

KOENIG SOLUTIONS • COURSE OUTLINE

Securing Windows Server 2022

Learn to secure Windows Server 2022 through hardening, encryption, network defence, file infrastructure and privileged identity management.

9

MODULES

115

TOPICS

COURSE OVERVIEW

This course covers securing Windows Server 2022, beginning with server hardening using BitLocker and EFS encryption, followed by Windows Defender, AppLocker and backup solutions. It then addresses update management with WSUS, security baselines, Credential Guard, and shielded virtual machine infrastructure. Further modules cover Windows Firewall, secure file infrastructure, SMB security, log auditing, Nano Server and container deployments, concluding with privileged identity management using Just-in-Time and Just-Enough-Administration.

WHO THIS COURSE IS FOR

System Administrators

Security Administrators

Network Administrators

Infrastructure Engineers

Identity Administrators

LEARNING OBJECTIVES

- Deploy BitLocker encryption across devices, clusters and virtual machines
- Configure Windows Defender, AppLocker and Code Integrity policies
- Implement WSUS and security baseline deployments
- Configure Credential Guard, Host Guardian Service and shielded VMs
- Configure Windows Firewall and Datacenter Firewall policies
- Implement a secure file infrastructure using FSRM and Work Folders
- Configure SMB security settings and auditing policies
- Implement privileged identity management using JIT and JEA

9 Modules, 115 Topics

01

Server Hardening Solutions

TOPICS

- 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

02

Security with Windows Defender and Windows Backups

TOPICS

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

03

Credentials and Baselines

TOPICS

- 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

04

Virtualization Infrastructure

TOPICS

- 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

05

Securing Network Infrastructure

TOPICS

- 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

06

Implement a Secure File Infrastructure

TOPICS

- 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

07

SMB Security and Log Auditing

TOPICS

- 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

08

Nano Servers and Windows Containers

TOPICS

- 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

09

Manage Privileged Identities

TOPICS

- 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
- 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

Manage Privileged Identities (continued)

TOPICS (CONTINUED)

- 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 2022
- 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
- Configuring Rights Management Services

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com