

Course Description: 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.

Who Should Attend: The audience for this course is IT Professionals interested in learning how to implement IDA solutions in an enterprise environment. Most students will be IT professionals who are responsible for integrating applications and platforms with enterprise directory and security services while increasing access to a growing number of customers and partners.

Prerequisites: Before attending this course, students must have technical knowledge equivalent to the course 6424: Fundamentals of Windows Server 2008 Active Directory, and technical background knowledge and hands-on experience of Active Directory Domain Services (AD DS from the AD TS foundation exam). This includes technical knowledge equivalent to the course 6425: Configuring and Troubleshooting Windows Server 2008 Active Directory Domain Services.

Benefits of Attendance: Upon completion of this course, students will be able to:

- Describe identity and access solutions.
- Configure Active Directory Certificate Services.
- Deploy and manage certificates.
- Configure Active Directory Lightweight Directory Services.
- Configure Active Directory Federation Services.
- Configure Active Directory Rights Management Services.
- Maintain access management solutions.
- Troubleshoot identity and access solutions.

Course Outline:

Module 1: Exploring IDA Solutions

Overview of IDA Management
Active Directory Server Roles in IDA Management
Overview of ILM 2007
Lab 1: Exploring IDA Solutions
Explore how Active Directory Server Roles will provide IDA Management solutions

Module 2: Configuring AD CS

Overview of PKI
Deploying a CA Hierarchy
Installing AD CS
Managing CA
Lab 2: Configuring AD CS
Installing the AD CS Server Role
Issuing and Installing a Subordinate Certificate
Publishing the CRL

Module 3: Deploying and Managing Certificates

Deploying Certificates by Using AD CS
Deploying Certificates by Using Autoenrollment
Revoking Certificates
Configuring Certificate Templates
Configuring Certificate Recovery
Lab 3: Deploying and Managing Certificates
Configuring AD CS Web Enrollment
Configuring Certificate Enrollment
Configuring AD CS Certificate Revocation
Configuring AD CS Certificate Templates
Managing Key Archival and Recovery

Module 4: Configuring AD LDS

Installing and Configuring AD LDS
Configuring AD LDS Instances
Configuring AD LDS Replication
Configuring AD LDS Integration with AD DS
Lab 4: Configuring AD LDS
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

Module 5: Configuring AD FS

Overview of AD FS
AD FS Deployment Scenarios
Deploying AD FS
Implementing AD FS Claims
Lab 5A: Configuring AD FS for Federated Web SSO by Using Forest Trust Scenario
Installing the AD FS Server Role
Configuring Certificate Requirements
Configuring the AD FS Web Agent
Configuring the Web Server application on a 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
Lab 5B: Configuring Active Directory Federation Services by Using Federated Web SSO Scenario
Installing the AD FS Server Role
Configuring Certificate Requirements
Configuring the AD FS Web Agent
Configuring the Web Server application on a virtual computer
Configuring the Federation Trust Policies
Configuring the Account Partner Federation Service
Configuring the Resource Partner Federation Service
Testing the AD FS implementation

Module 6: Configuring AD RMS

Overview of AD RMS
Installing and Configuring AD RMS Server Components
Administering AD RMS
Implementing AD RMS Trust Policies
Lab 6: Configuring AD RMS
Installing the AD RMS Server Role
Managing AD RMS rights policy templates
Configuring Trust Policies
Testing AD RMS functionality

Module 7: Maintaining Access Management Solutions

Supporting AD CS
Maintaining AD LDS
Maintaining AD FS
Maintaining AD RMS
Lab 7: 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

Module 8: Troubleshooting IDA Solutions

Troubleshooting AD CS
Troubleshooting AD LDS
Resolving AD FS Issues
Solving AD RMS Issues
Lab 8: Troubleshooting IDA Solutions
Identifying Tools and Troubleshooting Techniques of IDA Solutions