Active Directory Services with Windows Server

Duration: 40 Hours (5 Days)

Course Overview

The "Active Directory Services with Windows Server" course is a comprehensive program designed for IT professionals looking to enhance their knowledge and skills in managing and implementing Active Directory technologies within Windows Server environments. Throughout the course, learners will delve into various aspects of Active Directory Services (AD DS), including deployment, administration, security, and troubleshooting. Module 1 kicks off with an introduction to Access and Information Protection (AIP) solutions, highlighting their importance in business and exploring the AIP features in Windows Server 2012, as well as the functionality of Forefront Identity Manager (FIM) 2010 R2. As learners progress through the modules, they will gain expertise in advanced deployment techniques, securing domain controllers, implementing Group Policy, managing certificates with Active Directory Certificate Services (AD CS), and administering rights with Active Directory Rights Management Services (AD RMS).The course also covers federation services with Active Directory Federation Services (AD FS), secure file access using Dynamic Access Control, and monitoring and recovery of AD DS. The training extends to Microsoft Azure Active Directory, providing insights into cloud-based identity services, and wraps up with Active Directory Lightweight Directory Services (AD LDS) for those who need to implement directory services in a distributed environment. Overall, this course equips learners with the necessary skills to manage and maintain a secure and efficient Active Directory infrastructure, including both on-premises Microsoft Active Directory Domain Services and Microsoft Azure Active Directory training components, ensuring they are well-versed in a variety of business scenarios.

Audience Profile

Master Active Directory Services with Windows Server in our comprehensive course designed for IT professionals seeking advanced skills. Target Audience for the Course:

- Systems Administrators
- Network Administrators
- IT Managers
- Technical Support Specialists
- Active Directory Engineers
- Security Analysts
- Infrastructure Architects
- IT Professionals aiming to specialize in Windows Server
- IT Consultants
- Professionals preparing for Microsoft certification exams related to Windows Server Active Directory Services

Course Syllabus

Module 1: Overview of Access and Information Protection

This module provides an overview of multiple Access and Information Protection (AIP) technologies and services 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 Identity 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

- 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

- 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 AD DS and its domain controllers.

Lessons

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

Lab: Securing AD DS

- Understand the importance of securing domain controllers.
- Describe the benefits 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

- 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

- 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 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

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

Module 7: Deploying and Managing AD CS

This module explains 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

- 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 the enrollment 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 Certificate Deployment, Revocation, and Recovery
- Implementing and Managing Smart Cards

Lab: Deploying and Using Certificates

- Use certificates in business environments.
- Deploy and manage certificate templates.
- Manage certificate 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, configure content protection, and 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

- 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 provides details on how to configure AD FS in both a single organization scenario and 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

- 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, and Workplace 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

- 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 DS

Lab: Recovering Objects in AD DS

- 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

- 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

- 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.