



## Securing Windows Server 2016

**OD20744; On-demand, Video-based**

### About this course

This course teaches IT professionals how they can enhance the security of the IT infrastructure that they administer. This course begins by emphasizing the importance of assuming that network breaches have occurred already, and then teaches you how to protect administrative credentials and rights to ensure that administrators can perform only the tasks that they need to, when they need to.

This course also details how you can mitigate malware threats, identify security issues by using auditing and the Advanced Threat Analysis feature in Windows Server 2016, secure your virtualization platform, and use new deployment options, such as Nano server and containers to enhance security. The course also explains how you can help protect access to files by using encryption and dynamic access control, and how you can enhance your network's security.

### Audience profile

This course is for IT professionals who need to administer Windows Server 2016 networks securely. These professionals typically work with networks that are configured as Windows Server domain-based environments, with managed access to the Internet and cloud services.

Students who seek certification in the 70-744 Securing Windows server exam also will benefit from this course.

### At course completion

After completing this course, students will be able to:

- Secure Windows Server
- Secure application development and a server workload infrastructure
- Manage security baselines
- Configure and manage just enough and just-in-time (JIT) administration
- Manage data security
- Configure Windows Firewall and a software-defined distributed firewall
- Secure network traffic
- Secure your virtualization infrastructure

- Manage malware and threats
- Configure advanced auditing
- Manage software updates
- Manage threats by using Advanced Threat Analytics (ATA) and Microsoft Operations Management Suite (OMS)

## Prerequisites

Students should have at least two years of experience in the IT field and should have:

- Completed courses 740, 741, and 742, or the equivalent
- A solid, practical understanding of networking fundamentals, including TCP/IP, User Datagram Protocol (UDP), and Domain Name System (DNS)
- A solid, practical understanding of Active Directory Domain Services (AD DS) principles
- A solid, practical understanding of Microsoft Hyper-V virtualization fundamentals
- An understanding of Windows Server security principles

## Course Outline

### Module 1: Attacks, breach detection, and 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

- Understanding attacks
- Detecting breaches
- Examining activity with the Sysinternals tool

#### Lab: Basic breach detection and incident response strategies

- Identifying attack types
- 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
- Privileged-Access Workstations and jump servers
- Local administrator-password solution

### Lab: Implementing 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 and configuring LAPs
- Deploying and testing 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
- Verifying and deploying JEA

### **Lab: Limiting administrator privileges with JEA**

- Creating a role-capability file
- Creating a session-configuration file
- Creating a JEA endpoint
- Connecting and testing a JEA endpoint
- Deploying a JEA configuration to another computer

After completing this module, students will be able to:

- Understand JEA
- Verify 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**

- ESAE forests
- Overview of Microsoft Identity Manager
- Overview of JIT administration and PAM

### **Lab: Limiting administrator privileges with PAM**

- Layered approach to security
- Configuring trust relationships and shadow principals
- Requesting privileged access
- Managing PAM roles

After completing this module, students will be able to:

- Understand ESAE forests
- Understand MIM
- Understand JIT administration and PAM

## **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

- Restricting software
- Configuring and using the Device Guard feature
- Deploying and using the EMET

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

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

After completing this module, students will be able to:

- Configure and manage Windows Defender
- Restrict software
- Configure and use the Device Guard feature
- Use and deploy the EMET

## **Module 6: Analyzing activity with advanced auditing and log analytics**

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

### **Lessons**

- Overview of auditing
- Advanced auditing
- Windows PowerShell auditing and logging

### **Lab: Configuring advanced auditing**

- Configuring auditing of file-system access
- Auditing domain sign-ins
- Managing advanced audit policy configuration
- 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: Deploying and configuring Advanced Threat Analytics and Microsoft 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 analyse the security of a Windows Server deployment.

### **Lessons**

- Deploying and configuring ATA
- Deploying and configuring Microsoft Operations Management Suite

### **Lab: Deploying ATA and Microsoft Operations Management Suite**

- Preparing and deploying ATA
- Preparing and deploying Microsoft Operations Management Suite

After completing this module, students will be able to:

- Deploy and configure ATA
- Deploy and configure Microsoft Operations Management Suite

## **Module 8: Secure Virtualization Infrastructure**

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

### **Lessons**

- Guarded Fabric
- Shielded and encryption-supported virtual machines

### **Lab: Guarded Fabric with administrator-trusted attestation and shielded VMs**

- Deploying a guarded fabric 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 SCM
- Introduction to Nano Server
- Understanding containers

### Lab: Using SCM

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

### Lab: Deploying and Configuring Nano Server

- Deploying, managing, and securing Nano Server
- Deploying, managing, and securing Windows container

After completing this module, students will be able to:

- Understand SCM
- Describe Nano Server
- Understand containers

## Module 10: Planning and protecting data

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: Protecting data by using encryption 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: Optimizing and securing file services**

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**

- File Server Resource Manager
- Implementing classification management and file-management tasks
- Dynamic Access Control

### **Lab: Quotas and file screening**

- Configuring File Server Resource Manager quotas
- Configuring file screening and storage reports

### **Lab: Implementing Dynamic Access Control**

- Preparing for implementing Dynamic Access Control
- Implementing Dynamic Access Control
- Validating and remediating Dynamic Access Control

After completing this module, students will be able to:

- Understand File Server Resource Manager
- Implement classification management and file-management tasks
- Understand Dynamic Access Control

## **Module 12: Securing network traffic with firewalls and encryption**

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

### **Lessons**

- Understanding network-related security threats
- Understanding Windows Firewall with Advanced Security
- Configuring IPsec

- Datacenter Firewall

### **Lab: Configuring Windows Firewall with Advanced Security**

- Creating and testing inbound rules
- Creating and testing outbound rules
- Creating and testing connection security rules

After completing this module, students will be able to:

- Understand network-related security threats
- Understand Windows Firewall with Advanced Security
- Configure IPsec
- Understand Datacenter Firewall

## **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: Securing DNS**

- Configuring and testing DNSSEC
- Configuring DNS policies and RRL

### **Lab: Microsoft Message Analyzer and SMB encryption**

- Installing and using Message Analyzer
- Configuring and verifying SMB encryption on SMB shares

After completing this module, students will be able to:

- Configure advanced DNS settings
- Examine network traffic with 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

After completing this module, students will be able to:

- Understand WSUS
- Deploy updates with WSUS