



# Securing Windows Server 2022

## Module 1:

### Server Hardening Solutions Lessons

- Determine hardware and firmware requirements for secure boot and encryption key functionality.
  - Deploy BitLocker encryption.
  - Deploy BitLocker without a Trusted Platform Module (TPM).
  - Deploy BitLocker with a TPM only configure the Network Unlock feature.
- 
- Configure BitLocker Group Policy settings.
  - Enable BitLocker to use secure boot for platform and BCD integrity validation.
- 
- Configure BitLocker on Cluster Shared Volumes (CSVs) and Storage Area Networks (SANs).
  - Implement BitLocker Recovery Process using self-recovery and recovery password retrieval solutions.
- 
- Configure BitLocker for virtual machines (VMs) in Hyper-V.
  - Determine usage scenarios for Encrypting File System (EFS).
  - Configure the EFS recovery agent to manage EFS and BitLocker certificates, including backup and restore.

## Module 2:

### **Security with Windows Defender and Windows Backups Lessons**

- Windows Security settings overview
  - Deploying AppLocker to defend against unwanted applications
  - Implement AppLocker rules
  - Implement AppLocker rules using Windows PowerShell.
  - Implement Control Flow Guard.
  - Overview of Microsoft Defender Antimalware.
  - Configure Windows Defender using Group Policy.
  - Configure Windows Defender scans using Windows PowerShell.
  - Scheduling antimalware scans.
  - Configuring Defender quarantine
  - Implement Anti crypto options using Defender
  - Enabling Volume Shadow Service and Windows Backups
- 
- Restoration of files and servers
  - Implement Code Integrity (Device Guard) Policies
  - Create Code Integrity policy rules
  - Anti-Ransomware features

## Module 3:

### **Credentials and Baselines Lessons :**

- The importance of Windows updates pertaining to security
- Deploying a WSUS server
- Implement antimalware solution with Windows Defender
- Integrate Windows Defender with WSUS and Windows Update.
- Create, view, and import security baselines
- Deploy configurations to domain and non-domain joined servers

## Module 4:

### Virtualization Infrastructure Lessons

- Determine requirements for implementing Credential Guard
- Configure Credential Guard using Group Policy, WMI, command prompt, and Windows PowerShell
- Install and configure Microsoft Security Compliance Toolkit
- 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
- Determine requirements and scenarios for implementing Shielded VMs
- Create a shielded VM using only a Hyper-V environment
- Enable and configure vTPM to allow an operating system and data disk encryption within a VM
- Determine requirements and scenarios for implementing encryption supported VMs
- Troubleshoot Shielded and encryption supported VMs

## Module 5:

### **Securing Network Infrastructure Lessons :**

- 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, the GUI management console, or Windows PowerShell
- Configure authenticated firewall exceptions
- Import and export settings
- Determine requirements and scenarios for Datacenter Firewall implementation with Software Defined Networking
- Determine usage scenarios for Datacenter Firewall policies and network security groups
- Configure Datacenter Firewall Access Control List
- Multi-factor authentication
- Windows VPN types and options
- Network Policy Server (NPS) and RADIUS deployments

## Module 6:

### **Implement a Secure File Infrastructure Lessons**

- 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
  - Configure Universal Access Control
  - Windows Certificate Server
  - Deploying trusted certificates in an infrastructure

## Module 7:

### **SMB Security and Log Auditing Lessons**

- NTFS Permissions
- Shared folder security
- Effective permission security
- Kerberos and NTLM authentication
- Server Message Block for accessing file shares
- Removing outdated SMB protocols
- Determine SMB 3.1.1 protocol security scenarios and implementations
- Enable SMB encryption on SMB shares
- Configure SMB signing
- Create SMB shares on a file cluster
- Setup auditing using group policy
- Advanced auditing policies
- Log auditing and review

## Module 8:

### **Nano Servers and Windows Containers Lessons**

- 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