TechyEdz Solutions

Training | Consulting | Developement | Outsourcing

Front MCSE 2016

9032803832

9032803832

contact@techyedz.com

www.techyedz.com

Microsoft Certified Solutions Expert (MCSE 2016)

MCSA – 2016 (70-740, 70-741 & 70742)

1. 70-740: Installation, Storage, and Compute with Windows Server 2016
2. 70-741: Networking with Windows Server 2016
3. 70-742: Identity with Windows Server 2016

MCSE-2016 (70-743 & 70-744)

4. 70-743: Upgrading Your Skills to MCSA: Windows Server 2016
5. 70-744: Securing Windows Server 2016

Upgrading Your Skills to MCSA: Windows Server 2016 (70-743)

- **Course Overview:**

Candidates for this exam are IT professionals who implement the Windows Server 2016 core infrastructure services. Candidates have already earned an MCSA: Windows Server 2008 or MCSA: Windows Server 2012 R2 certification. This exam covers key aspects of installation, storage, compute, networking, and identity functionality available in Windows Server 2016.

- **Course Outline:**

Install Windows Servers in Host and Compute Environments

Install, upgrade, and migrate servers and workloads

- Determine Windows Server 2016 installation requirements
- determine appropriate Windows Server 2016 editions per workloads
- install Windows Server 2016; install Windows Server 2016 features and roles
- install and configure Windows Server Core

- manage Windows Server Core installations using Windows PowerShell, command line, and remote management capabilities
- implement Windows PowerShell Desired State Configuration (DSC) to install and maintain integrity of installed environments
- perform upgrades and migrations of servers and core workloads from Windows Server 2008 and Windows Server 2012 to Windows Server 2016
- determine the appropriate activation model for server installation, such as Automatic Virtual Machine Activation (AVMA), Key Management Service (KMS), and Active Directory-based Activation

Create, manage, and maintain images for deployment

- Plan for Windows Server virtualization
- assess virtualization workloads using the Microsoft Assessment and Planning (MAP) Toolkit
- determine considerations for deploying workloads into virtualized environments
- update images with patches, hotfixes, last cumulative updates and drivers; install roles and features in offline images
- manage and maintain Windows Server Core, Nano Server images, and VHDs using Windows PowerShell

Implement Storage Solutions Implement server storage

- Configure storage pools
- implement simple, mirror, and parity storage layout options for disks or enclosures
- expand storage pools
- configure Tiered Storage
- configure iSCSI target and initiator
- configure iSNS
- configure Datacenter Bridging (DCB)
- configure Multi-Path IO (MPIO)
- determine usage scenarios for Storage Replica

- implement Storage Replica for server-to- server, cluster-to-cluster, and stretch cluster scenarios

Implement data deduplication

- Implement and configure Deduplication
- determine appropriate usage scenarios for Deduplication
- monitor Deduplication
- implement a backup and restore solution with Deduplication

Implement Hyper-V

Install and configure Hyper-V

- Determine hardware and compatibility requirements for installing Hyper-V
- install Hyper-V
- install management tools
- upgrade from existing versions of Hyper-V
- delegate virtual machine management
- perform remote management of Hyper-V hosts
- using Windows PowerShell Direct
- implement nested virtualization

Configure virtual machine (VM) settings

- Add or remove memory in a running VM
- configure dynamic memory
- configure Non-Uniform Memory Access (NUMA) support
- configure smart paging
- configure Resource Metering
- manage Integration Services
- create and configure Generation 1 and 2 VMs and determine appropriate usage scenarios
- implement enhanced session mode

- create Linux and FreeBSD VMs
- install and configure Linux Integration Services (LIS)
- install and configure FreeBSD Integration Services (BIS)
- implement Secure Boot for Windows and Linux environments
- move and convert VMs from previous versions of Hyper-V to Windows Server 2016 Hyper-V
- export and import VMs
- implement Discrete Device Assignment (DDA), Troubleshoot VM configuration versions

Configure Hyper-V storage

- Create VHDs and VHDX files using Hyper-V Manager
- create shared VHDX files
- configure differencing disks
- modify virtual hard disks
- configure pass-through disks
- resize a virtual hard disk
- manage checkpoints
- implement production checkpoints
- implement a virtual Fibre Channel adapter
- configure storage Quality of Service (QoS)

Configure Hyper-V networking

- Add and remove virtual network interface cards (vNICs)
- configure Hyper-V virtual switches
- optimize network performance
- configure MAC addresses
- configure network isolation
- configure synthetic and legacy virtual network adapters

- configure NIC teaming in VMs
- configure virtual machine queue (VMQ)
- enable Remote Direct Memory Access (RDMA) on network adapters bound to a Hyper-V virtual switch using Switch Embedded Teaming (SET)
- configure Bandwidth Management Implement Windows Containers

Deploy Windows containers

- Determine installation requirements and appropriate scenarios for Windows Containers
- install and configure Windows Server container host in physical or virtualized environments
- install and configure Windows Server container host configure Docker start-up options
- install a base container image
- tag an image
- remove a container
- create Windows Server containers
- create Hyper-V containers

Manage Windows containers

- Manage Windows containers by using Docker CLI manage container networking
- manage container data volumes
- manage Resource Control
- create new container images using Dockerfile
- manage container images using DockerHub repository for public and private scenarios
- manage container images using Microsoft Azure

Implement High Availability

Implement high availability and disaster recovery options in Hyper-V

- Implement Hyper-V Replica
- implement Live Migration including shared nothing Live Migration
- configure CredSSP or Kerberos authentication protocol for Live Migration
- implement storage migration

Implement failover clustering

- Implement Workgroup, Single, and Multi Domain clusters
- configure quorum
- configure cluster networking
- restore single node or cluster configuration
- configure cluster storage
- implement Cluster-Aware Updating
- implement Cluster Operating System Rolling Upgrade
- configure and optimize cluster shared volumes (CSVs)
- configure clusters without network names
- implement Scale-Out File Server (SoFS)
- determine different scenarios for the use of SoFS vs. File Server for general use
- determine usage scenarios for implementing guest clustering
- implement a Clustered Storage Spaces solution using Shared SAS storage enclosures
- implement Storage Replica
- implement Cloud Witness
- implement VM resiliency
- implement shared VHDX as a storage solution for guest clusters

Implement Storage Spaces Direct

- Determine scenario requirements for implementing Storage Spaces Direct
- enable Storage Spaces Direct using Windows PowerShell
- implement a disaggregated Storage Spaces Direct scenario
- implement a hyper-converged Storage Spaces Direct scenario

Manage failover clustering

- Configure role-specific settings, including continuously available shares
- configure VM monitoring
- configure failover and preference settings
- implement stretch and site-aware failover clusters
- enable and configure node fairness

Manage VM movement in clustered nodes

- Perform live migration
- perform quick migration
- perform storage migration
- import, export, and copy VMs
- configure VM network health protection
- configure drain on shutdown

Implement Domain Name System (DNS)

Install and configure DNS servers

- Determine DNS installation requirements
- determine supported DNS deployment scenarios on Nano Server
- install DNS
- configure forwarders
- configure Root Hints
- configure delegation
- implement DNS policies
- Configure DNS Server settings using Windows PowerShell
- configure Domain Name System Security Extensions (DNSSEC)
- configure DNS Socket Pool

- configure cache locking
- enable Response Rate Limiting
- configure DNS-based Authentication of Named Entities (DANE)
- configure DNS logging
- configure delegated administration
- configure recursion settings
- implement DNS performance tuning
- configure global settings

Implement and Maintain IP Address Management (IPAM)

- Provision IPAM manually or by using Group Policy
- configure server discovery
- create and manage IP blocks and ranges
- monitor utilization of IP address space
- migrate existing workloads to IPAM
- configure IPAM database storage using SQL Server
- determine scenarios for using IPAM with System Center Virtual Machine Manager for physical and virtual IP address space management
- manage DHCP server properties using IPAM; configure DHCP scopes and options
- configure DHCP policies and failover
- manage DNS server properties using IPAM
- manage DNS zones and records
- manage DNS and DHCP servers in multiple Active Directory forests

- delegate administration for DNS and DHCP using role-based access control (RBAC)
- audit the changes performed on the DNS and DHCP servers
- audit the IPAM address usage trail
- audit DHCP lease events and user logon events

Implement Network Connectivity and Remote Access Solutions

Implement virtual private network (VPN) and DirectAccess solutions

- Implement remote access and site-to-site (S2S) VPN solutions using remote access gateway
- configure different VPN protocol options
- configure authentication options
- configure VPN reconnect
- create and configure connection profiles
- determine when to use remote access VPN and site-to-site VPN and configure appropriate protocols
- install and configure DirectAccess
- implement server requirements
- implement client configuration
- troubleshoot DirectAccess

Implement an Advanced Network Infrastructure

Implement high performance network solutions

- Implement NIC Teaming or the Switch Embedded Teaming (SET) solution and identify when to use each
- enable and configure Receive Side Scaling (RSS)
- enable and configure network Quality of Service (QoS) with Data Center Bridging (DCB)
- enable and configure SMB Direct on Remote Direct Memory Access (RDMA)

enabled network adapters

- configure SMB Multichannel
- enable and configure virtual Receive Side Scaling (vRSS) on a Virtual Machine Queue (VMQ) capable network adapter
- enable and configure Virtual Machine Multi-Queue (VMMQ)
- enable and configure Single-Root I/O Virtualization (SR-IOV) on a supported network adapter

Determine scenarios and requirements for implementing Software Defined Networking (SDN)

- Determine deployment scenarios and network requirements for deploying SDN
- determine requirements and scenarios for implementing Hyper-V Network Virtualization (HNV) using Network Virtualization Generic Route Encapsulation (NVGRE) encapsulation or VirtualExtensible LAN (VXLAN) encapsulation
- determine scenarios for implementation of Software Load Balancer (SLB) for North-South and East-West load balancing
- determine implementation scenarios for various types of Windows Server Gateways, including L3, GRE, and S2S, and their use; determine requirements and scenarios for Datacenter firewall policies and network security groups

Install and Configure Active Directory Domain Services (AD DS)

Install and configure domain controllers

- Install a new forest
- add or remove a domain controller from a domain
- upgrade a domain controller
- install AD DS on a Server Core installation
- install a domain controller from Install from Media (IFM)
- resolve DNS SRV record registration issues
- configure a global catalog server
- transfer and seize operations master roles

- install and configure a read-only domain controller (RODC)
- configure domain controller cloning

Implement identity federation and access solutions

Install and configure Active Directory Federation Services (AD FS)

- Upgrade and migrate previous AD FS workloads to Windows Server 2016
- implement claims- based authentication, including Relying Party Trusts
- configure authentication policies
- configure multi-factor authentication
- implement and configure device registration
- integrate AD FS with Microsoft Passport
- configure for use with Microsoft Azure and Office 365
- configure AD FS to enable authentication of users stored in LDAP directories

Implement Web Application Proxy (WAP)

- Install and configure WAP
- implement WAP in pass-through mode
- implement WAP as AD FS proxy
- integrate WAP with AD FS
- configure AD FS requirements
- publish web apps via WAP
- publish Remote Desktop Gateway applications
- configure HTTP to HTTPS redirects
- configure internal and external Fully Qualified Domain Names (FQDNs)

Securing Windows Server 2016 (70-744)

Course Overview:

Candidates for this exam secure Windows Server 2016 environments. Candidates are familiar with the methods and technologies used to harden server environments and secure virtual machine infrastructures using Shielded and encryption-supported virtual machines and Guarded Fabric. Candidates manage the protection of Active Directory and Identity infrastructures and manage privileged identities using Just in Time (JIT) and Just Enough Administration (JEA) approaches, as well as implement Privileged Access Workstations (PAWs) and secure servers using the Local Administrator Password Solution (LAPS). Candidates should also be able to use threat detection solutions such as auditing access, implementing Advanced Threat Analytics (ATA), deploying Operations Management Suite (OMS) solutions, and identifying solutions for specific workloads.

Course Outline:

Implement Server Hardening Solutions (25-30%)

Configure disk and file encryption

- Determine hardware and firmware requirements for secure boot and encryption key functionality
- deploy BitLocker encryption
- deploy BitLocker without a Trusted Platform Module (TPM)
- deploy BitLocker with a TPM only
- configure the Network Unlock feature
- configure BitLocker Group Policy settings
- enable Bitlocker to use secure boot for platform and BCD integrity validation
- configure BitLocker on Cluster Shared Volumes (CSVs) and Storage Area Networks (SANs)
- implement BitLocker Recovery Process using self-recovery and recovery password retrieval solutions
- configure Bitlocker for virtual machines (VMs) in Hyper-V

- determine usage scenarios for Encrypting File System (EFS)
- configure the EFS recovery agent
- manage EFS and BitLocker certificates, including backup and restore

Implement malware protection

- Implement antimalware solution with Windows Defender
- integrate Windows Defender with WSUS and Windows Update
- configure Windows Defender using Group Policy
- configure Windows Defender scans using Windows PowerShell
- implement AppLocker rules
- implement AppLocker rules using Windows PowerShell
- implement Control Flow Guard
- implement Code Integrity (Device Guard) Policies
- create Code Integrity policy rules
- create Code Integrity file rules

Protect credentials

- Determine requirements for implementing Credential Guard
- configure Credential Guard using Group Policy, WMI, command prompt, and Windows PowerShell
- implement NTLM blocking

Create security baselines

- Install and configure Microsoft Security Compliance Toolkit
- create, view, and import security baselines
- deploy configurations to domain and non-domain joined servers

Secure a Virtualization Infrastructure

Implement a Guarded Fabric solution

- Install and configure the Host Guardian Service (HGS)

- configure Admin-trusted attestation
- configure TPM-trusted attestation
- configure the Key Protection Service using HGS
- migrate Shielded VMs to other guarded hosts
- troubleshoot guarded hosts

Implement Shielded and encryption-supported VMs

- Determine requirements and scenarios for implementing Shielded VMs
- create a shielded VM using only a Hyper-V environment
- enable and configure vTPM to allow an operating system and data disk encryption within a VM
- determine requirements and scenarios for implementing encryption-supported VMs
- troubleshoot Shielded and encryption-supported VMs

Secure a Network Infrastructure

Configure Windows Firewall

- Configure Windows Firewall with Advanced Security
- configure network location profiles
- configure and deploy profile rules
- configure firewall rules for multiple profiles using Group Policy
- configure connection security rules using Group Policy, the GUI management console, or Windows PowerShell
- configure Windows Firewall to allow or deny applications, scopes, ports, and users using Group Policy, the GUI management console, or Windows PowerShell
- configure authenticated firewall exceptions
- import and export settings

Implement a Software Defined Datacenter Firewall

- Determine requirements and scenarios for Datacenter Firewall implementation

with Software Defined Networking

- determine usage scenarios for Datacenter Firewall policies and network security groups
- Configure Datacenter Firewall Access Control Lists

Secure network traffic

- Configure IPsec transport and tunnel modes
- configure IPsec authentication options
- configure connection security rules
- implement isolation zones
- implement domain isolation
- implement server isolation zones
- determine SMB 3.1.1 protocol security scenarios and implementations
- enable SMB encryption on SMB Shares
- configure SMB signing via Group Policy
- disable SMB 1.0
- secure DNS traffic using DNSSEC and DNS policies
- install and configure Microsoft Message Analyzer (MMA) to analyze network traffic

Manage Privileged Identities

Implement Just-In-Time (JIT) Administration

- Create a new administrative (bastion) forest in an existing Active Directory environment using Microsoft Identity Manager (MIM)
- configure trusts between production and bastion forests
- create shadow principals in bastion forest
- configure the MIM Web portal
- request privileged access using the MIM Web portal

- determine requirements and usage scenarios for Privileged Access Management (PAM) solutions
- create and Implement MIM policies
- implement Just-in-Time administration principals using time-based policies
- request privileged access using Windows PowerShell

Implement Just-Enough-Administration (JEA)

- Enable a JEA solution on Windows Server 2016
- create and configure session configuration files
- create and configure role capability files
- create a JEA endpoint
- connect to a JEA endpoint on a server for administration
- view logs
- download WMF 5.1 to a Windows Server 2008 R2
- configure a JEA endpoint on a server using Desired State Configuration (DSC)

Implement Privileged Access Workstations (PAWs) and User Rights Assignments

- Implement a PAWS solution
- configure User Rights Assignment group policies
- configure security options settings in Group Policy
- enable and configure Remote Credential Guard for remote desktop access
- Implement an Enhanced Security Administrative Environment (ESAE) administrative forest design approach
- Determine usage scenarios and requirements for implementing ESAE forest design architecture to create a dedicated administrative forest

Implement Local Administrator Password Solution (LAPS)

- Install and configure the LAPS tool
- secure local administrator passwords using LAPS
- manage password parameters and properties using LAPS

Implement Threat Detection Solutions

Configure advanced audit policies

- Determine the differences and usage scenarios for using local audit policies and advanced auditing policies
- implement auditing using Group Policy and AuditPol.exe
- implement auditing using Windows PowerShell
- create expression-based audit policies
- configure the Audit PNP Activity policy
- configure the Audit Group Membership policy
- enable and configure Module, Script Block, and Transcription logging in Windows PowerShell

Install and configure Microsoft Advanced Threat Analytics (ATA)

- Determine usage scenarios for ATA
- determine deployment requirements for ATA
- install and configure ATA Gateway on a dedicated server
- install and configure ATA Lightweight Gateway directly on a domain controller
- configure alerts in ATA Center when suspicious activity is detected
- review and edit suspicious activities on the attack time line

Determine threat detection solutions using Operations Management Suite (OMS)

- Determine usage and deployment scenarios for OMS
- determine security and auditing functions available for use
- determine Log Analytics usage scenarios

Implement Workload-Specific Security

Secure application development and server workload infrastructure

- Determine usage scenarios, supported server workloads, and requirements for

deployments

- determine usage scenarios and requirements for Windows Server and Hyper-V containers
- install and configure containers

Implement a secure file services infrastructure and Dynamic Access Control (DAC)

- Install the File Server Resource Manager (FSRM) role service
- configure quotas
- configure file screens
- configure storage reports
- configure file management tasks
- configure File Classification Infrastructure (FCI) using FSRM
- implement work folders
- configure file access auditing
- configure user and device claim types
- implement policy changes and staging
- perform access-denied remediation
- create and configure Central Access rules and policies
- create and configure resource properties and lists

Prerequisites:

- An understanding of TCP/IP and networking concepts.
- A good working knowledge of both Windows Server 2012 R2 and Active Directory® Domain Services (AD DS). For example, domain user accounts, domain vs. local user accounts, user profiles, and group membership.
- An understanding of scripts and batch files.
- An understanding of security concepts such as authentication and authorization.

- An understanding of deployment, packaging, and imaging tools.
- Experience working in a team or a virtual team.
- Achieved the Windows Server 2012 MCSA certification as well as information in the course 20413C: Designing and Implementing an Enterprise Server Infrastructure

Who Should Attend:

- Who have knowledge about MCSA (Microsoft Certified Solutions Associate)
- Candidates for this exam are IT professionals who implement the Windows Server 2016 core infrastructure services.
- Candidates have already earned an MCSA: Windows Server 2008 or MCSA: Windows Server 2012 R2 certification. This exam covers key aspects of installation, storage, compute, networking, and identity functionality available in Windows Server 2016.
- Candidates for this exam secure Windows Server 2016 environments. Candidates are familiar with the methods and technologies used to harden server environments and secure virtual machine infrastructures using Shielded and encryption-supported virtual machines and Guarded Fabric.
- Candidates manage the protection of Active Directory and Identity infrastructures and manage privileged identities using Just in Time (JIT) and Just Enough Administration (JEA) approaches, as well as implement Privileged Access Workstations (PAWs) and secure servers using the Local Administrator Password Solution (LAPS).
- Candidates should also be able to use threat detection solutions such as auditing access, implementing Advanced Threat Analytics (ATA), deploying Operations

Management Suite (OMS) solutions, and identifying solutions for specific workloads.

- **Number of Hours: 50hrs**

- **Certification: 70-743, 70-744**

- **Key Features:**

- One to One Training
- Online Training
- Fastrack & Normal Track
- Resume Modification
- Mock Interviews
- Video Tutorials
- Materials
- Real Time Projects
- Virtual Live Experience
- Preparing for Certification