

G-MAC

Document ID: 05102009



Table of contents

Microsoft Certified Systems Engineer (MCSE) 3

Microsoft Certified Systems Engineer (MCSE)

No. of Course(s): 7

Duration per Course: 40 Hours

Total Duration: 280 Hours

Course: Managing and Maintaining a Windows Server 2003 Environment

Content:

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.
- Troubleshoot server hardware devices.
 - Diagnose and resolve issues related to hardware settings.
 - Diagnose and resolve issues related to server hardware and hardware driver upgrades.
- 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 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.

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

Content:

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.
- Install and configure software update infrastructure.
 - Install and configure software update services.
 - Install and configure automatic client update settings.
 - Configure software updates on earlier operating systems.

- 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.

Course: Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure

Content:

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.
- Plan a security update infrastructure. Tools might include Microsoft Baseline Security Analyzer and Microsoft Software Update Services.

Course: Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure

Content:

Planning and Implementing an Active Directory Infrastructure

- Plan a strategy for placing global catalog servers.
 - Evaluate network traffic considerations when placing global catalog servers.
 - Evaluate the need to enable universal group caching.
- Plan flexible operations master role placement.
 - Plan for business continuity of operations master roles.
 - Identify operations master role dependencies.
- Implement an Active Directory directory service forest and domain structure.
 - Create the forest root domain.
 - Create a child domain.
 - Create and configure Application Data Partitions.
 - Install and configure an Active Directory domain controller.
 - Set an Active Directory forest and domain functional level based on requirements.
 - Establish trust relationships. Types of trust relationships might include external trusts, shortcut trusts, and cross-forest trusts.
- Implement an Active Directory site topology.
 - Configure site links.
 - Configure preferred bridgehead servers.
- Plan an administrative delegation strategy.
 - Plan an organizational unit (OU) structure based on delegation requirements.
 - Plan a security group hierarchy based on delegation requirements.

Managing and Maintaining an Active Directory Infrastructure

- Manage an Active Directory forest and domain structure.
 - Manage trust relationships.
 - Manage schema modifications.
 - Add or remove a UPN suffix.
- Manage an Active Directory site.
 - Configure replication schedules.
 - Configure site link costs.
 - Configure site boundaries.
- Monitor Active Directory replication failures. Tools might include Replication Monitor, Event Viewer, and support tools.
 - Monitor Active Directory replication.
 - Monitor File Replication service (FRS) replication.
- Restore Active Directory directory services.
 - Perform an authoritative restore operation.
 - Perform a nonauthoritative restore operation.

- Troubleshoot Active Directory.
 - Diagnose and resolve issues related to Active Directory replication.
 - Diagnose and resolve issues related to operations master role failure.
 - Diagnose and resolve issues related to the Active Directory database.

Planning and Implementing User, Computer, and Group Strategies

- Plan a security group strategy.
- Plan a user authentication strategy.
 - Plan a smart card authentication strategy.
 - Create a password policy for domain users.
- Plan an OU structure.
 - Analyze the administrative requirements for an OU.
 - Analyze the Group Policy requirements for an OU structure.
- Implement an OU structure.
 - Create an OU.
 - Delegate permissions for an OU to a user or to a security group.
 - Move objects within an OU hierarchy.

Planning and Implementing Group Policy

- Plan Group Policy strategy.
 - Plan a Group Policy strategy by using Resultant Set of Policy (RSoP) Planning mode.
 - Plan a strategy for configuring the user environment by using Group Policy.
 - Plan a strategy for configuring the computer environment by using Group Policy.
- Configure the user environment by using Group Policy.
 - Distribute software by using Group Policy.
 - Automatically enroll user certificates by using Group Policy.
 - Redirect folders by using Group Policy.
 - Configure user security settings by using Group Policy.
- Deploy a computer environment by using Group Policy.
 - Distribute software by using Group Policy.
 - Automatically enroll computer certificates by using Group Policy.
 - Configure computer security settings by using Group Policy.

Managing and Maintaining Group Policy

- Troubleshoot issues related to Group Policy application deployment. Tools might include RSoP and the gpresult command.
- Maintain installed software by using Group Policy.
 - Distribute updates to software distributed by Group Policy.
 - Configure automatic updates for network clients by using Group Policy.
- Troubleshoot the application of Group Policy security settings. Tools might include RSoP and the gpresult command.

Course: TS: Configuring Microsoft Windows Vista Client

Content:

Installing and upgrading Windows Vista

- Identify hardware requirements.
- Perform a clean installation.
- Upgrade to Windows Vista from previous versions of Windows.
- Upgrade from one edition of Windows Vista to another edition.
- Troubleshoot Windows Vista installation issues.
- Install and configure Windows Vista drivers.

Configuring and troubleshooting Post-installation system settings

- Troubleshoot post-installation configuration issues.
- Configure and troubleshoot Windows Aero.
- Configure and troubleshoot parental controls.
- Configure Microsoft Internet Explorer.

Configuring Windows security features

- Configure and troubleshoot User Account Control.
- Configure Windows Defender.
- Configure Dynamic Security for Microsoft Internet Explorer 7.
- Configure security settings in Windows Firewall.

Configuring network connectivity

- Configuring networking by using the Network and Sharing Center.
- Troubleshoot connectivity issues.
- Configure remote access.

Configuring applications included with Windows Vista

- Configure and troubleshoot media applications.
- Configure Windows Mail.
- Configure Windows Meeting Space.
- Configure Windows Calendar.
- Configure Windows Fax and Scan.
- Configure Windows Sidebar.

Maintaining and optimizing systems that run Windows Vista

- Troubleshoot performance issues.
- Troubleshoot reliability issues by using built-in diagnostic tools.
- Configure Windows Update.
- Configure data protection.

Configuring and troubleshooting mobile computing

- Configure mobile display settings.
- Configure mobile devices.
- Configure Tablet PC software.

- Configure power options.

Course: Installing, Configuring, and Administering Microsoft Windows XP Professional

Content:

Installing Windows XP Professional

- Perform and troubleshoot an attended installation of Windows XP Professional.
- Perform and troubleshoot an unattended installation of Windows XP Professional.
 - Install Windows XP Professional by using Remote Installation Services (RIS).
 - Install Windows XP Professional by using the System Preparation Tool.
 - Create unattended answer files by using Setup Manager to automate the installation of Windows XP Professional.
- Upgrade from a previous version of Windows to Windows XP Professional.
 - Prepare a computer to meet upgrade requirements.
 - Migrate existing user environments to a new installation.
- Perform post-installation updates and product activation.
- Troubleshoot failed installations.

Implementing and Conducting Administration of Resources

- Monitor, manage, and troubleshoot access to files and folders.
 - Configure, manage, and troubleshoot file compression.
 - Control access to files and folders by using permissions.
 - Optimize access to files and folders.
- Manage and troubleshoot access to shared folders.
 - Create and remove shared folders.
 - Control access to shared folders by using permissions.
 - Manage and troubleshoot Web server resources.
- Connect to local and network print devices.
 - Manage printers and print jobs.
 - Control access to printers by using permissions.
 - Connect to an Internet printer.
 - Connect to a local print device.
- Configure and manage file systems.
 - Convert from one file system to another file system.
 - Configure NTFS, FAT32, or FAT file systems.
- Manage and troubleshoot access to and synchronization of offline files.

Implementing, Managing, Monitoring, and Troubleshooting Hardware Devices and Drivers

- Implement, manage, and troubleshoot disk devices.
 - Install, configure, and manage DVD and CD-ROM devices.
 - Monitor and configure disks.
 - Monitor, configure, and troubleshoot volumes.
 - Monitor and configure removable media, such as tape devices.
- Implement, manage, and troubleshoot display devices.
 - Configure multiple-display support.
 - Install, configure, and troubleshoot a video adapter.
- Configure Advanced Configuration Power Interface (ACPI).

- Implement, manage, and troubleshoot input and output (I/O) devices.
 - Monitor, configure, and troubleshoot I/O devices, such as printers, scanners, multimedia devices, mouse, keyboard, and smart card reader.
 - Monitor, configure, and troubleshoot multimedia hardware, such as cameras.
 - Install, configure, and manage modems.
 - Install, configure, and manage Infrared Data Association (IrDA) devices.
 - Install, configure, and manage wireless devices.
 - Install, configure, and manage USB devices.
 - Install, configure, and manage hand held devices.
 - Install, configure, and manage network adapters.
- Manage and troubleshoot drivers and driver signing.
- Monitor and configure multiprocessor computers.

Monitoring and Optimizing System Performance and Reliability

- Monitor, optimize, and troubleshoot performance of the Windows XP Professional desktop.
 - Optimize and troubleshoot memory performance.
 - Optimize and troubleshoot processor utilization.
 - Optimize and troubleshoot disk performance.
 - Optimize and troubleshoot application performance.
 - Configure, manage, and troubleshoot Scheduled Tasks.
- Manage, monitor, and optimize system performance for mobile users.
- Restore and back up the operating system, System State data, and user data.
 - Recover System State data and user data by using Windows Backup.
 - Troubleshoot system restoration by starting in safe mode.
 - Recover System State data and user data by using the Recovery console.

Configuring and Troubleshooting the Desktop Environment

- Configure and manage user profiles and desktop settings.
- Configure support for multiple languages or multiple locations.
 - Enable multiple-language support.
 - Configure multiple-language support for users.
 - Configure local settings.
 - Configure Windows XP Professional for multiple locations.
- Manage applications by using Windows Installer packages.

Implementing, Managing, and Troubleshooting Network Protocols and Services

- Configure and troubleshoot the TCP/IP protocol.
- Connect to computers by using dial-up networking.
 - Connect to computers by using a virtual private network (VPN) connection.
 - Create a dial-up connection to connect to a remote access server.
 - Connect to the Internet by using dial-up networking.
 - Configure and troubleshoot Internet Connection Sharing (ICS).
- Connect to resources by using Internet Explorer.
- Configure, manage, and implement Internet Information Services (IIS).
- Configure, manage, and troubleshoot Remote Desktop and Remote Assistance.
- Configure, manage, and troubleshoot an Internet Connection Firewall (ICF).

Configuring, Managing, and Troubleshooting Security

- Configure, manage, and troubleshoot Encrypting File System (EFS).
- Configure, manage, and troubleshoot a security configuration and local security policy.
- Configure, manage, and troubleshoot local user and group accounts.
 - Configure, manage, and troubleshoot auditing.
 - Configure, manage, and troubleshoot account settings.
 - Configure, manage, and troubleshoot account policy.
 - Configure, manage, and troubleshoot user and group rights.
 - Troubleshoot cache credentials.
- Configure, manage, and troubleshoot Internet Explorer security settings.

Course: Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure

Content:

Creating the Conceptual Design by Gathering and Analyzing Business and Technical Requirements

- Analyze the impact of Active Directory on the existing technical environment.
 - Analyze hardware and software requirements.
 - Analyze interoperability requirements.
 - Analyze current level of service within an existing technical environment.
 - Analyze current network administration model.
 - Analyze network requirements.
- Analyze DNS for Active Directory directory service implementation.
 - Analyze the current DNS infrastructure.
 - Analyze the current namespace.
- Analyze existing network operating system implementation.
 - Identify the existing domain model.
 - Identify the number and location of domain controllers on the network.
 - Identify the configuration details of all servers on the network. Server types might include primary domain controllers, backup domain controllers, file servers, print servers, and Web servers.
- Analyze security requirements for the Active Directory directory service.
 - Analyze current security policies, standards, and procedures.
 - Identify the impact of Active Directory on the current security infrastructure.
 - Identify the existing trust relationships.
- 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.
- 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.
- Identify network topology and performance levels.
 - Identify constraints in the current network infrastructure.
 - Interpret current baseline performance requirements for each major subsystem.
- Analyze the impact of the infrastructure design on the existing technical environment.
 - Analyze hardware and software requirements.
 - Analyze interoperability requirements.
 - Analyze current level of service within the existing technical environment.
 - Analyze network requirements.

Creating the Logical Design for an Active Directory Infrastructure

- Design an OU structure.
 - Identify the Group Policy requirements for the OU structure.
 - Design an OU structure for the purpose of delegating authority.
- Design a security group strategy.
 - Define the scope of a security group to meet requirements.
 - Define resource access requirements.
 - Define administrative access requirements.
 - Define user roles.
- Design a user and computer authentication strategy.
 - Identify common authentication requirements.
 - Select authentication mechanisms.
 - Optimize authentication by using shortcut trust relationships.
- Design a user and computer account strategy.
 - Specify account policy requirements.
 - Specify account requirements for users, computers, administrators, and services.
- Design an Active Directory naming strategy.
 - Identify Internet domain name registration requirements.
 - Specify the use of hierarchical namespace within Active Directory.
 - Identify NetBIOS naming requirements.
- Design migration paths to Active Directory.
 - Define whether the migration will include an in-place upgrade, domain restructuring, or migration to a new Active Directory environment.
- Design a strategy for Group Policy implementation.
 - Design the administration of Group Policy objects (GPOs).
 - Design the deployment strategy of GPOs.
 - Create a strategy for configuring the user environment with Group Policy.
 - Create a strategy for configuring the computer environment with Group Policy.
- Design an Active Directory directory service site topology.
 - Design sites.
 - Identify site links.

Creating the Logical Design for a Network Services Infrastructure

- Design a DNS name resolution strategy.
 - Create the namespace design.
 - Identify DNS interoperability with Active Directory, WINS, and DHCP.

- Specify zone requirements.
- Specify DNS security.
- Design a DNS strategy for interoperability with UNIX Berkeley Internet Name Domain (BIND) to support Active Directory.
- Design a NetBIOS name resolution strategy.
 - Design a WINS replication strategy.
- Design security for remote access users.
 - Identify security host requirements.
 - Identify the authentication and accounting provider.
 - Design remote access policies.
 - Specify logging and auditing settings.
- Design a DNS service implementation.
 - Design a strategy for DNS zone storage.
 - Specify the use of DNS server options.
 - Identify the registration requirements of specific DNS records.
- Design a remote access strategy.
 - Specify the remote access method.
 - Specify the authentication method for remote access.
- Design an IP address assignment strategy.
 - Specify DHCP integration with DNS infrastructure.
 - Specify DHCP interoperability with client types.

Creating the Physical Design for an Active Directory and Network Infrastructure

- Design DNS service placement.
- Design an Active Directory implementation plan.
 - Design the placement of domain controllers and global catalog servers.
 - Plan the placement of flexible operations master roles.
 - Select the domain controller creation process.
- Specify the server specifications to meet system requirements.
- Design Internet connectivity for a company.
- Design a network and routing topology for a company.
 - Design a TCP/IP addressing scheme through the use of IP subnets.
 - Specify the placement of routers.
 - Design IP address assignment by using DHCP.
 - Design a perimeter network.
- Design the remote access infrastructure.
 - Plan capacity.
 - Ascertain network settings required to access resources.
 - Design for availability, redundancy, and survivability.

Course: Implementing and Managing Microsoft Exchange Server 2003

Content:

Installing, Configuring, and Troubleshooting Exchange Server 2003

- Prepare the environment for deployment of Exchange Server 2003
- Install, configure, and troubleshoot Exchange Server 2003
- Install, configure, and troubleshoot Exchange Server 2003 in a clustered environment
- Upgrade from Exchange Server 5.5 to Exchange Server 2003

- Migrate from other messaging systems to Exchange Server 2003
 - Use the Migration Wizard to migrate from other messaging systems
 - Migrate from other Exchange organizations
- Configure and troubleshoot Exchange Server 2003 for coexistence with other Exchange organizations
- Configure and troubleshoot Exchange Server 2003 for coexistence with other messaging systems
- Configure and troubleshoot Exchange Server 2003 for interoperability with other SMTP messaging systems

Managing, Monitoring, and Troubleshooting Exchange Server Computers

- Manage, monitor, and troubleshoot server health
- Manage, monitor, and troubleshoot data storage
- Manage, monitor, and troubleshoot Exchange Server clusters
- Perform and troubleshoot backups and recovery
- Remove an Exchange Server computer from the organization

Managing, Monitoring, and Troubleshooting the Exchange Organization

- Manage and troubleshoot public folders
- Manage and troubleshoot virtual servers
- Manage and troubleshoot front-end and back-end servers
- Manage and troubleshoot connectivity
- Monitor, manage, and troubleshoot infrastructure performance

Managing Security in the Exchange Environment

- Manage and troubleshoot connectivity across firewalls
- Manage audit settings and audit logs
- Manage and troubleshoot permissions
- Manage and troubleshoot encryption and digital signatures
- Detect and respond to security threats

Managing Recipient Objects and Address Lists

- Manage recipient policies
- Manage user objects
- Manage distribution and security groups
- Manage contacts
- Manage address lists

Managing and Monitoring Technologies that Support Exchange Server 2003

- Diagnose problems arising from host resolution protocols
- Diagnose problems arising from Active Directory issues
- Diagnose network connectivity problems

Exam(s):

70-290 Managing and Maintaining a Windows Server 2003 Environment
70-291 Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure
70-270 Installing, Configuring, and Administering Microsoft Windows XP Professional (or)
70-620 TS: Configuring Microsoft Windows Vista Client
70-284 Implementing and Managing Microsoft Exchange Server 2003
70-293 Planning and Maintaining a Windows Server 2003 Network Infrastructure
70-294 Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory Infrastructure
70-297 Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure