Lesson 15: Creating and Managing Active Directory Groups and Organizational Units

MOAC 70-410: Installing and Configuring Windows Server 2012

Microsoft Official Academic Course

WILEY

Overview

- Exam Objective 5.3: Create and Manage Active Directory Groups and Organizational Units (OUs)
- Designing an Internal Domain Structure
- Working with Organizational Units
- Working with Groups

Designing an Internal Domain Structure

Lesson 15: Creating and Managing Active Directory Groups and Organizational Units

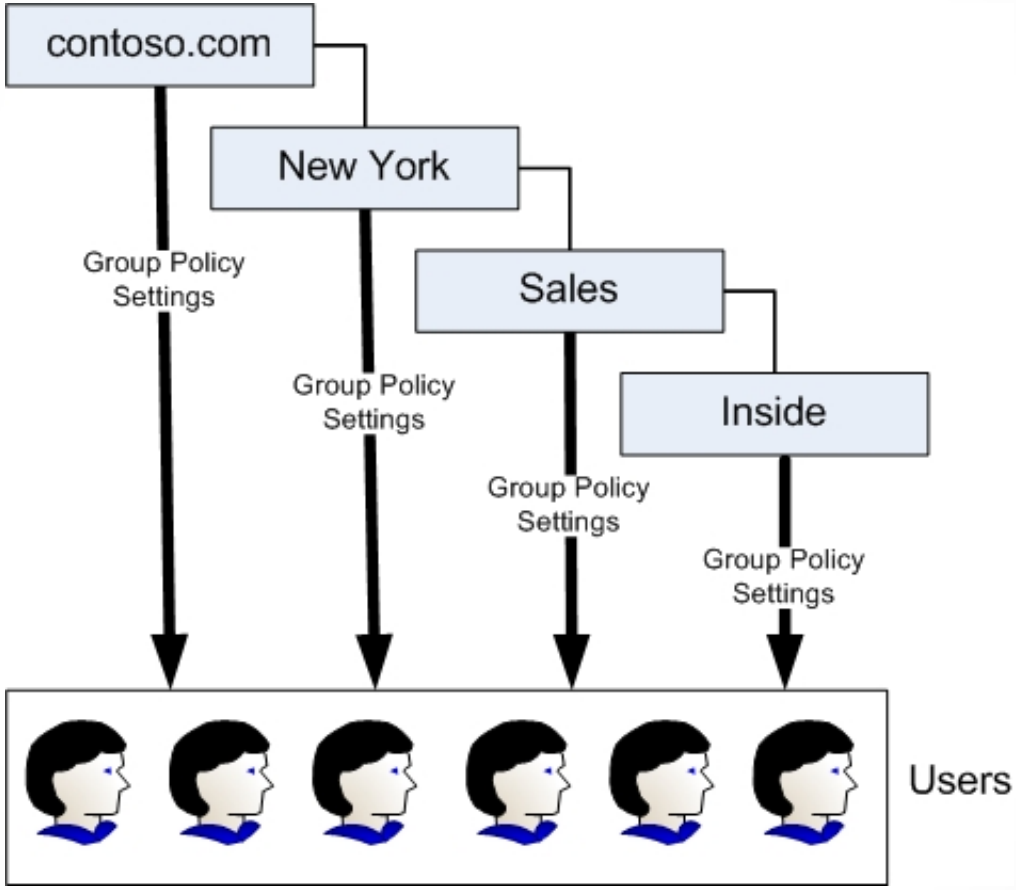
Designing an Internal Domain Structure

- Within a domain, the primary hierarchical building block is the organizational unit (OU).
- It is easier to build an Active Directory hierarchy using OUs than it is using domains.
- It is a simple matter to create new OUs, rename existing ones, and move them around.
- Creating a new domain means deploying additional domain controllers, and while it is possible to rename a domain, it is not a simple process.

Inheritance

- When you assign Group Policy settings to a domain, the settings apply to all of the objects in that domain, but not to the subdomains.
- when you assign Group Policy settings to an OU, those settings apply to all of the leaf objects in the OU and are inherited by any subordinate OUs it contains.

Inheritance



Group Policy inheritance within a domain

Using Organizational Units

Reasons for creating an OU:

- **Duplicating organizational divisions**: The structure of OUs within your domains should be an extension of the model you used to design the Active Directory domain structure:
  - Geographical
  - Departmental
  - Political
- **Assigning Group Policy settings**: To assign different Group Policy settings to a particular collection of objects.
- **Delegating administration**: To grant certain individuals administrative responsibility for a portion of the Active Directory hierarchy, without giving them full access to the entire domain.

Using Group Objects

- Create a group when you want to grant a collection of users permission to access a network resource, such as a file system share or a printer.
- Groups are not part of the AD hierarchy.
- members of a group inherit any permissions that you assign to the group, but they do not inherit the Group Policy settings from the group's parent OUs and domain.

Working with Organizational Units

Lesson 15: Creating and Managing Active Directory Groups and Organizational Units

Working with Organizational Units

- OUs can be nested to create a design that enables administrators to take advantage of inheritance.
- Limit the number of OUs that are nested, because too many levels can:
  - Slow the response time to resource requests
  - Complicate the application of Group Policy settings

Working with Organizational Units

- There is only one built-in OU by default: the **Domain Controllers OU**.
- All other OUs must be created by the domain administrator.

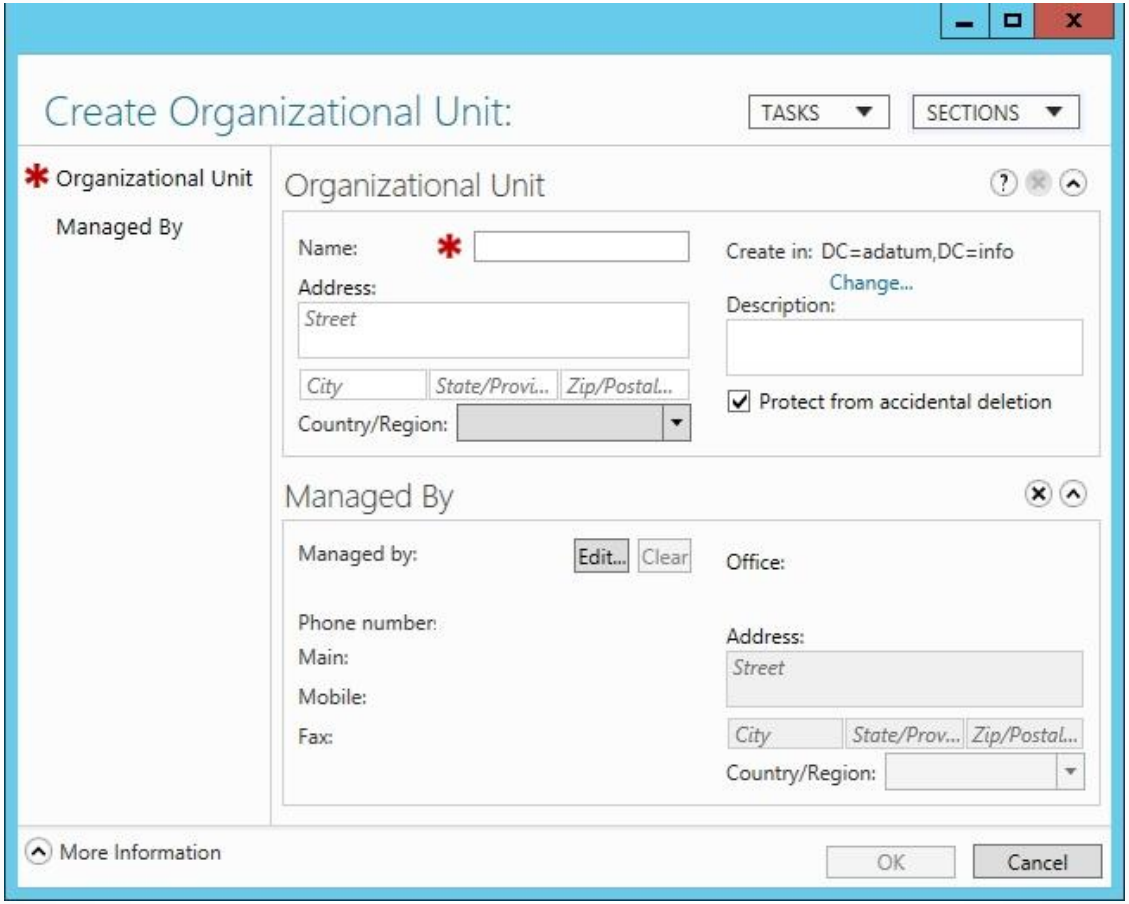
Containers

Default container objects:

- **Users:** Contains the domain's predefined users and groups.
- **Computer:** Contains computer objects in the domain.

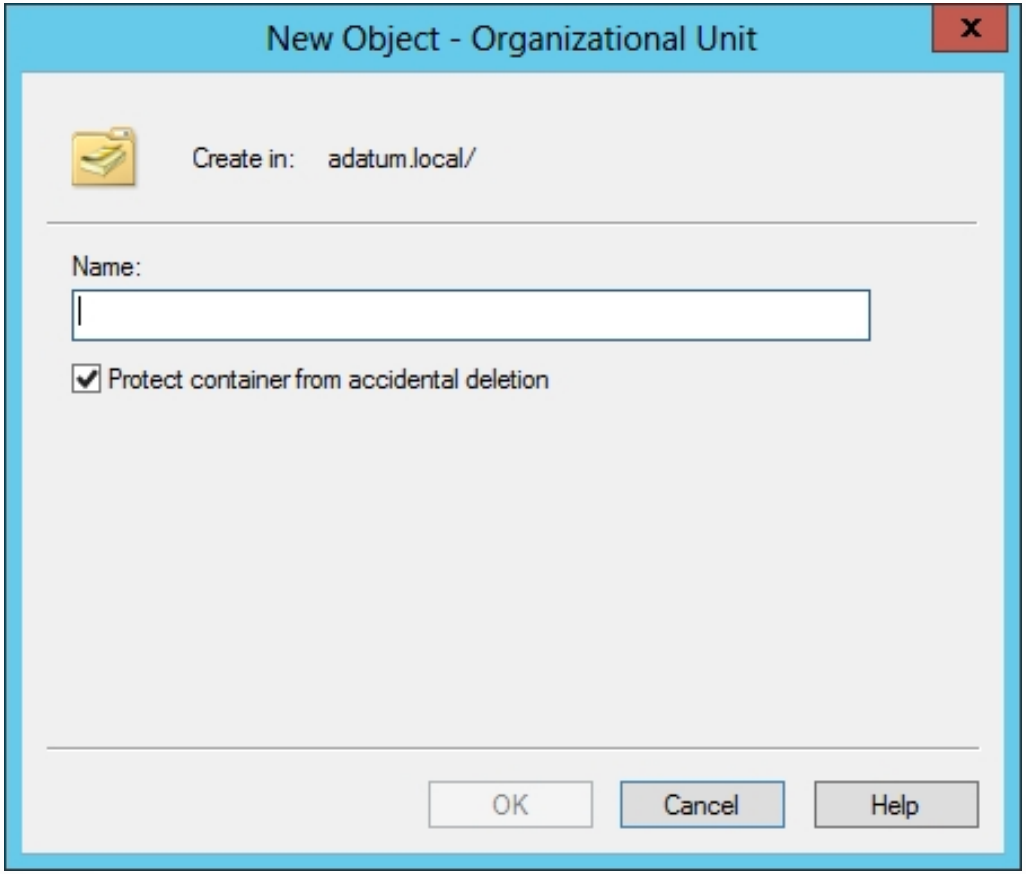
You cannot assign Group Policy settings to computer objects or delegate their administration.

Creating OUs



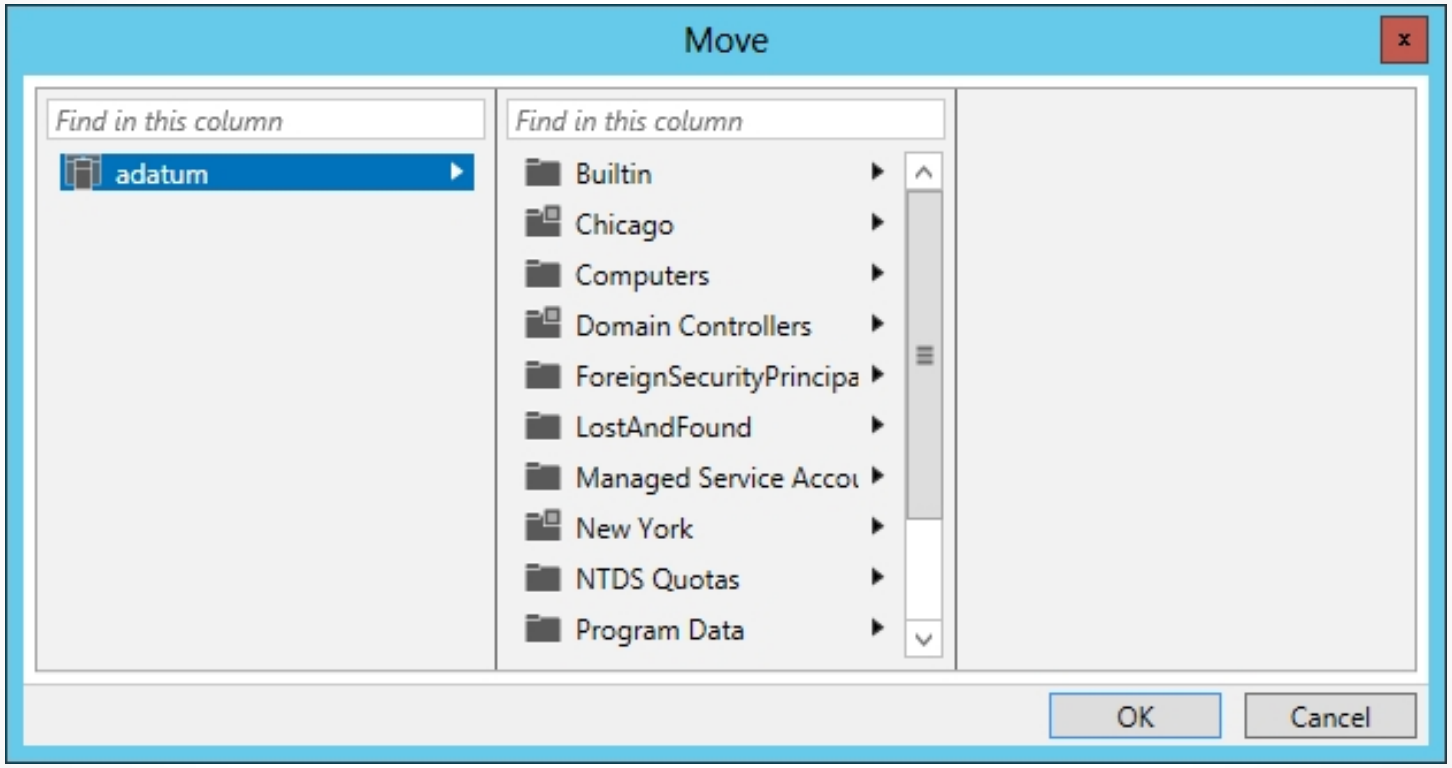
The Create Organizational Unit window in the Active Directory Administrative Center console

Creating OUs



The New Object – Organizational Unit dialog box in the Active Directory Users and Computers console

Creating OUs



The Move dialog box in the Active Directory Administrative Center console

Using OUs to Delegate AD Management Tasks

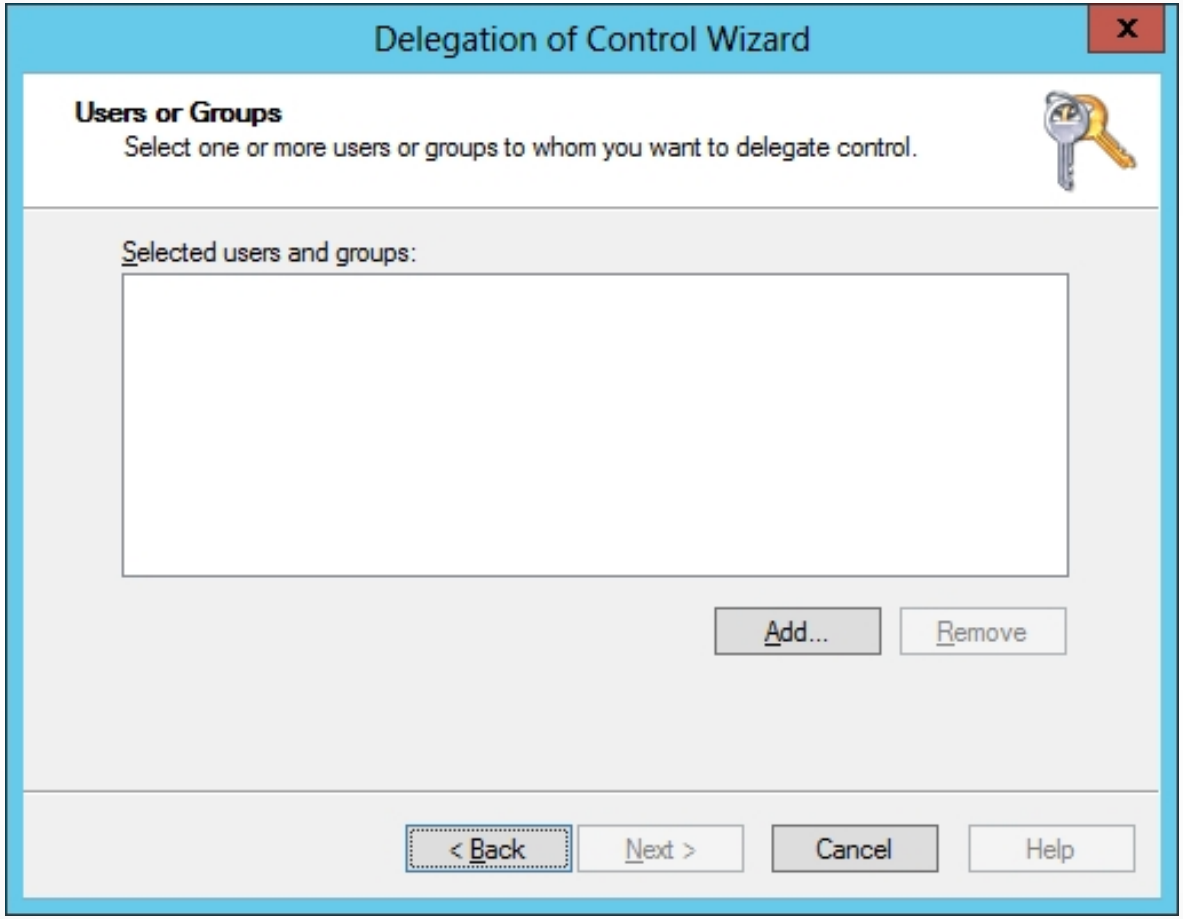
- Creating OUs enables you to implement a decentralized administration model, in which others manage portions of the AD DS hierarchy, without affecting the rest of the structure.
- Delegating authority at a site level affects all domains and users within the site.
- Delegating authority at the domain level affects the entire domain.
- Delegating authority at the OU level affects only that OU and its subordinate objects.

Using OUs to Delegate AD Management Tasks

By granting administrative authority over an OU structure, as opposed to an entire domain or site, you gain the following advantages:

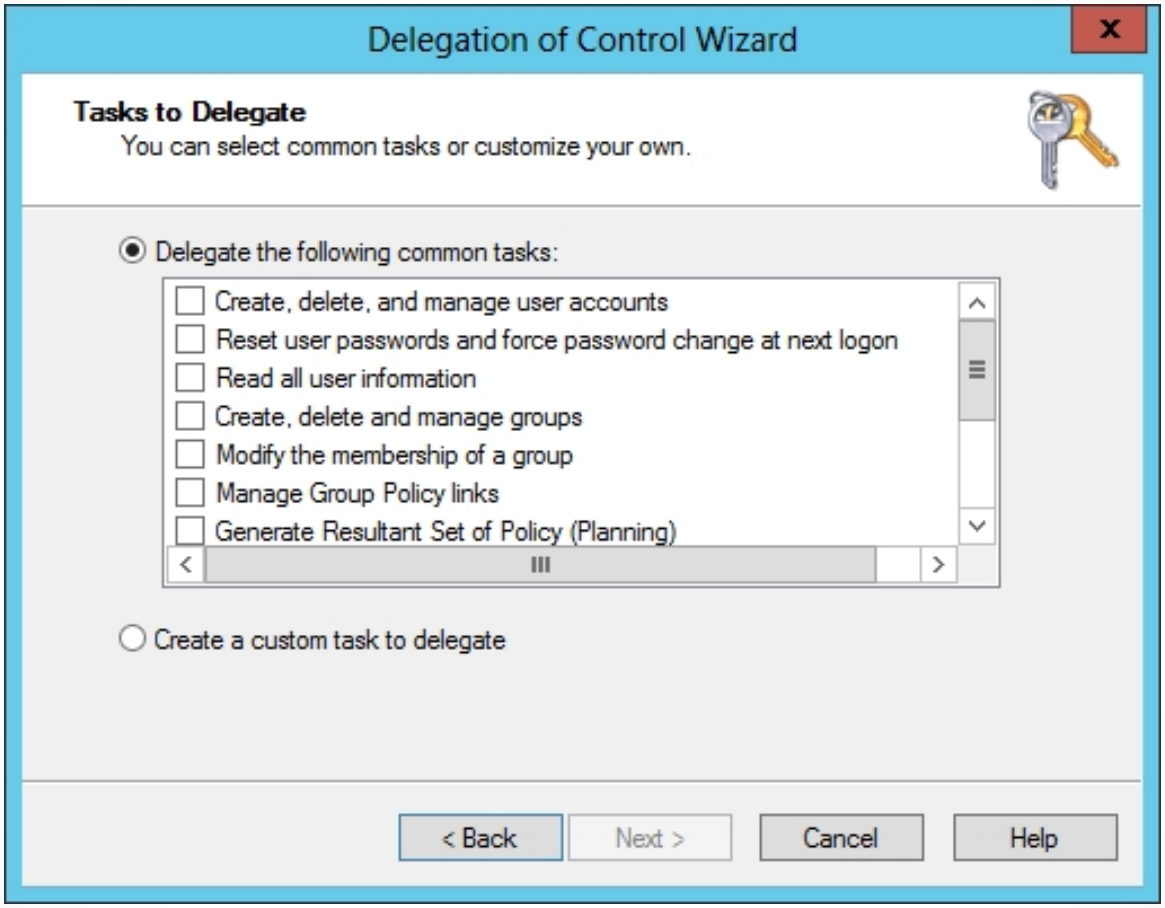
- **Minimal number of administrators with global privileges:** By creating a hierarchy of administrative levels, you limit the number of people who require global access.
- **Limited scope of errors:** Administrative mistakes such as a container deletion or group object deletion affect only the respective OU structure.

Delegate Administrative Control of an OU



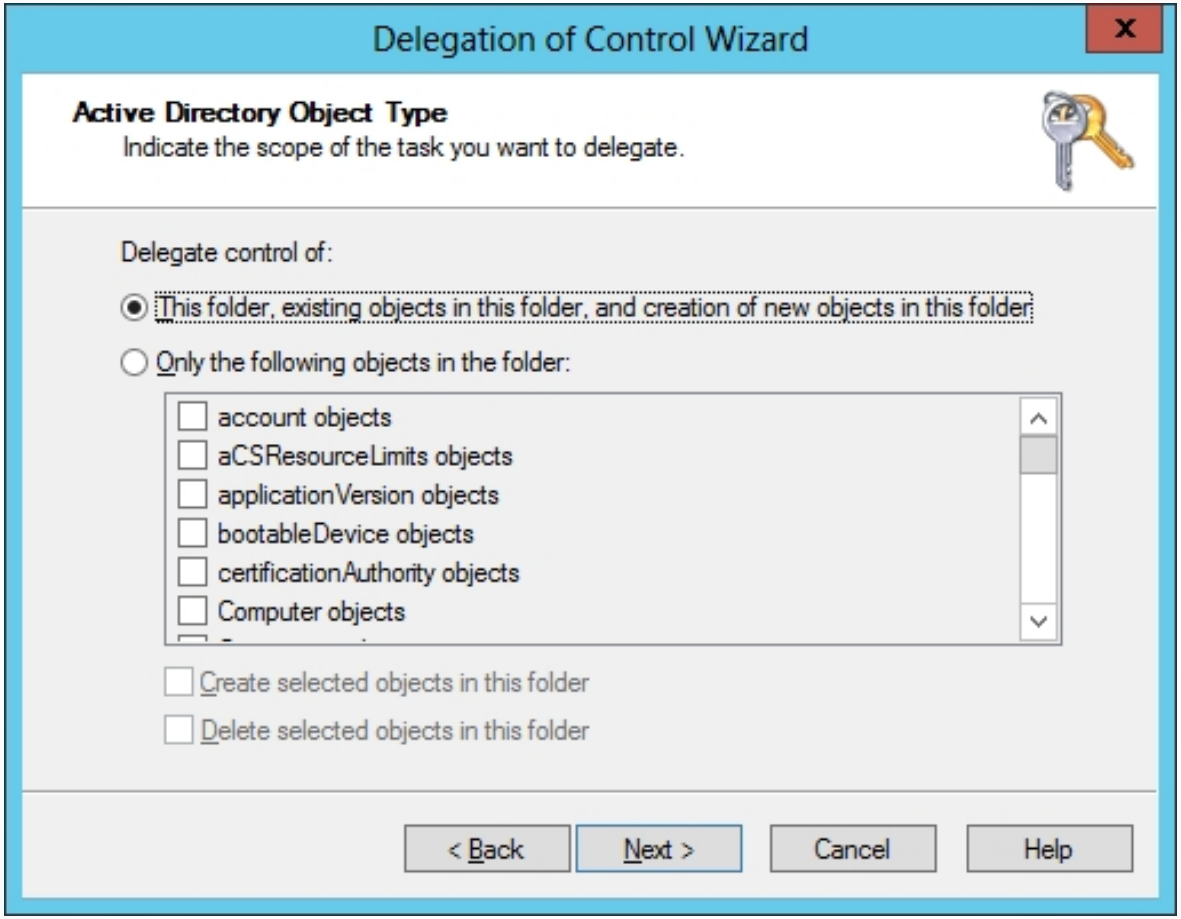
The Users or Groups page of the Delegation of Control Wizard

Delegate Administrative Control of an OU



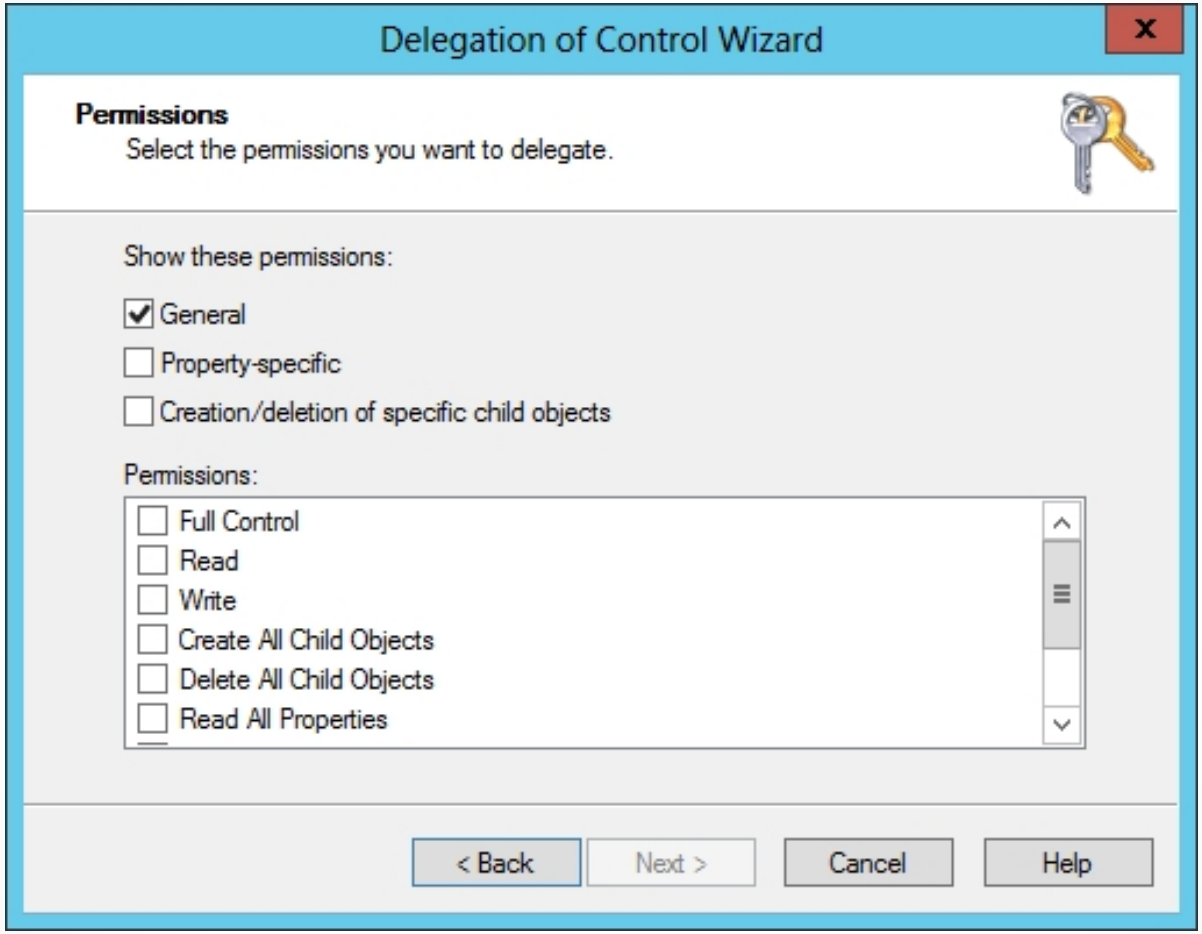
The Tasks to Delegate page of the Delegation of Control Wizard

Delegate Administrative Control of an OU



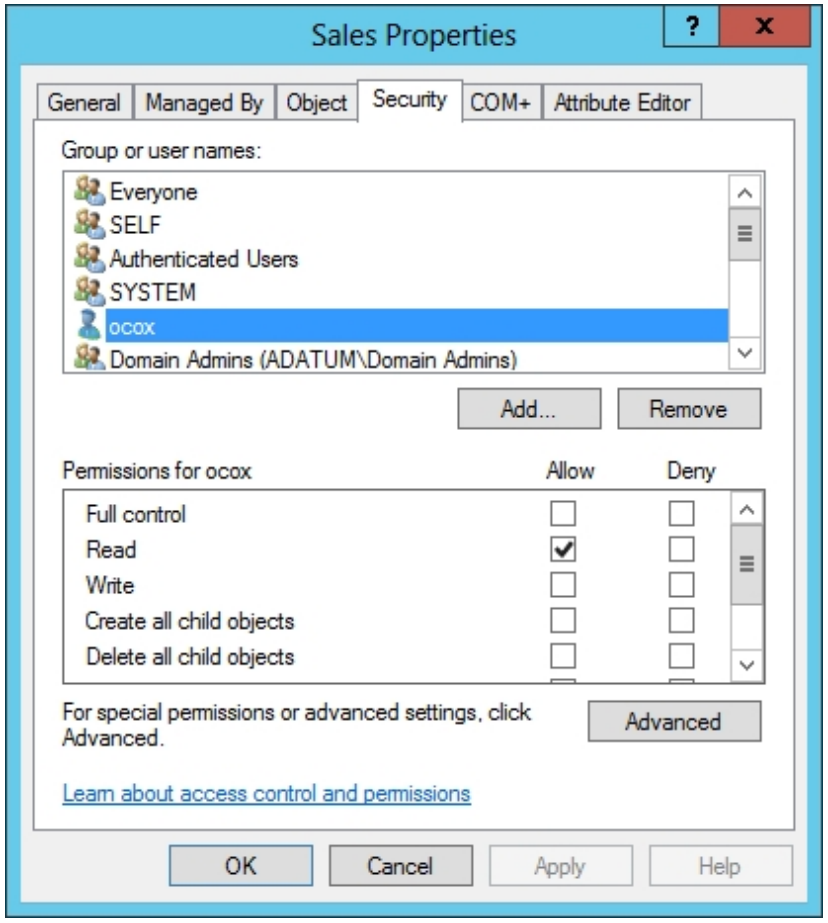
The Active Directory Object Type page of the Delegation of Control Wizard

Delegate Administrative Control of an OU



The Permissions page of the Delegation of Control Wizard

Delegate Administrative Control of an OU

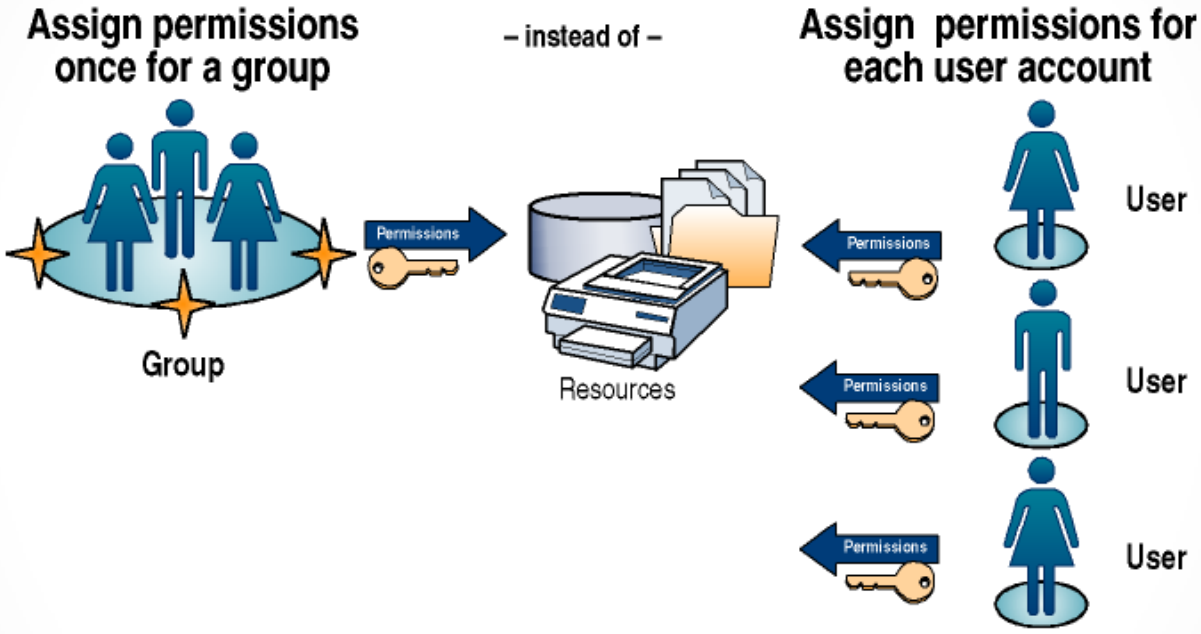


The Security tab of an organizational unit's Properties sheet

Working with Groups

Lesson 15: Creating and Managing Active Directory Groups and Organizational Units

Working with Groups



- Groups are collections of user accounts.
- Members receive permissions given to groups.
- Users can be members of multiple groups.
- Groups can be members of other groups.

Group Types

There are two Windows Server 2012 group types:

- **Distribution groups:** Non-security-related groups created for the distribution of information to one or more persons.
- **Security groups:** Security-related groups created for purposes of granting resource access permissions to multiple users.

Group Scopes

- The **group scope** controls which objects the group can contain.
- Limits the objects to the same domain or permits objects from remote domains.
- Controls the location in the domain or forest where the group can be used.
- Group scopes available in an Active Directory domain include **domain local groups**, **global groups**, and **universal groups.**

Domain Local Groups

Domain local groups can have any of the following as members:

- User accounts
- Computer accounts
- Global groups from any domain in the forest
- Universal groups
- Domain local groups from the same domain

Global Groups

Global groups can have the following as members:

- User accounts
- Computer accounts
- Other global groups from the same domain

Universal Groups

Universal groups can contain the following members:

- User accounts
- Computer accounts
- Global groups from any domain in the forest
- Other universal groups

Default Groups

- Several built-in security groups are created when you install AD DS.
- Many of the built-in groups have predefined user rights that enable their members to perform certain system-related tasks, such as backup and restore.
- Add accounts to these default groups to grant users the same rights, in addition to any resource access permissions the groups possess.
- The default groups are located in the Built-in and Users container objects in AD DS.
- The list of predefined groups you see in these containers varies depending on the installed services.

Nesting Groups

Group nesting is the term used when groups are added as members of other groups.

To allow users from multiple domains to access a resource in the parent domain:

1. Create global groups in each domain that contain all users needing access to the enterprise database.
2. Create a universal group in the parent domain. Include each location's global group as a member.
3. Add the universal group to the required domain local group to assign the necessary permission to access and use the enterprise database.

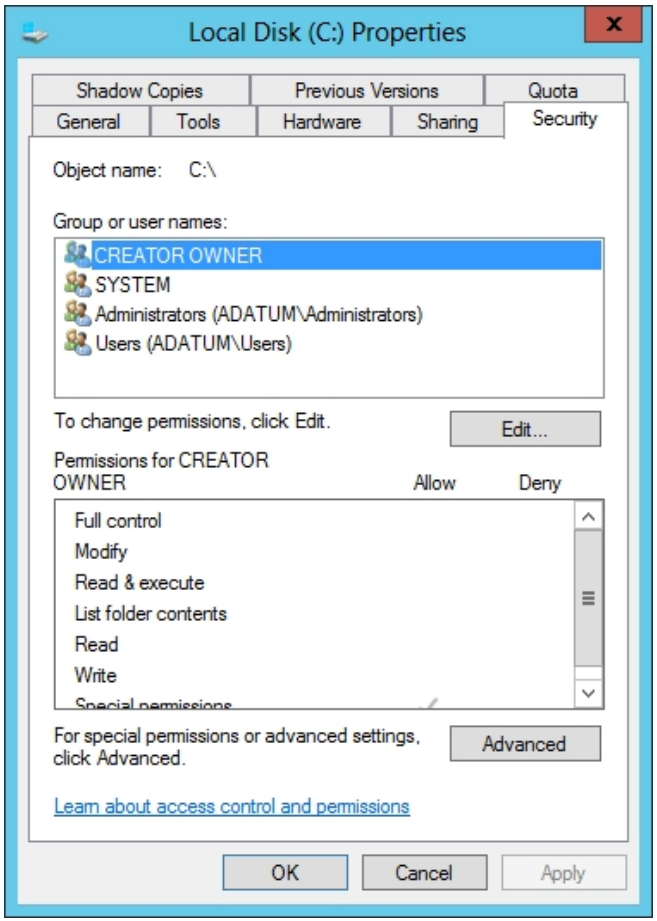
Active Directory Management Roles

Service Management Roles	***Data Management Roles***
Forest Configuration Operators	Business Unit Administrators
Domain Configuration Operators	Account Administrators
Security Policy Administrators	Workstation Administrators
Service Administration Managers	Server Operators
Domain Controller Administrators	Resource Administrators
Backup Operators	Security Group Administrators
Schema Administrators	Help Desk Operators
Replication Management Administrators	Application-Specific Administrators
Replication Monitoring Operators	
DNS Administrators	

Special Identities

- **Special identities** exist on all computers running Windows Server 2012.
- They are not groups because you cannot create them, delete them, or directly modify their memberships.
- They do not appear as manageable objects in the AD DS utilities.
- You can use them like groups, by adding them to the ACLs of system and network resources.

Special Identities

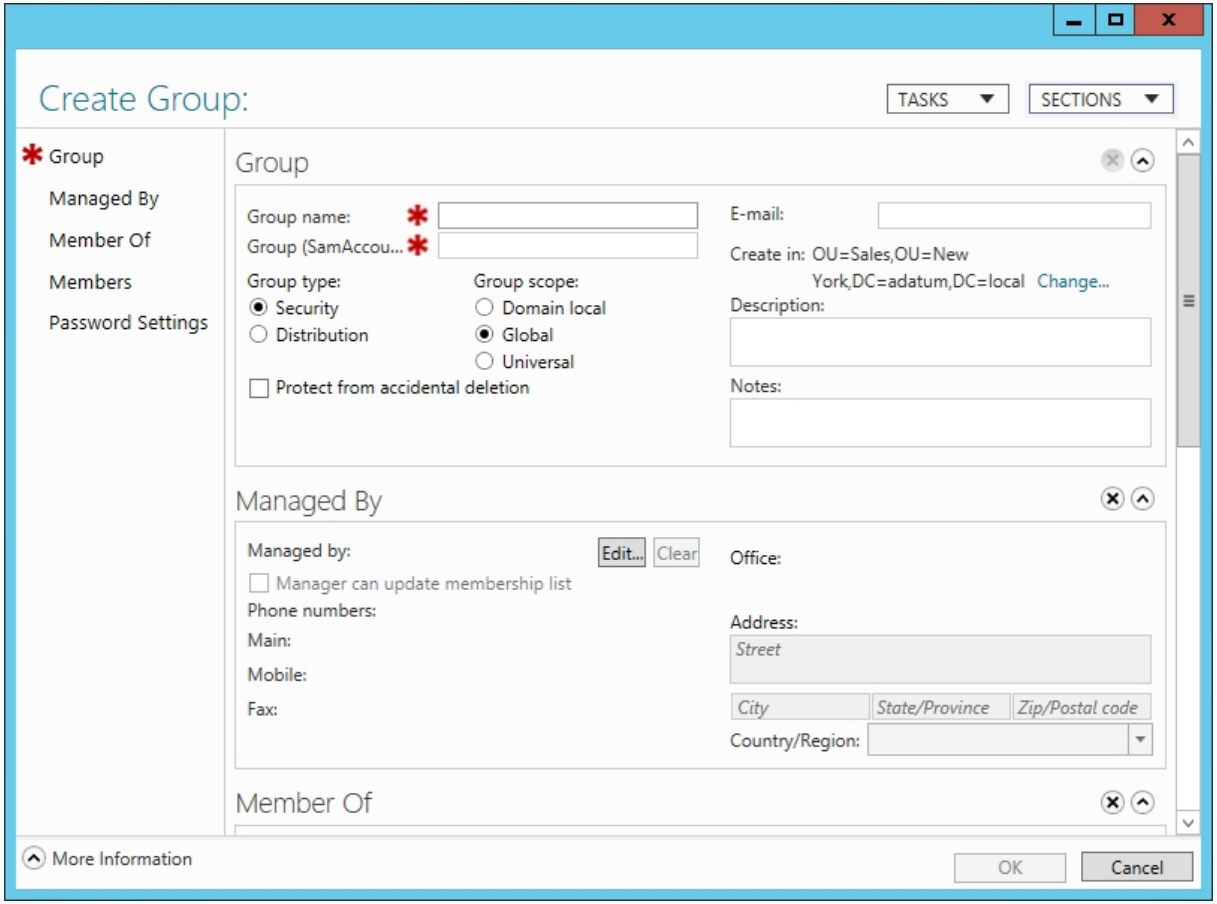


The Creator Owner special identity on a Security tab

Some Special Identities

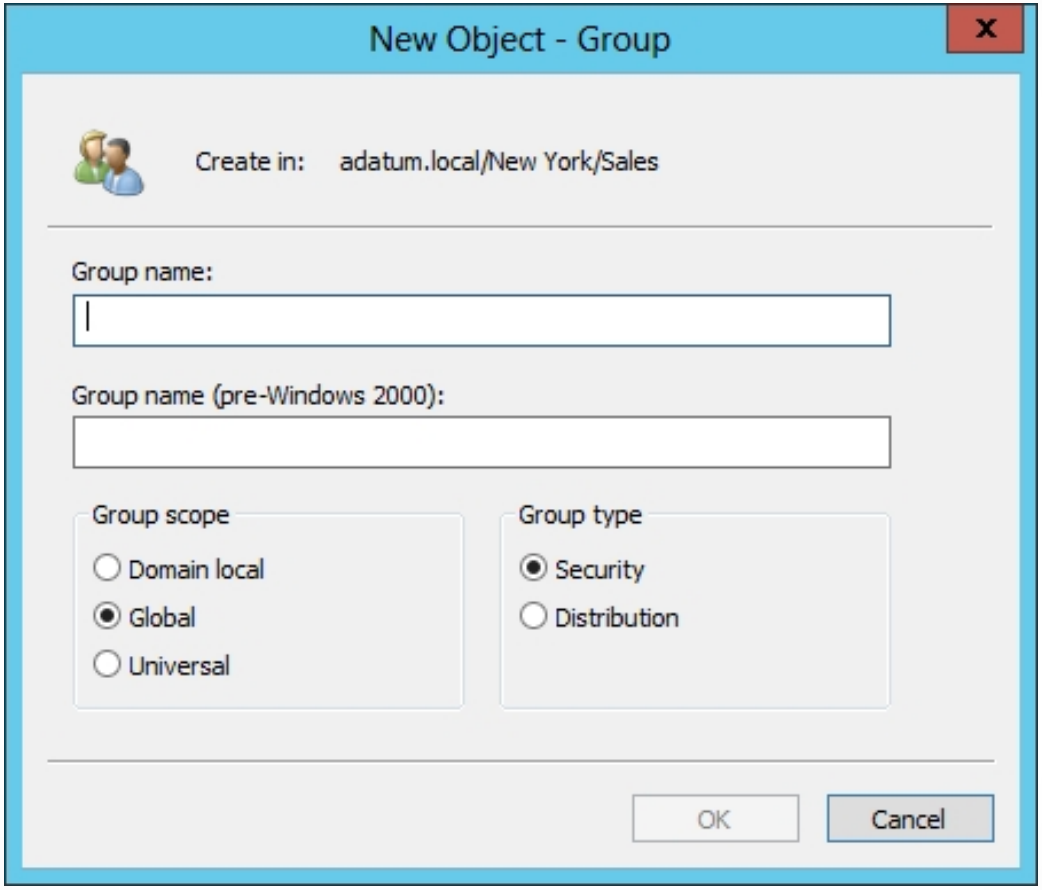
- **Authenticated Users:** All users with a valid local or domain user account whose identities have been authenticated. This special identity does not include the Guest user even if the Guest account has a password.
- **Creator Owner:** The account for the user who created or took ownership of a resource.
- **Dialup:** All users who are currently logged on through a dial-up connection.
- **Everyone:** The Authenticated Users special identity plus the Guest user account, but not the Anonymous Logon special identity.
- **Interactive:** All users who are currently logged on locally or through a Remote Desktop connection.
- **Network:** All users who are currently logged on through a network connection.
- **Remote Desktop Users:** When installed in application serving mode, this identity includes any users who are currently logged on to the system using an RDS terminal server.

Creating Groups



Creating a group in Active Directory Administrative Center

Creating Groups



The New Object – Group dialog box

Creating Groups from the Command Line

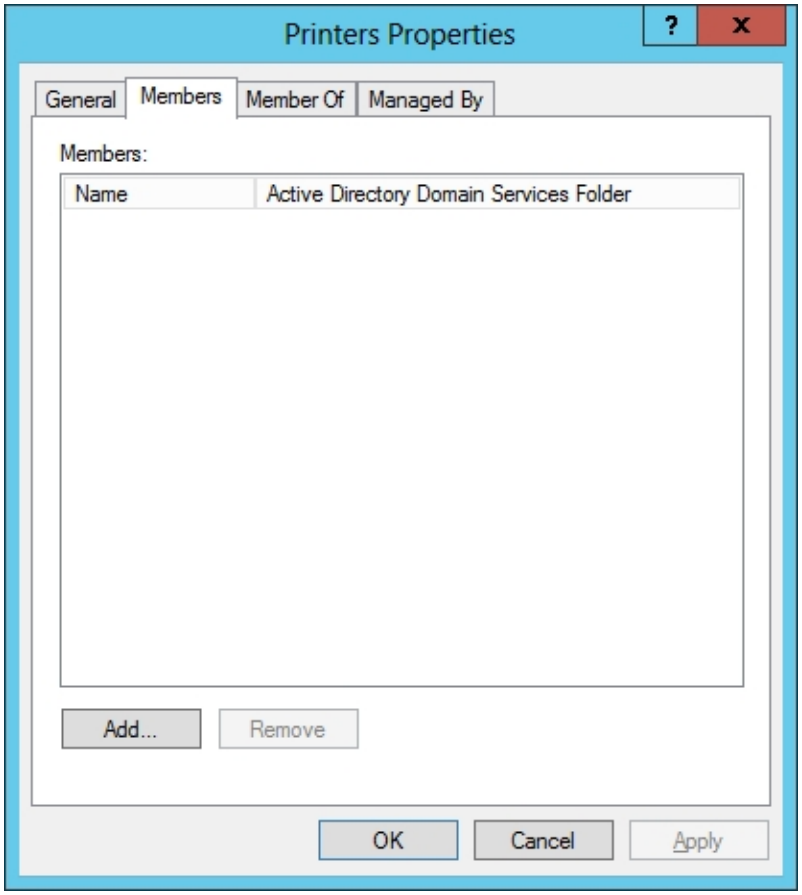
The basic syntax for creating group objects with **Dsadd.exe** is as follows:

```
dsadd group <GroupDN> [parameters]
```

To create a new group object using **Windows PowerShell**, you use the New-ADGroup cmdlet, with the following syntax:

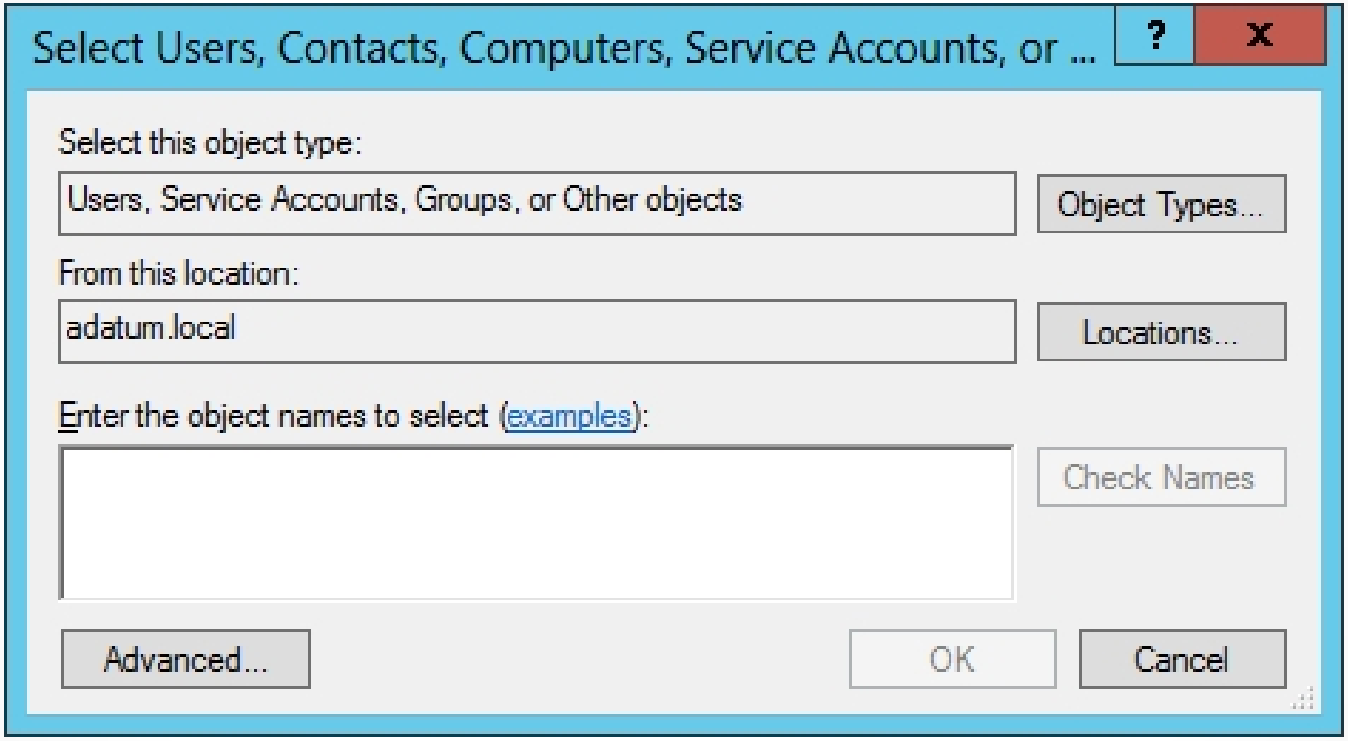
```
New-ADGroup
   -Name <group name>
   -SamAccountName <SAM name>
   -GroupCategory Distribution|Category
   -GroupScope DomainLocal|Global|Universal
   -Path <distinguished name>
```

Managing Group Memberships



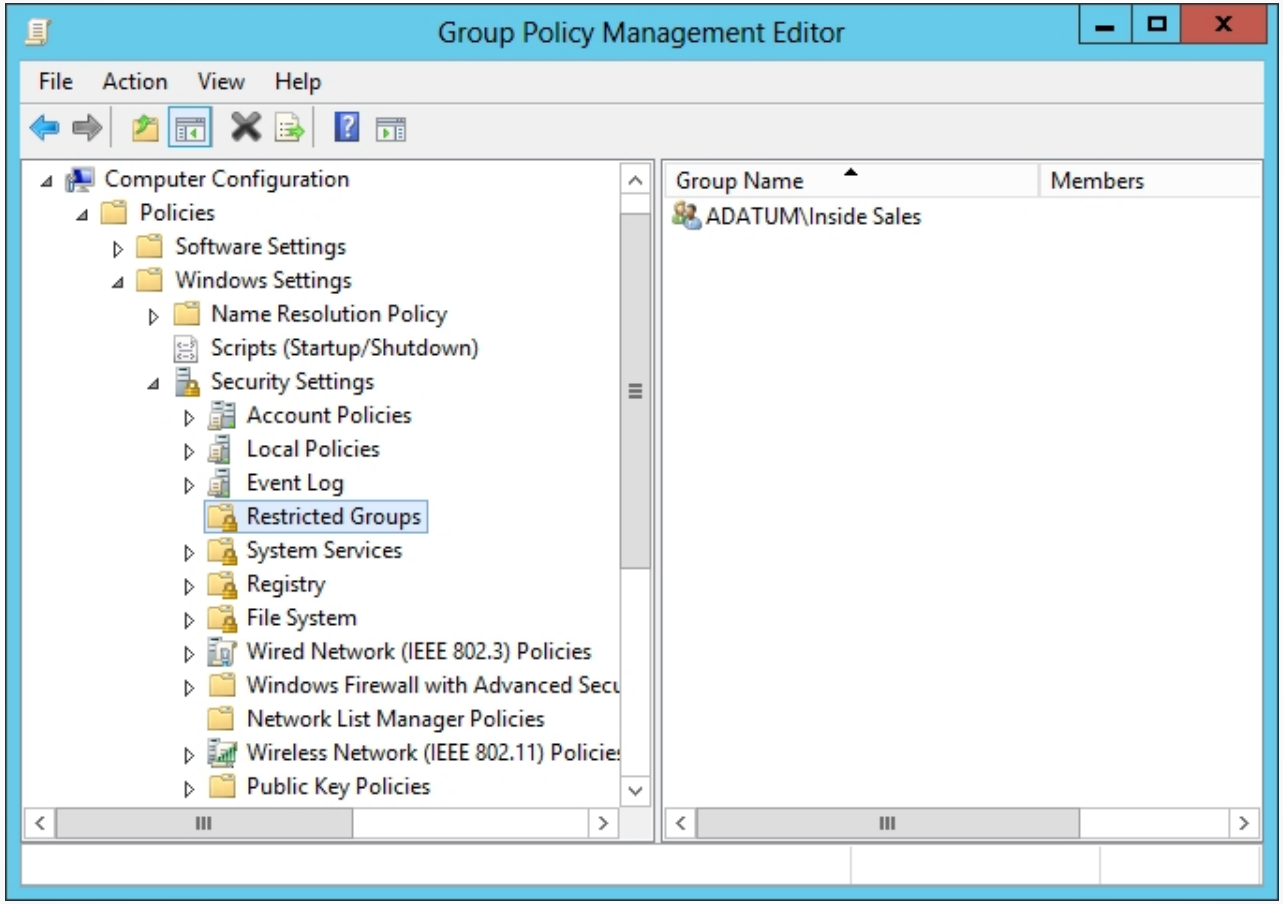
The Members tab of a group object's Properties sheet

Managing Group Memberships



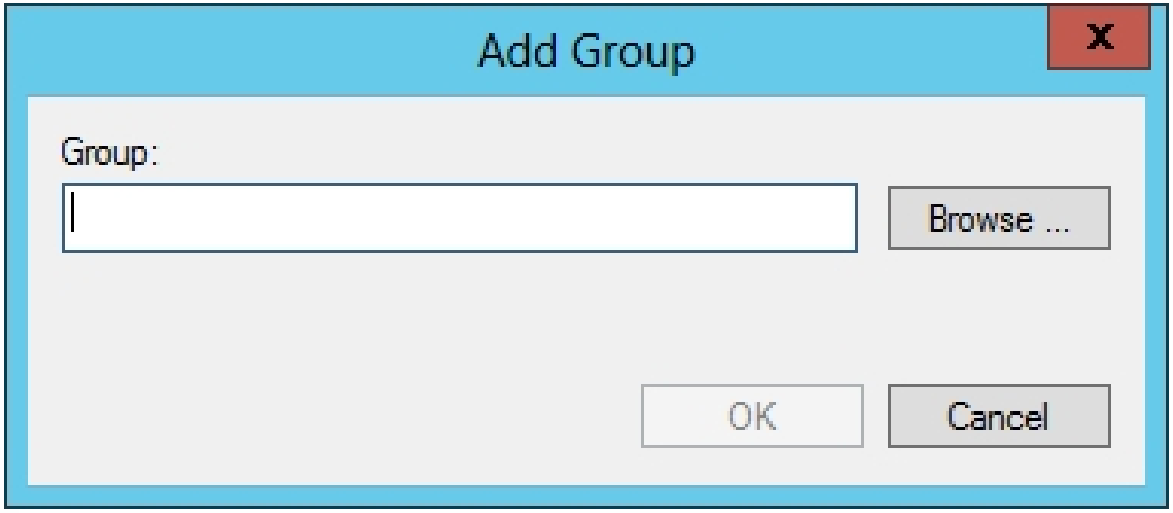
The Select Users, Contacts, Computers, Service Accounts, or Groups dialog box

Create a Restricted Groups Policy



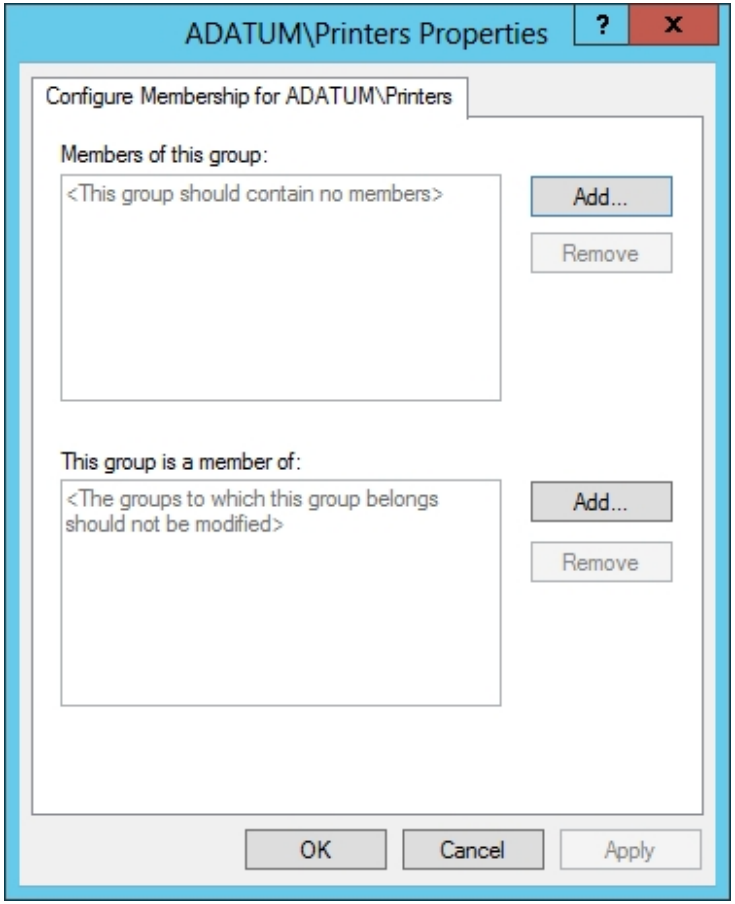
The Restricted Groups folder in the Group Policy object

Create a Restricted Groups Policy



The Add Group dialog box

Create a Restricted Groups Policy



The Properties sheet for a Restricted Groups policy

Managing Group Objects with Dsmod.exe

The basic syntax for **Dsmod.exe** is as follows:

dsmod group <*GroupDN*> [*parameters*]

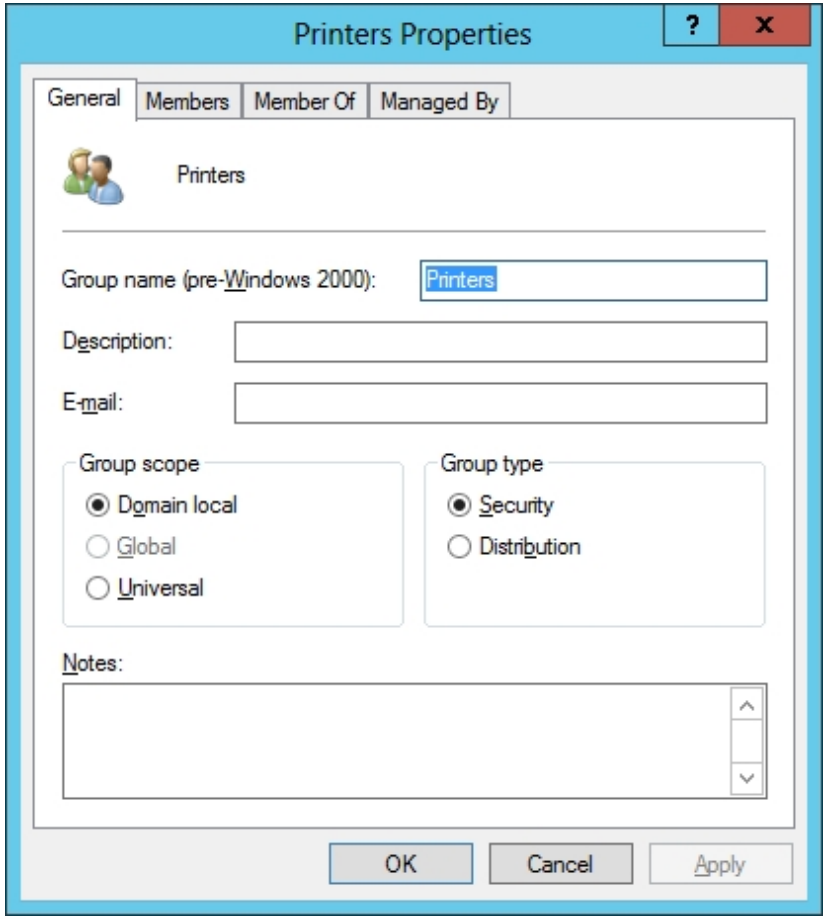
For example, to add the Administrator user to the Guests group, you would use the following command:

```
dsmod group "CN=Guests,CN=Builtin,DC=adatum,DC=com" -
  addmbr "CN=Administrator,CN=Users,DC=adatum,DC=com"
```

Converting Groups

- As group functions change, you might need to change a group object from one type to another.
- You can also change a group's scope.

Converting Groups



The General tab in a group object's Properties sheet

Deleting a Group

- When you delete a group, Windows Server 2012 does not use the same SID for that group again.
- Even if you create a new group with the same name as the one you deleted, you cannot restore the access permissions you assigned to resources.
- You must add the newly re-created group as a security principal in the resource's ACL all over again.
- When you delete a group, you delete only the group object and the permissions and rights specifying that group as the security principal.
- Deleting a group does not delete the objects that are members of the group.

Lesson Summary

- Once you have created a design for your Active Directory domains and the trees and forests superior to them, it is time to zoom in on each domain and consider the hierarchy you want to create inside it.
- Adding organizational units (OUs) to your Active Directory hierarchy is not as difficult as adding domains; you don't need additional hardware, and you can easily move or delete an OU at will.
- When you want to grant a collection of users permission to access a network resource, such as a file system share or a printer, you cannot assign permissions to an OU; you must use a security group instead. Although they are container objects, groups are not part of the Active Directory hierarchy in the same way that domains and OUs are.

Lesson Summary

- There is no simpler object type to create in the AD DS hierarchy than an OU. You only have to supply a name for the object and define its location in the Active Directory tree.
- Creating OUs enables you to implement a decentralized administration model, in which others manage portions of the AD DS hierarchy, without affecting the rest of the structure.
- Groups enable administrators to assign permissions to multiple users simultaneously. A group can be defined as a collection of user or computer accounts that functions as a security principal, in much the same way that a user does.

Lesson Summary

- In Active Directory, there are two types of groups: security and distribution; there are also three group scopes: domain local, global, and universal.
- **Group nesting** is the term used when groups are added as members of other groups.
- It is possible to control group memberships by using Group Policy. When you create Restricted Groups policies, you can specify the membership for a group and enforce it, so that no one can add or remove members.