Securing Windows Server 2016 (MOC20744)

Securing Windows Server 2016 (MOC20744)

Seminar | Zurzeit keine Termine | Teilnahmebescheinigung

Präsenz / Virtual Classroom | 40 Unterrichtseinheiten

Seminarnummer: 29454 | Herstellernummer: MOC20744

Stand: 08.05.2024. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/29454

Dieser fünftägige Kurs vermittelt IT-Experten, wie sie die Sicherheit der von ihnen verwalteten IT-Infrastruktur mit Windows Server Technologien optimieren können. Zu Beginn wird hervorgehoben, wie wichtig es ist, davon auszugehen, dass es vielleicht bereits zu Sicherheitsverletzungen im Netzwerk gekommen ist.

Letzte Durchführung Anfang April. Ggf. auf AZ-801 und/oder SC-300 ausweichen.

Nutzen

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 networks security.

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).

Zielgruppe

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.

Voraussetzungen

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

- Completed courses MOC20740, MOC20741, and MOC20742, or the equivalent like the Upgrade course MOC20743.
- 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.

Inhalte des Seminars

Module 1: Breach detection and using the Sysinternals tools In this module, students will learn about breach detection, attack types and vectors, cybercrime, and how you can analyse your systems activity by using the Sysinternals tool suite.

Lessons

- Overview of breach detection
- Using the Sysinternals tools to detect breaches

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
- Understanding privileged-access workstations and jump servers
- Deploying 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
- Configuring and deploying 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

- Understanding ESAE forests
- Overview of MIM
- Implementing JIT and Privileged Access Management by using MIM

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
- Using software restricting policies (SRPs) and AppLocker
- Configuring and using Device Guard
- Using and deploying the Enhanced Mitigation Experience Toolkit

Module 6: Analysing activity by using advanced auditing and log analytics This module explains how to use advanced auditing and Windows PowerShell transcripts.

Lessons

- Overview of auditing
- Understanding advanced auditing
- Configuring Windows PowerShell auditing and logging

Module 7: Analysing activity with Microsoft Advanced Threat Analytics feature and 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

- Overview of Advanced Threat Analytics
- Understanding OMS

Lab : Advanced Threat Analytics and Operations Management Suite

- Using ATA and OMS
- Preparing and deploying ATA
- Preparing and deploying OMS

Module 8: Securing your virtualization an infrastructure This module explains how to configure Guarded Fabric virtual machines (VMs), including the requirements for shielded and encryption-supported VMs.

Lessons

- Overview of Guarded Fabric VMs
- Understanding shielded and encryption-supported VMs

Lab : Deploying and using Guarded Fabric with administrator-trusted attestation and shielded VMs

- Deploying Guarded Fabric VMs with administrator-trusted attestation
- Deploying a shielded VM

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 Security Compliance Manager
- Introduction to Nano Server
- Understanding containers

Lab : Using Security Compliance Manager

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

Lab : Deploying and Configuring Nano Server and containers

- Deploying, managing, and securing Nano Server
- Deploying, managing, and securing Windows Server containers
- Deploying, managing, and securing Hyper-V containers

Module 10: Protecting data with encryption 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 : Configuring EFS and BitLocker

- Encrypting and recovering access to encrypted files
- Using BitLocker to protect data

Module 11: Limiting access to file and folders 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 devices data by using encryption or BitLocker. Students also will learn how to manage access to shared files by configuring Dynamic Access Control (DAC).

Lessons

- Introduction to FSRM
- Implementing classification management and file-management tasks
- Understanding Dynamic Access Control (DAC)

Module 12: Using firewalls to control network traffic flow This module explains the firewalls that are present on Windows Server.

Lessons

- Understanding Windows Firewall
- Software-defined distributed firewalls

Lab : Windows Firewall with Advanced Security

- Creating and testing inbound rules
- Creating and testing outbound rules

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 analysing 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
- Deploying Windows Defender definition updates by using WSUS

Wichtige Hinweise

Dieses Seminar wird mit deutschen Unterlagen und Übungsumgebungen durchgeführt.

Letzte Durchführung Anfang April. Ggf. auf AZ-801 und/oder SC-300 ausweichen!

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/29454 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto

- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.