



20742: Identity with Windows Server® 2016

Duration: 5 Days

Method: Instructor-Led

Certification: Microsoft® Certified Solutions Associate (MCSA): Windows Server 2016 — Exam 3 of 3: 70-742 Identity with Windows Server® 2016

Course Description

This course teaches Information Technology (IT) Professionals how to deploy and configure Active Directory® Domain Services (AD DS) in a distributed environment, how to implement Group Policy, how to perform backup and restore, and how to monitor and troubleshoot Active Directory®-related issues with Windows Server® 2016. Additionally, this course teaches how to deploy other Active Directory® server roles such as Active Directory® Federation Services (AD FS) and Active Directory® Certificate Services (AD CS).

Target Audience

This course is intended for:

- IT Professionals who have some AD DS knowledge and experience and who aim to develop knowledge about identity and access technologies in Windows Server® 2016. This would typically include:
 - AD DS Administrators who are looking to train in identity and access technologies with Windows Server® 2012 or Windows Server® 2016.
 - System or Infrastructure Administrators with general AD DS experience and knowledge who are looking to cross-train in core and advanced identity and access technologies in Windows Server® 2012 or Windows Server® 2016.
- IT Professionals who are looking to consolidate their knowledge about AD DS and related technologies.
- IT Professionals who want to prepare for the third exam required for certification.



Microsoft Partner
Silver Learning



Prerequisites

To attend this course, participants should have:

- Some exposure to and experience with AD DS concepts and technologies in Windows Server® 2012 or Windows Server® 2016.
- Experience working with and configuring Windows Server® 2012 or Windows Server® 2016
- Experience and an understanding of core networking technologies such as IP addressing, name resolution, and Dynamic Host Configuration Protocol (DHCP).
- Experience working with and an understanding of Microsoft® Hyper-V® and basic server virtualization concepts.

Course Objectives

Upon successful completion of this course, participants will be able to:

- Install and configure domain controllers.
- Manage objects in AD DS by using graphical tools and Windows® PowerShell®.
- Implement AD DS in complex environments.
- Implement AD DS sites, and configure and manage replication.
- Implement and manage Group Policy Objects (GPOs).
- Manage user settings by using GPOs.
- Secure AD DS and user accounts.
- Implement and manage a certificate authority (CA) hierarchy with AD CS.
- Deploy and manage certificates.
- Implement and administer AD FS.
- Implement and administer Active Directory® Rights Management Services (AD RMS).
- Implement synchronization between AD DS and Azure AD.
- Monitor, troubleshoot, and establish business continuity for AD DS services.

Course Content

Module 1: Installing and Configuring Domain Controllers

- Overview of AD DS
- Overview of AD DS domain controllers
- Deploying a domain controller

Module 2: Managing Objects in AD DS

- Managing user accounts
- Managing groups in AD DS
- Managing computer objects in AD DS
- Using Windows® PowerShell® for AD DS administration
- Implementing and managing OUs



Course Content, *Continued*

Module 3: Advanced AD DS Infrastructure Management

- Overview of advanced AD DS deployments
- Deploying a distributed AD DS environment
- Configuring AD DS trusts

Module 4: Implementing and Administering AD DS Sites and Replication

- Overview of AD DS replication
- Configuring AD DS sites
- Configuring and monitoring AD DS replication

Module 5: Implementing Group Policy

- Introducing Group Policy
- Implementing and administering GPOs
- Group Policy scope and Group Policy processing
- Troubleshooting the application of GPOs

Module 6: Managing User Settings with Group Policy

- Implementing administrative templates
- Configuring Folder Redirection, software installation, and scripts
- Configuring Group Policy preferences

Module 7: Securing Active Directory Domain Services

- Securing domain controllers
- Implementing account security
- Implementing audit authentication
- Configuring managed service accounts

Module 8: Deploying and managing AD CST

- Deploying CAs
- Administering CAs
- Troubleshooting and maintaining CAs

Module 9: Deploying and managing certificates

- Deploying and managing certificate templates
- Managing certificate deployment, revocation, and recovery
- Using certificates in a business environment
- Implementing and managing smart cards



Course Content, *Continued*

Module 10: Implementing and Administering AD FS

- Overview of AD FS
- AD FS requirements and planning
- Deploying and configuring AD FS
- Overview of Web Application Proxy

Module 11: Implementing and Administering AD RMS

- Overview of AD RMS
- Deploying and managing an AD RMS infrastructure
- Configuring AD RMS content protection

Module 12: Implementing AD DS Synchronization with Microsoft® Azure® AD

- Planning and preparing for directory synchronization
- Implementing directory synchronization by using Azure® AD Connect
- Managing identities with directory synchronization

Module 13: Monitoring, Managing, and Recovering AD DS

- Monitoring AD DS
- Managing the Active Directory® database
- Active Directory® backup and recovery options for AD DS and other identity and access solutions

LABS INCLUDED

