Diploma in Infocomm & Security

IT2654: Systems Administration & Security

TOPIC 3: IMPLEMENTING AND MANAGING GROUPS

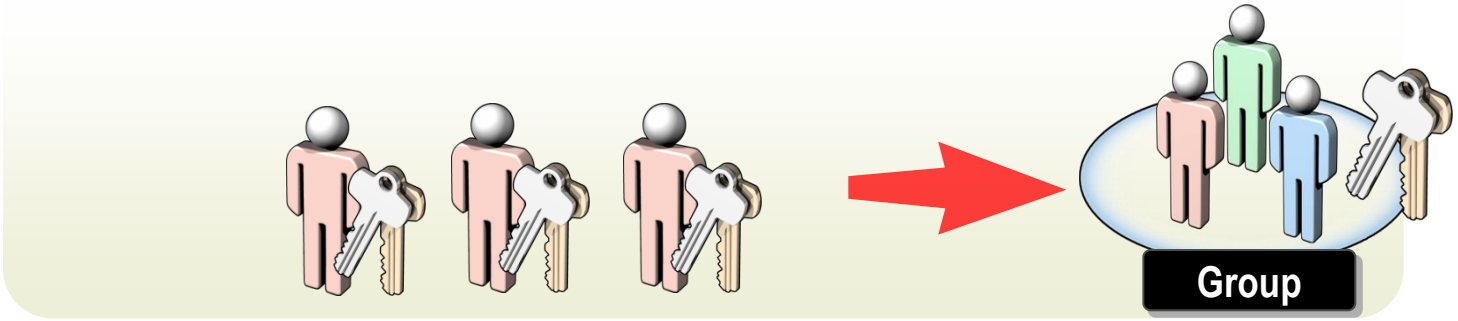
Objectives

- Understand the purpose of using group accounts to simplify administration
- Create group objects using both graphical and command-line tools
- Explain the purpose of the built-in groups created when Active Directory is installed
- Manage security groups and distribution groups

What Are Groups?

- Used to organize collections of users, computers, contacts, other groups

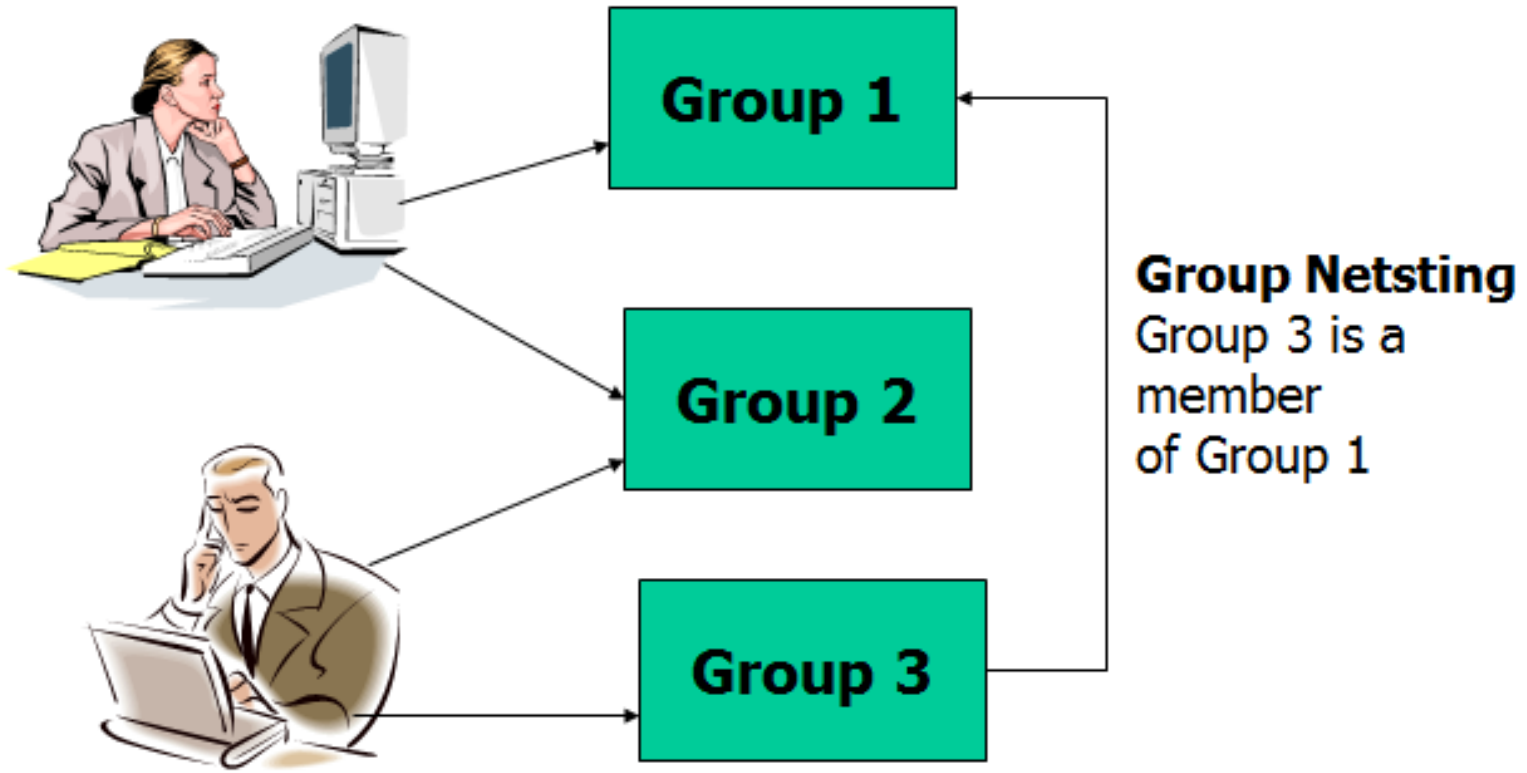
- Simplify administration by enabling you to assign permissions for resources



Groups are characterized by :

1) Scope – Domain Local, Global, Universal
2) Type – Security, Distribution

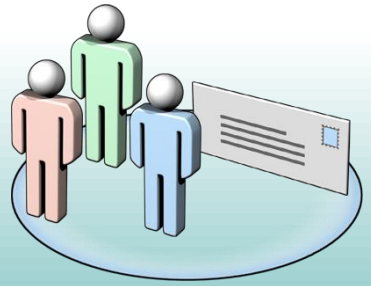
Group/User relationship



Group Types

- **Security groups**
  - Defined by Security Identifier (SID)
  - Used to assign user rights and permissions
  - Can be assigned rights to perform different tasks
  - Can be used as an e-mail distribution list

- **Distribution groups**
  - Can be used only with e-mail applications
  - Do not have associated SID
  - Cannot be used to assign permissions



Group Scopes

- The group scope determines whether the group spans multiple domains or is limited to a single domain
- Both Security and Distribution Groups have scopes
- Three group scopes are:
  1) **Domain local group**
  2) **Global group**
  3) **Universal group**

Domain Local Groups (DL)

- Designed to contain Global Groups and Universal Groups.
- Can contain also User Accounts and other DL groups.
- The scope of a Domain Local group is the domain in which the group exists
- 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

Global Groups

- Organize groups of Users, Computers, Groups within the same domain
- Usually represents a geographic location or job function group
- Can be granted access to resources or placed into local/domain local groups in any trusting 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
- Global groups placed into Domain Local groups or Local groups.

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

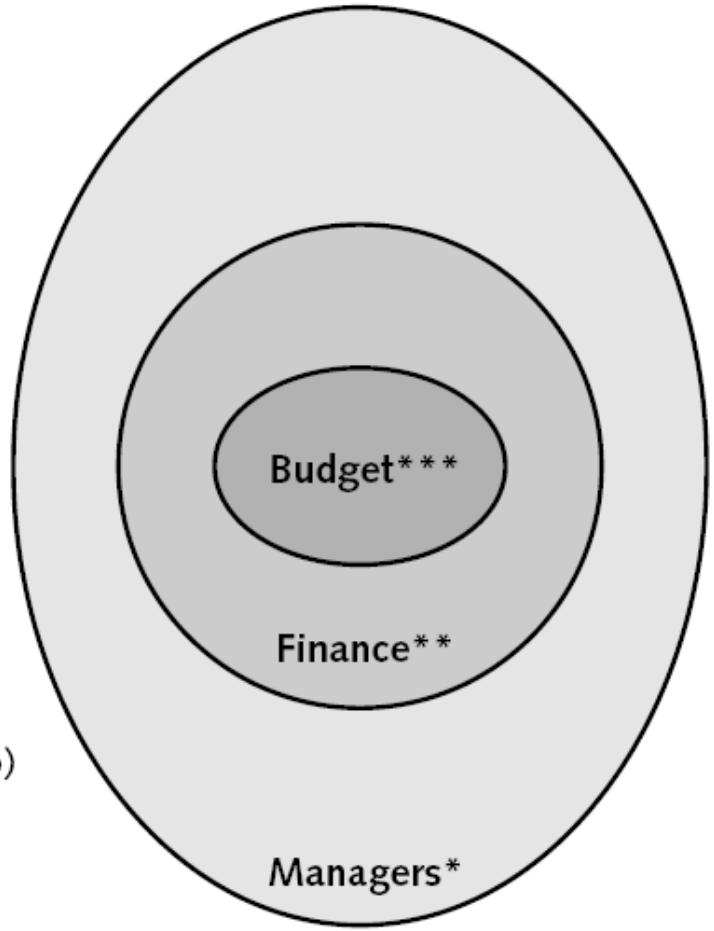


Figure 4-18 Nested global groups

Implementing Global Groups (continued)

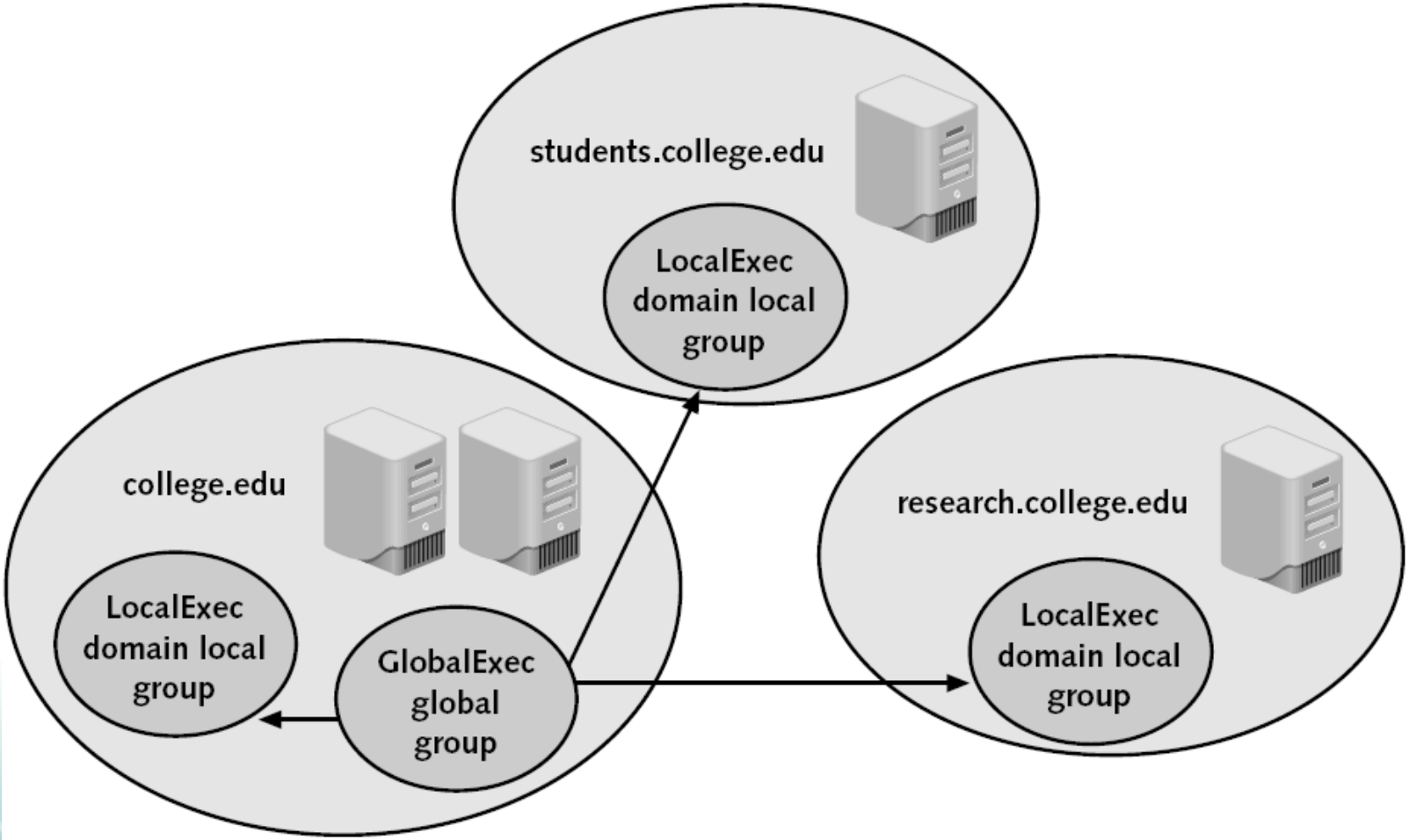


Figure 4-19 Managing security through domain local and global groups

Universal Groups

- Purpose: Organize users and groups across domains and to grant access to resources across domains
  - Can be assigned rights and permissions for any resource within a forest
- Can contain users, global groups, and local groups from any domain in the forest
- **Cannot** contain users or groups from other domains outside of the forest
- Stored on domain controllers configured as global catalog servers

Implementing Universal Groups (continued)

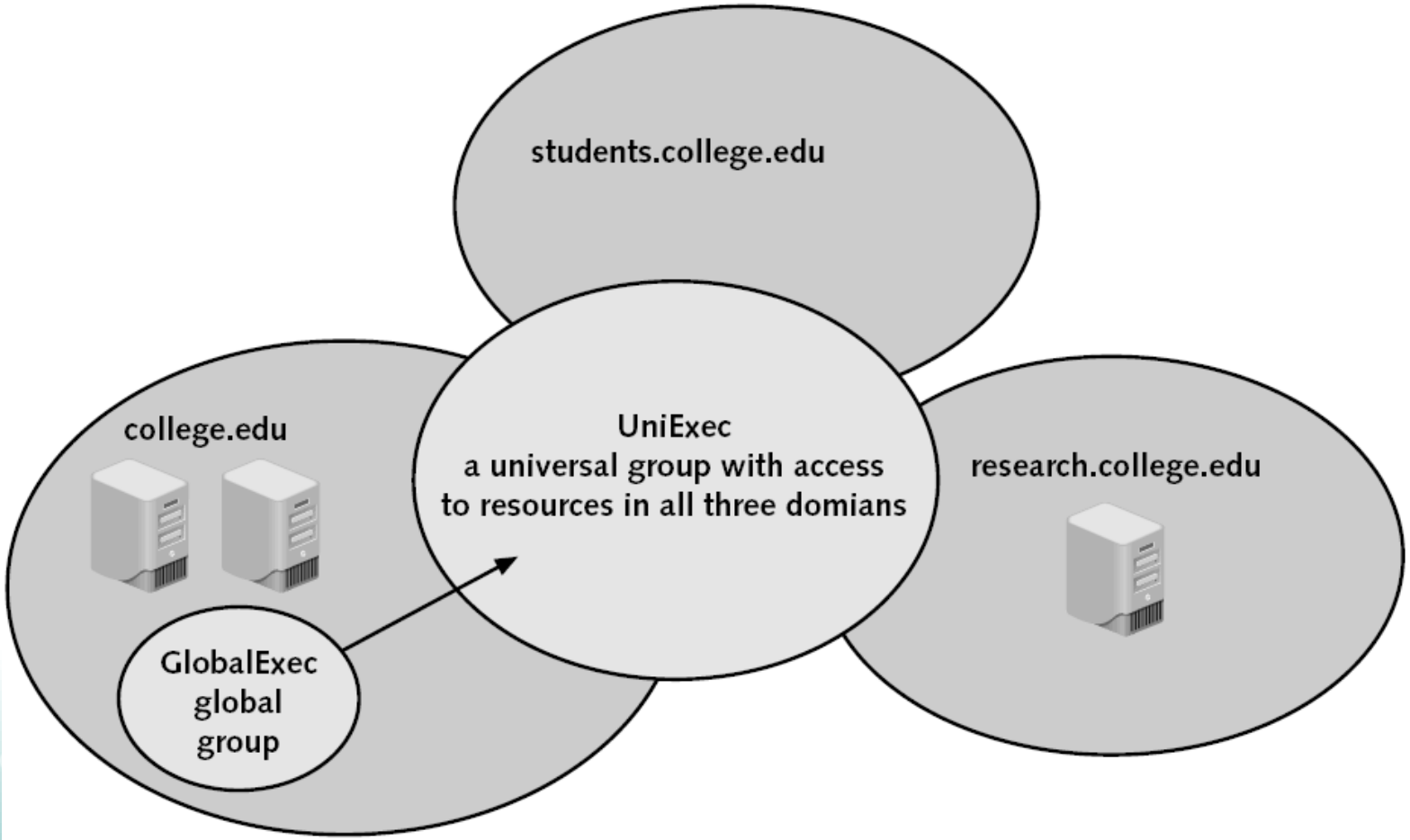
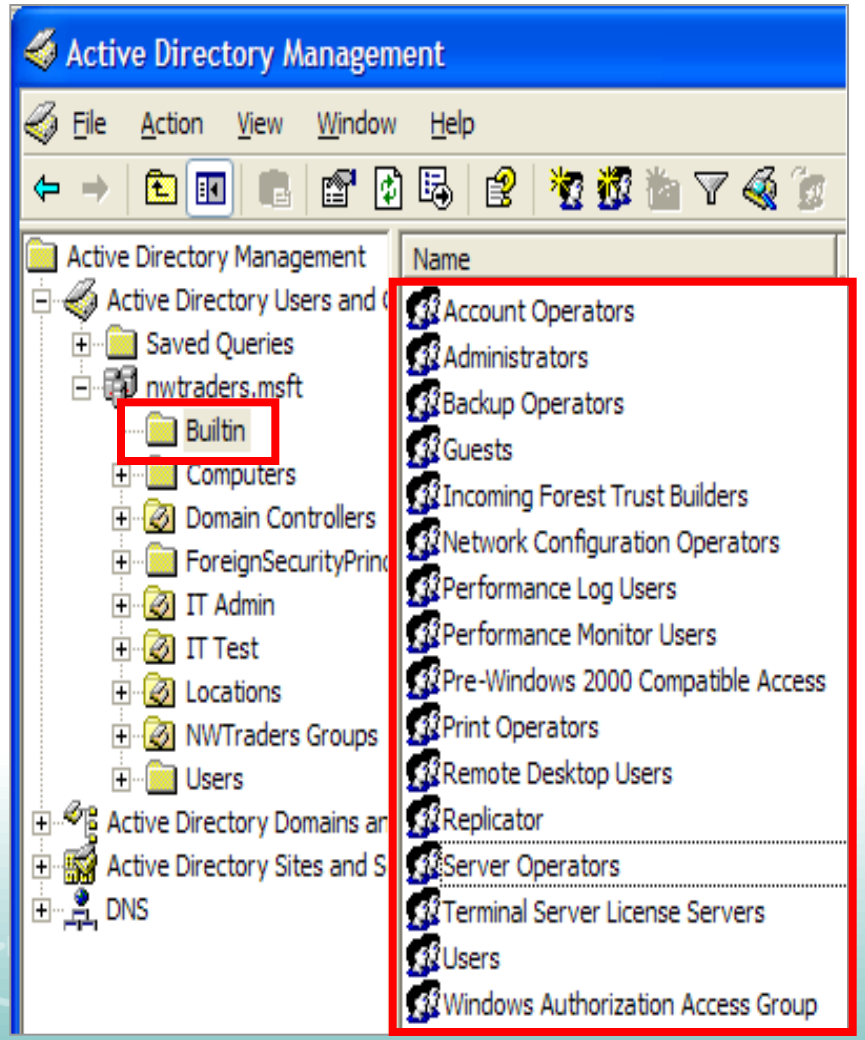
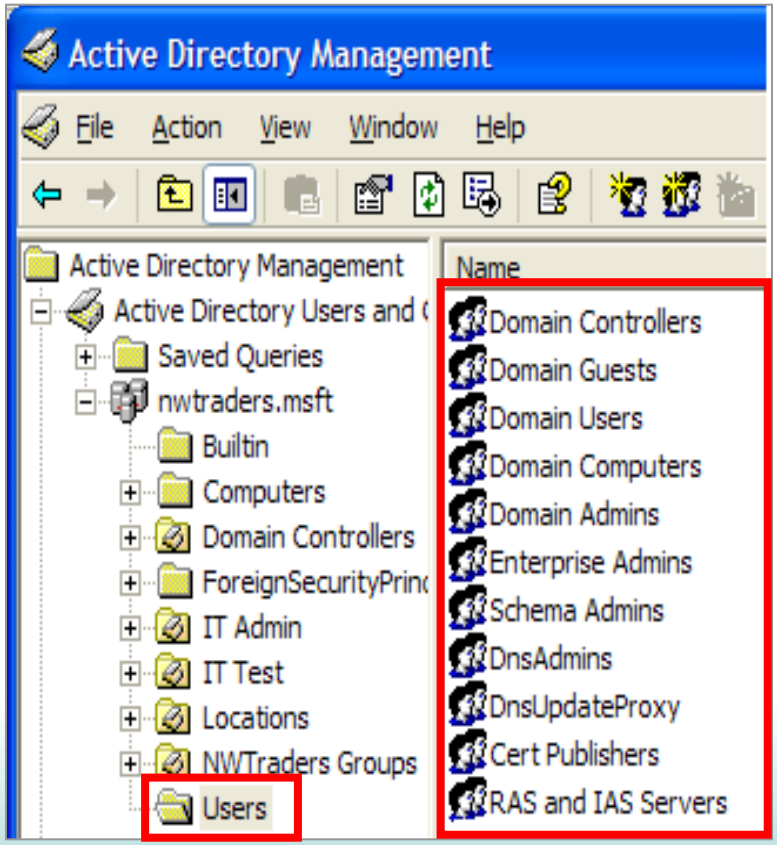


Figure 4-21 Managing security through universal and global groups

Default Groups in Active Directory





When to Use Default Groups

- Default groups are:
  - Created during the installation of the operating system or when services are added such as Active Directory or DHCP
  - Automatically assigned a set of user rights
- Use Default groups to:
  - Control access to shared resources
  - Delegate specific domain-wide administration

Group Account vs. OU

- Similar to Organizational Units except
  - OUs are not security principals, groups are
  - OUs can only contain objects from their parent domain, groups can contain objects from within forest

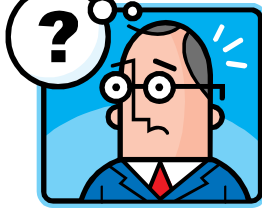
Creating Group Objects

- Group objects are stored in Active Directory database
- Variety of tools can be used for creation and management
  - Active Directory Users and Computers
  - Command-line utilities
    - DSADD, DSMOD, DSQUERY, etc.

Active Directory Users and Computers

- Primary tool
  - To create group accounts
  - Can also be used to configure properties of group accounts
- Groups can be created in any built-in containers, at root of the domain object, or in custom OU objects
- Possible group scopes determined by the functional level the domain is configured to

Determining Group Membership



- Important task for administrators is to ensure that users are members of correct groups
- One method is via Member Of tab in the properties of a user account
  - Only shows first level of groups (not groups of groups)
- Second method is to use DSGET
- Returns values to a query

Example:

```
dsget group "cn=Domain Users,cn=users,dc=frontier,dc=net" –members
dsget user "cn=ali,ou=Sales,ou=nypmcp,dc=frontier,dc=net" -memberof
```

Determining Group Membership

- Syntax is
  - dsget group *distinguished-name switches*
- Switches include: -members, -memberof
- Can also be used as dsget user to get membership information about a specific user
- Output can be saved to a file:
  - dsget group *distinguished-name switches* >> *filename*

Example:

dsget user "cn=user1 it, ou=nypmcp, dc=frontier, dc=net" -memberof

Converting Group Scopes

- Scope of a group can be changed
- Domain functional level must be at least Windows 2003
- Supported changes
  - Global to Universal
  - Domain Local to Universal
  - Universal to Global (*if it does not contain other universal groups)*
  - Universal to Domain Local

Command Line Utilities

- An alternative to Active Directory Users and Computers
  - Some administrators have a preference for command-line utilities
  - Command-line utilities are more flexible for group management and creation in some situations

DSADD

- Used to create new user and group accounts
- Syntax is
  - dsadd group *distinguished-name switches*
- Switches include: -secgrp, -scope, -memberof, -members
- More help is available for switches and options at Windows Server Help and Support Center or at command-line

Example – adds a group

dsadd group "cn=demo, ou=nypmcp, dc=frontier, dc=net" –secgrp yes –scope g

DSMOD

- Allows various object types to be modified from the command line
- Syntax is
  - dsmod group *distinguished-name switches*
- Switches include: -desc, -rmmbr, -addmbr
- More help is available for switches and options at Windows Server Help and Support Center or command-line

Example - adds description to group info

dsmod group "cn=G Marketing Users, ou=nypmcp, dc=frontier, dc=net" –desc "Frontier Marketing Users Global Group"

DSQUERY

- Used to query various object types from the command line, returns values
- Syntax for groups is
  - dsquery group *query*
- Supports wildcard character (*)
- Output can be piped as input to other command-line tools

Example:

dsquery group "ou=nypmcp,dc=frontier,dc=net"

DSMOVE

- Used to move or rename various object types from the command line
- Syntax for groups is
  - dsmove group *distinguished-name switches*
- Switches include: -newparent, -newname
- Can only be used for groups within a single domain
- More help is available for switches and options at Windows Server Help and Support Center or at the command-line

DSRM

- Used to delete various object types from the command line
- Syntax for groups is
  - dsrm group *distinguished-name switches*
- Switches include: -noprompt

Example – remove demo group

dsrm "cn=demo,ou=nypmcp,dc=frontier,dc=net"

Security Groups Strategy

- Strategy for managing security groups in a SINGLE-DOMAIN environment use acronym

  A G DL P:

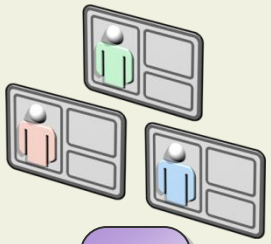
  1. Create user Accounts (A) and make them members of
  2. Global groups (G), which are members of
  3. Domain Local groups (DL) which are assigned
  4. Permissions (P) to resources.

Managing Security Groups

- Strategy for managing security groups in MULTI-DOMAIN environment use acronym A G U DL P:
  1. Create user Accounts (A) and organize them within Global groups (G)
  2. Optional: Create Universal groups (U) and place global groups from any domain in universal groups
  3. Create Domain Local groups (DL) and add global and universal groups
  4. Assign Permissions (P) to the domain local groups

Group Strategies

User Accounts



A

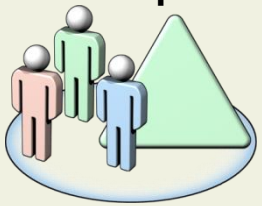
Global Groups

G

Universal Groups

U

Domain Local Groups

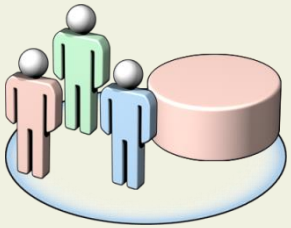


DL

Permissions

P

Local Groups



L

Group strategies:

- A G P
- A DL P
- A G DL P
- A G U DL P
- A G L P

View presentation

Best Practices for Managing Groups

- Create groups based on administrative needs
- Use local groups on a computer that is not a member of a domain
- Add user accounts to the group that is most restrictive
- Use the built-in group when possible instead of creating a new group
- Use the Authenticated Users group instead of the Everyone group to grant most user rights and permissions
- Limit the number of users in the Administrators group
- Trust all personnel that are members of the Administrators, Power Users, Print Operators, and Backup Operators groups

Summary

- Group accounts reduce administrative effort by enabling assignment of common rights and permissions to multiple users simultaneously
- Two group security types:
  1. Security groups
  2. Distribution groups
- Three types of scoping possible for groups
  1. Global groups
  2. Domain local groups
  3. Universal groups
- Group Strategies – A G DL P

Summary (continued)

- Group and computer accounts can be created and managed
  - From Active Directory Users and Computers
  - From command-line utilities
- Built-in and User groups and containers are automatically created at installation with specific pre-assigned rights and permissions
- Windows NT and above require computer accounts in Active Directory