Microsoft®
Training &
Certification

Module 1: Introduction to Active Directory in Windows 2000

Contents

Microsoft®

Overview

- Introduction to Active Directory
- Active Directory Logical Structure
- Active Directory Physical Structure
- Methods for Administering a Windows 2000 Network

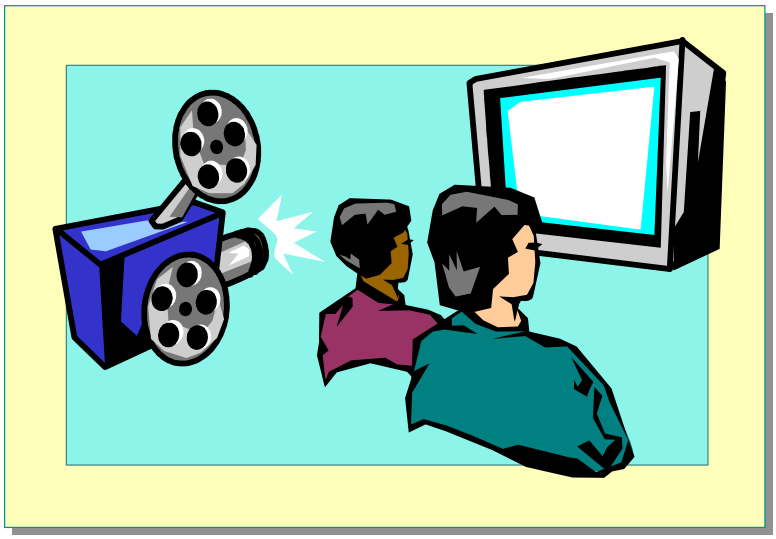
In a Microsoft® Windows® 2000 network, the Active Directory® directory service provides the structure and functions for organizing, managing, and controlling network resources. To implement and administer a Windows 2000 network, you must understand the purpose and structure of Active Directory.

Active Directory also provides the capability to centrally manage your Windows 2000 network. This capability means that you can centrally store information about the enterprise and administrators can manage the network from a single location. Active Directory supports the delegation of administrative control over Active Directory objects. This delegation enables administrators to assign specific administrative permissions for objects, such as user or computer accounts, to other users and administrators.

At the end of this module, 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 methods for administering a Windows 2000 network.

Multimedia: Concepts of Active Directory in Windows 2000



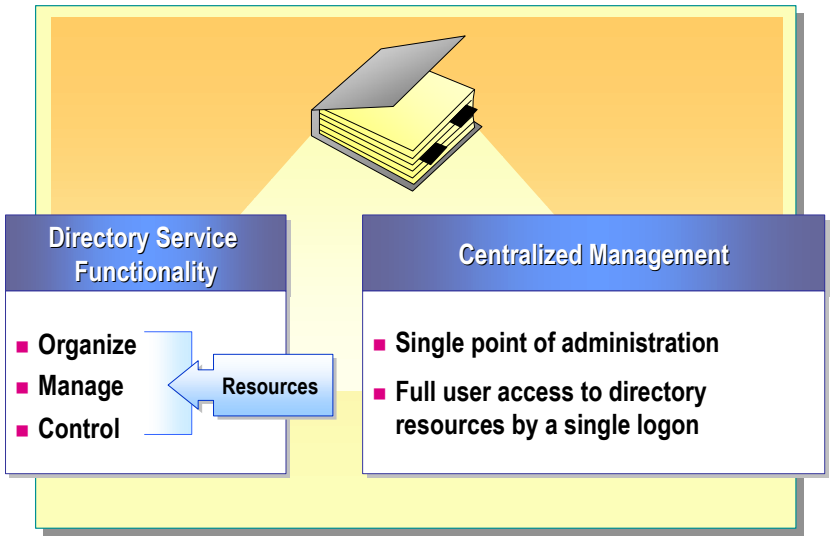
This multimedia presentation describes basic Active Directory concepts, such as organizational units (OUs), trees, forests, DNS naming conventions, and sites.

Introduction to Active Directory

- What Is Active Directory?
- Active Directory Objects
- Active Directory Schema
- Lightweight Directory Access Protocol (LDAP)

Active Directory stores information about resources on the entire network and makes it easy for users to locate, manage, and use these resources. Active Directory is made up of multiple components. You should understand the components and how to use them to administer Active Directory.

What Is Active Directory?



Active Directory is the directory service in a Windows 2000 network. A *directory service* is a network service that stores information about network resources and makes the resources accessible to users and applications. Directory services provide a consistent way to name, describe, locate, access, manage, and secure information about these resources.

Directory Service Functionality

Active Directory provides directory service functionality, including a means of centrally organizing, managing, and controlling access to network resources. Active Directory makes the physical network topology and protocols transparent so that a user on a network can gain access to any resource without knowing where the resource is or how it is physically connected to the network. An example of this type of resource would be a printer.

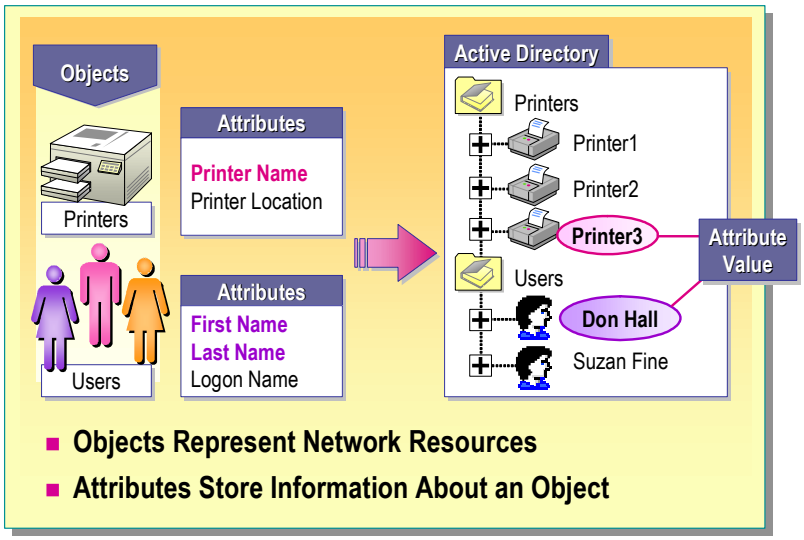
Active Directory is organized into sections that permit storage for a very large number of objects. As a result, Active Directory can expand as an organization grows, so that an organization that has a single server with a few hundred objects can grow to having thousands of servers and millions of objects.

Centralized Management

A server running Windows 2000 stores system configuration, user profiles, and application information in Active Directory. Combined with Group Policy, Active Directory enables administrators to manage distributed desktops, network services, and applications from a central location while using a consistent management interface.

Active Directory also provides centralized control of access to network resources by allowing users to log on only once to gain full access to resources throughout Active Directory.

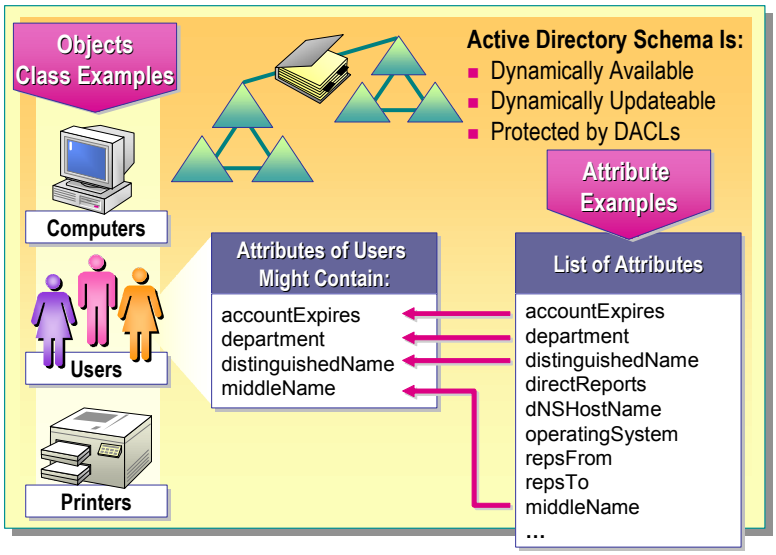
Active Directory Objects



Active Directory stores information about network objects. Active Directory *objects* represent network resources, such as users, groups, computers, and printers. Moreover, all servers, domains, and sites in the network are also represented as objects. Because Active Directory represents all network resources as objects in a distributed database, a single administrator can centrally manage and administer these resources.

When you create an object, the properties, or *attributes* of that object store the information that describes the object. Users can locate objects throughout Active Directory by searching for specific attributes. For example, a user can locate a printer in a specific building by searching the Location attribute of the printer object class.

Active Directory Schema



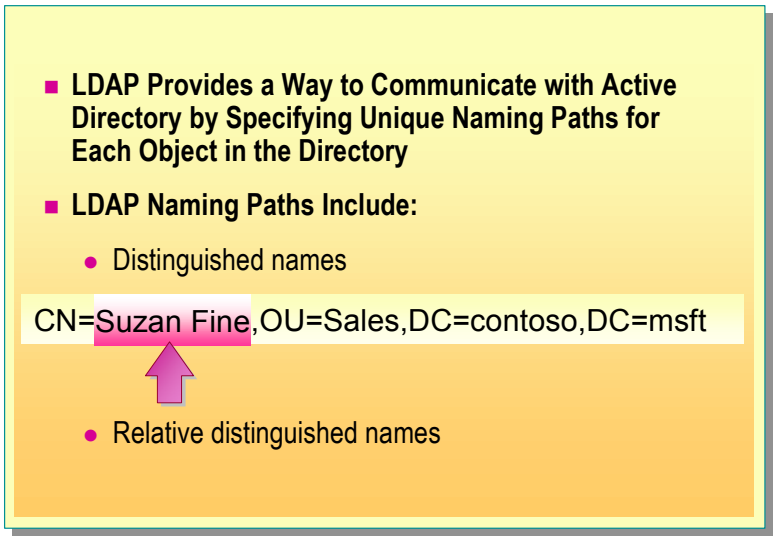
The Active Directory *schema* contains the definitions of all objects, such as computers, users, and printers that are stored in Active Directory. In Windows 2000, there is only one schema for an entire forest, so that all objects created in Active Directory conform to the same rules.

The two types of definitions in the schema are object classes and attributes. *Object classes* describe the possible directory objects that can be created. 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.

The Active Directory database stores the schema. Storing the schema in a database means that the schema:

- Is dynamically available to user applications, which means that user applications can read the schema to discover which objects and properties are available for use.
- Is dynamically updateable, which enables an application to extend the schema with new attributes and object classes, and then use these schema extensions immediately.
- Can use discretionary access control lists (DACLs) to protect all object classes and attributes. The use of DACLs allows only authorized users to make schema changes.

Lightweight Directory Access Protocol (LDAP)



Lightweight Directory Access Protocol (LDAP) is a directory service protocol that is used to query and update Active Directory. The protocol specification for LDAP specifies that an Active Directory object be represented by a series of domain components, OUs, and common names, which creates an LDAP naming path within Active Directory. LDAP naming paths are used to access Active Directory objects and include the following:

- Distinguished names
- Relative distinguished names

Distinguished Name

Every object in Active Directory has a distinguished name. The *distinguished name* identifies the domain where the object is located, and the complete path by which the object is reached. An example of a typical distinguished name is:

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

Key	Attribute	Description
DC	Domain Component	A component of the DNS name of the domain, such as com.
OU	Organizational Unit	An organizational unit that can be used to contain other objects.
CN	Common Name	Any object other than domain components and organizational units, such as user and computer objects.

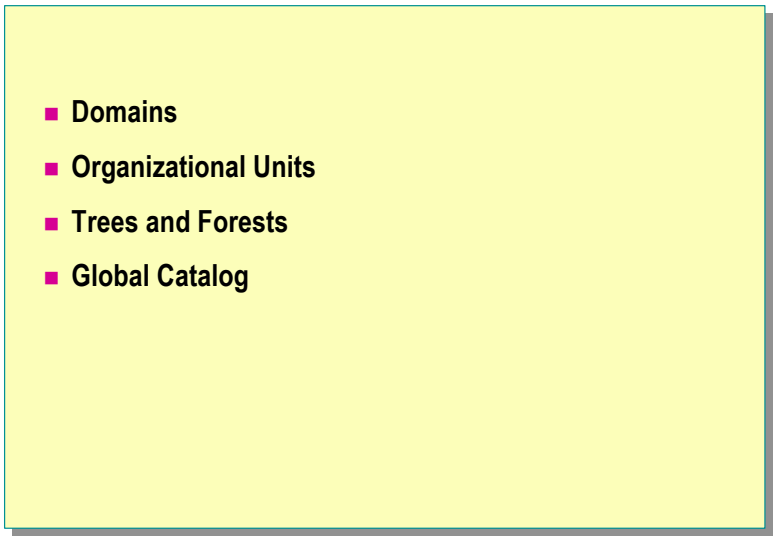
Relative Distinguished Name

The LDAP *relative distinguished name* is the portion of the LDAP distinguished name that uniquely identifies the object in its container. Its composition varies depending upon the extent of the existing search context established by the client. The search context may vary from the domain component level to the common name level. In the preceding example, the relative distinguished name of the Suzan Fine user object is Suzan Fine.

The following table provides examples of distinguished names, the search context established by the client, and relative distinguished names.

Distinguished name	Relative distinguished name
OU=Sales,DC=contoso,DC=msft	OU=Sales
CN=Suzan Fine,OU=Sales,DC=contoso, DC=msft	CN=Suzan Fine
CN=Judy Lew,OU=Shipping, DC=europe,DC=contoso,DC=msft	CN=Judy Lew

Active Directory Logical Structure

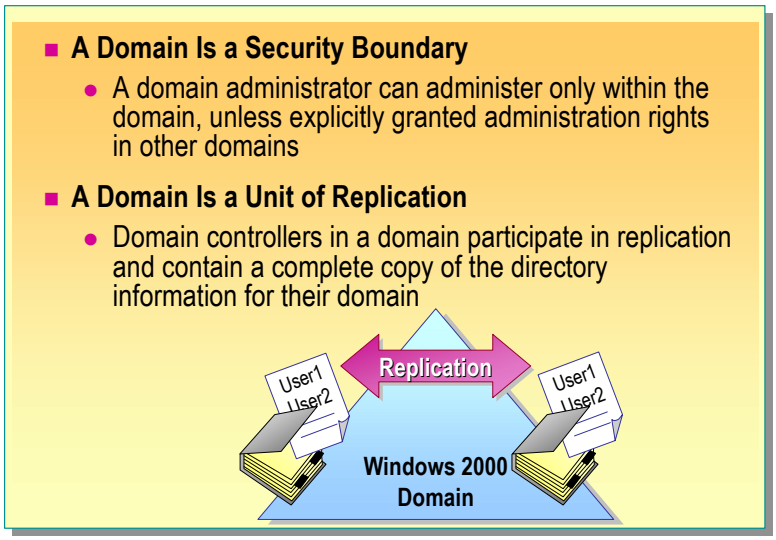


The logical structure of Active Directory is flexible and provides a method for designing a hierarchy within Active Directory,which is comprehensible to both users and administrators. The logical components of the Active Directory structure include:

- Domains
- Organizational units
- Trees and forests
- Global catalog

You should understand the purpose and function of the logical components of the Active Directory structure so that you can complete a variety of tasks, including installing, configuring, administering, and troubleshooting Active Directory.

Domains



The core unit of the logical structure in Active Directory is the domain. A *domain* is a collection of computers, defined by an administrator, which share a common directory database. A domain has a unique name and provides access to the centralized user accounts and group accounts maintained by the domain administrator.

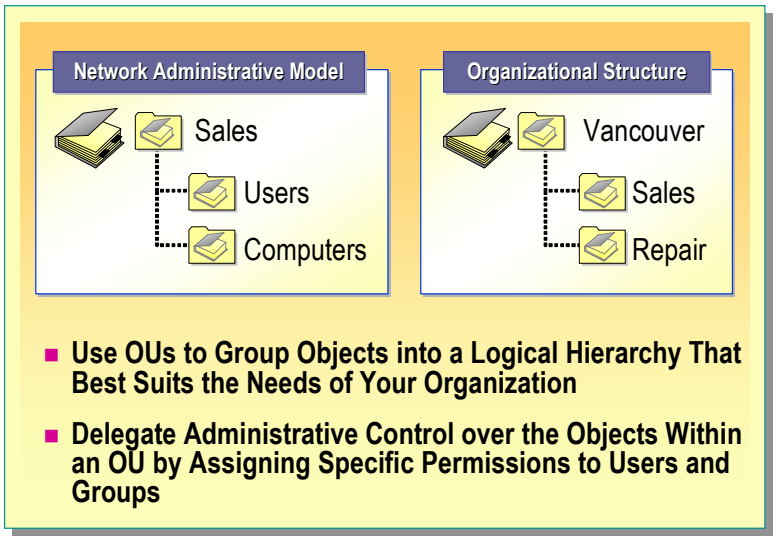
Security Boundary

In a Windows 2000 network, the domain serves as a *security boundary*. The purpose of a security boundary is to ensure that an administrator of a domain has the necessary permissions and rights to perform administration only within that domain, unless the administrator is explicitly granted these rights in another domain too. Every domain has its own security policies and security relationships with other domains.

Unit of Replication

Domains are also units of replication. In a domain, computers called *domain controllers* contain a replica of Active Directory. All of the domain controllers in a particular domain can receive changes to information in Active Directory and replicate these changes to all of the other domain controllers in the domain.

Organizational Units



An *organizational unit* (OU) is a container object that you use to organize objects within a domain. An OU may contain objects, such as user accounts, groups, computers, printers, and other OUs.

OU Hierarchy

You can use OUs to group objects into a logical hierarchy that best suits the needs of your organization. For example, you can create an OU hierarchy to represent the following for an organization:

- Network administrative model based on administrative responsibilities. For example, an organization might have one administrator who is responsible for all of the user accounts and another who is responsible for all of the computers. In this case, you would create one OU for users and another OU for computers.
- Organizational structure based on departmental or geographical boundaries.

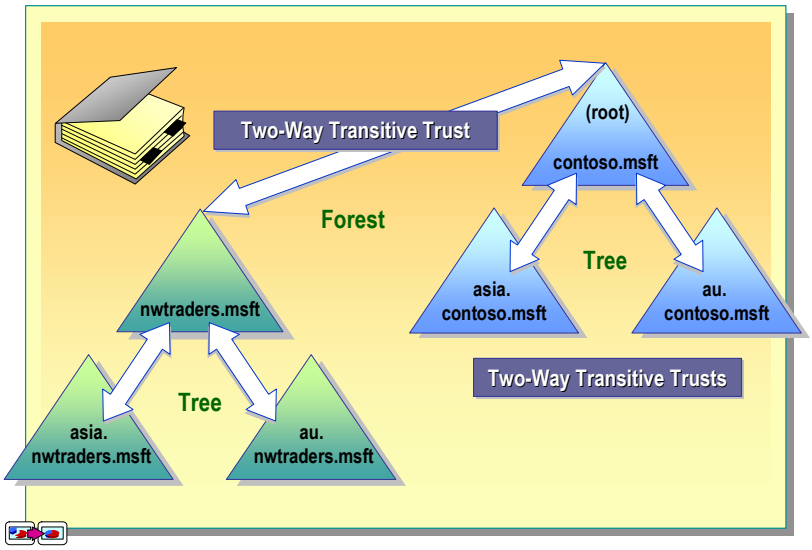
The OU hierarchy within a domain is independent of the OU hierarchy structure of other domains—each domain can implement its own OU hierarchy.

Administrative Control of OUs

You can delegate administrative control over the objects within an OU. To delegate administrative control of an OU, you assign specific permissions for the OU and the objects that the OU contains to one or more users and groups.

For an OU, you can assign either complete administrative control, such as full control over all objects in the OU, or limited administrative control, such as the ability to modify e-mail information on user objects in the OU.

Trees and Forests



The first Windows 2000 domain that you create is called the *forest root domain*. Additional domains are added to the root domain to form the tree structure or the forest structure, depending on the domain name requirements.

Trees

A *tree* is a hierarchical arrangement of Windows 2000 domains that share a contiguous namespace.

When you add a domain to an existing tree, the new domain is a child domain of an existing parent domain. The name of the child domain is combined with the name of the parent domain to form its DNS name. Every child domain has a two-way, transitive trust relationship with its parent domain.

Two-Way, Transitive Trusts

Two-way, transitive trust relationships are the default trust relationships between Windows 2000 domains. A two-way, transitive trust is a combination of a transitive trust and a two-way trust.

A *transitive trust* means that the trust relationship extended to one domain is automatically extended to all other domains that trust that domain. For example, domain au.contoso.msft directly trusts contoso.msft. Domain asia.contoso.msft also directly trusts contoso.msft. Because both trusts are transitive, au.contoso.msft indirectly trusts asia.contoso.msft.

A *two-way trust* means that there are two trust paths going in opposite directions between two domains. For example, domain au.contoso.msft trusts contoso.msft in one direction, and contoso.msft trusts au.contoso.msft in the opposite direction.

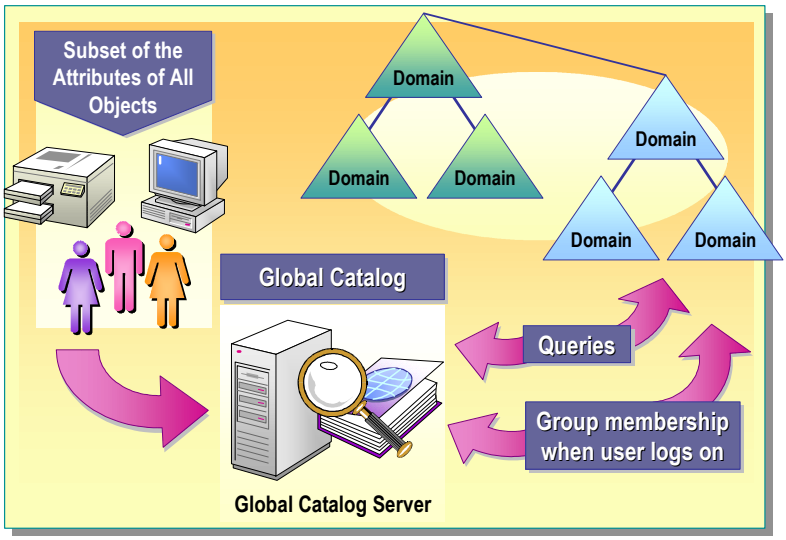
The advantage of two-way, transitive trusts in Windows 2000 domains is that there is complete trust between all domains in an Active Directory domain hierarchy. Trees linked by trust relationships form a forest.

Forests

A *forest* is one or more trees. The trees in a forest do not share a contiguous namespace. However, the trees in a forest share a common schema and global catalog. A single tree that is related to no other trees constitutes a forest of one tree. Thus, every tree root domain has a transitive trust relationship with the forest root domain. The name of the forest root domain is used to refer to a given forest.

Each tree in a forest has its own unique namespace. For example, Contoso, Ltd. creates a separate organization called Northwind Traders. Contoso, Ltd. decides to create a new Active Directory domain name for Northwind Traders, called nwtraders.msft. Although the two organizations do not share a common namespace, adding the new Active Directory domain as a new tree in an existing forest allows the two organizations to share resources and administrative functions.

Global Catalog



The *global catalog* is a repository of information that contains a subset of the attributes of all objects in Active Directory. By default, the attributes that are stored in the global catalog are those that are most frequently used in queries, such as a user's first name, last name, and logon name. The global catalog contains the information that is necessary to determine the location of any object in the directory.

The global catalog enables users to perform two important functions:

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

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

The global catalog makes the directory structure within a forest transparent to users who perform a search. 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.

The global catalog also contains the access permissions for each object and attribute stored in the global catalog. If you are searching for an object and you do not have the appropriate permissions to view the object, you will not see the object in the list of search results. This ensures that users can find only objects to which they have been assigned access.

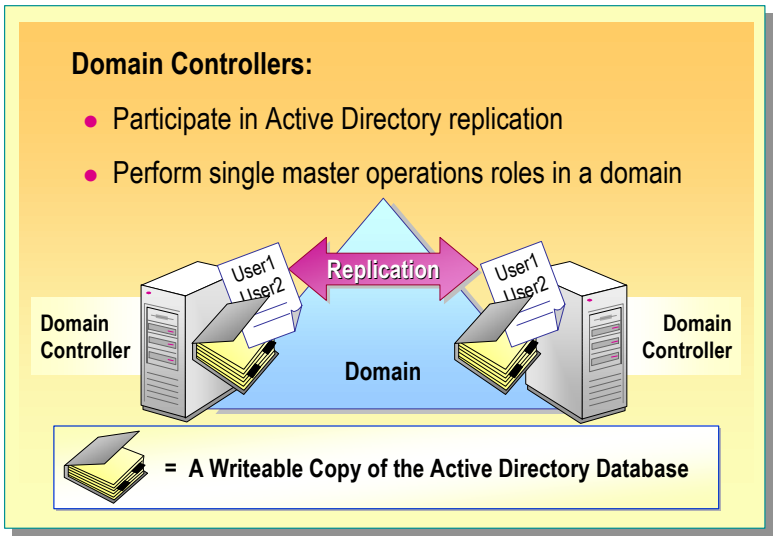
Active Directory Physical Structure

- Domain Controllers
- Sites

In Active Directory, the logical structure is separate and distinct from the physical structure. You use the logical structure to organize your network resources, and you use the physical structure to configure and manage your network traffic. Domain controllers and sites make up the physical structure of Active Directory.

The physical structure of Active Directory defines where and when replication and logon traffic occur. Understanding the physical components of Active Directory is critical to optimizing network traffic and the logon process. Also, knowing the physical structure can help in troubleshooting replication and logon problems.

Domain Controllers



A *domain controller* is a computer running Windows 2000 Server that stores a replica of the directory. A domain controller also manages the changes to directory information and replicates these changes to other domain controllers in the same domain. Domain controllers store directory data and manage user logon processes, authentication, and directory searches.

A domain can have one or more domain controllers. A small organization that uses a single local area network (LAN) may need only one domain with two domain controllers to provide adequate availability and fault tolerance, whereas a large organization with many geographical locations needs one or more domain controllers in each location to provide adequate availability and fault tolerance.

Active Directory Replication

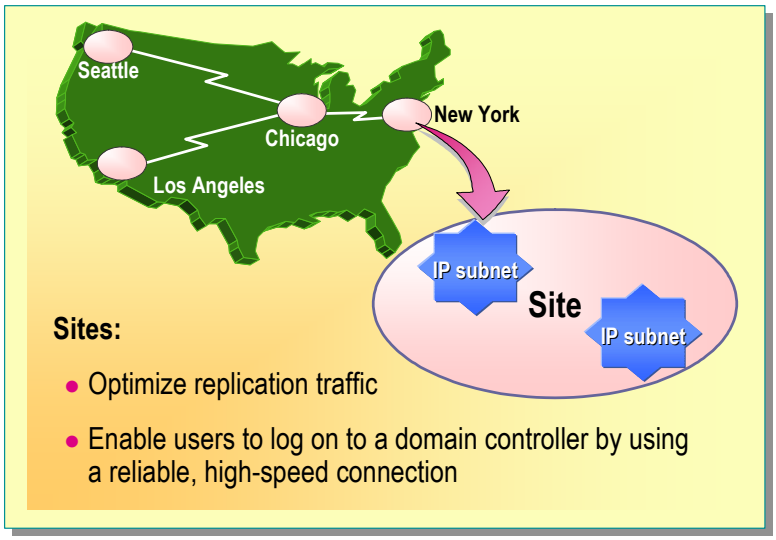
Domain controllers in a domain and in a forest automatically replicate any change to the Active Directory database to each other. Replication ensures that all of the information in Active Directory is available to all domain controllers and client computers across the entire network. The physical structure of Active Directory determines when and how replication occurs.

Active Directory uses a *multi-master replication model*. In a multi-master replication model, each Windows 2000 domain has one or more domain controllers. Each domain controller stores a writeable copy of the Active Directory database for its domain and manages the changes and updates to its copy of the directory. When a user or administrator performs an action that causes an update to the directory in one domain controller, that update is replicated to all domain controllers in the domain. However, domain controllers might hold different information for short periods of time until all of the domain controllers have synchronized their changes to Active Directory.

Single Master Operations

Some changes to Active Directory are impractical to perform using multi-master replication because of the potential for conflicts in essential operations. For these reasons, *single master operations* are assigned only to specific domain controllers. An operations master is a domain controller that has been assigned one or more single master operations roles in an Active Directory domain or forest. The domain controllers that are assigned these roles perform operations, such as adding or removing a domain from a forest, that are not permitted to simultaneously occur on different domain controllers in the network.

Sites



A *site* consists of one or more Internet Protocol (IP) subnets that are connected by a high-speed link. By defining sites, you can configure the access and replication topology for Active Directory so that Windows 2000 uses the most efficient links and schedules for replication and logon traffic.

You create sites for two primary reasons:

- To optimize replication traffic.
- To enable users to connect to a domain controller by using a reliable, high-speed connection.

Sites map the physical structure of your network, whereas domains map the logical structure of your organization. The logical and physical structures of Active Directory are independent of each other, which has the following consequences:

- There is no necessary correlation between the network's physical structure and its domain structure.
- Active Directory allows multiple domains in a single site, and multiple sites in a single domain.
- There is no necessary correlation between site and domain namespaces.

Note For more information about the logical and physical structures of Active Directory, see *Active Directory Architecture* under **Additional Reading** on the Web page on the Student Materials compact disc.

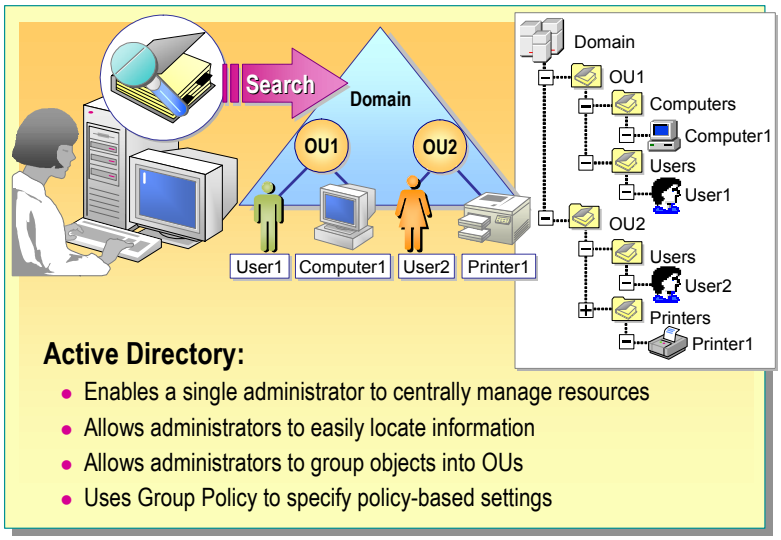
Methods for Administering a Windows 2000 Network

- Using Active Directory for Centralized Management
- Managing the User Environment
- Delegating Administrative Control

Windows 2000 and Active Directory provide administrators with the methods and utilities to centralize the management of all desktop computers in an organization and to decentralize administrative tasks. Administrators perform the following administrative tasks:

- Centralize management. Active Directory allows administrators to centrally manage large numbers of users, computers, printers, and network resources from a central location. Active Directory enables users to centrally organize network resources according to administrative requirements.
- Manage the user environment. Group Policy enables administrators to specify settings and apply management Group Policy settings to OUs in Active Directory. Moreover, Group Policy enables administrators to define a Group Policy for a user or computer once, and then use Windows 2000 to reinforce it continually.
- Delegate administrative control. Active Directory allows an administrator with the proper authority to delegate a selected set of administrative privileges to appropriate individuals or groups within an organization. This administrator can specify the privileges that these individuals have to manage different containers and objects in Active Directory. Windows 2000 also provides the tools to match administrative responsibilities and to delegate network administrative responsibilities to other administrators.

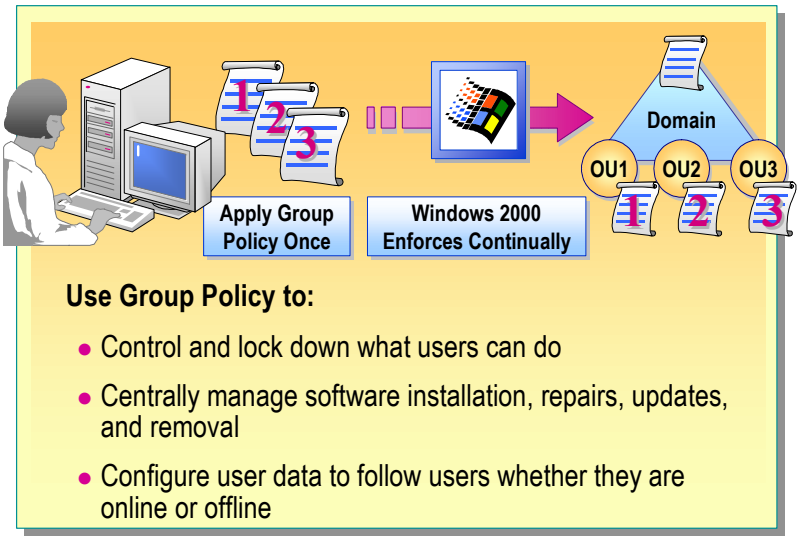
Using Active Directory for Centralized Management



Active Directory provides administrators with the capability to manage resources centrally. The advantages of managing resources centrally are:

- Active Directory enables a single administrator to centrally manage and administer network resources. Active Directory contains information about all objects and their attributes. The attributes hold data that describes the resource that the directory object identifies.
- Active Directory allows administrators to easily locate information about objects. By searching for selected attributes, you can find an object located anywhere in the Active Directory tree.
- Active Directory allows you to group objects with similar administrative and security requirements into OUs. OUs provide multiple levels of administrative authority for both applying Group Policy settings and delegating administrative control. This delegation of administrative authority simplifies the task of managing these objects and allows administrators to structure Active Directory to fit their needs.
- Active Directory uses Group Policy to provide administrators with the ability to specify Group Policy settings for a site, domain, or OU. Active Directory then enforces these Group Policy settings for all of the users and computers within the container.

Managing the User Environment



Group Policy in Windows 2000 enables policy-based centralized management of a network. Policy-based administration eases the management of even the most complex network by allowing you to apply a Group Policy to an object once, and then to rely on Windows 2000 to continually enforce the Group Policy throughout the network.

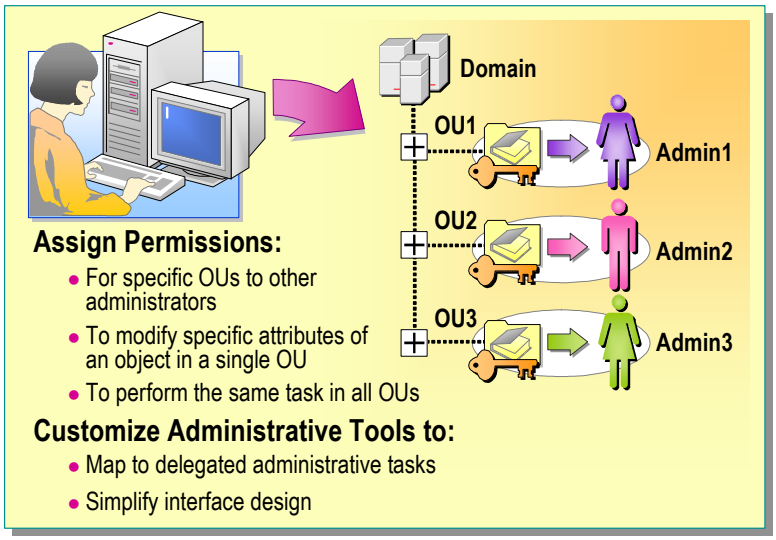
Group Policy utilizes Active Directory containers (sites, domains, and OUs) as administrative units. A Group Policy set on a container affects all users and computers that it contains. Windows 2000 applies Group Policy settings to users and computers when the computer starts or the user logs on. Group Policy provides settings for controlling computer services and users' desktop environments and capabilities. Group Policy allows you to control users' data, personal computer settings, computing environment, and software.

Group Policy settings that are associated with the user enable administrators to provide users with consistent access to all of the users' information and software, regardless of which computer they are working on.

You can use Group Policy to manage the user environment by:

- Controlling what users can do when logged on to the network, and locking down features that they should not access. This control ensures that users can gain access to the tools and information that they need but cannot gain access to anything that is not required for their jobs. You can also restrict the applications and tools that are available to users. Limiting the scope of what a user can do ensures that no unnecessary time is spent troubleshooting operating system and application configuration problems.
- Centrally managing the installation of applications, service packs, and operating system updates, and the repairs, updates, and removal of software. If you use Group Policy to install software, you can ensure that the same applications are available on any computer to which a user logs on. You can also ensure that missing files and settings are repaired automatically whenever an application is started.
- Configuring user data to *follow* users whether they are online, connected to the network, or temporarily offline. Following means that even though the user data is stored in specified network locations, it always appears as local to the user. Offline files cache network data to the local computers, so it is available when the user disconnects from the network.

Delegating Administrative Control



Windows 2000 enables you to delegate administrative privileges for certain objects to appropriate groups within an organization. This is possible because the structure of Active Directory allows you to assign permissions and grant user rights in very specific ways.

You can delegate the following types of administrative control:

- Assigning permissions, such as Full Control, for specific OUs to different domain local groups. Thus, three OUs could have three different domain local groups.
- Assigning the permissions to modify specific attributes of an object in a single OU. For example, assigning the permission to change name, address, and telephone number, and to reset passwords on a user account object.
- Assigning the permissions to perform the same task, such as resetting passwords, in all OUs of a domain.

Windows 2000 also provides you with the capability to customize administrative tools so that the tools match the administrative tasks that you delegate to other administrators. You can create customized administrative tools to:

- Map to the permissions that have been assigned to a user for an administrative task.
- Simplify interface design for users with limited administrative privileges.

You can also combine all of the tools needed for each administrative function into a single console.

Review

- Introduction to Active Directory
- Active Directory Logical Structure
- Active Directory Physical Structure
- Methods for Administering a Windows 2000 Network

1. What is the purpose of Active Directory in Windows 2000?

2. What are sites and domains, and how are they different from each other?

3. What are trees and forests, and how are they different from each other? What do they have in common?