Active Directory Services with Windows Server (MS-10969)

Modality: Virtual Classroom

Duration: 5 Days

SATV Value: 5

CLC:

NATU:

SUBSCRIPTION: Master

About this course:

This 5- day Microsoft official IT Ops Training course give students hands on instruction and training for governing Active Directory technologies in Windows Server 2012 and Windows Server 2012 R2. You will acquire the skills you required to better manage and safe data access and information, make simpler deployment and administration of your individuality infrastructure, and offer more protected access to data. You will learn how to configure several of the key features in Windows Server training and Active Directory Services such as Active Directory Domain Services (AD DS), Group Strategy, Dynamic Access Control (DAC), Work Folders, Work Place Join, Certificate Service area, Rights Management Services (RMS), Federation Service area, as well as incorporating your on-premise setting with cloud centered technologies such as Windows Azure Active Directory. As part of the learning experience, you will execute hands-on exercises in a virtual lab environment.

A professional Microsoft Windows Server Administrator earns an average of **$82,000** per year.

Course Objectives:

After finishing this course, students will be capable to:

- Comprehend accessible solutions for identity administration and be capable to address circumstances with correct solutions
- Set up and manage AD DS in Windows Server 2012
- Protected AD DS deployment
- Incorporate AD DS sites, configure and handle replication
- Incorporate and manage Group Policy
- Handle user settings with Group Policy
- Execute certification authority (CA) grading with AD CS and how to manage CAs.
- Incorporate, deploy and handle certificates
- Apply and manage AD RMS
- Apply and administer AD FS
- Safe and provision data entree utilizing technologies such as Dynamic Access Control, Work Folders and Workplace Link
- Observe, troubleshoot and create business stability for AD DS services.
- Implement Windows Azure Active Directory.
- Implement and administer Active Directory Lightweight Directory Services (AD LDS).

Audience:

This course is proposed for Information Technology (IT) Authorities who have Active Directory Domain Services (AD DS) knowledge and are looking to for a particular course that will further cultivate information and skills using Access and Information Protection technologies in Windows Server 2012 and Windows Server 2012 R2. This would usually include:

- AD DS Managers who are considering furthering increase skills in the current Access and Information Protection technologies with Windows Server 2012 and Windows Server 2012 R2
- Structure or Setup administrators with corporate AD DS experience and understanding who are looking to construct upon that basic knowledge and cross-train into progressive Active Directory technologies in Windows Server 2012 and Windows Server 2012 R2
- IT Specialists who have engaged the 10967A: Basics of a Windows Server Infrastructure course and are considering to construct upon that Active directory information

Prerequisites:

- Before attending this course for windows server training, students must have:
- Familiarity working with Active Directory Domain Services (AD DS)
- Experience working in a Windows Server Structure enterprise setting
- Knowledge working with and troubleshooting main networking structure technologies such as name resolution, IP Addressing, Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP)
- Understanding working with Hyper-V and Server Virtualization conceptions
- An alertness and understanding of common safety best practices
- Understanding working hands on with Windows client functioning systems such as Windows Vista, Windows 7 or Windows 8

Course Outline:

Module 1: Overview of Access and Information Protection

This module provides an overview of multiple Access and Information Protection (AIP) technologies and services what are available with Windows Server 2012 and Windows Server 2012 R2 from a business perspective and maps business problems to technical solutions. It also includes coverage of Forefront Identify Manager (FIM).

Lessons

- Introduction to Access and Information Protection Solutions in Business
- Overview of AIP Solutions in Windows Server 2012
- Overview of FIM 2010 R2

Lab : Choosing an Appropriate Access and Information Protection Management Solution

After completing this module students will be able to:

- Describe Access and Information Protection solutions in business.

- Describe Access and Information Protection solutions in Windows Server 2012 and Windows Server 2012 R2.
- Describe Microsoft Forefront Identity Manager (FIM) 2010 R2.

Module 2: Advanced Deployment and Administration of AD DS

This module explains how to deploy AD DS remotely and describes the virtualization safeguards, cloning abilities and extending AD DS to the cloud.

Lessons

- Deploying AD DS
- Deploying and Cloning Virtual Domain Controllers
- Deploying Domain Controllers in Windows Azure
- Administering AD DS

Lab : Deploying and Administering AD DS

After completing this module, students will be able to:

- Describe and perform various deployment techniques for AD DS.
- Describe virtual domain controller deployment considerations.
- Explain how new technologies in Windows Server 2012 and Windows Server 2012 R2 support virtual domain controllers.
- Describe Domain Controller cloning.
- Implement AD DS using the tools provided in Windows Server 2012 and Windows Server 2012 R2.

Module 3: Securing AD DS

This module describes the threats to domain controllers and what methods can be used to secure the AD DS and its domain controllers.

Lessons

- Securing Domain Controllers
- Implementing Account Security
- Implementing Audit Authentication

Lab : Securing AD DS

After completing this module, students will be able to:

- Understand the importance of securing domain controllers.
- Describe the benefit of read-only domain controllers (RODCs).
- Explain and implement password and account lockout policies.
- Implement audit authentication.

Module 4: Implementing and Administering AD DS Sites and Replication

This module explains how AD DS replicates information between domain controllers within a single site and throughout multiple sites. This module also explains how to create multiple sites and how to monitor replication to help optimize AD DS replication and authentication traffic.

Lessons

- Overview of AD DS Replication
- Configuring AD DS Sites
- Configuring and Monitoring AD DS Replication

Lab : Implementing AD DS Sites and Replication

After completing this module, students will be able to:

- Describe AD DS replication.
- Configure AD DS sites.
- Configure and monitor AD DS replication.

Module 5: Implementing Group Policy

This module describes Group Policy, how it works, and how best to implement it within your organization.

Lessons

- Introducing Group Policy
- Implementing and Administering GPOs
- Group Policy Scope and Group Policy Processing
- Troubleshooting the Application of GPOs

Lab : Implementing and Troubleshooting a Group Policy Infrastructure

After completing this module, students will be able to:

- Describe Group Policy.
- Implement and administer GPOs.
- Describe Group Policy scope and Group Policy processing.
- Troubleshoot the application of GPOs.

Module 6: Managing User Settings with Group Policy

This module describes how to how to use GPO Administrative Templates, Folder Redirection, and Group Policy features to configure users? computer settings.

Lessons

- Implementing Administrative Templates
- Configuring Folder Redirection and Scripts
- Configuring Group Policy Preferences

Lab : Managing User Desktops with Group Policy

After completing this module, students will be able to:

- Implement Administrative Templates.
- Configure Folder Redirection and scripts.
- Configure Group Policy preferences.

Module 7: Deploying and Managing AD CS

This module explain how to deploy and manage Certificate Authorities (CAs) with Active Directory Certificate Services (AD CS)

Lessons

- Deploying CAs
- Administering CAs
- Troubleshooting, Maintaining, and Monitoring CAs

Lab : Deploying and Configuring a Two-Tier CA Hierarchy

After completing this module, students will be able to:

- Deploy Certificate Authorities.
- Administer Certificate Authorities.
- Troubleshoot, maintain, and monitor Certificate Authorities.

Module 8: Deploying and Managing Certificates

This module describes certificate usage in business environments and explains how to deploy and manage certificates, configure certificate templates and manage enrolment process. This module also covers the deployment and management of smart cards.

Lessons

- Using Certificates in a Business Environment
- Deploying and Managing Certificate Templates
- Managing Certificates Deployment, Revocation, and Recovery
- Implementing and Managing Smart Cards

Lab : Deploying and Using Certificates

After completing this module, students will be able to:

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

Module 9: Implementing and Administering AD RMS

This module introduces Active Directory Rights Management Services (AD RMS). It also describes how to deploy AD RMS, how to configure content protection, and how to make AD RMS?protected documents available to external users.

Lessons

- Overview of AD RMS
- Deploying and Managing an AD RMS Infrastructure
- Configuring AD RMS Content Protection
- Configuring External Access to AD RMS

Lab : Implementing an AD RMS Infrastructure

After completing this module, students will be able to:

- Describe AD RMS.
- Explain how to deploy and manage an AD RMS infrastructure.
- Explain how to configure AD RMS content protection.
- Explain how to configure external access to AD RMS.

Module 10: Implementing and Administering AD FS

This module explains AD FS, and then provides details on how to configure AD FS in both a single organization scenario and in a partner organization scenario. This module also describes the Web Application Proxy feature in Windows Server 2012 R2 that functions as an AD FS proxy and reverse proxy for web-based applications.

Lessons

- Overview of AD FS
- Deploying AD FS
- Implementing AD FS for a Single Organization
- Deploying AD FS in a Business-to-Business Federation Scenario
- Extending AD FS to External Clients

Lab : Implementing AD FS

After completing this module, students will be able to:

- Describe AD FS.
- Explain how to configure the AD FS prerequisites, and deploy AD FS services.

- Describe how to implement AD FS for a single organization.
- Deploy AD FS in a business-to-business federation scenario.
- Deploy the Web Application Proxy.

Module 11: Implementing Secure Shared File Access

This module explains how to use Dynamic Access Control (DAC), Work Folders, Work place Join and how to plan and implement these technologies.

Lessons

- Overview of Dynamic Access Control
- Implementing DAC Components
- Implementing DAC for Access Control
- Implementing Access Denied Assistance
- Implementing and Managing Work Folders
- Implementing Workplace Join

Lab : Implementing Secure File Access

After completing this module, students will be able to:

- Describe DAC.
- Implement DAC components.
- Implement DAC for access control.
- Implement access-denied assistance.
- Implement and manage Work Folders.
- Implement Workplace Join.

Module 12: Monitoring, Managing, and Recovering AD DS

This module explains how to use tools that help monitor performance in real time, and how to record performance over time to spot potential problems by observing performance trends. This module also explains how to optimize and protect your directory service and related identity and access solutions so that if a service does fail, you can restart it as quickly as possible.

Lessons

- Monitoring AD DS
- Managing the AD DS Database
- AD DS Backup and Recovery Options for AD DS and Other Identity and Access Solutions

Lab : Monitoring AD DSLab : Recovering Objects in AD DS

After completing this module, students will be able to:

- Monitor AD DS.
- Manage the AD DS database.

- Recover objects from the AD DS database.

Module 13: Implementing Windows Azure Active Directory

This module explains the concepts and technologies in Windows Azure Active Directory and how to implement and integrate it within your organization

Lessons

- Overview of Windows Azure AD
- Managing Windows Azure AD Accounts

Lab : Implementing Windows Azure AD

After completing this module, students will be able to:

- Describe Windows Azure AD.
- Administer Azure AD.

Module 14: Implementing and Administering AD LDS

This module explains how to deploy and configure Active Directory Lightweight Directory Services (AD LDS)

Lessons

- Overview of AD LDS
- Deploying AD LDS
- Configuring AD LDS Instances and Partitions
- Configuring AD LDS Replication
- Integrating AD LDS with AD DS

Lab : Implementing and Administering AD LDS

After completing this module, students will be able to:

- Describe AD LDS.
- Explain how to deploy AD LDS.
- Explain how to configure AD LDS instances and partitions.
- Explain how to configure AD LDS replication.