

# **Identity with Windows Server 2016 - MOC On Demand (MS-20742)**

**Modality:** On Demand

**Duration:** 2 Days

**SATV Value:** 2

## **About this course:**

A Server Operating System is a platform to run network applications. Here, in this course, we will focus on the Windows Server 2016, which is a Server OS.

This course is an intermediate level course that will help a student learn about the deployment and configuration of Active Directory Domain Services (AD DS), and how to control it in a distributed environment. The course shall also cover the implementation of Group Policy, the backup and restore aspect, and the troubleshooting of Active Directory in the Windows 2016.

Also, the course outline covers the deployment of other AD Servers such as Federation Services (AD FS) and Certificate Services (AD CS). At the end of this course, students shall be fully prepared to take the exam for the certification of Microsoft 70-742: Identity with Windows Server 2016.

A Windows Server Administrator earns \$55,929 annually on average.

## **Course Objective:**

At the end of this course, students shall know about:

- Installation and configuration of Domain Controllers
- Management of AD DS with graphical tools and Windows PowerShell
- Implementation of AD DS in complex functional environments
- Implementation, configuration, and management of AD DS sites and replication
- Implementation and management of GPOs
- Management of GPO user settings
- Security of AD DS user accounts
- Implementation and management of CA with AD CS hierarchy
- Deployment and management of certifications
- Implementation and administration of AD FS
- Implementation and administration of AD RMS – Active Directory Rights Management Services
- Implementation of Synchronization between AD DS and Azure AD
- Monitoring, troubleshooting, and establishing AD DS services

## **Audience:**

This course targets:

- IT professionals with experience of AD DS, who want to learn about identity and access technology with the Windows Server 2016, which includes:
- AD DS admin officers, who wish to learn about identity and access technology with the Windows Server 2012 or Windows Server 2016
- System Administrators who prior knowledge of AD DS and want to widen their horizons by learning about advance identity and access technology with the Windows Server 2012 or Windows Server 2016

## **Prerequisites:**

Before enrolling for the course, students should fulfill the following requirements:

- Previous experience of working with AD DS technologies and core concepts in Windows 2012 or 2016
- General experience of configuring Windows Server 2012 or Windows Server 2016
- Strong Concepts of network terminologies including IP addressing, Dynamic Host Configuration Protocol (DHCP), and name resolution
- Knowledge of Microsoft Hyper-V and virtualization concepts
- Understanding of best security practices
- Experience of working on Windows Client OS such as Windows 8, Windows 8.1, Windows 7 or Windows 10
- Understanding of Windows PowerShell command-line interface

## **Course Outline:**

### **Module 1: Installing and configuring domain controllers**

This module describes 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

### **Lab : Deploying and administering AD DS**

- 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 of domain controllers and their roles.
- 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

### Lab : Managing AD DS objects

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

### Lab : Administering 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

### Lab : Domain and trust management in AD DS

- 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.
- Explain how to deploy a distributed AD DS environment.
- Explain how to 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

### **Lab : Implementing AD DS sites and replication**

- 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

### **Lab : Implementing a Group Policy infrastructure**

- Creating and configuring GPOs
- Managing GPO scope

## **Lab : Troubleshooting Group Policy infrastructure**

- 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

## **Lab : Managing user settings with GPOs**

- 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

## **Lab : Securing AD DS**

- 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

## **Lab : Deploying and configuring a two-tier CA hierarchy**

- 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

### **Lab : Deploying and using certificates**

- 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.

### **Lessons**

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

### **Lab : Implementing AD FS**

- 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

## Lab : Implementing an AD RMS infrastructure

- 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.
- Describe usage scenarios for AD RMS.
- Describe the AD RMS components.

## 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

## Lab : Configuring directory synchronization

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

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

## Lab : Recovering objects in AD DS

- 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.