

MICROSOFT CERTIFIED SYSTEM ADMINISTRATOR(MCSA) Training program



A TRAINING PROGRAM IS DESIGNED AND DEVELOPED BY CERTIFIED AND EXPERIENCED TRAINERS

This highly specialized and concentrated Program is ideally suited to following individuals who are:

- **Fresh University Graduates and like to pursue a career in Computer's networking.**
- **Already working and interested to switch over to field in Networking.**
- **Already working in a Networking position and like to excel in terms of better position and compensation.**
- **Already working in a Network Position in Companies and want to get the certification in International market.**

Program is offered by: 3D Educators – Trainers & Consultants

Table of Contents

Detail

Inauguration

Structure

Topics & Time Allocation

Other Learning Activities

About the Program Designer & Instructor

Syllabus

3D EDUCATORS

TRAINERS & CONSULTANTS

Program Details

Inauguration

The Training Program will be inaugurated by a senior member of 3DEducators

Program Structure

Number of classes in a week	Three Class Per Week
Duration of each class	2 - Hour
Fee Per Paper:	Rs.2800/- Only
Total Paper	Six
Total Fee	Rs.16800/- Only

Other Learning Activities:

Classroom Assignments	2
Presentations by Trainees	2

About the Program Designer & Instructor

The Profile of Program Designers & Instructors is given below:

The “**Microsoft Certified System Administrator**” Program has been designed by the Microsoft Company as an International Certification. Where its credibility is so high and people will earn the international recognition after having this course and certification. This course is conducted by the Senior Network Administrators and Network Managers,

The Person are qualified and certified in Networking and MCS and MCSE, MCSA.

At present, faculty is working with FMCG in a senior position, also involved in training and development for last ten years.

3D EDUCATORS

TRAINERS & CONSULTANTS

Program Syllabus

- ❖ Managing and Maintaining a Windows Server 2003 Environment, Skills measured by Exam 70-290
- ❖ Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure, Skills measured by Exam 70-291
- ❖ Installing, Configuring, and Administering Microsoft Windows XP Professional, Skills measured by Exam 70-270
- ❖ Implementing and Managing Microsoft Exchange Server 2003, Skills measured by exam 70-284
- ❖ Implementing Microsoft Internet Security and Acceleration (ISA) Server 2004, Skills measured by Exam 70-350
- ❖ Implementing and Administering Security in a Microsoft Windows Server 2003 Network, Skills measured by exam 70-299

3D EDUCATORS

TRAINERS & CONSULTANTS

DETAIL OUTLINE

Course Outline of MCSA (Messaging and Security)

Managing and Maintaining a Windows Server 2003 Environment Skills measured by Exam 70-290

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 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.

Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Skills measured by Exam 70-291

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.

Installing, Configuring, and Administering Microsoft Windows XP Professional

Skills measured by Exam 70-270

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.

Implementing and Managing Microsoft Exchange Server 2003

Skills measured by exam 70-284

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.

Implementing Microsoft Internet Security and Acceleration (ISA) Server 2004

Skills measured by Exam 70-350

Planning and Installing ISA Server 2004
Plan an ISA Server 2004 deployment
Assess and configure the operating system, hardware, and network services
Deploy ISA Server 2004
Installing and Configuring Client Computers
Install Firewall Client software
Configure client computers for ISA Server 2004. Types of client computers include Web Proxy, Firewall Client, and SecureNAT
Configure a local domain table (LDT)
Configure ISA Server 2004 for automatic client configuration by using Web Proxy Automatic Discovery (WPAD)
Diagnose and resolve client computer connectivity issues
Configuring and Managing ISA Server 2004
Configure the system policy
Back up and restore ISA Server 2004
Define administrative roles
Configure firewall settings
Configure ISA Server 2004 for Network Load Balancing
Configure ISA Server 2004 to support a network topology
Configuring Web Caching
Configure forward and reverse caching
Optimize performance of the ISA Server 2004 cache

Diagnose and resolve caching issues
Configuring Firewall Policy
Plan a firewall policy
Create policy elements, access rules, and connection limits. Policy elements include schedule, protocols, user groups, and network objects
Create policy rules for Web publishing
Create policy rules for mail server publishing
Create policy rules for server publishing
Configuring and Managing Remote Network Connectivity
Configure ISA Server 2004 for site-to-site VPNs
Configure ISA Server 2004 as a remote access VPN server
Diagnose and resolve VPN connectivity issues
Monitoring and Reporting ISA Server 2004 Activity
Monitor ISA Server 2004 activity
Configure and run reports
Configure logging and alerts.

Implementing and Administering Security in a Microsoft Windows Server 2003 Network Skills measured by exam 70-299

Implementing, Managing, and Troubleshooting Security Policies

Plan security templates based on computer role. Computer roles include SQL Server computer, Microsoft Exchange Server computer, domain controller, Internet Authentication Service (IAS) server, and Internet Information Services (IIS) server.

Configure security templates.

- Configure registry and file system permissions.
- Configure account policies.
- Configure .pol files.
- Configure audit policies.
- Configure user rights assignment.
- Configure security options.
- Configure system services.
- Configure restricted groups.
- Configure event logs.

Deploy security templates.

- Plan the deployment of security templates.
- Deploy security templates by using Active Directory-based Group Policy objects (GPOs).
- Deploy security templates by using command-line tools and scripting.

Troubleshoot security template problems.

- Troubleshoot security templates in a mixed operating system environment.
- Troubleshoot security policy inheritance.
- Troubleshoot removal of security template settings.

Configure additional security based on computer roles. Server computer roles include SQL Server computer, Exchange Server computer, domain controller, Internet Authentication Service (IAS) server, and Internet Information Services (IIS) server. Client computer roles include desktop, portable, and kiosk.

- Plan and configure security settings.
- Plan network zones for computer roles.
- Plan and configure software restriction policies.

- Plan security for infrastructure services. Services include DHCP and DNS.
- Plan and configure auditing and logging for a computer role. Considerations include Windows Events, Internet Information Services (IIS), firewall log files, Netlog, and RAS log files.
- Analyze security configuration. Tools include Microsoft Baseline Security Analyzer (MBSA), the MBSA command-line tool, and Security Configuration and Analysis.

Implementing, Managing, and Troubleshooting Patch Management Infrastructure

Plan the deployment of service packs and hotfixes.

- Evaluate the applicability of service packs and hotfixes.
- Test the compatibility of service packs and hotfixes for existing applications.
- Plan patch deployment environments for both the pilot and production phases.
- Plan the batch deployment of multiple hotfixes.
- Plan rollback strategy.

Assess the current status of service packs and hotfixes. Tools include MBSA and the MBSA command-line tool.

- Assess current patch levels by using the MBSA GUI tool.
- Assess current patch levels by using the MBSA command-line tool with scripted solutions.

Deploy service packs and hotfixes.

- Deploy service packs and hotfixes on new servers and client computers. Considerations include slipstreaming, custom scripts, and isolated installation or test networks.
- Deploy service packs and hotfixes on existing servers and client computers.

Implementing, Managing, and Troubleshooting Security for Network Communications

Plan IPsec deployment.

- Decide which IPsec mode to use.
- Plan authentication methods for IPsec.
- Test the functionality of existing applications and services.

Configure IPsec policies to secure communication between networks and hosts. Hosts include domain controllers, Internet Web servers, databases, e-mail servers, and client computers.

- Configure IPsec authentication.
- Configure appropriate encryption levels. Considerations include the selection of perfect forward secrecy (PFS) and key lifetimes.
- Configure the appropriate IPsec protocol. Protocols include Authentication Header (AH) and Encapsulating Security Payload (ESP).
- Configure IPsec inbound and outbound filters and filter actions.

Deploy and manage IPsec policies.

- Deploy IPsec policies by using Local policy objects or Group Policy objects (GPOs).
- Deploy IPsec policies by using commands and scripts. Tools include IPsecPol and NetSh.
- Deploy IPsec certificates. Considerations include deployment of certificates and renewing certificates on managed and unmanaged client computers.

Troubleshoot IPsec.

- Monitor IPsec policies by using IP Security Monitor.
- Configure IPsec logging. Considerations include Oakley logs and IPsec driver logging.
- Troubleshoot IPsec across networks. Considerations include network address translation, port filters, protocol filters, firewalls, and routers.
- Troubleshoot IPsec certificates. Considerations include enterprise trust policies and certificate revocation list (CRL) checking.

Plan and implement security for wireless networks.

- Plan the authentication methods for a wireless network.
- Plan the encryption methods for a wireless network.

- Plan wireless access policies.
- Configure wireless encryption.
- Install and configure wireless support for client computers.

Deploy, manage, and configure SSL certificates, including uses for HTTPS, LDAPS, and wireless networks. Considerations include renewing certificates and obtaining self-issued certificates instead of publicly issued certificates.

- Obtain self-issued certificates and publicly issued certificates.
- Install certificates for SSL.
- Renew certificates.
- Configure SSL to secure communication channels. Communication channels include client computer to Web server, Web server to SQL Server computer, client computer to Active Directory domain controller, and e-mail server to client computer.

Configure security for remote access users.

- Configure authentication for secure remote access. Authentication types include PAP, CHAP, MS-CHAP, MS-CHAP v2, EAP-MD5, EAP-TLS, and multifactor authentication that combines smart cards and EAP.
- Configure and troubleshoot virtual private network (VPN) protocols. Considerations include Internet service provider (ISP), client operating system, network address translation devices, Routing and Remote Access servers, and firewall servers.
- Manage client configuration for remote access security. Tools include remote access policy and the Connection Manager Administration Kit.

Planning, Configuring, and Troubleshooting Authentication, Authorization, and PKI

Plan and configure authentication.

- Plan, configure, and troubleshoot trust relationships.
- Plan and configure authentication protocols.
- Plan and configure multifactor authentication.
- Plan and configure authentication for Web users.
- Plan and configure delegated authentication.

Plan group structure.

- Decide which types of groups to use.
- Plan security group scope.
- Plan nested group structure.

Plan and configure authorization.

- Configure access control lists (ACLs).
- Plan and troubleshoot the assignment of user rights.
- Plan requirements for digital signatures.

Install, manage, and configure Certificate Services.

- Install and configure root, intermediate, and issuing certification authorities (CAs). Considerations include renewals and hierarchy.
- Configure certificate templates.
- Configure, manage, and troubleshoot the publication of certificate revocation lists (CRLs).
- Configure archival and recovery of keys.
- Deploy and revoke certificates to users, computers, and CAs.
- Backup and restore the CA.