



MCSE Windows Server 2003 (Windows XP Professional)

To enrol on this course today,
go to www.intec24.com

Overview

Microsoft Certified Systems Engineer on Windows Server 2003 (Windows XP Professional) certification is designed to validate the knowledge and skills necessary to understand the functions and features of Windows XP Professional and to troubleshoot network-connectivity and applications issues.

Who should enrol?

Students interested in the MCSE on Windows Server 2003 (Windows XP Professional) should have at least one year of IT experience in medium to large computing environments, resolving network connectivity issues and working with desktop operating systems, security, and applications.

Jobs linked to this certification

- Systems engineer
- Network engineer
- Systems analyst
- Network analyst
- Technical consultant

What are my options?

To earn your MCSE on Windows Server 2003 certification (Windows XP Professional), you must pass seven exams:

- Four core exams on networking systems
- One core exam on client operating systems (in this case, Windows XP Professional)
- One core design exam
- One elective exam

For MCSE on Windows Server 2003 certification (Windows XP Professional), INTEC24 offers exam-preparation courses towards the following exams:

The four compulsory core exams on networking systems:

- Managing and Maintaining a Windows Server 2003 Environment Exam 70-290
- Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Exam 70-291
- Planning and Maintaining a Windows Server 2003 Network Infrastructure Exam 70-293
- Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory Infrastructure Exam 70-294

The core exams on client operating system:

- Installing, Configuring, and Administering Windows XP Professional Exam 70-270

The core design exams (choose 1):

- Designing a Windows Server 2003 Active Directory and Network Infrastructure Exam 70-297 (free practice exam)
- Designing Security for a Windows Server 2003 Network Exam 70-298 (free practice exam)

The elective exams (choose 1):

- Implementing and Administering Security in a Windows Server 2003 Network Exam 70-299 (2 free practice exams)
- Implementing and Managing Microsoft Exchange Server 2003 Exam 70-284 (2 free practice exams)

INTEC24 therefore offers you four MCSE on Windows Server 2003 (Windows XP Professional) options.

MCSE on Windows Server 2003 (Windows XP Professional) options

	Option 1	Option 2	Option 3	Option 4
Core networking system	70-290	70-290	70-290	70-290
	70-291	70-291	70-291	70-291
	70-293	70-293	70-293	70-293
	70-294	70-294	70-294	70-294
Core client operating system	70-270	70-270	70-270	70-270
Core design	70-297	70-297	70-298	70-298
Elective	70-299	70-284	70-299	70-284

Examinations and certification

When you pass your elected seven MCSE exams, you will be a *Microsoft Certified Systems Engineer*. For information about an authorized Microsoft test centre in your area, please go to <http://www.prometric.com/Microsoft/default.htm>.

Course price

This course costs R13 995, which means you save R3 470 on the full price.

Your course fees exclude your Microsoft exam fees. Your Microsoft exam fees vary, depending on the approved testing venue. For your convenience, exam vouchers are available from INTEC24.

You get 12 months' access to your online course material, with online support from your INTEC24 tutor. You will also get an INTEC24 Student Card, which will allow you the same discounts that other students get.

The four compulsory core exams on networking systems

Managing and Maintaining a Windows Server 2003 Environment MCSE Exam 70-290 Lessons

Lesson Title	Minimum time to work through lesson	Lesson Code
Overview of Windows Server 2003	4.0 hour(s)	w29001
Managing Physical and Logical Disks	6.0 hour(s)	w29002
Configuring, Monitoring, and Troubleshooting Server Hardware	4.0 hour(s)	w29003
Managing User, Group, and Computer Accounts	7.0 hour(s)	w29004
Managing Access to Resources	4.0 hour(s)	w29005
Configuring Terminal Services	4.0 hour(s)	w29006
Managing and Troubleshooting Terminal Services	3.0 hour(s)	w29007
Using Server Management Tools	4.0 hour(s)	w29008
Managing Web Servers with IIS 6.0	5.0 hour(s)	w29009
Monitoring Performance and Security	7.0 hour(s)	w29010
Planning Disaster Recovery	2.0 hour(s)	w29011
Implementing Disaster Recovery	4.0 hour(s)	w29012

Lesson 1: Overview of Windows Server 2003

Summary

This lesson introduces you to new features and capabilities available in Windows Server 2003. You learn how to license and activate Windows Server 2003, how to perform a new installation, and how to upgrade a server that uses an earlier Windows operating system.

Objectives

- Identify and describe new or enhanced features of Windows 2003 Server
- Choose the correct edition of Windows 2003 Server for your needs
- Manage licensing and activation of Windows 2003 Server
- Install Windows 2003 Server on a new computer
- Upgrade an existing server to Windows 2003 Server

Topics

- New Active Directory features
- New file and print services features
- Revised IIS architecture
- New clustering and load balancing features
- New networking and communications features
- New security features
- New storage management features
- New terminal services features
- New media services
- XML web services
- The Windows 2003 Server family
- Licensing Windows 2003 Server
- Activating Windows 2003 Server
- Installing Windows 2003 Server
- Upgrading to Windows 2003 Server

Lesson 2: Managing Physical and Logical Disks

Summary

This lesson explains how the operating system enables you to interface with the physical and logical disks in a computer. You learn how to optimize disk performance to increase the overall performance of a server using the Windows 2003 Server operating system.

Objectives

- Understand disk terminology and concepts
- Understand and manage physical and logical disks
- Optimize disk performance
- Understand and use remote storage
- Troubleshoot disks and volumes

Topics

- Understanding disk terminology and concepts
- Managing disks with the MMC
- Managing disks with command-line utilities
- Managing basic disks
- Managing dynamic disks
- Understanding disk fragmentation
- Using the disk defragmenter
- Understanding disk quotas
- Enabling and configuring disk quotas
- Implementing RAID Solutions
- Understanding remote storage
- Installing and configuring remote storage
- Administering remote storage
- Troubleshooting disks and volumes

Lesson 3: Configuring, Monitoring, and Troubleshooting Server Hardware

Summary

This lesson explains driver signing and how to configure driver-signing options. In addition, it explains how to use Device Manager, the Hardware Troubleshooting Wizard, Control Panel applets, and included command-line utilities to monitor server hardware.

Objectives

- Understand server hardware vulnerabilities
- Install and configure server hardware devices
- Monitor server hardware
- Troubleshoot hardware devices

Topics

- Understanding Server Hardware
- Understanding Device Drivers
- Configuring Driver Signing Options
- Understanding Windows File Protection
- Understanding the System File Checker
- Understanding File Signature Verification
- Using the New Hardware Wizard
- Using Device Manager
- Device Installation and Configuration Best Practices
- Monitoring Server Hardware
- Monitoring Server Hardware with Command-Line Utilities
- Using the Performance Console
- Hardware Monitoring Best Practices

- Troubleshooting Hardware Devices
- Diagnosing and Resolving Startup Issues
- Hardware Troubleshooting Best Practices

Lesson 4: Managing User, Group, and Computer Accounts

Summary

This lesson explains how Windows Server 2003 treats users, groups, and computers in the Active Directory environment. You will learn how to use common management tools, including Active Directory Users and Computers (ADUC) and other useful utilities. This lesson shows you how to create and modify user, group, and computer accounts with ADUC. Finally, you will learn about command-utilities that can be used to automate account creation and import user accounts.

Objectives

- Understand security objects
- Use management tools
- Create and manage user accounts
- Create and manage group accounts
- Create and manage computer accounts

Topics

- Understanding Security Objects
- Understanding Management Tools
- Understanding Command-Line Management Tools
- Managing User Accounts
- Managing User Accounts with Command-Line Utilities
- Troubleshooting User Accounts
- Understanding Group Accounts
- Creating Group Accounts
- Managing Group Accounts with Command-Line Utilities
- Managing Group Accounts
- Group Membership Management Best Practices
- Creating and Managing Computer Accounts
- Managing Computer Accounts with Command-Line Utilities
- Creating a Replica Domain Controller
- Creating a Domain Controller for a New Forest
- Creating a Domain Controller for a New Child Domain
- Creating a Domain Controller for a New Domain Tree
- Assigning Domain Controller Operations Master Roles
- Troubleshooting Computer Accounts

Lesson 5: Managing Access to Resources

Summary

This lesson explains how to manage access to files and folders, printers, computers, and other resources on the network. You will learn about different types of permissions and user rights that can be configured, how permissions are inherited, and how command-line utilities can be used to manage access control. This lesson also explains how to troubleshoot common access problems, how to use the Encrypting File System to encrypt files and folders, and how to implement a PKI using Windows Server 2003's Certificate Services.

Objectives

- Understand access control
- Understand and use access permissions
- Set user rights and privileges
- Troubleshoot access problems

- Use new command-line utilities to manage access control
- Use EFS encryption
- Implement a Public Key Infrastructure

Topics

- Understanding Access Control
- Assigning NTFS Permissions
- Denying NTFS Permissions
- Using NTFS Special Permissions
- Copying or Moving Files and Folders
- Using Shared-Folder Permissions
- Understanding the Interaction of Share Permissions and NTFS Permissions
- Using Shared Folders in Active Directory
- Understanding Permission Inheritance
- Understanding User Rights
- Using Group Policy to Set User Rights
- Troubleshooting Access Problems
- Managing Access with Command-Line Utilities
- Understanding Disk Encryption
- Understanding EFS Architecture
- Encrypting Files and Folders
- EFS Best Practices
- Understanding Public Key Infrastructure
- Installing and Using Windows Server 2003 Certificate Services

Lesson 6: Configuring Terminal Services

Summary

This lesson provides an overview of the benefits of using Windows Server 2003 Terminal Services. You learn how to select the Terminal Services functionality that best fits your needs. This lesson discusses installation and configuration of the terminal server role, the Terminal Services client software, and licensing issues.

Objectives

- Understand Windows Terminal Services
- Use Terminal Services components for remote administration
- Install and configure the terminal server role

Topics

- Understanding Windows Terminal Services
- Understanding Terminal Services Components
- Configuring Remote Desktop for Administration
- Planning Remote Desktop Security
- Understanding Remote Assistance
- Configuring Remote Assistance
- Configuring Windows Messenger
- Planning Remote Assistance Security
- Installing and Configuring the Terminal Server Role
- Installing Terminal Server Licensing
- Installing the Remote Desktop Connection Utility
- Configuring the Remote Desktop Connection Utility
- Installing the Remote Desktops MMC Snap-In
- Installing the Remote Desktop Web Connection Utility

Lesson 7: Managing and Troubleshooting Terminal Services

Summary

This lesson shows you how to use Terminal Services administrative tools, including the Terminal Services Manager and Terminal Services Configuration console tools. This lesson also covers the Remote Desktop MMC snap-in, using group policies to control Terminal Services learners and clients, Terminal Services extensions to the properties of user accounts and the Terminal Services command-line tools. Finally, you learn how to troubleshoot problems with Terminal Services.

Objectives

- Use Terminal Services client tools
- Use Terminal Services administrative tools
- Troubleshoot Terminal Services

Topics

- Using Remote Assistance as a Novice
- Using Remote Assistance as an Expert
- Completing a Remote Assistance Connection
- Managing Remote Assistance Invitations
- Using the Remote Desktop Connection Utility
- Using the Terminal Services Manager
- Using the Terminal Services Configuration Tool
- Managing Terminal Services Server Settings
- Managing Terminal Services Sessions at the User Level
- Controlling Terminal Services with Group Policy
- Using Terminal-Services Command-Line Tools
- Troubleshooting Terminal-Services

Lesson 8: Using Server Management Tools

Summary

This lesson introduces you to many of the graphical management consoles and command-line administrative utilities that are included in Windows Server 2003. You learn how to use these tools to manage servers and networks.

Objectives

- Recognize types of management tools
- Manage your server remotely
- Use Emergency Management Services
- Manage printers and print queues
- Manage and troubleshooting services
- Use wizards to configure and manage your server

Topics

- Understanding Management Tools
- Understanding Remote Assistance and Administration
- Using Computer Management to Manage a Remote Computer
- Using Emergency Management Services
- Configuring Printers
- Managing Printers and Print Queues
- Managing Printers with Command-Line Tools
- Configuring Services
- Managing Services
- Managing Services with Command-Line Tools
- Using Server Management Wizards

Lesson 9: Managing Web Servers with IIS 6.0

Summary

This lesson explains the installation and configuration process for IIS 6.0 and introduces you to its new features. You are shown how to use the Web Server Security Lockdown Wizard and how to manage security issues for Web servers. This lesson also covers troubleshooting issues and the new IIS command-line utilities.

Objectives

- Install and configure IIS 6.0
- Find out what's new in IIS 6.0
- Manage IIS 6.0
- Troubleshoot IIS 6.0
- Use new IIS command-line utilities

Topics

- Preparing to Install IIS 6.0
- Installing and Configuring IIS 6.0
- New Features of IIS 6.0
- Setting Up Web Sites with IIS Manager
- Administering Web Sites with IIS 6.0
- Managing IIS 6.0 Security
- Troubleshooting IIS 6.0
- Creating and Managing Web Sites with Command-Line Utilities
- Creating Virtual Directories with Command-Line Utilities
- Administering FTP Sites with Command-Line Utilities
- Creating Virtual Directories for FTP Sites with Command-Line Utilities
- Creating IIS Backups with Command-Line Utilities
- Managing IIS 6.0 Configuration Settings with Command-Line Utilities

Lesson 10: Monitoring Performance and Security

Summary

This lesson shows you how to use monitoring tools such as Task Manager, System Monitor, and command-line utilities to monitor server performance and security. You will learn how to use the information in the security log to track successful or failed breaches of security. Finally, you will learn how to optimize the performance of common server applications.

Objectives

- Monitor performance
- Optimize servers for application performance
- Audit security events
- Use Event Viewer
- Use command line tools
- Use the shutdown event tracker

Topics

- Using Task Manager
- Using System Monitor
- Using Performance Logs and Alerts
- Using Command-Line Tools
- Monitoring Memory Objects
- Monitoring Network Objects
- Monitoring Process Objects
- Monitoring Disk Objects
- Auditing Security Events
- Enabling Object Auditing

- Working with Audit Policy Settings
- Using Event Viewer
- Managing Event Logs
- Troubleshooting Event Logs
- Managing Events with Command-Line Tools
- Monitoring Shutdown Events
- Tracking Shutdown Events

Lesson 11: Planning Disaster Recovery

Summary

This lesson explains how to create a comprehensive disaster recovery plan for an organization's network and servers.

Objectives

- Create a backup plan
- Create a system recovery plan

Topics

- Understanding Disaster Recovery
- Developing a Business Continuity Plan
- Assessing Threats
- Evaluating Assets
- Creating an Incident Response Team
- Using Disaster Recovery Best Practices
- Creating a Backup Plan
- Understanding Backup Concepts
- Choosing Backup Media
- Managing Backup Media

Lesson 12: Implementing Disaster Recovery

Summary

This lesson shows you how to use the backup and recovery tools included with the Windows Server 2003 operating system.

Objectives

- Implement a backup plan
- Implement a system recovery plan
- Work with volume shadow copies
- Recover server hardware failure

Topics

- Using Emergency Management Services
- Backing Up Data Files
- Setting Backup Options
- Backing Up System State Options
- Configuring Security for Backup Operations
- Delegating Authority to Perform Backups via Group Policy
- Verifying Successful Completion of Backup Jobs
- Managing Backup Media
- Restoring Data from a Backup
- Scheduling Backup Jobs
- Performing Backups with Command-Line Utilities
- Creating a System Recovery Plan
- Restoring Active Directory
- Creating an Automated System Recovery Set

- Installing and Using the Recovery Console
- Using Windows Startup Options
- Creating Volume Shadow Copies
- Restoring Data from within Volume Shadow Copies
- Recovering from Server Hardware Failure

Technical features of this course

- Show Me Hows allow you to access instructional demonstrations from all courses in the series.
- Simulations teach you to perform specific tasks in applications through guided, multi-step exercises.
- Activities allow you to apply course concepts in an interactive questioning environment.
- Exercises allow you to practice in the actual application being studied.
- A Course Topics list contains active hyperlinks, permitting quick access to specific topics.
- Find-A-Word allows you to look up an unfamiliar term in the Glossary, on the Web, or in a dictionary. In addition, it lets you find other occurrences of the term in the same course.
- Search text enables you to rapidly search all text within a course to easily retrieve information required.
- Courses challenge you with a variety of question formats, including multi-step simulations, true/false, multiple choice, and fill-in-the-blank.
- A skill assessment generates a customized learning path based on the results of a pre-test.
- A glossary provides a reference for definitions of unfamiliar terms.
- Bookmarking tracks your progress in a course.

Technical requirements

P500+ Processor, 128MB of RAM; Windows 2000, 2003, XP, Vista, Minimum screen resolution 800x600, Internet Explorer 5.5 or higher; Windows Media Player 9.0 or higher; Flash 8.0 or higher; 56K minimum connection; broadband (256 kbps or higher) connection recommended; Javascript, DHTML and cookies enabled; Sound card with speakers or headphones strongly recommended.

Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure MCSE Exam 70-291

Lesson Title	Minimum time to work through lesson	Lesson Code
TCP/IP Protocol	3.0 hour(s)	w29101
IP Addressing and Routing	3.0 hour(s)	w29102
Classless Subnet Masking and Client Address Configuration	3.0 hour(s)	w29103
The Dynamic Host Configuration Protocol (DHCP)	5.0 hour(s)	w29104
Integrating and Troubleshooting DHCP	4.0 hour(s)	w29105
Windows Internet Name Server (WINS)	4.0 hour(s)	w29106
WINS Client and Interoperability and NetBIOS	4.0 hour(s)	w29107
Domain Naming System Concepts	5.0 hour(s)	w29108
The DNS Server	5.0 hour(s)	w29109
Routing and Remote Access Service VPN Services	5.0 hour(s)	w29110
Security Templates and Software Updates	3.0 hour(s)	w29111
Monitoring and Troubleshooting Network Activity	3.0 hour(s)	w29112
LAN Routing and Dial-Up Services	3.0 hour(s)	w29113
LAN and Dial-Up Security	4.0 hour(s)	w29114

Lesson 1: TCP/IP Protocol

Summary

This lesson provides an overview of the OSI, Microsoft, and TCP/IP Networking Models, as well as major application layer protocols.

Objectives

- Understand the purpose and function of networking models
- Identify the seven layers of the OSI networking model
- Identify the Microsoft networking model
- Identify the four layers of the TCP/IP protocol suite
- Identify several application layer protocols of the TCP/IP protocol suite

Topics

- OSI networking model: physical and data link layers
- Network and transport layers
- Session, presentation, and application layers
- Microsoft networking model
- Protocol suite network interface layer
- Protocol suite internet layer
- Protocol suite host-to-host transport layer
- Protocol suite application layer

Lesson 2: IP Addressing and Routing

Summary

This lesson provides an overview of IP addressing and routing, including binary conversion, network classes, subnetting, and name resolution.

Objectives

- Convert IP addresses to binary and to decimal
- Identify the network and host ID portions of an IP address based on address class
- Explain subnetting and subnet masking
- Perform bitwise ANDing
- Distinguish between static and dynamic routing table updates
- Explain the use of four commonly used routing utilities

Topics

- IP addresses and binary conversions
- Network ID and host ID
- Classes
- Subnetting and subnet masking
- Custom subnet masks
- Public and private IP addresses
- IP routing name resolution
- IP routing tables
- ARP
- Static and dynamic IP routers
- Routing utilities and example network

Lesson 3: Classless Subnet Masking and Client Address Configuration

Summary

This lesson provides an overview of subnetting, supernetting, the XP/2000 routing table, assigning IP addresses, and APIPA.

Objectives

- Subnet Class A, B, and C networks
- Supernet a Class C network
- Make changes to the routing table
- Configure a static IP address
- Use alternate IP addressing configurations

Topics

- Classless subnet masking
- Subnetting Class B networks
- Subnetting Class C networks
- Example classless subnetting
- Supernetting a Class C network
- The Windows XP/2000 routing table
- Windows XP/2000 routing table entries
- The Windows 2003 routing table
- Disabling automatic metric calculation
- Adding and removing routing table entries
- Assigning static IP addresses
- Assigning dynamic IP addresses and APIPA

Lesson 4: The Dynamic Host Configuration Protocol (DHCP)

Summary

This lesson provides an overview of DHCP leases, as well as installing and configuring DHCP service.

Objectives

- Explain the DHCP lease process
- Install DHCP service
- Create and configure different type of DHCP scopes
- List DHCP option types
- Create DHCP/BOOTP reservations
- Allocate IP addresses appropriately

Topics

- DHCP leases
- The DHCP lease process
- Lease renewal
- Installing the DHCP service
- Configuring scopes
- Configuring server and scope options
- Configuring user and vendor class options
- Configuring reservations and BOOTP tables
- Superscopes
- Multicast scopes
- IP address allocation

Lesson 5: Integrating and Troubleshooting DHCP

Summary

This lesson provides an overview of configuring the DHCP Relay Agent, Dynamic DNS, Routing and Remote Access, and Active Directory. It also covers automatic addressing, as well as managing and monitoring DHCP.

Objectives

- Configure the DHCP Relay Agent
- Use DNS upgrading options
- Configure your RRAS server to use DHCP
- Integrate DHCP with Active Directory
- Disable APIPA
- Back up and restore a DHCP database

Topics

- Configuring the DHCP relay agent
- DHCP server and Dynamic DNS
- DHCP and Routing and Remote Access
- DHCP and Active Directory
- Automatic private IP addressing
- Managing the DHCP server database
- Server statistics and administration
- Monitoring DHCP
- Data sniffing and audit log
- Log files and client-side troubleshooting

Lesson 6: Windows Internet Name Server (WINS)

Summary

This lesson provides an overview of WINS, including installation, push and pull replication, records management, and database administration.

Objectives

- Install and configure WINS
- Manage WINS records and its database
- Configure WINS replication
- Reconcile WINS records
- Backup and restore the WINS database

Topics

- Overview of WINS
- Installing the WINS server
- Creating replication partners
- Configuring pull replication
- Configuring push replication
- Managing WINS records
- Creating static records
- State and expiration fields
- Record reconciliation and integrity
- Database consistency
- Database size and advanced options
- WINS database backup
- Ntbackup and database restores

Lesson 7: WINS Client and Interoperability and NetBIOS

Summary

This lesson provides an overview of configuring WINS clients, troubleshooting WINS clients and servers, and NetBIOS name resolution, registration, and node types.

Objectives

- Configure network clients to support WINS either directly or through a WINS proxy agent
- Describe how WINS interoperates with DNS and DHCP

- Configure WINS with RRAS
- Describe the WINS browser list
- Describe the NetBIOS name registration and resolution processes
- Define NetBIOS concepts such as node types and LMHOSTS file

Topics

- Configuring the WINS client
- WINS and DHCP
- WINS and DNS
- WINS and RRAS or Active Directory
- WINS and Browser service or Win9x/NT clients
- WINS System Monitor Objects
- Troubleshooting WINS Clients
- Troubleshooting WINS servers
- NetBIOS name resolution
- Name registration and resolution
- NetBIOS terminology
- NetBIOS node types
- The LMHOSTS file

Lesson 8: Domain Naming System Concepts

Summary

This lesson provides an overview of DNS conventions, resolution, namespace, concepts, resource records, zones, and Active Directory service integration.

Objectives

- Explain the function of DNS
- Describe the DNS namespace
- Create DNS zones and records
- Outline DNS server roles
- Manage record aging and scavenging
- Integrate Active Directory and DNS

Topics

- DNS overview
- Name conventions and resolution
- The DNS namespace
- Basic DNS concepts
- Zones and records
- Adding records and zone transfers
- Host name resolution
- Server roles and testing
- Adding zones
- Dynamic DNS servers
- Stale records and extensions
- AD integrated DNS zones

Lesson 9: The DNS Server

Summary

This lesson provides an overview of installing, configuring, monitoring, and troubleshooting a DNS server.

Objectives

- Install DNS on a server
- Configure forward and reverse lookup zones

- Configure and manage DNS
- Monitor and troubleshoot DNS

Topics

- Installing the configuring the DNS server
- Configuring forward lookup zones
- Adding DNS database records
- Configuring reverse lookup zones
- Configuring your DNS server
- Configuring your DNS zones
- Configuring DNS clients
- Resolving DNS queries
- Integrating the DNS server with DHCP
- DNSUpdateProxy group security
- WINS and DNS
- Integrating the DNS server with BIND
- Monitoring the server with DNS console
- Monitoring the server with System Monitor
- Monitoring the server with Network Monitor
- Troubleshooting the DNS server

Lesson 10: Routing and Remote Access Service VPN Services

Summary

This lesson provides an overview of enabling remote access, configuring a VPN server, authenticating VPN clients, creating dial-up connections and gateways, and troubleshooting VPN.

Objectives

- Enable remote access on a VPN server
- Identify available authentication protocols
- Describe the process of tunneling
- Configure a VPN server for remote access
- Configure a VPN client for remote access
- Create a VPN Gateway

Topics

- Remote access concepts
- Enabling remote access
- VPN server network structure
- VPN server infrastructure
- PPP authentication process, PAP and SPAP
- Authentication protocols CHAP, MS-CHAP, and EAP
- VPN tunneling protocols
- Configuring the VPN server
- Configuring the VPN server for remote access
- Configuring the VPN remote access clients
- VPN gateway infrastructure
- Demand-dial connections and IP addressing support
- Creating gateways and static packet filters
- VPN gateway configuration
- Troubleshooting VPN services

Lesson 11: Security Templates and Software Updates

Summary

This lesson provides an overview of network security settings, analyzing security, applying security templates, and installing software updates.

Objectives

- Implement secure network administration procedures
- Implement security baseline settings and audit security settings using security templates
- Install and configure the Software Update Service
- Install and configure Automatic Client Update Settings
- Support Legacy clients
- Install and configure WINS redundancy

Topics

- Security templates
- Network security settings
- Analyzing baseline security
- Applying baseline security
- Installing security templates
- Installing software updates
- Installing automatic client update settings
- Configuring automatic client update settings
- Legacy clients and testing

Lesson 12: Monitoring and Troubleshooting Network Activity

Summary

This lesson provides an overview of installing and configuring Network Monitor, including trace interpretation, NAT logging, troubleshooting name resolution and client configuration, quarantine control, DHCP issues, and monitoring IPsec connection.

Objectives

- Install and configure Network Monitor
- Use Network Monitor to troubleshoot network problems
- Identify network problems relating to Network Address Translation, name resolution, IP addressing, and IP security
- Troubleshoot IPsec connections using the IPsec Security Monitor

Topics

- Installing network monitor
- Configuring network monitor
- Interpreting a trace
- NAT logging
- Troubleshooting name resolution
- IP addressing client configuration issues
- Quarantine control and DHCP issues
- Monitoring IPsec connections

Lesson 13: LAN Routing and Dial-Up Services

Summary

This lesson provides an overview of configuring LAN routing, RAS, PPP Multilink, BAP, and wireless connections.

Objectives

- Configure LAN routing
- Configure RRAS packet filters

- Configure a Windows Server 2003 Routing and Remote Access Service
- Configure a Routing and Remote RAS dial-up Gateway
- Configure wireless networking

Topics

- Configuring LAN routing
- Setting up LAN routing
- Configuring RRAS packet filters
- Configuring dial-up RRAS server
- Configuring dial-up RRAS gateway
- PPP multilink and bandwidth allocation protocol
- Configuring multilink with BAP
- Configuring wireless connections
- Wireless networking policies
- Configuring wireless networking

Lesson 14: LAN and Dial-Up Security

Summary

This lesson provides an overview of remote access policies, router protocols, RIP, OSPF, IGMP, firewall support, NAT, ICMP, remote access client and server connections, and IAS.

Objectives

- Configure remote access policies
- Identify and describe the router protocols supported by Windows Server 2003
- Enable and configure basic firewall support
- Enable and configure Network Address Translation (NAT) services
- Describe and configure ICMP router discovery
- Troubleshoot remote access client and server connections
- Configure Internet Authentication Services

Topics

- Remote access policies
- Configuring remote access policies
- Understanding router protocols
- RIP
- OSPF and IGMP
- Configuring basic firewall support
- RRAS NAT services
- ICMP router discovery
- Troubleshooting remote access client connections
- Troubleshooting remote access server connections
- Internet Authentication Services
- Configuring IAS

Technical features of this course

- Show Me Hows allow you to access instructional demonstrations from all courses in the series.
- Simulations teach you to perform specific tasks in applications through guided, multi-step exercises.
- Activities allow you to apply course concepts in an interactive questioning environment.
- Exercises allow you to practice in the actual application being studied.
- A Course Topics list contains active hyperlinks, permitting quick access to specific topics.
- Find-A-Word allows you to look up an unfamiliar term in the Glossary, on the Web, or in a dictionary. In addition, it lets you find other occurrences of the term in the same course.
- Search text enables you to rapidly search all text within a course to easily retrieve information required.

- Courses challenge you with a variety of question formats, including multi-step simulations, true/false, multiple choice, and fill-in-the-blank.
- A skill assessment generates a customized learning path based on the results of a pre-test.
- A glossary provides a reference for definitions of unfamiliar terms.
- Bookmarking tracks your progress in a course.

Technical requirements

P500+ Processor, 128MB of RAM; Windows 2000, 2003, XP, Vista, Minimum screen resolution 800x600, Internet Explorer 5.5 or higher; Windows Media Player 9.0 or higher; Flash 8.0 or higher; 56K minimum connection; broadband (256 kbps or higher) connection recommended; Javascript, DHTML and cookies enabled; Sound card with speakers or headphones strongly recommended.

Planning and Maintaining a Windows Server 2003 Network Infrastructure MCSE Exam 70-293

Lesson Title	Minimum time to work through lesson	Lesson Code
Using Planning Tools and Documentation	2.0 hour(s)	w29301
Server Roles and Security	6.0 hour(s)	w29302
TCP/IP Infrastructure	5.0 hour(s)	w29303
Routing	5.0 hour(s)	w29304
Internet Connectivity	4.0 hour(s)	w29305
DNS Name Resolution	6.0 hour(s)	w29306
NetBIOS Name Resolution	3.0 hour(s)	w29307
Remote Access	4.0 hour(s)	w29308
High Availability	3.0 hour(s)	w29309
Windows Cluster Services and Network Load Balancing	3.0 hour(s)	w29310
Internet Protocol	3.0 hour(s)	w29311
Security Framework	4.0 hour(s)	w29312
Public Key Infrastructure	3.0 hour(s)	w29313

Lesson 1: Using Planning Tools and Documentation

Summary

This lesson shows you how to plan an infrastructure for a Windows Server 2003-based network.

Objectives

- Identify the fundamentals of network design
- Analyze organizational needs
- Explain legal and regulatory considerations
- Develop, build and implement a test network

Topics

- Network infrastructure planning
- Generating a group policy modeling report
- Analyzing organizational needs
- Communication and collaboration
- User services
- Legal considerations and TCO
- Developing a test network environment
- Building a test lab
- Implementing the test network
- Documenting the test process

Lesson 2: Server Roles and Security

Summary

This lesson provides information on server roles and planning server security.

Objectives

- Describe and configure server roles
- Describe operating system security features and functional levels
- Identify minimum security requirements for your organization
- Use security templates and tools
- Enforce default security settings
- Create custom security templates and deploy security configurations

Topics

- Understanding server roles
- Domain controllers
- File, print, and name servers
- Web, database, and mail servers
- Certificate Authorities
- Application and terminal servers
- Operating system security features
- Operating system functional levels
- Identifying minimum security requirements
- Security templates and tools
- Planning baseline installation parameters
- Enforcing default security settings
- Security issues for all servers
- Securing specific servers
- Creating custom security templates
- Deploying security configurations

Lesson 3: TCP/IP Infrastructure

Summary

This lesson gives an in-depth look at the protocols you can use with Windows Server 2003, especially the TCP/IP protocol suite. It shows how to subnet networks and how to use the utilities and tools included with Windows Server 2003.

Objectives

- List the protocols supported by Windows Server 2003
- Describe the OSI reference model and TCP/IP networking model
- Design an effective subnetting scheme
- Install IPv6 and use IPv6 utilities
- Use Network Monitor and System Monitor to track network performance

Topics

- Network protocols
- Configuring TCP/IP manually
- TCP/IP basics
- New TCP/IP features
- Creating a subnetting scheme
- Understanding ANDing and binary numbering
- Subnetting networks
- Troubleshooting IP addressing
- Transitioning to IPv6
- IPv6 utilities

- Planning the network topology
- Planning network traffic management

Lesson 4: Routing

Summary

This lesson provides information on planning and implementing routing on a Windows Server 2003 network.

Objectives

- Explain the basics of IP routing
- Use the Netsh utility
- Configure a Windows Server 2003 machine as a router
- Troubleshoot routing issues

Topics

- Routing basics
- Routing tables
- Static and dynamic routing and gateways
- Routing protocols
- Netsh commands
- Routing devices
- Switches and routers
- Configuring Windows Server as a router
- Configuring RIP and OSPF
- Security
- Router-to-router VPNs
- Packet filtering, firewalls and logging
- Troubleshooting IP routing

Lesson 5: Internet Connectivity

Summary

This lesson provides information that will help you develop the best strategy for connecting your company's Windows Server 2003 network to the Internet.

Objectives

- Decide between routed or translated connections
- Install NAT
- Configure VPN access
- Install and configure IAS and RADIUS
- Create service profiles using CMAK

Topics

- Connecting to the Internet
- Internet Connection Sharing
- Internet-based VPNs
- Router-to-router VPNs
- VPN protocols and security
- Internet Authentication Service (IAS)
- Activating and managing IAS
- PPP-based protocols and EAP
- Authorization methods
- Installing the CMAK
- Using the CMAK
- Connection Manager profiles and security issues

Lesson 6: DNS Name Resolution

Summary

This lesson provides information that will help you plan, develop, secure, and maintain a host name resolution strategy with the Domain Name System (DNS).

Objectives

- Plan a DNS namespace design
- Plan zone replication requirements
- Plan a forwarding configuration
- Consider the interoperability of DNS with other DNS solutions
- Plan for DNS security
- Troubleshoot host name resolution

Topics

- Host naming
- DNS
- Lookup zones
- DNS namespace
- DNS and Active Directory
- Multiple namespaces
- Planning DNS server deployment
- DNS server roles
- Zone replication and forwarding
- DNS/DHCP interaction
- DNS and BIND
- Split DNS configurations
- DNS and WINS
- DNS security
- Monitoring DNS servers
- Troubleshooting host name resolution

Lesson 7: NetBIOS Name Resolution

Summary

This lesson provides information on planning, implementing and maintaining NetBIOS name resolution on a Windows Server 2003 network.

Objectives

- Describe the NetBIOS name resolution process
- Describe the WINS name resolution process
- Deploy and replicate WINS servers
- Configure WINS clients
- Plan for WINS database backup and restoration
- Troubleshoot NetBIOS name resolution

Topics

- NetBIOS naming
- WINS
- WINS server deployment
- WINS replication
- Replication models
- WINS issues
- WINS client configuration
- WINS server performance issues
- Security issues

- WINS database backup and restoration
- Troubleshooting NetBIOS name resolution

Lesson 8: Remote Access

Summary

This lesson provides an overview of the issues and procedures involved in devising a remote access strategy.

Objectives

- Implement secure access between private networks.
- Plan security
- Plan Remote Access policies
- Analyze protocol security requirements.
- Plan authentication methods for remote access clients

Topics

- Planning a Remote Access strategy
- Enabling Remote Access
- VPN design considerations
- Wireless Remote Access Design considerations
- Domain Functional Level
- Selecting authentication methods
- Authorizing Remote Access by user
- Restricting Remote Access
- Controlling remote connections
- Configuring Remote Assistance
- Requesting Remote Assistance
- Establishing a Remote Assistance connection
- Offering Remote Assistance
- Planning for Remote Administration

Lesson 9: High Availability

Summary

This lesson provides guidelines that can help you ensure that network resources are available when users need them.

Objectives

- Plan services for high availability
- Identify bottlenecks in memory, processor, disk, and network
- Plan a backup and recovery strategy
- Plan for fault tolerance

Topics

- Memory and processor bottlenecks
- Disk and network bottlenecks
- Using the System Monitor tool
- Using Event Viewer
- Planning a backup strategy
- Determining what to back up
- Using backup tools
- Scheduling backups
- Planning system recovery with ASR
- Planning for fault tolerance

Lesson 10: Windows Cluster Services and Network Load Balancing

Summary

This lesson provides information on how to use two powerful tools to enhance fault tolerance and high availability: server clustering and Network Load Balancing.

Objectives

- Differentiate between the server cluster models
- Create a new server cluster
- Differentiate between server clusters and network load balancing clusters
- Use the NLB Manager or NLB.exe utility to monitor the NLB cluster
- Create a network load balancing cluster

Topics

- Server clustering
- Server cluster deployment options
- Server cluster administration
- Server clustering best practices
- Cluster network configuration
- Creating a new cluster
- Network load balancing (NLB)
- Managing NLB clusters
- NLB monitoring and best practices
- Creating a NLB cluster

Lesson 11: Internet Protocol

Summary

This lesson provides guidelines for setting up IPSec on your Windows Server 2003 network.

Objectives

- Identify the purpose and goals of IPSec
- Identify the protocols used with IPSec
- Deploy IPSec on your network
- Manage IPSec

Topics

- IP Security (IPSec)
- IPSec protocols
- IPSec components
- Deploying IPSec
- Managing IPSec
- IPSec policies
- IP Security Policy Wizard
- Modifying IPSec policies
- Applying policies
- Monitoring and troubleshooting IPSec
- Using Event Viewer and packet event logging
- Using IKE detailed tracing and Network Monitor
- Disabling hardware offload functions
- IPSec security considerations
- Using RSoP

Lesson 12: Security Framework

Summary

This lesson provides information on planning, implementing, and maintaining a security framework on a Windows Server 2003 network.

Objectives

- Implement Active Directory security
- Implement wireless security
- Monitor and optimize security
- Plan a security update infrastructure

Topics

- Active Directory security
- Permission types
- Security relationships
- Account security
- Implementing wireless security
- Wireless authentication
- Authentication protocols
- Wireless security issues
- Wireless monitor and object-based access control
- Setting auditing
- Auditing objects
- Security policies
- Security update infrastructure
- Microsoft Software Update Services (SUS)

Lesson 13: Public Key Infrastructure

Summary

This lesson provides information on planning, implementing and maintaining a Public Key Infrastructure on a Windows Server 2003 network.

Objectives

- Explain the basics of a Public Key Infrastructure
- Install and configure a Certification Authority
- Plan the enrollment and distribution of certificates
- Plan a Certification Authority hierarchy
- Implement the use of smart card authentication

Topics

- Public Key Infrastructure (PKI) basics
- Certification authorities
- Configuring a certification authority
- Analyzing certificate needs
- Certificate templates
- Certificate requests
- Smart card authentication
- Implementing and using smart cards
- Using smart cards for remote access VPNs

Technical features of this course

- Show Me Hows allow you to access instructional demonstrations from all courses in the series.
- Simulations teach you to perform specific tasks in applications through guided, multi-step exercises.

- Activities allow you to apply course concepts in an interactive questioning environment.
- Exercises allow you to practice in the actual application being studied.
- A Course Topics list contains active hyperlinks, permitting quick access to specific topics.
- Find-A-Word allows you to look up an unfamiliar term in the Glossary, on the Web, or in a dictionary. In addition, it lets you find other occurrences of the term in the same course.
- Search text enables you to rapidly search all text within a course to easily retrieve information required.
- Courses challenge you with a variety of question formats, including multi-step simulations, true/false, multiple choice, and fill-in-the-blank.
- A skill assessment generates a customized learning path based on the results of a pre-test.
- A glossary provides a reference for definitions of unfamiliar terms.
- Bookmarking tracks your progress in a course.

Technical requirements

P500+ Processor, 128MB of RAM; Windows 2000, 2003, XP, Vista, Minimum screen resolution 800x600, Internet Explorer 5.5 or higher; Windows Media Player 9.0 or higher; Flash 8.0 or higher; 56K minimum connection; broadband (256 kbps or higher) connection recommended; Javascript, DHTML and cookies enabled; Sound card with speakers or headphones strongly recommended.

Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory Infrastructure MCSE Exam 70-294

Lesson Title	Minimum time to work through lesson	Lesson Code
Active Directory Infrastructure Overview	4.0 hour(s)	w29401
Working with User, Group, and Computer Accounts	5.0 hour(s)	w29402
Creating User and Group Strategies	3.0 hour(s)	w29403
Working with Forests and Domains	5.0 hour(s)	w29404
Restructuring a Forest and Renaming Domains	3.0 hour(s)	w29405
Working with Trusts and Organizational Units	2.0 hour(s)	w29406
Working with Active Directory Sites	3.0 hour(s)	w29407
Working with Domain Controllers	2.0 hour(s)	w29408
Working with Global Catalog Servers and Schema	2.0 hour(s)	w29409
Working with Group Policy	3.0 hour(s)	w29410
Deploying Software via Group Policy	2.0 hour(s)	w29411
Ensuring Active Directory Availability	3.0 hour(s)	w29412

Lesson 1: Active Directory Infrastructure Overview

Summary

This lesson provides an overview of the Active Directory infrastructure along with basic terms and concepts.

Objectives

- Identify and describe basic Active Directory terms, concepts, and components
- Install Active Directory to create a domain controller
- Use graphical and command-line administrative tools
- Set permissions on Active Directory objects

Topics

- Active Directory basic concepts
- Naming schemes
- Installing Active Directory
- Logical components

- Physical components
- Organizational components
- Using administrative tools
- MMC snap-ins
- Command-line tools
- More command-line tools
- Access control
- Authentication
- New features

Lesson 2: Working with User, Group, and Computer Accounts

Summary

This lesson provides an introduction to the concept of security principles and Security Identifiers (SIDs). It also discusses how to work with Active Directory user accounts, group accounts, and computer accounts.

Objectives

- Understand Active Directory security principal accounts
- Work with Active Directory user accounts
- Work with Active Directory group accounts
- Work with Active Directory computer accounts
- Manage multiple accounts

Topics

- Security principal accounts
- Naming conventions and limitations
- Working with user accounts
- Creating user accounts
- Managing user accounts
- Working with group accounts
- Built-in group accounts
- Creating group accounts
- Managing group accounts
- Working with computer accounts
- Managing computer accounts
- Managing multiple accounts
- Moving account objects
- Troubleshooting account problems

Lesson 3: Creating User and Group Strategies

Summary

This lesson provides information about planning effective strategies for managing users and groups in Active Directory. The lesson addresses the creation of user authentication strategies, authentication concepts, and how to plan a smart card authentication strategy. Throughout the lesson, new smart card authentication features for Windows Server 2003 are highlighted.

Objectives

- Create a password policy for domain users
- Plan a user authentication strategy
- Plan a smart card authentication strategy
- Plan a security group strategy

Topics

- Planning a password policy
- Defining a password policy

- Authentication strategies
- Authentication types
- Planning for smart cards
- Preparing enrollment stations
- Enrolling users
- Understanding groups
- Security strategies for groups

Lesson 4: Working with Forests and Domains

Summary

This lesson provides an overview of forests and domains. The lesson walks you through the steps of creating a forest and domain structure, installing domain controllers, creating the forest root domain and a child domain, and setting the functional level of a forest and domain. It also provides information about integrating DNS zones into Active Directory and how to configure DNS servers for use with Active Directory.

Objectives

- Implement and manage an Active Directory forest and domain structure
- Create the forest root domain and a child domain
- Create and configure application data partitions

Topics

- The role of the forest
- The role of the domain
- Forest and domain functional levels
- Raising the functional level
- Creating a forest root domain
- Creating a new domain tree and a new child domain
- Creating a new domain controller
- Assigning and transferring forestwide master roles
- Assigning and transferring domainwide master roles
- Using application directory partitions
- Establishing trust relationships
- Implementing DNS
- Configuring DNS servers

Lesson 5: Restructuring a Forest and Renaming Domains

Summary

This lesson explains the procedures involved in restructuring an existing forest. It explains how to prepare for a domain rename, how to execute the domain rename, and how to verify that the rename was successful.

Objectives

- Prepare for a domain rename
- Execute a domain rename
- Perform the appropriate steps after a domain rename

Topics

- Domain rename issues
- Preparing for a domain rename
- More domain rename preparation
- Domain rename planning and documentation
- Creating the domain rename instructions
- Executing the domain rename instructions
- Repairing the domain after a rename

- Other tasks to perform after a domain rename
- Changing DNS host names of domain controllers

Lesson 6: Working with Trusts and Organizational Units

Summary

This lesson provides information on two important components of Active Directory: trust relationships and OUs.

Objectives

- Establish and manage trust relationships
- Create organizational units
- Plan OU structures and strategies
- Delegate OU permissions

Topics

- Active Directory Trusts
- Working with Active Directory Trusts
- Working with organization units
- Creating organizational units
- Planning an OU structure and strategy

Lesson 7: Working with Active Directory Sites

Summary

This lesson examines the role of sites in the Active Directory infrastructure, and how replication, authentication, and distribution of services information work within and across sites.

Objectives

- Discuss the role of sites in the Active Directory infrastructure
- Create sites, subnets, and site links
- Configure bridges, and bridgehead servers
- Configure, monitor, and troubleshoot site replication

Topics

- The role of sites
- Relationship of sites to other components
- Creating and renaming sites
- Creating subnets
- Creating site links
- Site replication overview
- Configuring site replication
- Configuring bridges and bridgehead servers
- Troubleshooting replication failure
- Monitoring FRS replication

Lesson 8: Working with Domain Controllers

Summary

This lesson provides information about installing and configuring domain controllers. It also provides information on planning and diagnosing operation master roles.

Objectives

- Install and configure an Active Directory domain controller
- Plan flexible operations master role placement
- Diagnose and resolve issues related to operations master role failure
- Plan for business continuity of operations master roles
- Identify operations master roles dependencies

Topics

- Planning Domain Controllers
- Using the Active Directory Installation Wizard
- Creating additional Domain Controllers
- Upgrading and placing Domain Controllers
- Backing up and restoring Domain Controllers
- Managing Operations Masters
- Transferring Operations Master roles
- Seizing the Master and responding to failures
- Schema naming RID PCD infrastructure promotion upgrading restoring transferring

Lesson 9: Working with Global Catalog Servers and Schema

Summary

This lesson examines the role of Global Catalog servers and schema in Active Directory, including how to create, manage, and place GC servers and how to troubleshoot GC and schema issues.

Objectives

- Work with the GC and GC Servers
- Plan a strategy for placing GC servers
- Work with the Active Directory schema
- Use the Schema MMC snap-in

Topics

- Functions of the Global Catalog
- Customizing the Global Catalog
- Working with the Global Catalog and GC servers
- More Global Catalog issues
- Active Directory Schema components
- Working with the Active Directory Schema

Lesson 10: Working with Group Policy

Summary

This lesson provides an overview about the basics of Group Policy terminology and concepts as well as strategies for planning and implementing Group Policy

Objectives

- Plan a Group Policy strategy
- Manage and maintain Group Policy
- Configure the user environment by using Group Policy
- Troubleshoot issues related to Group Policy application deployment

Topics

- Understanding Group Policy
- Planning a Group Policy strategy
- Strategy for configuring user and computer environments
- Creating, configuring, and managing GPOs
- Configuring application of Group Policy
- Delegating administrative control and verifying Group Policy
- Automatically enrolling user and computer certificates
- Redirecting folders and configuring security settings
- Software restriction policies and Group Policy best practices
- Troubleshooting Group Policy

Lesson 11: Deploying Software via Group Policy

Summary

This lesson introduces you to Group Policy's software installation feature. The lesson explains how to use the components of software installation: Windows installer packages, transforms, patches, and application assignment scripts. You will walk through the steps of preparing for Group Policy software installation, working with the GPO Editor and setting installation options. Finally, the lesson covers how to upgrade applications, manage applications, and troubleshoot problems that can occur with Group Policy software deployment.

Objectives

- Describe Group Policy software installation options
- Identify Group Policy software installation components
- Prepare for Group Policy software installation
- Assign and publish applications
- Manage applications
- Troubleshoot software deployment

Topics

- Introduction to Group Policy software deployment
- Group Policy software installation options
- Group Policy software installation components
- Preparing for Group Policy software installation
- Working with the GPO Editor
- Assigning and publishing applications
- Configuring properties and upgrading applications
- Managing applications
- Troubleshooting software deployment

Lesson 12: Ensuring Active Directory Availability

Summary

This lesson provides information to help you diagnose and resolve Active Directory database issues, restore Active Directory directory services, and perform both an authoritative and nonauthoritative restore operation to ensure that your Windows Server 2003 network directory services are highly available.

Objectives

- Diagnose and resolve issues related to the Active Directory database
- Restore Active Directory directory services
- Perform an authoritative restore operation
- Perform a nonauthoritative restore operation

Topics

- The Active Directory database
- Tombstone process and Garbage Collection
- Fault tolerance and performance
- Defragmenting the database
- Moving the database or log file
- Monitoring the database
- Backing up Active Directory
- Performing a normal restore
- Authoritative and primary restores
- Troubleshooting availability
- Using Ntdsutil command options
- More Ntdsutil command options

Technical features of this course

- Show Me Hows allow you to access instructional demonstrations from all courses in the series.
- Simulations teach you to perform specific tasks in applications through guided, multi-step exercises.
- Activities allow you to apply course concepts in an interactive questioning environment.
- Exercises allow you to practice in the actual application being studied.
- A Course Topics list contains active hyperlinks, permitting quick access to specific topics.
- Find-A-Word allows you to look up an unfamiliar term in the Glossary, on the Web, or in a dictionary. In addition, it lets you find other occurrences of the term in the same course.
- Search text enables you to rapidly search all text within a course to easily retrieve information required.
- Courses challenge you with a variety of question formats, including multi-step simulations, true/false, multiple choice, and fill-in-the-blank.
- A skill assessment generates a customized learning path based on the results of a pre-test.
- A glossary provides a reference for definitions of unfamiliar terms.
- Bookmarking tracks your progress in a course.

Technical requirements

P500+ Processor, 128MB of RAM; Windows 2000, 2003, XP, Vista, Minimum screen resolution 800x600, Internet Explorer 5.5 or higher; Windows Media Player 9.0 or higher; Flash 8.0 or higher; 56K minimum connection; broadband (256 kbps or higher) connection recommended; Javascript, DHTML and cookies enabled; Sound card with speakers or headphones strongly recommended.

The core exam on client operating system

Windows XP Professional MCSE Exam 70-270 Lessons

Lesson Title	Minimum time to work through lesson	Lesson Code
Installation	3.0 hour(s)	x27001
Administering Resources	5.0 hour(s)	x27002
Configuring Hardware	5.0 hour(s)	x27003
Optimizing the System	5.0 hour(s)	x27004
Configuring the Desktop	3.0 hour(s)	x27005
Networking the System	6.0 hour(s)	x27006
Securing the System	4.0 hour(s)	x27007

Lesson 1: Installation

Summary

This lesson provides you with an overview of the installation process for Microsoft Windows XP Professional.

Objectives

- Devise an installation plan for Windows XP Professional
- Perform an attended Windows XP Professional install
- Perform an unattended Windows XP Professional install
- Troubleshoot failed installations

Topics

- Attended Installations
- Automating Installations
- Creating Unattended Installation Files
- Upgrading and Troubleshooting

Lesson 2: Administering Resources

Summary

This lesson shows how to manage files, folders, and file systems. In addition, it describes the process and capabilities of managing resources shared on a network.

Objectives

- Configure and manage compression and encryption for files and folders
- Configure file systems using FAT, FAT32, or NTFS
- Convert from one file system to another
- Control access to files and folders by using NTFS permissions
- Explain network printing under Windows XP
- Set up and manage a print server with Windows XP

Topics

- Sharing Files
- NTFS Permissions
- Managing File Resources
- Administering Printers

Lesson 3: Configuring Hardware

Summary

This lesson describes how to view properties of disks, configure disks, maintain disks, and work with removable media. It also describes the installation and configuration of hardware devices in Windows XP Professional.

Objectives

- Describe features of basic and dynamic storage
- View disk properties on local and remote computers
- Format disks and perform disk maintenance
- Manage removable media
- Install, configure, and manage input/output devices
- Troubleshoot hardware devices
- Update device drivers

Topics

- Installing Hardware
- Media Devices
- Input and Output Devices
- Other Devices

Lesson 4: Optimizing the System

Summary

This lesson teaches users how to monitor, troubleshoot, and back up the system for optimum performance.

Objectives

- Manage and troubleshoot driver signing
- Configure, manage, and troubleshoot the Task Scheduler
- Manage and troubleshoot the use and synchronization of offline files
- Optimize and troubleshoot the performance of Windows XP Professional
- Manage hardware profiles
- Back up and recover system state and user data

Topics

- Driver Signing and Hardware Profiles
- Scheduling and Offline Profiles
- Optimizing Performance
- Optimizing Disks, Network, and Applications
- Recovering from Disaster

Lesson 5: Configuring the Desktop

Summary

This lesson describes how to configure user profiles and support for multiple languages and locations.

Objectives

- Configure and manage user profiles
- Configure support for multiple languages or multiple locations
- Manage applications using Windows Installer packages
- Configure and troubleshoot desktop settings
- Configure and troubleshoot fax support
- Configure and troubleshoot accessibility services

Topics

- Configuring User Profiles
- Configuring and Securing the Desktop
- Installing and Configuring Applications
- Fax and Internet Options

Lesson 6: Networking the System

Summary

This lesson teaches users how to configure and connect a network with Microsoft Windows XP Professional. It also shows you how to configure and troubleshoot the TCP/IP protocol in a Windows XP environment.

Objectives

- Configure network components
- Connect to computers using dial-up networking
- Connect to shared resources on a Microsoft network
- Configure and troubleshoot the TCP/IP protocol

Topics

- Networking Models
- Networking Basics
- Configuring TCP/IP
- Troubleshooting TCP/IP
- Name Resolution
- Connecting to Resources
- IIS and Remote Desktop

Lesson 7: Securing the System

Summary

This lesson provides you with an overview of user and group accounts. It also provides you with an overview of configuring, monitoring, and maintaining systems security using audit policies, security templates, and encryption technology for Microsoft Windows XP Professional.

Objectives

- Create and manage local user accounts
- Create and manage domain user accounts
- Create and manage group accounts
- Modify user rights for users and groups
- Encrypt data on a hard disk by using Encrypting File System (EFS)
- Implement, configure, manage, and troubleshoot local security policy
- Implement, configure, manage, and troubleshoot a security configuration

Topics

- Managing Users
- Creating User Accounts
- Managing Groups
- User Rights and Policies
- Security Events
- Security Templates and File Encryption

Technical features of this course

- Exercises allow you to practice in the actual application being studied.
- A file contains the text of the exercises.
- Activities that allow you to apply course concepts in an interactive questioning environment.
- A glossary provides a reference for definitions of unfamiliar terms.
- A skill assessment generates a customized learning path based on the results of a pre-test.

Technical requirements

P500+ Processor, 128MB of RAM; Windows 2000, 2003, XP, Vista, Minimum screen resolution 800x600, Internet Explorer 5.5 or higher; Windows Media Player 9.0 or higher; Flash 8.0 or higher; 56K minimum connection; broadband (256 kbps or higher) connection recommended; Javascript, DHTML and cookies enabled; Sound card with speakers or headphones strongly recommended.

The core design exams (choose 1)

Designing a Windows Server 2003 Active Directory and Network Infrastructure MCSE Exam 70-297

Lesson Title	Minimum time to work through lesson	Lesson Code
Assessing the Environment	3.0 hour(s)	srin01
Developing the Active Directory Infrastructure Design	4.0 hour(s)	srin02
Developing the Network Services Design	2.0 hour(s)	srin03
Designing Logical Components	3.0 hour(s)	srin04
Name Resolution	3.0 hour(s)	srin05
Remote Access and Address Management	2.0 hour(s)	srin06
Service Placement and Sizing	2.0 hour(s)	srin07
The Physical Design	2.0 hour(s)	srin08
Practice Exam	1.0 hour(s)	srin09

Lesson 1: Assessing the Environment

Summary

This lesson explains how to assess your company's business and technical environment in preparation for implementing Windows Server 2003.

Objectives

- Analyze the impact of Active Directory on the existing technical environment.
- Analyze security requirements for the Active Directory directory service.
- Identify network topology and performance levels.
- Analyze the impact of the infrastructure design on the existing technical environment.

Topics

- Administrative models
- Assessing the current model
- Formulating new models
- Service levels
- Hardware and software deployments
- Interoperability
- Assessing the current domain model
- Infrastructure placement
- Analyzing DNS namespaces
- Assessing DNS infrastructure
- Analyzing network topography
- Creating a network map
- Analyzing network performance
- Assessing impact of proposed designs

Lesson 2: Developing the Active Directory Infrastructure Design

Summary

This lesson details how to design the Active Directory infrastructure for a Windows Server 2003 network.

Objectives

- Design the Active Directory infrastructure to meet business and technical requirements.
- Design the envisioned administration model.
- Create the conceptual design of the Active Directory forest structure.
- Create the conceptual design of the Active Directory domain structure.
- Design the Active Directory replication strategy
- Create the conceptual design of the organizational unit (OU) structure.

Topics

- Designing the administrative model
- Defining the forest design
- Forest models
- Ownership
- Creating a domain design
- Domain names and hierarchies
- Domain models
- Trees and domains
- Developing an OU model
- OU design models
- Developing a replication design
- Replication models
- Replication topology options

Lesson 3: Developing the Network Services Design

Summary

This lesson explains how to design the network services infrastructure for a Windows Server 2003 network.

Objectives

- Design the network services infrastructure to meet business and technical requirements.
- Create the conceptual design of the DNS infrastructure.
- Create the conceptual design of the WINS infrastructure.
- Create the conceptual design of the DHCP infrastructure.
- Create the conceptual design of the Remote Access infrastructure.

Topics

- Developing DNS designs
- DNS design features
- DNS and the Internet
- DNS and Active Directory
- Developing WINS designs
- DHCP design principles
- DHCP design features
- Developing a Remote Access strategy

Lesson 4: Designing Logical Components

Summary

This lesson explains how to design the logical components (organizational units, user accounts, and security groups) of a Windows Server 2003 network.

Objectives

- Design an OU structure.
- Design a security group strategy.
- Design a user and computer authentication strategy.
- Design a user and computer account strategy.
- Design an Active Directory naming strategy.
- Design migration paths to Active Directory.

Topics

- Defining standards
- Defining a forest structure and hierarchy
- Naming a forest
- Domains in the forest
- Assessing and defining a migration path
- Defining authentication mechanisms
- Trusts and collaboration
- Designing the organizational unit model
- OU design and group policy
- Group policy requirements
- Group policy and delegation
- Group policy settings
- Exploring groups
- Exploring roles
- Defining replication topology

Lesson 5: Name Resolution

Summary

This lesson provides an overview of the name resolution capabilities of Windows Server 2003 and explains how to incorporate DNS into a Windows Server 2003 network design.

Objectives

- Design a DNS name resolution strategy.
- Design a NetBIOS name resolution strategy.

- Design a Remote Access strategy.
- Design a DNS strategy for interoperability with UNIX Berkeley Internet Name Domain (BIND) to support Active Directory.
- Identify DNS interoperability with Active Directory, WINS, and DHCP.

Topics

- Understanding DNS design
- DNS design options
- DNS interoperability
- DNS zones
- DNS requirements
- DNS zone placement
- Delegation and security
- DNS servers
- WINS design strategy
- WINS topologies

Lesson 6: Remote Access and Address Management

Summary

This lesson explains how to design a strategy for Remote Access in a Windows Server 2003 network.

Objectives

- Design security for Remote Access users.
- Design a Remote Access strategy.
- Design an IP address assignment strategy.
- Specify DHCP integration with DNS infrastructure.
- Identify security host requirements.
- Identify the authentication and accounting provider.

Topics

- Remote Access Service servers
- ISO/OSI reference model
- Remote Access requirements
- Remote Access authentication requirements
- Authentication design
- Implementing Remote Access
- Defining security policies
- Defining the audit strategy
- IP address management and DHCP
- DHCP security considerations

Lesson 7: Service Placement and Sizing

Summary

This lesson explains how to place and size services in a Windows Server 2003 network.

Objectives

- Design DNS service placement
- Design an Active Directory implementation plan.
- Specify the server specifications to meet system requirements.
- Design the placement of domain controllers and global catalog servers.
- Plan the placement of flexible operations master roles.
- Select the domain controller creation process.

Topics

- Planning service placement
- Active directory implementation
- Active directory sizing
- Domain controller sizing
- Global catalog and DNS server sizing
- Flexible single master operations roles
- Placing FSMO roles
- FSMO failover and recovery

Lesson 8: The Physical Design

Summary

This lesson explains how to plan the physical layout and design of a Windows Server 2003 network.

Objectives

- Design Internet connectivity for a company.
- Design a network and routing topology for a company.
- Design the Remote Access infrastructure.
- Design a TCP/IP addressing scheme through the use of IP subnets.
- Design IP address assignment by using DHCP.

Topics

- Internet connectivity
- Domain name registration
- Segmenting the Intranet from the Internet
- Network topologies
- Subnets
- Addressing and DHCP
- Router placement
- The network perimeter
- Design requirements for Remote Access
- Authentication requirements for Remote Access
- RADIUS
- Remote Access infrastructure

Lesson 9: Practice Exam

Summary

This lesson provides a case study of a hypothetical organization and a series of review questions covering the design and implementation of this organization's Windows Server 2003 network.

Topics

- Taking the exam
- Practice exam

Technical features of this course

- A glossary provides a reference for definitions of unfamiliar terms.
- A skill assessment generates a customized learning path based on the results of a pre-test.

Technical requirements

P500+ Processor, 128MB of RAM; Windows 2000, 2003, XP, Vista, Minimum screen resolution 800x600, Internet Explorer 5.5 or higher; Windows Media Player 9.0 or higher; Flash 8.0 or higher; 56K minimum connection; broadband (256 kbps or higher) connection recommended;

Javascript, DHTML and cookies enabled; Sound card with speakers or headphones strongly recommended

Designing Security for a Windows Server 2003 Network MCSE Exam 70-298 Lessons

Lesson Title	Minimum time to work through lesson	Lesson Code
Designing a Secure Network Framework	2.0 hour(s)	srsc01
Defining a Baseline Security Template	3.0 hour(s)	srsc02
Designing Role-Based Server Security	2.0 hour(s)	srsc03
Securing a Public Key Infrastructure and Network Management Processes	4.0 hour(s)	srsc04
Designing Network Infrastructure Security	3.0 hour(s)	srsc05
Securing Data Transmissions and Wireless Networks	2.0 hour(s)	srsc06
Securing Internet Information Services	2.0 hour(s)	srsc07
Securing VPNs, Extranets, and Network Clients	4.0 hour(s)	srsc08
Securing Active Directory	3.0 hour(s)	srsc09
Designing an Access Control Strategy for Files and Folders	3.0 hour(s)	srsc10
Designing an Encrypted File System and Securing Backup/Restore Processes	3.0 hour(s)	srsc11
Practice Exam	2.0 hour(s)	srsc12

Lesson 1: Designing a Secure Network Framework

Summary

This lesson explains how to design a secure Windows Server 2003 network framework by analyzing business requirements, and both internal and external threats. It also details how to create an incident response plan and examines interoperability issues.

Objectives

- Analyze existing security policies and procedures
- Analyze requirements for securing different types of data
- Predict threats to a network from internal and external sources
- Design a process for incident response and recovery
- Identify capabilities of existing infrastructures including interoperability constraints

Topics

- Analyzing existing security Policies and procedures
- Determining requirements for securing data
- Analyzing current security practices
- Predicting network threats
- Recognizing external threats
- Implementing risk analysis
- Responding to security incidents
- Analyzing technical constraints

Lesson 2: Defining a Baseline Security Template

Summary

This lesson explains what you need in order to apply consistent security settings across a network. It also details how to deploy security templates efficiently throughout a network, focusing on the use of Group Policy Objects (GPO) and scripting techniques.

Objectives

- Design, create, and deploy a security template
- Configure security for down-level clients
- Analyze results of security settings
- Deploy security using scripts

Topics

- Administrative security tools overview
- Working with predefined security templates
- Adding security templates snap-ins
- Reapplying default security settings
- Configuring security templates
- Configuring security for down-level clients
- Deploying security templates
- Reviewing the result of security policy settings
- Using security configuration and analysis to review security settings
- Using the secedit.exe command-line tool

Lesson 3: Designing Role-Based Server Security

Summary

This lesson explains how to modify baseline security templates based on functions of an individual or group of servers. This lesson specifically addresses security configurations for Domain Controllers, Internet Information Services (IIS) Servers, POP3 Mail Servers, and other infrastructure servers.

Objectives

- Knowledge of common server roles and best security practices
- Modify baseline security templates according to role
- Configure security for Domain Controllers, Internet Information Services, Application, Mail, Infrastructure, File, Print, and Member, Terminal, Remote Access, and Streaming Media servers
- Apply security across an enterprise

Topics

- Common server roles
- Adding or changing server roles
- Configuring security for domain controllers
- Securing the Internet Information Server (IIS)
- Configuring security for POP3 mail servers
- Securing network infrastructure servers
- Securing remote access servers
- Securing file, print, terminal, and streaming media servers
- Modifying baseline security templates according to role

Lesson 4: Securing a Public Key Infrastructure and Network Management Processes

Summary

This lesson explains the deployment of public key infrastructures (PKI), the certificate authorities that establish and verify identities of organizations, and the implementation of PKI in the Windows Server 2003 environment. This lesson also covers security administration and the related tasks and tools needed to secure a Microsoft operating system.

Objectives

- Design a public key infrastructure (PKI) that uses Certificate Services
- Design a logical authentication strategy

- Design security for network management
- Design a security update infrastructure

Topics

- PKI basics
- Designing a certification authority implementation
- Designing a logical authentication strategy
- Designing security for CA servers
- Designing certificate distribution
- Requesting, approving, and revoking certificates
- Renewing and auditing certificates
- Managing the risks of network administration
- Securing MMC, Remote Assistance, and Telnet
- Securing Terminal Services and Remote Desktop
- Designing security for EMS
- Designing a Security Update infrastructure
- Trust relationship basics
- Designing forest and domain trust models
- Designing security for interoperability

Lesson 5: Designing Network Infrastructure Security

Summary

This lesson examines how to protect data as it is transmitted through a network infrastructure by use of IP Security (IPSec). This lesson also explains how to secure the Domain Naming System (DNS) service, another area of an enterprise network subject to security vulnerabilities.

Objectives

- Design network infrastructure security
- Design an IPSec policy
- Design IP filtering
- Specify the required protocols for a firewall configuration
- Secure a DNS implementation

Topics

- Network infrastructure security basics
- Assessing risk for network services
- IPSec overview
- Phase I security association
- Phase II security association
- IPSec policies overview
- IPSec rules
- How IPSec policy is applied
- IPSec driver modes and best practices
- Designing IPSec policies
- Designing IP filtering and configuring a firewall
- Securing DNS

Lesson 6: Securing Data Transmissions and Wireless Networks

Summary

This lesson explains how to secure wireless network traffic including the technologies available and the challenges they present. This lesson also discusses common vulnerabilities in a wireless network and how to design a secure wireless LAN.

Objectives

- Design security for data transmission
- Use segmented networks
- Design security for wireless networks
- Design public and private wireless LANs
- Design 802.11x authentication for wireless networks
- Design user authentication for Internet Information Services (IIS)

Topics

- SSL/TLS, S/MIME and SMB
- Configuring IIS to use SSL
- Securing switches and segments
- Wireless network types and threats
- Wireless history
- PKI and RADIUS/IAS overview
- WLAN network infrastructure
- Creating a wireless network policy
- Designing authentication for wireless networks
- Designing and testing wireless access infrastructure

Lesson 7: Securing Internet Information Services

Summary

This lesson explains how to create a secure IIS deployment for an enterprise network with a focus on user authentication. It also examines common vulnerabilities of Web servers, along with how to secure Web server software with options offered in Windows Server 2003.

Objectives

- Design user authentication for Internet Information Services (IIS) and a Web site
- Design security for IIS
- Design security for Web sites
- Design a monitoring strategy for IIS
- Design an IIS baseline based on business requirements
- Design a content management strategy for updating an IIS server

Topics

- Designing user authentication for IIS
- Designing certificate authentication
- Configuring anonymous and basic authentication
- Configuring digest and integrated Windows authentication
- Designing RADIUS authentication
- Securing IIS installations
- Hardening IIS
- New security features in IIS 6.0
- Designing a monitoring strategy for IIS
- Configuring IIS logging and monitoring Event Log activities
- Enabling security auditing and health detection

Lesson 8: Securing VPNs, Extranets, and Network Clients

Summary

This lesson discusses the use of Windows Server 2003 as a VPN and provides details on the use of two common, standards-based routing protocols: Routing Information Protocol (RIP) and Open Shortest Path First (OSPF). This lesson also explains how to secure client workstations and remote access services for end users.

Objectives

- Design security for communication between networks
- Design security for communication with external organizations
- Design a client authentication strategy
- Design a security strategy for client remote access
- Design a strategy for securing client computers

Topics

- Using Windows Server 2003 as a router
- Building routing tables
- Designing demand dial routing between internal networks
- Designing VPN connectivity
- PPTP
- L2TP
- Using remote access policies
- Designing an extranet infrastructure
- Hardening client operating systems
- Securing laptop computers
- Analyzing authentication requirements
- Choosing authentication protocols
- Choosing a remote access method
- Designing remote access policies
- Creating a remote access policy
- Using Internet Authentication service

Lesson 9: Securing Active Directory

Summary

This lesson explains how to secure Active Directory user accounts and use auditing to identify any security incidents to the Active Directory database. This lesson also discusses best practices in assigning user permissions to network resources and data.

Objectives

- Design an access control strategy for directory services
- Establish account and password requirements for security
- Analyze auditing requirements
- Create a delegation strategy
- Design the appropriate group strategy for accessing resources
- Design a permission structure for directory service objects

Topics

- Designing an access control strategy for directory services
- Analyzing risks to directory services
- Establishing account security policies
- Using restricted groups
- Creating a Kerberos policy
- Establishing password security
- Creating an account lockout policy
- Creating an auditing policy
- Auditing logon events and object access
- Analyzing auditing data
- Creating a delegation strategy
- Designing the appropriate group strategy for accessing resources

Lesson 10: Designing an Access Control Strategy for Files and Folders

Summary

This lesson examines common risks such as data corruption and security breaches that can affect a network's file shares. This lesson also explains how to design a permission structure for files and folders, as well as best practices for securing the Windows Registry.

Objectives

- Design an access control strategy for files and folders
- Analyze auditing requirements
- Design an access control strategy for the registry
- Design a permission structure for registry objects

Topics

- Analyzing risks to data
- Reviewing access control and access control lists
- Access to resources
- Working with security groups
- Defining a security group retirement policy
- Delegating security group maintenance
- Analyzing auditing requirements
- Designing an access control strategy for the registry
- Setting registry access permissions via group policy
- Designing a permission structure for registry objects

Lesson 11: Designing an Encrypted File System and Securing Backup/Restore Processes

Summary

This lesson explains how to encrypt files using the Encrypted File System (EFS). The lesson also discusses how to design a secure backup and recovery strategy for network resources, including securing the backup process.

Objectives

- Design a strategy for the encryption and decryption of files and folders
- Design security for a backup and recovery strategy
- Implement Encrypted File System (EFS)
- Configure a file recovery agent

Topics

- Encrypted File System
- Encrypting files and folders
- Certificate storage, enrollment, and renewal
- Creating a strategy for the encryption and decryption of files and folders
- Configuring file recovery agents
- Backing up keys
- Disabling EFS
- Backup and restore process security basics
- Designing a secure backup process
- Designing a secure recovery process
- Securing EMS
- Securing the Recovery Console
- Configuring startup and recovery options

Lesson 12: Practice Exam

Summary

This lesson provides five practice exams for the Microsoft 70-298 certification exam.

Topics

- Practice Exam 1
- Practice Exam 2
- Practice Exam 3
- Practice Exam 4
- Practice Exam 5

Technical features of this course

- A glossary provides a reference for definitions of unfamiliar terms.
- A skill assessment generates a customized learning path based on the results of a pre-test.

Technical requirements

P500+ Processor, 128MB of RAM; Windows 2000, 2003, XP, Vista, Minimum screen resolution 800x600, Internet Explorer 5.5 or higher; Windows Media Player 9.0 or higher; Flash 8.0 or higher; 56K minimum connection; broadband (256 kbps or higher) connection recommended; Javascript, DHTML and cookies enabled; Sound card with speakers or headphones strongly recommended.

The elective exams (choose 1)

Implementing and Managing Microsoft Exchange Server 2003 MCSA MCSE Exam 70-284 Lessons

Lesson Title	Minimum time to work through lesson	Lesson Code
Implementing and Troubleshooting	2.0 hour(s)	exma01
Managing Exchange Recipient Objects	2.0 hour(s)	exma02
Managing Address Lists and Policies	2.0 hour(s)	exma03
Managing the Exchange Organization	2.0 hour(s)	exma04
Managing Computers and Performance	4.0 hour(s)	exma05
Security and Troubleshooting	2.0 hour(s)	exma06
Practice Exams	2.0 hour(s)	exma07

Lesson 1: Implementing and Troubleshooting

Summary

This lesson provides an introduction to Microsoft Exchange Server 2003 and shows you how to prepare an environment, install the system, and troubleshoot an installation.

Objectives

- Prepare a Windows Server 2000/2003 system for installation of Exchange Server 2003
- Install Microsoft Exchange Server 2003
- Troubleshoot common installation problems
- Upgrade and integrate Exchange Server 2003 in mixed environments
- Troubleshoot Exchange Server 2003 in mixed environments

Topics

- Overview of Exchange Server 2003
- Preparing a new Exchange environment
- Installation
- Unattended installation Installation in a clustered environment
- Post-installation configuration Upgrading from Exchange Server 2000

- Establishing coexistence
- Migration wizards
- Migration from other messaging systems

Lesson 2: Managing Exchange Recipient Objects

Summary

This lesson shows users how to use Microsoft Exchange Server 2003 to create and manage contacts, user accounts, distribution groups, security groups.

Objectives

- Create and manage contacts
- Manage and modify user accounts
- Create and manage distribution groups
- Create and manage security groups

Topics

- Understanding Exchange recipients
- Creating new users
- Mailbox-enabling users
- Deleting and moving mailboxes
- Modifying email addresses
- Hiding and reconnecting mailboxes
- Configuring mailbox storage limits
- Configuring permission
- Managing contacts
- Managing groups
- Creating query-based distribution groups
- Using expansion servers

Lesson 3: Managing Address Lists and Policies

Summary

This lesson shows you how to use Microsoft Exchange Server 2003 to create and manage address lists and policies.

Objectives

- Create and manage address lists
- Create and manage recipient policies
- Create and manage mailbox store policies
- Create and manage server policies
- Create and manage public folder store policies

Topics

- Understanding Exchange address lists
- Creating global address lists
- Creating custom address lists
- Creating offline address lists
- Hiding address lists
- Forcing address lists
- Setting mailbox store policies
- Setting public folder store and server policies
- Setting recipient policies
- Managing system policies
- Managing recipient policies

Lesson 4: Managing the Exchange Organization

Summary

This lesson shows you how to use Microsoft Exchange Server 2003 to create, manage, and troubleshoot public folders. It also covers how to configure, manage and troubleshoot virtual front-end and back-end servers. Finally, it discusses troubleshooting techniques.

Objectives

- Create and manage public folders
- Troubleshoot public folder issues
- Configure and manage virtual servers
- Configure and manage front-end and back-end servers
- Troubleshoot front-end and back-end servers

Topics

- Understanding public folders
- Permissions, replication, and referrals
- Creating public folders
- Managing replication and referral
- Managing full-text indexing
- Troubleshooting public folders
- Understanding virtual servers
- Managing virtual servers
- Limiting inbound connections
- Managing SMTP relay settings
- Front-end/back-end arrangements

Lesson 5: Managing Computers and Performance

Summary

This lesson shows you how to use Microsoft Exchange Server 2003 to manage, monitor, and troubleshoot Exchange organization and server computers.

Objectives

- Configure, manage, and troubleshoot Exchange server clusters
- Plan and perform Exchange back-ups and restorations
- Manage and troubleshoot client connectivity
- Manage, monitor, and troubleshoot infrastructure performance, data storage, and server health

Topics

- Understanding clustering
- Cluster models
- Creating a cluster
- Planning Exchange backups
- Performing Exchange backups
- Understanding restoration strategies
- Restoring Exchange data
- Removing Exchange servers
- Understanding client connectivity
- Using monitoring tools
- Using system monitor
- Managing data storage

Lesson 6: Security and Troubleshooting

Summary

This lesson explains how to manage security, as well as manage and monitor supporting technologies of Microsoft Exchange Server 2003.

Objectives

- Manage connections to Exchange Server 2003 across firewalls
- Manage auditing settings, audit logs, permissions, and encryption for Exchange Server 2003
- Understand and respond to threats to security
- Perform an nslookup query to locate the Mail Exchanger (MX) settings for a particular domain
- Use the ipconfig utility to determine the preferred and alternate Domain Name System (DNS) settings for a client
- Use nondelivery reports to locate problems in mail transmission

Topics

- Managing connectivity across firewalls
- Managing audit settings
- Managing permissions
- Understanding encryption and digital signatures
- Managing encryption and digital signatures
- Detecting security threats
- Troubleshooting mail queues
- Troubleshooting DNS issues
- Troubleshooting Active Directory issues
- Troubleshooting networking issues

Lesson 7: Practice Exams

Summary

This lesson provides two practice exams for the Microsoft 70-284 certification exam.

Topics

- Preparing for the exam
- Practice exam 1
- Practice exam 2

Technical features of this course

- A glossary provides a reference for definitions of unfamiliar terms.
- A skill assessment generates a customized learning path based on the results of a pre-test.

Technical requirements

P500+ Processor, 128MB of RAM; Windows 2000, 2003, XP, Vista, Minimum screen resolution 800x600, Internet Explorer 5.5 or higher; Windows Media Player 9.0 or higher; Flash 8.0 or higher; 56K minimum connection; broadband (256 kbps or higher) connection recommended; Javascript, DHTML and cookies enabled; Sound card with speakers or headphones strongly recommended

Server 2003 Security Admin MCSA/MCSE Exam 70-299 Lessons

Lesson Title	Minimum time to work through lesson	Lesson Code
Implementing, Managing, and Troubleshooting Security Policies	2.0 hour(s)	svse01
Network Communications Security and Patch Management	2.0 hour(s)	svse02
PKI Administration and IPSec Troubleshooting	3.0 hour(s)	svse03
Planning and Implementing Security for Remote Users and Wireless Networks	2.0 hour(s)	svse04
Practice Exams	2.0 hour(s)	svse05

Lesson 1: Implementing, Managing, and Troubleshooting Security Policies

Summary

This lesson provides an introduction to implementing, managing, and troubleshooting security policies.

Objectives

- Develop a network security structure
- Use Active Directory Group Policy Objects, scripting, and command-line tools to apply security templates
- Configure auditing and logging based on computer roles
- Configure security templates

Topics

- Planning security
- Configuring security mechanisms
- Planning and deploying security templates
- Configuring security based on server roles
- Configuring security based on client roles
- Auditing and logging
- Troubleshooting security policy inheritance
- Troubleshooting security template problems

Lesson 2: Network Communications Security and Patch Management

Summary

This lesson provides an introduction to network communications security and patch management.

Objectives

- Develop a network security structure
- Use Active Directory Group Policy Objects, scripting, and command-line tools to apply security templates
- Configure auditing and logging based on computer roles
- Configure security templates

Topics

- Planning security
- Configuring security mechanisms
- Planning and deploying security templates
- Configuring security based on server roles
- Auditing and logging
- Troubleshooting security policy inheritance
- Troubleshooting security template problems

Lesson 3: PKI Administration and IPSec Troubleshooting

Summary

This lesson provides an introduction to PKI administration and IPSec troubleshooting.

Objectives

- Monitor IPSec policies
- Troubleshoot IPSec certificates
- Plan, build, and manage certification authority
- Archive and recover keys
- Back up, restore, and recover certificate authority

Topics

- Public key infrastructure and certification authority
- Installing a root CA and issuing CA
- Installing and configuring an Intermediate CA
- Managing CAs
- Configuring, managing, and troubleshooting CRLs
- Configuring archival and recovery of keys
- Deploying and revoking certificates
- Backing up and restoring the CA
- Troubleshooting PKI and IPSec
- Troubleshooting IPSec across networks

Lesson 4: Planning and Implementing Security for Remote Users and Wireless Networks

Summary

This lesson provides an introduction to planning and implementing security for remote users and wireless networks

Objectives

- Deploy, manage, and configure SSL certificates
- Configure and troubleshoot VPN protocols
- Configure Group Policy wireless network settings
- Configure Windows XP and Windows 2000 client computers for wireless access

Topics

- Deploying, managing, and configuring SSL certificates
- Configuring security and authentication for remote access users
- Configuring and troubleshooting virtual private network (VPN) protocols
- Managing client configuration for remote access security
- Planning the authentication methods for a wireless network
- Planning the encryption methods for a wireless network
- Planning and configuring wireless access policies
- Configuring SSL certificates for wireless networks
- Configuring wireless encryption
- Installing and configuring wireless support for client computers

Lesson 5: Practice Exams

Summary

This lesson provides practice exams to prepare you for the MCSA/MCSE 70-299 exam.

Topics

- Key facts for the MCSA/MCSE 70-299 exam
- Practice Exam 1
- Practice Exam 2

Technical features of this course

- A glossary provides a reference for definitions of unfamiliar terms.
- A skill assessment generates a customized learning path based on the results of a pre-test.

Technical requirements

P500+ Processor, 128MB of RAM; Windows 2000, 2003, XP, Vista, Minimum screen resolution 800x600, Internet Explorer 5.5 or higher; Windows Media Player 9.0 or higher; Flash 8.0 or higher; 56K minimum connection; broadband (256 kbps or higher) connection recommended; Javascript, DHTML and cookies enabled; Sound card with speakers or headphones strongly recommended.