



Exam	70-291
Title	Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure
Updated	Verion 5.8
Product Type	Study Guide Demo File = Become premium member to view complete file



TABLE OF CONTENTS

LIST OF TABLES

Topic 1: Installing and Deploying Windows Server 2003

Section 1.1: System Requirements

Section 1.2: Installing Windows Server 2003 from the CD-Rom

Section 1.3: Installing Windows Server 2003 from a Network Share

Section 1.4: Performing an Unattended Installation

1.4.1: Using an Unattended Answer File

1.4.2: Using the System Preparation Tool

1.4.3: Using Remote Installation Services (RIS)

Section 1.5: Windows Server 2003 Licensing

Section 1.6: Deploying Software Applications

1.6.1: Software Installation and Maintenance Technology

1.6.1.1: Acquiring and Modifying Software Packages

1.6.1.2: Deploying Software Packages

1.6.1.3: Assigning Software Packages

1.6.1.4: Publishing Software Packages

1.6.1.5: Deploying .zap Files

1.6.2: Upgrading Software

1.6.2.1: Mandatory Upgrades

1.6.2.2: Optional Upgrades

1.6.2.3: Redeploying Software

1.6.2.4: Removing or Disabling Software

1.6.3: Deploying Service Packs and Hotfixes

1.6.3.1: Installing Service Packs and Hotfixes

1.6.3.2: Removing a Service Pack or Hotfix

1.6.3.3: Slipstreaming Service Packs and Hotfixes

1.6.3.4: Adding Service Packs and Hotfixes to a Network Installation Share

1.6.3.5: Installing Multiple Hotfixes

1.6.4: Microsoft Software Update Services

1.6.4.1: Windows Update

1.6.4.2: Windows Update Catalog

1.6.4.3: Automatic Updates

1.6.4.4: Software Update Services

Section 1.7: The Windows Server 2003 Boot Process

1.7.1 Files Used in the Boot Process

1.7.2 The Boot.ini File

1.7.3: Advanced Boot Options

Section 1.8: The Recovery Console

1.8.1: Installing and Starting the Recovery Console

1.8.2: Using the Recovery Console

Topic 2: Configuring the Windows Server 2003 Network

Section 2.1: Creating Network Connections

Section 2.2: Configuring Automatic IP Addressing

2.2.1: DHCP Addressing

2.2.2: Automatic Private IP Addressing

2.2.3: The DHCP Lease Process

2.2.3.1: Automatic Lease Renewal

2.2.3.2: Manual Lease Renewal

2.2.4: DHCP and BOOTP Relay Agents

2.2.5: DHCP Backup and Fault Tolerance

Section 2.3: Testing IP Connections

2.3.1: Using the IPConfig Utility

2.3.2: Using the ping Utility

2.3.3: Using the tracert Utility

2.3.4: Using the net and nbtstat Utilities

Topic 3: Name Resolution

Section 3.1: NetBIOS Name Resolution

Section 3.2: Host Name Resolution

Section 3.3: Domain Name Space

3.3.1: DNS Zones

3.3.1.1: Zone Files

3.3.1.2: Resource Records

3.3.1.3: File Types

3.3.1.4: Zone Types

Section 3.4: Name Servers

3.4.1: Name Server Roles

3.4.2: Zone Transfers

3.4.3: Zone Transfer Security

3.4.4: Active Directory Integrated Zones

Section 3.5: Resolving Names

3.5.1 Forward Lookup Query

3.5.2 Reverse Lookup Query

3.5.3 DNS Recursion

Section 3.6: Installing the DNS Service

3.6.1: Configuring the DNS Service

3.6.2 Configuring a DNS Name Server

3.6.3 Creating Forward Lookup Zones and Reverse Lookup Zones

3.6.4 Configuring Clients for DNS

3.6.5: Configuring Dynamic DNS

3.6.5.1: Dynamic Updates

3.6.5.2: Secure Dynamic Updates

3.6.5.3 SRV Resource Records and A Resource Records

3.6.5.4 Creating Resource Records

3.6.5.5: Configuring Scavenging

Section 3.7: Troubleshooting DNS

3.7.1 Disabling DNS on an Interface

Topic 4: The Windows Server 2003 Network Infrastructure

Section 4.1: Directory Service Functionality

4.1.1: Simplified Administration

4.1.2: Scalability and Extensibility

Section 4.2: Active Directory Support for Client Computers

Section 4.3: Active Directory Structure

4.3.1: Logical Structure

4.3.1.1: Domains

4.3.1.2: Organizational Units (OUs)

4.3.1.3: Schema

4.3.2: Physical Structure

4.3.2.1: Sites

4.3.2.2: Domain Controllers

4.3.3: Domain Controller Roles

4.3.3.1: The Global Catalog

4.3.3.2: Master Operation Roles

4.3.3.3: PDC Emulator

4.3.3.4: RID Master

4.3.3.5: Infrastructure Master

4.3.3.6: Domain Naming Master

4.3.3.7: Schema Master

4.3.3.8: Seizing a Role Master

4.3.4: Renaming Domain Controllers

Section 4.4: Installing Active Directory Directory Services

4.4.1: The Database and Shared System Volume

4.4.2: Domain Functional Levels

4.4.2.1: Windows 2000 Mixed Domain Functional Level

4.4.2.2: Windows 2000 Native Domain Functional Level

4.4.2.3: Windows Server 2003 Domain Functional Level

4.4.3: Forest Functional Levels

Section 4.5: Active Directory Replication

4.5.1: Replication Within Sites

4.5.2: Replication Between Sites

4.5.2.1: Site Link Attributes

4.5.2.2: Site Link Bridges

4.5.3: Replication Latency

4.5.4: Resolving Replication Conflicts

4.5.5: Single Master Operations

Section 4.6: Active Directory Objects

4.6.1: Active Directory Naming Contexts

4.6.1.1: Application Naming Contexts

4.6.1.2: Configuration Naming Context

4.6.2: Moving Active Directory Objects

4.6.2.1: The MoveTree Utility

4.6.2.2: The ClonePrincipal

- 4.6.2.3: The Active Directory Migration Tool
- 4.6.3: Controlling Access to Active Directory Objects
- 4.6.4: Delegating Administrative Control

Section 4.7: Publishing Resources

- 4.7.1: Setting Up and Managing Published Printers
- 4.7.2: Setting Up and Managing Published Shared Folders

Section 4.8: Auditing Access to Active Directory Objects

- 4.8.1: Monitoring User Access to Shared Folders
 - 4.8.1.1: Monitoring User Sessions
 - 4.8.1.2: Sending Administrative Messages to Users

Topic 5: Creating and Managing User and Computer Accounts

Section 5.1: User Accounts

- 5.1.1: Local User Accounts
- 5.1.2: Domain User Accounts
 - 5.1.2.1: Creating DomainUser Accounts
 - 5.1.2.2: Copying Domain User Accounts
- 5.1.3: Built-In User Accounts
 - 5.1.3.1: Administrator
 - 5.1.3.2: Guest
 - 5.1.3.3: HelpAssistant
 - 5.1.3.4: Support_388945a0

Section 5.2: Computer Accounts

Section 5.3: Modifying User Accounts and Computer Accounts

Section 5.4: Group Accounts

- 5.4.1: Group Scope
 - 5.4.2: Group Nesting
 - 5.4.3: Creating Groups
 - 5.4.4: Adding a User to a Group
- #### **Section 5.5: Managing The User Environment**

- 5.5.1: User Profiles
 - 5.5.1.1: Roaming User Profiles
 - 5.5.1.2: Mandatory User Profiles
- 5.5.2: Administrative Templates
- 5.5.3: Desktop Security Settings
- 5.5.4: Group Policy Script Settings
- 5.5.5: Folder Redirection

Topic 6: Routing and Remote Access Service (RRAS)

Section 6.1: Routing and Remote Access Service Features

Section 6.2: Installation and Configuration

Section 6.3: Connecting to RRAS

- 6.3.1: Remote Access Protocols
- 6.3.2: The PPP Authentication Process

Section 6.4: Remote Access Security

- 6.4.1: Secure User Authentication

6.4.1.1: Mutual Authentication

6.4.1.2: Data Encryption

6.4.1.3: Callback

6.4.1.4: Caller ID

6.4.2: Managing Authentication

6.4.2.1: Windows Authentication

6.4.2.2: RADIUS Authentication and IAS

Section 6.5: Securing RRAS Clients

6.5.1: Remote Access Policies

6.5.2 The Connection Manager Administration Kit

Section 6.6: Virtual Private Networks (VNP)

6.6.1: VPN Protocols

6.6.2: Configuring VPN Protocols

6.6.3: IPsec and NAT Transversal

6.6.4: Integrating VPN in a Routed Network

6.6.5: Integrating VPN Servers with the Internet

6.6.6: Configuring Client VPN Settings

Section 6.7: RRAS Tools

Section 6.8: Routing

6.8.1: Routing Tables

6.8.1.1: Static Routing

6.8.1.2: Dynamic Routing

6.8.2: Routing Protocols

6.8.2.1: Routing Information Protocol (RIP)

6.8.2.2: Open Shortest Path First (OSPF)

Topic 7: Controlling Network Security

Section 7.1: Access Control List

Section 7.2: NTFS Permissions

7.2.1: NTFS Folder Permissions

7.2.2: NTFS File Permissions

7.2.3: Multiple NTFS Permissions

7.2.3.1: Cumulative Permissions

7.2.3.2: The Deny Permission

7.2.4: Setting NTFS Permissions

7.2.5: NTFS Permissions Inheritance

7.2.6: Assigning Special Access Permissions

7.2.6.1: Changing Permissions

7.2.6.2: Taking Ownership

Section 7.3: Copying and Moving Files and Folders

Section 7.4: Troubleshooting NTFS Permission Problems

Topic 8: Shared Files and Folders

Section 8.1: Shared Folder Permissions

Section 8.2: Shared Application Folders

Section 8.3: Data Folders

Section 8.4: Administrative Shared Folders

Section 8.5: Offline Files

8.5.1: Enabling Offline Files

8.5.2: Offline File Synchronization

Section 8.6: Combining Shared Folder Permissions and NTFS Permissions

Topic 9: Monitoring Network Resources

Section 9.1: Monitoring Access to Shared Folders

9.1.1: Monitoring Shared Folders

9.1.2: Modifying Shared Folder Properties

9.1.3: Monitoring Open Files

9.1.4: Disconnecting Users from Open Files

9.1.5: Monitoring Network Users

9.1.6: Monitoring User Sessions

9.1.7: Disconnecting Users

Section 9.2: Auditing

9.2.1: Using an Audit Policy

9.2.2: Using Event Viewer to View Security Logs

9.2.3: Setting Up Auditing

9.2.4: Auditing Object Access

9.2.4.1: Auditing Access to Files and Folders

9.2.4.2: Auditing Access to Printers

Section 9.3: Using Event Viewer

9.3.1: Viewing Security Logs

9.3.2: Locating Events

9.3.3: Managing Audit Logs

Section 9.4: Using Group Policy

Section 9.5: The Shutdown Event Tracker

Topic 10: Monitoring System Performance

Section 10.1: The System Monitor

Section 10.2: Adding Performance Counters

Section 10.3: Performance Logs and Alerts

10.3.1 Counter Logs and Tracer Logs

10.3.2 Alerts

INDEX

LIST OF TABLES

Table 1.1: Windows Server 2003 Minimum System Requirements

Table 1.2: Files Used in the Windows Server 2003 Boot Process

Table 1.3: ARC Path Naming Conventions

Table 1.4: Some Recovery Console Commands

Table 2.1: IPConfig Switches

Table 2.2: Ping Errors

Table 2.3: Nbtstat Commands

Table 3.1: Top-Level Domains
Table 3.2: Zone Types
Table 4.1: Schema Active Directory Service Interface Objects
Table 4.2: Common Active Directory Objects
Table 4.3: Find Dialog Box Options
Table 4.4: Standard Active Directory Object Permissions
Table 5.1: The Dsadd Command-line Parameters
Table 5.2: The User Account Properties
Table 5.3: The Computer Account Properties
Table 5.4: The Dsmod Command-line Parameters
Table 5.5: The Dsadd Command-line Parameters
Table 5.6: Administrative Templates
Table 5.7: Desktop Security Settings
Table 5.8: Group Policy Settings to control the Network Environment
Table 5.9: Group Policy Settings to Control Access to the Administrative Tools
Table 6.1: Remote Access Policy Conditions
Table 6.2: Additional RADIUS Remote Access Policy Conditions
Table 6.3: Netsh Command-line Options
Table 6.4: Netsh global Commands
Table 6.5: Route Command Parameters
Table 7.1: Permission Inheritance Options
Table 7.2: Troubleshooting Permission problems
Table 8.1: Shared Folder Permissions
Table 9.1: Options for Filtering and Finding Events
Table 10.1: Some Useful Performance Counters

Implementing, Managing and Maintaining a Microsoft Windows Server 2003 Network Infrastructure

Exam Code: 70-291

Certifications:

Microsoft Certified (MCP)

Microsoft Certified Systems Administrator (MCSA 2003)

Microsoft Certified Systems Engineer (MCSE 2003)

Core

Core

Prerequisites:

None

About This Study Guide

This Study Guide provides all the information required to pass the Microsoft 70-291 exam - Implementing, Managing and Maintaining a Microsoft Windows Server 2003 Network Infrastructure. It however, does not represent a complete reference work but is organized around the specific skills that are tested in the exam. Thus, the information contained in this Study Guide is specific to the 70-291 exam and not only to Implementing, Managing and Maintaining a Microsoft Windows Server 2003 Network Infrastructure. It includes the information required to answer questions related to the maintaining Windows Server 2003 environment, Windows 2000, Windows XP Professional, Windows NT, and Windows 98 that may be asked during the exam. Topics covered in this Study Guide include: Installing Windows Server 2003, Implementing, Managing, and Maintaining IP Addressing; Configuring TCP/IP Addressing on a Server Computer; Managing DHCP; Managing DHCP Clients and Leases; Managing DHCP Relay Agent; Managing DHCP Databases; Managing DHCP Scope Options; Managing Reservations and Reserved Clients; Troubleshooting TCP/IP Addressing; Diagnosing and Resolve Issues Related To Automatic Private IP Addressing (APIPA); Diagnosing and Resolve Issues Related To Incorrect TCP/IP Configuration; Troubleshoot DHCP; Diagnosing and Resolving Issues Related to DHCP Authorization; Verifying DHCP Reservation Configuration; Examining the System Event Log and DHCP Server Audit Log Files to Find Related Events; Diagnosing and Resolve Issues Related To Configuration of DHCP Server and Scope Options; Verifying the DHCP Relay Agent; Verifying Database Integrity; Implementing, Managing, and Maintaining Name Resolution; Installing and Configuring the DNS Server Service; Configuring DNS Server Options; Configuring DNS Zone Options; Configuring DNS Forwarding; Managing DNS; Manage DNS Zone Settings; Manage DNS Record Settings; Manage DNS Server Options; Monitor DNS; Implementing, Managing, and Maintaining Network Security; Implementing Secure Network Administration Procedures; Using Security Templates; Monitoring Network Protocol Security; Implementing, Managing, and Maintaining Routing and Remote Access; Configuring Routing and Remote Access User Authentication; Configuring Remote Access Authentication Protocols; Configuring Internet Authentication Service (IAS) To Provide Authentication for Routing and Remote Access Clients; Configuring Routing and Remote Access Policies to Permit or Deny Access; Managing Remote Access; Managing Packet Filters; Managing Routing and Remote Access Routing Interfaces; Managing Devices and Ports; Managing Routing Protocols; Managing Routing and Remote Access Clients; Managing TCP/IP Routing; Managing Routing Protocols; Managing Routing Tables; Managing Routing Ports; Implementing Secure Access between Private Networks; Troubleshooting User Access to Remote Access Services; Diagnosing and Resolving Issues Related To Remote Access VPNs; Diagnosing and Resolving Issues Related To Establishing a Remote Access Connection; Diagnosing and Resolving User Access to Resources beyond the Remote Access Server; Troubleshooting Routing and Remote Access Routing; Troubleshooting Demand-Dial Routing; Troubleshooting Router-To-Router VPNs; Maintaining a Network Infrastructure; Monitoring Network Traffic; Troubleshooting Connectivity to the Internet;

Intended Audience

This Study Guide is targeted specifically at people who wish to take the Microsoft MCSA / MCSE exam 70-291 exam - Implementing, Managing and Maintaining a Microsoft Windows Server 2003 Network Infrastructure. This information in this Study Guide is specific to the exam. It is not a complete reference work. Although our Study Guides are aimed at new comers to the world of IT, the concepts dealt with in this Study Guide are complex and require an understanding of material provided for the CompTIA A+, Network+ and Server+ exams.

Note: There is a fair amount of overlap between the 70-291 and the 70-290 exams. Don't skim over the information that seems familiar. Read over it again to refresh your memory.

How To Use This Study Guide

To benefit from this Study Guide we recommend that you:

- Study each chapter carefully until you fully understand the information. This will require regular and disciplined work.
- If possible, perform all the walk-throughs that are included in this Study Guide to gain practical experience, referring back to the text so that you understand the information better. Remember, it is easier to understand how tasks are performed by practicing those tasks rather than trying to memorize each step.
- Be sure that you have studied and understand the entire Study Guide before you take the exam.

Note: Remember to pay special attention to these note boxes as they contain important additional information that is specific to the exam.

Good luck!

Topic 1: Installing and Deploying Windows Server 2003

You can install Windows Server 2003 directly from the CD-Rom or from a network share. The Windows Server 2003 installation process consists of five stages

Stage 1: Hard Drive Preparation: In text mode Setup checks the hard drive for consistency and errors. It allows you to format and create the Windows Server 2003 partition if you need to and copies setup files to the hard drive. Setup then reboots the computer.

Stage 2: Setup Wizard: The graphical user interface Setup Wizard gathers information from you; such as regional settings, your name and organization, the Windows Server 2003 CD-key, and computer name. The Windows Server 2003 Setup Program then creates the local Administrator user account and requests a password for it.

Stage 3: Installing Network Components: After the Setup Wizard has gathered the necessary information from you in Stage 2, it begins the network components installation. It detects your network adapter card; allows you to choose which network components, such as the network client, file and printer sharing and protocols, to install; allows you to join a workgroup or domain; and installs the components you have chosen.

Stage 4: Completing the Installation: The Setup Wizard completes the installation by installing the startmenu items and applying and saving the configuration settings you chose in the previous stages. It then deletes the temporary setup files and reboots the computer.

Stage 5: Post Installation: After the installation is complete, you must perform the "Product Activation"

and configure your server. You should also check your device manager for undetected or nonfunctioning hardware components.

Section 1.1: System Requirements

Before installing Windows Server 2003, you must ensure that the computer meets the minimum system requirements for Windows Server 2003.

Table 1.1: Windows Server 2003 Minimum System Requirements

Component	Minimum Requirement
Processor	Pentium 133 MHz (Pentium III 550 MHz recommended for Standard Edition and Pentium III 733 MHz for Enterprise Edition)
Memory	128 MB Ram (256 MB Ram recommended)
Hard Disk Space	1.5 GB hard disk free space
Networking	Standard network adapter card
Display	Monitor and adapter with minimum resolution of the VGA standard
I/O devices	CD-ROM, keyboard, mouse, or other pointing devices.

Section 1.2: Installing Windows Server 2003 from the CD-Rom

When installing Windows Server 2003 on a new computer from the CD-Rom you must boot directly from the CD-Rom. Unlike Windows 2000, Windows Server 2003 does not support booting from boot disks. Therefore, if your computer does not support booting from the CD-Rom, you must install Windows Server 2003 from a network share or from within an existing operating system. Place the Windows Server 2003 installation disk in the CD-Rom and reboot the computer. During the boot process you will be prompted to "press any key to boot from CD-Rom". Once you have pressed a key the installation of Windows Server 2003 will begin.

Section 1.3: Installing Windows Server 2003 from a Network Share

To install Windows Server 2003 over the network you must copy the i386 folder from the Windows Server 2003 Installation CD to a shared network folder. You must also ensure that the computer has a can connect to the network share when it has booted.

Section 1.4: Performing an Unattended Installation

Microsoft allows for the automated installation of Windows Server 2003 through unattended installations. There are three mechanisms through which an unattended installation can be performed. These are through:

- unattended answer files;
- disk imaging using the System Preparation Tool; and
- Remote Installation Services

1.4.1: Using an Unattended Answer File

The first mechanism you can use to perform an unattended installation of Windows Server 2003 is to use an answer file. An answer file is an automated script that supply's the Windows Server 2003 Setup program with all the information it would require during the installation.

- You can use Setup Manager located in the deploy.cab file in the /support/tools folder of the Windows Server 2003 Installation CD to create and modify an answer file or you can manually create the Answer file. You can use Setup Manager to create an answer file for an unattended installation, a sysprep install, and for a Remote Installation Services.

1.4.2: Using the System Preparation Tool

With disk imaging it is possible to install and configure Windows Server 2003 and all the applications and application update packs on a test computer and then create an exact image of the hard drive that can then be used to install Windows Server 2003 and the applications on other client computers. However, all the target computers to which the image is to be applied must have the same hardware configuration as the test computer. You will also have to change the computer name of all the target computers as each computer on the network must have a unique name.

You should use the Sysprep, after installing and configuring Windows Server 2003, the applications and application update packages on a test computer, to prepare the computer of disk imaging. You should then run the disk imaging program after Sysprep has completed. Sysprep adds a mini-Setup Wizard to the disk image that will request the user-specific information such as productID, user name, network configuration, etc, on the first reboot of the target computer. This information can either be supplied by the user or by an answer file.

1.4.3: Using Remote Installation Services (RIS)

Unlike Windows 2000 Server, Windows Server 2003 can be deployed using Remote Installation Services (RIS). Remote installation is the process of connecting to Remote Installation Services (RIS) server from a target computer and then performing an automated installation of Windows Server 2003 on the target computer. This is the most effective method of deploying Windows Server 2003. Remote Installation allows administrators to use a centrally located computer to install Windows Server 2003 on a target computer, i.e. the computer on which the Windows Server 2003 operating system is to be installed, anywhere on a network. It however requires that your network already has a Windows Server 2003 server infrastructure in place and that the target computers support remote booting.

Section 1.5: Windows Server 2003 Licensing

The use of Windows Server 2003 requires two distinct types of licensing: a product license, i.e., the CDkey, which allows you to install the Windows Server 2003 operating system on a computer; and a Client Access License (CAL), which allows clients to connect to the Windows Server 2003 computer.

Windows Server 2003 provides three CAL modes: a per server mode, which sets the number of concurrent users or clients that can log on to a specific Windows Server 2003 computer; a per user mode, which permits an unlimited number of concurrent users to connect to the Windows Server 2003 computer, providing each has a CAL; and a per device mode, which permits an unlimited number of concurrent client computers, or devices, to connect to the Windows Server 2003 computer, providing that each device has a CAL.

Section 1.6: Deploying Software Applications

1.6.1: Software Installation and Maintenance Technology

The software installation and maintenance technology in Windows Server 2003 uses Group Policy in conjunction with Windows Installer to automate and manage software installations, updates and removal from a centralized location. Group Policy can be used to assign the software application to a group of users that are members of an OU, and allows you to manage the various phases of software deployment.

There are four phases of software life cycle:

- **Preparation:** preparing the files that allows you to use Group Policy to deploy the application software. This involves copying the Windows Installer package files to a software distribution point. The Windows Installer application files can be obtained from the application's vendor or can be created through the use of third-party utilities.
- **Deployment:** the administrator creates a Group Policy Object (GPO) that installs the software on the target computers and links the GPO to the appropriate Organizational Unit. During this phase the software is installed.
- **Maintenance:** the software is upgraded with a new version or redeployed with a patch or a service pack. MCSE 70-291
- **Removal:** to remove software that is no longer required, you must remove the Windows installer package from the GPO that was used to deploy the software. The software is then automatically removed when a user log on or when the computer restarts.

Windows Installer consists of Windows Installer service, which is a client-side service, and Windows Installer package. Windows Installer package uses the .msi file extension that replaces the Setup.exe file and contains all the information that Windows Installer services requires to install the software. The software developer provides the Windows Installer package with the application. If a Windows Installer package does not come with an application, you can create a Windows Installer package or repackaging the application, using a third-party utility. Alternatively you could create an application file (.zap) that uses the application's existing setup program. A .zap file is not a native Windows Installer package.

Advantages of using Native Windows Installer packages:

- **Automatic File Repair** when a critical application file becomes corrupt. The application automatically returns to the installation source to retrieve a new copy of the file.
- **Clean Removal** without leaving orphaned files and without deleting shared files used by another application.
- **Transformable.** You can customize a Windows Installer package to meet the requirements set by your company by using authoring and repackaging tools. Transformed Windows Installer packages are identified by the .mst file extension.
- **Patches.** Patches and upgrades can be applied to the installed applications. These patches use the .msp file extension.

Note: A .zap file is not a native Windows Installer package and does not offer the same benefits as Windows Installer packages. It therefore does not support automatic repairing and cannot be transformed.

1.6.1.1: Acquiring and Modifying Software Packages

The preparation phase involves two key processes: package acquisition and package modification. The

Software Installation and Maintenance technology can only deploy and manage Windows Installer package files. Thus, you must have a package file for an application before that application can be deployed using Group Policy. Administrators have the following three options for acquiring package files:

- Obtain a package file from the software vendor;
- Repackage an application by create a package file using repackaging software; and
- Create a text file with the .zap extension.

Package modifications are similar to Windows Installer package files but have an .mst file extension. Modifications allow you to take one software application, such as Microsoft Office, and create any number of custom installations. You can then create GPOs, assign these different versions to different users, and install the software.

1.6.1.2: Deploying Software Packages

When you deploy software packages, you can assign the package to a user or computer, or you can publish the software package. In addition, you can also deploy .zap files.

1.6.1.3: Assigning Software Packages

Software packages can be assigned to users or computers.

- When you assign a software package to a user, the program is advertised when the user logs on, but is not installed until the first time the user starts the application. The user can start the installation of the application by selecting it from the Start menu or by document invocation, i.e., by double-clicking an icon or a file type associated with the application. By initially only advertising applications, you can minimize the impact on the local hard disk while keeping applications available to the user at all times. To assign an application to users, do the following:

- Click on the START button
- Point to PROGRAMS
- Click on ADMINISTARTIVE TOOLS
- Click on ACTIVE DIRECTORY USERS AND COMPUTERS
- Expand the domain containing the users to whom you want to assign an application
- In the list of Group Policy Object Links, select the appropriate GPO (if no GPO exists, create one)
- Then click EDIT
- Expand the User Configuration node
- Expand the Software Settings node
- Then right-click the Software Installation node
- On the pop-up menu, point to NEW
- Then click PACKAGE
- In the File Name text box, enter the path to the package
- Then click OPEN
- In the Deploy Software dialog box, click ASSIGNED
- Then click OK

- When you assign a software package to a computer, you ensure that certain applications will be available on that computer regardless of who logs on to the computer. When you assign an application to a computer, the software is installed automatically when the computer is next turned on.

The steps for assigning an application to computers are almost identical to the steps for assigning an application to users. To assign an application to computers, do the following:

- Click on the START button
- Point to PROGRAMS
- Click on ADMINISTRATIVE TOOLS
- Click on ACTIVE DIRECTORY USERS AND COMPUTERS
- Expand the domain containing the computer to which you want to assign an application
- In the list of Group Policy Object Links, select the appropriate GPO (if no GPO exists, create one)
- Then click EDIT
- Expand the Computer Configuration node
- Expand the Software Settings node
- Then right-click the Software Installation node
- On the pop-up menu, point to NEW
- Then click PACKAGE
- In the File Name text box, enter the path to the package
- Then click OPEN
- In the Deploy Software dialog box, click ASSIGNED
- Then click OK

1.6.1.4: Publishing Software Packages

When an application is published to a user, it is not installed. The advertisement is stored in Active Directory directory services, so the software is readily available. A user can install the application by using Add/Remove Programs or by using document invocation.

- To use Add/Remove Programs, the user would start Control Panel and double-click the Add/Remove Programs icon. When he or she clicks Add New Programs, the set of programs available to the user is displayed in user friendly names. The user can then select the desired program and install the software.
- The user will install the application by document invocation when he or she double-clicks an unknown file type. When the user does this, the computer sends a query to Active Directory directory services to see if there are any applications associated with the file extension. If Active Directory directory services contain such an application, the computer then checks if this application has either been published or assigned to the user. If the application has been published or assigned to the user, the computer then checks if the application is set for Auto-Install This Application By File Extension Activation. If the administrator has set the application to Auto-Install, the application is installed.

1.6.1.5: Deploying .zap Files

Software Installation normally works only with Windows Installer package files. However, you can get around this requirement by creating a .zap file that provides instructions for deploying the application. You should only use .zap files to publish applications when it is not feasible to use repackaging software to repackage an application and when a Windows Installer package file from a software vendor is unavailable. A .zap file is a text file that can be parsed and executed by Software Installation. These files allow you to publish non-Windows Installer applications with the following limitations:

- The applications cannot be assigned to either users or computers. They can only be published.
- The applications do not automatically repair themselves when key files have been deleted or become corrupted. Instead, the application will invoke and rerun its setup program any time it is unable to start.
- The applications are rarely able to install without user intervention. These applications run the software's original setup program, and few of these programs support an unattended installation.
- The applications cannot install with elevated privileges. If you intend to deploy .zap files, users must have permission to install software on their local computers. Native package files install using the privileges assigned to the Windows Installer. This allows package files to be installed on computers regardless of the user's privileges. In other words, security is based on the GPO that deployed the application rather than on the individual user's security rights.

A .zap file can be created with Notepad or any other text editor. The file itself has two primary sections: [Application], which is the Application section and [Ext], which is the File Extensions section.

1.6.2: Upgrading Software

You must be able to upgrade users' software to ensure that users' computers have the most current version of an organization's software. There are two types of upgrades: mandatory and optional.

1.6.2.1: Mandatory Upgrades

Mandatory upgrades automatically replace an older version of a program with the upgraded version. To deploy a mandatory upgrade, right-click the new version in Software Installation, and then click Properties. In the package file's Properties dialog box, select the Upgrades tab. In the Packages That This Package Will Upgrade section, click Add, and then select the older version of the program that you want to upgrade. If both versions of the program are native Windows Installer packages, this step will be done automatically. If the older version has been installed, it will be replaced with the newer version the next time that the user activates the program. You can use this same strategy to change from one vendor's product to another.

1.6.2.2: Optional Upgrades

Optional upgrades allow users to use either the old or the new version of a program. After an optional upgrade, users can also install and use both versions of the application simultaneously. To deploy an optional upgrade, right-click the new version in Software Installation and click Properties. Then select the Upgrades tab in the package file's Properties dialog box. In the Packages That This Package Will Upgrade section, click Add, and then select the older version of the program. If both versions of the program are native Windows Installer packages, this step will be done automatically. Clear the Required Upgrade For Existing Packages check box, and then click OK.

If the older version has been installed, existing shortcuts will still launch the older version. The next time the user logs on, the user can install either version from Add/Remove Programs. Document invocation will only install the newer version if the GPO deploying the newer version has the highest order of precedence. If the older version has not yet been installed, the next time that the user logs on, advertised shortcuts will start an installation of the newer version. The user can install either version from Add/Remove Programs, and document invocation will only install the later version if the GPO deploying the later version has the highest order of precedence.

If you want new users to install the newer version of the program but don't want to uninstall the application for people who are currently using the older version of the program, deploy the newer version as an optional upgrade, and then disable the older version.

1.6.2.3: Redeploying Software

Windows Server 2003 simplifies the deployment of service packs and software patches. When you mark a package file for redeployment, the application is re-advertised to everyone who has been granted access to the program, either through assigning or publishing. Then, depending on how the original package was deployed, one of the following happens:

- If the application was published and installed, the Start menu, desktop shortcuts, and registry settings relevant to that application will be updated the next time that the user logs on. The first time that the user starts the application, the service pack or software patch will be automatically applied.
- If the application was assigned to a user, the Start menu, desktop shortcuts, and registry settings relevant to that application will be updated the next time that the user logs on. The first time that the user starts the application, the service pack or software patch will be automatically applied.
- If the application has been assigned to a computer, the service pack or software patch will be automatically applied the next time that the computer is turned on. The application does not need to be activated for this to occur.

To redeploy a software package, obtain the service pack or software patch from the application vendor and place the files in the appropriate installation folders. The service pack must include a new .msi file. If it does not, you will be unable to redeploy the software because the original package file will contain instructions for deploying the new files added by the service pack or software patch. Open the GPO that originally deployed the application. In Software Installation, right-click the package filename, point to All Tasks, and click Redeploy Application. In the Redeployment dialog box, click Yes.

1.6.2.4: Removing or Disabling Software

Windows Server 2003 allows you to automatically remove software you no longer want deployed in your organization. To remove software, right-click the package file name in Software Installation, point to All Tasks, and then click Remove. In the Remove Software dialog box, select Immediately Uninstall The Software From Users And Computers (Forced Removal) to automatically delete the application from the computer, either the next time the computer is turned on or the next time a user logs on; or select Allow Users To Continue To Use The Software, But Prevent New Installations (Optional Removal).

Note: Only software that has been installed from a Windows Installer package file can be removed using Group Policy. Any software that was installed without using Windows Installer must be removed manually.

1.6.3: Deploying Service Packs and Hotfixes

Between operating system version releases, Microsoft releases regular updates to correct bugs and security vulnerabilities. These updates are distributed in two basic forms:

- Service Packs, which are packages that contain a large number of updates; and
- Hotfixes, which are small, incremental updates released between service packs.

A service pack contains all of the updates for an operating system over a period of time, and all the updates found in previously released hotfixes. Service packs are eventually rolled into the distribution of the operating system and become a stable part of the operating system. Fixes in service packs continue to work as you uninstall and reinstall other components, unless you uninstall the service pack. Hotfixes, on the other hand, can be overridden by the installation of new software. Thus, if you install a hotfix and then later update a component affected by the hotfix, you will need to reinstall the hotfix.

You can use the Qfecheck.exe program to check the current service pack and hotfix status of a computer. The Qfecheck.exe program is available for download from the Microsoft support Web site. To display a Qfecheck report, run Qfecheck.exe from the command prompt. The report includes the current service pack level of the operating system and a list of installed hotfixes. Qfecheck indicates whether each hotfix is current on the system or needs to be reinstalled.

1.6.3.1: Installing Service Packs and Hotfixes

You can download the latest service packs for your operating system from the Microsoft Web site. These service packs are distributed in two downloadable forms:

- Express Installation, which you can use when you do not need the software for additional computers. This option scans the computer and downloads and installs only the updates that are needed.
- Network Installation, which you can use when you need to install the service pack on other computers or deploy it across a network. This option includes the entire service pack in a single .exe file.

For enterprise deployment of service packs, you need the network installation download or a service pack CD. The service pack is distributed in the form of an .exe file. You can execute this file directly to install the service pack on the current computer. This extracts the files to a temporary directory and runs the Update.exe program, which performs the update. Instead of installing a downloaded service pack on the local computer, you can extract the files to a directory by specifying the -x option with the service pack executable at a command prompt. This will prompt you for a destination directory for the service pack files and allows you to make the service pack available over the network or to specify options to Update.exe. Hotfixes are distributed as .exe files, similar to service packs, but they are smaller in size. Microsoft uses a standard naming convention for hotfixes beginning with the Microsoft Knowledge Base article number describing the hotfix.

To install a hotfix on a local computer, run the executable file. Because the changes made by hotfixes are usually rolled into a service pack, the hotfix verifies that you have the correct service pack level. If you have a newer service pack, the hotfix is not required, and the installer exits without making any changes. The hotfix installation is performed by an Update.exe program located within the self-extracting archive. As with service pack distributions, you can use the -x option with a hotfix to extract its files into a directory for later use.

1.6.3.2: Removing a Service Pack or Hotfix

If a service pack or hotfix causes incompatibilities with software or causes other issues, you can remove it. The current service pack and any installed hotfixes are listed with other installed software in the Add/Remove programs control panel. Hotfixes are listed with the Microsoft Knowledge Base article number that uniquely identifies each hotfix. To uninstall a service pack or hotfix, select its entry from the list and click the Change/Remove button.

1.6.3.3: Slipstreaming Service Packs and Hotfixes

Windows 2000, Windows Server 2003 and Windows XP support the integration of service packs and hotfixes with the Windows 2000, Windows Server 2003 or Windows XP installation files. This is called slipstreaming and allows you to create an installation image of the operating system with the service packs and hotfixes applied to it. You can then use this image to install the operating system with the service packs and hotfixes already applied during the deployment of new computers. You can also apply a service pack to computers that are already running Windows 2000, Windows Server 2003 or Windows XP by running the update.exe program.

To apply a new service pack to an existing installation image of the operating system, run the update.exe program from the service pack with the /slip switch. This will replace the existing installation files with the appropriate files from the service pack.

Note: You cannot uninstall service packs or hotfixes that were installed from a slipstream installation of the operating system.

1.6.3.4: Adding Service Packs and Hotfixes to a Network Installation Share

The Update.exe program included with each service pack includes an option to update a network installation share with the service pack files. To use this option, you must first extract the service pack files to a folder using the -x option on the distributed .exe file. After the files are extracted, you can update the network share. From the i386\Update folder of the service pack files, execute the following command:

```
update.exe -s:<folder>
```

where folder is the folder where the installation files were extracted to.

Adding a hotfix to a network installation share is a more complex. To add a hotfix, extract its files using the -x option to the .exe file, and then copy the catalog file (.cat) and the .exe file for the hotfix into the i386\svcpack folder. You must create this directory if it does not exist. Then copy the hotfix binary files into the network installation folder and create a Svcpack.inf file describing the additional hotfix to be installed.

1.6.3.5: Installing Multiple Hotfixes

When a large number of hotfixes have been released, especially critical security updates, you might find it inconvenient to install multiple hotfixes at each computer in the network, especially when a reboot is required after each installation. You can use Qchain.exe or a batch file to simplify this process and install several hotfixes at once.

- The Qchain.exe utility configures the computer after you install several hotfixes so that a single reboot can correctly install all the hotfixes. You can obtain Qchain.exe from the <http://support.microsoft.com/> Web site by searching for Knowledge Base article #Q296861. To use Qchain.exe, first run the .exe file for each hotfix. Then use the -z option to prevent the hotfix from rebooting the computer after installation.

- You can combine several hotfixes and the Qchain.exe program, if necessary, into a batch file to install multiple hotfixes in a single operation. Use the -m option with each hotfix .exe file to suppress its output, along with the -z option to prevent rebooting. If Qchain.exe is required, include it as the last command in the batch file.

1.6.4: Microsoft Software Update Services

Windows server 2003 also supports automated methods to download and install hotfixes and service packs. These include the following methods:

- Windows Update, which is a Web-based interface that displays updates for a computer and allows users to install their choice of updates.
- Automatic Updates, which is a feature of Windows Update that notifies users of critical updates and optionally installs updates automatically.
- Software Update Services (SUS), which provides a service similar to Windows Update for enterprises and allows administrators to manage the installation of available updates.

1.6.4.1: Windows Update

Windows Update is a Web-based service that scans the local computer, determines which updates have not been installed, and then displays potential updates and provides a convenient interface for installing them. You can access the Windows Update site with the shortcut installed by default in the Start menu, or by going to the Windows Update site at <http://windowsupdate.microsoft.com/>.

Once the site is displayed, you click the Scan For Updates link to scan the computer. After the scan completes, Windows Update displays a list of available updates. Critical updates and new service packs are listed first, followed by non-critical operating system updates and updated hardware drivers. Click the Add button next to an update description to add the update to the list of updates to install. After you are finished adding items, click the Review And Install Updates link to install the updates.

1.6.4.2: Windows Update Catalog

Windows Update is a convenient service for computers that have Internet connections, it is not useful for a computer that does not have an Internet connection. To service computers that are not connected to the Internet, you can use the Windows Update Catalog, which provides local copies of the available updates. Once you have local copies of the updates on a computer that is connected to the Internet, you can distribute those updates to computers that are not connected to the Internet by using a local network or removable media such as CD-R. The Windows Update Catalog can then be configured on those computers to use the local sources for installation rather than connect to the Internet.

1.6.4.3: Automatic Updates

In computers with Windows Server 2003, Windows 2000 Service Pack 3 or Windows XP Service Pack 1 installed, Critical Update Notification, a utility that periodically checked the Windows Update Web site for critical updates to a computer, has been replaced by Automatic Updates. This service expands the original concept of the Critical Update Notification utility by not only notifying users of updates, but also downloading and installing them automatically if desired.

Automatic Updates downloads updates directly from the Microsoft web site and stores them in a temporary directory on each computer until they are installed. For large enterprises or for those that do not have a direct connection to the Internet, this default behavior is not always desirable. Automatic Updates can also act as a client for Microsoft Software Update Services (SUS), which allows administrators to establish a local server that can distribute updates.

1.6.4.4: Software Update Services

Microsoft Software Update Services (SUS) provides the same benefit on local servers as the Windows Update servers provide on the Internet. It allows you to make your choice of updates available to clients using Automatic Updates. The SUS server synchronizes with the Windows Update server to obtain the latest updates, and multiple SUS servers can synchronize with each other.

SUS requires at least a Windows 2000 Server computer with Service Pack2 configured as a stand-alone server or member server. It cannot be installed on a domain controller. It also requires Internet Information Services (IIS). To install SUS, first download the server software from the Microsoft Web site. SUS is provided as a file, Sussetup.msi, that uses the Windows Installer to install the service. Run this program to begin the installation. A wizard guides you through the installation process.

When using SUS, you must configure each client to use the SUS server and you must approve updates before they will be made available to clients. This approval process allows you to pre-test updates before deploying them across the enterprise. The updates you approve will be installed by clients running Automatic Updates on their next scheduled connection to the SUS server.

Note: You can remove approval from updates that have been previously approved. However, this does not remove them from any clients that have already installed the update.