MCSE 2003

Microsoft Certified Systems Engineer (MCSE) candidates on the Microsoft Windows Server™ 2003 track are required to satisfy the following requirements:

Core Exams (6 Exams Required)

- Four networking system exams
- One client operating system exam
- One design exam

Elective Exams (1 Exam Required)

Core exams (Networking)

Exam 70–290: Managing and Maintaining a Microsoft Windows Server 2003 Environment

Exam 70–291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure

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

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

One Client OS Exam

Exam 70–270: Installing, Configuring, and Administering Microsoft Windows® XP Professional

One Design Exam

Exam 70-297[2, 3]: Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure

One Elective exam

Exam 70-227[4]: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition

Exam 70–290 Objectives (8 Lectures)

Managing and Maintaining Physical and Logical Devices

Manage basic disks and dynamic disks.
Monitor server hardware. Tools might include Device Manager, the Hardware Troubleshooting Wizard, and appropriate Control Panel items.

Optimize server disk performance.

- Implement a RAID solution.
- Defragment volumes and partitions.

Install and configure server hardware devices.

- Configure driver signing options.
- Configure resource settings for a device.
- Configure device properties and settings.

Managing Users, Computers, and Groups

Manage local, roaming, and mandatory user profiles.
Create and manage computer accounts in an Active Directory environment.

Create and manage groups.

- Identify and modify the scope of a group.
- Find domain groups in which a user is a member.
- Manage group membership.
- Create and modify groups by using the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in.
- Create and modify groups by using automation.

Create and manage user accounts.

- Create and modify user accounts by using the Active Directory Users and Computers MMC snap-in.
- Create and modify user accounts by using automation.
- Import user accounts.

Troubleshoot computer accounts.

- Diagnose and resolve issues related to computer accounts by using the Active Directory Users and Computers MMC snap-in.
- Reset computer accounts.

Troubleshoot user accounts.

- Diagnose and resolve account lockouts.
- Diagnose and resolve issues related to user account properties.

Troubleshoot user authentication issues.

Managing and Maintaining Access to Resources

Configure access to shared folders.

- Manage shared folder permissions.

Troubleshoot Terminal Services.

- Diagnose and resolve issues related to Terminal Services security.
- Diagnose and resolve issues related to client access to Terminal Services.

Configure file system permissions.

- Verify effective permissions when granting permissions.
- Change ownership of files and folders.

Troubleshoot access to files and shared folders.

Managing and Maintaining a Server Environment

Monitor and analyze events. Tools might include Event Viewer and System Monitor.
Manage software update infrastructure.
Manage software site licensing.
Manage servers remotely.

- Manage a server by using Remote Assistance.
- Manage a server by using Terminal Services remote administration mode.
- Manage a server by using available support tools.

Troubleshoot print queues.

Monitor system performance.

Monitor file and print servers. Tools might include Task Manager, Event Viewer, and System Monitor.

- Monitor disk quotas.
- Monitor print queues.
- Monitor server hardware for bottlenecks.

Monitor and optimize a server environment for application performance.

- Monitor memory performance objects.
- Monitor network performance objects.
- Monitor process performance objects.
- Monitor disk performance objects.

Manage a Web server.

- Manage Internet Information Services (IIS).
- Manage security for IIS.

Managing and Implementing Disaster Recovery

Perform system recovery for a server.

- Implement Automated System Recovery (ASR).
- Restore data from shadow copy volumes.
- Back up files and System State data to media.
- Configure security for backup operations.

Manage backup procedures.

- Verify the successful completion of backup jobs.
- Manage backup storage media.

Recover from server hardware failure.

Restore backup data.
Schedule backup jobs.

Exam 70–291: Objectives (7 Lectures)

Implementing, Managing, and Maintaining IP Addressing
Configure TCP/IP addressing on a server computer.
Manage DHCP.

- Manage DHCP clients and leases.
- Manage DHCP Relay Agent.
- Manage DHCP databases.
- Manage DHCP scope options.
- Manage reservations and reserved clients.

Troubleshoot TCP/IP addressing.

- Diagnose and resolve issues related to Automatic Private IP Addressing (APIPA).
- Diagnose and resolve issues related to incorrect TCP/IP configuration.

Troubleshoot DHCP.

- Diagnose and resolve issues related to DHCP authorization.
- Verify DHCP reservation configuration.
- Examine the system event log and DHCP server audit log files to find related events.
- Diagnose and resolve issues related to configuration of DHCP server and scope options.
- Verify that the DHCP Relay Agent is working correctly.
- Verify database integrity.

Implementing, Managing, and Maintaining Name Resolution
Install and configure the DNS Server service.

- Configure DNS server options.
- Configure DNS zone options.
- Configure DNS forwarding.

Manage DNS.

- Manage DNS zone settings.
- Manage DNS record settings.
- Manage DNS server options.

Monitor DNS. Tools might include System Monitor, Event Viewer, Replication Monitor, and DNS debug logs.

Implementing, Managing, and Maintaining Network Security
Implement secure network administration procedures.

- Implement security baseline settings and audit security settings by using security templates.
- Implement the principle of least privilege.

Monitor network protocol security. Tools might include the IP Security Monitor Microsoft Management Console (MMC) snap-in and Kerberos support tools.

Troubleshoot network protocol security. Tools might include the IP Security Monitor MMC snap-in, Event Viewer, and Network Monitor.

Implementing, Managing, and Maintaining Routing and Remote Access

Configure Routing and Remote Access user authentication.

- Configure remote access authentication protocols.
- Configure Internet Authentication Service (IAS) to provide authentication for Routing and Remote Access clients.
- Configure Routing and Remote Access policies to permit or deny access.

Manage remote access.

- Manage packet filters.
- Manage Routing and Remote Access routing interfaces.
- Manage devices and ports.
- Manage routing protocols.
- Manage Routing and Remote Access clients.

Manage TCP/IP routing.

- Manage routing protocols.
- Manage routing tables.
- Manage routing ports.

Implement secure access between private networks.

Troubleshoot user access to remote access services.

- Diagnose and resolve issues related to remote access VPNs.
- Diagnose and resolve issues related to establishing a remote access connection.
- Diagnose and resolve user access to resources beyond the remote access server.

Troubleshoot Routing and Remote Access routing.

- Troubleshoot demand-dial routing.
- Troubleshoot router-to-router VPNs.

Maintaining a Network Infrastructure

Monitor network traffic. Tools might include Network Monitor and System Monitor.

Troubleshoot connectivity to the Internet.

Troubleshoot server services.

- Diagnose and resolve issues related to service dependency.
- Use service recovery options to diagnose and resolve service-related issues.

Exam 70-293: Objectives (8 Lectures)

Planning and Implementing Server Roles and Server Security
Configure security for servers that are assigned specific roles.

Plan a secure baseline installation.

- Plan a strategy to enforce system default security settings on new systems.
- Identify client operating system default security settings.
- Identify all server operating system default security settings.

Plan security for servers that are assigned specific roles. Roles might include domain controllers, Web servers, database servers, and mail servers.

- Deploy the security configuration for servers that are assigned specific roles.
- Create custom security templates based on server roles.

Evaluate and select the operating system to install on computers in an enterprise.

- Identify the minimum configuration to satisfy security requirements.

Planning, Implementing, and Maintaining a Network Infrastructure
Plan a TCP/IP network infrastructure strategy.

- Analyze IP addressing requirements.
- Plan an IP routing solution.
- Create an IP subnet scheme.

Plan and modify a network topology.

- Plan the physical placement of network resources.
- Identify network protocols to be used.

Plan an Internet connectivity strategy.

Plan network traffic monitoring. Tools might include Network Monitor and System Monitor.

Troubleshoot connectivity to the Internet.

- Diagnose and resolve issues related to Network Address Translation (NAT).
- Diagnose and resolve issues related to name resolution cache information.
- Diagnose and resolve issues related to client configuration.

Troubleshoot TCP/IP addressing.

- Diagnose and resolve issues related to client computer configuration.
- Diagnose and resolve issues related to DHCP server address assignment.

Plan a host name resolution strategy.

- Plan a DNS namespace design.
- Plan zone replication requirements.
- Plan a forwarding configuration.
- Plan for DNS security.
- Examine the interoperability of DNS with third-party DNS solutions.

Plan a NetBIOS name resolution strategy.

- Plan a WINS replication strategy.
- Plan NetBIOS name resolution by using the Lmhosts file.

Troubleshoot host name resolution.

- Diagnose and resolve issues related to DNS services.
- Diagnose and resolve issues related to client computer configuration.

Planning, Implementing, and Maintaining Routing and Remote Access
Plan a routing strategy.

- Identify routing protocols to use in a specified environment.
- Plan routing for IP multicast traffic.

Plan security for remote access users.

- Plan remote access policies.
- Analyze protocol security requirements.
- Plan authentication methods for remote access clients.

Implement secure access between private networks.

- Create and implement an IPSec policy.

Troubleshoot TCP/IP routing. Tools might include the route, tracert, ping, pathping, and netsh commands and Network Monitor.

Planning, Implementing, and Maintaining Server Availability
Plan services for high availability.

- Plan a high availability solution that uses clustering services.
- Plan a high availability solution that uses Network Load Balancing.

Identify system bottlenecks, including memory, processor, disk, and network related bottlenecks.

- Identify system bottlenecks by using System Monitor.

Implement a cluster server.

- Recover from cluster node failure.

Manage Network Load Balancing. Tools might include the Network Load Balancing Monitor Microsoft Management Console (MMC) snap-in and the WLBS cluster control utility.
Plan a backup and recovery strategy.

- Identify appropriate backup types. Methods include full, incremental, and differential.
- Plan a backup strategy that uses volume shadow copy.
- Plan system recovery that uses Automated System Recovery (ASR).

Planning and Maintaining Network Security
Configure network protocol security.

- Configure protocol security in a heterogeneous client computer environment.
- Configure protocol security by using IPSec policies.

Configure security for data transmission.

- Configure IPSec policy settings.

Plan for network protocol security.

- Specify the required ports and protocols for specified services.
- Plan an IPSec policy for secure network communications.

Plan secure network administration methods.

- Create a plan to offer Remote Assistance to client computers.
- Plan for remote administration by using Terminal Services.

Plan security for wireless networks.

Plan security for data transmission.

- Secure data transmission between client computers to meet security requirements.
- Secure data transmission by using IPSec.

Troubleshoot security for data transmission. Tools might include the IP Security Monitor MMC snap-in and the Resultant Set of Policy (RSoP) MMC snap-in.

Planning, Implementing, and Maintaining Security Infrastructure.
Configure Active Directory directory service for certificate publication.

Plan a public key infrastructure (PKI) that uses Certificate Services.

- Identify the appropriate type of certificate authority to support certificate issuance requirements.
- Plan the enrollment and distribution of certificates.
- Plan for the use of smart cards for authentication.

Plan a framework for planning and implementing security.

- Plan for security monitoring.
- Plan a change and configuration management framework for security.