

Windows Server[®] 2008 Active Directory Domain Services: Hands-On - 4 Days

Course 962 Overview

- You Will Learn How To**
- Install, manage and secure Active Directory Domain Services (AD DS)
 - Restructure existing domains and migrate to Windows Server 2008 Active Directory
 - Troubleshoot domain creation and manage Flexible Single Master Operation (FSMO) failures
 - Configure Active Directory replication topology with sites
 - Leverage Read-Only Domain Controllers (RODC) to implement database security
 - Lessen the server attack surface with Windows Server Core

Course Benefits Windows Server 2008 Active Directory Domain Services includes features that allow organisations to simplify and secure deployment, and to administer AD DS more efficiently. In this comprehensive hands-on course, you gain the essential skills required to effectively manage and secure a high-availability AD enterprise and ensure a successful migration to Windows Server 2008 Active Directory.

Who Should Attend IT professionals who want to enhance their skills to support a Windows Server 2008 Active Directory. A working knowledge of Windows Server 2003 AD or Course 960, "Windows Server 2008 Comprehensive Introduction", is assumed.

Hands-On Training Practical hands-on exercises provide experience installing, troubleshooting and securing the Active Directory. Exercises include:

- Revealing the AD infrastructure with DNS
- Upgrading a Windows Server 2003 Active Directory
- Troubleshooting domain controller creation
- Removing superfluous domain and DC objects
- Correcting Active Directory service failures
- Configuring a reliable replication topology
- Creating and managing an RODC
- Installing domain services on Server Core
- Recovering deleted objects from the AD Recycle Bin

Windows Server® 2008 Active Directory Domain Services: Hands-On - 4 Days

Course 962 Outline

Windows Server 2008 AD Fundamentals

- Exploring the AD infrastructure
- The role of DNS in an AD environment

Deploying a Windows Server 2008 AD Upgrading existing AD environments

- Planning and preparing for the upgrade
- Analysing supported paths
- Modifying the Active Directory with ADPREP

Managing domain controllers with Server Manager

- Adding and removing server roles
- Enhancing server functionality with features
- Analysing security logs with Event Viewer
- Monitoring current server status

Creating the Active Directory Forest Building domain controllers and domains

- Troubleshooting domain creation
- Working with new DCPROMO features

Cleaning up metadata from the AD

- Properly retiring domains and domain controllers
- Removing unwanted objects with NTDSUTIL

Managing Flexible Single Master Operation (FSMO) roles

- Documenting the role holders
- Transferring roles between domain controllers
- Recovering from FSMO failures

Planning and configuring Active Directory sites

- Creating sites to delineate the replication topology
- Defining site properties to control replication traffic
- Assigning clients to sites dynamically

Enumerating domain logon service requirements

- Assessing the impact of Global Catalog availability
- Analysing the role of DNS
- Building a Kerberos time convergence hierarchy

Managing Active Directory Replication

Windows Server is a registered trademark of Microsoft Corporation.

The fundamentals of multimaster replication

- Identifying the Update Sequence Numbers (USN)
- Monitoring replication data with administrative tools
- Resolving data collision issues

Creating and customising replication topology

- Analysing the role of the Knowledge Consistency Checker (KCC)
- Monitoring intra- and inter-site replication
- Troubleshooting replication failures
- Controlling replication with site-links and site-link bridges
- Configuring site-link transitivity

Distributed File System Replication (DFSR)

- Minimising the impact on network traffic with Remote Differential Compression (RDC)
- Migrating SYSVOL replication to DFSR

Recovering from Active Directory disasters

- Viewing and reanimating deleted objects
- Backing up and restoring the database
- Comparing authoritative and non-authoritative restores

Securing the Active Directory

Enforcing object security

- Configuring security settings
- Utilising inheritance to control object access

Leveraging AD auditing

- Monitoring object access
- Minimising the impact of auditing on domain controller performance

Troubleshooting Active Directory services

- Diagnosing AD service failures
- Identifying AD service malfunctions with operating system tools
- Recovering from AD service failures
- Developing a consistent troubleshooting technique

Installing a Read-Only Domain Controller (RODC)

- Setting a password replication policy
- Adding DNS and the Global Catalog to an RODC
- Delegating RODC management

Windows Server Core benefits

- Adding supported roles
- Building a domain controller on Server Core

Windows Server 2008 Functionality Modes

Domain functionality levels

- Setting the domain functionality
- Analysing features at various domain functionality modes

Forest functionality levels

- Forest functionality requirements
- Setting the functionality of the forest