# CSI3670
# A Bit More on Containers

Erik Fredericks (fredericks@oakland.edu)

# Organizational Units (AD)

Containers

- Other OUs
- Computers
- Users
- Groups
- Etc.

Why an OU?

- Delegation
- Managing GPOs
- (Less overhead / possible complexities than domains)

# So what are AD Groups?

Collection of users/computers/devices
- Not strictly an AD container
  - (Again, can’t apply a GPO to a group)
  - (But you can force a group to participate in a GPO)

What do groups get us?
- Can assign permissions to group
- Delegate user rights
- etc.

# Types of Groups

- Default groups
  - Built-in to AD
    - Domain Admins, Enterprise Admins, Users, etc.
    - Give appropriate permissions to objects in group

    - E.g., Enterprise Admin can do *anything* to any device within AD-scope

- Custom groups
  - Defined by you
  - Including policies/permissions/etc

# Group Scope

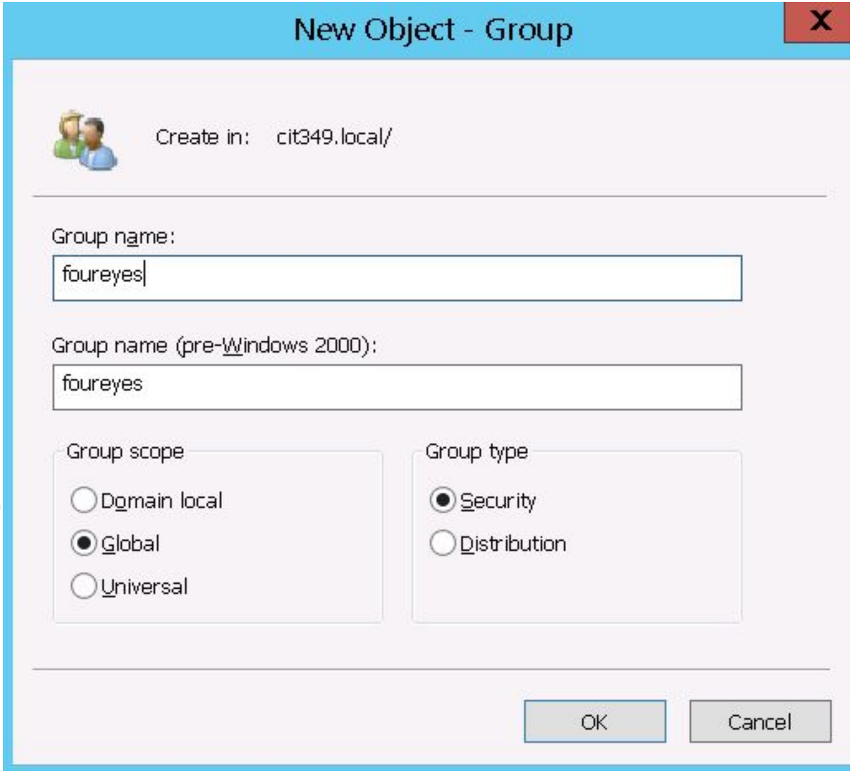
Domain local

- Only assigned permissions within domain

Who can be domain local

- Other domain local groups (same domain)
- Global groups (any domain)
- Universal groups (any domain)
- User accounts (any domain)

➜ Only visible within domain



New Object - Group

Create in: cit349.local/

Group name: foureyes

Group name (pre-Windows 2000): foureyes

Group scope

○ Domain local
● Global
○ Universal

Group type

● Security
○ Distribution

# Group Scope

Global

- Forest-wide scope
- Any resource in any domain *within forest*

Who can participate?

- Global groups (same domain)
- User accounts (same domain)

➡ Visible throughout forest, but same domain

- ➡ Employees who share job descriptions / departments

# Group Scope

Universal

- Can include member from any domain in forest
- Only use when users/groups requires access to *shared resources*

➡ Generally used for nesting global groups

# Group Type

Select after defining a group

Security

- Assigned permissions

Distribution

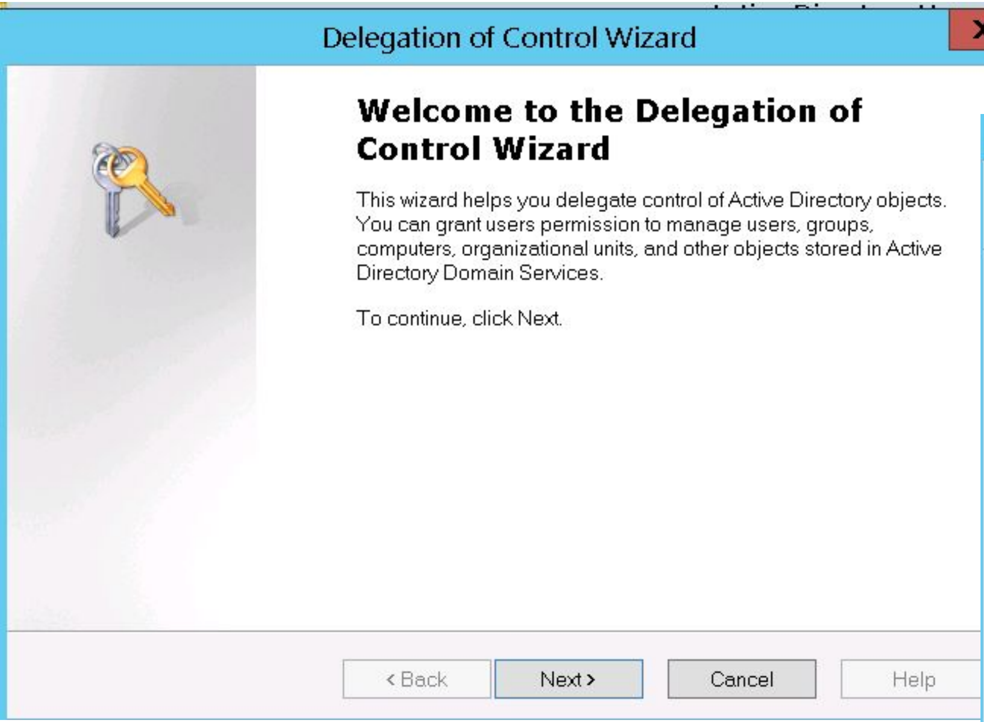
- Email lists (cannot be assigned permissions)

# Domain vs. Group vs. Organizational Unit

Domain ➔ Security boundary
Group ➔ Collections of users/devices
Organizational unit ➔ Organize AD objects

Why use an OU?

1) Easy application of GPOs
2) Can delegate tasks to OU
   For example, assume your group has a helpdesk
   You need to be able to reset user accounts/passwords
      …I don’t want to do that for you
      …So, I’ll delegate that task to you
         (Not as easy to apply to a group)
3) Reasonable boundary

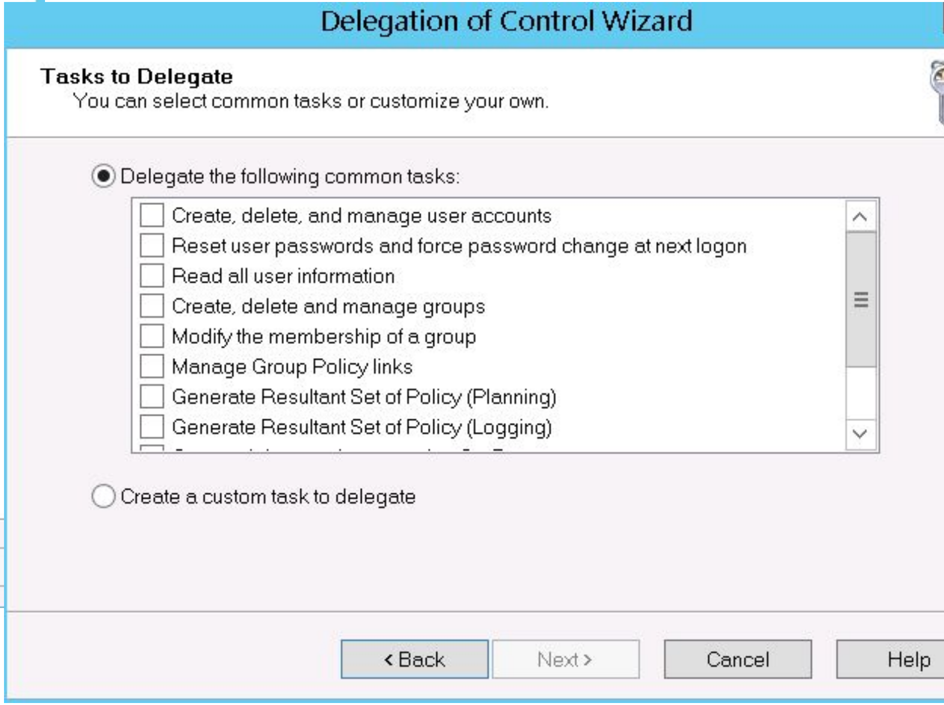


Delegation of Control Wizard

## Welcome to the Delegation of Control Wizard

This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory Domain Services.

To continue, click Next.



Delegation of Control Wizard

**Tasks to Delegate**
You can select common tasks or customize your own.

● Delegate the following common tasks:

- □ Create, delete, and manage user accounts
- □ Reset user passwords and force password change at next logon
- □ Read all user information
- □ Create, delete and manage groups
- □ Modify the membership of a group
- □ Manage Group Policy links
- □ Generate Resultant Set of Policy (Planning)
- □ Generate Resultant Set of Policy (Logging)

○ Create a custom task to delegate

# Applying GPO to OU

Create a GPO as before

Right-click on OU instead of domain

- Link Existing GPO

Or

Locate OU

- Right-click and Add New GPO