

6425 – Configuring Windows Server 2008 Active Directory Domain Services

Vendor Course Code: 6425

Course Length: 5 days

Overview: This five-day instructor-led course provides in-depth training on configuring Active Directory Domain Services (AD DS) in a distributed environment, implementing Group Policies, performing backup and restore, and monitoring and troubleshooting Active Directory related issues.

Skills Gained: After completing this course, students will be able to:

- Describe the features and functionality of Active Directory Domain Services.
- Perform secure and efficient administration of Active Directory.
- Manage users and service accounts.
- Manage groups.
- Manage computer accounts.
- Implement a Group Policy infrastructure.
- Manage enterprise security and configuration by using Group Policy settings.
- Secure administration.
- Improve the security of authentication in an AD DS Domain.
- Configure Domain Name System.
- Administer AD DS domain controllers.
- Manage sites and Active Directory.
- Monitor, maintain, and back up directory Service to ensure continuity.
- Manage multiple domains and forests.

Key Topics:

Module 1: Introducing Active Directory Domain Services

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

Lessons

Lesson 1: Overview of Active Directory, Identity, and Access

Lesson 2: Active Directory Components and Concepts

Lesson 3: Install Active Directory Domain Services

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

Perform Post-Installation Configuration Tasks

Install a New Windows Server 2008 Forest with the Windows Interface

Raise Domain and Forest Functional Levels

After completing this module, students will be able to:

- Describe the functionality of AD DS in an enterprise in relation to identity and access.
- Describe the major components of AD DS.
- Install AD DS and configure it as a domain controller.

Module 2: Administering Active Directory Securely and Efficiently

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

Lessons

Work with Active Directory Administration Tools

Custom Consoles and Least Privilege

Find Objects in Active Directory

Use Windows PowerShell to Administer Active Directory

Lab : Administer Active Directory Using Administrative Tools

Perform Administrative Tasks by Using Administrative Tools

Create a Custom Active Directory Administrative Console

Perform Administrative Tasks with Least Privilege, Run As Administrator, and User Account Control

Lab : Find Objects in Active Directory
Find Objects in Active Directory
Use Saved Queries

Lab : Use Windows PowerShell to Administer Active Directory
Use PowerShell Cmdlets to Administer Active Directory

After completing this module, students will be able to:

- Describe and work with Active Directory administration tools.
- Describe the purpose and functionality of custom consoles and least privilege.
- Locate objects in Active Directory.
- Administer Active Directory by using Windows PowerShell.

Module 3: Managing Users and Service Accounts

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
Create and Configure Managed Service Accounts

Lab : Create and Administer User Accounts
Create User Accounts
Administer User Accounts

Lab : Configure User Object Attributes
Examine User Object Attributes
Manage User Object Attributes
Create Users from a Template

Lab : Automate User Account Creation
Export and Import Users with CSVDE
Import Users with LDIFDE

Lab : Create and Administer Managed Service Accounts
Create and Associate a Managed Service Account

After completing this module, students will be able to:

- Create and administer user accounts.
- Configure user object attributes.
- Automate user account creation.
- Create and configure managed service accounts.

Module 4: Managing Groups

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

Lessons

Overview of Groups
Administer Groups
Best Practices for Group Management

Lab : Administer Groups
Implement Role-Based Management by Using Groups
(Advanced Optional) Explore Group Membership Reporting Tools
(Advanced Optional) Understand "Account Unknown" Permissions

Lab : Best Practices for Group Management
Implement Best Practices for Group Management

After completing this module, students will be able to:

- Describe the role of groups in managing an enterprise.
- Administer groups with by using the built-in tools in Windows Server 2008 CSVDE and LDIFDE.
- Describe the best practices for managing groups.

Module 5: Managing Computer Accounts

This module explains how to create and configure computer accounts.

Lessons

Create Computers and Join the Domain
Administer Computer Objects and Accounts
Perform an Offline Domain Join

Lab : Create Computers and Join the Domain
Join a computer to the Domain with the Windows Interface
Secure Computer Joins
Manage Computer Account Creation

Lab : Administer Computer Objects and Accounts
Administer Computer Objects Through Their Life Cycle
Administer and Troubleshoot Computer Accounts

Lab : Configure an Offline Domain Join
Configure an Offline Domain Join

After completing this module, students will be able to:

- Create computer accounts and join them to a domain.
- Administer computer objects and accounts by using the Windows Interface and command-line tools.
- Describe and perform the Offline Domain Join process.

Module 6: Implementing a Group Policy Infrastructure

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

Lessons

Understand Group Policy
Implement GPOs
Deeper Look at Settings and GPOs
Group Policy Preferences
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
Use Filtering and Commenting
Manage Administrative Templates

Lab : Managing Group Policy Preferences
Configure Group Policy Preferences
Verify the Application of Group Policy Preferences

Lab : Manage Group Policy Scope
Configure GPO Scope with Links
Configure GPO Scope with Filtering
Configure Loopback Processing

Lab : Troubleshoot Policy Application
Perform RSoP Analysis
Use the Group Policy Modelling Wizard
View Policy Events

After completing this module, students will be able to:

- Describe the components and technologies that comprise the Group Policy framework.
- Implement GPOs.
- Configure and understand a variety of policy setting types.
- Understand and configure Group Policy preferences.

- Scope GPOs by using links, security groups, Windows Management Instrumentation filters, loopback processing, and preference targeting.
- Describe how GPOs are processed.
- Locate the event logs containing Group Policy–related events and troubleshoot Group Policy application.

Module 7: Managing 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
Software Restriction Policy and AppLocker

Lab : Delegate the Support of Computers
Configure the Membership of Administrators by Using Restricted Groups

Lab : Manage Security Settings
Manage Local Security Settings
Create a Security Template

Lab : Manage Software with GPSI
Deploy Software with GPSI
Upgrade Applications with GPSI

Lab : Audit File System Access
Configure Permissions and Audit Settings
Configure Audit Policy
Examine Audit Events

Lab : Configure Application Control Policies
Configure Application Control Policies

After completing this module, students will be able to:

- Delegate the support of computers.
- Manage security settings.
- Manage software by using GPSI.
- Describe the purpose and functionality of auditing
- Describe the purpose of Software Restriction Policy and AppLocker.

Module 8: Securing Administration

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

Lessons

Delegate Administrative Permissions
Audit Active Directory Administration

Lab : Delegate Administration
Delegate Permission to Create and Support User Accounts
View Delegated Permissions
Remove and Reset Permissions

Lab : Audit Active Directory Changes
Audit Changes to Active Directory Using Default Audit Policy
Audit Changes to Active Directory Using Directory Service Changes Auditing

After completing this module, students will be able to:

- Delegate administrative permissions.
- Audit Active Directory administration.

Module 9: Improving the Security of Authentication in an 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
Configure the Domain's Password and Lockout Policies
Configure a Fine-Grained Password Policy

Lab : Audit Authentication
Audit Authentication

Lab : Configure Read-Only Domain Controllers
Exercise 1: Install an RODC
Exercise 2: Configure Password Replication Policy
Exercise 3: Manage Credential Caching

After completing this module, students will be able to:

- Configure password and lockout policies.
- Audit authentication.
- Configure read-only domain controllers.

Module 10: Configuring Domain Name System

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 of DNS Concepts, Components, and Processes
Install and Configure DNS in an AD DS Domain
Integration of AD DS, DNS, and Windows
Advanced DNS Configuration and Administration

Lab : Installing the DNS Service
Add the DNS Server Role
Configure Forward Lookup Zones and Resource Records

Lab : Advanced Configuration of DNS
Enable Scavenging of DNS Zones
Create Reverse Lookup Zones
Explore Domain Controller Location
Configure Name Resolution for External Domains

After completing this module, students will be able to:

- Describe DNS concepts, components, and processes.
- Install and configure DNS in an AD DS domain.
- Describe the integration of AD DS, DNS, and Windows.
- Describe advanced DNS configuration and administration tasks.

Module 11: Administering 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-R Replication of SYSVOL

Lab : Install Domain Controllers
Create an Additional DC with the Active Directory Domain Services Installation Wizard
Add a Domain Controller from the Command Line

Remove a Domain Controller
Create a Domain Controller from Installation Media

Lab : Install a Server Core DC
Perform Post-Installation Configuration on Server Core
Create a Domain Controller with Server Core

Lab : Transfer Operations Masters Roles
Identify Operations Masters
Transfer Operations Masters Roles

Lab : Configure DFS-R Replication of SYSVOL
Observe the Replication of SYSVOL
Prepare to Migrate to DFS-R
Migrate SYSVOL Replication to DFS-R
Verify DFS-R Replication of SYSVOL

After completing this module, students will be able to:

- Identify the domain controller installation options.
- Install a Server Core DC.
- Manage operations masters.
- Configure DFS-R replication of SYSVOL.

Module 12: Managing Sites and Active Directory

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
Configure the Default Site
Create Additional Sites

Lab : Configure the Global Catalog and Application Partitions
Configure a Global Catalog
Configure Universal Group Membership
Examine DNS and Application Directory Partitions

Lab : Configure Replication
Create a Connection Object
Create Site Links
Move Domain Controllers into Sites
Designate a Preferred Bridgehead Server
Configure Intersite Replication

After completing this module, students will be able to:

- Configure sites and subnets.
- Configure the global catalog and application partitions.
- Configure replication.

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
Active Directory Recycle Bin
Back Up and Restore AD DS and Domain Controllers

Lab : Monitor Active Directory

Monitor Real-Time Performance Using Task Manager and Resource Monitor
Use Reliability Monitor and Event Viewer to Identify Performance-Related Events
Monitor Events on Remote Computers with Event Subscriptions
Attach Tasks to Event Logs and Events
Monitor AD DS with Performance Monitor
Work with Data Collector Sets

Lab : Manage the Active Directory Database
Perform Database Maintenance
Work with Snapshots and Recovering a Deleted User

Lab : Using Active Directory Recycle Bin
Enable Active Directory Recycle Bin
Restore Deleted Objects with Active Directory Recycle Bin

Lab : Back Up and Restore Active Directory
Back Up Active Directory
Restore Active Directory and a Deleted OU

After completing this module, students will be able to:

- Monitor Active Directory.
- Manage the Active Directory database.
- Describe the purpose of the Active Directory Recycle Bin.
- Back up and restore AD DS and domain controllers.

Module 14: Managing 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
Move Objects between Domains and Forests

Lab : Administer a Trust Relationship
Configure Functional Levels and DNS
Create a Trust Relationship
Validate a Trust Relationship
Assign Permissions to Trusted Identities
Implement Selective Authentication

After completing this module, students will be able to:

- Configure domain and forest functional levels.
- Manage multiple domains and trust relationships.
- Move objects between domains and forests.

Target Audience:

This course is intended for Active Directory Technology Specialists, Server Administrators, and Enterprise Administrators who want to learn how to implement Active Directory in a distributed environment, secure domains by using Group Policies, back up, restore, monitor, and troubleshoot Active Directory configuration to ensure trouble-free operation.

Prerequisites:

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
- Basic concepts of backup and recovery in a Windows Server environment