70-744: Securing Windows Server 2016

Audience Profile:
Candidates for this exam secure Windows Server 2016 environments. Candidates are familiar with the methods and technologies used to harden server environments and secure virtual machine infrastructures using Shielded and encryption-supported virtual machines and Guarded Fabric.

Candidates manage the protection of Active Directory and Identity infrastructures and manage privileged identities using Just in Time (JIT) and Just Enough Administration (JEA) approaches, as well as implement Privileged Access Workstations (PAWs) and secure servers using the Local Administrator Password Solution (LAPS).

Candidates should also be able to use threat detection solutions such as auditing access, implementing Advanced Threat Analytics (ATA), deploying Operations Management Suite (OMS) solutions, and identifying solutions for specific workloads.

Objective Domain

Note: This document shows tracked changes that are effective as of November 2, 2018.

Implement Server Hardening Solutions (25-30%)

Configure disk and file encryption

This objective may include but is not limited to: 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; manage EFS and BitLocker certificates, including backup and restore

Implement malware protection

This objective may include but is not limited to: Implement antimalware solution with Windows Defender; integrate Windows Defender with WSUS and Windows Update; configure Windows Defender using Group Policy; configure Windows Defender scans using Windows

PowerShell; implement AppLocker rules; implement AppLocker rules using Windows PowerShell; implement Control Flow Guard; implement Code Integrity (Device Guard) Policies; create Code Integrity policy rules; create Code Integrity file rules

Protect credentials

This objective may include but is not limited to: Determine requirements for implementing Credential Guard; configure Credential Guard using Group Policy, WMI, command prompt, and Windows PowerShell; implement NTLM blocking

Create security baselines

This objective may include but is not limited to: Install and configure Microsoft Security Compliance Toolkit; create, view, and import security baselines; deploy configurations to domain and non-domain joined servers

Secure a Virtualization Infrastructure (5-10%)

Implement a Guarded Fabric solution

This objective may include but is not limited to: 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

Implement Shielded and encryption-supported VMs

This objective may include but is not limited to: 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

Secure a Network Infrastructure (10-15%)

Configure Windows Firewall

This objective may include but is not limited to: 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

Implement a Software Defined Datacenter Firewall

This objective may include but is not limited to: 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 Lists

Secure network traffic

This objective may include but is not limited to: Configure IPsec transport and tunnel modes; configure IPsec authentication options; configure connection security rules; implement isolation zones; implement domain isolation; implement server isolation zones; determine SMB 3.1.1 protocol security scenarios and implementations; enable SMB encryption on SMB Shares; configure SMB signing via Group Policy; disable SMB 1.0; secure DNS traffic using DNSSEC and DNS policies; install and configure Microsoft Message Analyzer (MMA) to analyze network traffic

Manage Privileged Identities (25-30%)

Implement Just-In-Time (JIT) Administration

This objective may include but is not limited to: Create a new administrative (bastion) forest in an existing Active Directory environment using Microsoft Identity Manager (MIM); 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 (PAM) solutions; create and Implement MIM policies; implement Just-in-Time administration principals using time-based policies; request privileged access using Windows PowerShell

Implement Just-Enough-Administration (JEA)

This objective may include but is not limited to: Enable a JEA solution on Windows Server 2016; 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 (DSC)

Implement Privileged Access Workstations (PAWs) and User Rights Assignments

This objective may include but is not limited to: 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; Implement an Enhanced Security Administrative Environment (ESAE) administrative forest design approach; Determine usage scenarios and requirements for implementing ESAE forest design architecture to create a dedicated administrative forest

Implement Local Administrator Password Solution (LAPS)

This objective may include but is not limited to: Install and configure the LAPS tool; secure local administrator passwords using LAPS; manage password parameters and properties using LAPS

Implement Threat Detection Solutions (15-20%)

Configure advanced audit policies

This objective may include but is not limited to: 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; configure the Audit Group Membership policy; enable and configure Module, Script Block, and Transcription logging in Windows PowerShell

Install and configure Microsoft Advanced Threat Analytics (ATA)

This objective may include but is not limited to: 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

Determine threat detection solutions using Operations Management Suite (OMS)

This objective may include but is not limited to: Determine usage and deployment scenarios for OMS; determine security and auditing functions available for use; determine Log Analytics usage scenarios

Implement Workload-Specific Security (5-10%)

Secure application development and server workload infrastructure

This objective may include but is not limited to: Determine usage scenarios, supported server workloads, and requirements for deployments; ~~install and configure Nano Server; implement security policies on Nano Servers using Desired State Configuration (DSC); Manage local policy on Nano Server;~~ determine usage scenarios and requirements for Windows Server and Hyper-V containers; install and configure containers

Implement a secure file services infrastructure and Dynamic Access Control (DAC)

This objective may include but is not limited to: Install the File Server Resource Manager (FSRM) role service; configure quotas; configure file screens; configure storage reports; configure file management tasks; configure File Classification Infrastructure (FCI) using FSRM; implement work folders; configure file access auditing; configure user and device claim types; implement policy changes and staging; perform access-denied remediation; create and configure Central Access rules and policies; create and configure resource properties and lists