Securing Windows Server 2016, Part 2 of 5: Administrative Access

Meet the expert: Patrick Loner has certifications for MCSA, MCSE, MCITP, A+, Network+, Security+, and more. He has been working as a Microsoft Certified Trainer, network administrator, and network consultant for over ten years. He has over a decade of experience working with and teaching about Windows networks with client and server operating systems. He has guided many students toward Microsoft and CompTIA certifications. Most recently, he has worked as a freelance trainer and network consultant specializing in Windows Server 2008 and Microsoft Exchange 2007 and Exchange 2010 implementations, design, and upgrades. Patrick continues to branch out now working with and training on Windows Server 2012, Windows 8, Exchange 2013, and System Center Configuration Manager 2012.

Prerequisites: This is Part 2 of the series.

Runtime: 02:36:29

Course description: This course is all about managing administrative access and a new feature JEA or Just Enough Administration--which is a least privilege model. Then it will cover anti-malware and patch management, configuring and managing windows defender, Device Guard and App Locker. Finally it will close out with WSUS and updating central management of patches.

Course outline:

Deploy JEA
- Introduction
- Introduction to JEA
- JEA Components
- Session Configuration Files
- Demo: Session Configuration File
- Role Capability Files
- Demo: Configure JEA
- Demo: DNSops File
- JEA Endpoints
- Demo: JEA Endpoint
- Connecting to JEA Endpoints
- Deploying JEA Endpoints
- Summary

Enhanced Security
- Introduction
- ESAE Forests
- Administrative Tiers
- ESAE Best Practices
- The Clean Source Principle
- Implementing the Clean Source Principle
- Summary

Identity Manager
- Introduction
- Overview of MIM
- MIM Requirements
- MIM Service Accounts
- Summary

IT Admin and PAM
- Introduction
- Overview of JIT Administration
- Privileged Access Management
- PAM Components
- Creating an Administrative Forest
- Configuring Trust Relationships
- Shadow Principals
- Configuring the MIM Web Portal
- Managing and Configuring PAM Roles
- Summary

Windows Defender
- Introduction
- Understanding Malware
- Malware Sources
- Mitigation Methods
- Windows Defender
- Demo: Configure Windows Defender
- Demo: Scan with Windows Defender
- Summary

Restricting Software
- Introduction
- Controlling Applications
- Software Restriction Policies
- Security Levels
- AppLocker
- AppLocker
- Support for AppLocker
- Creating Default Rules
- Demo: AppLocker
- Demo: Create Rules
- Summary

Using Device Guard
- Introduction
- Ovierview of Device Guard
- Device Guard Features
- Configuring Device Guard
- Device Guard Policies
- Deploying Code Integrity Policies
- Control Flow Guard
- Summary

Patch Management
- Introduction
- Overview of WSUS
- Deployment Options
- Server Requirements
- Configuring Clients
- Administering WSUS
- Approving Updates
- Demo: Installl WSUS
- Demo: Navigate WSUS
- Demo: WSUS Options
- Summary