REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
"Training You Can Really Use"

# 20744: Securing Windows Server® 2016

## Duration: 5 Days

## Method: Instructor-Led Training (ILT) | Live Online Training

## Course Description

This course teaches participants how they can enhance the security of the IT infrastructure that they administer. It begins by emphasizing the importance of assuming that network breaches have occurred already, and then teaches participants 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 participants can mitigate malware threats, identify security issues by using auditing and the Advanced Threat Analysis feature in Windows Server 2016, secure their virtualization platform, and use new deployment options, such as Nano server and containers to enhance security. The course also explains how participants can help protect access to files by using encryption and dynamic access control, and how they can enhance their network's security.

## Target Audience

This course is intended for:

- IT professionals who need to administer Windows Server 2016 networks securely.

## Prerequisites

To attend this course, candidates should have at least two years of experience in the IT field as well as the following:

- 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).
  - Active Directory® Domain Services (AD DS) principles.
  - Microsoft Hyper-V® virtualization fundamentals.
  - Windows Server security principles.

## Course Objectives

Upon successful completion of this course, attendees will be able to:

- Secure Windows Server.
- Protect credentials and implement privileged access workstations.
- Limit administrator rights with Just Enough Administration.
- Manage privileged access.
- Mitigate malware and threats.
- Analyse activity with advanced auditing and log analytics.
- Deploy and configure Advanced Threat Analytics and Microsoft Operations Management Suite.
- Configure Guarded Fabric virtual machines (VMs).
- Use the Security Compliance Toolkit (SCT) and containers to improve security.
- Plan and protect data.
- Optimize and secure file services.
- Secure network traffic with firewalls and encryption.
- Secure network traffic using DNSSEC and Message Analyzer.

## Course Topics

### Module 1: Attacks, Breach Detection, and Sysinternals Tools

- Understanding Attacks
- Detecting Security Breaches
- Examining Activity with the Sysinternals Tools

### Module 2: Protecting Credentials and Privileged Access

- Understanding User Rights
- Computer and Service Accounts
- Protecting Credentials
- Privileged Access Workstations and Jump Servers
- Local Administrator Password Solution

### Module 3: Limiting Administrator Rights with Just Enough Administration (JEA)

- Understanding JEA
- Verifying and Deploying JEA

### Module 4: Privileged Access Management and Administrative Forests

- Enhanced Security Administrative Environment (ESAE) Forests
- Overview of Microsoft Identity Manager (MIM)
- Overview of Just in Time (JIT) Administration and Privileged Access Management (PAM)

### Module 5: Mitigating Malware and Threats

- Configuring and Managing Windows Defender
- Restricting Software
- Configuring and Using the Device Guard Feature

## Course Topics *Continued*

### Module 6: Analysing Activity with Advanced Auditing and Log Analytics

- Overview of Auditing
- Advanced Auditing
- Windows PowerShell Auditing and Logging

### Module 7: Deploying and Configuring Advanced Threat Analytics (ATA) and Microsoft Operations Management Suite (OMS)

- Deploying and Configuring ATA
- Deploying and Configuring Microsoft OMS
- Deploying and Configuring Microsoft Azure® Security Center

### Module 8: Secure Virtualization Infrastructure

- Guarded Fabric
- Shielded and Encryption-Supported Virtual Machines

### Module 9: Securing Application Development and Server-Workload Infrastructure

- Using Security Compliance Toolkit (SCT)
- Understanding Containers

### Module 10: Planning and Protecting Data

- Planning and Implementing Encryption
- Planning and Implementing BitLocker
- Protecting Data by Using Azure Information Protection

### Module 11: Optimizing and Securing File Services

- File Server Resource Manager (FSRM)
- Implementing Classification and File Management Tasks
- Dynamic Access Control (DAC)

### Module 12: Securing Network Traffic with Firewalls and Encryption

- Understanding Network-Related Security Threats
- Understanding Windows Firewall with Advanced Security
- Configuring Internet Protocol Security (IPsec)
- Datacenter Firewall

### Module 13: Securing Network Traffic

- Configuring Advanced DNS Settings
- Examining Network Traffic with Message Analyzer
- Securing and Analyzing Server Message Block (SMB) Traffic

## LABS INCLUDED