SOFTCRAYONS
Tech Solutions Pvt. Ltd.

MCSE

MCSE

@softcrayons

About Course

An MCSE (Microsoft Certified Systems Engineer) is someone who has passed exams about the Microsoft Windows NT operating system, related desktop systems, networking, and Microsoft's BackOffice server products.

MCSE

CURRICULUM

1 Installing, Configuring servers

Introducing Windows Server
Preparing and installing Nano Server and Server Core

2 Configuring local storage

Managing disks in Windows Server
Managing volumes in Windows Server

3 Implementing enterprise storage solutions

Configuring sharing in Windows Server
Configuring iSCSI

4 Implementing Storage Data Deduplication

Implementing Storage
Managing Storage
Implementing Data Deduplication

5 Installing and configuring Hyper-V and virtual machines

Overview of Hyper-V

Installing Hyper-V
Configuring storage on Hyper-V host servers
Configuring networking on Hyper-V host servers

6 Deploying and managing Windows and Hyper-V

Configuring Hyper-V virtual machines
Managing virtual machines

7 Overview of high availability and disaster

Defining levels of availability of Domain Controllers
Backing up and restoring by using Windows Server Backup

8 Implementing failover clustering

Planning a failover DHCP cluster
Creating and configuring a new failover cluster
Maintaining a failover cluster

9 Implementing, Planning FSMO Roles

FSMO Roles and their transfer
Seizing roles

10 Implementing Network Load Balancing

Overview of NLB
Configuring an NLB cluster

Planning an NLB implementation

11 Creating and managing deployment OS (WDS)

Introduction to deployment os images
Creating and managing deployment images

12 Managing, monitoring Servers

Overview of Windows Server 2016 monitoring tools
Using Performance Monitor
Monitoring event logs

Networking with Windows Server

1 Planning and implementing an IPv4 network

Planning IPv4 addressing
Configuring an IPv4 host
Managing and troubleshooting IPv4 network connectivity

2 Implementing DHCP

Overview of the DHCP server role
Deploying DHCP
Managing and troubleshooting DHCP

3 Implementing IPv6

- Overview of IPv6 addressing
- Configuring an IPv6 host

4 Implementing DNS

- Implementing DNS servers
- Configuring zones in DNS
- Configuring name resolution between DNS zones
- Configuring DNS integration with Active Directory Domain Services (AD DS)
- Configuring advanced DNS settings

5 Implementing and managing IPAM

- Overview of IPAM
- Deploying IPAM
- Managing IP address spaces by using IPAM

6 Remote access in Windows Server 2016

- Overview of remote access
- Implementing the Web Application Proxy

7 Implementing DirectAccess

- Overview of DirectAccess

- Implementing DirectAccess by using the Getting Started Wizard
- Implementing and managing an advanced DirectAccess infrastructure

8 Implementing VPNs

- Planning VPNs
- Implementing VPNs

9 Implementing networking for branch offices

- Networking features and considerations for branch offices
- Implementing Distributed File System (DFS) for branch offices
- Implementing BranchCache for branch offices

10 Configuring advanced networking features

- Overview of high performance networking features
- NIC Teaming

Identity with Windows Server 2016

1 Installing and configuring domain controllers

- Overview of AD DS
- Overview of AD DS domain controllers
- Deploying a domain controller

2 Managing objects in AD DS

- Managing user accounts
- Managing groups in AD DS
- Managing computer objects in AD DS
- Using Windows PowerShell for AD DS administration
- Implementing and managing OUs

3 Advanced AD DS infrastructure management

- Overview of advanced AD DS deployments
- Deploying a distributed AD DS environment
- Configuring AD DS trusts

4 Implementing and administering AD DS sites and replication

- Overview of AD DS replication
- Configuring AD DS sites
- Configuring and monitoring AD DS replication

5 Implementing Group Policy

Introducing Group Policy
Implementing and administering GPOs

6 Managing user settings with Group Policy

Implementing administrative templates
Configuring Folder Redirection, software installation, and scripts

7 Configure and Manage Remote Desktop Services(RDS)

Configure RDS
Publishing Apps to users

8 Deploying and managing AD CS

Deploying CAs
Administering CAs
Troubleshooting and maintaining CAs

9 Deploying and managing certificates

How to deploy and manage certificates in an AD DS environment

Deploying and managing certificate templates.

10 Implementing and administering AD FS

Overview of AD FS
AD FS requirements and planning
Deploying and configuring AD FS

11 Implementing and administering AD RMS

Overview of AD RMS
Deploying and managing an AD RMS infrastructure

12 Managing the Active Directory database

Managing the Active Directory database
Integrity check and optimization

SECURING WINDOWS SERVER 2016

1 Deploy BitLocker Drive Encryption

Configure BitLocker Group Policy settings
Configure BitLocker on Storage
Configure the EFS data recovery agent

2 Install and configure WSUS

Create computer groups and configure Automatic Update
Manage updates using WSUS
Troubleshoot WSUS configuration and deployment

3 Configuring Windows Defender through Group Policy

Scheduled Scan
Specify The Time Of Day To Run A Scheduled Scan
Allow Users To Pause Scan

4 Implement AppLocker rules

Use this procedure to configure our AppLocker rules from an Active Directory-based Group Policy Object on a Windows Server 2016 domain controller.

5 Blocking NT LAN Manager (NTLM) authentication protocol

Network Security: Restrict NTLM: NTLM Authentication In This Domain
Network Security: Restrict NTLM: Incoming NTLM Traffic
Network Security: Restrict NTLM: Outgoing NTLM Traffic To Remote Servers

- Network Security: Restrict NTLM: Audit NTLM Authentication In This Domain
- Network Security: Restrict NTLM: Audit Incoming NTLM Traffic

6 Configure Windows Firewall Allow an app or feature through Windows Firewall

- Turn Windows Firewall on or off This option allows you to enable or disable Windows Firewall for each network location profile.
- Advanced settings with Advanced Firewall Security Settings

7 Configure Security Policy to harden Server Access

- User Rights Assignment
- User Account Policies
- Blocking Devices
- Create File Screens in FSRM
- Restrict local logon access to Administrators

8 Additional Security Protection

- Disable or uninstall unused services.

Disable or delete unused users.
Follow the Principle of Least Privilege
Ensure all volumes are using the NTFS file system.

9 Microsoft Baseline Security Analyzer

detailing missing patches
performs checks on basic security settings
Evaluate information on remediating any issues found

10 Implementing DNS Security

zone to be signed cryptographically
spoofing and cache-tampering
secure DNS infrastructure

SOFTCRAYONS Tech Solutions Pvt. Ltd.
www.softcrayons.com
info@softcrayons.com
(+91) 854 501 2345
693, Sector 14-A, Vasundhara, Ghaziabad (U.P.), 201012
@softcrayons