Chaffey College
Chino Information Technology Center

CISNTWK-11

Microsoft Network Server

Chapter 4

Introduction to Active Directory and Account Manager

Chaffey College
Chino Information Technology Center

Objectives

- Understand Active Directory basic concepts
- Install and configure Active Directory
- Implement Active Directory containers

Objectives (continued)

- Create and manage user accounts
- Configure and use security groups
- Describe and implement new Active Directory features

Active Directory Basics

- Active Directory
  - Directory service that houses information about all network resources such as servers, printers, user accounts, groups of user accounts, security policies, and other information
- **Directory service**
  - Responsible for providing a central listing of resources and ways to quickly find and access specific resources and for providing a way to manage network resources

Active Directory Basics (continued)

- Windows Server 2008 uses Active Directory to manage accounts, groups, and many more network management services
- **Domain controllers (DCs)**
  - Servers that have the AD DS server role installed
  - Contain writable copies of information in Active Directory
- **Member servers**
  - Servers on a network managed by Active Directory that do not have Active Directory installed

Active Directory Basics (continued)

- Domain
  - Container that holds information about all network resources that are grouped within it
  - Every resource is called an **object**
- **Multimaster replication**
  - Each DC is equal to every other DC in that it contains the full range of information that composes Active Directory
- Active Directory is built to make replication efficient

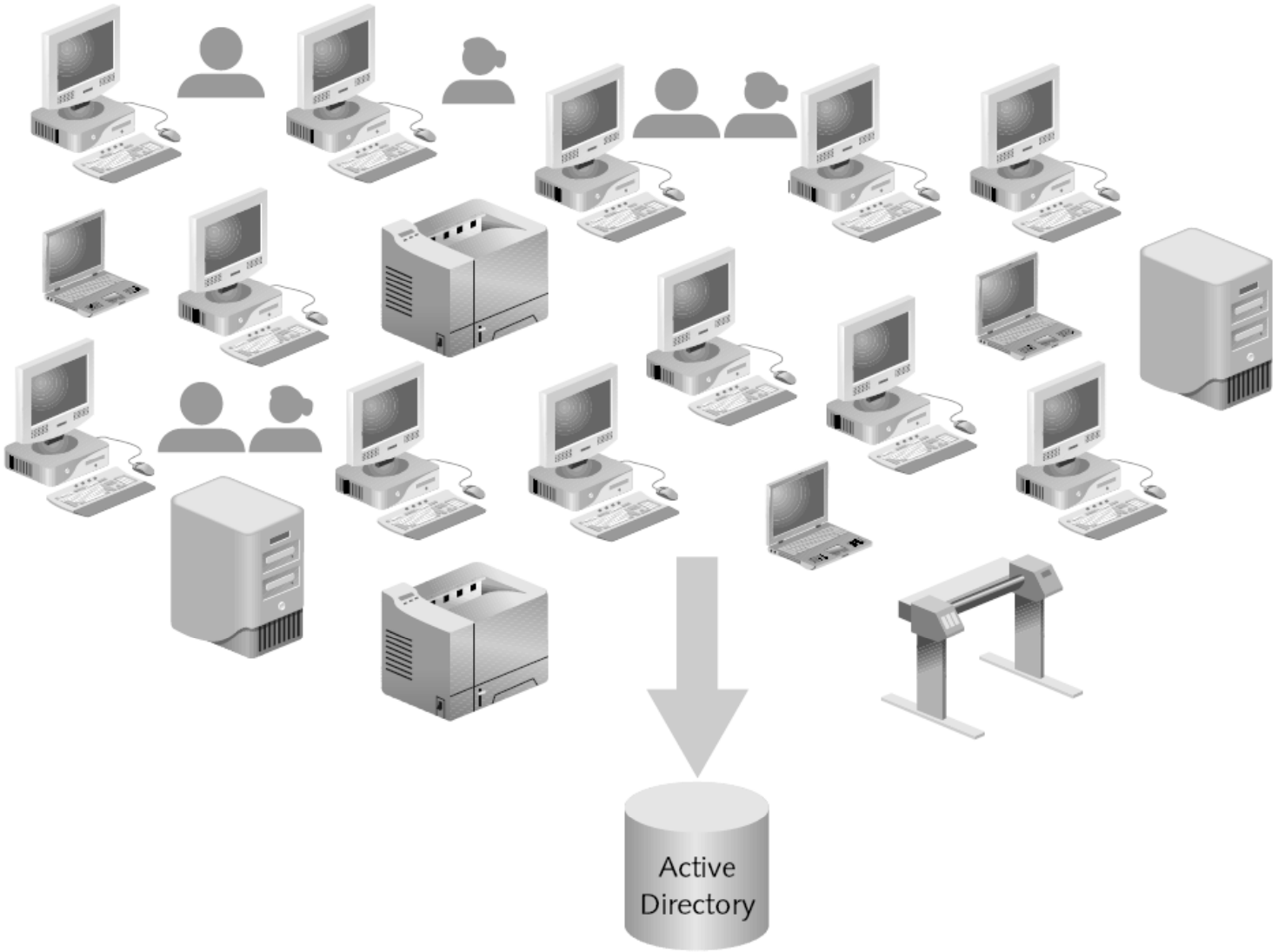

Figure 4-1 Active Directory domain objects include servers, workstations, printers, users, user groups, and other resources.

Active Directory Basics (continued)

- Activity 4-1: Installing Active Directory
  - Time Required: Approximately 20–30 minutes
  - Objective: Install Active Directory

Schema

- Active Directory **schema**
  - Defines the objects and the information pertaining to those objects that can be stored in Active Directory
- User account
  - One class of object in Active Directory that is defined through schema elements unique to that class

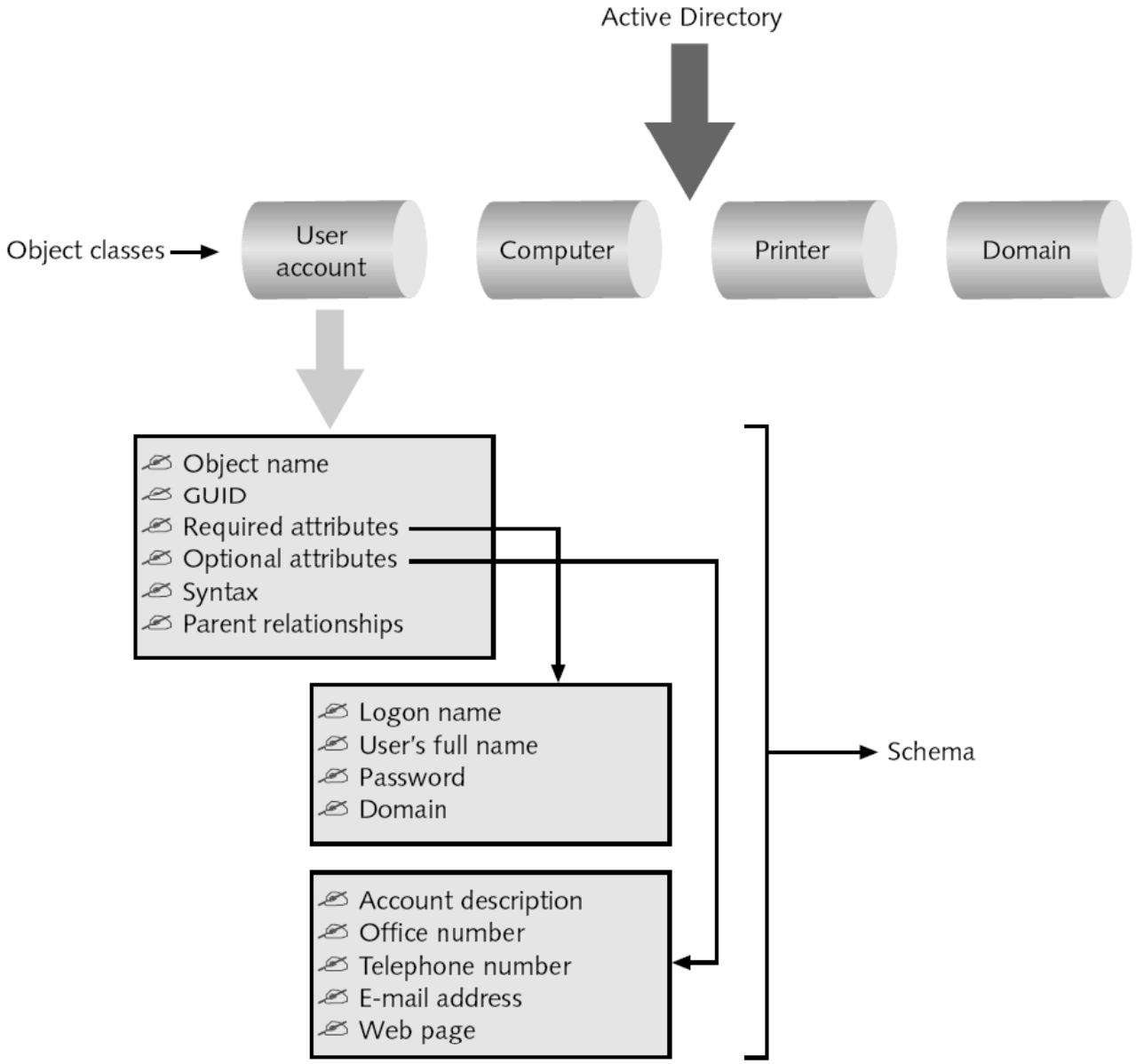

Figure 4-4 Sample schema information for user accounts

Global Catalog

- **Global catalog**
  - Stores information about every object within a forest
  - Store a full replica of every object within its own domain and a partial replica of each object within every domain in the forest
- The first DC configured in a forest becomes the global catalog server
- The global catalog server enables forest-wide searches of data

Global Catalog (continued)

- The global catalog serves the following purposes:
  - Authenticating users when they log on
  - Providing lookup and access to all resources in all domains
  - Providing replication of key Active Directory elements
  - Keeping a copy of the most used attributes for each object for quick access

Namespace

- Active Directory uses Domain Name System (DNS)
  - There must be a DNS server on the network that Active Directory can access
- **Namespace**
  - A logical area on a network that contains directory services and named objects
  - Has the ability to perform name resolution
- Active Directory depends on one or more DNS servers
- Active Directory employs two kinds of namespaces: contiguous and disjointed

Containers in Active Directory

- Active Directory has a treelike structure
- The hierarchical elements, or **containers**, of Active Directory include forests, trees, domains, organizational units (OUs), and sites

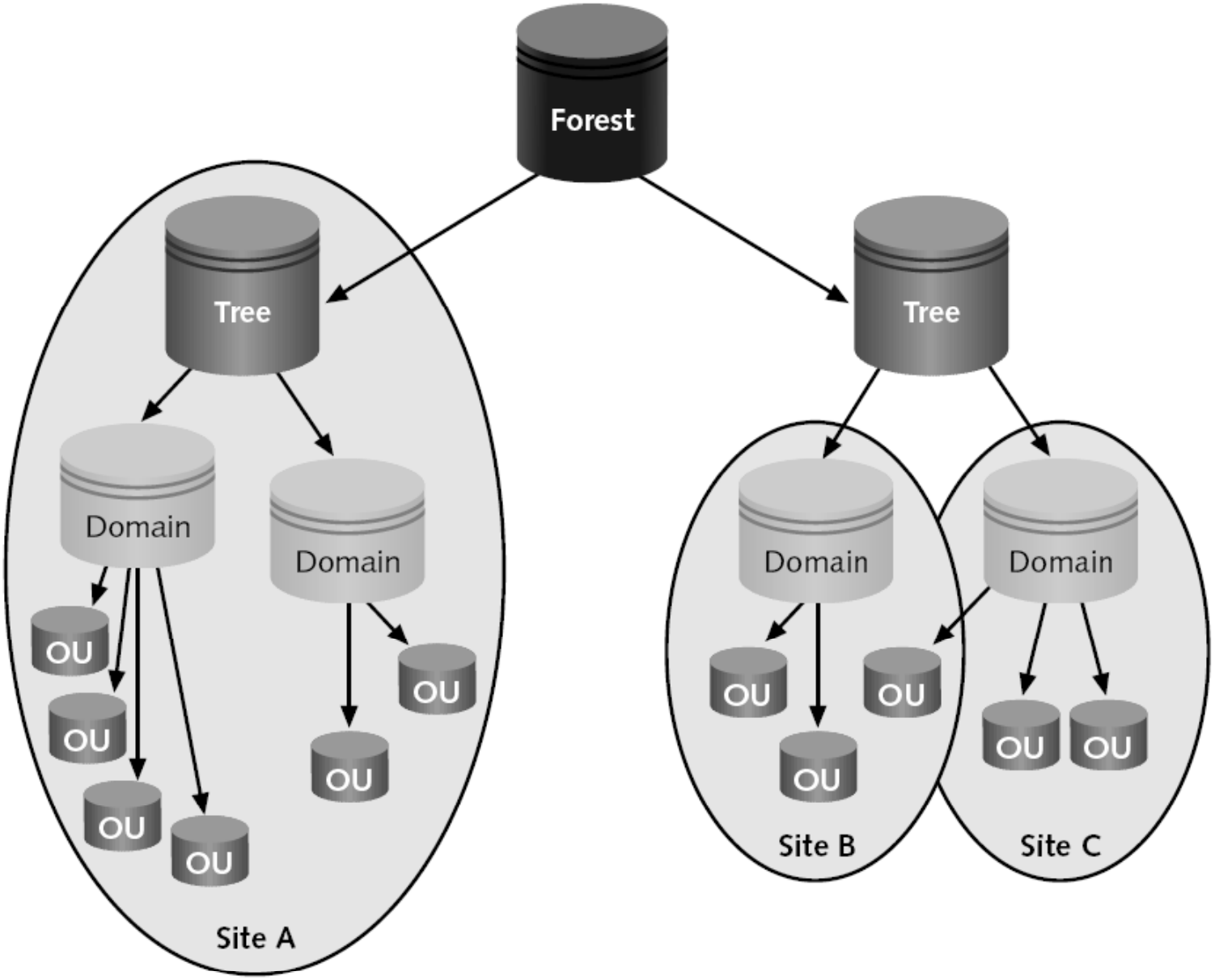

Figure 4-5 Active Directory hierarchical containers

Forest

- **Forest**
  - Consists of one or more Active Directory trees that are in a common relationship
- Forests have the following characteristics:
  - The trees can use a disjointed namespace
  - All trees use the same schema
  - All trees use the same global catalog
  - Domains enable administration of commonly associated objects, such as accounts and other resources, within a forest
  - Two-way transitive trusts are automatically configured between domains within a single forest

Forest (continued)

- Forest provides a means to relate trees that use a contiguous namespace in domains within each tree
  - But that have disjointed namespaces in relationship to each other
- The advantage of joining trees into a forest is that all domains share the same schema and global catalog
- **Forest functional level**
  - Refers to the Active Directory functions supported forest-wide

Forest (continued)

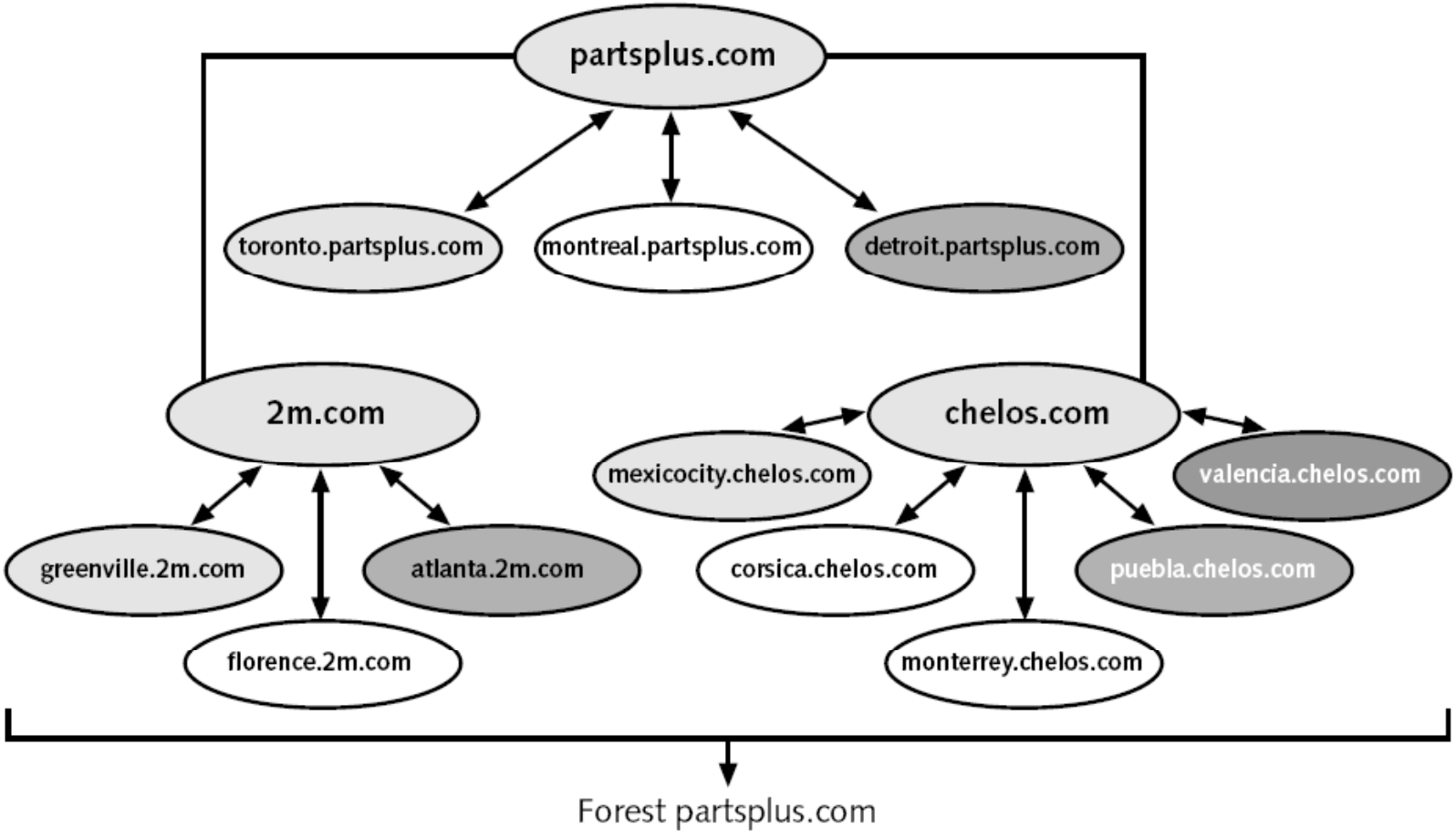

Figure 4-6 A forest

Forest (continued)

- Windows Server 2008 Active Directory recognizes three types of forest functional levels
  - Windows 2000 Native forest functional level
  - Windows Server 2003 forest functional level
  - Windows Server 2008 forest functional level

Tree

- **Tree**
  - Contains one or more domains that are in a common relationship
- Tree has the following characteristics:
  - Domains are represented in a contiguous namespace and can be in a hierarchy
  - Two-way trust relationships exist between parent domains and child domains
  - All domains in a single tree use the same schema for all types of common objects
  - All domains use the same global catalog

Tree (continued)

- The domains in a tree typically have a hierarchical structure
  - Such as a root domain at the top and other domains under the root
- The domains within a tree are in what is called a **Kerberos transitive trust relationship**
  - Which consists of **two-way trusts** between parent domains and child domains
- Because of the trust relationship between parent and child domains, any one domain can have access to the resources of all others

Tree (continued)

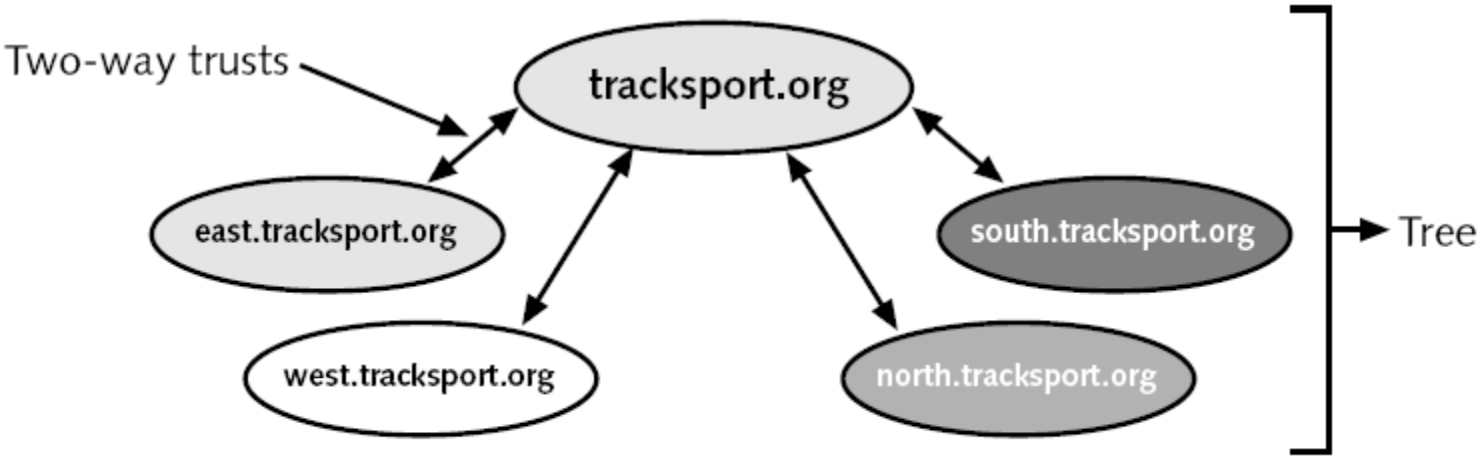

Figure 4-7 Tree with hierarchical domains

Domain

- Microsoft views a domain as a logical partition within an Active Directory forest
  - A domain is a grouping of objects that typically exists as a primary container within Active Directory
- The basic functions of a domain are as follows:
  - To provide an Active Directory ‘‘partition’’ in which to house objects that have a common relationship, particularly in terms of management and security
  - To establish a set of information to be replicated from one DC to another
  - To expedite management of a set of objects

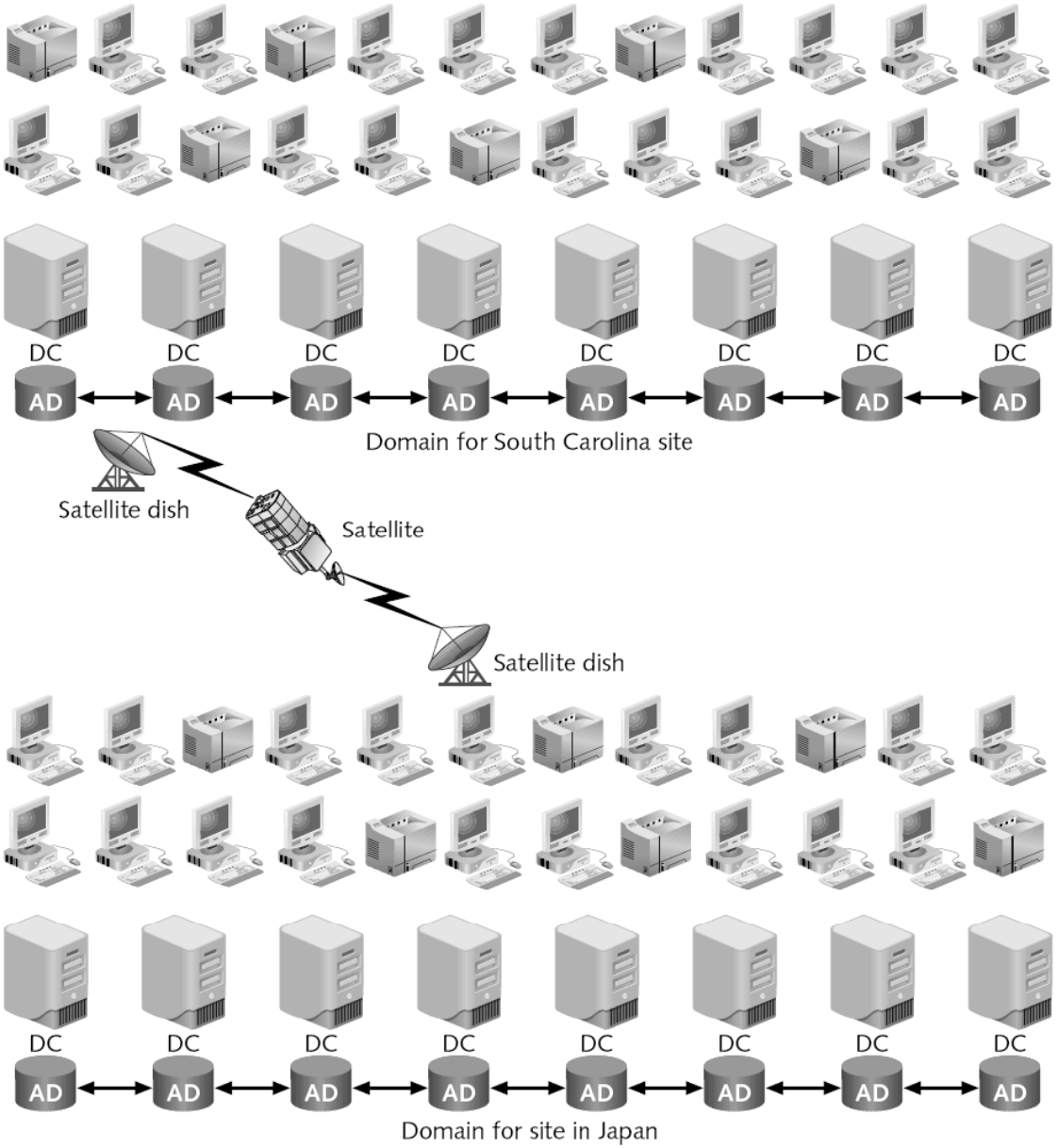

Figure 4-8 Using multiple domains

Domain (continued)

- **Domain functional levels**
  - Refers to the Windows Server operating systems on domain controllers and the domain-specific functions they support
- Windows Server 2008 Active Directory recognizes three domain functional levels
  - Windows 2000 domain functional level
  - Windows Server 2003 domain functional level
  - Windows Server 2008 domain functional level

Domain (continued)

- Activity 4-2: Managing Domains
  - Time Required: Approximately 10 minutes
  - Objective: Learn where to manage domains and domain trust relationships

Organizational Unit

- **Organizational unit (OU)**
  - Offers a way to achieve more flexibility in managing the resources associated with a business unit, department, or division
    - Than is possible through domain administration alone
- An OU is a grouping of related objects within a domain
  - OUs allow the grouping of objects so that they can be administered using the same group policies
- OUs can be nested within OUs

Organizational Unit (continued)

- When you plan to create OUs, keep three concerns in mind:
  - Microsoft recommends that you limit OUs to 10 levels or fewer
  - Active Directory works more efficiently when OUs are set up horizontally instead of vertically
  - The creation of OUs involves more processing resources because each request through an OU requires CPU time

Organizational Unit (continued)

- Activity 4-3: Managing OUs
  - Time Required: Approximately 10 minutes
  - Objective: Create an OU and delegate control over it

Site

- **Site**
  - A TCP/IP-based concept (container) within Active Directory that is linked to IP subnets
- A site has the following functions:
  - Reflects one or more interconnected subnets
  - Reflects the physical aspect of the network
  - Is used for DC replication
  - Is used to enable a client to access the DC that is physically closest
  - Is composed of only two types of objects, servers and configuration objects

Site (continued)

- Sites are based on connectivity and replication functions
- Reasons to define a site
  - Enable a client to access network servers using the most efficient physical route
  - DC replication is most efficient when Active Directory has information about which DCs are in which locations
- One advantage of creating a site is that it sets up redundant paths between DCs
  - Paths are used for replication

Site (continued)

- **Bridgehead server**
  - A DC that is designated to have the role of exchanging replication information
- Only one bridgehead server is set up per site

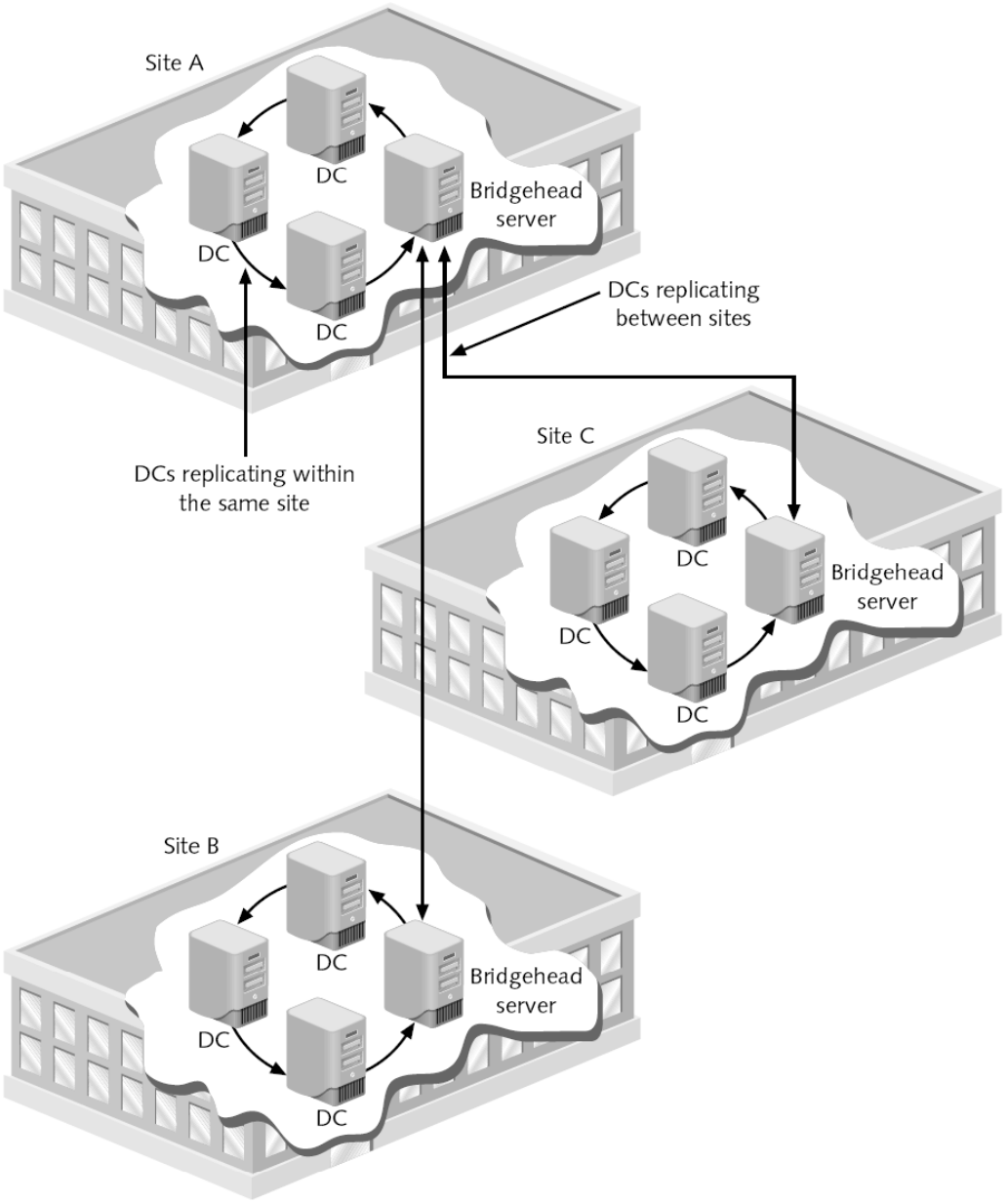

Figure 4-10 DCs replicating within and between sites

Active Directory Guidelines

- Above all, keep Active Directory as simple as possible
  - Plan its structure before you implement it
- Implement the least number of domains possible
  - With one domain being the ideal and building from there
- Implement only one domain on most small networks
- Use OUs to reflect the organization's structure
- Create only the number of OUs that are absolutely necessary

Active Directory Guidelines (continued)

- Do not build an Active Directory with more than 10 levels of OUs
- Use domains as partitions in forests to demarcate commonly associated accounts and resources governed by group and security policies
- Implement multiple trees and forests only as necessary
- Use sites in situations where there are multiple IP subnets and multiple geographic locations
  - As a means to improve logon and DC replication performance

User Account Management

- Default accounts:
  - Administrator and Guest
- Accounts can be set up in two general environments:
  - Accounts that are set up through a stand-alone server that does not have Active Directory installed
  - Accounts that are set up in a domain when Active Directory is installed

Creating Accounts When Active Directory Is Not Installed

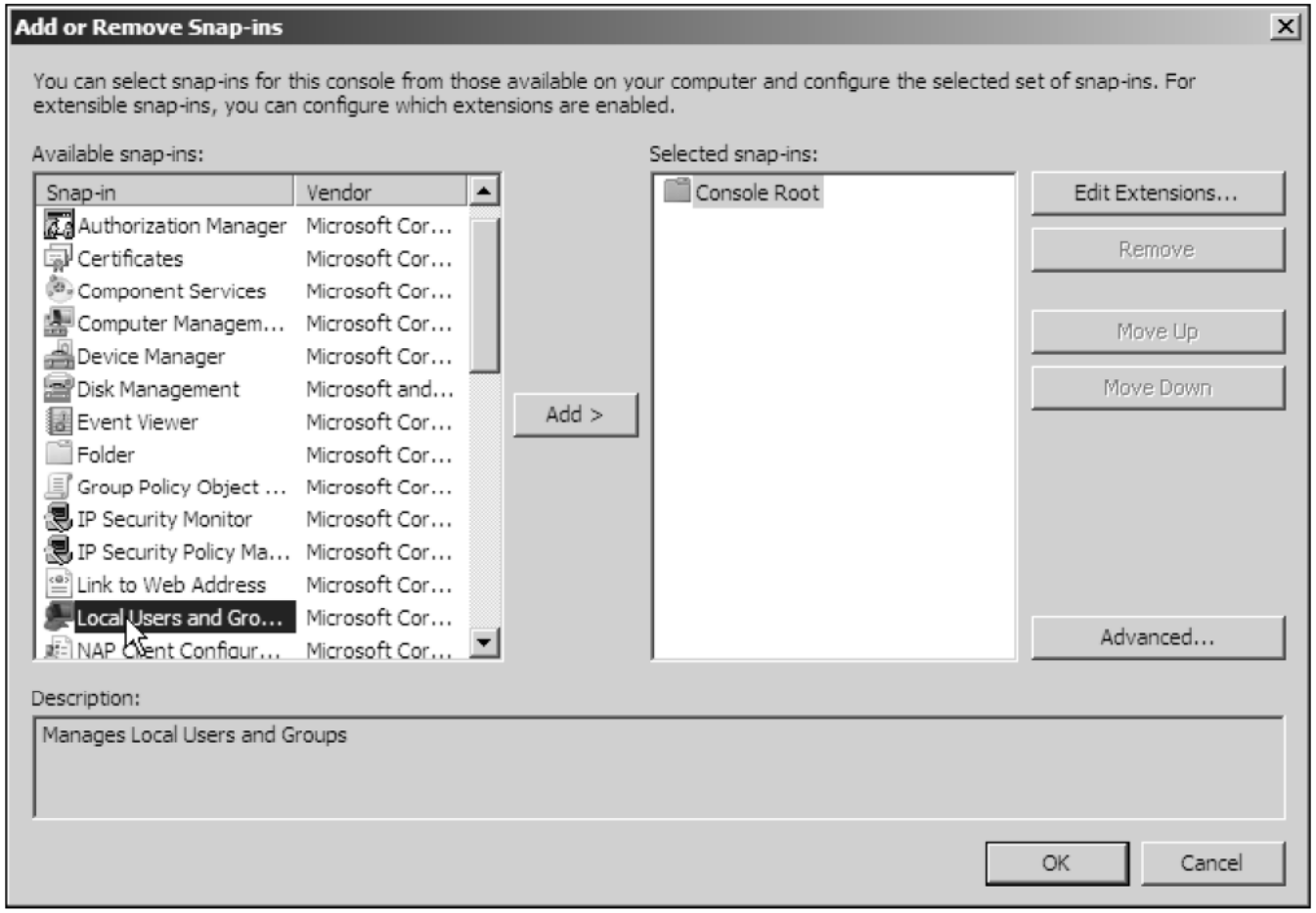

Figure 4-11 Selecting the Local Users and Groups MMC snap-in

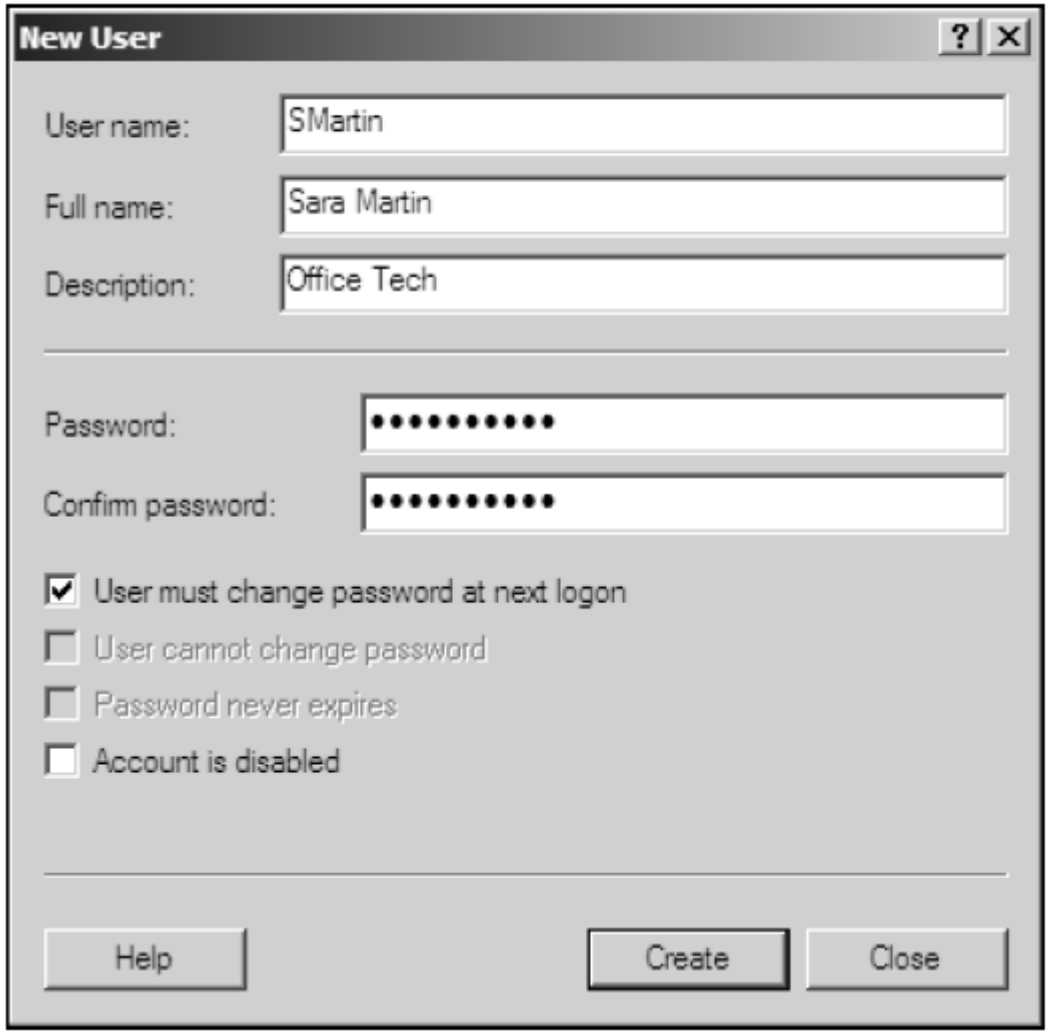

Figure 4-12 Creating a user account without Active Directory installed

Creating Accounts When Active Directory Is Installed

- Activity 4-4: Creating User Accounts in Active Directory
  - Time Required: Approximately 15 minutes
  - Objective: Learn how to create a user account in Active Directory

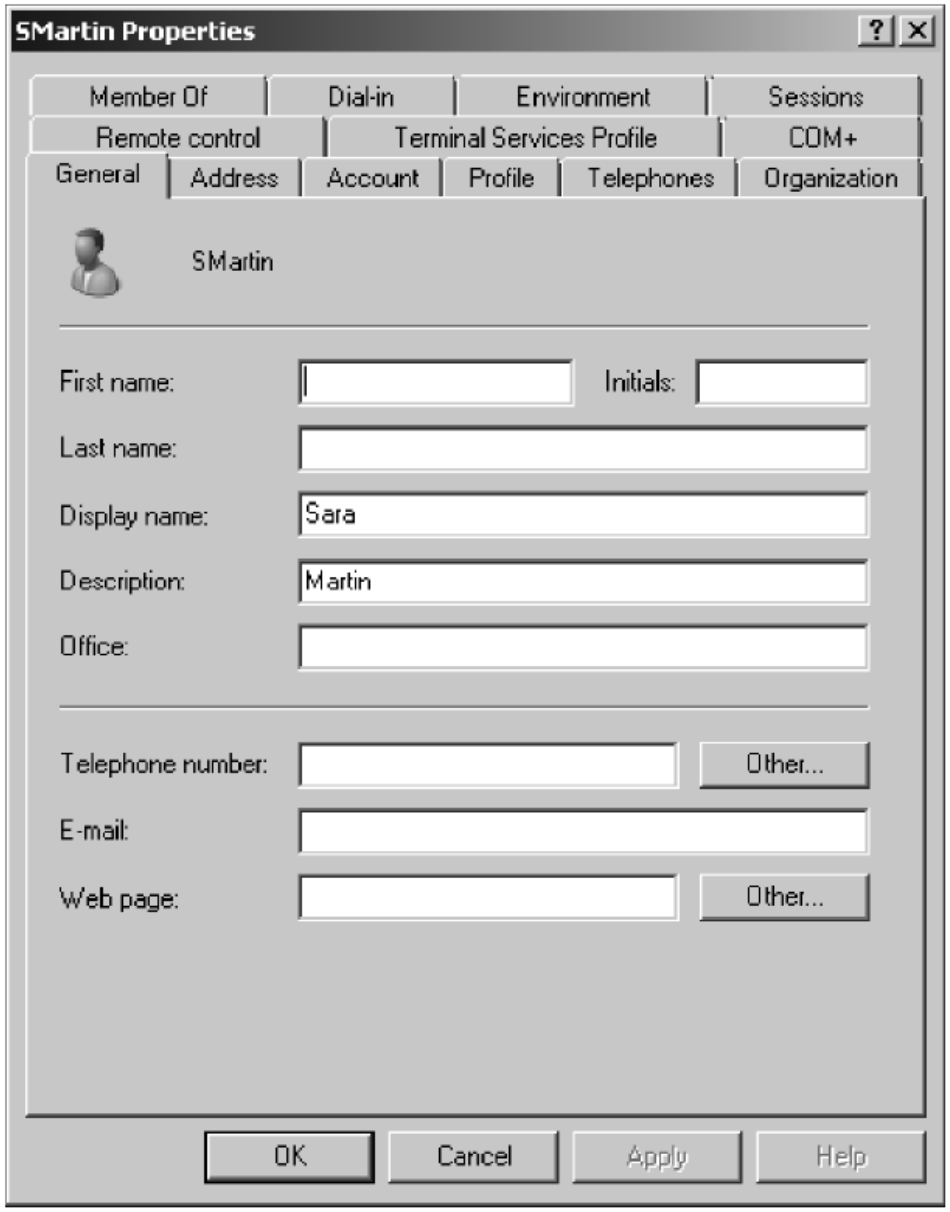

Figure 4-14 User account properties

Disabling, Enabling, and Renaming Accounts

- Activity 4-5: Disabling, Renaming, and Enabling an Account
  - Time Required: Approximately 5 minutes
  - Objective: Practice disabling, renaming, and then enabling an account

Moving an Account

- Activity 4-6: Moving an Account
  - Time Required: Approximately 5 minutes
  - Objective: Practice moving an account

Resetting a Password

- Activity 4-7: Changing an Account's Password
  - Time Required: Approximately 5 minutes
  - Objective: Practice changing an account's password

Deleting an Account

- Activity 4-8: Deleting an Account
  - Time Required: Approximately 5 minutes
  - Objective: Practice deleting an account

Security Group Management

- One of the best ways to manage accounts is by grouping accounts that have similar characteristics
- **Scope of influence** (or **scope**)
  - The reach of a group for gaining access to resources in Active Directory
- Types of groups:
  - Local
  - Domain local
  - Global
  - Universal

Security Group Management (continued)

- All of these groups can be used for security or distribution groups
- **Security groups**
  - Used to enable access to resources on a stand-alone server or in Active Directory
- **Distribution groups**
  - Used for e-mail or telephone lists, to provide quick, mass distribution of information

Implementing Local Groups

- **Local security group**
  - Used to manage resources on a stand-alone computer that is not part of a domain and on member servers in a domain
- Instead of installing Active Directory, you can divide accounts into local groups
  - Each group would be given different security access based on the resources at the server

Implementing Domain Local Groups

- **Domain local security group**
  - Used when Active Directory is deployed
  - Typically used to manage resources in a domain and to give global groups from the same and other domains access to those resources
- The scope of a domain local group is the domain in which the group exists
- The typical purpose of a domain local group is to provide access to resources
  - You grant access to servers, folders, shared folders, and printers to a domain local group

Implementing Domain Local Groups (continued)

Table 4-1 Membership capabilities of a domain local group

Active Directory objects that can be members of a domain local group	Active Directory objects that a domain local group can join as a member
User accounts in the same domain	Access control (security) lists for objects in the same domain, such as permissions to access a folder, shared folder, or printer
Domain local groups in the same domain	Domain local groups in the same domain
Global groups in any domain in a tree or forest (as long as there are transitive or two-way trust relationships maintained)	
Universal groups in any domain in a tree or forest (as long as there are transitive or two-way trust relationships maintained)	

Implementing Global Groups

- **Global security group**
  - Intended to contain user accounts from a single domain
  - Can also be set up as a member of a domain local group in the same or another domain
- A global group can contain user accounts and other global groups from the domain in which it was created
- A global group can be converted to a universal group
  - As long as it is not nested in another global group or in a universal group

Implementing Global Groups (continued)

*Managers global group (top-level global group)
Amber Richards
Joe Scarpelli
Kathy Brown
Sam Rameriz
**Finance global group (second-level global group)
Martin LeDuc
Sarah Humphrey
Heather Shultz
Sam Weisenberg
Jason Lew
***Budget global group (third-level global group)
Michele Gomez
Kristin Beck
Chris Doyle

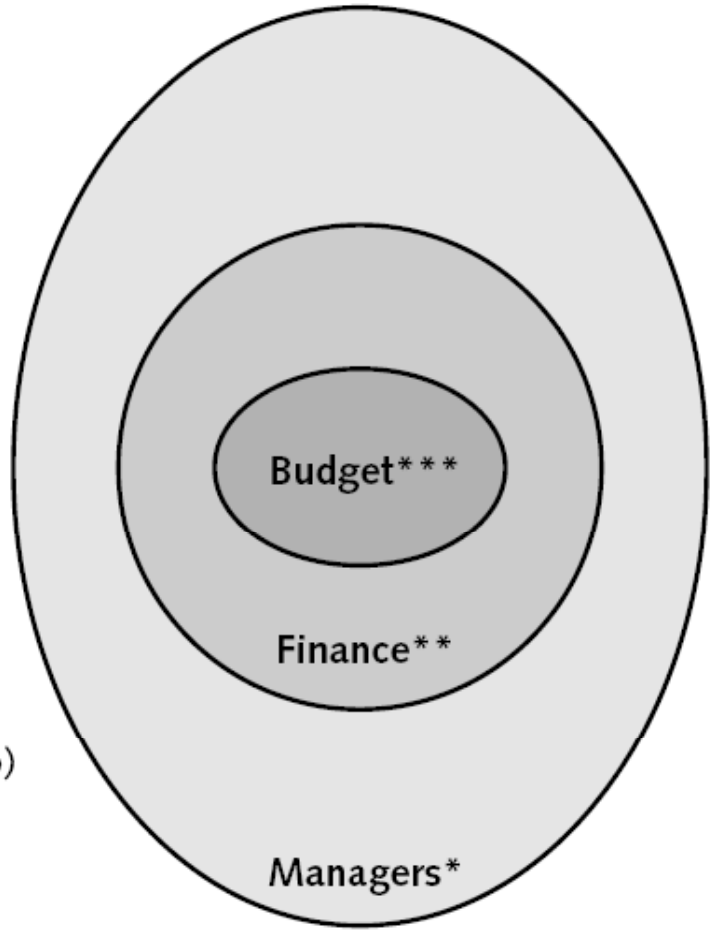

Figure 4-18 Nested global groups

Implementing Global Groups (continued)

- A typical use for a global group is to build it with accounts that need access to resources in the same or in another domain
  - And then to make the global group in one domain a member of a domain local group in the same or another domain
- This model enables you to manage user accounts and their access to resources through one or more global groups
  - While reducing the complexity of managing accounts

Implementing Global Groups (continued)

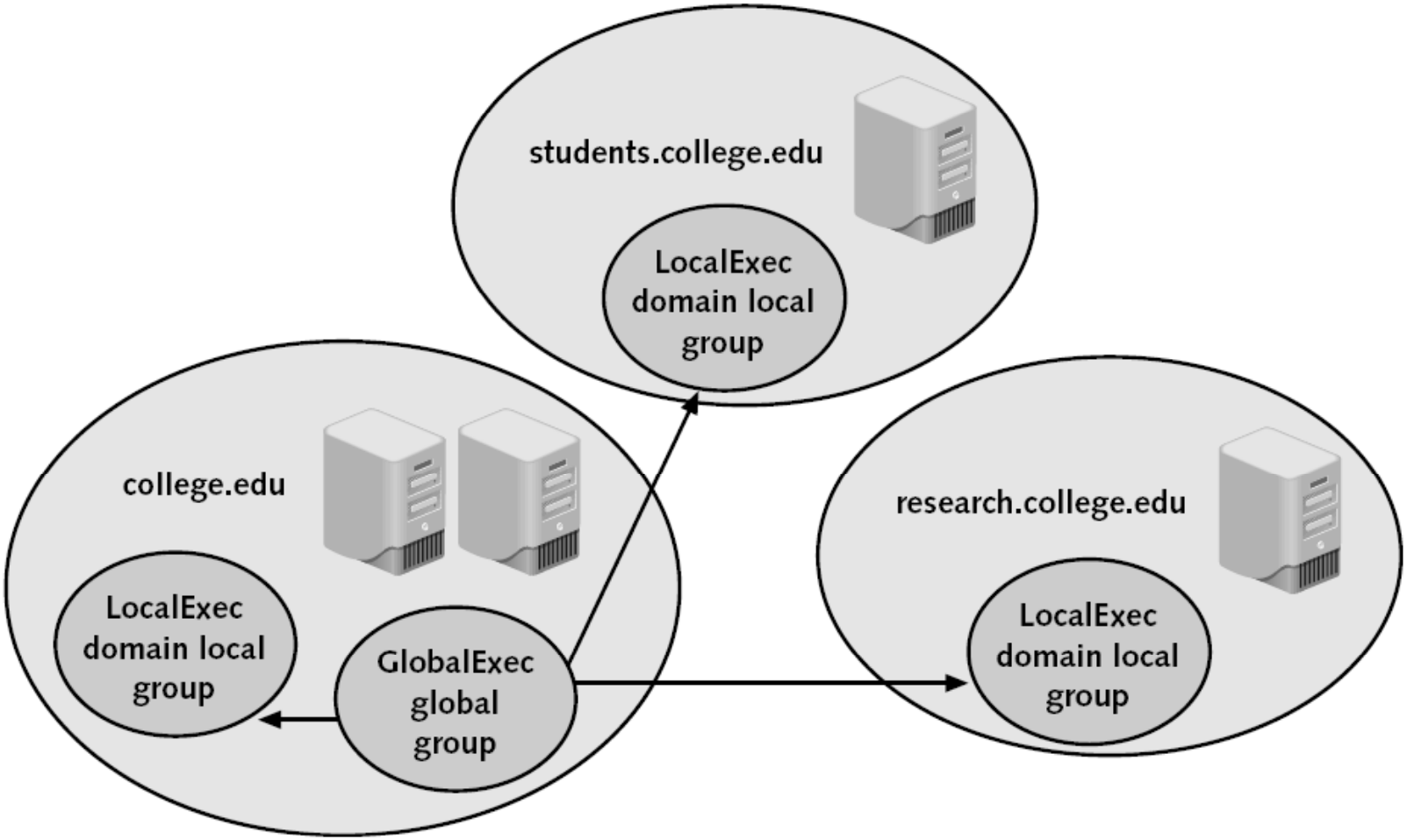

Figure 4-19 Managing security through domain local and global groups

Implementing Global Groups (continued)

- Activity 4-9: Creating Domain Local and Global Security Groups
  - Time Required: Approximately 15 minutes
  - Objective: Create a domain local and a global security group and make the global group a member of the domain local group

Implementing Universal Groups

- **Universal security groups**
  - Provide a means to span domains and trees
- Universal group membership can include user accounts from any domain, global groups from any domain, and other universal groups from any domain
- Universal groups are offered to provide an easy means to access any resource in a tree
  - Or among trees in a forest

Implementing Universal Groups (continued)

- Guidelines to help simplify how you plan to use groups:
  - Use global groups to hold accounts as members
  - Use domain local groups to provide access to resources in a specific domain
  - Use universal groups to provide extensive access to resources

Implementing Universal Groups (continued)

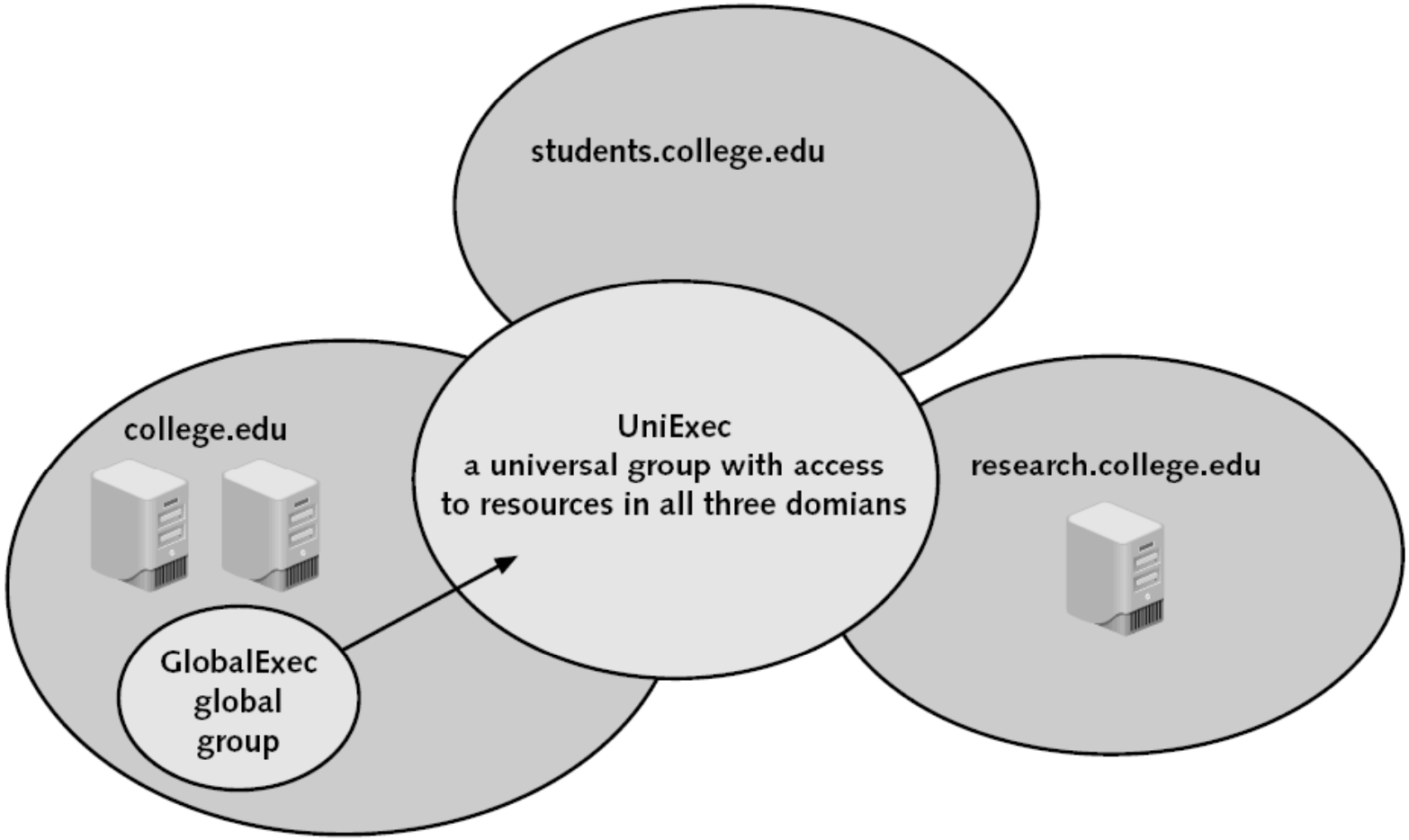

Figure 4-21 Managing security through universal and global groups

Properties of Groups

- You can configure the properties of a specific group
  - By double-clicking that group in the Local Users and Groups tool for a stand-alone (nondomain) or member server
  - Or in the Active Directory Users and Computers tool for DC servers in a domain
- Properties are configured using the following tabs:
  - General
  - Members
  - Member Of
  - Managed By

Implementing User Profiles

- A **local user profile** is automatically created at the local computer when you log on with an account for the first time
  - The profile can be modified to consist of desktop settings that are customized for one or more clients who log on locally

Implementing User Profiles (continued)

- User profiles advantages
  - Multiple users can use the same computer and maintain their own customized setting
  - Profiles can be stored on a network server so they are available to users regardless of the computer they use to log on (**roaming profile)**
  - Profiles can be made mandatory so users have the same settings each time they log on (**mandatory profile**)

Implementing User Profiles (continued)

- One way to set up a profile is to first set up a generic account on the server with the desired desktop configuration
  - Then copy the Ntuser.dat file to the \Users\Default folder in Windows Server 2008
- To create the roaming profile, set up a generic account and customize the desktop
  - Set up those users to access a profile by opening the Profile tab in each user's account properties and entering the path to that profile

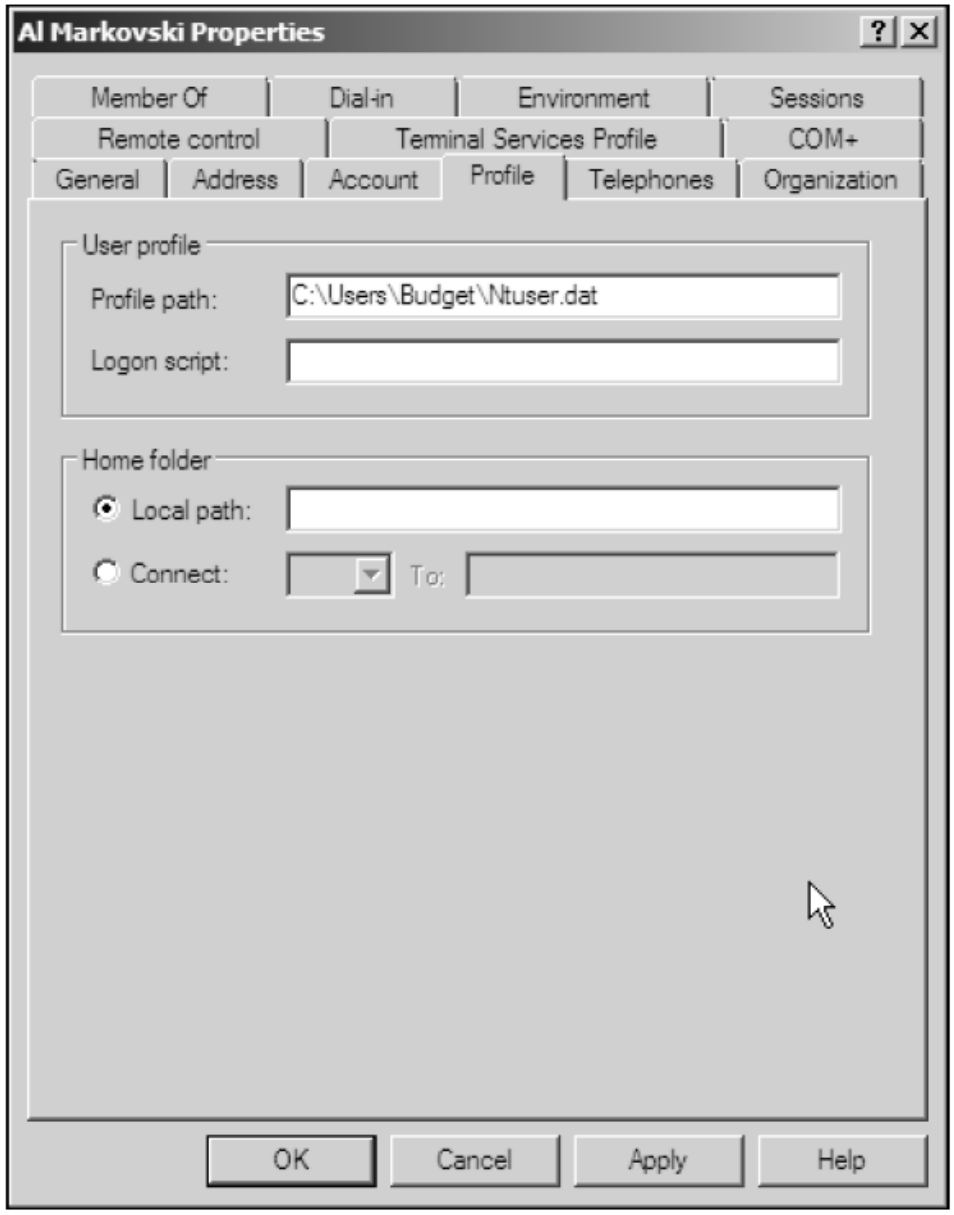

Figure 4-22 Setting a roaming profile in an account's properties

What's New in Windows Server 2008 Active Directory

- Five new features deserve particular mention:
  - Restart capability
  - Read-Only Domain Controller
  - Auditing improvements
  - Multiple password and account lockout policies in a single domain
  - Active Directory Lightweight Directory Services role

Restart Capability

- Windows Server 2008 provides the option to stop Active Directory Domain Services
  - Without taking down the computer
- After your work is done on Active Directory, you simply restart Active Directory Domain Services

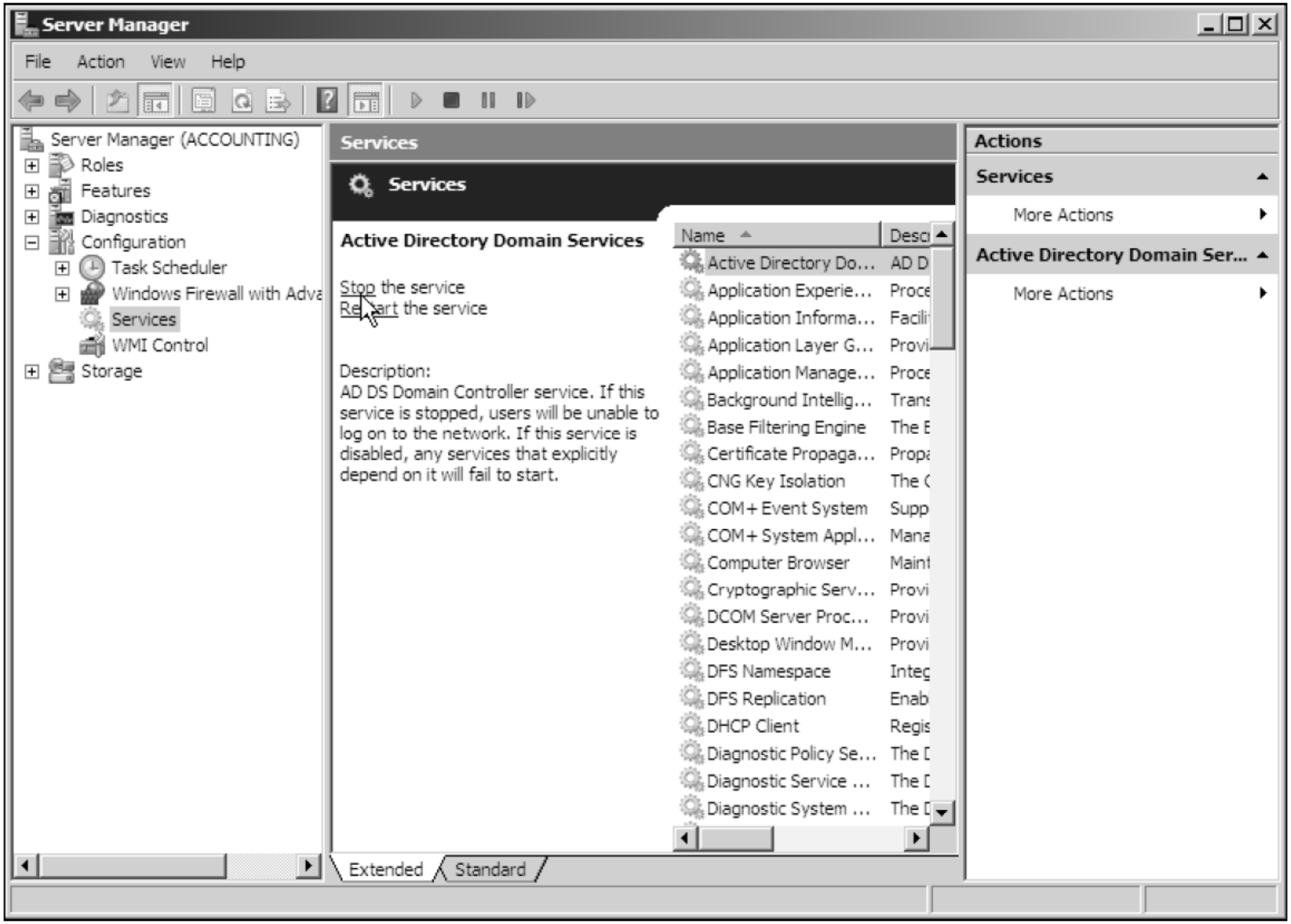

Figure 4-23 Stopping Active Directory Domain Services

Read-Only Domain Controller

- **Read-Only Domain Controller (RODC)**
  - You cannot use it to update information in Active Directory and it does not replicate to regular DCs
- An RODC can still function as a Key Distribution Center for the Kerberos authentication method
- The purpose of having an RODC is for better security at branch locations
  - Where physical security measures might not be as strong as at a central office
- An RODC can also be configured as a DNS server

Auditing Improvements

- Server administrators can now create an audit trail of many types of changes that might be made in Active Directory, including when:
  - There are attribute changes to the schema
  - Objects are moved, such as user accounts moved from one OU to a different one
  - New objects are created, such as a new OU
  - A container or object is deleted and then brought back, even if it is moved to a different location than where it was originally located

Auditing Improvements (continued)

- You must set up Active Directory auditing in two places:
  - Enable a Domain Controllers (global) Policy to audit successful or failed Active Directory change actions
  - Configure successful or failed change actions on specific Active Directory objects or containers

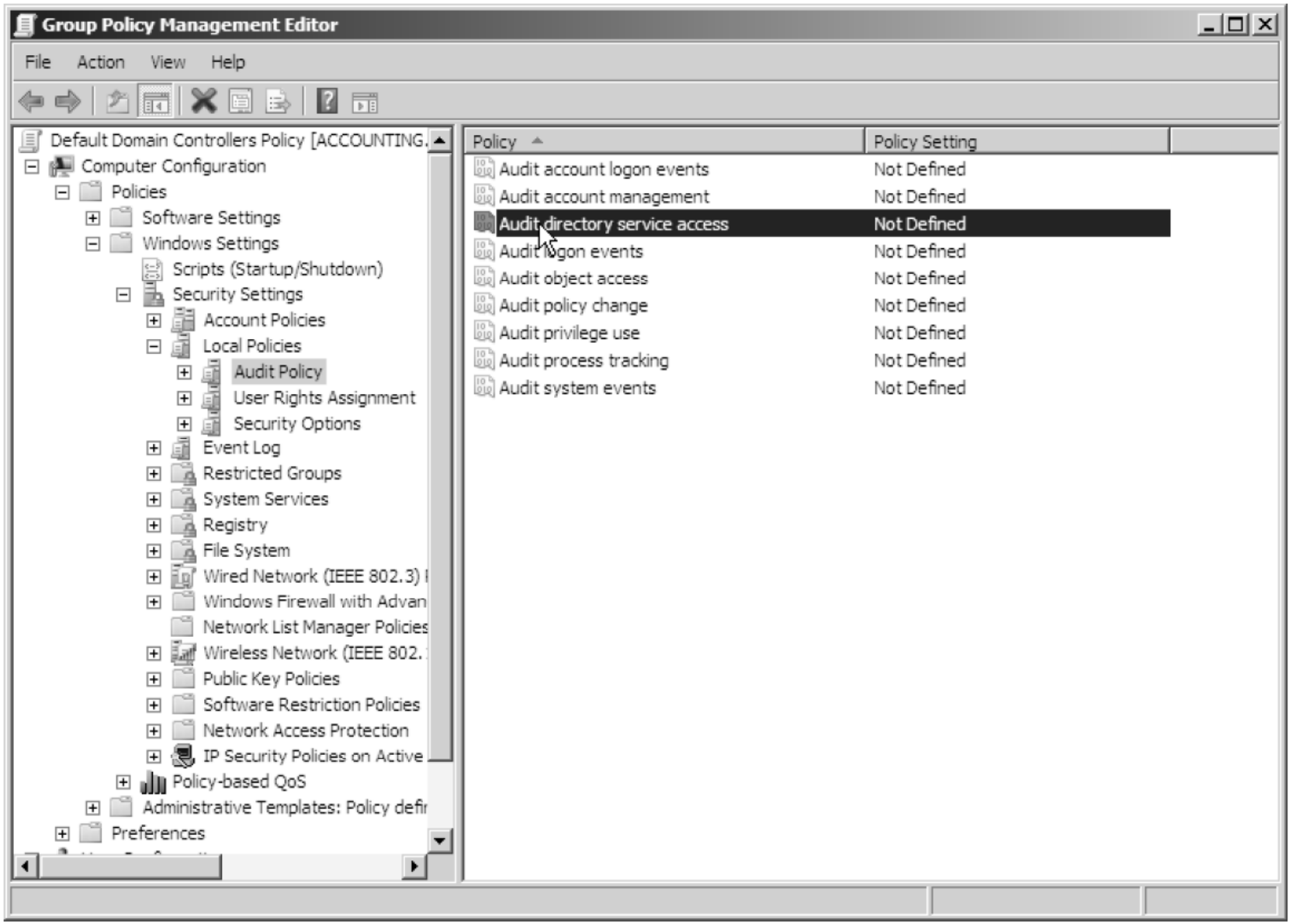

Figure 4-24 Setting up directory service access auditing

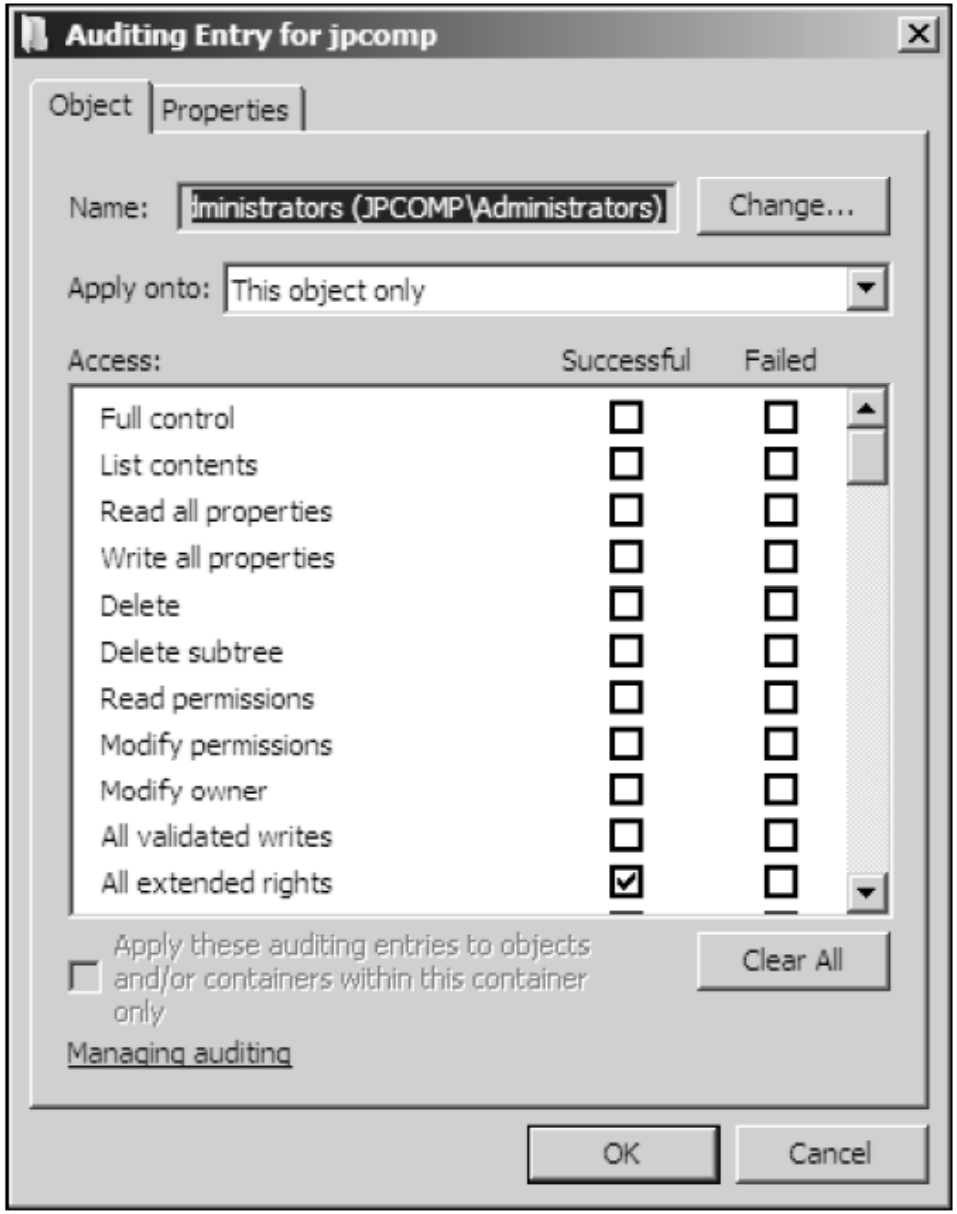

Figure 4-25 Configuring object auditing for a domain

Multiple Password and Account Lockout Policies in a Single Domain

- You can set up multiple password and account lockout security requirements
  - And associate them with a security group or user
- You can also associate them with an OU by creating a ‘‘global shadow security group’’
  - A group that can be mapped to an OU
  - This process is called setting up ‘‘fine-grained password policies’’

Active Directory Lightweight Directory Services Role

- Active Directory Lightweight Directory Services (AD LDS) role
  - Targeted for servers that manage user applications
  - Enables the applications to store configuration and vital data in a central database
- AD LDS is more forgiving than AD DS
  - If you make a mistake in a modification the mistake in most circumstances does not affect how users access their accounts and resources in a domain
- AD LDS is installed as a server role via Server Manager

Summary

- Active Directory (or AD DS) is a directory service to house information about network resources
- Servers housing Active Directory are called domain controllers (DCs)
- The most basic component of Active Directory is an object
- The global catalog stores information about every object, replicates key Active Directory elements, and is used to authenticate user accounts when they log on

Summary (continued)

- A namespace consists of using the Domain Name System for resolving computer and domain names to IP addresses and vice versa
- Active Directory is a hierarchy of logical containers: forests, trees, domains, and organizational units
- You can delegate management of many Active Directory containers to specific types of administrators
- User accounts enable individual users to access specific resources

Summary (continued)

- On a stand-alone or member server, you can create local security groups to help manage user accounts
- User profiles are tools for customizing accounts
- The ability to stop and restart Active Directory without taking down a DC is new to Windows Server 2008
- Three additional new features include new Active Directory auditing capabilities, fine-grained password policies, and the Active Directory Lightweight Directory Services role