



www.chinatag.com

CHINATAG

Microsoft **70-293**

Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure

Study Guide
DEMO Version

Copyright (c) 2003 Chinatag LLC. All rights reserved.

Important Note Please Read Carefully

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website. Our IT certification products start at only **\$7.99**.

Study Tips

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 180 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to feedback@chinatag.com.

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team
Chinatag LLC.

TABLE OF CONTENTS

List of Tables

Introduction

1. Planning A Network Infrastructure

- 1.1 Fundamentals of Network Design
 - 1.1.1 Analyzing Organizational Needs
 - 1.1.2 Availability and Security
 - 1.1.3 Scalability
- 1.2 Server Roles and Server Security
 - 1.2.1 Domain Controllers (Authentication Servers)
 - 1.2.1.1 Active Directory
 - 1.2.1.2 Flexible Single Master of Operations Roles
 - 1.2.1.3 PDC Emulator
 - 1.2.1.4 RID Master
 - 1.2.1.5 Infrastructure Master
 - 1.2.1.6 Domain Naming Master
 - 1.2.1.7 Schema Master
 - 1.2.1.8 Securing Domain Controllers
 - 1.2.2 File and Print Servers
 - 1.2.2.1 Print Servers
 - 1.2.2.2 Securing File Servers
 - 1.2.2.3 File Servers
 - 1.2.2.4 Securing Print Servers
 - 1.2.3 DHCP Servers
 - 1.2.4 Name Resolution
 - 1.2.4.1 WINS Servers
 - 1.2.4.2 DNS Servers
 - 1.2.5 Web Servers
 - 1.2.5.1 Securing Web Servers
 - 1.2.5.2 Firewalls
 - 1.2.6 Database Servers
 - 1.2.7 Mail Servers
 - 1.2.8 Application Servers and Terminal Servers
 - 1.2.8.1 Application Servers
 - 1.2.8.2 Terminal Servers
 - 1.2.9 Certificate Authorities
- 1.3 Planning a Server Security Strategy
 - 1.3.1 Windows Security Features
 - 1.3.2 Minimum Requirements for the Operating System
- 1.4 Identifying Minimum Security Requirements

- 1.5 Planning Baseline Security
 - 1.5.1 Predefined Security Templates
 - 1.5.1.1 Default Security Templates
 - 1.5.1.2 Secure Security Templates
 - 1.5.1.3 High Security Templates
 - 1.5.1.4 Backward Compatible Security Templates
 - 1.5.1.5 Miscellaneous Security Templates
 - 1.5.2 Managing Security Templates
 - 1.5.3 Enforcing Default Security Settings on New Computers
- 1.6 General Server Security Issues
 - 1.6.1 Physical Security
 - 1.6.2 Service Packs and Hotfixes
 - 1.6.3 Antivirus Protection
 - 1.6.4 Accounts and Services
 - 1.6.5 Secure Passwords
 - 1.6.6 File Systems

2. Planning and Implementing the TCP/IP Infrastructure

- 2.1 Data Transmission
- 2.2 The TCP/IP Protocol Suite
 - 2.2.1 The Multiprotocol Network Environment
- 2.3 The TCP/IP Model
- 2.4 IP Addressing
 - 2.4.1 Analyzing Addressing Requirements
 - 2.4.2 IPv4 Addressing
 - 2.4.2.1 Binary Format
 - 2.4.2.2 Dotted Decimal Format
 - 2.4.2.3 Classful IP Addresses
 - 2.4.2.4 Classless Interdomain Routing (CIDR) Notation
 - 2.4.2.5 Subnetting
- 2.5 Automatic IP Addressing
 - 2.5.1 DHCP Addressing
 - 2.5.2 Automatic Private IP Addressing
 - 2.5.3 The DHCP Lease Process
 - 2.5.3.1 Automatic Lease Renewal
 - 2.5.3.2 Manual Lease Renewal
 - 2.5.4 DHCP and BOOTP Relay Agents
 - 2.5.5 DHCP Backup and Fault Tolerance
- 2.6 Troubleshooting IPv4 Addressing
 - 2.6.1 The IPConfig Utility

- 2.6.2 The Ping Utility
- 2.6.3 The Tracert Utility
- 2.6.4 Client Configuration Issues
- 2.6.5 DHCP Issues

2.7 IP version 6

- 2.7.1 Implementing IPv6
- 2.7.2 IPv6 Utilities
 - 2.7.2.1 The netsh Command
 - 2.7.2.2 The Ipsec6 Utility
- 2.7.3 6to4 Tunneling
- 2.7.4 Teredo (IPv6 with NAT)

2.8 Planning the Network Topology

- 2.8.1 Analyzing Hardware Requirements
- 2.8.2 Planning the Placement of Physical Resources
- 2.8.3 Planning Network Traffic Management
 - 2.8.3.1 Network Monitor
 - 2.8.3.2 System Monitor
- 2.8.4 Determining Bandwidth Requirements

3. Implementing Network Security

3.1 Packet Filtering

- 3.1.1 Ports and Protocols
- 3.1.2 Packet Filtering Criteria
- 3.1.3 Windows Server 2003 Packet Filtering
 - 3.1.3.1 TCP/IP Packet Filtering
 - 3.1.3.2 Routing and Remote Access Service Packet Filtering

3.2 IPsec

- 3.2.1 IPsec Applications
- 3.2.2 Internet Key Exchange
 - 3.2.2.1 IKE in Windows Server 2003
 - 3.2.2.2 Distributing IKE Secret Keys
- 3.2.3 IPsec Within a Private Network
- 3.2.4 IPsec in Untrusted Networks
 - 3.2.4.1 Providing a Secret Key
 - 3.2.4.2 Creating IPsec Policy
 - 3.2.4.3 IPsec Exceptions
- 3.2.5 IPsec on Web Servers
- 3.2.6 Troubleshooting IPsec
 - 3.2.6.1 Using the IP Security Monitor Snap-in
 - 3.2.6.2 Using the Resultant Set of Policy Snap-in
 - 3.2.6.3 Examining IPsec Traffic

3.3 Wireless Networks

- 3.3.1 Wireless Protocols

- 3.3.1.1 The 802.11 Protocol
- 3.3.1.2 The 802.11b Protocol
- 3.3.1.3 The 802.11a Protocol
- 3.3.1.4 The 802.11g Protocol
- 3.3.2 Wireless Access Security
 - 3.3.2.1 Configuring Clients for Wireless Security
 - 3.3.2.2 802.1x Authentication
 - 3.3.2.3 802.1x Security Problems
 - 3.3.2.4 Troubleshooting 802.1x Connections
- 3.3.3 Wired Equivalent Privacy (WEP)
 - 3.3.3.1 WEP Security Problems
 - 3.3.3.2 Managing WEP on the Client
- 3.3.4 Wi-Fi Protected Access (WPA)
 - 3.3.4.1 WPA Key Management
 - 3.3.4.2 Michael
 - 3.3.4.3 Supporting WPA and WEP Clients

4. Planning and Implementing Name Resolution

- 4.1 NetBIOS Name Resolution
 - 4.1.1 The LMHOSTS File
 - 4.1.2 Windows Internet Naming Service (WINS)
- 4.2 Host Name Resolution
- 4.3 Domain Name Space
 - 4.3.1 DNS Zones
 - 4.3.1.1 Zone Files
 - 4.3.1.2 Resource Records
 - 4.3.1.3 File Types
 - 4.3.1.4 Zone Types
- 4.4 Name Servers
 - 4.4.1 Name Server Roles
 - 4.4.2 Zone Transfers
 - 4.4.3 Zone Transfer Security
 - 4.4.4 Active Directory Integrated Zones
- 4.5 Resolving Names
 - 4.5.1 Forward Lookup Query
 - 4.5.2 Reverse Lookup Query
 - 4.5.3 DNS Recursion
- 4.6 Installing the DNS Service
- 4.7 Configuring the DNS Service
 - 4.7.1 Configuring a DNS Name Server

- 4.7.2 Creating Forward Lookup Zones and Reverse Lookup Zones
- 4.7.3 Configuring Clients for DNS
- 4.7.4 Configuring Dynamic DNS
 - 4.7.4.1 Dynamic Updates
 - 4.7.4.2 Secure Dynamic Updates
 - 4.7.4.3 SRV Resource Records and A Resource Records
 - 4.7.4.4 Creating Resource Records
 - 4.7.4.5 Configuring Scavenging
- 4.8 Troubleshooting DNS
 - 4.8.1 Disabling DNS on an Interface
 - 4.8.2 Using nslookup to resolve DNS problems
- 4.9 WINS and DNS Interoperability
 - 4.9.1 Enabling WINS Lookup on DNS Zones
 - 4.9.2 Enabling WINS Lookup with Third-Party DNS Servers
 - 4.9.3 Configuring DNS to Forward Queries to WINS Servers

5. Planning and Implementing Internet and Remote Access

- 5.1 Internet Access
 - 5.1.1 Routed Internet Connections
 - 5.1.2 Translated Internet Connections
- 5.2 Network Address Translation (NAT)
 - 5.2.1 Installing the NAT Service
 - 5.2.2 Managing NAT
- 5.3 Internet Connection Sharing (ICS)
 - 5.3.1 Enabling ICS
 - 5.3.2 Configuring Services
- 5.4 Virtual Private Networks (VNP)
 - 5.4.1 VPN Protocols
 - 5.4.2 Configuring VPN Protocols
 - 5.4.3 Integrating VPN in a Routed Network
 - 5.4.4 Integrating VPN Servers with the Internet
 - 5.4.5 Configuring Client VPN Settings
 - 5.4.6 VNP Security
 - 5.4.6.1 IPsec
 - 5.4.6.2 Microsoft Point-to-Point Encryption (MPPE)
 - 5.4.6.3 Connection Manager
- 5.5 Internet Authentication Service (IAS)
 - 5.5.1 Installing IAS
 - 5.5.2 IAS Authentication Methods
 - 5.5.2.1 PPP-based Authentication Methods
 - 5.5.2.2 Extensible Authentication Protocol (EAP) Types

5.5.3 IAS Authorization Methods

5.6 Routing

5.6.1 Routing Tables

5.6.1.1 Viewing Routing Tables

5.6.1.2 Static Routing

5.6.1.3 Dynamic Routing

5.6.2 Routing Protocols

5.6.2.1 Routing Information Protocol (RIP)

5.6.2.2 Open Shortest Path First (OSPF)

5.7 Selecting Connectivity Devices

5.7.1 Hubs

5.7.2 Bridges

5.7.3 Switches

5.7.3.1 Layer 2 Switches

5.7.3.2 Layer 3 Switches

5.7.3.3 Layer 4 Switches

5.7.4 Routers

5.7.4.1 Windows Server 2003 Routers

5.7.4.2 Demand-dial Routing

5.7.4.3 Router-to-Router VPNs

5.8 Router Security

5.8.1 Packet Filtering and Firewalls

5.8.2 Logging

5.9 Troubleshooting IP Routing

5.9.1 The pathping Command

5.9.2 The mtrinfo Command

5.9.3 Common Routing Problems

5.9.3.1 Interface Configuration Problems

5.9.3.2 RRAS Configuration Problems

5.9.3.3 Routing Protocol Problems

6. Ensuring High Availability

6.1 Hardware and System Performance

6.1.1 Memory

6.1.1.1 Minimum RAM Requirement

6.1.1.2 Memory Leaks

6.1.1.3 Virtual Memory

6.1.2 The Processor

6.1.2.1 Level 1 and Level 2 Cache Memory

6.1.2.2 CPU Bus Architecture

6.1.2.3 Multiprocessing and Hyperthreading

6.1.3 Hard Disk Drives

6.1.3.1 Disk Controller Technology

6.1.3.2 Drive Life Expectancy

- 6.1.3.3 Arrangement of Data on Drives
- 6.1.3.4 The Ratio of Drive Controllers to the Number of Drives
- 6.1.4 Network Components
- 6.2 Monitoring System Performance
 - 6.2.1 The System Monitor
 - 6.2.1.1 Adding Performance Counters
 - 6.2.1.2 Performance Logs and Alerts
 - 6.2.1.3 Counter Logs and Tracer Logs
 - 6.2.1.4 Alerts
 - 6.2.2 Using Task Manager to Monitor Performance
 - 6.2.3 Command-Line Monitoring Tools
 - 6.2.3.1 The Logman Utility
 - 6.2.3.2 The relog Utility
 - 6.2.3.3 The typeperf Utility
 - 6.2.4 Creating a Performance Baseline
- 6.3 Using Event Viewer to Monitor Servers
 - 6.3.1 Locating Events
- 6.4 Planning a Backup and Recovery Strategy
 - 6.4.1 Backing Up and Restoring Data
 - 6.4.2 Backup Types
 - 6.4.3 Backing Up System State Data
 - 6.4.4 Restoring Files and Folders
 - 6.4.5 Restoring Active Directory Directory Services
 - 6.4.5.1 Failed Domain Controllers
 - 6.4.5.2 Damaged Active Directory Databases
 - 6.4.5.3 Authoritative Restores
- 6.5 Planning System Recovery with Automated System Recovery (ASR)
- 6.6 Planning for Fault Tolerance
 - 6.6.1 Network Fault-Tolerance Solutions
 - 6.6.2 Disk Fault-Tolerance Solutions
 - 6.6.2.1 Disk Controllers
 - 6.6.2.2 Redundant Array of Independent Disks (RAID)
 - 6.6.2.3 Hot Spare Drives
 - 6.6.3 Server Fault-Tolerance Solutions
 - 6.6.3.1 Hardware Redundancy
 - 6.6.3.2 Uninterruptible Power Supply (UPS)
- 6.7 Clustering Servers
 - 6.7.1 Server Clusters
 - 6.7.2 Network Load Balancing
 - 6.7.3 Scaling Clusters
 - 6.7.4 Dispersing Clusters
 - 6.7.5 Recovering from Cluster Node Failure

7. Implementing Certificate Services and Certificate Authorities

7.1 Encryption

- 7.1.1 Secret Key Encryption
- 7.1.2 Public Key Encryption
- 7.1.3 Digital Signatures

7.2 Certificates

7.3 Certificate Management

- 7.3.1 Certificate Enrollment
- 7.3.2 Certificate Expiration
- 7.3.3 Certificate Renewal
- 7.3.4 Certificate Revocation
- 7.3.5 Certificate and Key Recovery
- 7.3.6 Certificate Trust

7.4 Uses for Certificates

7.5 Installing Windows Server 2003 Certificate Services

- 7.5.1 Types of CAs
 - 7.5.1.1 Enterprise Root CA
 - 7.5.1.2 Enterprise Subordinate CA
 - 7.5.1.3 Stand-Alone Root CA
 - 7.5.1.4 Stand-Alone Subordinate CA
- 7.5.2 CA Security and Recovery
- 7.5.3 Cryptographic Service Providers
- 7.5.4 Issuing Certificates
- 7.5.5 Cryptographic Key Storage
- 7.5.6 Backing Up and Restoring CAs

7.6 Computer Certificates

- 7.6.1 Certificate Templates
- 7.6.2 Deploying Computer Certificates
- 7.6.3 Deploying User Certificates
 - 7.6.3.1 Automated Deployment of User Certificates
 - 7.6.3.2 Manually Creating Certificates
 - 7.6.3.3 Moving Certificates

7.7 Smart Card Certificates

- 7.7.1 Personal Identification Number
- 7.7.2 Types of Smart Card Certificates
- 7.7.3 Issuing Smart Cards
- 7.7.4 Smart Card Removal Behavior Policy
- 7.7.5 Troubleshooting Smart Card Certificates

7.8 S/MIME Certificates

LIST OF TABLES

TABLE 1.1	Minimum System Requirements for Windows Server Operating Systems
TABLE 1.2	The SecEdit Command Parameters
TABLE 2.1	IPConfig Command Line Switches
TABLE 2.2	Ping Errors
TABLE 3.1	Well-Known Port Numbers
TABLE 4.1	Top-Level Domains
TABLE 4.2	Zone Types
TABLE 5.1	Route Command Parameters
TABLE 5.2	The Pathping Commands Parameters
TABLE 5.3	The Mrinfo Commands Parameters
TABLE 6.1	Some Useful Performance Counters
TABLE 6.2	Logman Collection Parameters
TABLE 6.3	Relog Command Options
TABLE 6.4	Typeperf Command Parameters and Options
TABLE 6.5	Options for Filtering and Finding Events
TABLE 6.6	Operating System Scaling Up Limits
TABLE 6.7	Operating System Scaling Out Limits
TABLE 7.1	CSP Encryption Algorithms
TABLE 7.2	Standard PKI Certificate Stores
TABLE 7.3	The Windows Server 2003 Certificate Templates

Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure

Exam Code: 70-293

Certifications:

Microsoft Certified (MCP)

Microsoft Certified Systems Engineer (MCSE 2003)

Core

Prerequisites:

None

About This Study Guide

This Study Guide provides all the information required to pass the Microsoft 70-293 exam – Planning 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 70-293 exam and not only to Managing and Maintaining a Microsoft Windows Server 2003 Environment. It includes the information required to answer questions related to the installation of Windows Server 2003, Windows 2000 Server, Windows XP Professional, Windows 2000 Professional, Windows NT, and Windows 98 that may be asked during the exam. Topics covered in this Study Guide include: Planning and Implementing Server Roles and Server Security; Planning a Secure Baseline Installation; Planning a Strategy to Enforce System Default Security Settings on New Systems; Identifying Client Operating System Default Security Settings; Identifying Server Operating System Default Security Settings; Planning Security for Domain Controllers, DNS Server, WINS Server, DHCP Server, Web Servers, Database Servers, and Mail Servers; Creating Custom Security Templates Based on Server Roles; Evaluating and Selecting the Operating System to Install on Computers in an Enterprise; Identifying the Minimum Configuration to Satisfy Security Requirements; Planning, Implementing, and Maintaining a Network Infrastructure; Planning a TCP/IP Network Infrastructure; Analyzing IP Addressing Requirements; Planning an IP Routing Solution; Creating an IP Subnet Scheme; Planning and Modifying a Network Topology; Planning the Physical Placement of Network Resources; Identifying and Implementing Network Protocols; Planning an Internet Connectivity Strategy; Planning Network Traffic Monitoring using Network Monitor and System Monitor; Troubleshooting Connectivity to the Internet; Diagnosing and Resolving Issues Related to Network Address Translation (NAT), Name Resolution Cache Information, and Client Configuration; Troubleshooting TCP/IP Addressing; Diagnosing and Resolving Issues Related to Client Computer Configuration and DHCP Server Address Assignment; Planning a Host Name Resolution Strategy; Planning a DNS Namespace; Planning Zone Replication; Planning for DNS Security; Planning a NetBIOS Name Resolution Strategy; Plan WINS Replication; Planning NetBIOS Name Resolution using the Lmhosts File; Troubleshooting Host Name Resolution; Diagnosing and Resolving Issues Related to DNS Services and Client Computer Configuration; Planning, Implementing, and Maintaining Routing and Remote Access; Planning a Routing Strategy; Identifying Routing Protocols; Planning Routing for IP Multicast Traffic; Planning Security for Remote Access; Planning Remote Access Policies; Analyzing Protocol Security Requirements; Planning Authentication

Methods for Remote Access Clients; Implementing Secure Access Between Private Networks; Creating and Implement an IPSec Policy; Troubleshooting TCP/IP Routing using the **route**, **tracert**, **ping**, **pathping**, and **netsh** Command-Line Utilities and Network Monitor; Planning, Implementing, and Maintaining Server Availability; Planning a High Availability Solution using Server Clustering and Network Load Balancing; Identifying System Bottlenecks, including Memory, Processor, Hard Disk Drives, and Network Related Bottlenecks; Identifying System Bottlenecks using System Monitor; Implementing a Cluster Server; Recovering from Cluster Node Failure; Managing Network Load Balancing using the Network Load Balancing Monitor Snap-in and the WLBS Cluster Control Utility; Planning a Backup and Recovery Strategy; Identifying Appropriate Backup Types; Planning a Backup Strategy using Volume Shadow Copy; Planning System Recovery using Automated System Recovery (ASR); Planning and Maintaining Network Security; Configuring Network Protocol Security; Configuring Protocol Security using IPSec Policies; Configuring Security for Data Transmission; Configuring IPSec Policy Settings; Planning Network Protocol Security; Using Firewalls; Specify the Required Ports and Protocols for Specified Services; Planning Security for Wireless Networks; Troubleshooting Security for Data Transmission using the IP Security Monitor Snap-in and the Resultant Set of Policy (RSOP) snap-in; Planning, Implementing, and Maintaining Security Infrastructure; Planning a Public Key Infrastructure (PKI) using Certificate Services; Identifying the Appropriate Types of Certificate Authority; Planning the Enrollment and Distribution of Certificates; and Planning for the use of Smart Card Authentication.

Intended Audience

This Study Guide is targeted specifically at people who wish to take the Microsoft MCSE exam 70-293 exam – Planning 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. Study Guides for these exams are available from Real-exams.com.

Note: There is a fair amount of overlap between the 70-293 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!

1. Planning A Network Infrastructure

1.1 Fundamentals of Network Design

Proper planning of a network infrastructure is essential to ensuring high network performance and availability. There are a number of factors that you must take into consideration when designing your network, the most important of which is the **business requirements** of your organization. You would need to create a network infrastructure that addresses the needs of your management structure, such as fault tolerance, security, scalability, performance, and cost. You would also need to balance these requirements with the types of services that your users and clients will expect from a modern network, including e-mail, calendaring, project collaboration, Internet access, file, print, and application services. The best way to do this is through face-to-face interactions, by interviewing relevant managers and staff members of each department, branch, or business unit. Not only does this allow you to construct a complete picture of your network requirements, but it also involves stakeholders from the various departments. This sort of involvement is critical in ensuring the successful deployment of any new or upgraded technology.

Once you have determined the business requirements for your network, you should consider the **technical requirements** of your organization. These requirements may apply to any applications that are already in use or that you plan to implement, as well as to the associated hardware and operating system. You should also analyze and document the existing network, including any hardware, software, and network services that are already in place. In a small office environment, you can accomplish this by taking a walk to determine the physical layout of network cables, routers, and the like. In a medium- to large-sized enterprise network, you can rely on automated inventory tools such as Microsoft's **Systems Management Server (SMS)**. You should take as detailed of an inventory as possible, including the hardware configuration of server and workstation machines as well as vendor names and the version numbers of the operating system and business applications the systems are running. You can use a network analyzer, such as the **Network Monitor** utility that is provided by Windows Server 2003 or the version of Network Monitor included in SMS, to create a baseline of the current utilization of your network bandwidth. If this utilization is already near capacity, you can use this baseline to justify and plan upgrades to your network infrastructure.

Note: The Windows Server 2003 version of **Network Monitor** can analyze only traffic addressed to the network interface card (NIC) on the local server or that is sent by the local server. The SMS version of Network Monitor operates in **promiscuous mode**, which allows it to capture all network traffic on a given segment, even if the traffic is not addressed to or from the local server.

You should also ensure that your network design is scalable. It must be flexible enough to allow for future growth and changes to the organization, including support for new technologies and operating systems, additional hardware and users, as well as mergers and acquisitions.

1.1.1 Analyzing Organizational Needs

Understanding the needs of the organization is a fundamental step in the network design process. This includes understanding the required information flow for an organization; and the organization's management model and organizational structure.

Understanding the organization's required for information flow is an important aspect of the network design. All appropriate personnel must have on-demand access to critical data in order to understand how their

organization's profits and losses are occurring, to call up a customer's account information, and to collate information from multiple sources to allow for effective decision making. This requires that you to determine the location of your users, the data that they require, and the frequency and level of access they require.

Understanding an organization's organizational structure is another important factor in designing a network to meet the organization's business requirements. You should analyze the high-level divisions within an enterprise and how they related to one another. Once you have an understanding of the organizational structure, you should analyze the individual departments themselves. This information will benefit you when designing network functions such as user groups and Active Directory Organizational Units (OUs), as well as the appropriate delegation of network administration.

You should also determine whether the organizational structure is a centralized or decentralized. A centralized structure adheres to a hierarchical reporting structure that resembles a family tree, with each sublevel reporting to a subsequently higher level and a single individual or group at the top of the hierarchy. In an Active Directory environment, this type of structure lends itself to a system of nested OUs.

A decentralized structure allow for greater autonomy within the business units, where various departments function more independently. In an Active Directory environment, this type of structure lends itself to a multiple domain system. An organization with a decentralized management structure can still handle network management centrally and vice versa. The transitive trust relationships built into Windows Server 2003 can allow centralized management of a multi-domain or multi-forest environment, or for tasks to be divided among departmental IT administrators.

1.1.2 Availability and Security

The efficient running and profit making of most organizations are dependent on the availability of information. This rationale is even more crucial to e-commerce sites and other Web-based businesses. Planning for high availability and fault tolerance will help you to minimize the downtime experienced by end users and customers. Windows Server 2003 offers **server clustering** and **Network Load Balancing**, both of which can provide the high availability required by most enterprises.

While availability is important, data access must be restricted only to those users that require access to the data. This requires that you consider protecting the data against unauthorized or illicit access. Establishing an information security strategy is critical in ensuring that your network design is prepared to address security concerns when they arise. Your security policy should provide a common baseline of security procedures based on your organization's security requirements.

When addressing security concerns within your network design, your three primary concerns are the confidentiality, i.e., restricting access to the data; data integrity, i.e., ensuring that the data has not been corrupted or altered in any way; and availability of your data.

Fault Tolerance

Fault Tolerance specifically refers to the ability of a piece of hardware or software to withstand the failure of a key component. This can be implemented at the hardware level using redundant power supplies or a Redundant Array of Inexpensive Disks (RAID) hard drive array. Clustering provides the ultimate in fault tolerance: completely redundant systems.

1.1.3 Scalability

When planning a network design, you should consider the scalability of your design. Scalability refers to how well a service or application can grow to meet client performance demands that will inevitably increase over time. It can refer to increasing system resources such as processors, memory, disk drives, and network adapters to an existing piece of hardware, or being able to replace existing hardware with more powerful equipment without causing network disruptions. It can also refer to adding new servers to meet increased demands.

Scalability

A scalable network is one that can expand over time to address network growth and improve client response time. Server clustering can also be used to address scalability issues by allowing you to add nodes to a cluster when your network encounters a period of growth.

1.2 Server Roles and Server Security

The default installation of Windows Server 2003 provides a wide variety of tools and functionality. However, additional features may still need to be installed and configured on the server to provide clients the specific services they require. Windows Server 2003 can be configured for various server roles, which allows it to provide specific functionality to the network. When you configure a server to perform a specific role, various services and tools are enabled or installed, and the server is configured to provide additional services and resources to network clients. These roles can be applied using the **Configure Your Server Wizard** and you can use the **Manage Your Server** tool to manage them.

Windows Server 2003 can be configured to perform 11 different roles. These roles are:

- **Domain controller**, which are used to manage domains and domain objects and provides user authentication through Active Directory;
- **File server**, which provides access to files stored on the server;
- **Print server**, which provides network printing functionality;
- **DHCP server**, which allocates IP addresses and provides configuration information to clients;
- **DNS server**, which resolves IP addresses to domain names;
- **WINS server**, which resolves IP addresses to NetBIOS names;
- **Mail server**, which provides e-mail services;
- **Application server**, which makes distributed applications and Web applications available to clients;
- **Terminal server**, which provides Terminal Services for clients to access applications running on the server;
- **Remote access/VPN server**, which provides remote access to machines through dial-up connections and virtual private networks (VPNs); and
- **Streaming media server**, which provides Windows Media Services so that clients can access streaming audio and video.

1.2.1 Domain Controllers (Authentication Servers)

Domain controllers are required to manage domains and domain-based objects. An important aspect of this management is the authentication and access control of users.

1.2.1.1 Active Directory

In order to perform these functions, the domain controller must have information about users and other objects in the domain. This information is provided by a directory service. In Windows 2000 and Windows Server 2003, the directory service is provided by Active Directory, which runs on domain controllers. It stores information about network resources and makes the resources accessible to users, computers and applications by uniquely identifying resources on a network. It also provides you with mechanisms to name, describe, locate, access, manage, and secure **network resources**. In addition, it allows for the **central management** of the Windows Server 2003 network, and for the **delegation of administrative control** over Active Directory objects, which are resources such as user data, printers, servers, databases, groups, computers, and security principals and security policies that are stored in the directory. Thus, the Active Directory directory service provides the structure and functions for organizing, managing, and controlling network resources.

When you install Active Directory on a Windows Server 2003 computer, the server becomes a domain controller. However, Active Directory cannot be installed on Windows Server 2003, Web Edition. Windows Server 2003, Web Edition computers can be only stand-alone or member servers that provide resources and services to the network.

You can use the **Active Directory Installation wizard** to install Active Directory on a Windows Server 2003 computer. To launch the Active Directory Installation wizard, click **RUN** on the **Start Menu** and type **DCPromo.exe** in the **Run** text box. **DCPromo** is a tool that promotes a stand-alone server or a member server to a domain controller. The first computer in a domain on which you install Active Directory will become the root domain controller. If the domain controller is being installed in an existing Windows domain or if it is being configured as a child domain, the Active Directory installation process will automatically make the appropriate connections and establish initial default trust relationships.

Note: Running **DCPromo.exe** on a domain controller also allows you to remove Active Directory directory services from the domain controller and demotes the domain controller to a member server or stand-alone server. If you remove Active Directory directory services from all domain controllers in a domain, you also delete the directory database for the domain, and the domain will no longer exist.

During the installation of Active Directory, a writable copy of the Active Directory database is placed on the server's hard disk. The file used to store directory information is called *NTDS.dit* and, by default, is located in the `%systemroot%\NTDS` folder. Each domain controller retains its own copy of the directory database, containing information about the domain in which it is located. If one domain controller becomes unavailable, users and computers can still access the Active Directory data store on another domain controller in that domain. Because a domain can have more than one domain controller, changes made to the directory on one domain controller must be updated on others. The process of copying these updates is called **replication**, which is used to synchronize information in the directory database across all domain controllers in a domain.

Domains

In Windows Server 2003, a domain is a logical grouping of network elements, including computers, users, printers, and other components that make up the network.

Stand-Alone Servers

In Windows Server 2003, a stand-alone server is a Server computer that does not have Active Directory installed on it and does not belong to a domain.

Member Server

In Windows Server 2003, a member server is a Server computer that belongs to a domain but does not have Active Directory installed on it. Once Active Directory is installed on a member server, it ceases to be a member server and becomes a domain controller.

1.2.1.2 Flexible Single Master of Operations Roles

By default, all domain controllers in a domain are equal peers. However, there are certain Active Directory functions that can be performed by only a single domain controller to prevent possible conflict. These functions are called **Flexible Single Master Operations (FSMOs)**. The domain controller assigned a particular FSMO is called a role master.

Some FSMO roles are unique to each domain while others are unique to the forest. There are the five FSMO roles: the PDC Emulator; the RID Master; the Infrastructure Master; the Domain Naming Master; and the Schema Master. The Domain Naming Master role and the Schema Master role are forest-wide roles that apply at the forest level, while the PDC Emulator role; the RID Master role; and the Infrastructure Master role are domain-wide roles that apply at the domain level.

Forests

A forest can either consist of a single tree or number of trees that do not share a contiguous namespace but do share a common schema and global catalog. In this arrangement, every tree root domain has a transitive trust relationship with the root domain. A single tree that is not related to any other tree constitutes a forest of one tree. The root domain contains the configuration and schema data for all trees in the forest.

1.2.1.3 PDC Emulator

In the default Windows 2000 mixed domain functional level, Active Directory supports the presence of downlevel Windows NT 4.0 Backup Domain Controllers (BDCs) by emulating a Windows NT 4.0 Primary Domain Controller (PDC) on a Windows 2000 or Windows Server 2003 domain controller. This is necessary because BDCs will only replicate from a PDC. The Windows 2000 or Windows Server 2003 domain controller that performs this function is the PDC Emulator role master. While in the Windows 2000 mixed domain functional level, objects representing security principals, i.e., users, computers, and groups, can only be created by the PDC Emulator. In addition, when a user changes a password, or an administrator resets a password for a user, the update is replicated to the PDC Emulator. The domain controllers in a domain check with the PDC emulator to see if a user's password has been changed when a user enters an "invalid" password. If the password has been changed, and is in fact valid, the user is allowed to logon.

You can transfer the PDC Emulator master role to another domain controller through the **Active Directory Users and Computers** snap-in.

1.2.1.4 RID Master

In a Windows domain, all security objects have a security identifier (SID). This SID is a combination of the SID of the domain and a sequential number called the Relative ID (RID), which is supplied by the RID Master. In domains that are in the default Windows 2000 mixed domain functional level, only the PDC Emulator can create security principals, therefore the PDC Emulator and the RID Master roles are held by the same domain controller. This guarantees that the SIDs will be sequential and unique. However, in the Windows 2000 native domain functional level, any domain controller can create security principals. In this type of domain, the RIDs may not be in sequence, but must still be unique. For this reason, only one domain controller can perform the role of the RID Master per domain. The RID Master ensures the uniqueness of the SID by assigning sections of the RID list to the domain controllers when they request it.

You can transfer the RID Master role to another domain controller through the Active Directory Users and Computers snap-in.

1.2.1.5 Infrastructure Master

The domain controller assigned the Infrastructure Master role is responsible for managing group and user references. When you add a user to a group, the user's distinguished name is added to the **Member** attribute for the group. The **User** object has a corresponding **MemberOf** attribute that contains the distinguished names of the groups to which the user belongs. These two attributes are examples of linked attributes. In linked attributes, the primary attribute is termed a forward link and the other attribute is a back-link. Only the forward link can be modified directly. The back-link is calculated. Thus, when a forward link is changed, such as when a new user is added to a group, the user's distinguished name is replicated to all domain controllers hosting a replica of the affected naming context. When a domain controller applies the update, it recalculates the back-link attribute for the affected user object. If the user's distinguished name changes, the system must update all the group objects that have the user as a member as quickly as possible. Updates to the **Member** attribute for group objects in the same domain as the user with the changed name occur immediately because the domain controller holds both the user object and the group object. But when a user is a member of a group in another domain, a domain controller in the remote domain must be informed about the name change so it can change the **Member** attribute for any affected groups in that domain. Updates to the remote domain are made by the Infrastructure Master domain controller via **multimaster replication**. You can transfer the Infrastructure Master role to another domain controller through the **Active Directory Users and Computers** snap-in.

Except in single-domain controller environments, and an environment where every domain controller retains a copy of the GC, the GC should not be hosted on the Infrastructure Master. The Infrastructure Master compares its data with the GC, therefore may be significant replication impacts and full replication may fail.

1.2.1.6 Domain Naming Master

Active Directory stores pointers to other domains in a special **CrossRef** object located in a **Partitions** container in the **Configuration** naming context. This object contains attributes that describe the distinguished name, DNS name, the flat name, and the name of the Domain naming context along with the kind of trust relationship that binds the domain to the forest. When you create a new domain in an existing forest, the new domain represents a separate naming context and necessitates the creation of a **CrossRef** object in a **Partitions** container. Only one domain controller in a forest, the Domain Naming Master, can make changes to the **Partitions** container. This ensures that two administrators cannot create new domains

Trees

A tree is a hierarchical arrangement of Windows Server 2003 domains that share a contiguous namespace. In such an arrangement the root domain name is attached as a suffix to the new domain names. The new domain is called a child domain of an existing parent domain and has a two-way, transitive trust relationship with its parent domain. Thus, a domain tree structure is formed by adding child domains to the root domain. The root domain contains the configuration and schema data for the tree.

The Schema

The schema is a framework of definitions that establishes the type of objects available to Active Directory. These definitions are divided into object classes and attributes, which is the information that describes the object. The schema is stored in the Active Directory database file *Ntds.dit*.

The Global Catalog

The Global Catalog provides data that permits network logon; stores the information that is necessary to locate an object in Active Directory; and contains the access permissions for each object and attribute stored in the global catalog and thus ensures that users can find only objects to which they have been assigned access.

with identical names during the same replication interval. By default, the Domain Naming Master is the first domain controller in a forest. You can transfer this role to any domain controller in any domain through the **Active Directory Domains and Trusts** snap-in. However, it is recommended that this domain controller reside in the root domain.

1.2.1.7 Schema Master

The schema is a framework of definitions that establishes the type of objects available to Active Directory. The objects in the schema thus define the very structure and identity of Active Directory for a forest. Objects can only be added, modified, or removed from the schema under strictly controlled circumstances. Only one domain controller in the entire forest can update the schema, which is then replicated to other domain controllers in the forest, and that is the Schema Master. The Schema Master role can be transferred to another domain controller through the **Active Directory Schema Master** snap-in.

Note: FSMO roles that are applied to a forest affect all domains within that forest. FSMO roles that are applied to a domain apply only to that domain. There is only one schema master and one domain naming master in a forest. There is only one RID master, PDC emulator, and infrastructure master in a domain.

1.2.1.8 Securing Domain Controllers

The effects of an insecure domain controller can be far-reaching. Information in Active Directory is replicated to other domain controllers, so changes on one domain controller can affect all of them. This means that if an unauthorized entity accessed the directory and made changes, every domain controller would be updated with these changes. This includes disabled or deleted accounts, modifications to groups, and changes to other objects in the directory.

It is important that group membership is controlled, so that the likelihood of accidental or malicious changes being made to Active Directory is minimized. This especially applies to the **Enterprise Admins**, **Domain Admins**, **Account Operators**, **Server Operators**, and **Administrators** groups.

Because anyone who has physical access to the domain controller can make changes to the domain controller and Active Directory, it is important that these servers have heightened security. You should consider using smart cards to control authentication at the server console.

Encryption should also be used to protect data and authenticate users. As mentioned, NTFS partitions allow file encryption, and **Kerberos** provides strong authentication security. In Windows Server 2003, Kerberos is the default authentication protocol for domain members running Windows 2000 or later. However, it is not compatible with pre-Windows 2000 computers such as Windows NT 4.0 and Windows 98.

To ensure domain controllers are secure, there are a number of password requirements that Windows Server 2003 enforces on domain controllers by default. The password cannot contain any part of the user's account name and must be a minimum of six characters in length. In addition, the password must contain characters from three of the four categories: lowercase letters, uppercase letters, numerals, and special characters.

1.2.2 File and Print Servers

Two of the basic network functions are the saving of files in a central location on the network and printing documents to shared printers. When a Windows Server 2003 computer is configured as a file server or print server, additional functions become available that makes using and managing the server more effective.

1.2.2.1 Print Servers

Print servers are used provide access to printers across the network. A benefit of print servers for administrators is that they provide an added level of manageability for network printing. Print servers allow you to control when print devices can be used by allowing you to schedule the availability of printers, set priority for print jobs, and configure printer properties. Using a browser, an administrator can also view, pause, resume, and/or delete print jobs. By configuring Windows Server 2003 in the role of a print server, you can manage printers remotely and by using **Windows Management Instrumentation (WMI)**, which allows an administrator to manage components like print servers and print devices from the command line.

1.2.2.2 Securing File Servers

Because file servers are used to store data in a central location, it is important that they are kept secure. You need to ensure that only those who are authorized are able to use the files. Thus, the volumes on a file server should be formatted with NTFS so that file and folder permissions can be on. You should also implement EFS on these disks. When EFS is used, unauthorized users and malicious programs are prevented from accessing the content of files, regardless of their permissions. Although the process involved in the encryption and decryption of data can be quite complex, EFS file encryption is completely transparent to the user. However, you cannot encrypt system files and you cannot share files that have been encrypted. Also, encrypted files cannot be compressed and compressed files will be decompressed when you encrypt them.

1.2.2.3 File Servers

File servers provide centralized access and storage of files that are stored on the server's hard disks. Users can store their files on a file server, rather than to their local hard disks, and share them with other users. When a file is saved to a volume on a file server, clients who have access to the directory in which the file was saved can access it remotely from the server. This type of server is also important when multiple employees use network-accessible applications. In such cases, data may need to be saved from the application to a shared database, spreadsheet, or other type of file.

File servers allow administrators to manage disk space allocation and control user access. If the file server's disks are **NTFS** volumes, **disk quotas** can be set and the **Encrypted File System (EFS)** can be enabled. With EFS, data can be encrypted using a public key system. This makes it difficult for unauthorized users to access data, while being transparent to authorized users.

The **Distributed File Service (Dfs)** can be implemented to make it easier for users to access shared files. Dfs allows data that is located on different volumes, shares, or servers appear as if they reside in the same location. This makes it easier for users to find the data they need, because they do not need to search through multiple locations to access the files they are permitted to use.

1.2.2.4 Securing Print Servers

Files that are being printed may also require protection. **IPSec** can be implemented to protect the transmission of data being sent to printers. Physical security issues can be very important for printers as anyone with access to a printer can remove printed documents from it.

You can implement printer permissions to control who can print and manage network printing. **Printer** permissions are set on the **Security** tab of a printer's properties dialog box. There are three printer permissions that you can allow or deny. These are: **Print**, which allows the user to print documents; **Manage Printers**, which allows users to perform administrative tasks, such as starting, pausing, and stopping the printer; changing spooler settings; sharing the printer; modifying permissions; and changing property settings on a printer; and **Manage Documents**, which allows users to perform administrative tasks relating to documents being printed, such as starting, pausing, resuming, reordering, and canceling documents.

You can assign the **Manage Printers** permission to a user only if that user has the **Print** permission. However, the **Print** permission is assigned to the **Everyone** group. Thus, all users have access to print to a printer once it is shared on the network, therefore, you should remove the **Print** permission from this group and assign the permission to the specific groups or users that should have access to the printer.

1.2.3 DHCP Servers

A **Dynamic Host Configuration Protocol (DHCP)** Server automatically issues IP addresses to clients on TCP/IP networks. An IP address uniquely identifies a client on the network allowing them to send and receive packets of data. When information is transmitted across a network, the data is broken up into smaller packets, which are reassembled by the receiver. Each packet contains the IP address of who is sending the data and who should receive it. Therefore, no two computers on a network can have the same IP address at the same time. DHCP assigns dynamic IP addresses. When an IP address is dynamically assigned, the client contacts the DHCP server for an IP address. The DHCP server responds by issuing an IP address from a pool of available addresses stored in a database, as well as other IP configuration information that is required by the client.

Because DHCP provide IP address and configuration information to clients while DNS and WINS servers resolve names to IP addresses, malicious persons and programs may be able to prohibit users from connecting to the network, redirect traffic to other locations, and impact the ability to use network resources.

DHCP servers do not require authentication when providing a lease. Any client that contacts the DHCP server can obtain a lease and connect to the network. In addition to receiving an IP address as part of the lease, clients may also be automatically configured with WINS or DNS server information. To avoid this, it is important that you restrict physical and wireless access to your network. This helps to prevent unauthorized persons from successfully connecting to your network and obtaining a valid DHCP lease. In addition, auditing should be enabled on the DHCP server so that you can review requests for leased addresses. By reviewing the logs, you may be able to identify possible problems.

Rogue DHCP servers can also be a problem on the network. When a client requests a DHCP lease, it does so by broadcast. If an unauthorized person puts a DHCP server on the network, the incorrect IP address and configuration information could be provided to clients. This is not the case if the rogue DHCP server is running Windows 2000 or Windows Server 2003, because these must be authorized in Active Directory. If the server determines that it is not authorized, the DHCP service will not start. However, pre-Windows 2000

and non-Windows DHCP servers require no authorization and can be effectively used as rogue DHCP servers in a Windows Server 2003 environment. Handing out bogus DHCP leases that do not expire can be a very effective DoS technique. Because of this, it is important to monitor network traffic for DHCP server traffic that does not come from your network's authorized DHCP servers.

Restricting access to DHCP tools and limiting membership in groups that can modify DHCP settings are other important steps in securing a DHCP server. To administer DHCP servers remotely using the DHCP console or **netsh** utility, you need to be a member of the Administrators group or the DHCP Administrators group. By restricting membership in these groups, you limit the number of people who can authorize a DHCP server to service client requests.

1.2.4 Name Resolution

Windows Server 2003 supports the use of user-friendly domain names to represent the IP address of a host or a client. This however requires name resolution so that the computer can identify the IP address that the user-friendly name refers to. Windows Server 2003 supports name resolution through the **Windows Internet Naming Service (WINS)** and through the **Domain Name Services (DNS)**.

1.2.4.1 WINS Servers

The Windows Internet Name Service (WINS) resolves IP addresses to **NetBIOS** names, and vice versa. NetBIOS names are used by pre-Windows 2000 servers and clients, and they allow users of those operating systems to log on to Windows Server 2003 domains. They are supported in Windows Server 2003 for backward-compatibility with these older systems. By implementing a WINS server, you allow pre-Windows 2000 clients to search for computers and other resources by computer name, rather than by IP address.

WINS is designed to work with **NetBIOS over TCP/IP (NetBT)**, which does not require any authentication. Because a user does not need to provide credentials to use WINS, it is potentially available to unauthorized persons or programs. These entities could request a massive number of names to be registered or resolved by the WINS server, so that the server becomes bogged down and unable to process other requests. This type of attack is called a denial of service (DoS) and is designed to overload systems and prevent access for legitimate users.

1.2.4.2 DNS Servers

The Domain Name Service (DNS) is a common method of name resolution that is used on TCP/IP networks. **Active Directory** is integrated with DNS, and it uses DNS servers to allow users, computers, applications, and other elements of the network to easily find domain controllers and other resources on the network. DNS is a hierarchical, distributed database that maps user-friendly domain names to IP addresses. When a user enters a DNS name into a browser or other application, it is sent to a DNS server, which looks up the IP address for that domain. This IP address is sent back to the client, which uses the numeric address to locate and communicate with the computer at this address.

1.2.5 Web Servers

Web servers allow organizations to host their own Web sites on the Internet or a local intranet. Implementing a Web server in an organization allows users to benefit by accessing information, downloading files, and using Web-based applications.

Internet Information Services (IIS), which is included in Windows Server 2003, is required for configuring a Web Server. IIS allows users to access information using a number of protocols that are part of the TCP/IP suite. These protocols include:

- **Hypertext Transfer Protocol (HTTP)**, which is used by the **World Wide Web Publishing** service in IIS. It allows users to access Web pages using a Web browser or other Web-enabled applications. HTTP supports the Hypertext Markup Language (HTML), Active Server Pages (ASP), and Extensible Markup Language (XML).
- **File Transfer Protocol (FTP)**, which is used for transferring files between clients and servers. Using this service, clients can copy files to and from FTP sites using a Web browser or FTP client software.
- **Network News Transfer Protocol (NNTP)**, which is used for newsgroups or discussion groups. The NNTP service in IIS allows users to post news messages. Other users can browse through messages stored on the server, respond to existing messages, and post new ones using a newsreader program.
- **Simple Mail Transfer Protocol (SMTP)**, which is used to provides e-mail capabilities. The SMTP service that is installed with IIS provides limited services for transferring e-mail messages. Using this service, Web developers can collect information from users of a Web site, such as having them fill out a form online. Rather than storing the results of the form locally in a file, the information can be e-mailed using this service.

Note: A Web server is not a role that is configured using the **Configure Your Server Wizard**. It is installed as part of the **application server role**.

1.2.5.1 Securing Web Servers

IIS provides a variety of services that allow users to access information from the Web server service. It therefore provides potential avenues of attack for unauthorized users, malicious programs, and other sources. For this reason, it is not installed by default and should remain uninstalled if you do not need a Web server on your network.

Once IIS is installed on Windows Server 2003, it is locked down to prevent any unneeded from being exploited and will provide only static content to users. If dynamic content is required, you will need to enable the necessary features.

By default, IIS will not compile, execute, or serve files with dynamic extensions. Dynamic content can contain malicious code or have weaknesses that can be exploited. If files that provide dynamic content need to be used on the Web server, you must add the file extensions to the Web service extensions list. Any file types that are not needed should not be added.

1.2.5.2 Firewalls

Implementing a firewall will provide additional security for Web servers. Firewalls prevent direct access between a network and clients by having traffic pass through the firewall, which determines if the traffic should be blocked or allowed. The firewall thus acts as a buffer between the Web server and clients using it or between the internal network and other networks like the Internet. Rules can be set up on the firewall controlling what kinds of traffic may pass and who can perform certain actions.

If you provide public services on your Web server, you have at least three security zones:

- The public Internet, which is untrusted;
- The perimeter network, which is semi-trusted; and
- The private network, which is trusted.

This three-zone infrastructure creates two borders: one between the public and the perimeter network, and the other between the perimeter network and the private network. Each of these two borders must have a separate policy to allow data to flow through it. Perimeter security is usually accomplished using a two-stage firewall system: one stage allows access to public servers, and another stage prevents all access to the internal network.

The network between the public and private networks is called a perimeter network or a **demilitarized zone (DMZ)**. The public side of the perimeter network is protected by a firewall that allows public access to the services you intend to provide, such as Web access. The private side of the perimeter network is protected by another firewall that allows only encrypted and authenticated protocols required for remote access and to allow public servers to exchange data with private servers.

The private network must be strongly blocked against servers in the perimeter network. If your private-side firewall policy allows those servers wide access to your private network, hackers will be able to bounce through the perimeter network to the private side of the network. Policies that allow access on the private side of the firewall should be restricted to the specific protocols and computers that the public servers actually require access to. Servers in the perimeter network should never be linked to the domain, so that domain account information cannot be gleaned from them if they are exploited.

Some firewalls, including **Microsoft Internet Security and Acceleration (ISA) Server**, allow you to create a virtual perimeter network by employing a third network adapter in the firewall with its own policy. The Internet is attached to one adapter, the private network to another, and the perimeter network to the third. These firewalls are frequently referred to as being tri-homed or as having DMZ support. These firewalls are just as effective as using two firewalls to enforce your public security policy as long as they are correctly configured. Some software-based firewalls such as ISA Server have no inherent limit to the number of interfaces you can use. However, because policy can be configured strictly based on IP addresses, it is usually not necessary to use more than three network interfaces in a single firewall.

Because the Internet does not require a log on, wireless access points located in a typical perimeter network can be exploited to gain Internet access. It has recently become popular for hackers to connect to wireless devices for a free Internet connection rather than attempting to break into the network that they serve. To prevent this type of use, you should place RRAS dial-in servers and wireless access points in a fourth security zone that blocks both Internet access and private network access to users who have not established a VPN connection. Once hackers find that they cannot easily reach the Internet, they will stop using your resources and go elsewhere.

1.2.6 Database Servers

Database servers are used to store and manage databases, and to provide data access for authorized users. This type of server keeps the data in a central location that can be regularly backed up. It also allows users and applications to centrally access the data across the network. A large number of the databases used in your organization can be kept on one server or a group of servers that are specifically configured to protect data and service client requests.

Note: A Database server is not a role that is configured using the **Configure Your Server Wizard**. It is any server that runs a network database application, such as Microsoft SQL Server or Oracle.

When securing databases, you can take advantage of the security features offered by the database software. Microsoft SQL Server, for example, provides two methods of authenticating clients to access data: **Windows Authentication Mode** and **Mixed Mode**. When Windows Authentication Mode is used, the SQL Server administrator has the ability to grant logon access to Windows user accounts and groups. If Mixed Mode is used, users can be authenticated through either Windows authentication or separate accounts created within SQL Server.

In addition, most database applications allow you to control access to data at a granular level. You can set permissions to control the operations that a user can perform on the data contained in the database. In many database applications, you can set permissions at the server, database, or table level. These permissions are different from those that can be set through Active Directory and NTFS, and apply only within the database program.

1.2.7 Mail Servers

Mail servers allow users to send and receive e-mail messages. Users send e-mail to other users through at least one mail server. When the message arrives, the destination mail server stores the message until it is retrieved by the user. If the mail server does not handle the email account for an intended recipient, it will transfer the message to a mail server that does. In this way, mail servers will work together to ensure a message reaches its intended audience.

When Windows Server 2003 is configured as a mail server, the **Simple Mail Transfer Protocol (SMTP)** and **Post Office Protocol (POP3)** are enabled. SMTP is used by clients and mail servers to send e-mail, while POP3 is used by clients when retrieving e-mail from their mail server.

When Windows Server 2003 is configured with the mail server role, it should be set up to require secure authentication from e-mail clients. Client software and the mail server's POP3 service can be configured to accept only passwords that are encrypted in order to prevent them from being intercepted by unauthorized parties.

In Windows Server 2003, the Microsoft POP3 Service uses **Secure Password Authentication (SPA)** to ensure that authentication between the mail server and clients is encrypted. SPA is integrated with Active Directory, which is used to authenticate users as they log on to retrieve their e-mail. SPA can also authenticate to local accounts on the mail server. When the POP3 service is configured to accept only authentication using SPA, clients must also be configured to use encrypted authentication. If they are not, clients will attempt to authenticate using clear text and will be rejected by the mail server.

1.2.8 Application Servers and Terminal Servers

Application servers and terminal servers allow users to access applications running on the server rather than on the user's computer. This frees resources on the client computer and enables users to benefit from newer application technologies.

1.2.8.1 Application Servers

Application servers allow users to run Web applications and distributed programs from the server. By using the application server role, the server is configured to provide greater reliability and performance to these applications.

Servers configured in the application server role also have IIS 6.0 installed by default. IIS lets the application server provide Web-based applications to users of the network. Because the application server may have a Web server installed on it, steps need to be taken to ensure the Web server is also secure. If IIS is not required, it should be uninstalled.

1.2.8.2 Terminal Servers

Terminal servers allow remote access to applications using thin-client technology. This makes the user's computer act as a terminal emulator. The user connects to the terminal server using client software installed on their computer, logs on to the Terminal Services session, and is presented with a user interface. Keystrokes and mouse clicks generated by the user at the client are sent to the terminal server. Updated screen images are sent back from terminal server to the client system. When working in a session, the user is essentially working at the server. All processing is occurring at the server, which is being interacted with through the client software.

Because terminal servers provide access to applications and data, they also need to be configured to ensure that users and hosts do not achieve unauthorized access. By setting permissions on connections, you can control who can access a server and perform specific tasks. This is in addition to the permissions that can be set on files accessed by users in a terminal server session. By limiting access in these ways, you can control who is able to use files and applications and what actions they are able to perform.

Terminal servers can also be configured to use specific levels of encryption. When a communications link is established between a client and the terminal server, the data transmitted between them can be encrypted to prevent others from being able to view and use it. The encryption levels that can be set are:

- **High**, which is the default level and uses 128-bit encryption. If clients do not support this level of encryption, they will be unable to connect to the terminal server.
- **Low**, which provides only one-way encryption. Clients send data to the server using 56-bit encryption, but any data sent from the server to the client is unencrypted.
- **FIPS compliant**, which encrypts data using **Federal Information Processing Standard (FIPS)** encryption algorithms and is mandated for use by the US government.
- **Client compliant**, which encrypts data using the strongest possible key strength supported by the client. Because the level of encryption depends on the client, it may be a good idea to use it if legacy clients or a mix of clients are used on the network. However, if you have strong security requirements, this level does not allow you to specify the encryption level clients will use, so it should not be used.

1.2.9 Certificate Authorities

Certificate authorities (CAs) are servers that issue and manage certificates. **Certificates** can be used for a variety of purposes, including encryption, integrity, and verifying the identity of an entity, such as a user,

Web Applications

Web applications are programs that use Internet technologies to provide functionality and are accessible across networks and the Internet through Web browsers. Because Web applications require Internet technologies, IIS subcomponents such as ASP should be installed.

Distributed Applications

Distributed applications divide the program so that part of it runs on the client while the rest runs on one or more servers.

computer, or application. Certificates can be used as a proof of identity. They are digitally signed files that contain data a wide range of information, often including a cryptographic key, information about whom or what the key is issued to, an expiration date, where the validity of the certificate can be checked, and which CA signed the certificate. Certificates are typically part of a larger security process known as a **Public Key Infrastructure (PKI)**.

In Windows Server 2003, **Certificate Services** is used to create a CA, format and modify the contents of certificates, verify information provided by those requesting certificates, issue and revoke certificates, and publish a **Certificate Revocation List (CRL)**, which is a list of certificates that are expired or invalid, and it is made available so that network users can identify whether certificates they receive are valid.

Certificate Services supports implementing a hierarchy of CAs, so that a single CA is not responsible for providing certificates to the entire network or authenticating the entire intranet or Internet. In this hierarchy, there is a single **root CA** and any number of **subordinate CAs**. The root CA is the most trusted CA in the hierarchy and any client that trust the root CA will also trust certificates issued by any CA below it. These subordinate CAs use the root CA's public key and bind it to its own identity. In doing so, the subordinate can also issue certificates to users and computers.

Because of the trust between root and subordinate CAs, if the root CA is compromised, subordinate CAs continue trusting it. This compromises all certificates issued by the CAs in the hierarchy. As a security measure, you should disable the root CA's ability to issue certificates online and allow only child CAs to perform this function. An offline root CA is more difficult to compromise, since physical access to it is required.

Additional benefits can be derived from the use of enterprise CAs. When a user requests a certificate from an enterprise CA, that CA is able to validate the information provided by the user through Active Directory. This can provide an extra measure of security. Standalone CAs require manual inspection and approval of requests by a CA administrator. Manual processes are typically much more error-prone than automated ones.

When certificates are found to be invalid, they should immediately be revoked. After a certificate is revoked, the CRL should be immediately updated and published. The CRL is used to inform the world of certificates that are no longer valid. If the certificate is invalid, the software used to check it often allows the user to decide whether or not to trust the certificate holder.

CA and the Windows Server 2003 KPI are discussed in more detail in [Section 7](#).

1.3 Planning a Server Security Strategy

In creating a security plan, it is important to realize that the network environment will never be completely secure. If people are willing to invest enough time, effort, and money into hacking a system, they will probably find a way in. The goal is to make it difficult for intruders to obtain unauthorized access. It is also critical to protect servers from potential disasters and to have methods to restore systems in the event that they are compromised.

A good security plan considers the minimum security requirements for an organization. This is the major determining factor when considering which Windows operating system you should install, and will identify the configurations necessary to meet the organization's security requirements. The various Windows server operating systems offer differing security features with the latest version offering the better security features. In addition, the various editions of the operating system offer extra security features.

1.3.1 Windows Security Features

Windows 2000 offers a number of security features that were not available in Windows NT 4.0. Many of these features have been updated in Windows Server 2003. In addition, new features have been added to Windows Server 2003 and make Windows Server 2003 the most secure Microsoft Windows server product available.

Windows 2000 Server was the first version of Microsoft Windows to provide **encryption** of data over the network and in the file system through IPSec, which allows encryption of data across the network and Encrypted File System (EFS), which uses a public key system to encrypt data on hard disks; built-in support for **smart cards**; Kerberos authentication, which is an industry-standard security protocol that uses mutual authentication to verify the identity of a user or computer, as well as the network service that is being accessed; and the **Active Directory** directory service.

Smart Cards

A smart card is approximately the size of a credit card. When a smart card is inserted into a smart card device, it provides authentication information. With smart cards, the security of a network can be greatly enhanced because it is necessary to physically possess the card to log on.

1.3.2 Minimum Requirements for the Operating System

Other considerations in the choice of the operating system are the minimum system requirements for the operating system. If your existing server cannot handle a particular version of Windows, you will have to upgrade the hardware, purchase a new server to support the operating system you want, or choose an operating system for which the current server's hardware is sufficient. The minimum system requirements for the various Windows server operating systems are shown in Table 1.1.

TABLE 1.1: *Minimum System Requirements for Windows Server Operating Systems*

OS	Hardware	Minimum System Requirements
Windows NT Server 4.0	Processor	Intel 486 / 33 MHz Processor or equivalent
	Memory	16 MB Ram (32 MB Recommended)
	Hard Disk Space	125 MB for x86 based computers and 160 MB for RISC-based computers
Windows 2000 Server	Processor	Intel 133 MHz Pentium Processor
	Memory	128 MB Ram (256 MB Recommended)
	Hard Disk Space	2 GB available hard disk space with 1GB free space
Windows 2000 Advanced Server	Processor	Intel 133 MHz Pentium Processor
	Memory	128 MB Ram (256 MB Recommended)
	Hard Disk Space	2 GB available hard disk space with 1GB free space
Windows 2000 Datacenter Server	Processor	Pentium III Xeon processor
	Memory	256 MB Ram
	Hard Disk Space	2 GB available hard disk space with 1GB free space
Windows Server 2003,	Processor	Intel 133 MHz Pentium Processor
	Memory	128 MB Ram

Standard Edition	Hard Disk Space	1.5 GB
Windows Server 2003, Web Edition	Processor	Intel 133 MHz Pentium Processor
	Memory	128 MB Ram
	Hard Disk Space	1.5 GB
Windows Server 2003, Enterprise Edition	Processor	Intel 133 MHz Pentium Processor for x86-based computers; Intel 733 MHz Pentium III Processor for Itanium-based computers
	Memory	128 MB Ram
	Hard Disk Space	1.5 GB available hard disk space x86-based computers; 2 GB available hard disk space for Itanium-based computers
Windows Server 2003, Datacenter Edition	Processor	Intel 400 MHz Pentium III Processor for x86-based computers; Intel 733 MHz Pentium III Processor for Itanium-based computers
	Memory	512 MB Ram
	Hard Disk Space	1.5 GB available hard disk space x86-based computers; 2 GB available hard disk space for Itanium-based computers

In addition, you must identify potentially threats to the network and the available countermeasures to deal with them.

1.4 Identifying Minimum Security Requirements

Before you can begin implementing security measures, you need to know what needs protecting. Different organizations have different needs. You need to determine which risks could threaten the organization, what impact these threats would have on the organization, what assets will be affected by a potential problem, what assets the organization needs to function, and how a potential threat can be minimize. The three main types of threats are:

- Environmental threats**, which can be natural disasters, such as storms, floods, fires, earthquakes, tornadoes, and land slides; and man-made disasters. The types of natural disasters that can occur generally vary from one geographical region to another. When dealing with this type of disaster, it is important to analyze the entire company's risks, considering any branch offices located in different areas that may be prone to different natural disasters. Man-made disasters can also occur when someone creates an event that has an adverse impact on the company's environment. For example, faulty wiring can cause a fire or power outage. In the same way, a company could be impacted by equipment failures, such as the air conditioning breaking down in the server room, a critical system failing, or any number of other problems.

Assets

Assets are property and resources that have value to the company, and can include hardware, such as servers, workstations, hubs, and printers; software; data; personnel; sundry equipment, such as office supplies, furniture, and tools; and facilities.

Risk

Risk is the possibility of experiencing some form of loss. To address risks, you need to determine which events and factors in an organization are potential threats, and then devise ways to deal with them before they become actual problems. There are many different risks that can affect an organization, and the types of risks will often vary from business to business.

- **Deliberate threats**, which is a threat that was intentionally caused. These types of threats result from malicious persons or programs, and they can include potential risks such as hackers, viruses, Trojan horses, and various other attacks that can damage data and equipment or disrupt services. This type of threat can also include disgruntled employees who have authorized access to such assets and have the ability to harm the company from within.
- **Accidental threats**, which is a threat that was not caused intentionally. Employees can accidentally delete a file, modify information with erroneous data, or make other mistakes that cause some form of loss. Because people are fallible by nature, this type of risk is one of the most common.

1.5 Planning Baseline Security

Windows Server 2003 provides a number of **security templates** that allow you to apply security settings to the various computers in the organization. These templates provide a baseline for analyzing security.

Security templates are text files that contain numerous policy settings pertaining to computer security within the **Security Settings** namespace of a Group Policy Object (GPO). Because security templates are text files, they can be exported from one GPO and imported into any number of other GPOs, allowing you to distribute security settings among individual computers or independent domains. They thus provide a centralized method for creating a standardized security baseline in a Windows 2000 environment.

1.5.1 Predefined Security Templates

Windows Server 2003 provides a number of predefined security templates that can be copied to a new name and customized using the **Security Templates** snap-in. Each security policy template has a default set of categories:

- **Account Policy**, which defines the policy for user account or security account authentication. This category has three subcategories:
 - **Password Policy**, which defines the policy for password restrictions, such as minimum password length, password history maintenance, etc.
 - **Account Lockout Policy**, which defines the policy for account lockout when the incorrect password is provided for a security account at logon.
 - **Kerberos Policy**, which defines the policy for the use of the Kerberos protocol, including maximum lifetimes for Ticket Granting Tickets (TGTs), Service Tickets (STs), maximum lifetimes for ticket renewal, maximum tolerance for computer clock synchronization deviance, and the verification of group memberships and account lockout status.
- **Local Policy**, which defines the policies for the local computer on which the security template is applied. This category also has three subcategories:
 - **Audit Policy**, which defines the policy for the type of events that is to be audited and stored in the local computer's security log.
 - **User Rights Assignment**, which defines the policy for user rights.
 - **Security Options**, which define the policy for security options that can be located in the Registry.
- **Event Log**, which defines the configuration options for the Application, System, and Security event logs that can be viewed through **Event Viewer**.
- **Restricted Groups**, which is used to define memberships of security groups.
- **Systems Services**, which defines restrictions for services installed on a computer.

- **Registry**, which defines security for registry keys and their subtrees. This includes permissions and auditing for Registry objects.
- **File System**, which defines discretionary access control list (DACL) and system access control list (SACL) settings for any folders included within this policy. This policy requires the use of NTFS.

The default installation of Windows Server 2003 automatically copy's several pre-configured security templates into the %SystemRoot%\Security\Templates folder. These templates are:

- **Setup security.inf**, which contains the default security settings for a default installation of Windows Server 2003;
- **DC security.inf**, which contains the default security settings for a domain controller;
- **Securedc.inf**, which contains enhanced security settings for domain controllers;
- **Securews.inf**, which contains enhanced security settings for workstations;
- **Hisecdc.inf**, which contains high-level security settings for domain controllers;
- **Hisecws.inf**, which contains high-level security settings for workstations;
- **Compatws.inf**, which relaxes security settings on a workstation or server to resolve application compatibility problems;
- **Rootsec.inf**, which contains the default security settings for the system volume (%systemdrive%);
- **Iesacis.inf**, which contains settings to lock down Internet Explorer;

1.5.1.1 Default Security Templates

There are two default security templates in Windows Server 2003: *Setup security.inf* and *DC security.inf*.

- The **Setup security.inf** template is created and applied during the installation of Windows Server 2003. It can vary from one computer to another, depending on whether the installation was a clean installation or an upgrade. *Setup security.inf* can be used on servers and client computers but not on domain controllers. You should not use Group Policy to apply *Setup security.inf* as it contains a large amount of data. Because Group Policy is periodically refreshed, a large amount of data would move through the domain if *Setup security.inf* is applied through Group Policy, and can seriously degrade performance. On a clean installation of Windows Server 2003, the *Setup security.inf* template does not enforce a **password history**, a **minimum password age** and a **minimum password length** of 8 characters but sets the **maximum password age** to 42 days. It also does not define an **account lockout**, **Kerberos** and **audit** policies.
- The **DC security.inf** template is created when a Windows Server 2003 computer is promoted to a domain controller. It contains a number of default security settings, including settings for the file system, Registry, and system services. This template allows you to reapply the default domain controller security settings. However, reapplying the default setting may overwrite permissions on new files, registry keys and system services created by other applications. You can reapply the *DC security.inf* template using the **Security Configuration and Analysis** snap-in or the `secedit` command-line tool.

1.5.1.2 Secure Security Templates

Windows Server 2003 provides two secure security templates, *securews.inf* and *securedc.inf* which are designed to increase the security provided by the default security templates. These templates do not contain configuration settings in the **Restricted Groups**, **Systems Services**, **Registry**, and **File System** categories.

But, because these templates apply an incremental increase in security, they build on the default security template. Therefore, the secure setting for the Restricted Groups, Systems Services, Registry, and File System categories that are applied by the default templates are retained.

The secure security templates increase security by enforcing a **password history** of 24 passwords and a **minimum password length** of 8 characters. It also sets the **account lockout duration** to 30 minutes and an **account lockout** policy of 5 bad attempts. These templates also set an **auditing policy** to audit the logon events, account management, object access, audit policy changes, and audit privilege use. However, these templates do not define **user rights** policies. The **event logs** for the secure security template increases the size of the security logs to 5120 KB. Restrictions to guest access to the event logs have been enabled. The retention days are not defined and will thus use the settings enforced by the basic security template. The retention method for the security log is set to **As needed**.

The *securedc.inf* template is used on domain controllers to enhance security while minimizing the impact on applications. This template configures servers to refuse LAN Manager responses, which computers running operating systems such as Windows for Workgroups, Windows 95, and Windows 98 use for authentication purposes. For these clients to be able to connect to a domain controller with the *securedc.inf* template applied, the clients will need to have a patch or the **Active Directory Client Extensions Pack** installed on them.

The *securews.inf* template provides the same settings as the *securedc.inf* template, but it applies to workstations or servers that are not configured as domain controllers. This template limits the use of NTLM by configuring clients accessing the machine to respond with NTLMv2 responses. When this template is applied, the domain controllers that contain user accounts for those who will log on to the client must run at least Windows NT 4.0 with Service Pack 4.

1.5.1.3 High Security Templates

Windows Server 2003 provides two secure templates, *hiseaws.inf* and *hiseadc.inf* which enforce security requirements on network traffic and protocols. It is designed for Windows Server 2003 computers operating in a Windows 2000 native domain functional level or a Windows Server 2003 domain functional level. All network communications are digitally signed or encrypted and these systems will not be able to communicate with Windows NT, Windows 98 or Windows 95 hosts. The high security templates have a **maximum password age** of 42 days and a **lockout duration** of 0, thus, an account remains locked until an administrator unlocks it. However the **built-in administrator account** cannot be locked out. The local policy settings for the high security templates audits success and failure for logon events, object access, privilege use, and system events. For the event policy, the security log is increased from 5120 kilobytes, on the secure policy, to 10240 kilobytes, on the *hiseaws.inf* template.

The *hiseadc.inf* template is used to apply high-level security settings to a domain controller. This template will cause the domain controller to require encrypted authentication and will prevent most pre-Windows 2000 computers from being able to communicate with the server, because the domain controller will require clients to communicate using **NTLM version 2** (NTLMv2).

1.5.1.4 Backward Compatible Security Templates

The *compatws.inf* security template is designed to provide backward compatibility with pre-Windows 2000 operating systems such as Windows NT 4.0 and Windows 98. The default security templates do not permit the **Users group** to run applications that access **Registry** settings, operating system files, program files, or

other users' data. Therefore members of the Users group who are not members of the **Administrators group** or **Power Users group** cannot run most legacy software applications on Windows Server 2003 as most of these legacy applications need to access, write to or modify system files and the Registry. The *compatws.inf* security template relaxes the default permissions for the Users group so that legacy software applications not conforming to the security setting enforced by the default security template would be more likely to run correctly. The template grants members of the **Users group** permission to modify and write to certain areas of the file system and certain registry keys commonly accessed by legacy applications. It only has settings for items in the **Registry** and **File System** categories. It also includes a setting in the **Restricted Groups** category that removes all the members of the **Power Users group**.

Note: An alternative to applying the *compatws.inf* security template is to add the users who need to run legacy software applications to the **Power Users group**. This, however, is not recommended because membership to the Power Users group provides some administrative capabilities, such as adding local users or managing NTFS permissions on the local computer.

1.5.1.5 Miscellaneous Security Templates

Windows Server 2003 ships with two other security templates: *rootsec.inf*, which provides system root security; and *iesacsl.inf*, which provides lockdown security for Internet Explorer.

- The *rootsec.inf* security template specifies the permissions for the system drive root. As such, it only contains settings in the **File System** category and can be used to reapply the root folder permissions if they are inadvertently changed. This template does not overwrite explicit permissions that are defined on child objects; it propagates only the permissions that are inherited by child objects.
- The *iesacsl.inf* template is used to lock down security settings used by Internet Explorer (IE), which can be used to access data on the Internet or on a corporate intranet. You can use this template to enhance security by enforcing stricter settings on Internet Explorer. This template has entries only in the **Registry** category for registry keys pertaining to Internet Explorer.

1.5.2 Managing Security Templates

In addition to the **Security Templates snap-in**, Windows Server 2003 provides three other tools which you can use to manage security templates. These are the **Security Configuration and Analysis snap-in**; the **Group Policy Object Editor**; and the `secedit.exe` command-line utility.

- The **Security Configuration and Analysis snap-in** can be used to analyze how closely a computer's effective security settings match a specific security template and to apply security template settings to a specific computer. The Security Configuration and Analysis snap-in can create a database of a computer's security settings and compare that database against numerous security templates. It also allows you to export the computer's security settings to a new template file that can then be applied to other computers.
- The **Group Policy Object Editor** can be used to import and export security template files but cannot be used to analyze the security settings of a computer. When you import security settings into a GPO, those settings apply automatically to all computers within that GPO's scope. Using the Group Policy Object Editor, you can import policies stored in templates or export current security settings to a template file that can then be used to configure other computers.

- The **SecEdit.exe** command-line utility provides powerful scripting functions to accomplish tasks that cannot be accomplished using management console snap-ins. It also allows you to analyze and configure computers using templates, and to automate security configurations. However, you cannot use **SecEdit** modify or export a template file. The **SecEdit** command-line utility supports a number of parameters. These parameters are listed in Table 1.2.

TABLE 1.2: The SecEdit Command Parameters

Parameter	Function
/analyze	Analyzes the security settings of a computer
/configure	Applies the security template to a computer
/export	Exports the security settings in the database to a template file
/import	Imports a template into the database so that its settings can be used to analyze the computer or to configure the computer's security settings
/validate	Validates the syntax of a template before importing it into the database
/GenerateRollback	Creates a rollback template that can be used to restore the computer's security settings to the way they were before applying a configuration template

1.5.3 Enforcing Default Security Settings on New Computers

In Windows Server 2003, you can enforce security settings can be enforced on local computers, using the **Security Configuration and Analysis** snap-in or through Active Directory. Security templates can also be imported into the group policy of a domain, site, or OU in Active Directory, so that the settings can be applied to multiple computers. When a security template is imported into a GPO, any computers that have the GPO applied to them will automatically receive the configured settings. As mentioned earlier, **the Group Policy Object Editor** allows you to view and modify settings in a GPO. You can view and modify the group policies of domains, sites, and OUs using the Active Directory Sites and Services console to access the group policy configuration of a site, and the **Active Directory Users and Computers** console to access the group policy configuration of a domain and OU.

1.6 General Server Security Issues

1.6.1 Physical Security

Physical security addresses the need to protect servers from physical threats. Such threats may affect any number of assets in an organization and can result in widespread damage. These types of threats always involve some level of tangible risk. Taking steps to prevent physical interaction with equipment and implementing methods to ensure that equipment is safe from environmental threats will help promote physical security. A large part of physical security involves protecting systems from unauthorized physical access. Physical security controls access to hardware and software, so that people are unable to damage or steal devices and the data they may contain.

To prevent physical contact, all servers in an organization should be located in a secure area. In addition, all installation CDs and backup tapes used by the server should be physically secure.

1.6.2 Service Packs and Hotfixes

Practically all Windows operating systems have shipped with vulnerabilities or bugs that may be discovered after the software has been released. Once vulnerabilities or bugs have been discovered, manufacturers release **service packs**, which contain updates that may improve the reliability, security, and software compatibility of a program or operating system; or **patches** and **bug fixes**, which are used to repair errors in code or security issues. Failure to install the appropriate service packs, patches or bug fixes may cause certain features of the application or operating system to behave improperly or may leave your system open to attacks from hackers or viruses. In most cases, the service packs, patches, or bug fixes can be acquired from the manufacturer's Web site.

Vulnerabilities and Bugs

Vulnerabilities are unforeseen weaknesses in the programming code that can be exploited by hackers while bugs are defects that may cause the software to function incorrectly. In terms of security, vulnerabilities are a major concern as it may allow a hacker to gain access to your system.

Updates for Windows operating systems are made available on the **Windows Update** Web site (<http://windowsupdate.microsoft.com>). The Windows Update Web site determines what software is recommended to secure your system, and then allows you to download and install it from the site. Windows 2000, Windows XP, and Windows Server 2003 also provide an automated update and notification tool that allows critical updates to be downloaded and installed without user intervention. When enabled, this tool regularly checks Microsoft's Web site for updates, and if one or more are found, it downloads and installs the update. However, this tool requires an internet connecting to the Microsoft web site and can, thus, be used only if the servers or workstations have Internet access.

1.6.3 Antivirus Protection

Viruses, Trojan horses, and other malicious programs are a threat to any organization, especially if the organization is connected to the Internet. If these programs infect a network, data and systems can be damaged or destroyed. To prevent these malicious programs from causing problems, antivirus software should be installed on servers and workstations throughout the network.

When antivirus software is installed, it will scan for viruses and remove them using information stored in signature files. *Signature files* are used to identify viruses and let the software know how to remove them. Because new viruses appear every month, signature files need to be updated regularly by downloading them from the vendor's Web site.

1.6.4 Accounts and Services

Hackers and malicious programs can use insecure elements of a system to acquire access to the network and to cause damage. To keep these entities from exploiting elements of your system, you should disable any services that are not required. By disabling unnecessary services, you can reduce the possibility of attacks without affecting functionality.

Certain accounts in Windows Server 2003 should also be disabled or deleted. If an account is no longer being used, it should be removed to avoid a person or program using it to obtain unauthorized access. If an account will not be used temporarily, it should be disabled. In addition, certain built-in accounts should also be disabled. The **Administrator** account has full access to a system and is a well-known account. Windows Server 2003 and previous versions of Windows NT all have an account named **Administrator**. Because hackers already know the username of this account, they only need to obtain password to achieve this level of access. The **Administrator** account cannot be deleted, but it can be disabled or renamed. You can create

a new user account and add it to the **Administrators** group. Then you can disable the **Administrator** account. Attackers will then not be able to target that account.

Another Windows Server 2003 account that is disabled by default is the **Guest** account. This account is used to provide anonymous access to users who do not have their own account. Because there is the possibility that this account could accidentally be given improper levels of access and could be exploited, it should remain disabled.

1.6.5 Secure Passwords

Passwords are a key component of the default method of authentication for Windows Server 2003. They are used to prevent unauthorized access to computers and networks by forcing anyone who wants access to provide a password, which should be known only to the authorized user. Hackers often attempt to gain access to a computer or network by cracking the password for a known user account. Strong passwords are more difficult to crack than simple ones. These types of passwords use a combination of keyboard characters, including lowercase letters; uppercase letters; numerals; and special characters (` ~ ! @ # \$ % ^ & * () _ + - = { } | [] \ : " ; ' < > ? , . /).

The length of a password also affects how quickly it can be cracked because the more characters that are used, the greater the variations of letters, numbers, and special characters the password can contain. You can use security templates and group policies to control how long a password is valid, the length of a password, and other aspects of password management.

In addition, you should avoid using passwords that contain your username, real names, or company name, because these make passwords easier to guess. You should also avoid using passwords that contain actual words that appear in the dictionary, because hacking programs can be used to crack such passwords.

1.6.6 File Systems

Windows Server 2003 supports the FAT, FAT32, and NTFS file systems. Of these, NTFS provides the highest level of security. When using NTFS, you can set permissions on individual files and folders; control which accounts have access to file system resources; implement file encryption, which prevents unauthorized users from accessing files and folders; and implement disk quotas, which allows you to control how much hard disk space users may use.

Disk partitions can be formatted with NTFS when a server is initially installed. If a volume is formatted as FAT or FAT32, you can convert it to NTFS. You can convert partitions to NTFS by using the **convert** command-line utility without incurring data loss.