COURSE TECHNOLOGY
CENGAGE Learning

Hands-On Microsoft Windows Server 2008

Chapter 4

Introduction to Active Directory and Account Manager

Objectives

- Understand Active Directory basic concepts
- Install and configure Active Directory
- Implement Active Directory containers
- Create and manage user accounts
- Configure and use security groups
- Describe and implement new Active Directory features

Active Directory Basics

- Active Directory (AD)
  - 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 (DS)**
  - 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

Active Directory Basics (continued)

- **Domain**
- Container that holds information about all network resources that are grouped within it
  - Every resource (User-Printer-Scanner) is called an **object**

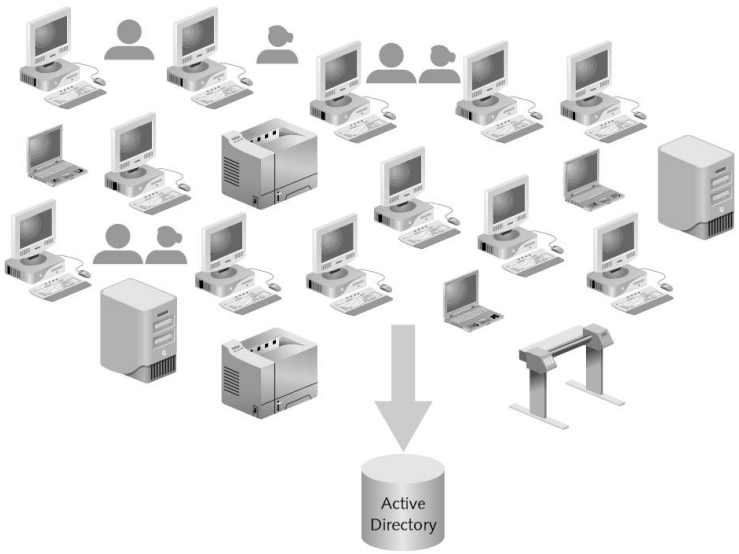


Figure 4-1 Active Directory domain objects include servers, workstations, printers, users, user groups, and other resources.

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

Organizational Unit

- **Organizational unit (OU)**
  - 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 the following 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

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

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

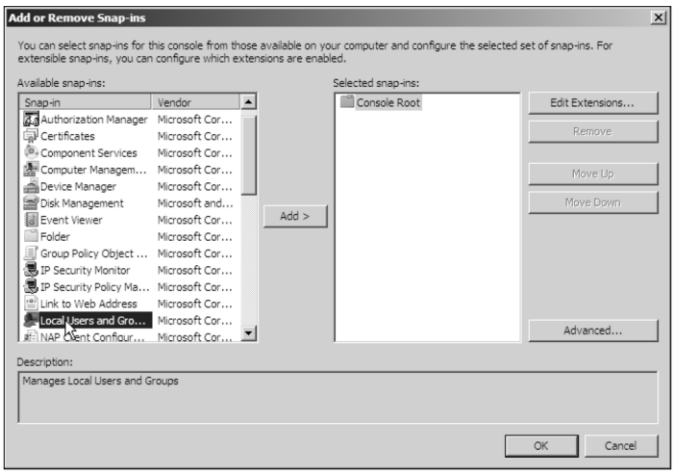


Figure 4-11 Selecting the Local Users and Groups MMC snap-in

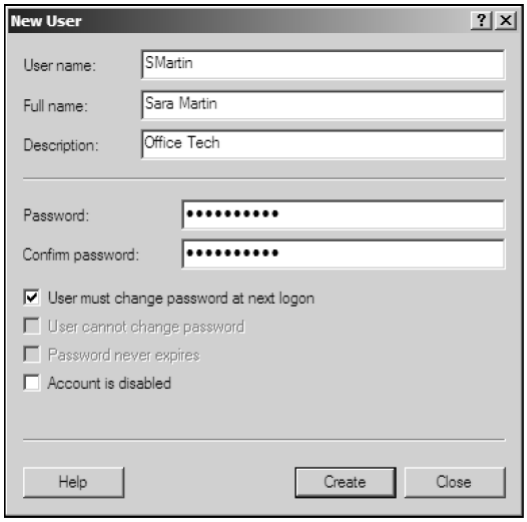


Figure 4-12 Creating a user account without Active Directory installed

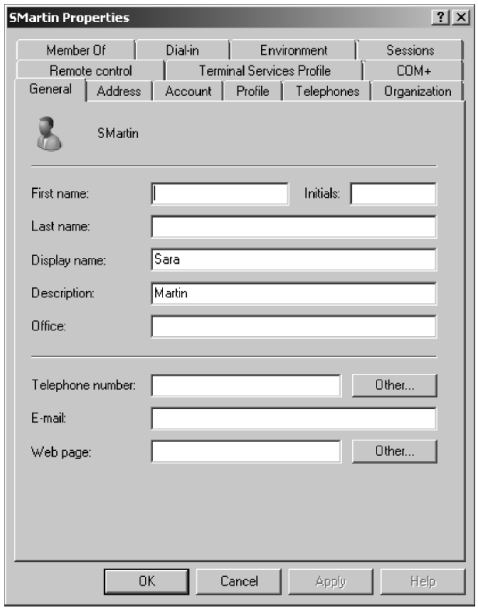
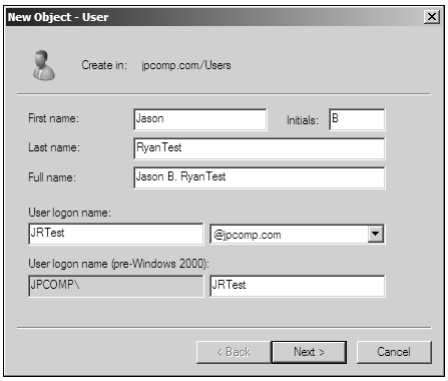


Figure 4-14 User account properties

Creating Accounts When Active Directory is Installed



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, huge 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
    - **Stand-alone Computer :**are computers that are not part of any domain
    - **Member Servers:** Servers on a network managed by Active Directory that do not have Active Directory installed.
  - 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 Global Groups

- **Global security group**
  - Intended to contain user accounts and other global groups from the domain in which it was created
  - Can also be set up as a member of a domain local group in the same or another domain
- 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

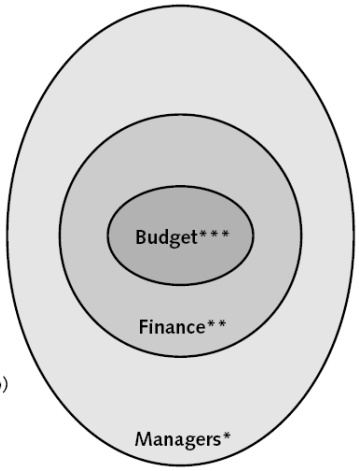


Figure 4-18 Nested global groups

Implementing Global Groups (continued)

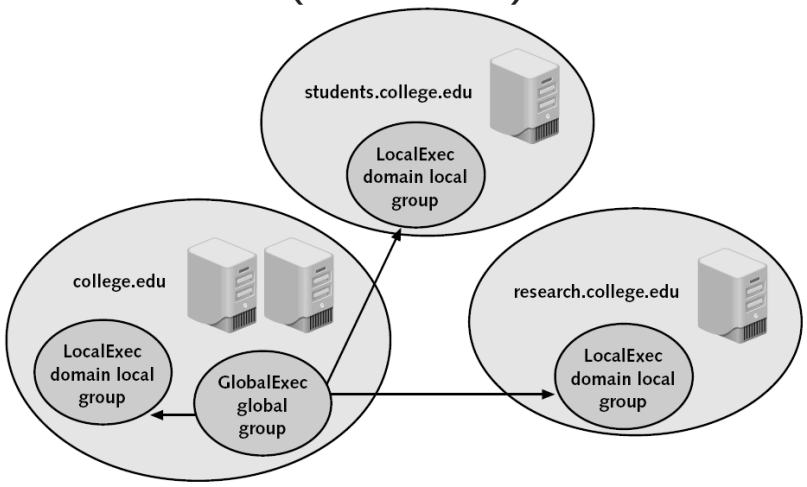


Figure 4-19 Managing security through domain local and global groups

Implementing Universal Groups

- **Universal security groups**
- 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 any domain.**

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)

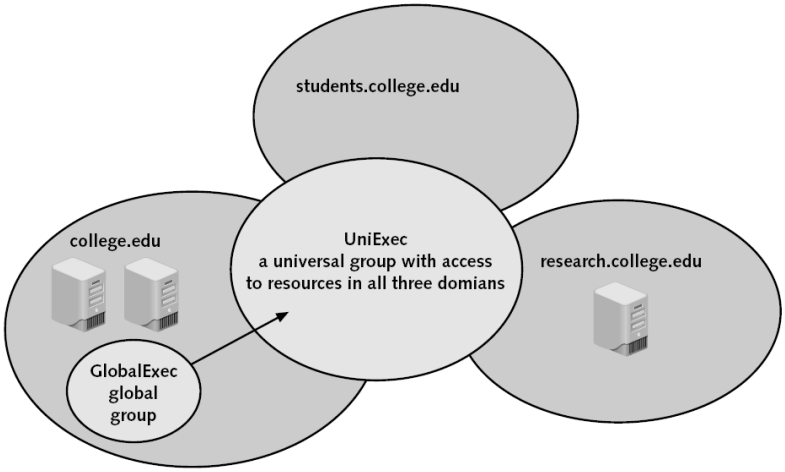


Figure 4-21 Managing security through universal and global groups

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**)

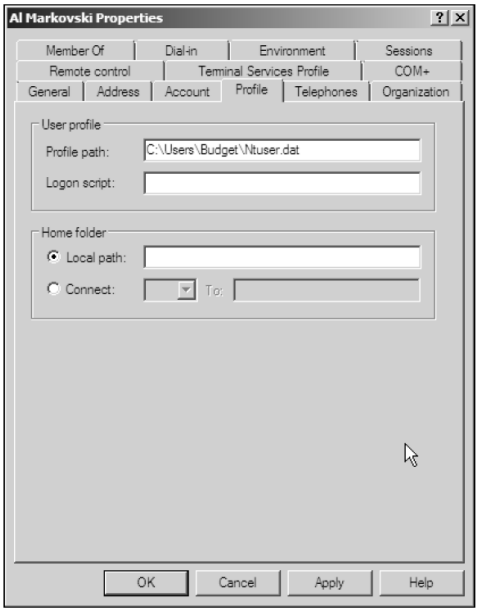


Figure 4-22 Setting a roaming profile in an account's properties

What's New in Windows Server 2008 Active Directory

- Five new features deserve particular mention:
  - Restart capability
  - Read-Only Domain Controller
  - 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

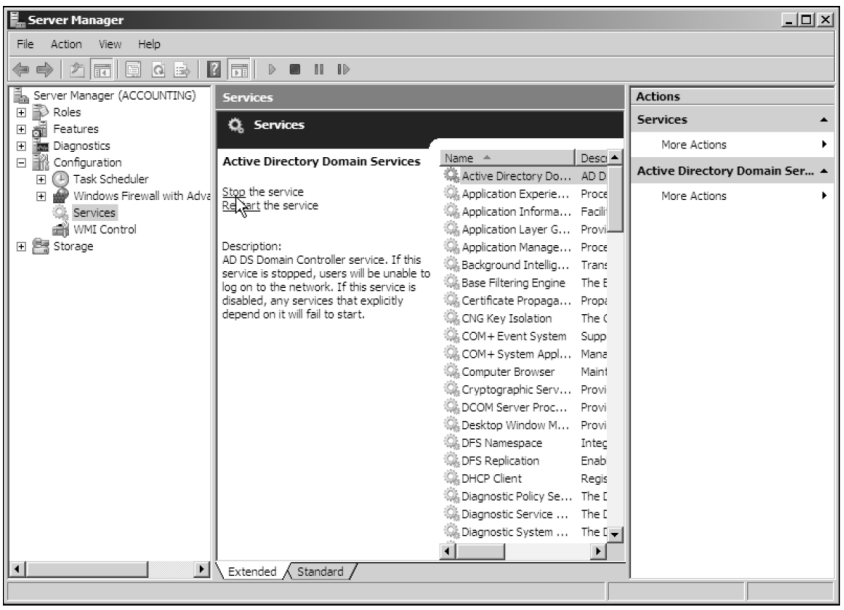


Figure 4-23 Stopping Active Directory Domain Services