



# Securing Windows Server 2016



Exam Ref 70-744

Timothy L. Warner  
Craig Zacker

# Exam Ref 70-744 Securing Windows Server 2016

Timothy Warner  
Craig Zacker

# Exam Ref 70-744 Securing Windows Server 2016

## Table of Contents

Cover

Title Page

Copyright Page

Contents

Introduction

- Organization of this book

- Microsoft certifications

- Acknowledgments

- Free ebooks from Microsoft Press

- Microsoft Virtual Academy

- Quick access to online references

- Errata, updates, & book support

- We want to hear from you

- Stay in touch

- Preparing for the exam

Chapter 1 Implement server hardening solutions

- Skill 1.1: Configure disk and file encryption

  - Determine hardware and firmware requirements for Secure Boot and encryption  
key functionality

  - Deploy BitLocker Drive Encryption

  - Configure Network Unlock

# **Table of Contents**

Implement the BitLocker Recovery Process

Manage Encrypting File System

## **Skill 1.2: Implement server patching and updating solutions**

Install and configure WSUS

Create computer groups and configure Automatic Updates

Manage updates using WSUS

Configure WSUS reporting

Troubleshoot WSUS configuration and deployment

## **Skill 1.3: Implement malware protection**

Implement an antimalware solution with Windows Defender

Integrate Windows Defender with WSUS and Windows Update

Implement AppLocker rules

Implement Control Flow Guard

Implement Device Guard policies

## **Skill 1.4: Protect credentials**

Determine requirements for Credential Guard

Configure Credential Guard

Implement NTLM blocking

## **Skill 1.5: Create security baselines**

Install and Configure Security Compliance Manager

Create and import security baselines

Deploy configurations to domain and non-domain-joined servers

Chapter summary

## **Thought Experiment**

## **Thought experiment answers**

## **Chapter 2 Secure a Virtualization Infrastructure**

### **Skill 2.1: Implement a Guarded Fabric solution**

Install and configure the Host Guardian Service

# **Table of Contents**

Configure admin and TPM-trusted attestation

Configure Key Protection Service Using HGS

Configuring the guarded host

Migrate shielded VMs to other guarded hosts

Troubleshoot guarded hosts

## **Skill 2.2: Implement shielded and encryption-supported VMs**

Determine requirements and scenarios for implementing shielded VMs

Create a shielded VM using Hyper-V

Enable and configure vTPM

Determine requirements and scenarios for implementing encryption-supported VMs

Shielded VM recovery

Chapter summary

Thought experiment

Thought experiment answers

## **Chapter 3 Secure a network infrastructure**

### **Skill 3.1: Configure Windows Firewall**

Configure Windows Firewall with Advanced Security

Configure network location profiles and deploy profile rules using Group Policy

Configure connection security rules using Group Policy, the GUI console, or Windows PowerShell

Configure Windows Firewall to allow or deny applications

Configure authenticated firewall exceptions

### **Skill 3.2: Implement a software-defined Distributed Firewall**

Determine requirements and scenarios for Distributed Firewall implementation with Software Defined Networking

Determine usage scenarios for Distributed Firewall policies and network security groups

### **Skill 3.3: Secure network traffic**

# **Table of Contents**

- Determine SMB 3.1.1 protocol security scenarios and implementations
- Enable SMB encryption on SMB shares
- Configure SMB signing and disable SMB 1.0
- Secure DNS traffic using DNSSEC and DNS policies
- Install and configure Microsoft Message Analyzer to analyze network traffic
- Chapter summary
- Thought experiment
- Thought experiment answer

## **Chapter 4 Manage Privileged Identities**

### **Skill 4.1: Implement an Enhanced Security Administrative Environment administrative forest design approach**

- Determine usage scenarios and requirements for implementing ESAE forest design architecture to create a dedicated administrative forest
- Determine usage scenarios and requirements for implementing clean source principles in an Active Directory architecture

### **Skill 4.2: Implement Just-in-Time administration**

- Create a new administrative (bastion) forest in an existing Active Directory environment using Microsoft Identity Manager
- 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 solutions
- Create and implement MIM policies
- Implement just-in-time administration principals using time-based policies
- Request privileged access using Windows PowerShell

### **Skill 4.3: Implement Just-Enough-Administration**

- Enable a JEA solution on Windows Server 2016

# **Table of Contents**

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

## **Skill 4.4: Implement Privileged Access Workstations 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

## **Skill 4.5: Implement Local Administrator Password Solution**

Install and configure the LAPS tool

Secure local administrator passwords using LAPS

Manage password parameters and properties using LAPS

## **Chapter summary**

Thought experiment

Thought experiment answers

## **Chapter 5 Implement threat detection solutions**

### **Skill 5.1: 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

# **Table of Contents**

Configure the Audit Group Membership policy

Enable and configure module, script block, and transcription logging in  
Windows PowerShell

## **Skill 5.2: Install and configure Microsoft Advanced Threat Analytics**

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

## **Skill 5.3: Determine threat detection solutions using Operations Management Suite**

Determine Usage and Deployment Scenarios for OMS

Determine security and auditing functions available for use

Determine log analytics usage scenarios

Chapter summary

Thought experiment

Thought experiment answers

## **Chapter 6 Implement workload-specific security**

### **Skill 6.1: Secure application development and server workload infrastructure**

Determine usage scenarios, supported server workloads, and requirements for  
Nano Server deployments

Install and configure Nano Server

Implement security policies on Nano Servers using Desired State  
Configuration

Determine usage scenarios and requirements for Windows Server and Hyper-V  
containers

Install and configure Hyper-V containers



# **Table of Contents**

## **Skill 6.2: Implement a Secure File Services infrastructure and Dynamic Access Control**

- Install the File Server Resource Manager role service
- Configure quotas
- Configure file screens
- Configure Storage Reports
- Configure File Management Tasks
- Configure File Classification Infrastructure using FSRM
- Implement Work Folders
- Configure user and device claim types
- Create and configure resource properties and lists
- Create and configure central access rules and policies
- Implement policy changes and staging
- Configure file access auditing
- Perform access-denied remediation
- Chapter summary

Thought experiment

Thought experiment answers

Index

About the authors

Free ebooks

Survey