

Identity with Windows Server 2016 (20742)

Duration: 5 Days (*Face-to-Face & Remote-Live*), or 35 Hours (*MOC On-Demand*)

Price: \$2495 (*Face-to-Face & Remote-Live*), or \$895 (*MOC On-Demand*)

Discounts: We offer multiple discount options. [Click here](#) for more information.

Delivery Options: Attend face-to-face in the classroom, [remote-live](#) or via [MOC On-Demand](#).

Students Will Learn

- Installing and configuring domain controllers
- Managing objects in AD DS by using graphical tools and Windows PowerShell
- Implementing AD DS in complex environments
- Implementing AD DS sites and configuring and managing replication
- Implementing and managing Group Policy Objects (GPOs)
- Managing user settings by using GPOs
- Securing AD DS and user accounts
- Implementing and managing a certificate authority (CA) hierarchy with AD CS
- Deploying and managing certificates
- Implementing and administering AD FS
- Implementing and administering Active Directory Rights Management Services (AD RMS)
- Implementing synchronization between AD DS and Azure AD
- Monitoring, troubleshooting and establishing business continuity for AD DS services

Course Description

This is a Microsoft Official Course (MOC) and includes Microsoft courseware and hands-on labs. This course teaches 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).

This course is primarily intended for existing 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. This would also include 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.

The secondary audience for this course includes IT professionals who take this course as preparation material for exam [70-742: Identity with Windows Server 2016](#).

Course Prerequisites

Before attending this course, students must 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
- An awareness of basic security best practices
- Hands-on working experience with Windows client operating systems such as Windows 7, Windows 8, Windows 8.1, or Windows 10
- Basic experience with the Windows PowerShell command-line interface

Completion of the courses [Installation, Storage, and Compute with Windows Server 2016](#) and [Networking with Windows Server 2016](#) or equivalent knowledge.

About MOC On-Demand

This course is also available via Microsoft Official Courses On-Demand. MOC On-Demand uses a combination of streaming video, text, lab exercises and assessment checks throughout the course. MOC On-Demand courses are available for 90 days and recommend the following system requirements:

- Browser: Current version of Internet Explorer, Microsoft Edge, Google Chrome or Firefox
- Internet: Broadband Internet connection of over 4Mbps
- Screen Resolution: 1280 x 1024 or higher

Course Overview

Module 1: Installing and Configuring Domain Controllers

This module describes the features of AD DS and how to install domain controllers (DCs). It also covers the considerations for deploying DCs.

Lessons

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

Labs

- Deploying AD DS
- Deploying domain controllers by performing domain controller cloning
- Administering AD DS

After completing this module, students will be able to:

- Describe AD DS and its main components
- Describe the purpose and roles of domain controllers
- Describe the considerations for deploying domain controllers

Module 2: Managing Objects in AD DS

This module describes how to use various techniques to manage objects in AD DS. This includes creating and configuring user, group, and computer objects.

Lessons

- 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

Labs

- Creating and managing groups in AD DS
- Creating and configuring user accounts in AD DS
- Managing computer objects in AD DS

- Delegate administration for OUs
- Creating and modifying AD DS objects with Windows PowerShell

After completing this module, students will be able to:

- Manage user accounts in AD DS
- Manage groups in AD DS
- Manage computer objects in AD DS
- Use Windows PowerShell for AD DS administration
- Implement and manage OUs
- Administer AD DS

Module 3: Advanced AD DS Infrastructure Management

This module describes how to plan and implement an AD DS deployment that includes multiple domains and forests. The module provides an overview of the components in an advanced AD DS deployment, the process of implementing a distributed AD DS environment, and the procedure for configuring AD DS trusts.

Lessons

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

Labs

- Implementing forest trusts
- Implementing child domains in AD DS

After completing this module, students will be able to:

- Describe the components of an advanced AD DS deployment
- Deploy a distributed AD DS environment.
- Configure AD DS trusts

Module 4: Implementing and Administering AD DS Sites and Replication

This module describes how to plan and implement an AD DS deployment that includes multiple locations. The module explains how replication works in a Windows Server 2016 AD DS environment.

Lessons

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

Labs

- Modifying the default site
- Creating additional sites and subnets
- Configuring AD DS replication
- Monitoring and troubleshooting AD DS replication

After completing this module, students will be able to:

- Describe how AD DS replication works
- Configure AD DS sites to help optimize authentication and replication traffic
- Configure and monitor AD DS replication

Module 5: Implementing Group Policy

This module describes how to implement a GPO infrastructure. The module provides an overview of the components and technologies that compose the Group Policy framework.

Lessons

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

Labs

- Creating and configuring GPOs
- Managing GPO scope

- Verify GPO application
- Troubleshooting GPOs

After completing this module, students will be able to:

- Explain what Group Policy is
- Implement and administer GPOs
- Describe Group Policy scope and Group Policy processing
- Troubleshoot GPO application

Module 6: Managing User Settings with Group Policy

This module describes how to configure Group Policy settings and Group Policy preferences. This includes implementing administrative templates, configuring folder redirection and scripts, and configuring Group Policy preferences.

Lessons

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

Labs

- Using administrative templates to manage user settings
- Implement settings by using Group Policy preferences
- Configuring Folder Redirection
- Planning Group Policy (optional)

After completing this module, students will be able to:

- Implement administrative templates
- Configure Folder Redirection, software installation, and scripts
- Configure Group Policy preferences

Module 7: Securing Active Directory Domain Services

This module describes how to configure domain controller security, account security, password security, and Group Managed Service Accounts (gMSA).

Lessons

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

Labs

- Implementing security policies for accounts, passwords, and administrative groups
- Deploying and configuring an RODC
- Creating and associating a group MSA

After completing this module, students will be able to:

- Secure domain controllers
- Implement account security
- Implement audit authentication

- Configure managed service accounts (MSAs)

Module 8: Deploying and Managing AD CS

This module describes how to implement an AD CS deployment. This includes deploying, administering, and troubleshooting CAs.

Lessons

- Deploying CAs
- Administering CAs
- Troubleshooting and maintaining CAs

Labs

- Deploying an offline root CA
- Deploying an enterprise subordinate CA

After completing this module, students will be able to:

- Deploy CAs
- Administer CAs
- Troubleshoot and maintain CAs

Module 9: Deploying and Managing Certificates

This module describes how to deploy and manage certificates in an AD DS environment. This involves deploying and managing certificate templates, managing certificate revocation and recovery, using certificates in a business environment, and implementing smart cards.

Lessons

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

Labs

- Configuring certificate templates
- Enrolling and using certificates
- Configuring and implementing key recovery

After completing this module, students will be able to:

- Deploy and manage certificate templates
- Manage certificates deployment, revocation, and recovery
- Use certificates in a business environment
- Implement and manage smart cards

Module 10: Implementing and Administering AD FS

This module describes AD FS and how to configure AD FS in a single-organization scenario and in a partner-organization scenario.

Labs

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

Labs

- Configuring AD FS prerequisites
- Installing and configuring AD FS
- Configuring an internal application for AD
- Configuring AD FS for federated business partners

After completing this module, students will be able to:

- Describe AD FS
- Explain how to deploy AD FS
- Explain how to implement AD FS for a single organization
- Explain how to extend AD FS to external clients
- Implement single sign-on (SSO) to support online services

Module 11: Implementing and Administering AD RMS

This module describes how to implement an AD RMS deployment. The module provides an overview of AD RMS, explains how to deploy and manage an AD RMS infrastructure, and explains how to configure AD RMS content protection.

Lessons

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

Labs

- Installing and configuring AD RMS
- Configuring AD RMS templates
- Using AD RMS on clients

After completing this module, students will be able to:

- Describe AD RMS
- Deploy and manage an AD RMS infrastructure
- Configure AD RMS content protection

Module 12: Implementing AD DS Synchronization with Microsoft Azure AD

This module describes how to plan and configure directory syncing between Microsoft Azure Active Directory (Azure AD) and on-premises AD DS. The modules describes various sync scenarios, such as Azure AD sync, AD FS and Azure AD, and Azure AD Connect.

Lessons

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

Labs

- Preparing for directory synchronization
- Configuring directory synchronization
- Managing Active Directory users and groups and monitoring directory synchronization

After completing this module, students will be able to:

- Plan and prepare for directory synchronization
- Implement directory synchronization by using Microsoft Azure Active Directory Connect (Azure AD Connect)
- Manage identities with directory synchronization

Module 13: Monitoring, Managing and Recovering AD DS

This module describes how to monitor, manage, and maintain AD DS to help achieve high availability of AD DS.

Lessons

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

Labs

- Backing up and restoring AD DS
- Recovering objects in AD DS

After completing this module, students will be able to:

- Monitor AD DS
- Manage the Active Directory database
- Describe the backup and recovery options for AD DS and other identity access solutions

Hands On Technology Transfer
The Best Way to Transfer Technology Skills

1 Village Square, Suite 8
14 Fletcher Street
Chelmsford, MA 01824

Copyright© 2020