

---

# Module 1: Introduction to Active Directory Infrastructure

## Contents

Overview	1
Lesson: The Architecture of Active Directory	2
Lesson: How Active Directory Works	10
Lesson: Examining Active Directory	19
Lesson: The Active Directory Design, Planning, and Implementation Processes	29



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

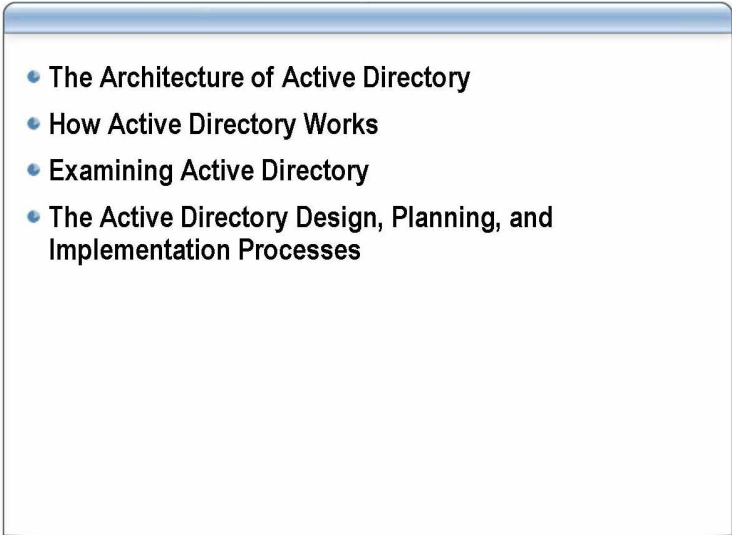
Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows NT, Active Directory, Active X, MSDN, PowerPoint, Visio, Visual Basic, Visual C++, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

# Overview

- 
- The Architecture of Active Directory
  - How Active Directory Works
  - Examining Active Directory
  - The Active Directory Design, Planning, and Implementation Processes

---

## Introduction

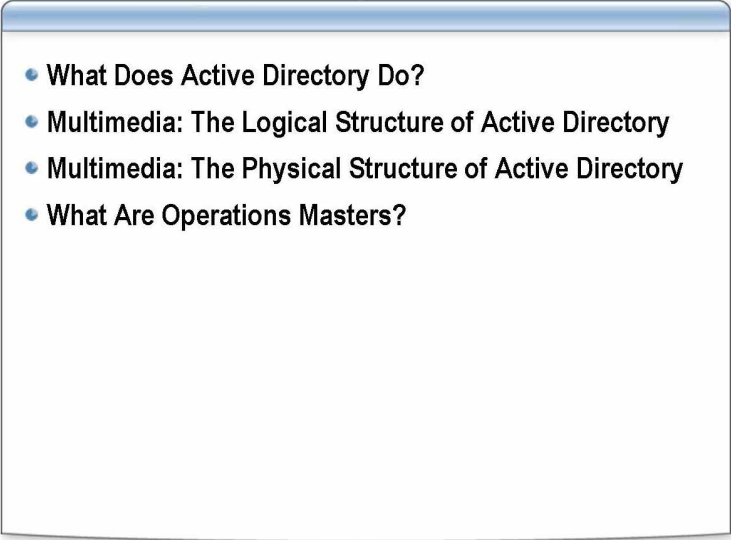
This module introduces the logical and physical structure of the Active Directory® directory service and its function as a directory service. The module also introduces the snap-ins, the command-line tools, and the Windows Script Host that you can use to manage the components of Active Directory and the Active Directory design, planning, and implementing processes.

## Objectives

After completing this module, you will be able to:

- Describe the architecture of Active Directory.
- Describe how Active Directory works.
- Use administrative snap-ins to examine the components of Active Directory.
- Describe the Active Directory design, planning, and implementation processes.

## Lesson: The Architecture of Active Directory

- 
- What Does Active Directory Do?
  - Multimedia: The Logical Structure of Active Directory
  - Multimedia: The Physical Structure of Active Directory
  - What Are Operations Masters?

---

### Introduction

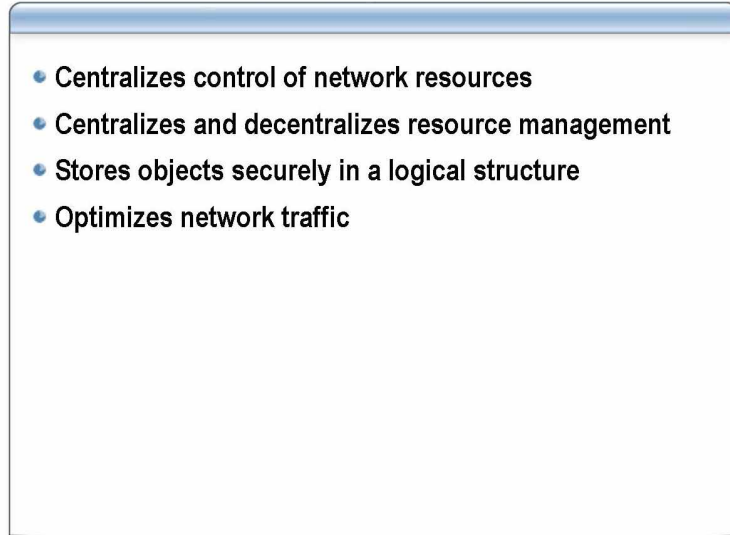
Active Directory consists of components that constitute its logical and physical structure. You must plan both the logical and physical structures of Active Directory to meet your organization's requirements. To manage Active Directory, you must understand the purpose of these components and how to use them.

### Lesson objectives

After completing this lesson, you will be able to:

- Describe the function of Active Directory.
- Describe the logical structure of Active Directory.
- Describe the physical structure of Active Directory.
- Describe the operations master roles.

## What Does Active Directory Do?



---

### Introduction

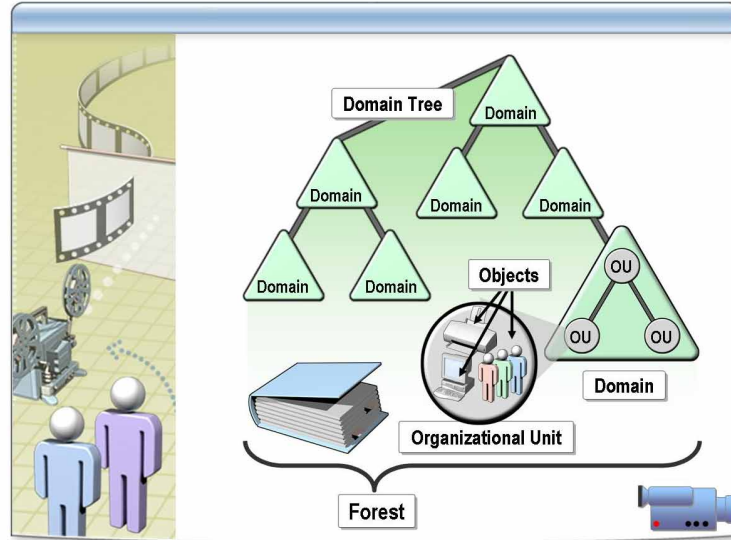
Active Directory stores information about users, computers, and network resources and makes the resources accessible to users and applications. It provides a consistent way to name, describe, locate, access, manage, and secure information about these resources.

### The function of Active Directory

Active Directory provides the following functions:

- *Centralizes control of network resources.* By centralizing control of resources such as servers, shared files, and printers, only authorized users can access resources in Active Directory.
- *Centralizes and decentralizes resource management.* Administrators can manage distributed client computers, network services, and applications from a central location by using a consistent management interface, or they can distribute administrative tasks by delegating the control of resources to other administrators.
- *Stores objects securely in a logical structure.* Active Directory stores all of the resources as objects in a secure, hierarchical logical structure.
- *Optimizes network traffic.* The physical structure of Active Directory enables you to use network bandwidth more efficiently. For example, it ensures that, when users log on to the network, they are authenticated by the authentication authority that is nearest to the user, thus reducing the amount of network traffic.

## Multimedia: The Logical Structure of Active Directory



### File location

To view the presentation, *The Logical Structure of Active Directory*, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation. Do not open this presentation unless the instructor tells you to.

### Objectives

At the end of this presentation you will be able to:

- Define the elements of the logical structure of Active Directory.
- Discuss the purposes of those elements.

### Key points

Active Directory provides secure storage of information about objects in its hierarchical logical structure. Active Directory *objects* represent users and resources, such as computers and printers. Some objects are containers for other objects. By understanding the purpose and function of these objects, you can complete a variety of tasks, including installing, configuring, managing, and troubleshooting Active Directory.

The logical structure of Active Directory includes the following components:

- *Objects*. These are the most basic components of the logical structure. *Object classes* are templates or blueprints for the types of objects that you can create in Active Directory. Each object class is defined by a group of *attributes*, which define the possible values that you can associate with an object. Each object has a unique combination of attribute values.
- *Organizational units*. You use these container objects to arrange other objects in a manner that supports your administrative purposes. By arranging objects by organizational unit, you make it easier to locate and manage objects. You can also delegate the authority to manage an organizational unit. Organizational units can be *nested* in other organizational units, which further simplifies the management of objects.

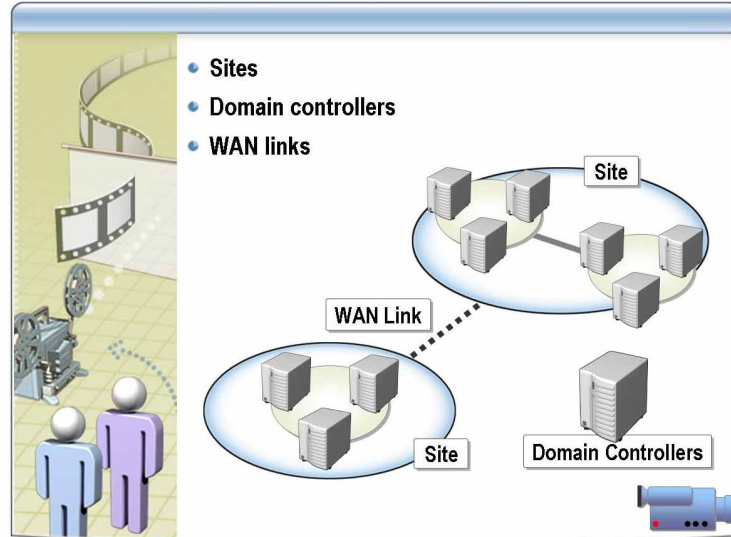
- *Domains.* The core functional units in the Active Directory logical structure, domains are a collection of administratively defined objects that share a common directory database, security policies, and trust relationships with other domains. Domains provide the following three functions:
  - An administrative boundary for objects
  - A means of managing security for shared resources
  - A unit of replication for objects
- *Domain trees.* Domains that are grouped together in hierarchical structures are called domain trees. When you add a second domain to a tree, it becomes a *child* of the tree root domain. The domain to which a child domain is attached is called the *parent domain*. A child domain may in turn have its own child domain.

The name of a child domain is combined with the name of its parent domain to form its own unique Domain Name System (DNS) name such as corp.nwtraders.msft. In this manner, a tree has a *contiguous namespace*.

- *Forests.* A forest is a complete instance of Active Directory. It consists of one or more trees. In a single two-level tree, which is recommended for most organizations, all child domains are made children of the forest root domain to form one contiguous tree.

The first domain in the forest is called the *forest root domain*. The name of that domain refers to the forest, such as nwtraders.msft. By default, the information in Active Directory is shared only within the forest. This way, the forest is a security boundary for the information that is contained in the instance of Active Directory.

## Multimedia: The Physical Structure of Active Directory



### File location

To view the presentation, *The Physical Structure of Active Directory*, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation. Do not open this presentation unless the instructor tells you to.

### Objectives

At the end of this presentation, you will be able to:

- Define the elements of the physical structure of Active Directory.
- Discuss the purpose of those elements.

### Key points

In contrast to the logical structure, which models administrative requirements, the physical structure of Active Directory optimizes network traffic by determining when and where replication and logon traffic occur. To optimize Active Directory's use of network bandwidth, you must understand the physical structure. The elements of the Active Directory physical structure are:

- *Domain controllers.* These computers run Microsoft® Windows® Server 2003 or Windows 2000 Server, and Active Directory. Each domain controller performs storage and replication functions. A domain controller can support only one domain. To ensure continuous availability of Active Directory, each domain should have more than one domain controller.



- 
- *Active Directory sites*. These sites are groups of well-connected computers. When you establish sites, domain controllers within a single site communicate frequently. This communication minimizes the *latency* within the site; that is, the time required for a change that is made on one domain controller to be replicated to other domain controllers. You create sites to optimize the use of bandwidth between domain controllers that are in different locations.

---

**Note** For more information about Active Directory sites, see Module 7, “Implementing Sites to Manage Active Directory Replication” in Course 2279: *Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure*.

---

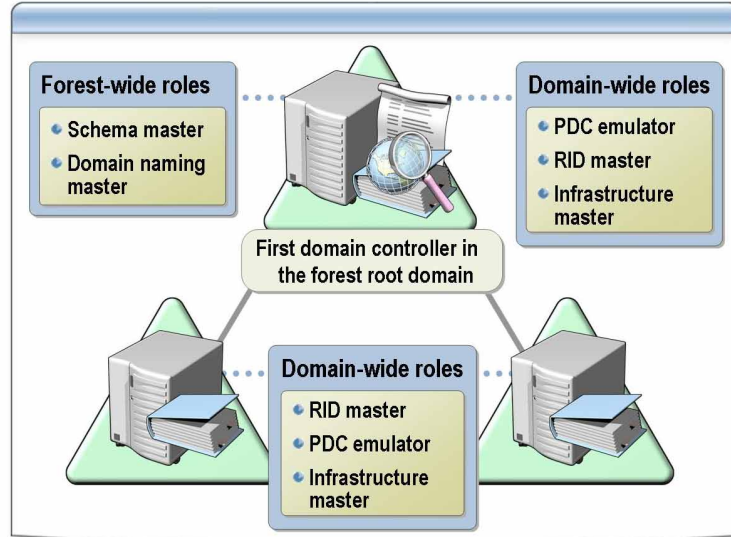
- *Active Directory partitions*. Each domain controller contains the following Active Directory partitions:
  - The *domain partition* contains replicas of all of the objects in that domain. The domain partition is replicated only to other domain controllers in the same domain.
  - The *configuration partition* contains the forest topology. *Topology* is a record of all domain controllers and the connections between them in a forest.
  - The *schema partition* contains the forest-wide schema. Each forest has one schema so that the definition of each object class is consistent. The configuration and schema partitions are replicated to each domain controller in the forest.
  - Optional *application partitions* contain objects that are unrelated to security and that are used by one or more applications. Application partitions are replicated to specified domain controllers in the forest.

---

**Note** For more information about Active Directory partitions, see Module 7, “Implementing Sites to Manage Active Directory Replication,” in Course 2279: *Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure*.

---

## What Are Operations Masters?



### Introduction

When a change is made to a domain, the change is replicated across all of the domain controllers in the domain. Some changes, such as those made to the schema, are replicated across all of the domains in the forest. This replication is called *multimaster replication*.

### Single master operations

During multimaster replication, a replication conflict can occur if originating updates are performed concurrently on the same object attribute on two domain controllers. To avoid replication conflicts, you use *single master replication*, which designates one domain controller as the only domain controller on which certain directory changes can be made. This way, changes cannot occur at different places in the network at the same time. Active Directory uses single master replication for important changes, such as the addition of a new domain or a change to the forest-wide schema.

### Operations master roles

Operations that use single-master replication are arranged together in specific roles in a forest or domain. These roles are called *operations master roles*. For each operations master role, only the domain controller that holds that role can make the associated directory changes. The domain controller that is responsible for a particular role is called an *operations master* for that role. Active Directory stores information about which domain controller holds a specific role.

Active Directory defines five operations master roles, each of which has a default location. Operations master roles are either forest-wide or domain-wide.

- *Forest-wide roles.* Unique to a forest, forest-wide roles are:
  - *Schema master.* Controls all updates to the schema. The schema contains the master list of object classes and attributes that are used to create all Active Directory objects, such as users, computers, and printers.
  - *Domain naming master.* Controls the addition or removal of domains in the forest. When you add a new domain to the forest, only the domain controller that holds the domain naming master role can add the new domain.

There is only one schema master and one domain naming master in the entire forest.

- *Domain-wide roles.* Unique to each domain in a forest, the domain-wide roles are:
  - *Primary domain controller emulator (PDC).* Acts as a Windows NT PDC to support any backup domain controllers (BDCs) running Microsoft Windows® NT within a *mixed-mode domain*. This type of domain has domain controllers that run Windows NT 4.0. The PDC emulator is the first domain controller that you create in a new domain.
  - *Relative identifier master.* When a new object is created, the domain controller creates a new security principal that represents the object and assigns the object a unique security identifier (SID). This SID consists of a domain SID, which is the same for all security principals created in the domain, and a relative identifier (RID), which is unique for each security principal created in the domain. The RID master allocates blocks of RIDs to each domain controller in the domain. The domain controller then assigns a RID to objects that are created from its allocated block of RIDs.
  - *Infrastructure master.* When objects are moved from one domain to another, the infrastructure master updates object references in its domain that point to the object in the other domain. The object reference contains the object's globally unique identifier (GUID), distinguished name, and a SID. Active Directory periodically updates the distinguished name and the SID on the object reference to reflect changes made to the actual object, such as moves within and between domains and the deletion of the object.

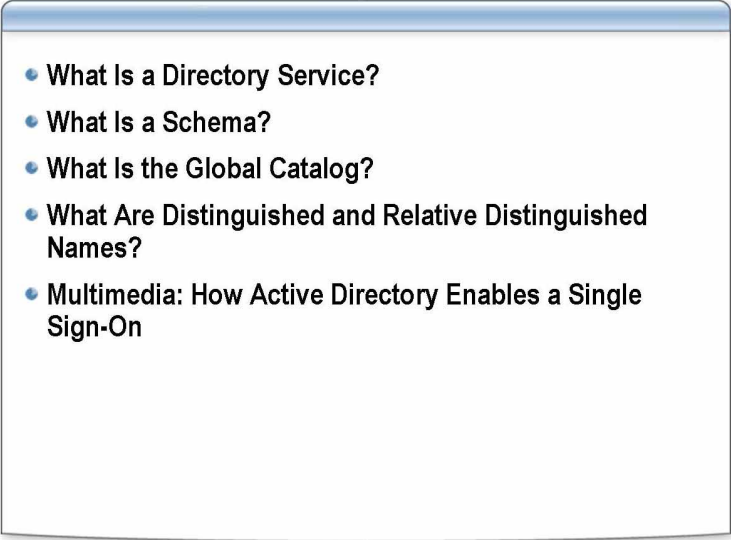
Each domain in a forest has its own PDC emulator, RID master, and infrastructure master.

---

**Note** For more information about operations master roles see, Module 9, *Managing Operations Masters in Course 2279: Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure*.

---

## Lesson: How Active Directory Works

- 
- What Is a Directory Service?
  - What Is a Schema?
  - What Is the Global Catalog?
  - What Are Distinguished and Relative Distinguished Names?
  - Multimedia: How Active Directory Enables a Single Sign-On

---

### Introduction

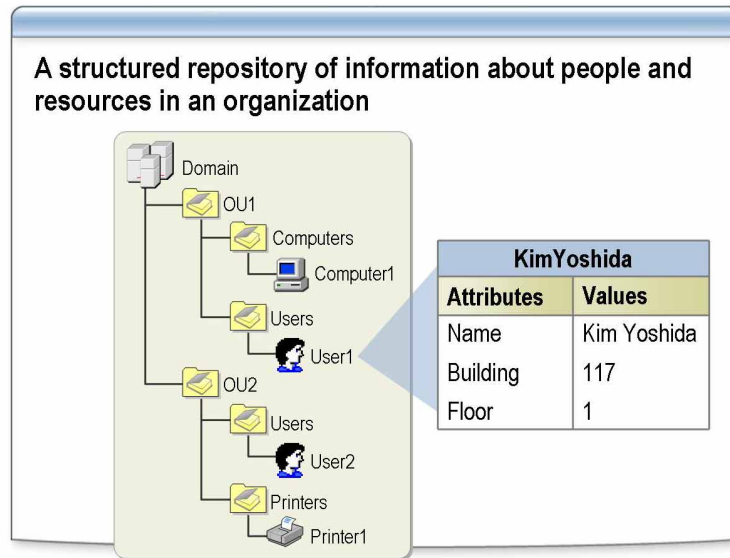
This lesson introduces the function of Active Directory as a directory service. Understanding how Active Directory works will help you manage resources and troubleshoot problems with accessing resources.

### Lesson objectives

After completing this lesson, you will be able to:

- Describe the function of Active Directory as a directory service.
- Define the purpose of the Active Directory schema and how it is used.
- Define the purpose of the global catalog.
- Determine the distinguished name and relative distinguished name of an Active Directory object.
- Describe how Active Directory enables single sign-on.

## What Is a Directory Service?



### Introduction

Resources in large networks are shared by many users and applications. To enable users and applications to access these resources and information about them, you require a consistent way to name, describe, locate, access, manage, and secure information about these resources. A directory service performs this function.

### What is a directory service?

A directory service is a structured repository of information about people and resources in an organization. In a Windows Server 2003 network, the directory service is Active Directory.

### Capabilities of Active Directory

Active Directory has the following capabilities:

- *Enables users and applications to access information about objects.* This information is stored in the form of attribute values. You search for objects on the basis of their object class, attributes, attribute values, their location within the Active Directory structure, or any combination of these values.
- *Makes the physical network topology and protocols transparent.* This way, a user on a network can access any resource, such as a printer, without knowing where the resource is or how it is physically connected to the network.

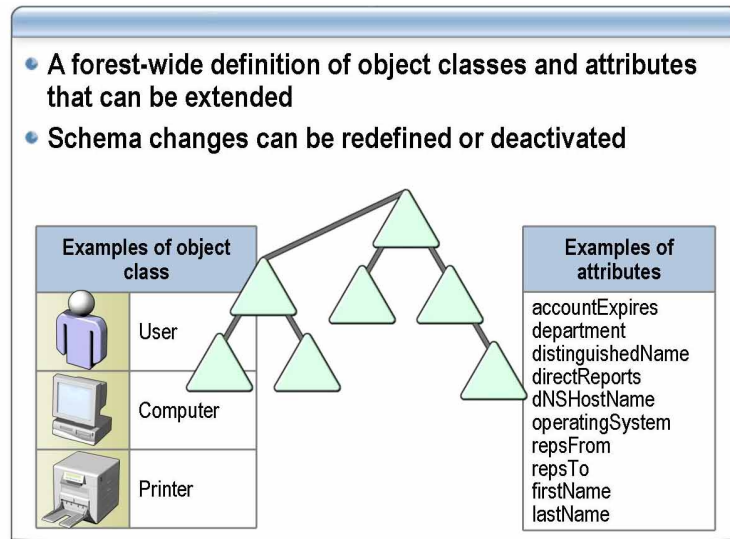
- *Permits the storage of a very large number of objects.* Because it is organized in partitions, Active Directory can expand as an organization grows. For example, a directory can expand from a single server with a few hundred objects to thousands of servers and millions of objects.
- *Can run as a non-operating system service.* Active Directory in Application Mode (AD/AM) is a new capability of Microsoft Active Directory that addresses certain deployment scenarios related to directory-enabled applications. AD/AM runs as a non-operating system service and, as such, does not require deployment on a domain controller. Running as a non-operating system service means that multiple instances of AD/AM can run concurrently on a single server, with each instance being independently configurable.

---

**Note** For more information about AD/AM, see “Introduction to Active Directory in Application Mode” at <http://www.microsoft.com/windowsserver2003/techinfo/overview/adam.msp>.

---

## What Is a Schema?



### Introduction

The Active Directory schema defines the kinds of objects, the types of information about those objects, and the default security configuration for those objects that can be stored in Active Directory.

### What is the Active Directory schema?

The Active Directory *schema* contains the definitions of all objects, such as users, computers, and printers that are stored in Active Directory. On domain controllers running Windows Server 2003, there is only one schema for an entire forest. This way, all objects that are created in Active Directory conform to the same rules.

The schema has two types of definitions: object classes and attributes. *Object classes* such as user, computer, and printer describe the possible directory objects that you can create. Each object class is a collection of attributes.

Attributes are defined separately from object classes. Each attribute is defined only once and can be used in multiple object classes. For example, the **Description** attribute is used in many object classes, but is defined only once in the schema to ensure consistency.

### Active Directory schema and extensibility

You can create new types of objects in Active Directory by extending the schema. For example, for an e-mail server application, you could extend the user class in Active Directory with new attributes that store additional information, such as users' e-mail addresses.

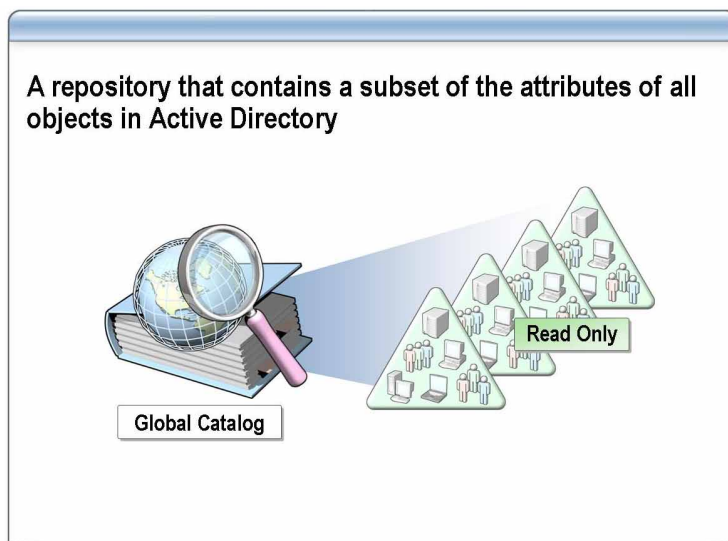
**Note** For more information about extending the Active Directory schema, see *Extending the Schema* in the MSDN Library online reference.

### Schema changes and deactivation

On Windows Server 2003 domain controllers, you can reverse schema changes by deactivating them, thus enabling organizations to better exploit Active Directory's extensibility features.

You may also redefine a schema class or attribute. For example, you could change the Unicode String syntax of an attribute called SalesManager to Distinguished Name.

## What Is the Global Catalog?



### Introduction

Resources in Active Directory can be shared across domains and forests. The global catalog feature in Active Directory makes searching for resources across domains and forests transparent to the user. For example, if you search for all of the printers in a forest, a global catalog server processes the query in the global catalog and then returns the results. Without a global catalog server, this query would require a search of every domain in the forest.

### What is the global catalog?

The *global catalog* is a repository of information that contains a subset of the attributes of all objects in Active Directory. Members of the Schema Admins group can change which attributes are stored in the global catalog, depending on an organization's requirements. The global catalog contains:

- The attributes that are most frequently used in queries, such as a user's first name, last name, and logon name.
- The information that is necessary to determine the location of any object in the directory.
- A default subset of attributes for each object type.
- The access permissions for each object and attribute that is stored in the global catalog. If you search for an object that you do not have the appropriate permissions to view, the object will not appear in the search results. Access permissions ensure that users can find only objects to which they have been assigned access.

### What is a global catalog server?

A *global catalog server* is a domain controller that efficiently processes intraforest queries to the global catalog. The first domain controller that you create in Active Directory automatically becomes a global catalog server. You can configure additional global catalog servers to balance the traffic for logon authentication and queries.



**Functions of the global catalog**

The global catalog enables users to perform two important functions:

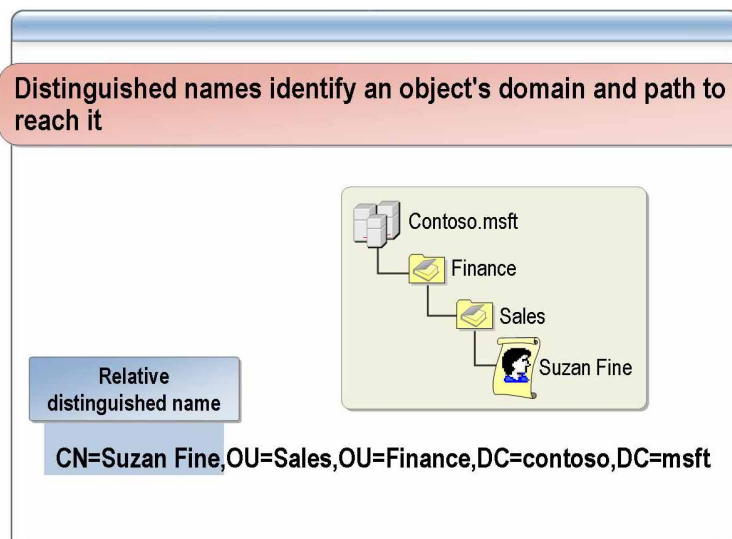
- Find Active Directory information anywhere in the forest, regardless of the location of the data.
- Use universal group membership information to log on to the network.

---

**Note** For more information about the global catalog, see Module 8, “Implementing the Placement of Domain Controllers,” in Course 2279: *Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure*.

---

## What Are Distinguished and Relative Distinguished Names?



### Introduction

Client computers use the Lightweight Directory Access Protocol (LDAP) protocol to search for and modify objects in an Active Directory database. LDAP is a subset of X.500, an industry standard that defines how to structure directories. LDAP uses information about the structure of a directory to find individual objects, each of which has a unique name.

### Definition

LDAP uses a name that represents an Active Directory object by a series of components that relate to the logical structure. This representation, called the *distinguished name* of the object, identifies the domain where the object is located and the complete path by which the object is reached. A distinguished name must be unique in an Active Directory forest.

The *relative distinguished name* of an object uniquely identifies the object in its container. No two objects in the same container can have the same name. The relative distinguished name is always the first component of the distinguished name, but it may not always be a common name.

### Example of a Distinguished Name

For a user named Suzan Fine in the Sales organizational unit in the Contoso.msft domain, each element of the logical structure is represented in the following distinguished name:

```
CN=Suzan Fine,OU=Sales,DC=contoso,DC=msft
```

- CN is the common name of the object in its container.
- OU is the organizational unit that contains the object. There can be more than one OU value if the object resides in a nested organizational unit.
- DC is a domain component, such as “com” or “msft”. There are always at least two domain components, but possibly more if the domain is a child domain.

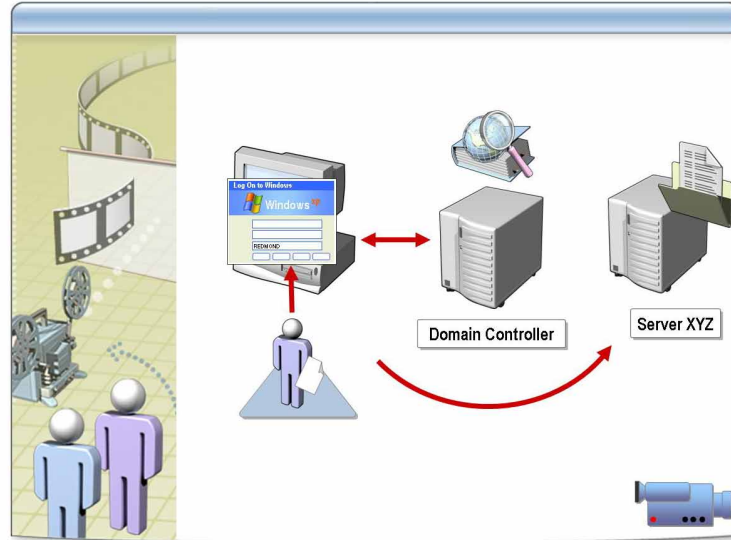
The domain components of the distinguished name are based on the Domain Name System (DNS).

**Example of a Relative Distinguished Name**

In the following example, Sales is the relative distinguished name of an organizational unit that is represented by this LDAP naming path:

```
OU=Sales,DC=contoso,DC=msft
```

## Multimedia: How Active Directory Enables a Single Sign-on



### File location

To view the presentation, *How Active Directory Enables a Single Sign-on*, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation. Do not open this presentation unless the instructor tells you to.

### Objectives

At the end of this presentation, you will be able to:

- Describe the process by which Active Directory enables a single sign-on.
- Discuss the importance of a single sign-on.

### Key points

By enabling a single sign-on, Active Directory makes the complex processes of authentication and authorization transparent to the user. Users do not need to manage multiple sets of credentials.

A single sign-on consists of:

- *Authentication*, which verifies the credentials of the connection attempt.
- *Authorization*, which verifies that the connection attempt is allowed.

As a systems engineer, you must understand how these processes work in order to optimize and troubleshoot your Active Directory structure.

---

## Lesson: Examining Active Directory

- 
- Active Directory Management
  - Active Directory Administrative Snap-ins and Tools
  - How to Examine Active Directory

---

### Introduction

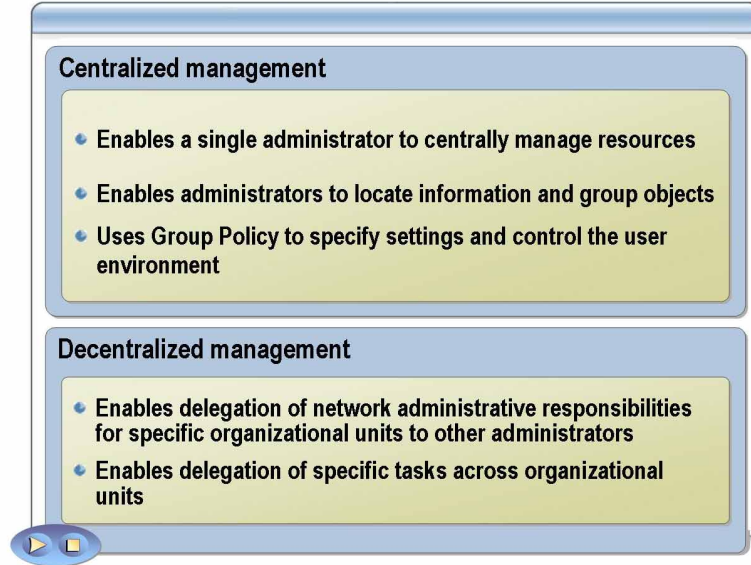
Windows Server 2003 provides administrators with snap-ins and command-line tools to manage Active Directory. This lesson introduces these snap-ins and command-line tools and explains how you use them to examine the logical and physical structure of Active Directory.

### Lesson objectives

After completing this lesson, you will be able to:

- Explain how Active Directory is designed to enable centralized and decentralized management.
- Describe common Active Directory administrative snap-ins and command-line tools.
- Examine the logical and physical structure of Active Directory.

## Active Directory Management



---

### Introduction

By using Active Directory, you can manage large numbers of users, computers, printers, and network resources from a central location, using the administrative snap-ins and tools in Windows Server 2003. Active Directory also supports decentralized administration. An administrator with the proper authority can delegate a selected set of administrative privileges to other users or groups in an organization.

### How Active Directory supports centralized management

Active Directory includes several features that support centralized management:

- *It contains information about all objects and their attributes.* The attributes contain data that describes the resource that the object identifies. Because information about all network resources is stored in Active Directory, one administrator can centrally manage and administer network resources.
- *You can query Active Directory by using protocols such as LDAP.* You can easily locate information about objects by searching for selected attributes of the object, using tools that support LDAP.
- *You can arrange objects that have similar administrative and security requirements into organizational units.* Organizational units provide multiple levels of administrative authority, so that you can apply Group Policy settings and delegate administrative control. This delegation simplifies the task of managing these objects and enables you to structure Active Directory to fit your organization's requirements.
- *You can specify Group Policy settings for a site, a domain, or an organizational unit.* Active Directory then enforces these Group Policy settings for all of the users and computers within the container.

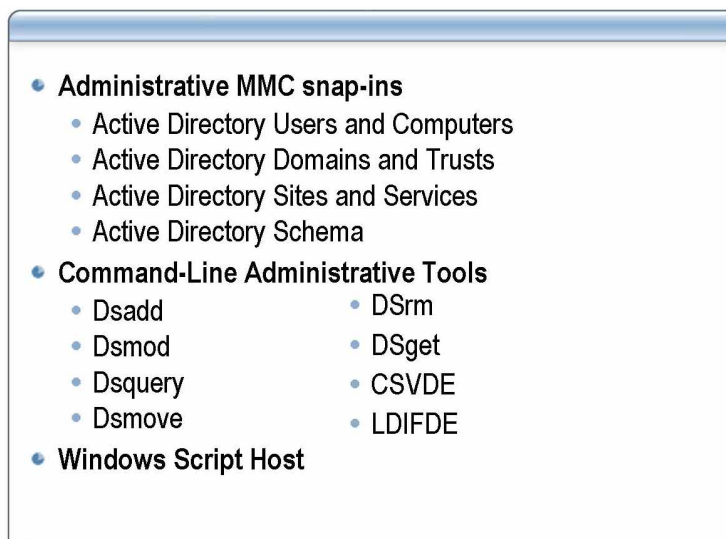
**How Active Directory supports decentralized management**

Active Directory also supports decentralized management. You can assign permissions and grant user rights in very specific ways. For example, you can delegate administrative privileges for certain objects to the sales and marketing teams in an organization.

You can delegate the assigning of permissions:

- For specific organizational units to different domain local groups. For example, delegating the permission Full Control for the Sales organizational unit.
- To modify specific attributes of an object in an organizational unit. For example, assign the permission to change the name, address, and telephone number and to reset passwords on a user account object.
- To perform the same task, such as resetting passwords, in all organizational units of a domain.

## Active Directory Administrative Snap-ins and Tools



### Introduction

Windows Server 2003 provides a number of snap-ins and command-line tools to manage Active Directory. You can also manage Active Directory by using Active Directory Service Interfaces (ADSI) objects from Windows Script Host scripts. ADSI is a simple yet powerful interface to Active Directory for creating reusable scripts to manage Active Directory.

### Administrative snap-ins

The following table describes some common administrative snap-ins for managing Active Directory.

Snap-in	Description
Active Directory Users and Computers	A Microsoft Management Console (MMC) that you use to manage and publish information in Active Directory. You can manage user accounts, groups, and computer accounts, add computers to a domain, manage account policies and user rights, and audit policy.
Active Directory Domains and Trusts	An MMC that you use to manage domain trusts and forest trusts, add user principal name suffixes, and change the domain and forest functional levels.
Active Directory Sites and Services	An MMC that you use to manage the replication of directory data.
Active Directory Schema	An MMC that you use to manage the schema. It is not available by default on the Administrative Tools menu. You must add it manually.

**Note** You can also use the ADSI Editor to view, create, modify, and delete objects in Active Directory. ADSI Editor is not installed by default. To install the ADSI Editor, install the Windows Server 2003 support tools from the \Support\Tools folder on the product compact disc.

You can customize administrative consoles to match the administrative tasks that you delegate to other administrators. You can also combine all of the consoles required for each administrative function into one console.



**Command-line administrative tools**

The following table describes some common command-line tools to use when you manage Active Directory.

<b>Tool</b>	<b>Description</b>
Dsadd	Adds objects, such as computers, users, groups, organizational units, and contacts, to Active Directory.
Dsmode	Modifies objects, such as computers, servers, users, groups, organizational units, and contacts, in Active Directory.
Dsquery	Runs queries in Active Directory according to specified criteria. You can run queries against servers, computers, groups, users, sites, organizational units, and partitions.
Dsmove	Moves a single object, within a domain, to a new location in Active Directory, or renames a single object without moving it.
Dsrm	Deletes an object from Active Directory.
Dsget	Displays selected attributes of a computer, contact, group, organizational unit, server, or user in Active Directory.
Csvde	Imports and exports Active Directory data by using comma-separated format.
Ldifde	Creates, modifies, and deletes Active Directory objects. Can also extend the Active Directory schema, export user and group information to other applications or services, and populate Active Directory with data from other directory services.

---

**Note** For more information about command-line tools provided by Windows Server 2003, see “Managing Active Directory from the command-line” in Help and Support.

---

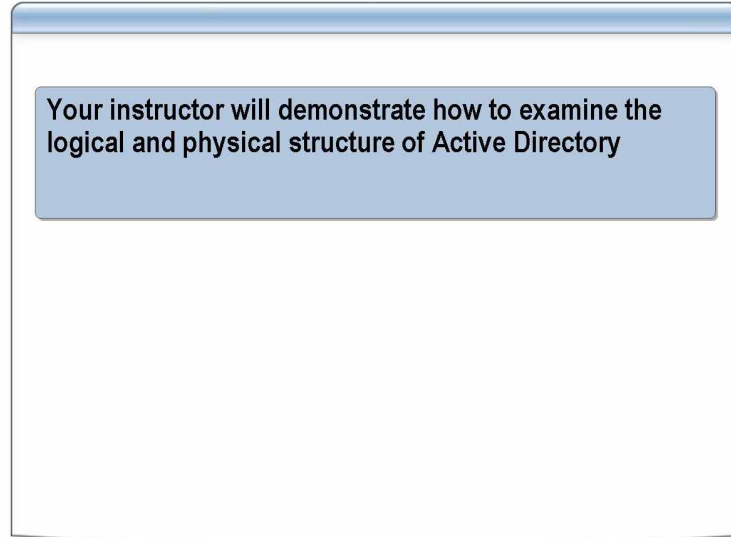
**Windows Script Host**

Although Windows Server 2003 provides a number of snap-ins and command-line tools to manage Active Directory, they are not suited to doing batch operations to perform changes in Active Directory that involve complex conditions. In such cases, you can make changes more quickly by using scripts. For example, you can change the first digit of the telephone extension number from 3 to 5 and from 4 to 5 for all employees who had moved to building 5. You can create Windows Script Host scripts that use ADSI to perform the following tasks:

- Retrieve information about Active Directory objects
- Add objects to Active Directory
- Modify attribute values for Active Directory objects
- Delete objects from Active Directory
- Extend the Active Directory schema

ADSI uses the LDAP protocol to communicate with Active Directory.

## How to Examine Active Directory



---

### Introduction

You can view the logical and physical structure of Active Directory by using Active Directory Users and Computers, Active Directory Sites and Services, and Active Directory Domains and Trusts.

### Procedure

To view the Active Directory logical and physical structure, perform the following steps:

1. Open Active Directory Users and Computers and view the organizational units in Active Directory. To do so, perform the following steps:
  - a. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
  - b. In the console tree, expand **Active Directory Users and Computers**.
  - c. In the console tree, expand the domain for which you want to view the organizational units.
  - d. Display the **Properties** page for each container in the console tree.
  - e. Determine the object type by using the Object class information on the **Object** tab. The Object class for organizational units is *Organizational Unit*.
2. Open Active Directory Domains and Trusts to view the logical structure of Active Directory. To do so, perform the following steps:
  - a. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Domains and Trusts**.
  - b. In the left pane, expand the node that represents the forest-root domain to view the domains that make up the logical structure of Active Directory.

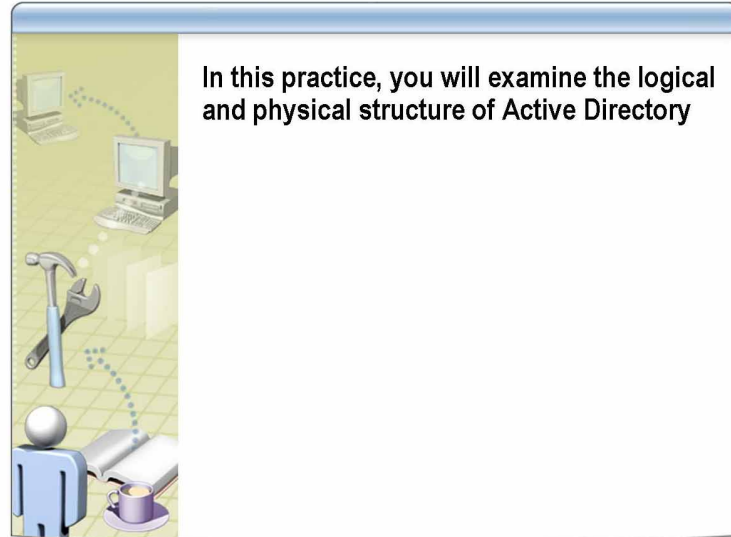
3. Open Active Directory Sites and Services and view the physical structure of Active Directory. To do so, perform the following steps:
  - a. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Sites and Services**.
  - b. In the console tree, expand **Sites**, and then expand the folder that represents the site for which you want to view a list of servers.
  - c. Click **Servers** to view a list of servers in the right pane.

---

**Note** For more information about examining Active Directory, see “How to Examine Active Directory” in Module 1 in the Appendices on the Student Materials compact disc.

---

## Practice: Examining the Active Directory Structure



---

### Objectives

In this practice, you will examine the logical and physical structure of Active Directory.

### Scenario

Today is your first day as a systems engineer at Northwind Traders. Your manager has asked you to study the logical and physical structure of Active Directory at Northwind Traders.

### Practice

► **Examine the default structure of Active Directory objects by using Active Directory Users and Computers**

1. Log on as `nwtraders\ComputerNameUser` with a password of `P@ssw0rd`
2. Install the Windows Server 2003 Administration Tools Pack. To do so, perform the following steps:
  - a. Click **Start**, right-click **Command Prompt**, and then click **Run as**.
  - b. In the **Run As** dialog box, click **The following user**, type a user name of `nwtraders\administrator` and a password of `P@ssw0rd` and then click **OK**.
  - c. At the command prompt, type `\\London\OS\i386\Adminpak.msi` and then press ENTER.
  - d. In the **File Download** dialog box, click **Open**, and then complete the installation.
  - e. Close the command prompt window.
3. Open Active Directory Users and Computers.
4. Enable Advanced Features.

- 
5. Expand **nwtraders.msft**, and locate the Locations object. What is the object type?

---

---

6. Expand **Locations**. What are the object types in the folder?

---

---

7. The objects in the Locations folder represent geographical locations in an organization. Each location contains three objects. What is the purpose for these objects?

---

---

8. Open any of the containers that represent a location, and then open the Users container.

What do you observe about the objects that are located in this container?

---

► **Examine the default structure of Active Directory by using Active Directory Sites and Services**

1. Open Active Directory Sites and Services.
2. Expand **Sites**, right-click **Default-First-Site-Name**, and then click **Properties**.

3. On the **Security** tab, view the permissions for the Domain Admins group. What are the permissions?

---

---

4. View the permissions that are assigned to the Domain Admins group for the **Default-First-Site-Name \Servers\London** object. What do you observe?

---

---

► **Examine the default structure of Active Directory by using Active Directory Domains and Trusts**

1. Open Active Directory Domains and Trusts.
2. Expand **nwtraders.msft**, and then view the properties for nwtraders.msft. What do you observe?

---

3. Choose to manage the corp.nwtraders.msft domain. What do you notice happens?

---

# Lesson: The Active Directory Design, Planning, and Implementation Processes

- Overview of Active Directory Design, Planning, and Implementation
- The Active Directory Design Process
- The Active Directory Planning Process
- The Active Directory Implementation Process

---

## Introduction

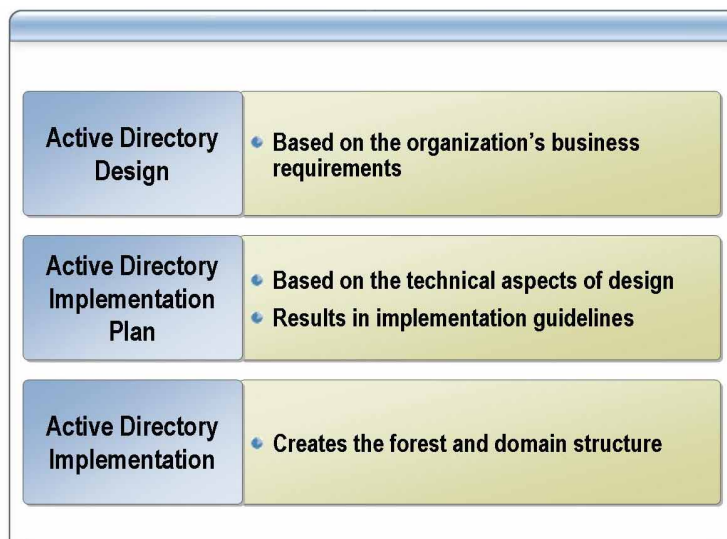
This lesson provides an overview of the Active Directory design, planning, and implementation processes.

## Lesson objective

After completing this lesson, you will be able to:

- Differentiate between Active Directory design, planning, and implementation.
- Describe the phases of the Active Directory design process.
- Describe the phases of the Active Directory planning process.
- Describe the phases of the Active Directory implementation process.

## Overview of Active Directory Design, Planning, and Implementation



### Introduction

The implementation of Active Directory begins with the creation of the Active Directory design. You use the design to plan the implementation of Active Directory and then implement Active Directory.

### Active Directory design

One or more systems architects create the Active Directory design, based on the business requirements of an organization. These business requirements determine the functional specifications for the design.

### Active Directory implementation plan

The Active Directory implementation plan determines how the Active Directory design is implemented based on the hardware infrastructure of the organization. For example, the Active Directory design may specify the number of domain controllers for each domain on the basis of a specific server configuration. However, if this configuration is not available, in the planning phase, you may decide to alter the number of servers to meet the business requirements of the organization.

After you implement Active Directory, you must manage and maintain it to ensure availability, reliability, and network security. This course describes the planning and implementation phases. The detailed design of Active Directory is beyond the scope of this course.

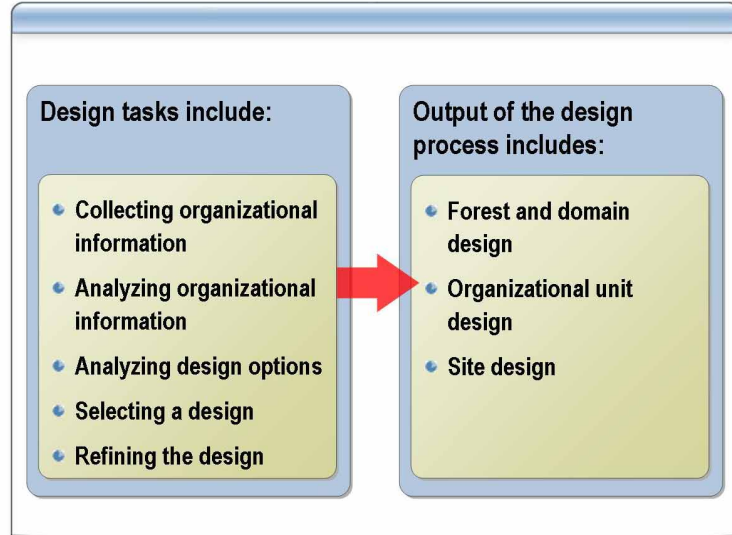
### Active Directory implementation

During deployment of Active Directory, systems engineers:

- Create the forest and domain structure and deploy the servers.
- Create the organizational unit structure.
- Create the user and computer accounts.
- Create the security and distribution groups.
- Create Group Policy objects (GPOs) and apply them to domains, sites, and organizational units.
- Create software distribution policies.



## The Active Directory Design Process



### Introduction

An Active Directory design includes several tasks, each of which defines the functional requirements for a component of an Active Directory implementation.

### Tasks in the Active Directory Design process

The Active Directory design process includes the following tasks:

- *Collecting organizational information.* This first task defines the need for the directory service and the business requirements for the project. Examples of organizational information include a high-level organizational profile, geographic locations of the organization, technical and network infrastructure, and plans for change in the organization.
- *Analyzing organizational information.* You analyze the collected information to assess its relevance and value to the design process. You determine the most important information and which components of the Active Directory design the information will affect. Be prepared to apply that information throughout the design process.
- *Analyzing design options.* When you analyze specific business requirements, several design options may satisfy the business requirements. For example, an administrative requirement may be met with either a domain design or an organizational unit structure. Each choice that you make affects the other components of the design, so stay flexible in your approach to the design throughout the entire process.

- *Selecting a design.* Develop several Active Directory designs and then compare their strengths and weaknesses. When you select a design, examine conflicting business requirements and consider their effects on your design choices. There may not be a clear winner among the design choices. Choose the design that meets most of your business requirements and presents the best overall choice.
- *Refining the design.* The first version of your design plan is likely to change before the pilot phase of the implementation. The design process is iterative because you must consider so many variables when you design an Active Directory infrastructure. Review and refine each design concept several times to accommodate all of the business requirements.

### Output of the Active Directory Design process

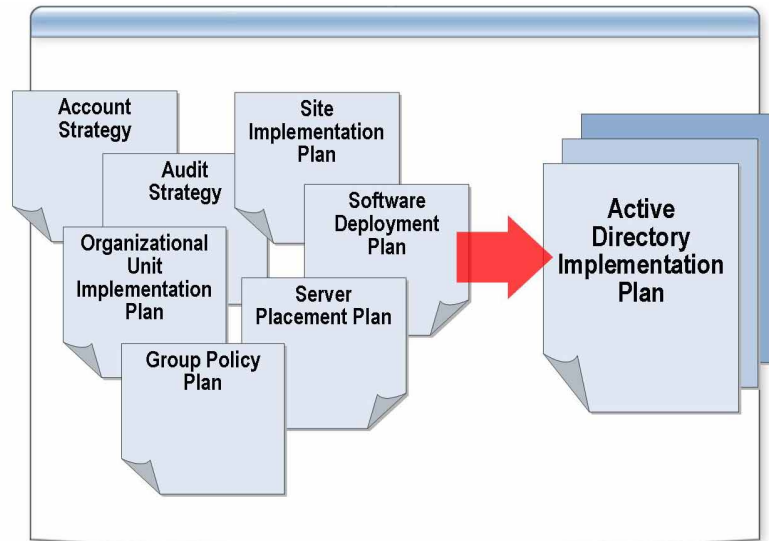
The output of the Active Directory design phase includes the following elements:

- *The forest and domain design.* The forest design includes information such as the number of forests required, the guidelines for creating trusts, and the fully qualified domain name (FQDN) for the forest root domain for each forest. The design also includes the forest change control policy, which identifies the ownership and approval processes for configuration changes that have a forest-wide impact. Identify who is responsible for determining the forest change control policy for each forest in the organization. If multiple forests are in your design plan, you can assess if forest trusts are necessary to share network resources across forests.

The domain design indicates the number of domains required in each forest, which domain will be the forest root domain for each forest, and the domain hierarchy if there are multiple domains in the design. The domain design also includes the DNS name for each domain and any trust relationships between domains.

- *The organizational unit design.* Specifies how you will create the organizational units for each domain in the forest. Include a description of the administrative authority that will apply to each organizational unit and to whom that administrative authority will be delegated. Finally, include the strategy for applying Group Policy to the organizational unit structure.
- *The site design.* Specifies the number and location of sites in the organization, the necessary site links, and the cost of the links.

## The Active Directory Planning Process



### Introduction

The output of the planning process is the Active Directory implementation plan. This plan consists of several plans that define the functional requirements for a specific component of an Active Directory implementation.

### Components of an Active Directory plan

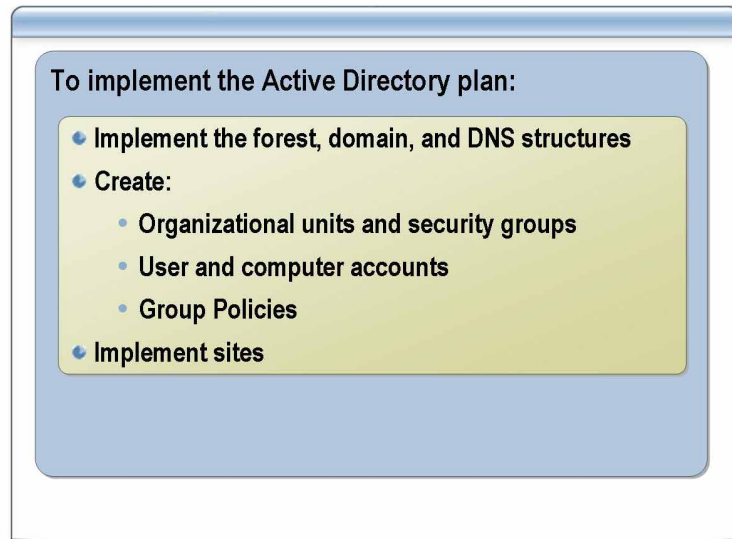
An Active Directory plan includes the following components:

- *Account strategy*. Includes information, such as the guidelines for account naming and lockout policy, the password policy, and the guidelines for setting security on objects.
- *Audit strategy*. Determines how to monitor modifications to Active Directory objects.
- *Organizational unit implementation plan*. Defines how and which organizational units to create. For example, if the organizational unit design specifies that organizational units will be created geographically and organized by business unit within each geographical area, the organizational unit implementation plan defines the organizational units to implement, such as sales, human resources, and production. The plan also provides guidelines for the delegation of authority.
- *Group Policy plan*. Determines who creates, links, and manages Group Policy objects, and how Group Policy will be implemented.
- *Site plan*. Specifies the sites, site links, and the link schedule. It also specifies the replication schedule and interval and the guidelines for securing and configuring the replication between sites.

- *Software deployment plan.* Specifies how you will use Group Policy to deploy new software and upgrades to software. For example, it can specify whether software upgrades are mandatory or optional.
- *Server placement plan.* Specifies the placement of domain controllers, global catalog servers, Active Directory-integrated DNS servers, and operations masters. It also specifies whether you will enable universal group membership caching for sites that do not have a global catalog server.

After each component plan is complete, you combine them to form the complete Active Directory implementation plan.

## The Active Directory Implementation Process



### Introduction

After the Active Directory implementation plan is in place, you can begin to implement Active Directory in accordance with your design plan.

### The implementation process

You perform the following tasks when you implement Active Directory:

- *Implement the forest, domain, and DNS structure.* Create the forest root domain, domain trees, and any child domains that make up the forest and domain hierarchy.
- *Create organizational units and security groups.* Create the organizational unit structure for each domain in each forest, create security groups, and delegate administrative authority to administrative groups in each organizational unit.
- *Create user and computer accounts.* Import user accounts into Active Directory.
- *Create Group Policy objects.* Create GPOs based on the Group Policy strategy, and then link them to sites, domains, or organizational units.
- *Implement sites.* Create sites according to the site plan, create site links, set site link schedules, and deploy domain controllers, global catalog servers, DNS servers, and operations masters in sites.

