the roles to exist on a single domain controller, but it isn't required. In a two-domain forest, the first domain controller in the root domain would hold all five roles by default. The first domain controller in the child domain would hold the three domain roles. These roles can be transferred to other domain controllers if desired or seized if the domain controller holding the role is no longer operational.

Schema Master The Schema Master role holds the only writable copy of the schema. If the schema needs to be modified (such as when installing Microsoft Exchange for the first time), the Schema Master must be on line and reachable. Only one server in the entire forest holds the role of Schema Master.

Domain Naming Master The Domain Naming Master role is the sole role used to manage the creation of new domains within the forest. It ensures that domains are not created with duplicate names. Only one server in the entire forest holds the role of Domain Naming Master.

RID Master The RID Master is used to create new unique security identifiers (SIDs). While you and I refer to users and computers based on their names, resources refer to this objects based on their SIDs. When granting permissions to resources, the SID is added to the access control list. SIDs must be unique—one of kind, never to be repeated. If you have duplicate SIDs on your network, you end up with a painful assortment of problems that become quite challenging to troubleshoot.

A SID is created by a domain SID and relative identifiers (RIDs) issued by the RID Master role. The RID Master role issues RIDS to other domain controllers. It keeps track of what RIDs have been issued, ensuring no duplicate SIDs exist on your network. One server in each domain within a forest holds the role of RID Master.

PDC Emulator The PDC Emulator role is the miscellaneous role. It fulfills a variety of purposes in the domain.

In NT 4.0 (yes, a long, long time ago), there was one Primary Domain Controller (PDC) and multiple Backup Domain Controllers (BDCs). The PDC held the only writable copy of the domain database. When changes occurred, the BDC had to contact the PDC to make the change. When Windows 2000 was introduced, domain controllers were created as multiple masters with loose convergence. In other words, all held writable copies of Active Directory, and given enough time, the database would converge and all copies would be identical. However, it was unlikely that all domain controllers would be upgraded to Windows 2000 immediately. Instead, the PDC was upgraded first, and it held the role of PDC Emulator. All BDCs contacted the PDC Emulator just as if it were the PDC.

Let me ask you a question: Are you running NT 4.0 today? No, I see. The designers of the FSMO roles peered into their crystal balls and predicted this. They gave the PDC other jobs.

It is the time synchronizer for the domain. You can synchronize the PDC emulator with a third-party time source to ensure it's accurate. All domain controllers in the domain get their time from the PDC Emulator. All client computers get their time from the domain

controller they authenticate with when they start. This ensures that all computers within the domain have the same time. This is critical for the support of Kerberos; if computers are more than five minutes off, they are locked out of the domain.

The PDC Emulator is the point of contact for managing password changes. When a user changes their password, it is recorded with the PDC Emulator. Ultimately, Active Directory Domain Services will replicate the new password to all domain controllers, but there will be a short period of time when the change hasn't been replicated to all. If the user tries to log in shortly after changing their password and contacts a different domain controller before the password is replicated, they could be denied access even though they've given the correct password. Instead, the logon services queries the PDC Emulator to see whether the user has recently changed their password.

New to Windows Server 2008 is support for read-only domain controllers. To support read-only domain controllers, the server holding the role of PDC Emulator must be running Windows Server 2008.

One server in each domain within a forest holds the role of PDC Emulator.

Infrastructure Master The Infrastructure Master role is useful only in a multiple domain forest. It keeps track of changes in group membership in other domains that affect a group in its domain.

For example, consider a domain local group named DL_ColorPrinter in DomainA. It could have a global group from DomainB named G_Managers as a member. If the group membership in DomainB changes, DomainA wouldn't be aware of the changes since the change occurred in another domain. To resolve this issue, the Infrastructure Master role periodically queries the global catalog to identify any changes.

The one restriction on the Infrastructure Master role is that it won't function as desired if it is also holding the role of the global catalog server. In a multiple domain forest, the Infrastructure Master should not be a global catalog server. If it's a single domain forest, it doesn't matter.

One server in each domain within a forest holds the role of Infrastructure Master.

Promoting a Server to a Domain Controller

Most Windows Server 2008 servers can be promoted to the role of a domain controller. The exception is Server 2008 Web edition and Itanium edition.

By promoting a server to a domain controller, you are installing Active Directory Domain Services on the server (and the other necessary pieces) for Active Directory Domain Services to work.

The tool used to promote a server is DCPromo. It can be run from the command line or the Run box.

To support Active Directory Domain Services, Domain Name System (DNS) must be running on the network. If it is not installed and available, DCPromo will identify the omission, and you'll be prompted to install DNS as part of the promotion process.

When running DCPromo, you will be asked what function the new domain controller will fulfill. The choices are as follows:

- First domain controller in the forest
- First domain controller in a new domain within an existing tree within an existing forest
- First domain controller in a new domain in a new tree within an existing forest
- Replica domain controller in an existing domain

If this is the first domain controller in a new domain or the first domain controller in the forest, you'll also be asked to choose the domain functional level and the forest functional level. The choice is guided by what version of Windows is running on all the domain controllers.

The choices for domain functional level are as follows:

- Windows Server 2000 native
- Windows Server 2003
- Windows Server 2008

Once all the domain controllers are Windows Server 2003 or Windows Server 2008, then the domain functional level can be raised to the higher level. The domain functional level is raised using Active Directory Users and Computers. At higher levels, additional features and functionality are available.

The choices for forest functional level are as follows:

- Windows Server 2000 native
- Windows Server 2003
- Windows Server 2008

Once all domains are at a given domain functional level, the forest functional level can be raised to that level. The forest functional level is raised using Active Directory Domains and Trusts.

Another requirement for promoting a server to a domain controller is that the IP addresses should be static. If you have dynamically assigned IP addresses (either IPv4 or IPv6), a warning will appear indicating you should assign static IP addresses for both IPv4 and IPv6.

Promoting a server to a domain controller involves two distinct steps:

1. Add the Active Directory Domain Services role using Server Manager.
2. Run the DCPromo wizard to install Active Directory Domain Services.

Exercise 1.3 and Exercise 1.4 walk you through the necessary steps to promote a server to a domain controller.

Domain Functional Level and Forest Functional Level

The domain functional level and forest functional level identify features available within your domain and forest. If all **DOMAIN CONTROLLERS** are Windows Server 2008, the domain functional level could be raised to Windows 2008. Once all domains are raised to Windows Server 2008, the forest functional level can be raised to Windows 2008.

Notice how I've bolded and capitalized **DOMAIN CONTROLLERS**? The editors really don't like it, but there's an important reason for this: a quirk I've noticed in the classroom is that students often change this definition in their heads. Instead of remembering that all **DOMAIN CONTROLLERS** must be Windows Server 2008 to raise the functional level to 2008, students often change this definition to all servers must be Windows Server 2008. However, a domain can be in the domain functional level of 2008 with Windows Server 2000 servers, Windows Server 2003 servers, and Windows Server 2008 servers. The difference is that all **DOMAIN CONTROLLERS** must be Windows Server 2008 to be able to raise the domain functional level to 2008.

EXERCISE 1.3

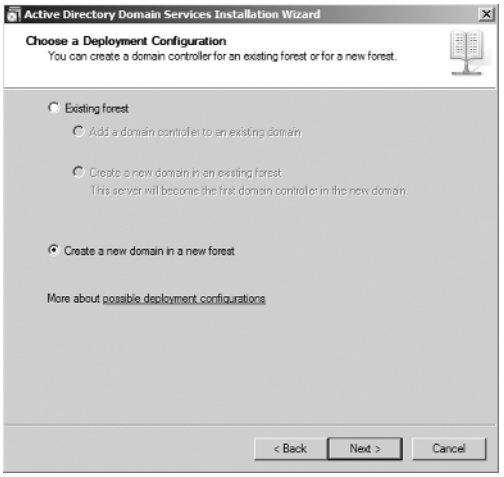
Adding the Active Directory Domain Services Role

1. Launch Server Manager. Click Start ➢ Administrator Tools ➢ Server Manager.
2. In Server Manager, select Roles.
3. Select Add Roles.
4. On the Before You Begin page, review the requirements, and click Next.
5. On the Select Server Roles page, select the check box next to Active Directory Domain Services, and click Next.
6. On the Active Directory Domain Services page, review the information, and click Next.
7. On the Confirm Installation Selections page, click Install.
8. On the Installation Results page, review the information. Note that you must still run the Active Directory Domain Services Installation Wizard (DCPromo) to make the server a fully functional domain controller. Click Close.

EXERCISE 1.4

Installing Active Directory Domain Services

1. Boot into a Windows Server 2008 server.
2. Click Start ➢ Run. At the Run line, enter DCPromo, and click OK.
3. On the Welcome screen, click Next.
4. On the Operating System Compatibility screen, review the information, and click Next.
5. On the Choose a Deployment Configuration page, select Create a New Domain in a New Forest. Your display will look similar to the following graphic. Click Next.



If your computer were part of an existing forest, you could create a replica domain controller within an existing domain. However, this exercise is assuming your server will be the first domain controller in the forest.

6. On the Name the Forest Root Domain page, enter MCITPSuccess.com as the fully qualified domain name. Click Next.
7. If the Domain NetBIOS Name page appears, accept the default of MCITPSUCESS.
8. On the Set Forest Functional Level page, accept the Forest functional level of Windows 2000. Click Next.
9. On the Set Forest Functional Level page, accept the default of Windows 2000. Click Next.
10. On the Set Domain Functional Level page, accept the default of Windows 2000 Native. Click Next.

EXERCISE 1.4 *(continued)*

11. On the Additional Domain Controller Options page, note that both the DNS server and the global catalog are selected as options. Active Directory Domain Services requires DNS, and if not available on the network, DCPromo will give you the option of installing it. Additionally, the first domain controller within a domain is a global catalog server. Click Next.

    If you have dynamically assigned addresses assigned, a warning will appear indicating you must assign static IP addresses for both IPv4 and IPv6. Either assign static IP addresses or click Yes; the computer will use a dynamically assigned IP address and configure static IP addresses later. As a best practice, domain controllers should use statically assigned IP addresses.

12. If this server is on an isolated network without other DNS servers, a warning dialog box will appear indicating that a delegation for this DNS server can't be created and other hosts may not be able to communicate with your domain from outside the domain. This is normal when installing DNS for the first domain controller in a forest. Click Yes to continue.

13. On the Location for Database, Log Files, and SYSVOL page, accept the defaults, and click Next.

14. On the Directory Services Restore Mode Administrator Password page, enter P@ssw0rd in both the Password and Confirm password boxes. This password is needed if you need to restore Active Directory Domain Services. On a production domain controller, a more secure password would be required. Click Next.

15. On the Summary page, review your selections, and click Next. Active Directory Domain Services will be installed.

16. After a few minutes, the wizard will complete. On the Completion page, click Finish.

17. On the Active Directory Domain Services dialog box, click Restart Now. Once your system reboots, Active Directory Domain Services will be installed.

Active Directory Domain Services Tools

When Active Directory Domain Services is installed, several tools are installed with it. These tools are used to manage and maintain Active Directory Domain Services and are as follows:

- Active Directory Users and Computers
- Active Directory Sites and Services
- Active Directory Domains and Trusts

- DSADD
- DSDButil
- DSGet
- DSMGMT
- DSMod
- DSMove
- DSQuery
- DSRM
- GPFixup
- Ksetup
- LDP
- NetDOM
- NLtest
- NSlookup
- Repadmin
- W32tm

Summary

Windows Server 2008 brings a lot of new features and benefits that will drive a lot of migrations to the new operating system. This chapter presented many of these new additions.

One of the significant benefits of Windows Server 2008 is virtualization. Three editions (Windows Server 2008 Standard with Hyper-V, Windows Server 2008 Enterprise with Hyper-V, and Windows Server 2008 Datacenter with Hyper-V) support virtualization. Each edition can be purchased with or without Hyper-V, which is the technology that supports virtualization. The Standard edition supports one virtual server, the Enterprise edition supports as many as four virtual servers, and the Datacenter edition supports an unlimited number of virtual servers. Virtualization is supported on only 64-bit operating systems.

In this chapter, you learned about many of the new features of Windows Server 2008. These included Server Manager, Server Core, PowerShell, Windows Deployment Services, and read-only domain controllers.

Exercises led you through the process of installing Windows Server 2008 on a Virtual PC. After reviewing many of the basics of Active Directory Domain Services, you learned how to promote the server to a domain controller.

Exam Essentials

Know the different Windows Server editions and the capabilities of each. You should know which edition to use for a strictly IIS deployment and which editions support virtualization, including how many virtual servers are supported in the different editions. You should also know which editions support clustering.

Know the different ways Windows Server 2008 can be activated. You should know the differences between the Multiple Activation Key (MAK) and the Key Management Service (KMS) both used within corporate networks to activate. KMS is used when multiple computers don't have access to the Internet.

Know the impact of adding multiple virtual servers to a Windows Server 2008 server. Remember that each virtual server has its own hardware requirements. Adding virtual servers may require adding additional processing, disk, memory, and/or network capabilities.

Know how to launch and use Server Manager. Server Manager is the primary tool used to manage and maintain server roles. You should be very familiar with this GUI.

Know how to promote a server to a domain controller. Know that promoting a domain controller is a two-step process. First you use Server Manager to add the role to the server, and second you run DCPromo to promote the server.

Review Questions

1. Which of the following Windows Server 2008 editions support Active Directory Domain Services? (Choose all that apply.)
   - **A.** Web edition
   - **B.** Itanium edition
   - **C.** Standard edition
   - **D.** Enterprise edition
   - **E.** Datacenter edition
2. You need to create a DHCP server. Which editions of Windows Server 2008 will support this role? (Choose all that apply.)
   - **A.** Web edition
   - **B.** Itanium edition
   - **C.** Standard edition
   - **D.** Enterprise edition
   - **E.** Datacenter edition
3. Your company is consolidating servers and has decided to use the virtualization features in Windows Server 2008. A single server will be used to support five virtual servers. What editions support this? (Choose all that apply.)
   - **A.** Web edition with Hyper-V
   - **B.** Itanium edition with Hyper-V
   - **C.** Standard edition with Hyper-V
   - **D.** Enterprise edition with Hyper-V
   - **E.** Datacenter edition with Hyper-V
4. What command-line tool can you use to configure a server role?
   - **A.** Server Manager
   - **B.** Initial Configuration Tasks
   - **C.** `ServerManagerCmd.exe`
   - **D.** `RoleConfig.exe`
5. A fellow administrator is trying to create a read-only domain controller within an existing domain but has been unsuccessful. What might you suggest he do?
   - **A.** Verify DCPromo is installed.
   - **B.** Verify that PDC Emulator is a Windows Server 2008 server.
   - **C.** Verify that DNS is running on the network.
   - **D.** Verify the Write Protect feature is enabled for Active Directory Domain Services.

6. You help manage a seven-domain forest with two trees. How many schemas exist in this forest?
   - **A.** 1
   - **B.** 2
   - **C.** 4
   - **D.** 7

7. You help manage a seven-domain forest with two trees. How many Domain Naming Masters exist in this forest?
   - **A.** 1
   - **B.** 2
   - **C.** 4
   - **D.** 7

8. You help manage a seven-domain forest with two trees. How many RID Master roles exist in this forest?
   - **A.** 1
   - **B.** 2
   - **C.** 4
   - **D.** 7

9. Users in the research and development department use laptops, and often these laptops hold proprietary information. Management wants to protect the data on these laptops. What technology would you implement?
   - **A.** NTFS permissions
   - **B.** Server Core
   - **C.** NAP
   - **D.** BitLocker Drive Encryption

10. You manage a server that has been used as a file server. Management has decided to have this server host IIS as well. What should you do to support this additional functionality?
    - **A.** Use Server Manager to add a feature.
    - **B.** Use Server Manager to add a role.
    - **C.** Install Windows Server 2008 Web edition.
    - **D.** Add BitLocker Drive Encryption.

11. You are running a Windows Server 2008 Enterprise edition server. It is currently hosting two virtual servers, and you are planning on adding a virtual server. What should you do or check before you add the virtual server?

A. Upgrade the server to the Datacenter edition.

B. Ensure the hardware resources are adequate.

C. Remove one of the virtual servers.

D. Add Hyper-V to the server.

12. You've decided to consolidate two servers onto an existing 32-bit Windows Server 2008 Enterprise edition server with 4GB of RAM. However, you are unable to get virtualization running on this server. What's a likely problem?

A. The server must be running the 64-bit operating system.

B. Not enough memory is installed.

C. The Enterprise edition doesn't support virtualization.

D. The Enterprise edition supports only one virtual server.

13. You boot into a Windows Server 2008 server, and instead of a GUI, you get only a command line. What's the reason for this behavior?

A. The server is booted into safe mode.

B. Server Core is installed.

C. Server Manager is not installed.

D. `ServerManagerCmd.exe` is running on startup.

14. Before raising the domain functional level to Windows Server 2008, what must exist in your domain?

A. All servers must be running Windows Server 2008.

B. PDC Emulator must be running Windows Server 2008.

C. All domain controllers must be running Windows Server 2008.

D. The global catalog server must be installed on the Infrastructure Master.

15. You manage a two-domain forest. Each domain hosts two domain controllers. All domain controllers are global catalog servers. What should be done to optimize this configuration?

A. Remove one of the global catalog servers in the root domain.

B. Remove one of the global catalog servers in each domain.

C. Add a redundant domain controller to each of the domains.

D. Move the PDC emulator to a different domain controller in each of the domains.

16. You are an administrator for a multiple-site company. A remote office has 10 users with little physical security. They are complaining that it takes too long to log in. They do not have a domain controller at the remote location. What can you do to resolve the problem?
    - **A.** Add a domain controller.
    - **B.** Add a read-only domain controller.
    - **C.** Reduce the bandwidth of the link between the remote office and headquarters.
    - **D.** Add a global catalog server to the remote office.

17. A fellow administrator created a PowerShell script. She has shared it with you, and you try to run it on your system but are unsuccessful. What do you need to do to run a PowerShell script?
    - **A.** You must be a member of the Enterprise Admins group.
    - **B.** You must be a member of the Domain Admins group.
    - **C.** The server role of PowerShell must be added using Server Manager.
    - **D.** The server feature of PowerShell must be added using Server Manager.

18. Your company has purchased 50 new computers that will be deployed to employees with Windows Vista and several applications. What Microsoft technology can you use to streamline this deployment?
    - **A.** Use Ghost to create images and cast the images to the systems.
    - **B.** Run Sysprep on all the computers before installing the operating system.
    - **C.** Use Windows Software Update Services.
    - **D.** Use Windows Deployment Services.

19. Clients access your network remotely via a virtual private network (VPN) that is hosted on a Windows Server 2003 server. Recently, clients infected by viruses have accessed the network and caused significant problems before the problem was identified and contained. What can you do to prevent this in the future?
    - **A.** Upgrade the server to Windows Server 2008, and add Windows Deployment Services.
    - **B.** Upgrade the server to Windows Server 2008, and implement Network Access Protection.
    - **C.** Upgrade the server to Windows Server 2008, and add read-only domain controllers.
    - **D.** Upgrade the server to Windows Server 2008, and implement BitLocker Drive Encryption.

20. You are planning on deploying 15 Windows Server 2008 servers in a secure network. These servers must have very limited access to the main network and may not connect with the Internet. You need to plan a method to automate the activation of these servers. What should you do?
    - **A.** Implement MAK in the secure network.
    - **B.** Implement MAK in the main network.
    - **C.** Implement KMS in the secure network.
    - **D.** Implement MAK in the secure network.

Answers to Review Questions

1. C, D, E. The Enterprise and Datacenter editions support all elements of Active Directory. The Standard edition supports most elements of Active Directory (including Active Directory Domain Services). Neither Web edition nor Itanium edition supports the installation of any Active Directory services on them; they can be members of an Active Directory Domain Services domain.

2. C, D, E. The Standard, Enterprise, and Datacenter editions support any of the standard roles (including DHCP). The Web edition supports only the Web Services role running IIS. The Itanium edition is targeted to high-end applications.

3. E. Only the Datacenter edition supports more than four virtual servers. The Enterprise edition supports four virtual servers. Standard supports one virtual server. Neither the Web edition nor the Itanium edition supports virtual servers.

4. C. The `ServerManagerCmd.exe` command-line tool allows you to do many of the same tasks via the command-line that you can do using the Server Manger GUI. Initial Configuration Tasks is a GUI that automatically launches when you start the server. There is no such program as `RoleConfig.exe`.

5. B. To support read-only domain controllers, the domain controller hosting the PDC Emulator FSMO role must be running Windows Server 2008. DCPromo is a tool used to promote a server to a domain controller. DNS is a core requirement for a Windows domain. If the domain is running, then DNS must already be running. There is no such thing as a Write Protect feature for Active Directory Domain Services.

6. A. Only one schema exists in a forest. It is hosted on the server holding the Flexible Single Master Operations (FSMO) role of the Schema Master role.

7. A. The Domain Naming Master is one of the FSMO roles that is unique in the forest. Only one Domain Naming Master exists in a forest.

8. D. The RID Master is one of the FSMO roles. One RID Master exists in every domain in the forest, and since the forest holds seven domains, there must be seven RID masters.

9. D. BitLocker Drive Encryption allows entire volumes to be encrypted. If the laptop is lost or stolen, the data protected by BitLocker Drive Encryption would be significantly harder to access. Using NTFS permissions would only marginally protect a system; if the local administrator password is cracked, NTFS permissions can be changed. Neither Server Core nor Network Access Protection provides any protection to a lost or stolen laptop.

10. B. Server Manager can be used to add features and roles. The Web Server (IIS) is a role and would be added with Server Manager. Since the server is currently being used as a file server, the operating system should not be reinstalled with Web Server edition. BitLocker will protect drives, but this isn't necessary for IIS.

11. B. You need to ensure that the server has enough hardware resources (CPU, memory, disk, and NIC bandwidth) to support the new virtual server. The Enterprise edition supports as many as four virtual servers, and only two are currently running; adding one will make it three, so there's no need to upgrade the edition or remove a virtual server. Since virtual servers are already running, Hyper-V must be running.

12. A. A core requirement to support virtualization is the host operating system must be running the 64-bit edition of the operating system. Without knowing how much memory the servers are currently using, it's difficult to determine whether 4GB would be enough. The Enterprise edition supports as many as four virtual servers (when the edition includes Hyper-V).

13. B. Server Core boots into the command line only. It doesn't have a graphical user interface (GUI). Safe mode has a GUI. Server Manager is an application and wouldn't affect the functionality of the operating system. `ServerManagerCmd.exe` is a command-line alternative to Server Manager, but it wouldn't cause the operating system to show only the command line.

14. C. Once all domain controllers are running Windows Server 2008, the domain can be raised to domain functional level of Windows Server 2008. It doesn't matter what operating system servers are running, only what operating system the domain controllers are running. Raising the domain functional level is not dependent on PDC Emulator or global catalog servers.

15. B. In a multiple domain forest, the domain controller holding the Infrastructure Master role should *not* also be hosting the global catalog. Since only four domain controllers exist and each of these is also a global catalog server, this requirement isn't being met, so the Infrastructure Master role won't function. With two domain controllers in each domain, you already have redundancy. There are no restrictions on the PDC Emulator role related to the global catalog server.

16. B. With little physical security, a real threat is the loss of any domain controller placed in the remote site. A read-only domain controller would hold only minimal data from the domain and is an ideal solution for this situation. Adding a domain controller would be too risky. A global catalog server is a domain controller first with the additional functionality of holding the global catalog, but since you don't have adequate physical security, you should not add any domain controller. Reducing the bandwidth would make the problem of slow logons worse since less bandwidth would be available.

17. D. PowerShell is not enabled by default. It can be enabled by using Server Manager and adding a feature. It is a feature, not a role. PowerShell does not require Domain Admins or Enterprise Admins permissions to run. These elevated permissions may be required depending on the script contents, but the actual script isn't explained.

18. D. Windows Deployment Services is Microsoft's solution to automate the process of deploying multiple computers quickly. After a single computer is installed as desired, an image can be captured and deployed to as many other computers as desired. Ghost is a popular imaging program, but it is owned by Symantec, not Microsoft. Sysprep is run on a computer immediately prior to capturing the image, not prior to installing the operating system. Windows Software Update Services is used to deploy approved Windows updates to client computers within a domain, not entire operating systems.

19. B. Network Access Protection is a set of technologies that can be used to check the health of VPN clients and quarantine them or restrict their access if unhealthy. Windows Deployment Services is used to automate the deployment of new workstations. Read-only domain controllers are used for remote offices and include only a few objects from the domain. BitLocker Drive Encryption is used to encrypt drives but wouldn't protect the clients from viruses.

20. C. You can the Key Management Service (KMS) in the secure network to automate the activation of these servers. Traffic to the main network must be minimized according to the scenario so any method that adds traffic to the main network is unacceptable. Multiple Activation Key (MAK) requires Internet access.