Identity with Microsoft Windows Server 2016 (MS-20742)

Modality: Virtual Classroom

Duration: 5 Days

SATV Value: 5

About this course:

The Microsoft Server 2016, previously known as Windows Server vNext, is a server OS developed specially so that it can perform its role as running network applications' platform. This is an intermediate difficulty level course. It has been designed to give training in Microsoft Server 2016 to the IT professionals. This course will enable them to configure and deploy AD DS without any difficulty in a distributed environment. Not only this, the course will also teach the professionals techniques like backing up and restoring, incorporating the Group Policy, and mend any issues that might occur in Active Directory with Windows Server 2016. Furthermore, they will be taught the deploying method for Active Directory server roles AD FS and AD CS. Regardless, however, the primary purpose of this course is to prepare the IT professionals for the Microsoft 70-742: Identity with Windows Server 2016 certification.

On average, the earning of a Windows Server Administrator amounts to be $55,929 per annum.

Learning objectives:

The course has the following learning objectives:

- Executing the Active Directory DS sites, and subsequently regulating and configuring the replication process
- Executing and regulating AD RMS (Active Directory Rights Management Services)
- Executing and regulating GPOs (Group Policy Projects)
- Executing AD DS in complicated atmospheres
- Configuring and installing domain controllers
- Regulating and deploying certificates
- Securing the user accounts and AD DS
- Troubleshooting, regulating, and designing business continuity for services pertaining to AD DS
- Making use of GPOs to regulate user settings
- Executing and regulating AD DS with CA (certificate authority) hierarchy
- Executing and administering AD FS
- Executing the synchronization between the Azure AD and AD DS
- Making use of Windows PowerShell and various other graphical tools in order to regulate AD DS objects

Audience:

This course has been designed for and is suitable for those who are expert IT professionals and do

have some fundamental knowledge of AD DS. These people, then, want to gain more insight and expertise in access technologies and identities in Windows Server 2016. This involves:

- The AD DS Administrators: professionals who want to gain access to Windows Server 2012/Windows Server 2016 comprising technologies and attain training in advanced identity
- Infrastructure or system administrators, having some general knowledge on the concepts of AD DS. For professionals who are eager to cross-train in advanced and also core identity. This will also include those people who want to attain access to Windows Server 2016 or 2012 based technologies

Requirements:

The course has some important requirements that should be fulfilled prior to starting it. These include:

- Having an experience in configuring Windows Server 2016 or 2012
- Having practical experience with operating in Windows 7, 8, 8.1, and other Windows client OS.
- Having experience in foundational virtualization concepts and Microsoft Hyper-V
- Having experience in networking technologies such as name resolution, IP addressing, DHCP etc.
- Having foundational knowledge on best security practices
- Must be having foundational experience of working with the command-line interface of Windows PowerShell
- Must be having foundational experience of AD DS based technologies as well as the concepts in Windows Server 2016 or 2012

Suggested pre-taken courses:

- Administering Windows Server 2012 (MS-20411)
- Automating Administration with Windows PowerShell (MS-10961)

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