

Course Description: This 3-day instructor-led course provides students with an understanding of Active Directory technology in Windows Server 2008. This course is intended to allow individuals who already have experience with Active Directory to upgrade their skills for Windows Server 2008. This course is based on an interim build of Windows Server 2008.

Who Should Attend: This course is intended for IT Professionals experienced on the technologies included in Windows Server 2000 and Windows Server 2003, and who hold an MCSE or MCSA certification and/or equivalent knowledge.

Prerequisites: Before attending this course, students must have one or more of the following: 1) On-the-job experience in planning, implementing, managing, or supporting Microsoft Windows Server 2000 or 2003, including Active Directory and Network Infrastructure; 2) Working knowledge of networking, for example, TCP/IP and Domain Name System (DNS); 3) Designed a Microsoft Windows Server 2003 Active Directory and Network Infrastructure; 4) Designed Security for a Microsoft Windows Server 2003 Network; or 5) Installed, Configured, and Administered Microsoft Windows 2000, Windows XP Professional, or Microsoft Vista.

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

- Describe and configure server roles with Active Directory Services in Windows Server 2008.
- Plan for and deploy Active Directory Domain Services.
- Install, configure, and manage the Server Core role as a domain controller.
- Manage accounts, subnets, Site-Links, Group Policy, and DNS configuration with Active Directory Domain Services.
- Manage new Active Directory services, including Active Directory Federation Services, Active Directory Lightweight Directory Services, and Active Directory Rights Management Services.
- Set up and manage Read-Only Domain Controllers (RODC).
- Use auditing features in Active Directory Domain Services.
- Manage credentials with Active Directory Certificate Services, including Credential Roaming.

Course Outline:

Introduction to Active Directory Technology in Windows Server 2008

Active Directory Improvements
Lab 1: Introduction to Active Directory Technology in Windows Server 2008
Use Three Phases to Configure a Server
Deploy New Server Roles and Features
Change a Server's Role
Change Role Services and Features

Planning for Windows Server 2008 Active Directory Services

Planning for ADDS Deployment
Upgrade Considerations
Lab 1: Installing a Windows Server 2008 Forest
Install a New Forest
Lab 2: Installing Windows Server 2008 in an Existing Forest
Install a Windows Server 2008 DC in an Existing Forest
Install a RODC in an Existing Forest
Verify Active Directory Installation
Install a New Forest

Server Core Domain Controllers

Server Core Domain Controllers
Lab 1: Server Core Domain Controller
Installing Server Core
Configure Server Core
Adding Roles and Features
Managing Server Core

Active Directory Domain Services

What's New in AD DS
Improved Security
Manageability and Reliability
Lab 1: Exploring Active Directory Domain Services
Create Accounts
Review Operations Masters Role
Review Sites
Working with Subnets
Working with Site-Links
AD DS and Group Policy
Review DNS Configuration

Active Directory Federation Services, Active Directory Lightweight Directory Services, Active Directory Rights Management Services

Active Directory Federation Services for identity access

solution
Active Directory Lightweight Directory Services (replaces Active Directory Account Management with Windows Server 2003), providing directory services for applications.
Active Directory Right Management Services, enabling the creation of information-protection solutions.
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Lab 1: Active Directory Federation Services
Install AD FS
Configure Web Server
Configure Federation Server
Access Application from Client Computer
Lab 2: Active Directory Rights Management Services
Install and Configure AD RMS
Add New AD RMS Cluster
Register the Service Connection Point in Active Directory
Verify AD RMS Functionality

Read-Only Domain Controllers

Read-Only Domain Controllers
Read-Only Domain Controller Operation
Lab 1: Read-Only Domain Controllers
Deploying an RODC
Administering an RODC

Auditing Active Directory Domain Services Changes

What's new in AD DS auditing
Who should use this new feature
Benefits of auditing changes in AD DS
Summary of new AD DS auditing events
Summary of attribute syntaxes
Lab 1: Auditing Active Directory Domain Services Changes
Prerequisites
Steps to set up auditing
Example audit events

Enterprise PKI (PKIView) Active Directory Certificate Services (ADCS)

Certificate Authority
Certificate Policy Settings
Microsoft Simple Certificate Enrollment Protocol
Online Revocation Services
Network Device Enrollment Services

Web Enrollment Services
Lab 1: Enterprise PKI (PKIView) Active Directory Certificate Services (ADCS)
Add a Certificate Server Role
Exploring the PKIView UI
Introducing Expiry Notifications
Introducing Credential Roaming
Introducing CA performance monitors
Exploring delegated enrollment
Introducing OSCP configuration
Revocation