Identity with Windows Server 2016, Part 3 of 6: Deploy and Replicate

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 3 of the course

Runtime: 04:00:00

Course description: This course looks at security and security on domain controllers and the Active Direction infrastructure both physically and the network. It will cover options for increasing security and branch office looking at complex Active Directory domain structures including multi-domain, multi-site, and multiple forests.

Course outline:

Secure Domain Controllers
- Introduction
- Understanding Security Risks
- Using Group Policy
- Group Policy Security Settings
- Securing the Authentication Process
- Physical Access Security
- Branch Office Domain Controllers
- RODC Features
- RODC Limitations and Considerations
- Deploying RODCs
- Demo: Install an RODC
- Demo: Advanced Password Replication Policy
- Password Replication Policies
- Summary

Implementing Account Security
- Introduction
- Account Security in Windows Server 2016
- Password Policies
- Account Lockout Policies
- Configuring Domain Password and Lockout Policies
- Demo: Account Policies
- Fine-Grained Password Policies
- Demo: Fine-Grained Password Policies
- Demo: Password Policies in PowerShell
- Demo: Resultant Policy
- Summary

Group Security and Authentication
- Introduction
- Restricted Groups
- Protected Users Security Groups
- Authentication Policies
- Authentication Silos
- Enhancing Password Authorization
- Summary

Auditing Active Directory
- Introduction
- Utilizing Auditing
- The Purpose of Auditing
- Types of Events
- Auditing Goals
- Auditing File and Object Access
- Advanced Auditing
- Demo: Auditing Configuration
- Demo: Advanced Auditing
- Demo: Access Auditing
- Summary

Configure Managed Service Accounts
- Introduction
- Overview of Service Accounts
- Challenges to Managing Service Accounts
- Managed Service Accounts
- Group MSAs
- Demo: Configure Group MSA
- Demo: Using MSA
- Summary

Overview of Advanced AD DS Deployments
- Introduction
- Domain Boundaries
- Forest Boundaries
- Reasons for Implementing Multiple Domains
- Reasons for Implementing Multiple Forests
- Deploying Domain Controllers in Azure
- Managing Objects
- Summary

Deploy Distributed AD Environment
- Introduction
- Domain Functional Levels
- Forest Functional Levels
- Deploying AD DS Domains
- DNS Considerations
- UPN Considerations
- Demo: Deploy Child Domain
- Summary

Trust Relationships
- Introduction
- Understanding Trust Relationships
- Types of Trusts
- How Trusts Work
- Forest Trusts
- Advanced Trust Settings
- Demo: Create a Forest Trust
- Demo: New Trust Wizard
- Summary

Overview of AD Replication
- Introduction
- AD DS Partitions
- AD DS Replication
- Types or Replication
- Resolving Replication Conflicts
- Summary

Configure AD Sites
- Introduction
- Reasons for Sites
- Overview of Sites and Subnets
- Moving Domain Controller Accounts
- Demo: Create a Site
- Demo: Using PowerShell
- Controlling Inter-Site Replication
- Defining Site Links
- Site Links
- Site Link Properties
- Demo: Site Link
- Bridgehead Servers
- Bridging Site Links
- Monitor and Manage Replication
- Summary