

Course Outline

6426- Configuring Identity and Access Solutions with Windows Server 2008 Active Directory



Duration: 3 day (18hours)

Target Audience:

This three-day instructor-led course provides the knowledge and skills that IT Professionals need to configure identity and access solutions with Windows Server 2008 Active Directory.

Prerequisites:

This course requires that students meet the following prerequisites:

- Technical knowledge equivalent to 6424: Fundamentals of Microsoft Server 2008 Active Directory
- Technical background knowledge and hands
- Technical background knowledge and hands
- Technical background knowledge and hands
- Technical background knowledge and hands

Topics Covered:

- Module 1: Exploring Identity and Access Solutions
 - The Business Case for Identity and access Control
 - Active Directory Server Roles in IDA Management
 - Overview of Identity Lifecycle Manager 2007
 - Lab 1: Exploring how Active Directory Server Roles Provide IDA Management Solutions

After completing this module, students will be able to:

- Identify and define IDA Solutions
- Identify Active Directory Server Roles in IDA Management
- Identify the uses and features of ILM 2007

- Module 2: Deploying and Managing Active Directory Certificate Services
 - Overview of PKI
 - Deploying a CA Hierarchy
 - Installing AD CS
 - Managing CAs
 - Lab 1: Installing and Configuring AD CS

After completing this module, students will be able to:

- Describe Public Key Infrastructure.
- Deploy a Certification Authority hierarchy.
- Install Active Directory Certificate Services.
- Manage a Certification Authority.

- Module 3: Deploying and Managing Certificates
 - Deploying Certificates by Using AD CS
 - Deploying Certificates by Using Auto enrollment
 - Revoking Certificates
 - Configure certificate templates.
 - Configure certificate recovery.
 - Lab: Configuring Active Directory Lightweight Directory Services
 - Configuring AD CS Certificate Templates
 - Configuring AD CS Web Enrollment
 - Configuring Certificate Autoenrollment
 - Configuring AD CS Certificate Revocation
 - Managing Key Archival and Recovery

After completing this module, students will be able to:

- Deploy certificates by using AD CS.
- Use autoenrollment to deploy certificates.
- Revoke certificates.
- Configure certificate templates.
- Configure certificate recovery..

- Module 4: Configuring Active Directory Lightweight Directory Services
 - Installing and Configuring AD LDS
 - Configuring AD LDS Instances
 - Configuring AD LDS Replication
 - Configuring AD LDS Integration with AD DS
 - Lab: Configuring Active Directory Lightweight Directory Services
 - Configuring an AD LDS Instance and an Application Partition
 - Configuring AD LDS Access Control
 - Configuring AD LDS Replication
 - Configuring AD DS and AD LDS Synchronization

After completing this module, students will be able to:

- Install and configure AD LDS.
- Configure AD LDS instances.
- Configure AD LDS replication.
- Configure AD LDS integration with AD DS.

- Module 5: Configuring Active Directory Federation Services
 - Overview of AD FS
 - AD FS Deployment Scenarios
 - Deploying AD FS
 - Implementing AD FS Claims
 - Lab: Configuring AD FS
 - Installing the AD FS Server Role
 - Configuring Certificate Requirements
 - Installing the AD FS Web Agent
 - Configuring the Web Server Application on the 6426B-NWTDC01 Virtual Computer
 - Configuring the Forest Trust and the Federated Trust Policies
 - Configuring the Federation Service Within the Internal Network

- Configuring the Federation Service Within the Extranet
- Testing the AD FS Implementation
- Installing the AD FS Server Role
- Configuring Certificate Requirements
- Configuring the AD FS Web Agent
- Configuring the Web Server Application on the 6426B-NWTDC01 Virtual Computer
- Configuring the Federation Trust Policies
- Configuring the Account Partner Federation Service
- Configuring the Resource Partner Federation Service
- Testing the AD FS Implementation

After completing this module, students will be able to:

- Identify the key aspects of AD FS.
- Explore AD FS deployment scenarios.
- Deploy AD FS.
- Implement AD FS claims.

➤ Module 6: Configuring Active Directory Rights Management Services

- Overview of AD RMS
- Installing and Configuring AD RMS Server Components
- Administering AD RMS
- Implementing AD RMS Trust Policies
 - Lab: Configuring Active Directory Rights Management Services
 - Installing and Configuring AD RMS Server Components
 - Configuring ADRMS Client Settings and AD RMS Templates
 - Managing AD RMS Rights Policy Templates
 - Testing AD RMS Functionality

After completing this module, students will be able to:

- Identify the key aspects of AD RMS.
- Install and configure AD RMS server components.
- Administer AD RMS.
- Implement AD RMS Trust Policies.

➤ Module 7: Maintenance Access Management Solutions

- Support for AD CS
- Maintaining AD LDS
- Maintaining AD FS
- Maintaining AD RMS
 - Lab: Maintaining Access Management Solutions
 - Configuring CA Event Auditing
 - Implementing Role-Based Administration in AD CS
 - Backing Up a CA
 - Reconfiguring AD RMS Cluster Settings
 - Generating AD RMS Reports
 - Configuring AD RMS Logging

After completing this module, students will be able to:

- Support AD CS.
- Maintain AD LDS.
- Maintain and Monitor AD FS.
- Maintain AD RMS.

- Module 8: Troubleshooting Identity and Access Solutions
 - Troubleshooting AD CS
 - Troubleshooting AD LDS
 - Troubleshooting AD FS Issues
 - Troubleshooting AD RMS Issues
 - Lab: Troubleshooting Active Directory Server Roles
 - Troubleshooting AD CS
 - Troubleshooting AD LDS
 - Resolving AD FS Issues
 - Solving AD RMS Issues

After completing this module, students will be able to:

- Troubleshoot AD CS.
- Troubleshoot AD LDS.
- Resolve AD FS issues.
- Solve AD RMS problems.