Identity with Windows Server 2016, Part 5 of 6: Active Directory and Azure

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 5 of the series

Runtime: 03:10:40

Course description: This course covers an understanding of how Azure AD and directory synchronization work. You will understand how to monitor the software for ongoing efficiency, CA types, and utilities within windows to provide the monitoring. This course finishes up with a discussion of certificate services and the foundation of public key infrastructure.

Course outline:

Introduction to Azure AD
- Introduction
- Overview of Azure AD
- Limitations of AD DS
- Extending AD DS Authentication
- Comparing AD DS and Azure AD
- Authentication Options
- Planning Directory Synchronization
- Enabling AD DS Synchronization
- Summary

Implemeting Azure AD Connect
- Introduction
- What Is Azure AD Connect
- Azure AD Connect Requirements
- Azure AD Connect Express Settings
- Azure AD Connect Custom Installation
- Monitoring Azure AD
- Privileged Identity Management
- Summary

Managing Identities with Directory Synch
- Introduction
- Managing Groups
- Filtering Azure AD Connect
- Monitoring Directory Synchronization
- Troubleshooting Directory Synchronization
- Summary

Monitoring AD DS
- Introduction
- Performance Monitoring Benefits
- Establishing Performance Baselines
- Introduction to Monitoring Tools
- Event Viewer
- Demo: Event Viewer
- Reliability Monitor
- Real-Time Monitoring
- Data Collector Sets
- Data Collection Points
- Common AD DS Counters
- Best Practices
- Summary

Database Management
- Introduction
- Physical Data Store
- Using NTDSUtil
- AD DS Maintenance
- Summary

Backup and Recovery in AD DS
- Introduction
- Disaster Recovery for Active Directory
- Backing Up Active Directory
- Using Backup Tools
- Backup Requirements
- Restoring Data
- Additional Restore Options
- Demo: Enable AD Recycle Bin
- Best Practices for Backup and Recovery
- Summary

Overview of Public Key Infrastructure
- Introduction
- What Is a PKI
- Encryption Types
- PKI Components
- PKI Enabled Applications
- Certificate Authorities
- CA Types
- Internal vs. External CAs
- AD CS in Windows Server 2016
- Summary

Deploy Certificate Authority Hierarchy
- Introduction
- Decision Factors for CA Hierarchy
- CA Hierarchy Roles
- Best Practices for CA Hierarchies
- Installing Root CAs
- Demo: Set Up Root CA
- Demo: Additonal Configuration
- Subordinate CAs
- Automating Installations
- Summary

Administering Certificate Authorities
- Introduction
- Administration Tools
- Configuring CA Security
- Security Roles for CA Administration
- Policy and Exit Modules
- Certificate Revocation List
- Publishing the CRL
- Publishing AIAs and CDPs
- Summary

Deploying and Managing Certificates
- Introduction
- Digital Certificates
- Certificate Templates
- Template Versions in Windows Server 2016
- Certificate Template Permissions
- Updating Templates
- Demo: Configure Certificate Template
- Enrollment Types
- Manual Enrollment
- Automating Enrollment
- Demo: Automatic Enrollment
- Demo: Automatic Certificate Request
- Credentials Roaming
- Summary

Manging Revocation and Distribution
- Introduction
- Certificate Revocation
- Online Responder
- Online Responder Process
- Comparing CRL and OCSP
- Configuring an Online Responder
- Summary

Configure Certificate Recovery
- Introduction
- Importance of Key Archival and Recovery
- Key Archival

(Continued on page 2)

Identity with Windows Server 2016, Part 5 of 6: Active Directory and Azure

page 2

- Data Revocery vs. Key Recovery
- Archival and Export Methods
- Automating Archival
- Recovering Lost Keys
- Summary