



Lesson Plans

Configuring Windows Server 2008 Active Directory

(Exam 70-640)

Version 2.1

Table of Contents

Course Overview	3
Section 0.1: Active Directory Organization.....	5
Section 0.2: Active Directory Features.....	6
Section 0.3: New 2008 Features	7
Section 1.1: Organizational Units.....	8
Section 1.2: User Accounts.....	9
Section 1.3: Computer Accounts	11
Section 1.4: Groups.....	12
Section 1.5: Group Strategy.....	13
Section 1.6: Object Management Tools.....	14
Section 2.1: DNS Concepts.....	15
Section 2.2: Installation	16
Section 2.3: Zones.....	17
Section 2.4: Resource Records	18
Section 2.5: Zone Transfers	19
Section 2.6: Advanced Zone Configuration.....	20
Section 2.7: Root Hints.....	21
Section 2.8: Round Robin.....	22
Section 2.9: Directory Partitions.....	23
Section 2.10: DNS Features.....	24
Section 3.1: Preparation	25
Section 3.2: Installation	26
Section 3.3: Removal.....	27
Section 4.1: Functional Levels.....	28
Section 4.2: Sites and Subnets	29
Section 4.3: Global Catalog Servers	31
Section 4.4: Operations Master Roles.....	32
Section 4.5: Trusts	34
Section 5.1: RODC Concepts	35
Section 5.2: RODC Installation	36
Section 5.3: RODC Administration	37
Section 5.4: RODC Removal.....	38
Section 6.1: Group Policy	39
Section 6.2: Group Policy Management	40
Section 6.3: GPO Application.....	42
Section 6.4: Software Deployment	43
Section 6.5: Password Policies	44
Section 6.6: Auditing	45
Section 7.1: Certificate Services.....	46
Section 7.2: AD CS Installation.....	47
Section 7.3: Certificate Templates.....	48
Section 7.4: Certificate Requests	50
Section 7.5: Certificate Revocation	51
Section 7.6: CA Management.....	52

Section 7.7: Certificate Implementations.....	53
Section 8.1: Lightweight Directory Services (AD LDS).....	54
Section 8.2: Federation Services (AD FS).....	55
Section 8.3: Rights Management Services (AD RMS).....	56
Section 9.1: Recovery and Availability	57
Section 9.2: Windows Server Backup	58
Section 9.3: Active Directory Backup and Restore	60
Section 9.4: Maintenance and Monitoring.....	61
Practice Exams.....	62

Course Overview

This course prepares students for the Microsoft Exam 70-640:TS: Windows Server 2008 Active Directory, Configuring. It focuses on the management tasks of an administrator to configure and manage the Active Directory for an organization.

Module 0 – Active Directory Overview

This module provides an overview of how Active directory is organized, features of Active Directory and how new features and functionality are provided by adding roles, role services and features.

Module 1 – Objects and Accounts

This module discusses creating and managing the following objects and accounts; organizational units, user accounts, computer accounts, and groups. It also discusses implementing group strategies and the tools for managing objects.

Module 2 – DNS

In this module students will learn how to configure Domain Name System (DNS) server settings, zones, zone transfers, replications, root zone, and root hints.

Module 3 – Installation

This module covers preparation, installation, and configuration of a domain controller.

Module 4 – Infrastructure

In Module 4 students will learn the basics of configuring the Active Directory infrastructure. Students will learn how to configure functional levels of a domain or forest, create and configure sites and subnets, configure a global catalog, and configure Operation Master roles and trusts.

Module 5 – Read-only Domain Controller

Module 5 teaches the students how to install and configure a Read-only Domain controller (RODC). Students will learn the functions and features of the RODC, how to administer the RODC account, and how to remove a RODC, if needed.

Module 6 – Group Policy

Module 6 discusses creating and implementing Group Policy Objects (GPOs) in Windows Server 2008. Students will learn how to configure GPOs for software deployment, apply password policies, and to enforce auditing and secure audit logs.

Module 7 – Certificate Services

In Module 7 students will learn details of certificate services. They will learn how to install Active Directory certificate services, manage certificate templates, request a certificate, manage certificate revocation, configure administrative permissions to manage CAs, and configure CA server settings for certificate implementation.

Module 8 – Active Directory Roles

This module discusses installing and configuring the following Active Directory roles; Lightweight Directory Services (AD LDS), Federation Services (AD FS), and Rights Management Service (AD RMS).

Module 9 – Maintenance

This module covers tools and methods for maintenance of the system. These include the tools for backup and restore, and disaster recovery of the Windows Server 2008. Tools and methods to monitor, backup and restore Active Directory are also presented.

Practice Exams

In Practice Exams students will have the opportunity to test themselves and verify that they understand the concepts and are ready to take the certification test.

Section 0.1: Active Directory Organization

Summary

In this section the students will learn how the Active Directory database is organized. They will become familiar with the hierarchical framework of the Active Directory structure:

- Domain
- Object
- Organizational Unit (OU)
- Generic Containers
- Trees and Forests
- Domain Controller
- Sites and Subnets

Students will learn how to:

- Use management tools to view the Active Directory structure and objects.

Lecture Focus Questions:

- Why is DNS important for Active Directory?
- What is the purpose of the *schema*?
- What are the advantages of using organizational units over generic containers?
- What is the difference between a *tree* and a *forest*? How can you tell when a new domain starts a new tree?
- How does a site differ from a domain?

Time

About 20 minutes

Section 0.2: Active Directory Features

Summary

This section discusses the following Active Directory features:

- Global Catalog
- Operations Master Roles
 - Forest Roles
 - Schema master
 - Domain naming master
 - Domain Roles
 - RID master
 - PDC emulator
 - Infrastructure master
- Functional Level
- Group Policy

Lecture Focus Questions:

- What is the purpose of a global catalog server?
- Which operation master roles are forest-wide roles?
- Why is the domain or forest functional level important? How does the functional level relate to the operating system versions you run on domain controllers in the domain?
- How does Group Policy simplify network administration?

Time

About 10 minutes

Section 0.3: New 2008 Features

Summary

This section explores the modularity of Windows Server 2008 and how new features and functionality are provided by adding roles, role services and features. Active Directory server roles include:

- Active Directory Domain Services (AD DS)
- Active Directory Lightweight Directory Service (AD LDS)
- Active Directory Federation Services (AD FS)
- Active Directory Rights Management Service (AD RMS)
- Active Directory Certificate Services (AD CS)

Server Core is a minimal server installation options with several limitations.

Students will learn how to:

- Use Server Manager to add and manage roles and features.

Lecture Focus Questions:

- What is the difference between a role, a role service, and a feature?
- Which Active Directory role helps you control access to digital documents?
Which role do you use to create a custom directory service?
- What are the advantages of using a Server Core installation over a regular installation?
- How does management of a Server Core system differ from managing a regular version of Windows?
- Which server roles cannot run on a Server Core system?

Time

About 20 minutes

Section 1.1: Organizational Units

Summary

This section discusses designing a workable and manageable strategy for using Organization Units (OUs). Students will learn how to plan for, create, and manage OUs including the default containers and OUs that are automatically created.

Students will learn how to:

- Create organizational units using Active Directory Users and Computers or Server Manager.
- Use the Delegation of Control wizard to allow administrators to manage objects and object properties.

Windows Server 2008 Active Directory Objectives

- 402. Maintain Active Directory accounts.

Lecture Focus Questions:

- What objects can an organizational unit contain?
- How is an organizational unit different than a generic container?
- How does inheritance affect child organizational units?
- How does object-based delegation differ from task-based delegation?

Time

About 25 minutes

Lab/Activity

- Create OUs

Section 1.2: User Accounts

Summary

In this section students will learn to create and manage user accounts. Two types of user accounts are available when creating user accounts; local and domain. Active Directory uses four types of name types to identify one object from another.

- User or logon name
- User Principle Name (UPN)
- LDAP Distinguished Name (DN)
- Relative Distinguished Name (RDN)

The administrator can manage user accounts by enabling, disabling, or restricting properties within the user account properties.

Students will learn how to:

- Create domain user accounts.
- Modify user account properties, including changing logon and password settings in the user account.
- Rename a user account.
- Reset a user account password and unlock the account.
- Enable and disable an account.

Windows Server 2008 Active Directory Objectives

- 401. Automate creation of Active Directory accounts.
- 402. Maintain Active Directory accounts.

Lecture Focus Questions:

- How is a domain user account different from a local user account?
- What is the purpose of a contact object? How is it similar and different from a user account?
- What is the difference between a disabled, locked out, or expired user account?
- What is the best way to handle a user's account when an employee quits the company and will be replaced by a new employee in the near future?
- What are the recommendations for using a template user account?
- What properties of a user account do not get duplicated when you copy the user?

Time

About 45 minutes

Lab/Activity

- Create User Accounts
- Manage User Accounts

Section 1.3: Computer Accounts

Summary

This section examines two methods of joining a computer to an Active Directory Domain. The administrator can manually join the computer to the domain or pre-create the account and give the user the rights to join the domain.

Students will learn how to:

- Create computer accounts and manage computer account properties.

Windows Server 2008 Active Directory Objectives

- 402. Maintain Active Directory accounts.

Lecture Focus Questions:

- What can the administrator do to allow a user to join a computer to a domain during installation?
- How can you control where a computer account is placed when it joins a domain?
- What are the things to consider if a computer account has been created on a domain but doesn't seem to be able to join the domain?
- What must you do after resetting a computer account?

Time

About 15 minutes

Lab/Activity

- Create Computer Accounts

Section 1.4: Groups

Summary

In this section students will learn how to simplify network management by assembling accounts into manageable units, called groups, to assign rights to users and computers. *Local groups* control access to local resources and *domain groups* control access to both domain and local resources. Two types of groups exist; a *security group* manages rights and permissions and a *distribution group* maintains a group of users such as an email list. Security group scopes and their membership and use are discussed: Global, domain local, and universal. Students will also become familiar with default groups for both local and domain groups.

Students will learn how to:

- Create security and distribution groups.
- Add members to groups.
- Change the group type or scope.

Windows Server 2008 Active Directory Objectives

- 401. Automate creation of Active Directory accounts.
- 402. Maintain Active Directory accounts.

Lecture Focus Questions:

- What are the advantages of using groups when setting permissions?
- What is the difference between a *security group* and a *distribution group*?
- What type of objects can be made members of a universal group? A domain local group?
- What happens to user accounts when a group is deleted?

Time

About 45 minutes

Lab/Activity

- Create Global Groups
- Create a Distribution Group
- Change the Group Scope

Section 1.5: Group Strategy

Summary

This section discusses three basic recommended strategies for designing groups to manage users, groups, and permissions. These consist of:

- AGDLP
- AGUDLP
- ALP

This section focuses on the AGDLP strategy.

Students will learn how to:

- Implement a group strategy following Microsoft's recommendations for group membership and nesting.

Windows Server 2008 Active Directory Objectives

- 402. Maintain Active Directory accounts.

Lecture Focus Questions:

- Based on Microsoft's recommendations, which group scope is added to the ACL for an object and assigned the permissions?
- Based on Microsoft's recommendations, which group scope type would you use to add user accounts as members?
- When is it appropriate to use universal groups? In which scenarios are they unnecessary?

Time

About 20 minutes

Lab/Activity

- Implement a Group Strategy 1
- Implement a Group Strategy 2

Section 1.6: Object Management Tools

Summary

In this section students will learn about tools for managing objects. To manage a small number of objects the following tools are available:

- Active Directory Users and Computers
- ADSI Edit
- Command Prompt Tools

To manage a large number of objects the following tools are available:

- Csvde
- Ldifde
- PowerShell
- Visual Basic scripts (VBscripts)
- Ldp
- Active Directory Migration Tool (ADMT)

Windows Server 2008 Active Directory Objectives

- 401. Automate creation of Active Directory accounts.

Lecture Focus Questions:

- What tools are available when managing Active Directory objects on a Server Core installation?
- When would you use ADSI Edit to manage objects instead of Active Directory Users and Computers?
- When would you choose **Csvde** over **Ldifde** when managing objects?
- What are cmdlets and how can they manage Active Directory objects?

Time

About 15 minutes

Section 2.1: DNS Concepts

Summary

This section examines how the Domain Name System (DNS) makes it possible for users to reference computers using friendly logical hostnames. A DNS server translates the hostnames into IP addresses which are recognized by the network. Students will learn the components of the DNS hierarchy and what is included in a fully qualified domain name (FQDN).

Windows Server 2008 Active Directory Objectives

- 101. Configure zones.

Lecture Focus Questions:

- What is the purpose of DNS?
- How does an FQDN identify a host?
- What is the difference between a *forward* lookup zone and a *reverse* lookup zone?
- What is the purpose of PTR records?
- How does DDNS simplify DNS management?
- What is the difference between *forwarding* and *recursion*?

Time

About 15 minutes

Section 2.2: Installation

Summary

In this section students will learn the basics of installing DNS on Windows Server 2008.

Students will learn how to:

- Add the DNS server role to a server.

Lecture Focus Questions:

- Which Windows Server 2008 versions do not support the DNS server role?
- How should the DNS server get its IP address?
- How do you install DNS on a Server Core system?

Time

About 5 minutes

Section 2.3: Zones

Summary

This section discusses different types of DNS zones:

- Primary
- Secondary
- Active Directory-integrated
- Stub
- GlobalNames

A forward lookup zone provides hostname-to-IP address resolution. *A reverse lookup zone* provides IP address-to-hostname resolution.

Students will learn how to:

- Create primary, secondary, and reverse lookup zones.
- Create an Active Directory-integrated zone and configure the replication scope.

Windows Server 2008 Active Directory Objectives

- 101. Configure zones.
- 103. Configure zone transfers and replication.

Lecture Focus Questions:

- How is an Active Directory-integrated zone different from a primary zone?
- What type of zone would you create if you wanted to use secure dynamic updates?
- What is the impact on network traffic of the **All domain controllers in this domain** versus the **All DNS servers in this forest** replication scope?
- What type of name resolution is performed by reverse lookup zones?
- What is the zone name format for the reverse lookup network of 1375:2614:DDAB:EE21?

Time

About 45 minutes

Lab/Activity

- Create a Primary Zone
- Create a Secondary Zone
- Create an Active Directory-integrated Zone
- Create a Reverse Lookup Zone

Section 2.4: Resource Records

Summary

This section examines how DNS resource records are used to locate resources on the Internet or in internal Active Directory environments. Common resource records include:

- SOA (Start of Authority)
- NS (name server)
- A (host address)
- AAAA (quad-A)
- CNAME (canonical name)
- DNAME (Domain Alias)
- PTR (pointer)
- WINS and WINS-R resource records

Dynamic DNS (DDNS) is required to support Active Directory. DDNS automatically creates and deletes resource records as resource information is modified.

Students will learn how to:

- Create common resource records.

Windows Server 2008 Active Directory Objectives

- 101. Configure zones.
- 103. Configure zone transfers and replication.

Lecture Focus Questions:

- What information does an SOA record contain?
- What is the difference between an A and a quad-A record?
- How is the DNAME record similar to a CNAME record?
- How does Windows Server 2008 handle the creation of SRV records?
- How does the use of DDNS facilitate record management?
- What is the difference in the default state of dynamic updates between primary and Active Directory-integrated zones?

Time

About 25 minutes

Lab/Activity

- Create a Zone and Add Records
- Create A and CNAME Records

Section 2.5: Zone Transfers

Summary

In this section students will learn the basics of configuring DNS zone transfers to provide replication of zone data between primary and secondary zones. There are two types of zone transfers in Windows Server:

- AXFR – Full zone transfer
- IXFR – Incremental zone transfer.

Students will learn to:

- Add authoritative name servers.
- Restrict zone transfers to name servers or specific servers only.
- Modify zone properties and enable or disable zone transfers.

Windows Server 2008 Active Directory Objectives

- 103. Configure zone transfers and replication.

Lecture Focus Questions:

- How is secondary zone data changed?
- What is the significance of the serial number during zone transfers?
- What is the difference between AXFR and IXFR zone transfers?
- What are the methods for restricting zone transfers?
- What happens if the serial number is greater on the secondary server?
- How can you use multiple DNS servers to improve DNS performance?
- What is the difference between a **reload** and a **reload from master** operation?

Time

About 30 minutes

Lab/Activity

- Allow Zone Transfers to Name Servers
- Allow Zone Transfers to Listed Servers
- Disable Zone Transfers

Section 2.6: Advanced Zone Configuration

Summary

This section examines advanced zone configuration concepts such as resolving queries for a record using a forwarder, controlling the server's use of forwarders, delegating a zone, and using GlobalNames for single-label name resolution.

Students will learn how to:

- Create a stub zone.
- Configure forwarders and conditional forwarding.
- Create delegated zones.

Windows Server 2008 Active Directory Objectives

- 101. Configure zones.
- 102. Configure DNS server settings.

Lecture Focus Questions:

- How does a stub zone differ from a secondary zone?
- How does conditional forwarding differ from standard forwarding?
- How is a stub zone dynamic? What records are copied to the zone when you create a stub zone?
- Why isn't a stub zone authoritative for the zone?
- Why might you decide to implement zone delegation?
- What records does the delegation contain?
- When can you use the GlobalNames zone to replace WINS servers on your network? When should you continue to use a WINS server?

Time

About 40 minutes

Lab/Activity

- Configure a Stub Zone
- Configure Conditional Forwarding
- Delegate Zones
- Create a Delegated Zone

Section 2.7: Root Hints

Summary

In this section students will learn the basics of how root hints are the pointers to top level DNS servers on the Internet. The Cache.dns file holds the 13 root hint addresses for the Internet root servers. Student will become familiar with the following:

- First Level Domain Names
- Country Domain Names
- Sub Divided Domain Names

Students will learn how to:

- Configure or delete a root zone.
- Configure other DNS servers to point to your server via root hints.

Windows Server 2008 Active Directory Objectives

- 102. Configure DNS server settings.

Lecture Focus Questions:

- Why would you want to create a zone named . (dot)?
- What is the purpose of the root hints file?
- Why would you delete the root hints?
- What is the name and location(s) of the root hints file on a Windows 2008 server?

Time

About 10 minutes

Lab/Activity

- Configure Root Hints

Section 2.8: Round Robin

Summary

This section discusses using Round Robin to distribute DNS records to multiple servers to load balance the distribution and sharing of network resource loads.

Students will learn how to:

- Configure DNS round robin.

Windows Server 2008 Active Directory Objectives

- 102. Configure DNS server settings.

Lecture Focus Questions:

- Why do round robin servers use different IP addresses?
- What type of resource record do you create in the DNS database when using round robin?
- Why does round robin provide load balancing but not fault tolerance?

Time

About 10 minutes

Lab/Activity

- Configure DNS Round Robin

Section 2.9: Directory Partitions

Summary

This section provides information about DNS application directory partitions, which can be used to:

- Reduce network traffic
- Reduce calls to Global Catalog servers
- Extend Web applications
- Control replication of Active Directory attributes to specific domain controllers

Windows Server 2008 Active Directory Objectives

- 103. Configure zone transfers and replication.

Lecture Focus Questions:

- How do application directory partitions control the scope of replication?
- Which group memberships allow users to create application directory partitions manually?
- What tool would you use to create an application directory partition?

Time

About 5 minutes

Section 2.10: DNS Features

Summary

In this section students will learn about DNS features in Windows Server 2008

- Background Zone Loading
- Read Only Domain Controller Support (RODC)
- IPv6 Support
- DC Locator
- Link Local Multicast Name Resolution
- GlobalNames Zone
- Global Query Block List
- Conditional Forwarding
- DNSSEC Support
- Aging
- Scavenging
- Debug Logging.

Windows Server 2008 Active Directory Objectives

- 101. Configure zones.

Lecture Focus Questions:

- How does background loading have a positive effect on name resolution?
- How do stale records affect DNS server performance?
- When is a DNS record considered stale?
- How does the **no-refresh interval** affect scavenging?
- When should you activate debug logging? For what period of time?

Time

About 15 minutes

Section 3.1: Preparation

Summary

This section covers the preparations that must be completed before installing the first domain controller running Windows Server 2008 to an existing Windows 2000 or Windows Server 2003 Active Directory environment.

- Set the forest and domain to the correct functional level.
- Update the Active Directory schema to support Windows Server 2008 domain controllers.

Students will learn how to:

- Prepare an existing forest and domain for installation of a Windows Server 2008 domain controller.

Windows Server 2008 Active Directory Objectives

- 201. Configure a forest or a domain.
- 303. Configure the read-only domain controller (RODC).

Lecture Focus Questions:

- Which forest and domain functional levels are required before installing a Windows Server 2008 domain controller?
- When do you use the **adprep /domainprep /gpprep** command instead of the **adprep /domainprep** command?
- On which domain controller should you run the **adprep /domainprep** command?
- What command would you run to prepare for installing a read-only domain controller (RODC)?

Time

About 15 minutes

Section 3.2: Installation

Summary

This section discusses the requirements and methods for installing Active Directory Domain Services. Students will learn the details of creating an answer file to use during installation and methods to verify installation.

Students will learn how to:

- Install a new domain controller using GUI and command-line tools.

Windows Server 2008 Active Directory Objectives

- 201. Configure a forest or a domain.

Lecture Focus Questions:

- What is the difference between a *forest* and a *tree*?
- How does an installation from media reduce network traffic?
- What tools can you use to create the installation media for installing a domain controller?
- How can you easily create an answer file for use with **Dcpromo**?
- When using an answer file for domain controller installation, what is the difference between a new domain and a replica?
- How can you verify that Active Directory is installed?

Time

About 35 minutes

Section 3.3: Removal

Summary

In this section students will learn how to remove a domain controller and the three different tools you can use to accomplish the task.

Students will learn how to:

- Uninstall a domain controller and remove Active Directory binaries.
- Force removal of Active Directory from a domain controller.

Windows Server 2008 Active Directory Objectives

- 201. Configure a forest or a domain.

Lecture Focus Questions:

- What does the **IsLastDCInDomain** parameter in an answer file do?
- When should you forcefully remove a domain controller? What should you try before doing so?
- What are the results of removing the last domain controller from a domain?
- How do you remove the Active Directory binaries from a system?

Time

About 10 minutes

Section 4.1: Functional Levels

Summary

This section discusses functional levels that determine the functions that can be performed by an Active Directory domain or forest. Students will compare the features that are available at each domain and forest functional level. They will also be presented with the guidelines for configuring the domain and forest functional levels.

Students will learn how to:

- Identify the current domain and forest functional levels.
- Raise the functional levels of domains and forests.

Windows Server 2008 Active Directory Objectives

- 201. Configure a forest or a domain.

Lecture Focus Questions:

- Which functional level is required to enable selective authentication?
- What forest functional level(s) let you rename domains?
- What features do you get by enabling a Windows Server 2008 functional level?
- When would you raise the domain functional level?
- What are the domain controller operating system requirements for raising a domain functional level to Windows Server 2008?

Time

About 25 minutes

Lab/Activity

- Raise Functional Levels
- Raise the Domain and/or Forest Levels

Section 4.2: Sites and Subnets

Summary

This section examines the function sites and subnets play to optimize and customize replication traffic during the process of Active Directory replication. Students will learn about the following objects that are used to control replication traffic:

- Subnet
- Site
- Site link
- Site link bridge
- Bridgehead server
- Connection

Students will be able to distinguish between intrasite and intersite replication and the steps to configure each type of replication. They will also learn how and when to use Distributed File System (DFS) replication to replicate the contents of the SYSVOL folder.

Students will learn how to:

- Create sites and subnets. Move servers into sites.
- Create site links and configure site link properties to customize replication.
- Customize intersite and intrasite replication frequencies and schedules.
- Designate preferred bridgehead servers.

Windows Server 2008 Active Directory Objectives

- 203. Configure sites.
- 204. Configure Active Directory replication.

Lecture Focus Questions:

- What is the purpose of a site link?
- What is the purpose of a site link bridge?
- Why would you typically *not* create a connection object?
- What are the differences between intrasite and intersite replication?
- What does a site link cost do?
- When would you use the SMTP protocol for replication?
- What is the function of the bridgehead server?
- How is a preferred bridgehead server determined?

Time

About 60 minutes

Lab/Activity

- Manage Sites and Subnets
- Configure Intersite Replication
- Configure Intrasite Replication

Section 4.3: Global Catalog Servers

Summary

This section explores the use of Global Catalog servers in multiple-domain and multiple-site network configurations to improve performance of user logon and forest-wide searches. Global Catalog uses the Lightweight Directory Access Protocol (LDAP) for directory communications. Guidelines for when to place a global catalog server or Universal Group Membership Caching in a site are discussed.

Students will learn how to:

- Add or remove the global catalog from a domain controller.
- Enable Universal Group Membership Caching for a site.

Windows Server 2008 Active Directory Objectives

- 205. Configure the global catalog.

Lecture Focus Questions:

- What are the advantages of having more than one Global Catalog server?
- Why does a single domain network not need a Global Catalog server?
- What is the function of Universal Group Membership caching?
- When should Universal Group Membership caching be implemented? When would you use global catalog servers instead?

Time

About 25 minutes

Lab/Activity

- Configure Global Catalog Servers
- Enable Universal Group Membership Caching

Section 4.4: Operations Master Roles

Summary

This section examines the function and configuration of Operations Master roles which are assigned to a domain controller in the domain or forest. The following Operation Master roles operate at either the forest or domain levels:

- Forest Level Roles
 - Schema Master
 - Domain Naming Master

- Domain Level Roles
 - Relative Identifier (RID) Master
 - Primary Domain Controller (PDC) Emulator
 - Infrastructure Master

Students will learn how to:

- Transfer operation master roles among domain controllers.
- Troubleshoot operation master roles to diagnose network problems.
- Seize an operation master role in the case of a failed role operations master.

Windows Server 2008 Active Directory Objectives

- 201. Configure a forest or a domain.

Lecture Focus Questions:

- What is the purpose of an operation master role server?
- What is the function of a PDC emulator? What does the infrastructure master do?
- Which operations master roles are located at the forest level? How many of these roles are there in a forest?
- How many domain operations masters are in a forest?
- You are installing a new domain controller in a new domain in an existing forest. How many operation master roles will that server hold?
- What might happen if the RID master becomes unavailable?
- Which role(s) should be placed on a global catalog server? Which roles should not?
- What is the difference between *transferring* a role and *seizing* a role?

Time

About 45 minutes

Lab/Activity

- Transfer RID and PDC Masters
- Transfer the Infrastructure Master
- Troubleshoot Operations Masters

Section 4.5: Trusts

Summary

This section provides an overview of how trusts can be used to establish relationships between different domains to allow access to resources between the domains.

Trust Types include:

- Parent/child
- Tree Root
- External
- Realm
- Forest
- Shortcut

Students will learn how to:

- Create external, shortcut, and forest root trusts.

Windows Server 2008 Active Directory Objectives

- 202. Configure trusts.

Lecture Focus Questions:

- What is the difference between a one-way trust and a two-way trust?
- Domain A trusts domain B. Users in which domain will be able to access resources in which domain? What is the relationship between the direction of trust and the direction of access?
- What is a *transitive* trust? Which trust types are transitive by default?
- When are trusts created automatically? What are the properties of those trusts?
- When should you use a shortcut trust?
- What are the domain and forest functional level requirements for creating a forest root trust? What type of trust would you use if you couldn't create a forest root trust?

Time

About 45 minutes

Lab/Activity

- Create a Shortcut Trust
- Create External Trusts
- Create a Forest Root Trust
- Design Trusts

Section 5.1: RODC Concepts

Summary

This section provides a summary of the functions and features of a read-only domain controller (RODC). Features of RODC discussed include:

- Administrator role separation
- Unidirectional replication
- Read-only data
- Password replication
- DNS Server service

Windows Server 2008 Active Directory Objectives

- 303. Configure the read-only domain controller (RODC).

Lecture Focus Questions:

- What is the purpose of administrator role separation?
- How does unidirectional replication protect your network?
- How does using an RODC allow for domain logon in the event of a WAN link failure?
- How do DNS zones work differently on an RODC?

Time

About 10 minutes

Section 5.2: RODC Installation

Summary

In this section students will learn the basics of an RODC installation. They will learn the prerequisites, considerations when deploying an RODC, and the steps to perform the installation.

Students will learn how to:

- Pre-create RODC accounts in Active Directory.
- Install an RODC.

Windows Server 2008 Active Directory Objectives

- 303. Configure the read-only domain controller (RODC).

Lecture Focus Questions:

- What are the domain and forest functional level requirements for installing an RODC?
- What operating system versions must run on the PDC emulator?
- What permissions do you need to install an RODC?
- What are two ways to replicate the installation source files to the RODC?
- How does BitLocker increase the security of an RODC?

Time

About 20 minutes

Lab/Activity

- Create RODC Accounts

Section 5.3: RODC Administration

Summary

This section discusses administration of the RODC account using the administrative role separation, password caching and replication features.

Students will learn how to:

- Configure password caching and replication for an RODC.

Windows Server 2008 Active Directory Objectives

- 303. Configure the read-only domain controller (RODC).

Lecture Focus Questions:

- How does password replication make user logons more efficient? What advantages are there to allowing password caching?
- When would you want to prevent password caching?
- Why does the Denied RODC Password Replication group contain default members?
- What are two ways you can allow a user password to be cached on an RODC?

Time

About 15 minutes

Lab/Activity

- Edit the Password Replication Policy

Section 5.4: RODC Removal

Summary

This section examines RODC removal steps to use in the event that the security of the RODC has been compromised.

Students will learn how to:

- Delete an RODC from your site.
- Generate a list of passwords cached on an RODC.

Windows Server 2008 Active Directory Objectives

- 303. Configure the read-only domain controller (RODC).

Lecture Focus Questions:

- What is the effect of resetting computer account passwords cached on the RODC?
- Why would you want a list of the accounts cached on the RODC?
- Why is it necessary to reset the user account passwords on a stolen RODC?

Time

About 5 minutes

Section 6.1: Group Policy

Summary

This section provides an overview of new Group Policy features in Windows Server 2008:

- ADMX and ADML files
- Network Location Awareness
- Group Policy preferences

Windows Server 2008 Active Directory Objectives

- 403. Create and apply Group Policy objects (GPOs).

Lecture Focus Questions:

- What is the difference between policies set in computer configuration and policies set in user configuration?
- How does network location awareness enhance Group Policy?
- How does inheritance affect Group Policy settings?
- To which Active Directory objects can GPOs be linked?

Time

About 10 minutes

Section 6.2: Group Policy Management

Summary

This section discusses elements of Group Policy management. Students will learn how the Group Policy settings are organized into categories and also how to configure registry-based settings within a Group Policy object using Administrative templates. To create another GPO with the same settings you can choose from the following methods:

- Copy
- Backup and Import
- Starter GPOs

Students will learn how to:

- Create and link GPOs.
- Edit GPOs settings.
- Enable or disable computer or user portions in a GPO.
- Enable the central Administrative Templates store and create a starter GPO.

Windows Server 2008 Active Directory Objectives

- 403. Create and apply Group Policy objects (GPOs).

Lecture Focus Questions:

- What is the difference between a user right and a security option?
- What are the advantages of the .admx file format?
- What is the Administrative Template central store? What advantages do you gain by enabling the central store?
- What is the difference between using a starter GPO and copying an existing GPO?
- What is the difference between deleting a GPO and deleting a GPO link?
- What is an undefined GPO setting? How does this affect the effective settings for a user or computer?
- When are computer configuration settings applied? When are user configuration settings applied?
- How can you copy a GPO from one domain to another? How can you copy starter GPOs?
- What is the difference between *restore* and *import* when working with GPO backups?

Time

About 70 minutes

Lab/Activity

- Configure User Rights
- Configure Security Options
- Configure Restricted Groups
- Modify GPO Links
- Create a Starter GPO

Section 6.3: GPO Application

Summary

This section provides details of the following elements used for applying and customizing GPOs:

- Group Policy Inheritance
- Block Inheritance
- GPO Permissions
- WMI Filtering
- Loopback Processing

Students will learn how to:

- Link GPOs to appropriate objects to take advantage of inheritance.
- Customize Group Policy application using block inheritance and no override.
- Use GPO permissions to limit the application of GPOs.
- Configure WMI filters and loopback processing.

Windows Server 2008 Active Directory Objectives

- 403. Create and apply Group Policy objects (GPOs).

Lecture Focus Questions:

- If a setting is configured in a GPO linked to the domain and a GPO linked to an OU, which setting will be in effect?
- If there is more than one group policy linked to a domain, what controls the order of application?
- How is the **Block Inheritance** setting affected by the **No Override** setting?
- How can you apply Group Policy settings to specific users or groups?
- How can you apply Group Policy settings to specific computers?
- How does *loopback processing* affect computer settings?

Time

About 35 minutes

Lab/Activity

- Control GPO Inheritance
- Configure GPO Permissions

Section 6.4: Software Deployment

Summary

This section explores steps in the software deployment lifecycle:

- Plan
- Deploy
- Manage (Upgrade)
- Remove

Students will learn how to:

- Assign and publish software installer packages.
- Configure software installation packages to customize deployment and removal.

Windows Server 2008 Active Directory Objectives

- 405. Configure software deployment GPOs.

Lecture Focus Questions:

- What is the difference between *assigned* and *published* software?
- Why should you use the UNC path to an installer package rather than the local path?
- What is file invocation?
- What does it mean when a user or computer is outside of the scope of management for a software installation package? What happens to the software when this condition exists?

Time

About 45 minutes

Lab/Activity

- Assign Software
- Deploy Software 1
- Deploy Software 2

Section 6.5: Password Policies

Summary

This section discusses Password Policy used to control characteristics enforced for user passwords and Account Lockout Policy settings used to control what happens when a user enters one (or more) incorrect passwords. Additionally, this section discusses how granular password policies allow you to create password policies for users and global groups separate from the password policy applied to the entire domain.

Students will learn how to:

- Configure and manage Account Policy settings.
- Use ADSI Edit to configure granular password policy settings.

Windows Server 2008 Active Directory Objectives

- 406. Configure account policies

Lecture Focus Questions:

- Users in a network have to change their passwords every 30 days, but many users have reported that they simply enter the same password to make the change. Which policy can you configure to prevent this?
- What is the effect of setting the minimum password age account policy to 5 days?
- How can you prevent users from creating passwords like *desk*, *mom*, *chair*, or *office*?
- What is the effect of setting the account lockout policy to 0?
- What happens when you configure Account Policies settings in a GPO linked to an OU?
- How can you configure different account policy settings for different users?
- Which object types can you associate with a granular password policy?
- A user has a granular password policy applied directly to the user account, and a different policy applied to a group of which the user is a member. Which policy will be in effect?

Time

About 40 minutes

Lab/Activity

- Configure Account Policies
- Modify Account Lockout

Section 6.6: Auditing

Summary

This section provides information about using auditing to record system events and system changes. The following audit policies are configurable through Group Policy:

- Account logon
- Account management
- Directory service access
- Logon
- Object access
- Policy change
- Privilege use
- Process tracking
- System

Students will learn how to:

- Use Group Policy to enforce auditing and secure audit logs.

Windows Server 2008 Active Directory Objectives

- 407. Configure audit policy by using GPOs.

Lecture Focus Questions:

- What is the difference between auditing for success and auditing for failure?
- What is the difference between Account Logon and Logon auditing?
- What additional step must you complete in order to audit NTFS file access?
- How can you configure auditing to track changes to Active Directory objects?
- What are the results of excessive auditing?
- Why should you design periodic reviews of the logs?

Time

About 45 minutes

Lab/Activity

- Configure Auditing

Section 7.1: Certificate Services

Summary

This section explores using Certificate services to provide proof of identity and encryption. Students will learn about the following elements of certificate and encryption services:

- Cipher/algorithm
- Key
- Symmetric encryption
- Asymmetric encryption (PKI)
- Public Key Infrastructure (PKI)
- Certificate Authority (CA)
- Certificate revocation list (CRL)
- Active Directory Certificate Services (AD CS)

Windows Server 2008 Active Directory Objectives

- 601. Install Active Directory Certificate Services.

Lecture Focus Questions:

- What is the difference between symmetric and asymmetric encryption?
- How do certificates prove identity?
- What kinds of information do certificates hold?
- What is the relationship of a CA to a PKI?
- How can you ensure that users outside your organization trust your certificate?
- What are the advantages of using an enterprise CA over a standalone CA?

Time

About 25 minutes

Section 7.2: AD CS Installation

Summary

In this section students will learn the steps to install Active Directory Certificate Services (AD CS).

Students will learn how to:

- Install and configure the Active Directory Certificate Services role.

Windows Server 2008 Active Directory Objectives

- 601. Install Active Directory Certificate Services.

Lecture Focus Questions:

- What is the advantage of taking the root CA offline?
- Why shouldn't you take an enterprise CA offline? How can you use an offline root CA but still use enterprise CAs?
- How do you request a CA certificate if the root CA is offline?
- What permissions do you need to install a standalone CA?
- When would you use a self-signed certificate for a CA? When should the CA get its certificate from another source?

Time

About 10 minutes

Section 7.3: Certificate Templates

Summary

This section discusses using certificate templates to reduce the administrative complexity of requesting and issuing certificates. Certificate template permissions which control requests for a certificate by users and computers include:

- Full Control
- Read
- Write
- Enroll
- Autoenroll

Version 2 and 3 templates also offer the following settings to customize the template.

- Validity Period
- Publish in Active Directory
- Key Type
- Cryptographic Service Provider (CSP)
- Subject Name
- Issuance Requirement
- Extensions

Students will learn how to:

- Duplicate and edit certificate templates.
- Issue (publish) certificate templates on a CA.

Windows Server 2008 Active Directory Objectives

- 603. Manage certificate templates.

Lecture Focus Questions:

- Why shouldn't you modify a default template?
- What does issuing a template accomplish?
- What is the effect of removing a template from the list of issued templates?
- What are the minimum permissions necessary for a user to request a certificate?
- What is the role of the Certificate Publishers group?
- What do you need to do in order to edit the subject name information in a version 1 template?
- What setting do you modify to require an administrator to approve certificate requests?

Time

About 35 minutes

Lab/Activity

- Modify Issued Certificate Templates
- Modify a Certificate Template

Section 7.4: Certificate Requests

Summary

In this section students will learn methods for requesting a certificate:

- Web Enrollment Pages
- Certificate Request Wizard through the Certificates snap-in
- Autoenrollment
- Command line using the Certreq.exe command

This section focuses on managing and configuring autoenrollment which allows certificates to be requested, issued, or renewed without user intervention.

Students will learn how to:

- Prepare an offline certificate request. After receiving the certificate, import it.
- Use the Web enrollment pages to request and install a certificate.
- On the CA, approve a pending certificate request.
- Configure a certificate template, the CA, and Group Policy for autoenrollment.

Windows Server 2008 Active Directory Objectives

- 602. Configure CA server settings.
- 603. Manage certificate templates.

Lecture Focus Questions:

- How does Web enrollment differ from autoenrollment?
- What type of certificates can users request through Web enrollment? What reasons might prevent a certificate from appearing in the list of certificates that can be requested?
- How do standalone CAs handle certificate requests?
- What permissions are required to enable autoenrollment? What additional tasks are required for autoenrollment to work?
- What certificate template settings might cause autoenrollment to fail?

Time

About 35 minutes

Lab/Activity

- Configure Templates for Autoenrollment
- Enable Autoenrollment for the Domain

Section 7.5: Certificate Revocation

Summary

This section discusses what certificate revocation is and possible reasons for revocation. Students will become familiar with the following terms and how to manage revocation:

- Certification Revocation List (CRL)
- CRL Distribution Point (CRP)
- Delta CRL
- Online Certificate Status Protocol (OCSP)
- Online Responder

Students will learn how to:

- Revoke and un revoke certificates.
- Configure CRL distribution point locations.
- Manage and publish CRLs.
- Install and configure the Online Responder role service.
- Configure a CA to support an online responder.

Windows Server 2008 Active Directory Objectives

- 602. Configure CA server settings.
- 605. Manage certificate revocations.

Lecture Focus Questions:

- What circumstances might cause you to need to revoke a certificate?
- When can a certificate in the Revoked Certificates folder be unrevoked?
- What is the relationship between the CRL and the CDP?
- What is the advantage of using delta CRLs?
- How is a CRL used by an online responder?
- What two certificates must the online responder have?
- How does the online responder use the OCSP Response Signing certificate? How many of these certificates should the online responder have?
- What is the difference between the CDP extensions and the AIA extensions? When would you use both?

Time

About 35 minutes

Lab/Activity

- Manage Certificate Revocation

Section 7.6: CA Management

Summary

This section provides details on management of CAs through the use of the following permissions:

- Read
- Issue and Manage Certificates
- Manage CA
- Request Certificates

Certificate management tasks are performed using the Certification Authority snap-in or the **Certutil.exe** command line utility.

Students will learn how to:

- Configure administrative permissions to a CA.
- Restrict certificate managers and enrollment agents on a CA.
- Configure CA auditing.

Windows Server 2008 Active Directory Objectives

- 602. Configure CA server settings.

Lecture Focus Questions:

- What permissions are required for an administrator to approve certificates?
- Which types of templates does key archival work with?
- You have a certificate template that is configured to issue the certificate without CA manager approval. On the CA, manager approval is required. How does the certificate request get approved?
- In addition to selecting auditing events on the CA, what else must you do to enable auditing for CAs?

Time

About 15 minutes

Section 7.7: Certificate Implementations

Summary

This section explores the following certificate implementations:

- Smart Card Deployment
- Key Archival
- Network Device Enrollment Service
- Certificate Roles

Students will learn how to:

- Configure certificate templates and CAs for smartcard deployment.

Windows Server 2008 Active Directory Objectives

- 602. Configure CA server settings.
- 603. Manage certificate templates.

Lecture Focus Questions:

- What is the difference between a Smartcard Logon and a Smartcard User certificate?
- How is the enrollment agent used with smartcards?
- What Group Policy settings control smartcard use?
- What is the purpose of *key archival*?
- What is the role of the recovery agent in key archival?
- What certificate template and CA settings are required to configure key archival?
- With NDES, what functions are performed by the registration authority?
- What is the **certsrv/mscep_admin** virtual directory used for?
- Your registration authority has 5 pending requests and will not issue any more passwords for device certificate requests. What options do you have if you need to get a request password immediately?

Time

About 25 minutes

Lab/Activity

- Create Certificates for Smart Cards
- Require Smart Cards for Logon

Section 8.1: Lightweight Directory Services (AD LDS)

Summary

This section discusses installing, configuring and managing Active Directory Lightweight Directory Services (AD LDS). AD LDS can be used as a flexible and secure solution to provide single sign-on (SSO) functionality for Web applications. The following tools are used to manage AD LDS instances:

- Active Directory Lightweight Directory Services console
- Adaminstall.exe
- ADSI Edit
- Ldp.exe
- Ldifde.exe
- Active Directory Schema snap-in
- ADSchemaAnalyzer
- Dsacls

The students will learn guidelines for the following methods of AD LDS instance configuration:

- Move an instance
- Import data into an instance
- Create a replication schedule
- Synchronize data

Students will learn how to:

- Install and configure an AD LDS instance.

Windows Server 2008 Active Directory Objectives

- 301. Configure Active Directory Lightweight Directory Service (AD LDS).

Lecture Focus Questions:

- What is an AD LDS *instance*? What is a *configuration set*?
- How does AD LDS replicate?
- Which port numbers would you not use if AD LDS and AD DS are running on the same system?
- What tools do you use to create an instance?
- What tools can you use to import or modify the schema of an AD LDS instance?
- How can you synchronize data between AD DS and AD LDS?

Time

About 35 minutes

Section 8.2: Federation Services (AD FS)

Summary

This section provides information about Active Directory Federation Services (AD FS). To understand how AD FS works, students need to be familiar with the following terms:

- Claim
- Security token
- Security Token Service (STS)
- Federation server
- Federation trust
- Trust policy
- AD FS-enabled Web server

The elements of the trust policy and the basic process for configuring AD FS are discussed.

Students will learn how to:

- Install the AD FS role.
- Configure claims, applications, and account partners.
- Map claims to directory service attributes.

Windows Server 2008 Active Directory Objectives

- 304. Configure Active Directory Federation Services (AD FS).

Lecture Focus Questions:

- You have users that need to access a Web application in a partner domain. Which domain is the account domain, and which is the resource domain?
- What are the differences between the Federation Service and Federation Service Proxy?
- What is a *claim*? What type of information can be included in a claim?
- Which directory services can AD FS use?
- What is the difference between a claims-aware application and a token-based application?
- You have users that need to access a Web application in a partner domain. What type of partner would you configure?

Time

About 35 minutes

Section 8.3: Rights Management Services (AD RMS)

Summary

This section explores installing and configuring Active Directory Rights Management Services (AD RMS) to safeguard digital information from unauthorized users.

Students will learn how to:

- Install the AD RMS server role.
- Protect content from within an AD RMS-aware application.

Windows Server 2008 Active Directory Objectives

- 302. Configure Active Directory Rights Management Service (AD RMS).

Lecture Focus Questions:

- What are the basic system components necessary for AD RMS?
- Which component in an AD RMS implementation is responsible for encrypting documents and enforcing the usage policies?
- What is the difference between a root cluster and a licensing-only cluster?
- When should you use the Windows Internal Database for AD RMS? When can you not use it?
- Why should you not use the AD RMS server name as the cluster address?
- Which certificate establishes a user's identity and which certificate specifies rights to protected content?

Time

About 30 minutes

Section 9.1: Recovery and Availability

Summary

In this section students will become familiar with the following tools available for managing disaster recovery and availability:

- Windows Server Backup
- Windows Recovery Environment
- Shadow Copies
- Clustering
- Network Load Balancing (NLB)

Windows Server 2008 Active Directory Objectives

- 501. Configure backup and recovery.

Lecture Focus Questions:

- What are the components of the Windows Recovery Environment?
- How does clustering optimize your network service availability?
- What happens when a server in an NLB configuration fails?

Time

About 5 minutes

Section 9.2: Windows Server Backup

Summary

This section discusses Windows Server Backup which is used to provide backup and recovery for Windows Server 2008. It replaces the NTbackup.exe utility in previous Windows versions. Windows Server Backup does not support backups to tape devices, but can save backups to the following storage types:

- Local disk
- External disk
- Shared folder
- DVD

Windows Server Backup can be used to perform automatic, manual, or scheduled backups, and also system state backup, from the command line.

Several tools used to perform system recovery are presented as well as the types of data that can be recovered:

- Files and folders
- Volumes
- Application
- Backup catalog
- Operating system or full server
- System state
- Backup created with Ntbackup

Students will learn how to:

- Install Windows Server Backup.
- Create a backup schedule.
- Perform a Backup Once operation.

Windows Server 2008 Active Directory Objectives

- 501. Configure backup and recovery.

Lecture Focus Questions:

- Which backup storage type(s) would you choose if you wanted to be able to restore individual folders or files?
- What volumes are always included in scheduled backups? How can you create a backup to exclude these volumes?
- What storage types are available when using automatic backups?

- What happens to a local disk when you designate it for use by Windows Server Backup?
- How can you create automatic backups with a frequency less than once a day?
- Which backup type can only be performed from the command prompt?

Time

About 30 minutes

Lab/Activity

- Back Up a Server

Section 9.3: Active Directory Backup and Restore

Summary

This section explores methods for restoring Active Directory with special considerations concerning the restoring of group membership.

There are two types of restore when restoring Active Directory:

- Nonauthoritative
- Authoritative

The following methods can be used to restore lost Active Directory data:

- LostAndFound container
- Authoritative restore
- View snapshots

Students will learn how to:

- Perform an authoritative and nonauthoritative restore using **Ntdsutil**.
- Reset the Directory Services Restore Mode (DSRM) password.
- Create AD DS snapshots.

Windows Server 2008 Active Directory Objectives

- 501. Configure backup and recovery.

Lecture Focus Questions:

- Which backup type should you perform if you want to protect Active Directory?
- What are the requirements for performing a system state backup?
- What is the difference between an authoritative and a nonauthoritative restore?
- What is replicated to a restored domain controller after a restore system state operation?
- What is the disadvantage of using the **dcpromo /forceremoval** command?
- Why might group membership not be restored with an authoritative restore?
When would this problem exist, and how can you overcome it?

Time

About 30 minutes

Section 9.4: Maintenance and Monitoring

Summary

This section discusses tools used for maintenance and monitoring of Active Directory and system events:

- Restartable Active Directory
- Event Viewer
- Network Monitor
- Task Manager
- Windows System Resource Manager

Students will learn how to:

- Monitor Active Directory using Server Manager, Event Viewer, and Performance and Reliability Monitor
- Start and stop AD DS to perform offline maintenance tasks.
- Control Group Policy by determining the RSoP.

Windows Server 2008 Active Directory Objectives

- 502. Perform offline maintenance
- 503. Monitor Active Directory.

Lecture Focus Questions:

- What additional tasks are performed during an offline defragmentation when compared to an online defragmentation? Which can be performed using restartable Active Directory?
- What are the advantages of using restartable Active Directory?
- When would you use Performance Monitor instead of Network Monitor?
- What is the relationship of *counters* to *objects*?
- What is the difference between RepMon and RepAdmin?
- What is the difference between Group Policy Modeling and Group Policy Results? Which would you use if you wanted to see the effects of changing group membership or OU location?

Time

About 35 minutes

Practice Exams

Summary

This section provides information to help prepare students to take the exam and to register for the exam.

Students will also have the opportunity of testing their mastery of the concepts presented in this course to reaffirm that they are ready for the certification exam. For example, all questions that apply to **Objective 100. Configuring Domain Name System (DNS) for Active Directory** are grouped together and presented in practice exam **100. DNS, All Questions**. Students will typically take about 60-90 minutes to complete each of the following practice exams.

- 100. DNS, All Questions (49 questions)
- 200. Infrastructure, All Questions (64 questions)
- 300. Server Roles, All Questions (28 questions)
- 400. Objects, All Questions (99 questions)
- 500. Maintenance, All Questions (28 questions)
- 600. Certificate Services, All Questions (52 questions)

The *Certification Practice Exam* consists of 42 questions that are randomly selected from the above practice exams. Each time the Certification Practice Exam is accessed different questions may be presented. The Certification Practice Exam has a time limit of 80 minutes -- just like the real certification exam. A passing score of 95% should verify that the student has mastered the concepts and is ready to take the real certification test.