

# Active Directory Services with Windows Server

Duration 5 Days

## COURSE DESCRIPTION

This course covers administering Active Directory technologies in Windows Server 2012 and Windows Server 2012 R2, managing and protecting data access and information, simplifying deployment and management of identity infrastructure, and providing more secure access to data. Students will also learn 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 and how to integrate an on-premise environment with cloud-based technologies such as Windows Azure Active Directory.

## COURSE OBJECTIVES

- Understand 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 DS deployment.
- Implement AD DS sites, configure and manage replication
- Implement and manage Group Policy
- Manage user settings with Group Policy
- Implement certification authority (CA) hierarchy with AD CS and how to manage CAs.
- Implement, deploy and manage certificates.
- Implement and manage AD RMS.
- Implement and administer 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 Windows Azure Active Directory.
- Implement and administer Active Directory Lightweight Directory Services (AD LDS).

## COURSE OUTLINE

### Module 1: Overview of Access and Information Protection

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

### Module 2: Advanced Deployment and Administration of AD DS

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

### Module 3: Securing AD DS

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

**Module 4: Implementing and Administering AD DS Sites and Replication**

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

**Module 5: Implementing Group Policy**

- 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**

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

**Module 7: Deploying and Managing AD CS**

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

**Module 8: Deploying and Managing Certificates**

- 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**

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

**Module 10: Implementing and Administering AD FS**

- 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**

- 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**

- Monitoring AD DS
- Managing the AD DS Database

- AD DS Backup and Recovery Options for AD DS and Other Identity and Access Solutions

#### **Module 13: Implementing Windows Azure Active Directory**

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

#### **Module 14: Implementing and Administering 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

#### **PREREQUISITES**

- Experience working with Active Directory Domain Services (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 working 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

#### **WHO SHOULD ATTEND**

- IT Professionals who have Active Directory Domain Services (AD DS) experience and are looking to for a single course that will develop knowledge and skills using Access and Information Protection technologies in Windows Server 2012 and Windows Server 2012 R2.
- AD DS Administrators who are looking to develop skills in the latest Access and Information Protection technologies with Windows Server 2012 and Windows Server 2012 R2.
- System or Infrastructure Administrators with general AD DS experience and knowledge who are looking to build upon that core knowledge and cross-train into advanced Active Directory technologies in Windows Server 2012 and Windows Server 2012 R2.
- IT Professionals who have taken the 10967A: Fundamentals of a Windows Server Infrastructure course and are looking to build upon that Active directory knowledge.