MCSE Core Infrastructure Certification Training Curriculum

STRUCTURE

MCSE Core Infrastructure Certification Course Content

This Certification validates your skills needed to run a highly efficient and modern data center, identity management, systems management, virtualization, storage, and networking.

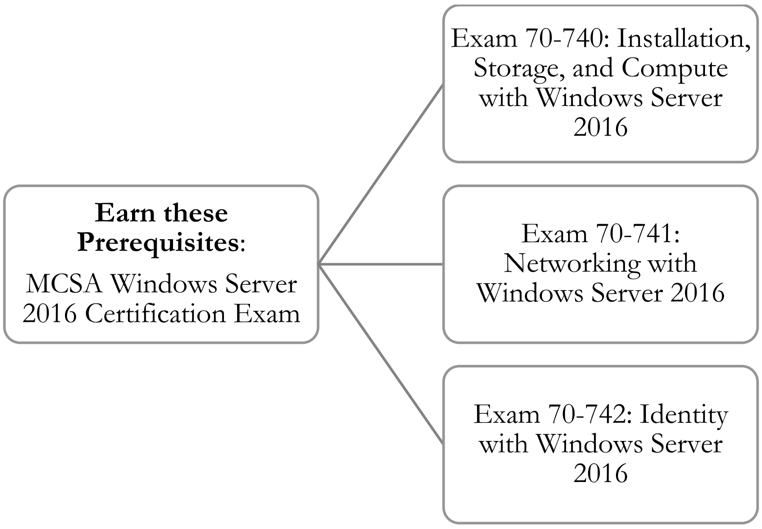
Certification Details:

To earn this Certification, you have to complete the following requirements:

Earn one Prerequisite Certification:

1. Prerequisite Option 1: MCSA: Windows Server 2012
2. Prerequisite Option 2: MCSA: Windows Server 2016

We will consider Option 2 here: MCSA: Windows Server 2016**.** To earn **MCSA: Windows Server 2016** Associate certification, you have to clear these three Certifications one by one.



Earn these Prerequisites:

MCSA Windows Server 2016 Certification Exam

Exam 70-740: Installation, Storage, and Compute with Windows Server 2016

Exam 70-741: Networking with Windows Server 2016

Exam 70-742: Identity with Windows Server 2016

And pass one of the elective exams:

- 70-744: Securing Windows Server 2016
- 70-745: Implementing a Software-Defined Data Center
- 70-413: Designing and Implementing a Server Infrastructure
- 70-414: Implementing an Advanced Server Infrastructure
- 70-537: Configuring and Operating a Hybrid Cloud with Microsoft Azure Stack Hub

We will opt for Course 70-744: Securing Windows Server 2016 in our training program.

Course Content

A. Exam 70-740: Installation, Storage, and Compute with Windows Server 2016

As the name suggests, this certification will guide you on installation, storage, and compute facilities available in Windows Server 2016.

Certification Cost: $165 USD

Certification Exam Structure:

- Install Windows Servers in Host and Compute Environments (10-15%)
- Implement Storage Solutions (15-20%)
- Implement Hyper-V (20-25%)
- Implement Windows Containers (5-10%)
- Implement High Availability (30-35%)
- Maintain and Monitor Server Environments (10-15%)

Exam 70-740 Curriculum

- Introduction to Windows Server 2016
- Install Windows Servers in Host and Compute Environments
  - Install, Upgrade, and Migrate Servers and Workloads
  - Create, Manage, and Maintain Images for Deployment
- Implement Storage Solutions
  - Configure Disks and Volumes
  - Implement Server Storage
  - Implement Data deduplication
- Implement Hyper V
  - Install and Configure Hyper V
  - Configure VM (Virtual Machine) Settings
  - Configuring Hyper V Storage
  - Configuring Hyper V networking
- Implementing Windows Containers
  - Deploying Windows Containers
  - Managing Windows Containers
- Implementing High Availability
  - Implement high availability and disaster recovery options in Hyper-V
  - Implement failover clustering
  - Implement Storage Spaces Direct
  - Manage failover clustering
  - Manage VM movement in clustered nodes
  - Implement Network Load Balancing (NLB)
- Maintain and Monitor Server Environments
  - Maintain Server installations
  - Monitor Server installations

B. Exam 70-741: Networking with Windows Server 2016

In this certification, you will gain skills about networking, features, and functionalities available in Windows Server 2016. You will learn to implement managing and implementing DNS, DHCP, IPAM, etc. You will also learn deploying remote access solutions like VPN and RADIUS.

Certification Cost: $165 USD

Certification Exam Structure:

- Implement Domain Name System (DNS) (15-20%)

- Implement DHCP and IPAM (25-30%)
- Implement Network Connectivity and Remote Access Solutions (20-25%)
- Implement Core and Distributed Network Solutions (15-20%)
- Implement an Advanced Network Infrastructure (15-20%)

Certification Exam Content

Module 1: Implement DNS

- Introduction
- Install and Configure DNS
  - DNS Installation Requirements
  - Install and Configure DNS
  - Implement DNS policies
  - DNS performance Tuning
  - Configure Global Settings
- Create and Configure DNS Zones and Records
  - What are DNS Zones?
  - Create and Configure DNS Primary Zones
  - Create and Configure DNS Secondary Zones
  - Create and Configure DNS Stub Zones
  - Analyze Zone-level Statistics
  - What are DNS Records?
  - Configure DNS Resources Records RR
  - Configure Zone Scavenging
  - Configure Record Options
  - Configure Round Robin
  - Configure Secure Dynamic Updates
  - Configure Unknown Record Support
  - DNS Audit Events & Analytical (Query) Events for Auditing, Troubleshooting
  - Configure Zone Scopes
  - Configure Records in Zone Scopes
  - Configure Policies for Zones

Module 2: Implement DHCP and IPAM

- Overview
  - Introduction to DHCP Servers
  - Installing DHCP
  - Configuring DHCP
  - Authorize DHCP Servers
- Introduction to Scopes
  - What are Scopes?
  - Creating Scopes
  - Configure Scope
  - Create and Configure Super Scopes
  - Create and Configure Multi-cast Scopes
- Configure DHCP
  - Configure DHCP Reservation

  - Configure DHCP options
  - DNS Configuration within DHCP
  - Configuration Policies
  - Configure Client and Server for PXE Boot
  - Configure DHCP Relay Agent
  - Implement Ipv6 Addressing Using Dhcpv6
  - Perform Export and Import of A DHCP Server
  - Perform DHCP Server Migration
- Manage and Maintain DHCP
  - Configure a Lease Period
  - Backup and Restore the DHCP Database
  - Configure High Availability Using DHCP Failover
  - Configure DHCP Name Protection
  - Troubleshoot DHCP
- Implement and Maintain IPAM
  - IPAM (IP Address Management) Overview
  - 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

Module 3: Implement Network Connectivity and Remote Access Solutions

- Implement Network Connectivity Solutions
  - Implement NAT (Network Address Translation)
  - Configure Routing
- Implement VPN and DirectAccess solutions
  - Implement remote access and site-to-site (S2S) VPN solutions
  - Remote Access Gateways
  - Configure VPN protocol options
  - Configure Authentication options
  - Configure VPN connect
  - Configure Connection Profiles
  - Remote Access VPN vs site-to-site VPN
  - Install and Configure Direct Access
  - Implement Server Requirements

  - Client Configuration Options
  - Troubleshooting VPN
- Implement Network Policy Server (NPS)
  - Configure a RADIUS server including RADIUS Proxy
  - Configure RADIUS clients
  - Configure NPS templates
  - Configure RADIUS Accounting
  - Configure Certificates
  - Configure Connection Request Policies
  - Configure Network Policies for VPN, Wireless, Wired Clients
  - Import and Export NPS Policies

Module 4: Implement Core and Distributed Network Solutions

- Implement IPv4 and IPv6 addressing
  - Configure IPv4 addresses and options;
  - Determine and Configure appropriate IPv6 addresses
  - Configure IPv4 or IPv6 subnetting
  - Implement IPv6 stateless addressing
  - Configure interoperability between IPv4 and IPv6 by using ISATAP
  - Configure Border Gateway Protocol (BGP)
  - Configure IPv4 and IPv6 Routing
- Implement DFS and Branch Office Solutions
  - Install and configure DFS Namespaces
  - Configure DFS replication targets
  - Configure replication scheduling;
  - Configure Remote Differential Compression (RDC) Settings
  - Configure Staging, Fault Tolerance
  - Clone a Distributed File System Replication (DFSR) database
  - Recover DFSR databases
  - Optimize DFS Replication
  - Install and configure BranchCache
  - Implement distributed and hosted cache modes
  - Implement BranchCache for web, file, and application servers
  - Troubleshoot BranchCache

Module 5: Implement an Advanced Network Infrastructure

- Implement high performance network solutions
  - Implement NIC Teaming
  - Implement Switch Embedded Teaming (SET) solution
  - NIC Teaming vs SET Solution
  - Enable and Configure Receive Side Scaling (RSS)
  - Enable and Configure Network Quality of Service (QoS) with 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)
  - Enable and Configure Virtual Machine Multi-Queue (VMMQ)

    - Enable and Configure Single-Root I/O Virtualization on a supported network adapter
- Determine scenarios and requirements for implementing (SDN)
    - What is SDN (Software Defined Networking)?
    - Deployment Scenarios for SDN
    - Network Requirements for SDN
    - Deploying SDN
    - Requirements & Scenarios for implementing Hyper V Network Virtualization
    - Determine Scenarios for Software Load Balancer (SLB)
    - Determine Scenarios for Windows Server Gateways
    - Datacentre Firewall Policies
    - Network Security Groups

C. Exam 70-742: Identity with Windows Server 2016

In this Certification Training, you will learn how to install, configure, manage, and maintain Active Directory Domain Services (AD DS) as well as implement Group Policy Objects (GPOs).

Certification Cost: $165 USD

Certification Course Structure:

- Install and Configure Active Directory Domain Services (AD DS) (20-25%)
- Manage and Maintain AD DS (15-20%)
- Create and Manage Group Policy (25-30%)
- Implement Active Directory Certificate Services (AD CS) (10-15%)
- Implement Identity Federation and Access Solutions (15-20%)

Certification Exam Content:

Module 1: Install and Configure Active Directory Domain Services (AD DS)

- Install and Configure Domain Controllers
    - About Domain Controllers
    - Installing a new forest
    - Add or Remove Domain Controllers
    - Upgrading 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
- Create and Manage Active Directory Users and Computers
    - Automatic Creation of Active Directory Users/Accounts
    - Create/Copy/Delete/Configure Users and Accounts
    - Configure Templates

  - Perform Bulk Active Directory Operations
  - Configure User Rights
  - Implement offline domain joins
  - Manage inactive and disabled accounts
  - Automate unlocking of disabled accounts using
  - Windows PowerShell Automate password resets
- Create and manage Active Directory groups and organizational units (OUs)
  - Configure group nesting
  - Convert and Manage Groups using Group Policy
  - Enumerate Group Membership
  - Automate group membership management using Windows PowerShell
  - Creation and management of Active Directory Groups and OUs
  - Manage default Active Directory Containers
  - Create/copy/configure/delete Groups & OUs

Module 2: Manage & Maintain AD DS

- Configure Service Authentication and Account Policies
  - Create and configure Service Accounts
  - Create and configure Group Managed Service Accounts
  - Configure Kerberos Constrained Delegation (KCD)
  - Manage Service Principal Names (SPNs)
  - Configure virtual accounts;
  - Configure domain and local user password policy settings
  - Configure and apply Password Settings Objects (PSOs)
  - Delegate password settings management
  - Configure account lockout policy settings
  - Configure Kerberos policy settings within Group Policy
  - Configure Authentication Policies and Authentication Policy Silos
- Active Directory Maintenance
  - Back up Active Directory and SYSVOL
  - Manage Active Directory offline
  - Perform offline defragmentation of an Active Directory database;
  - Clean up metadata
  - Configure Active Directory snapshots;
  - Perform object- and container-level recovery
  - Perform Active Directory restore
  - Configure and restore objects by using the Active Directory Recycle Bin
  - Configure replication to Read-Only Domain Controllers (RODCs)
  - Configure Password Replication Policy (PRP) for RODC
  - Monitor and manage replication
  - Upgrade SYSVOL replication to Distributed File System Replication (DFSR)
- Configure Active Directory in a complex enterprise environment
  - Configure a multi-domain and multi-forest
  - Active Directory Infrastructure
  - Deploy Windows Server 2016 domain controllers within a pre-existing Active Directory environment
  - Upgrade existing domains and forests
  - Configure domain and forest functional levels;
  - Configure multiple user principal name (UPN) suffixes;

  - configure external, forest, shortcut, and realm trusts;
  - Configure trust authentication
  - Configure SID filtering
  - Configure name suffix routing
  - Configure sites and subnets
  - Create and configure site links;
  - Manage site coverage
  - Manage Registration of SRV records
  - Move domain controllers between sites

Module 3: Create & Manage Group Policy

- Create & Manage Group Policy Objects
  - Configure a central store
  - Manage Starter GPOs
  - Configure GPO links
  - Configure multiple local Group Policies
  - Back up, import, copy, and restore GPOs
  - Create and configure a migration table
  - Reset default GPOs
  - Delegate Group Policy management
  - Detect health issues using the Group Policy Infrastructure Status Page
- Configure Group Policy processing
  - Configure processing order and precedence
  - Configure blocking of inheritance
  - Configure enforced policies
  - Configure security filtering
  - Windows management instrumentation (WMI) filtering
  - Configure loopback processing;
  - Configure and manage slow-link processing and group policy caching
  - Configure client-side extension (CSE) behavior
  - Force a group policy update
- Configure Group Policy settings
  - Configure software installation, folder redirection, Scripts
  - Configure administrative templates
  - Import security templates
  - Import a custom administrative template file
  - Configure filtering for administrative templates
- Configure Group Policy preferences
  - Configure printer preferences
  - Define Network Drive Mappings
  - Configure Power Options
  - Configure Custom Registry Settings;
  - Configure Control Panel Settings
  - Configure Internet Explorer Settings
  - Configure file and folder deployment
  - Configure shortcut deployment
  - Configure item-level targeting

Module 4: Implement Active Directory Certificate Services (AD CS)

- Install and configure AD CS
    - Install Active Directory Integrated Enterprise Certificate Authority (CA)
    - Install offline root and subordinate CAs
    - Install standalone CAs
    - Configure Certificate Revocation List (CRL) Distribution Points
    - Install and configure Online Responder
    - Implement administrative role separation
    - Configure CA backup and recovery
- Manage Certificates
    - Manage certificate templates
    - Implement and Manage Certificate Deployment, Validation, and Revocation
    - Manage Certificate Renewal;
    - Manage certificate enrolment and renewal using Group Policies;
    - Configure and Manage Key Archival and Recovery

Module 5: Implement Identity Federation and Access Solutions

- Install and configure Active Directory Federation Services
    - Upgrade & Migrate previous AD FS workloads to Windows Server 2016
    - Implement claims-based authentication
    - 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 requirement
    - Publish web apps via WAP
    - Publish Remote Desktop Gateway applications
    - Configure HTTP to HTTPS redirects
    - Configure internal and external Fully
    - Qualified Domain Names (FQDNs)
- Install and Configure Active Directory Rights Management Services (AD RMS)
    - Install a licensor certificate AD RMS Server
    - Manage AD RMS Service Connection Point (SCP)
    - Manage AD RMS templates
    - Configure Exclusion Policies
    - Backup and Restore AD RMS

D. Exam 70-744: Securing Windows Server 2016

In this Certification Training program, you will learn securing Windows 2016. Also, you will get 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.

Certification Cost: $165 USD

Certification Course Structure:

- Implement Server Hardening Solutions (25-30%)
- Secure a Virtualization Infrastructure (5-10%)
- Secure a Network Infrastructure (10-15%)
- Manage Privileged Identities (25-30%)
- Implement Threat Detection Solutions (15-20%)
- Implement Workload-Specific Security (5-10%)

Certification Course Content:

Module 1: Implement Server Hardening Solutions

- Configure Disk & File Encryption
  - Determine hardware and firmware requirements
  - Deploy BitLocker Encryption
  - Configure the Network Unlock feature
  - Configure BitLocker Group Policy settings
  - Configure BitLocker on Cluster Shared Volumes (CSVs) and Storage Area Networks (SANs)
  - Implement BitLocker Recovery Process
  - 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
- 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

Module 2: 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
    - Determine requirements and scenarios for implementing encryption-supported VMs
    - Troubleshoot Shielded and encryption-supported VMs

Module 3: 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
    - Configure authenticated firewall exceptions, import, and export settings
- Implement a Software Defined Data Center Firewall
    - Determine requirements and scenarios for Data center
    - Firewall implementation with Software Defined Networking
    - Determine usage scenarios for Data center Firewall policies and network security groups
    - Configure Data center 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

Module 4: 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) using Administrative forest design approach
  - Determine usage scenarios and requirements
- 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

Module 5: 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

Module 6: 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, file screens, 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