

Chapter 7  
**WORKING WITH GROUPS**

---

---

---

---

---

---

---

---

**CHAPTER OVERVIEW**

- Understand the functions of groups and how to use them.
- Understand the difference between local groups and domain groups.
- Identify the two group types and three group scopes, and their proper use.
- List the predefined and built-in groups included in Windows Server 2003.

---

---

---

---

---

---

---

---

**CHAPTER OVERVIEW (continued)**

- Understand the difference between groups and special identities.
- Create, manage, and delete groups using graphical and command-line tools.

---

---

---

---

---

---

---

---

### ACL AND SECURITY PRINCIPLES

- Access control list restrict or permit access to resource objects
- Objects in the ACL are called security principles
- Examples of security principles
  - User account
  - Computer account
  - Group
  - Printer
  - Shared folders

---

---

---

---

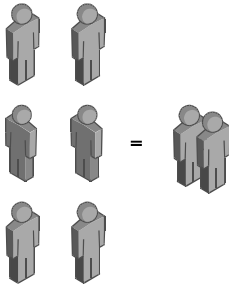
---

---

---

---

### UNDERSTANDING GROUPS



Example:  
Sales department resources  
Shared folders = 3  
Printers = 2  
Users = 15  
Per user permissions = 75  
Group = 1 [Sales]  
Group permission = 5

---

---

---

---

---

---

---

---

### USING GROUPS AND GROUP POLICIES

- Group policy and groups are not related.
- Group policy cannot be directly applied to a group, user and computer account object.
  - Group, user and computer account objects are security principals.
- Group policy is set on a site, domain, or OU
  - It can be configured to apply to groups in that site, domain, or OU.

---

---

---

---

---

---

---

---

### UNDERSTANDING DOMAIN FUNCTIONAL LEVELS

- Raising functional level action cannot be reversed
- Domain functional levels

#### Windows 2003:

- Windows 2003 domain controllers only.
- Universal security and distribution groups.
- Allows groups to be members of other groups.
- Allows group conversions (security and distribution).
- Allows migration of security principals from one domain to another domain (SID history).

---

---

---

---

---

---

---

---

### UNDERSTANDING DOMAIN FUNCTIONAL LEVELS (continued)

- Determines the level of functionality used by Active Directory
- Available levels depend on the operating system servers are running
- Some features are not available in certain levels
- Functional level can be raised but not lowered

---

---

---

---

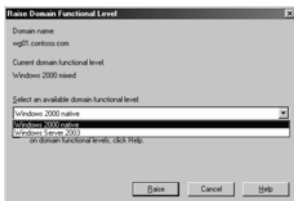
---

---

---

---

### RAISING THE DOMAIN FUNCTIONAL LEVEL



- Active Directory Domains and Trusts
- Right click
- Do not raise at this time

In addition to AD features, forest functional level allows domain rename.

---

---

---

---

---

---

---

---

### USING LOCAL GROUPS

- Can be used only on the system on which they are created
- In a workgroup environment, can contain only users from the local system
- In a domain environment, can contain users and global groups
- Cannot be created on a domain controller

---

---

---

---

---

---

---

---

### USING ACTIVE DIRECTORY GROUPS

- Group Types
  - Security
  - Distribution
- Group Scopes
  - Local
  - Global
  - Universal

Detail discussion on slides that follow

---

---

---

---

---

---

---

---

### GROUP TYPE: SECURITY GROUPS

- Used to assign access permissions for network resources.
- Membership depends on the type of security group and the domain functional level.
- Can also be used as a distribution group.
- The most common type of group created and used in Active Directory.

---

---

---

---

---

---

---

---

### GROUP TYPE: DISTRIBUTION GROUPS

- Cannot be used as security principals to grant permission to objects
- List of IDs used to group users together for use by applications in non-security-related functions
- Can be used only by directory-aware applications such as Microsoft Exchange
- Can be converted to a security group
- Security group can be used as distribution group, so distribution group may not be used

---

---

---

---

---

---

---

---

### GROUP SCOPES

- Domain local groups
  - Most often used to assign access permission to resources either directly or adding a global group to a domain local group.
- Global groups
  - Used primarily to provide categorized membership in domain local groups for individual security principals or for direct permission assignment.
  - Used to collect users or computers in the same domain that share the same job, role or function or that have similar network access requirements.
- Universal groups
  - Used primarily to grant access to resources in multiple domains.

---

---

---

---

---

---

---

---

### GROUP SCOPE: DOMAIN LOCAL GROUPS

- Available in all domain functional levels
- Can only be used to assign permissions to resources in the domain where they are created
- Membership depends on domain functional level
  - W2K mixed or W2K3 interim can include
    - User and computer accounts, and global groups from any domain in forest
    - No other group nesting
  - W2K native or W2K3 can include
    - User and computer accounts, global and universal groups from any domain in forest.
    - Can convert to universal scope if contains no domain local groups as members.

---

---

---

---

---

---

---

---

### GROUP SCOPE: GLOBAL GROUPS

- Available in all functional levels
- Can be converted to universal group as long as it is not a member of any other global group
- Can be member of machine local or domain local groups
- Can only include members from within their domain
- Membership depends on domain functional level
  - W2K native or W2K3 global group members can include user and computer account, and other global groups from the same domain
  - W2K mixed user and computer account from the same domain
- Can be granted access permissions to resources in any domain in the forest, and in domains in other trusted forests

---

---

---

---

---

---

---

---

---

---

### GROUP SCOPE: UNIVERSAL GROUPS

- Available only in the Windows 2000 native and Windows Server 2003 domain functional levels
- Can include user and computer accounts, global groups, and other universal group from any domain in the forest
- Can be granted access permissions for resources in any domain in the forest, and in domains in other trusted forests
- Can be converted to domain local groups or to global groups, as long as they do not have other universal groups as members
- Generally used to consolidate groups that span multiple domains

---

---

---

---

---

---

---

---

---

---

### NESTING GROUPS

	Members Allowed in Windows 2000 Mixed or Windows Server 2003	Members Allowed in Windows 2000 Native or Windows Server 2003
<b>Group Scope</b>	<b>Interim Functional Level</b>	<b>Functional Level</b>
Domain Local	User and computer accounts and global groups from any domain	User and computer accounts, universal groups, and global groups from any domain; other domain local groups from the same domain
Global	User and computer accounts from the same domain	User and computer accounts and other global groups from the same domain
Universal	Not available	User and computer accounts, other universal groups, and global groups from any domain

---

---

---

---

---

---

---

---

---

---

### CONVERTING GROUPS

	To Domain Local	To Global	To Universal
From Domain Local	Not applicable	Not permitted	Permitted only when the domain local group does not have other domain local groups as members
From Global	Not permitted	Not applicable	Permitted only when the global group is not a member of another global group
From Universal	No restrictions	Permitted only when the universal group does not have other universal groups as members	Not applicable

You may need to convert groups..... What you can do.....

---

---

---

---

---

---

---

---

### PLANNING GLOBAL AND DOMAIN LOCAL GROUPS

- Step 1—Create domain local groups for resources to be shared.
- Step 2—Assign resource permissions to the domain local group.
- Step 3—Create global groups for users with common job responsibilities.
- Step 4—Add global groups that need access to resources to the appropriate domain local group.

Best Practices.....

---

---

---

---

---

---

---

---

### WINDOWS SERVER 2003 DEFAULT GROUPS

- Built-in local groups
- Predefined Active Directory groups
- Built-in Active Directory groups
- Special identities

Refer to your textbook for the list.....

---

---

---

---

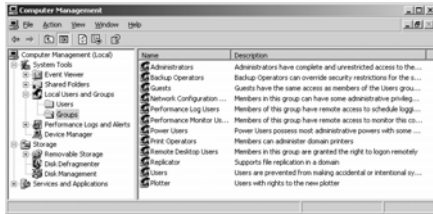
---

---

---

---

### BUILT-IN LOCAL GROUPS



---

---

---

---

---

---

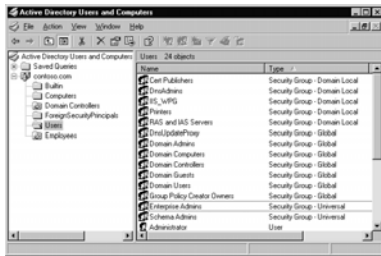
---

---

---

---

### PREDEFINED ACTIVE DIRECTORY GROUPS



Enterprise & Schema Admins appear in the first forest DC

---

---

---

---

---

---

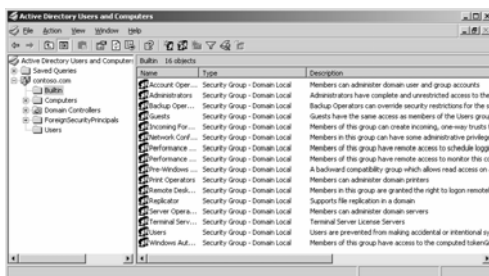
---

---

---

---

### BUILT-IN ACTIVE DIRECTORY GROUPS



---

---

---

---

---

---

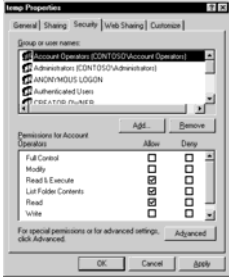
---

---

---

---

### SPECIAL IDENTITIES



- Member cannot be added directly but by action or access – Example: Authenticated Users

---

---

---

---

---

---

---

---

---

---

### CREATING AND MANAGING GROUP OBJECTS

- Creating local groups
- Creating security groups in Active Directory.

---

---

---

---

---

---

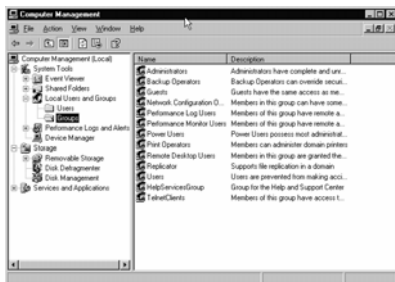
---

---

---

---

### CREATING LOCAL GROUPS



---

---

---

---

---

---

---

---

---

---

### WORKING WITH ACTIVE DIRECTORY GROUPS

- Creating security groups
- Managing group membership
- Nesting groups
- Changing group types and scopes
- Deleting a group

---

---

---

---

---

---

---

---

### CREATING SECURITY GROUPS



---

---

---

---

---

---

---

---

### MANAGING GROUP MEMBERSHIP



---

---

---

---

---

---

---

---

### NESTING GROUPS

- Both groups must be created separately, and then one is made a member of the other.
- Possible nestings depend on the domain functional level and scope type.
- Observe rules on group nesting.

---

---

---

---

---

---

---

---

### CHANGING GROUP TYPES AND SCOPES



---

---

---

---

---

---

---

---

### DELETING A GROUP

- Deletes only the group object, not the members of the group.
- Deletes the SID for the group. The SID cannot be re-created.
- Removes ACL entries for the group.

---

---

---

---

---

---

---

---

### AUTOMATING GROUP MANAGEMENT

The following command-line utilities can be used in scripts and batch files to automate group management:

- Dsadd.exe: Used to create new group objects
- Dsmod.exe: Used to configure existing group objects
- Dsget.exe: Used to locate groups in Active Directory

---

---

---

---

---

---

---

---

### CREATING GROUP OBJECTS WITH DSADD.EXE

- Allows groups to be created from a command line
- Useful when scripting group creation for large numbers of groups
- Can be used only to create new groups, not modify existing groups

---

---

---

---

---

---

---

---

### MANAGING GROUP OBJECTS WITH DSMOD.EXE

Can be used to configure group objects, including:

- Setting the group scope
- Adding and removing individual group members
- Replacing the entire group membership

---

---

---

---

---

---

---

---

### FINDING OBJECTS WITH DSGET.EXE

- Command-line utility
- Used to locate and show information on an object
- Cannot be used to create, modify, or delete an object

---

---

---

---

---

---

---

---

### SUMMARY

- A group is an object that consists of a list of users.
- All permissions assigned to the group are inherited by its members.
- The domain functional level determines which group types and scopes you can use, which groups can be nested, and which group conversions you can perform.
- Security groups can be assigned permissions, while distribution groups are used for query containers, such as e-mail distribution groups, and cannot be assigned permissions to a resource.

---

---

---

---

---

---

---

---

### SUMMARY (continued)

- Domain local groups are used for assigning permissions to resources. Global groups are used for gathering together users with similar resource requirements. Universal groups are used primarily to grant access to related resources in multiple domains.
- You can create domain groups in any container or OU in the Active Directory tree.

---

---

---

---

---

---

---

---

SUMMARY (continued)

- Group nesting refers to the ability to make one group a member of another group.
- Command-line tools such as Dsadd.exe, Dsmode.exe, and Dsget.exe allow you to automate group management tasks.

---

---

---

---

---

---

---

---