BOOST
THE LEADING TRAINING PROVIDER

Information Technology

Active Directory with Windows Server

Course Introduction

This training course is designed to provide participants with the knowledge and skills needed to better manage and protect data access and information, simplify deployment and management of identity infrastructure, and provide more secure access to data. This course will enable participants to know how to configure some of the key features in Active Directory such as Active Directory Domain Services (AD DS), Group Policy, Dynamic Access Control (DAC), Work Folders, Work Place Join, Certificate Services, Rights Management Services (RMS), Federation Services, as well as integrating on premise environment with cloud-based technologies such as Windows Azure Active Directory.

Target Audience

This training course is designed for IT professionals with Active Directory Domain Services (AD DS) experience and seeking to upgrade their knowledge and skills using Access and Information Protection technologies in Windows Server 2012 and Windows Server 2012 R2.

Learning Objectives

- Gain a comprehensive understanding of the available solutions for identity management and be able to address scenarios with appropriate solutions.
- Deploy and administer AD DS in Windows Server 2012.
- Secure AD deployment and AD DS sites, configure and manage replication
- Implement and manage Group Policy and its user settings.
- Implement certification authority (CA) hierarchy with AD CS and how to manage CAs.
- Administer, implement and manage AD RMS/ AD FS.

- Secure and provision data access using technologies such as Dynamic Access Control, Work Folders and Workplace Join
- Monitor, troubleshoot and establish business continuity for AD DS services.
- Implement and administer Windows Azure Active Directory and Active Directory Lightweight Directory Services (AD LDS).

Course Outline

- **Day 01**

  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)
  - Introduction to Access and Information Protection Solutions in Business
  - Overview of AIP Solutions in Windows Server 2012
  - Overview of 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.
  - Deploying AD DS
  - Deploying and Cloning Virtual Domain Controllers
  - Deploying Domain Controllers in Windows Azure
  - Administering AD DS

  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.
    - Securing Domain Controllers
    - Implementing Account Security
    - Implementing Audit Authentication
- **Day 02**

  #### 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.
    - Overview of AD DS Replication
    - Configuring AD DS Sites
    - Configuring and Monitoring 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.
    - Introducing Group Policy
    - Implementing and Administering GPOs
    - Group Policy Scope and Group Policy Processing
    - Troubleshooting 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.
    - Implementing Administrative Templates
    - Configuring Folder Redirection and Scripts

    - Configuring Group Policy Preferences
- **Day 03**

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

  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.
    - Using Certificates in a Business Environment
    - Deploying and Managing Certificate Templates
    - Managing Certificates Deployment, Revocation, and Recovery
    - Implementing and Managing 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.
    - Overview of AD RMS
    - Deploying and Managing an AD RMS Infrastructure
    - Configuring AD RMS Content Protection
    - Configuring External Access to AD RMS
- **Day 04**

  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.
  - 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

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.
  - 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

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

- **Day 05**

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

Module 14: Implementing and Administering AD LDS

- ◦ This module explains how to deploy and configure Active Directory Lightweight Directory Services (AD LDS)
- ◦ Overview of AD LDS
- ◦ Deploying AD LDS
- ◦ Configuring AD LDS Instances and Partitions
- ◦ Configuring AD LDS Replication
- ◦ Integrating AD LDS with AD DS

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
April 21, 2025	April 25, 2025	5 days	4250.00 $	UAE - Dubai
July 7, 2025	July 11, 2025	5 days	4950.00 $	Spain - Barcelona
Nov. 3, 2025	Nov. 7, 2025	5 days	4250.00 $	UAE - Abu Dhabi