Course 10969 B: Active Directory Services with Windows Server 2012

Days: 5

Prerequisites: Before attending this course, students must have:

- Experience working with AD DS
- Experience working in a Windows Server infrastructure enterprise environment
- Experience working with and troubleshooting core networking infrastructure technologies such as name resolution, IP Addressing, Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP)
- Experience with Hyper-V and Server Virtualization concepts
- An awareness and understanding of general security best practices
- Experience working hands on with Windows Client operating systems such as Windows Vista, Windows 7 or Windows 8

Audience: IT Professionals who work with Active Directory

Description: Get hands-on instruction and practice administering Active Directory technologies in Windows Server 2012 and Windows Server 2012 R2 in this 5-day Microsoft Official Course. You will learn the skills you need to better manage and protect data access and information, simplify deployment and management of your identity infrastructure, and provide more secure access to data from virtually anywhere.

You will learn how to configure some of the key features in Active Directory such as Active Directory Domain Services, Group Policy, Dynamic Access Control, Work Folders, Workplace Join, Certificate Services, Rights Management Services and Federation Services, as well as integrating your on premise environment with cloud based technologies such as Windows Azure Active Directory. As part of the learning experience, you will perform hands-on exercises in a virtual lab environment.

NOTE: This course is based on Windows Server 2012 and Windows Server 2012 R2. This course is designed for experienced IT professionals who support medium to large enterprises and have fundamental knowledge and experience administering Active Directory.

OUTLINE:

MODULE 1: OVERVIEW OF ACCESS AND INFORMATION PROTECTION

This module explains Access and Information Protection (AIP) solutions from the business perspective and maps business problems to technical solutions.

LESSONS

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

LAB: CHOOSING AN APPROPRIATE ACCESS AND INFORMATION PROTECTION MANAGEMENT SOLUTION

- Analyze the Lab Scenario and Identify Business Requirements
- Propose a 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 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

- Deploying AD DS
- Deploying Domain Controller by Performing Domain Controller Cloning
- 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 support virtual domain controllers.
- Describe Domain Controller cloning.
- Implement AD DS using the tools provided in Windows Server 2012.

MODULE 3: SECURING ACTIVE DIRECTORY DOMAIN SERVICES

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
- Audit Authentication

LAB: SECURING ACTIVE DIRECTORY DOMAIN SERVICES

- Implementing Security Policies for Accounts and Passwords and Administrative Groups
- Deploying and Configuring a RODC

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.

Course 10969 B: Active Directory Services with Windows Server 2012

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

- Creating Subnets and Sites
- Deploying an Additional Domain Controller
- Configuring AD DS Replication
- Troubleshooting AD DS 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 in 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

- Creating and Configuring GPOs
- Managing GPO Scope
- Verifying GPO Application
- Managing GPOs
- Troubleshooting GPOs

AFTER COMPLETING THIS MODULE, STUDENTS WILL BE ABLE TO:

- Describe Group Policy.
- Implement and administer GPOs.
- Describe Group Policy scope and Group Policy processing.
- Troubleshooting 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

- Implementing Settings by Using Group Policy Preferences
- Configuring Folder Redirection

AFTER COMPLETING THIS MODULE, STUDENTS WILL BE ABLE TO:

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

Course 10969 B: Active Directory Services with Windows Server 2012

MODULE 7: DEPLOYING AND MANAGING ACTIVE DIRECTORY CERTIFICATE SERVICES

This module explains how to deploy and manage CAs with AD CS

LESSONS

- Deploying CAs
- Administering CAs
- Troubleshooting, Maintaining, and Monitoring 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, maintain, and monitor CAs.

MODULE 8: DEPLOYING AND MANAGING CERTIFICATES

This module explains how to deploy and manage certificates, configure certificate templates and manage enrollment process. Also, this module describes certificate usage in business environments and about deployment and management of smart cards.

LESSONS

- Deploying and Managing Certificate Templates
- Managing Certificates 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 business environments.
- Implement and manage smart cards.

MODULE 9: IMPLEMENTING AND ADMINISTERING ACTIVE DIRECTORY RIGHTS MANAGEMENT SERVICES

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 AD RMS INFRASTRUCTURE

- Installing and Configure AD RMS
- Configuring AD RMS Templates
- Using ADRMS on Clients
- Configuring AD RMS Monitoring and Reporting

Course 10969 B: Active Directory Services with Windows Server 2012

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

- Installing and Configuring AD FS
- Configuring an Internal Application for AD FS
- Configuring AD FS for a Federated Business Partner
- Configuring a Web Application Proxy

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

- Preparing for DAC Deployment
- Implementing DAC
- Validating and Remediating DAC
- Implementing Work Folders

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.

Course 10969 B: Active Directory Services with Windows Server 2012

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 DS

- Monitoring AD DS with Performance Monitor

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 AD DS database.
- Recover objects from the AD DS database.

MODULE 13: IMPLEMENTING WINDOWS AZURE ACTIVE DIRECTORY

This module explains how to implement Windows Azure Active Directory.

LESSONS

- Overview of Windows Azure Active Directory
- Administering Windows Azure Active Directory

LAB: IMPLEMENTING AZURE AD

- Planning to Implement Azure AD
- Administering 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 AD LDS.

LESSONS

- Overview of AD LDS
- Deploying AD LDS
- Configuring AD LDS Instances and Partitions
- Configuring AD LDS Replication

LAB: IMPLEMENTING AND ADMINISTERING AD LDS

- Configuring AD LDS Instances and Partitions
- Configuring AD LDS Replication

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.