



Course 6425B:

# Configuring and Troubleshooting Windows Server 2008 Active Directory Domain Services

Length: 5 Days  
Language(s): English  
Audience(s): IT Professionals  
Level: 200  
Technology: Windows Server 2008  
Type: Course  
Delivery Method: Instructor-led (classroom)

A course towards becoming:  
**Microsoft**  
**CERTIFIED** | Server Administrator  
*IT Professional*

## About this Course

This five-day instructor-led course provides to teach Active Directory Technology Specialists with the knowledge and skills to configure Active Directory Domain Services in a distributed environment, implement Group Policies, perform backup and restore, and monitor and troubleshoot Active Directory related issues.

## Audience Profile

The primary audience for this course are AD Technology Specialists, Server Administrators, and Enterprise Administrators who want to learn how to implement AD in a distributed environment, secure domains using Group Policies, and perform backup, restore, and monitor and troubleshoot AD configuration to ensure trouble free operation.

## At Course Completion

After completing this course, students will be able to implement and configure Active Directory domain services in their enterprise environment.



## Pre-requisites

Before attending this course, students must have:

- Basic understanding of networking.
- Intermediate understanding of network operating systems.
- An awareness of security best practices.
- Basic knowledge of server hardware.
- Some experience creating objects in Active Directory.
- Foundation course (6424) or equivalent knowledge.
- Basic concepts of backup and recovery in a Windows Server Environment.

## Course Outline

### Module 1: Introducing Active Directory Domain Services (AD DS)

This module explains how to install and configure Active Directory Domain Services and install and configure a read-only domain controller.

#### Lessons

- Introducing Active Directory, Identity, and access
- Active Directory Components and Concepts
- Install Active Directory Domain Services
- Extend IDA with Active Directory Services

#### Lab: Install an AD DS DC to Create a Single Domain Forest

- Exercise 1: Perform Post-Installation Configuration Tasks
- Exercise 2: Install a New Windows Server 2008 Forest with the Windows Interface



After completing this module, students will be able to:

- Position the strategic role a directory service in an enterprise in relation to identity and access.
- Explain authentication and authorization processes.
- Identify the major components of ADDS.
- Understand the requirements for installing a domain controller to create a new forest
- Identify the roles of and relationships between ADDS, ADLDS, ADRMS, ADFS, and ADCS

## Module 2: Secure and Efficient Administration of Active Directory

This module explains how to work securely and efficiently in Active Directory.

### Lessons

- Work with Active Directory Snap-ins
- Custom Consoles and Least Privilege
- Find Objects in Active Directory
- Use DS Commands to Administer Active Directory

### Lab: Create and Run a Custom Administrative Console

- Exercise 1: Perform Basic Administrative Tasks Using the Active Directory Users and Computers Snap-in
- Exercise 2: Create a Custom Active Directory Administrative Console
- Exercise 3: Perform Administrative Tasks with Least Privilege, Run as Administrator and User Account Control
- Exercise 4: (Advanced Optional) Advanced MMC Customization and Remote Administration

### Lab: Find Objects in Active Directory

- Exercise 1: Finding Objects in Active Directory
- Exercise 2: Using Saved Queries
- Exercise 3: (Advanced Optional) Explore Saved Queries

### Lab: Use DS Commands to Administer Active Directory

- Exercise 1: Use DS Commands to Administer Active Directory



After completing this module, students will be able to:

- Install, locate, and describe the snap-ins used to administer AD DS
- Perform basic administrative tasks with the Active Directory Users and Computers snap-in
- Create a custom MMC console for administration
- Perform administrative tasks while logged on as a user
- Control the view of objects in the Active Directory Users and Computers snap-in
- Locate objects in Active Directory
- Work with saved queries
- Identify the distinguished name (DN), relative distinguished name (RDN), and common name (CN) of an Active Directory object
- Use the DS commands to administer Active Directory from the command line

## Module 3: Manage Users

This module explains how to manage and support user accounts in Active Directory.

### Lessons

- Create and Administer User Accounts
- Configure User Object Attributes
- Automate User Account Creation

### Lab: Create and Administer User Accounts

- Exercise 1: Create User Accounts
- Exercise 2: Administer User Accounts
- Exercise 3: (Advanced Optional) Explore User Account Name Attributes

### Lab: Configure User Object Attributes

- Exercise 1: Examine User Object Attributes
- Exercise 2: Manage User Object Attributes
- Exercise 3: Create Users from a Template
- Exercise 4: (Advanced Optional) Create Users with a Batch File



### Lab: Automate User Account Creation

- Exercise 1: Export and Import Users with CSVDE
- Exercise 2: Import Users with LDIFDE

After completing this module, students will be able to:

- Create and configure the account-related properties of a user object
- Identify the purpose and requirements of user account attributes
- Perform common administrative tasks to support user accounts including password reset and account unlock
- Enable and disable user accounts
- Delete, move and rename user accounts
- View and modify hidden attributes of user objects
- Identify the purpose and requirements of user object attributes
- Create users from user account templates
- Modify attributes of multiple users simultaneously
- Export user attributes with CSVDE
- Import users with CSVDE
- Import users with LDIFDE

## Module 4: Manage Groups

This module explains how to create, modify, delete, and support group objects in Active Directory.

### Lessons

- Manage an Enterprise with Groups
- Administer Groups
- Best Practices for Group Management

### Lab: Administer Groups

- Exercise 1: Implement Role-Based Management Using Groups
- Exercise 2: Manage Group Membership from the Command Line



- Exercise 3: (Advanced Optional) Explore Group Membership Reporting Tools
- Exercise 4: (Advanced Optional) Understand “Account Unknown” Permissions

#### **Lab: Best Practices for Group Management**

- Exercise 1: Implement Best Practices for Group Management

After completing this module, students will be able to:

- Understand the role of groups in managing an enterprise
- Create well-documented, secure, delegated groups
- Understand group types, scope, and nesting
- Understand the best practice for group nesting to achieve role-based management
- Create, delete and manage groups with DSCommands, CSVDE and LDIFDE
- Enumerate and copy group membership
- Understand Default (Built In) groups
- Understand Special Identities

## **Module 5: Support Computer Accounts**

This module explains how to create and configure computer accounts.

#### **Lessons**

- Create Computers and Join the Domain
- Administer Computer Objects and Accounts

#### **Lab: Create Computers and Join the Domain**

- Exercise 1: Join a Computer to the Domain with the Windows Interface
- Exercise 2: Securing Computer Joins
- Exercise 3: Managing Computer Account Creation with Best Practices

#### **Lab: Administer Computer Objects and Accounts**

- Exercise 1: Administer Computer Objects through their Lifecycle
- Exercise 2: Administer and Troubleshoot Computer Accounts



After completing this module, students will be able to:

- Understand the relationship between a domain member and the domain in terms of identity and access
- Identify the requirements for joining a computer to the domain
- Implement best practice processes for computer joins
- Secure AD DS to prevent the creation of unmanaged computer accounts
- Manage computer objects and their attributes using the Windows Interface and command line tools
- Administer computer accounts through their lifecycle

## Module 6: Implement a Group Policy Infrastructure

This module explains what Group Policy is, how it works, and how best to implement Group Policy in your organization.

### Lessons

- Understand Group Policy
- Implement a Group Policy
- Explore Group Policy Settings and Features
- Manage Group Policy Scope
- Group Policy Processing
- Troubleshoot Policy Application

### Lab: Implement Group Policy

- Create, Edit and Link GPOs

### Lab: Explore Group Policy Settings and Features

- Exercise 1: Use Filtering and Commenting
- Exercise 2: Manage Administrative Templates

### Lab: Manage Group Policy Scope

- Exercise 1: Configure GPO Scope with Links
- Exercise 2: Configure GPO Scope with Filtering



- Exercise 3: Configure Loopback Processing

#### **Lab: Troubleshoot Policy Application**

- Exercise 1: Perform RSoP Analysis
- Exercise 2: using the Group Policy Results Wizard
- Exercise 3: View Policy Events

After completing this module, students will be able to:

- Identify the business drivers for configuration management
- Understand the components and technologies that comprise the Group Policy framework
- Manage Group Policy objects
- Configure and understand a variety of policy setting types
- Scope GPOs using links, security group, WMI filters, loopback processing, and Preference targeting
- Explain GPO storage, replication, and versioning
- Administer a Group Policy infrastructure
- Evaluate GPO inheritance, precedence, and Resultant Set of Policy (RSoP)
- Locate the event logs containing Group Policy related events

## **Module 7: Manage Enterprise Security and Configuration with Group Policy Settings**

This module explains how to manage security and software installation and how to audit files and folders.

#### **Lessons**

- Delegate the Support of Computers
- Manage Security Settings
- Manage software with GPSI
- Auditing

#### **Lab: Delegate the Support of Computers**

- Exercise 1: Configure the Membership of Administrators Using Restricted Groups Policies



### Lab: Manage Security Settings

- Exercise 1: Manage Local Security Settings
- Exercise 2: Create a Security Template
- Exercise 3: Use Security Configuration and Analysis
- Exercise 4: Use the Security Configuration Wizard

### Lab: Manage Software with GPSI

- Exercise 1: Deploy Software with GPSI
- Exercise 2: Upgrade Applications with GPSI

### Lab: Audit File System Access

- Exercise 1: Configure Permissions and Audit Settings
- Exercise 2: Configure Audit Policy
- Exercise 3: Examine Audit Events

After completing this module, students will be able to:

- Delegate the administration of computers
- Use Restricted Groups policies to modify or enforce the membership of groups
- Use Group Policy Preferences to modify the membership of groups
- Configure security settings using the Local Security policy
- Create and apply security templates to manage security configuration
- Analyze security configuration based on security templates
- Create, edit, and apply security policies using the Security Configuration Wizard
- Deploy security configuration with Group Policy
- Deploy software using GPSI
- Remove software originally installed with GPSI

## Module 8: Secure Administration

This module explains how to administer Active Directory Domain Services Securely.



## Lessons

- Delegate Administrative Permissions
- Audit Active Directory Changes

### Lab: Delegate Administration

- Exercise 1: Delegate Permission to create and support User Accounts
- Exercise 2: View Delegated Permissions
- Exercise 3: Remove and Reset Permissions

### Lab: Audit Active Directory Changes

- Exercise 1: Audit Changes to Active Directory using Default Audit Policy
- Exercise 2: Audit Changes to Active Directory using Directory Service Changes auditing

After completing this module, students will be able to:

- Describe the business purpose of delegation.
- Assign permissions to Active Directory objects using the security editor user interfaces and the Delegation of Control Wizard.
- View and report permissions on Active Directory objects by using user interface and command line tools.
- Reset the permissions on an object to its default.
- Describe the relationship between delegation and OU design.
- Configure Directory Service Changes auditing
- Specify auditing settings on Active Directory objects
- Identify event log entries created by Directory Access auditing and Directory Service Changes auditing

## Module 9: Improve the Security of Authentication in an Active Directory Domain Services (AD DS) Domain

This module explains the domain-side components of authentication, including the policies that specify password requirements and the auditing of authentication-related activities.

## Lessons



- Configure Password and Lockout Policies
- Audit Authentication
- Configure Read-Only Domain Controllers

#### **Lab: Configure Password and Account Lockout Policies**

- Exercise 1: Configure the Domain's Password and Lockout Policies.
- Exercise 2: Configure Fine-Grained Password Policy

#### **Lab: Audit Authentication**

- Exercise 1: Audit Authentication

#### **Lab: Configure Read-Only Domain Controllers**

- Exercise 1: Install RODC
- Exercise 2: Configure Password Replication Policy
- Exercise 3: Manage Credential Caching

After completing this module, students will be able to:

- Implement your domain password and account lockout policy
- Configure and assign fine-grained password policies
- Configure auditing of authentication-related activity
- Distinguish between account logon and logon events
- Identify authentication-related events in the Security log
- Identify the business requirements for RODCs
- Install an RODC
- Configure password replication policy
- Monitor the caching of credentials on an RODC

## **Module 10: Configure Domain Name System (DNS)**

This module explains how to implement DNS to support name resolution both within your AD DS domain and outside your domain and your intranet.



## Lessons

- Review DNS Concepts, Components, and Processes
- Install and Configure DNS Server in an AD DS Domain
- AD DS, DNS, and Windows
- Advanced DNS Configuration and Administration

## Lab: Installing the DNS Service

- Exercise 1: Add the DNS Server Role
- Exercise 2: Configure Forward Lookup Zones and Resource Records

## Lab: Advanced Configuration of DNS

- Exercise 1: Enable Scavenging of DNS Zones
- Exercise 2: Create Reverse Lookup Zones
- Exercise 3: Explore Domain Controller Location
- Exercise 4: Configure Name Resolution for External Domains

After completing this module, students will be able to:

- Understand the structure role, structure and functionality of the domain name system (DNS)
- Describe client and server name resolution processes
- Install DNS
- Manage DNS records
- Configure DNS server settings
- Understand the integration between AD DS and DNS
- Choose a DNS domain for an Active Directory domain
- Create a zone delegation for a new Active Directory domain
- Configure replication for Active Directory integrated zones
- Describe the purpose of SRV records in the domain controller location process
- Understand read-only DNS servers
- Understand and configure single-label name resolution
- Configure advanced DNS server settings
- Audit, maintain, and troubleshoot the DNS server role



## Module 11: Administer Active Directory Domain Services (AD DS) Domain Controllers

This module explains how to add Windows Server 2008 domain controllers to a forest or domain, how to prepare a Microsoft Windows Server 2003 forest or domain for its first Windows Server 2008 DC, how to manage the roles performed by DCs, and how to migrate the replication of SYSVOL from the File Replication Service (FRS) used in previous versions of Windows to the Distributed File System Replication (DFS-R) mechanism that provides more robust and manageable replication.

### Lessons

- Domain Controller Installation Options
- Install a Server Core DC
- Manage Operations Masters
- Configure DFS Replication of SYSVOL

### Lab: Install Domain Controllers

- Exercise 1: Create an Additional DC with the Active Directory Domain Services Installation Wizard.
- Exercise 2: Add ad Domain Controller from the Command Line
- Exercise 3: Remove a Domain Controller
- Exercise 4: Create a Domain Controller from Installation Media

### Lab: Install a Server Core DC

- Exercise 1: Perform Post-Installation Configuration on Server Core
- Exercise 2: Create a Domain Controller with Server Core

### Lab: Transfer Operations Master Roles

- Exercise 1: Identify Operations Masters.
- Exercise 2: Transfer Operations Master Roles

### Lab: Configure DFS-R Replication of SYSVOL

- Exercise 1: Observe the Replication of SYSVOL
- Exercise 2: Prepare to Migrate to DFS-R
- Exercise 3: Migrate SYSVOL Replication to DFS-R



- Exercise 4: Verify DFS-R Replication of SYSVOL

After completing this module, students will be able to:

- Install a standard or read-only domain controller into new or existing domains or trees
- Add and remove domain controllers using a variety of GUI or command-line methods
- Configure a domain controller on Server Core
- Understand and identify operations master roles
- Manage the placement, transfer, and seizure of operations master roles
- Migrate SYSVOL replication from FRS to DFS-R

## Module 12: Manage Sites and Active Directory Replication

This module explains how to create a distributed directory service that supports domain controllers in portions of your network that are separated by expensive, slow, or unreliable links.

### Lessons

- Configure Sites and Subnets
- Configure the Global Catalog and Application Partitions
- Configure Replication

### Lab: Configure Sites and Subnets

- Exercise 1: Configure the Default Site
- Exercise 2: Create Additional Sites

### Lab: Configure the Global Catalog and Application Partitions

- Exercise 1: Configure a Global Catalog
- Exercise 2: Configure Universal Group Membership
- Exercise 3: Examine DNS and Application Directory Partitions

### Lab: Configure Replication

- Exercise 1: Create a Connection Object
- Exercise 2: Create Site Links
- Exercise 3: Move Domain Controllers into Sites



- Exercise 4: Designate a Preferred Bridgehead Server
- Exercise 5: Configure Intersite Replication

After completing this module, students will be able to:

- Configure sites and subnets
- Understand domain controller location and manage domain controllers in sites
- Configure replication of the partial attribute set to global catalog servers
- Implement universal group membership caching
- Understand the role of application directory partitions
- Configure replication topology with connection objects, bridgehead servers, site links, and site link bridges
- Report, analyze, and troubleshoot replication with repadmin.exe and dcdiag.exe

## Module 13: Directory Service Continuity

This module explains about the technologies and tools that are available to help ensure the health and longevity of the directory service. You will explore tools that help you monitor performance in real time, and you will learn to log performance over time so that you can keep an eye on performance trends in order to spot potential problems.

### Lessons

- Monitor Active Directory
- Manage the Active Directory Database
- Back Up and Restore AD DS and Domain Controllers

### Lab: Monitor Active Directory

- Exercise 1: Monitor Real-Time Performance Using Task Manager and Resource Monitor
- Exercise 2: Use Reliability Monitor and Event Viewer to Identify Performance-Related Events
- Exercise 3: Monitor Events on Remote Computers with Event Subscriptions
- Exercise 4: Attach Tasks to Event Logs and Events
- Exercise 5: Monitor AD DS with Performance Monitor



- Exercise 6: Work with Data Collector Sets

#### **Lab: Manage the Active Directory Database**

- Exercise 1: Perform Database Maintenance
- Exercise 2: Work with Snapshots and Recovering a Deleted User

#### **Lab: Backup and Restore Active Directory**

- Exercise 1: Back up Active Directory
- Exercise 2: Restore Active Directory and a Deleted OU

After completing this module, students will be able to:

- Monitor real-time performance and events with Task Manager, Event Viewer, and Windows Reliability and Performance Monitor
- Leverage new features of Event Viewer in Windows Server 2008, including custom views and event subscriptions
- Monitor real-time and logged performance with Performance Monitor, data collection sets, and reports
- Identify sources of performance and event information for AD DS domain controllers
- Create alerts based on events and performance metrics
- Maintain and optimize the Active Directory database
- Back up and restore AD DS and domain controllers
- Recover deleted objects and attributes

## **Module 14: Manage Multiple Domains and Forests**

This module explains how to raise the domain and forest functionality levels within your environment, how to design the optimal AD DS infrastructure for your enterprise, how to migrate objects between domains and forests, and how to enable authentication and resources access across multiple domains and forests.

#### **Lessons**

- Configure Domain and Forest Functional Levels



- Manage Multiple Domains and Trust Relationships

#### **Lab: Raise Domain and Forest Functional Levels**

- Exercise 1: Raise the Domain Functional Level to Windows Server 2003.
- Exercise 2: Raise the Forest Functional Level to Windows Server 2003
- Exercise 3: Raise the Domain Functional Level to Windows Server 2008

#### **Lab: Administer a Trust Relationships**

- Exercise 1: Configure DNS
- Exercise 2: Create a Trust Relationship
- Exercise 3: Validate a Trust Relationship
- Exercise 4: Assign Permission to Trusted Identities
- Exercise 5: Implement Selective Authentication

After completing this module, students will be able to:

- Understand domain and forest functional levels
- Raise domain and forest functional levels
- Identify capabilities added by each functional level
- Design an effective domain and tree structure for AD DS
- Identify the role of the Active Directory Migration Tool, and the issues related to object migration and domain restructure
- Understand trust relationships
- Configure, administer, and secure trust relationships