Securing Windows Server 2016 (MS-20744)

Modality: Virtual Classroom

Duration: 5 Days

SATV Value: 5

The exam associated with this course will retire on 31st January 2021. However, the course is still valid as training material for learning purposes.

About this course:

This five-day instructor-led course trains the IT professionals how they can improve the safety measures of the IT infrastructure that they manage. This training course begins by stressing the significance of presumptuous that network breaches have occurred previously, and then teaches you how to shield administrative identification and rights to make sure that administrator can carry out only the tasks that they must to, when they must to.

This IT Ops Training course also give details how you can diminish malware threats, categorize security issues by means of auditing and the Advanced Threat Analysis aspect in Windows Server 2016, secure your virtualization policy, and use new operation options, such as Nano server and containers to increase security. The course moreover explains how you can assist protect admittance to files via encryption and dynamic access run, and how you can improve your network's protection. This course moreover prepares the students for the Microsoft 70-744: Securing Windows Server 2016 certification exam.

The average salary IT Professional can earn is **$85,460** per year.

Course Objectives:

After finishing this course, students will be proficient to:

- Secure Windows Server
- Protect application development and a server workload communications
- Manage protection baselines
- Construct and administer just sufficient and just-in-time (JIT) administration
- Administer data protection
- Construct Windows Firewall and a software-defined circulated firewall
- Protect network traffic

- Make safe your virtualization infrastructure
- Administer malware and intimidation
- Construct advanced auditing
- Administer software updates
- Administer threats by means of Advanced Threat Analytics (ATA) and Microsoft Operations Management Suite (OMS)

Audience:

This course is designed for IT professionals who call for to manage Windows Server 2016 networks steadily. These professionals usually work with networks that are constructed as Windows Server domain-based environments, with managed entry to the Internet and cloud services.

Prerequisites:

Students must have minimum two years of experience in the IT field and must have:

- A firm, realistic understanding of networking basics, comprising of TCP/IP, User Datagram Protocol (UDP), and Domain Name System (DNS).
- A firm, functional understanding of Active Directory Domain Services (AD DS) principles.
- An actual, practical knowledge of Microsoft Hyper-V virtualization basics.
- An understanding of Windows Server safety ethics.

Recommended prerequisite courses:

- Server Virtualization with Windows Server Hyper-V and System Center (MS-20409)
- Securing Windows Server 2016 (MS-20744)

Course Outline:

Module 1: Breach detection and using the Sysinternals tools

In this module, students will learn about breach detection, attack types and vectors, cybercrime, and how you can analyze your system’s activity by using the Sysinternals tool suite.

Lessons

- Overview of breach detection
- Using the Sysinternals tools to detect breaches

Lab: Basic breach detection and incident response strategies

- Identifying attack types
- Using incident-response strategies
- Exploring the Sysinternals tools

After completing this course, students will be able to:

- Describe breach detection.
- Describe how to detect a breach by using the Sysinternals tools.

Module 2: Protecting credentials and privileged access

This module explains how you can configure user rights and security options, protect credentials by using credential guard, implement privileged-access workstations, and manage and deploy a local administrator-password solution so that you can manage passwords for local administrator accounts.

Lessons

- Understanding user rights
- Computer and service accounts
- Protecting credentials
- Understanding privileged-access workstations and jump servers
- Deploying a local administrator-password solution

Lab: User rights, security options, and group-managed service accounts

- Configuring security options
- Configuring restricted groups
- Delegating privileges
- Creating and managing group managed service accounts (MSAs)
- Configuring the Credential Guard feature
- Locating problematic accounts

Lab: Configuring and deploying LAPs

- Installing local administrator password solution (LAPs)
- Configuring LAPs
- Deploying LAPs

After completing this module, students will be able to:

- Understand user rights.
- Describe computer and service accounts.
- Help protect credentials.

- Understand privileged-access workstations and jump servers.
- Understand how to use a local administrator-password solution.

Module 3: Limiting administrator rights with Just Enough Administration

This module explains how to deploy and configure Just Enough Administration (JEA).

Lessons

- Understanding JEA
- Configuring and deploying JEA

Lab: Limiting administrator privileges by using JEA

- Creating a role-capability file
- Creating a session-configuration file
- Creating a JEA endpoint
- Connecting to a JEA endpoint
- Deploying JEA by using Desire State Configuration (DSC)

After completing this module, students will be able to:

- Understand JEA.
- Configure and deploy JEA.

Module 4: Privileged Access Management and administrative forests

This module explains the concepts of Enhanced Security Administrative Environment (ESAE) forests, Microsoft Identity Manager (MIM), and Just in Time (JIT) Administration, or Privileged Access Management.

Lessons

- Understanding ESAE forests
- Overview of MIM
- Implementing JIT and Privileged Access Management by using MIM

Lab: Limiting administrator privileges by using Privileged Access Management

- Using a layered approach to security
- Exploring MIM
- Configuring a MIM web portal
- Configuring the Privileged Access feature
- Requesting privileged access

After completing this module, students will be able to:

- Understand enhanced security administrative environment forests.

- Understand MIM.

- Understand how to implement JIT and Privileged Access Management by using MIM.

Module 5: Mitigating malware and threats

This module explains how to configure the Windows Defender, AppLocker, and Device Guard features.

Lessons

- Configuring and managing Windows Defender
- Using software restricting policies (SRPs) and AppLocker
- Configuring and using Device Guard
- Using and deploying the Enhanced Mitigation Experience Toolkit

Lab: Securing applications by using AppLocker, Windows Defender, Device Guard Rules, and the EMET.

- Configuring Windows Defender
- Configuring AppLocker
- Configuring and deploying Device Guard
- Deploying and using EMET

After completing this module, students will be able to:

- Configure and manage Windows Defender.
- Use Software Restricting Policies and AppLocker.
- Configure and use Device Guard.
- Use and deploy the EMET.

Module 6: Analyzing activity by using advanced auditing and log analytics

This module explains how to use advanced auditing and Windows PowerShell transcripts.

Lessons

- Overview of auditing
- Understanding advanced auditing
- Configuring Windows PowerShell auditing and logging

Lab: Configuring encryption and advanced auditing

- Configuring auditing of file-system access
- Auditing domain logons
- Managing the configuration of advanced audit policies
- Windows PowerShell logging and auditing

After completing this module, students will be able to:

- Understanding auditing.
- Understand advanced auditing.
- Audit and log Windows PowerShell.

Module 7: Analyzing activity with Microsoft Advanced Threat Analytics feature and Operations Management Suite

This module explains the Microsoft Advanced Threat Analytics tool and the Microsoft Operations Management suite (OMS), and details how you can use them to monitor and analyze the security of a Windows Server deployment.

Lessons

- Overview of Advanced Threat Analytics
- Understanding OMS

Lab: Advanced Threat Analytics and Operations Management Suite

- Using ATA and OMS
- Preparing and deploying ATA
- Preparing and deploying OMS

After completing this module, students will be able to:

- Understand Advanced Threat Analytics.
- Understand OMS.

Module 8: Securing your virtualization an infrastructure

This module explains how to configure Guarded Fabric virtual machines (VMs), including the requirements for shielded and encryption supported VMs.

Lessons

- Overview of Guarded Fabric VMs
- Understanding shielded and encryption supported VMs

Lab: Deploying and using Guarded Fabric with administrator-trusted attestation and shielded VMs

- Deploying Guarded Fabric VMs with administrator-trusted attestation
- Deploying a shielded VM

After completing this module, students will be able to:

- Understand Guarded Fabric VMs.

- Understand shielded and encryption supported VMs.

Module 9: Securing application development and server-workload infrastructure

This module details the Security Compliance Manager, including how you can use it to configure, manage, and deploy baselines. Additionally, students will learn how to deploy and configure Nano Server, Microsoft Hyper-V, and Windows Server Containers.

Lessons

- Using Security Compliance Manager
- Introduction to Nano Server
- Understanding containers

Lab: Using Security Compliance Manager

- Configuring a security baseline for Windows Server 2016
- Deploying a security baseline for Windows Server 2016

Lab: Deploying and Configuring Nano Server and containers

- Deploying, managing, and securing Nano Server
- Deploying, managing, and securing Windows Server containers
- Deploying, managing, and securing Hyper-V containers

After completing this module, students will be able to:

- Understand Security Compliance Manager.
- Describe Nano Server.
- Understand containers.

Module 10: Protecting data with encryption

This module explains how to configure Encrypting File System (EFS) and BitLocker drive encryption to protect data at rest.

Lessons

- Planning and implementing encryption
- Planning and implementing BitLocker

Lab: Configuring EFS and BitLocker

- Encrypting and recovering access to encrypted files
- Using BitLocker to protect data

After completing this module, students will be able to:

- Plan and implement encryption.
- Plan and implement BitLocker.

Module 11: Limiting access to file and folders

This module explains how to optimize file services by configuring File Server Resource Manager (FSRM) and Distributed File System (DFS). Students will learn how to protect a device's data by using encryption or BitLocker. Students also will learn how to manage access to shared files by configuring Dynamic Access Control (DAC).

Lessons

- Introduction to FSRM
- Implementing classification management and file-management tasks
- Understanding Dynamic Access Control (DAC)

Lab: Configuring quotas and file screening

- Configuring FSRM quotas
- Configuring file screening

Lab: Implementing DAC

- Preparing DAC
- Implementing DAC

After completing this module, students will be able to:

- Understand FSRM.
- Implement classification management and file-management tasks.
- Understand DAC.

Module 12: Using firewalls to control network traffic flow

This module explains the firewalls that are present on Windows Server.

Lessons

- Understanding Windows Firewall
- Software-defined distributed firewalls

Lab: Windows Firewall with Advanced Security

- Creating and testing inbound rules
- Creating and testing outbound rules

After completing this module, students will be able to:

- Describe Windows Firewall.
- Understand software-defined distributed firewalls.

Module 13: Securing network traffic

This module explains how to secure network traffic and how to use Microsoft Message Analyzer, Server Message Block (SMB) encryption, and Domain Name System Security Extensions (DNSSEC).

Lessons

- Network-related security threats and connection-security rules
- Configuring advanced DNS settings
- Examining network traffic with Microsoft Message Analyzer
- Securing SMB traffic, and analyzing SMB traffic

Lab: Connection security rules and securing DNS

- Creating and testing connection security rules
- Configuring and testing DNSSEC

Lab: Microsoft Message Analyzer and SMB encryption

- Using Microsoft Message Analyzer
- Configuring and verifying SMB encryption on SMB shares

After completing this module, students will be able to:

- Understand network-related security threats and connection security rules.
- Configure advanced DNS settings.
- Examine network traffic with Microsoft Message Analyzer.
- Secure SMB traffic, and analyze SMB traffic.

Module 14: Updating Windows Server

This module explains how to use Windows Server Update Services (WSUS) to deploy updates to Windows Servers and clients.

Lessons

- Overview of WSUS
- Deploying updates by using WSUS

Lab: Implementing update management

- Implementing the WSUS server role
- Configuring update settings
- Approving and deploying an update by using WSUS

- Deploying Windows Defender definition updates by using WSUS

After completing this module, students will be able to:

- Understand WSUS.
- Deploy updates with WSUS.