NOS 02

Managing objects in AD DS

Module Overview

- Managing user accounts
- Managing groups in AD DS
- Managing computer objects in AD DS
- Implementing and managing OUs

Lesson 1: Managing user accounts

- Creating user accounts
- Configuring user account attributes
- Demonstration: Managing user accounts
- Managing inactive and disabled user accounts
- User account templates
- Demonstration: Using templates to manage accounts

Creating user accounts

- Users accounts:
  - Allow or deny access to sign into computers
  - Grant access to processes and services
  - Manage access to network resources
- User accounts can be created by using:
  - Active Directory Users and Computers
  - Active Directory Administrative Center
  - Windows PowerShell
  - Directory command line tool **dsadd**
- Considerations for naming users include:
  - Naming formats
  - UPN suffixes

Configuring user account attributes

User properties include the following categories:

- Account
- Organization
- Member of
- Password Settings
- Profile
- Policy
- Silo
- Extensions

Managing inactive and disabled user accounts

- Users accounts that will be inactive for a period of time should be disabled rather than deleted
- To disable an account in Active Directory Users and Computers, right-click the account and click Disable Account from the menu

User account templates

User templates simplify the creation of new user accounts

Group memberships
Home directory path
Profile path
Logon scripts
Password settings
Department
Manager

Template account

New user account

Lesson 2: Managing groups in AD DS

- Group types
- Group scopes
- Implementing group management
- Managing group membership by using Group Policy
- Default groups
- Special identities
- Demonstration: Managing groups in Windows Server

Group types

- Distribution groups
  - Used only with email applications
  - Not security enabled (no SID)
  - Cannot be given permissions

- Security groups
  - Security principal with a SID
  - Can be given permissions
  - Can also be email-enabled

You can convert security groups to distribution groups and distribution groups to security groups

Group scopes

- **Local groups** can contain users, computers, global groups, domain-local groups and universal groups from the same domain, domains in the same forest and other trusted domain and can be given permissions to resources on the local computer only
- **Domain-local groups** have the same membership possibilities but can be given permission to resources anywhere in the domain
- **Universal groups** can contain users, computers, global groups and other universal groups from the same domain or domains in the same forest and can be given permissions to any resource in the forest
- **Global groups** can only contain users, computers and other global groups from the same domain and can be given permission to resources in the domain or any trusted domain

Implementing group management

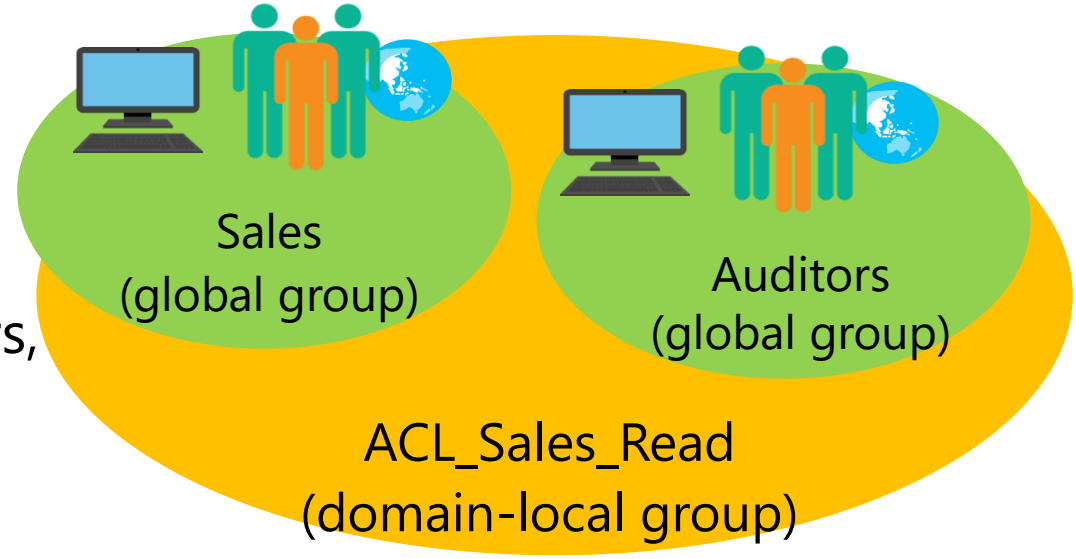
This best practice for nesting groups is known as IGDLA

I: Identities, users, or computers, which are members of

G: Global groups, which collect members based on members' roles, which are members of

DL: Domain-local groups, which provide management such as resource access which are

A: Assigned access to a resource



Implementing group management

I: Identities, users, or computers,
which are members of

Implementing group management

I: Identities, users, or computers, which are members of

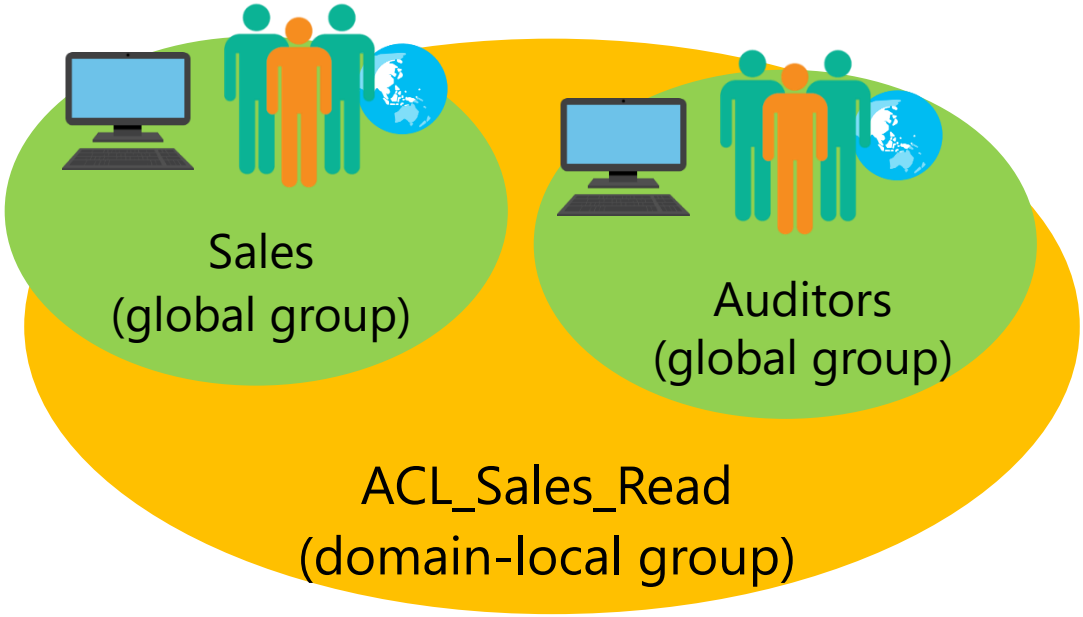
G: Global groups, which collect members based on members' roles, which are members of

Implementing group management

I: Identities, users, or computers, which are members of

G: Global groups, which collect members based on members' roles, which are members of

DL: Domain-local groups, which provide management such as resource access which are



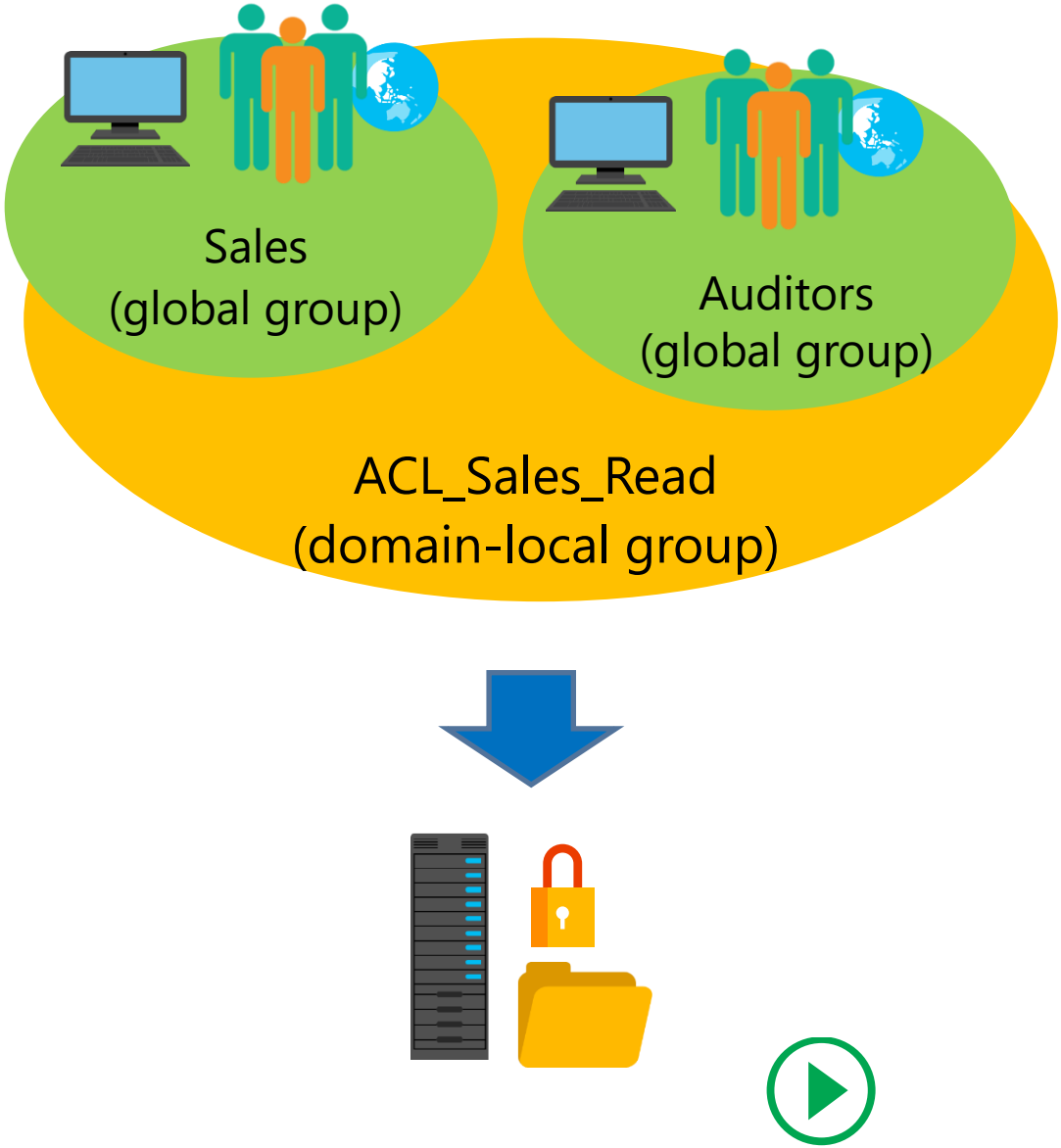
Implementing group management

I: Identities, users, or computers, which are members of

G: Global groups, which collect members based on members' roles, which are members of

DL: Domain-local groups, which provide management such as resource access which are

A: Assigned access to a resource



Implementing group management

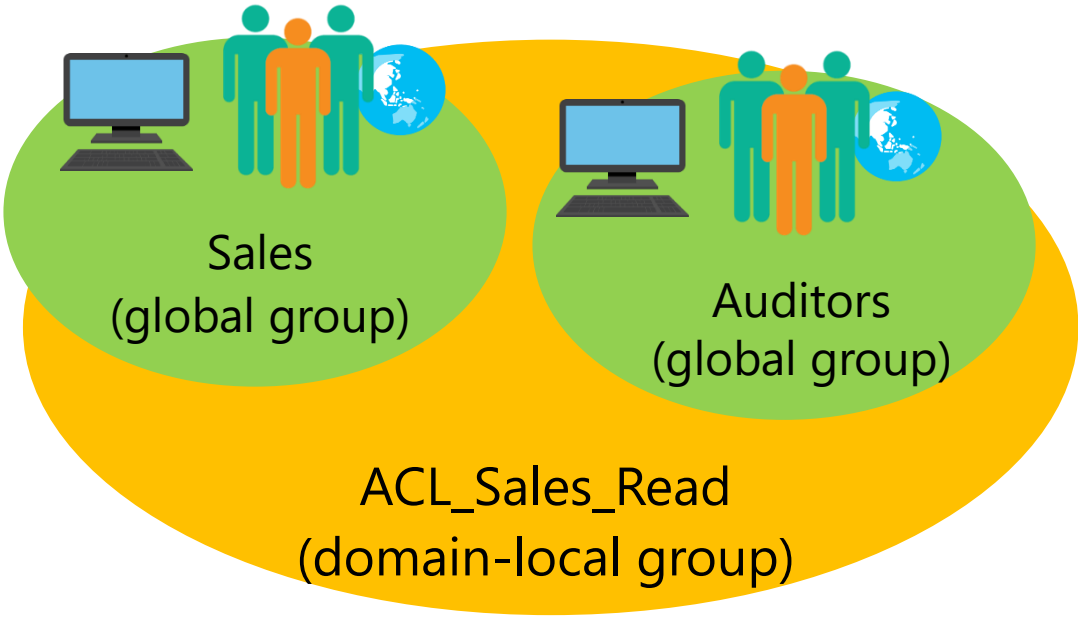
This best practice for nesting groups is known as IGDLA

I: Identities, users, or computers, which are members of

G: Global groups, which collect members based on members' roles, which are members of

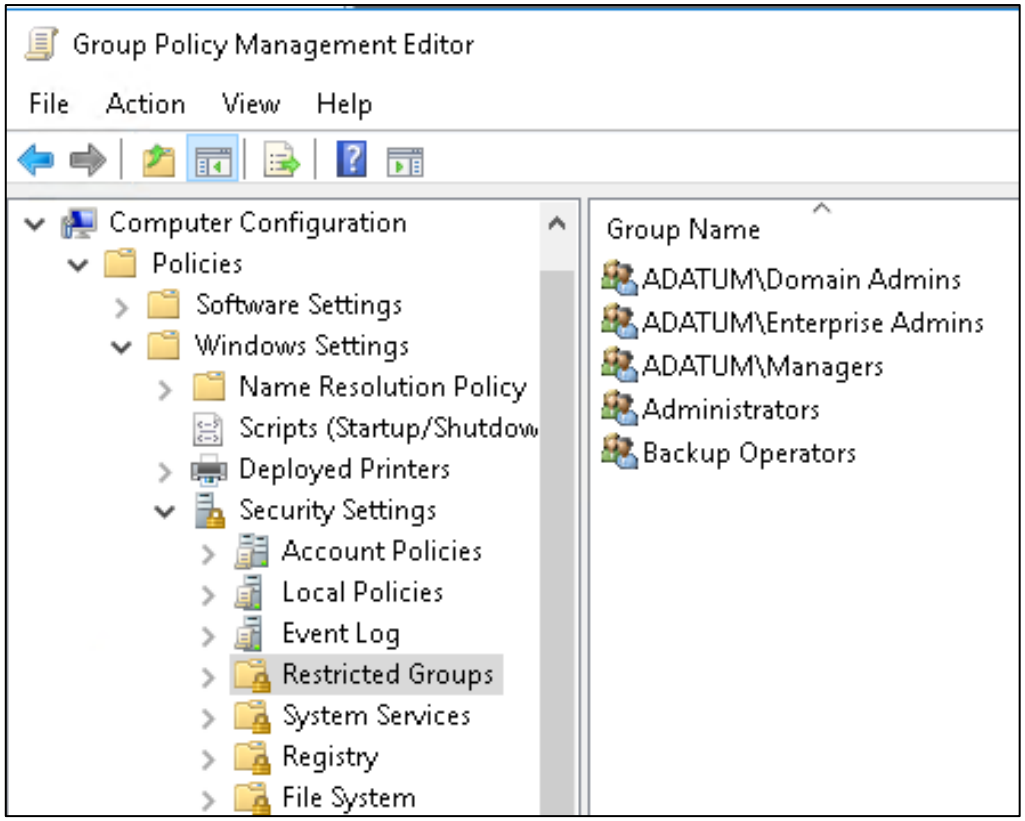
DL: Domain-local groups, which provide management such as resource access which are

A: Assigned access to a resource



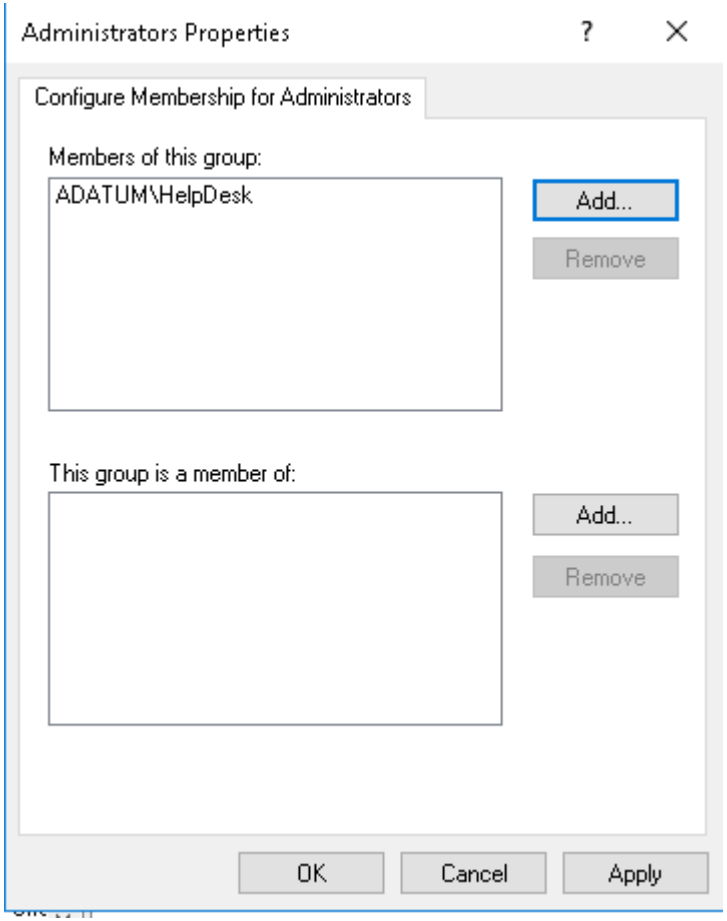
Managing group membership by using Group Policy

- Restricted Groups can simplify group management
- You use it to manage local and AD DS groups



Managing group membership by using Group Policy

Members can be added to the group and the group can be nested into other groups



Default groups

Carefully manage the default groups that provide administrative privileges, because these groups:

- Typically have broader privileges than are necessary for most delegated environments
- Often apply protection to their members

Group	**Location**
Enterprise Admins	Users container of the forest root domain
Schema Admins	Users container of the forest root domain
Administrators	Built-in container of each domain
Domain Admins	Users container of each domain
Server Operators	Built-in container of each domain
Account Operators	Built-in container of each domain
Backup Operators	Built-in container of each domain
Print Operators	Built-in container of each domain
Cert Publishers	Users container of each domain

Special identities

- Special identities:
  - Are groups for which the operating system controls membership
  - Can be used by the Windows Server operating system to provide access to resources based on the type of authentication or connection, not on the user account
- Important special identities include:
  - Anonymous Logon
  - Authenticated Users
  - Everyone
  - Interactive
  - Network
  - Creator Owner

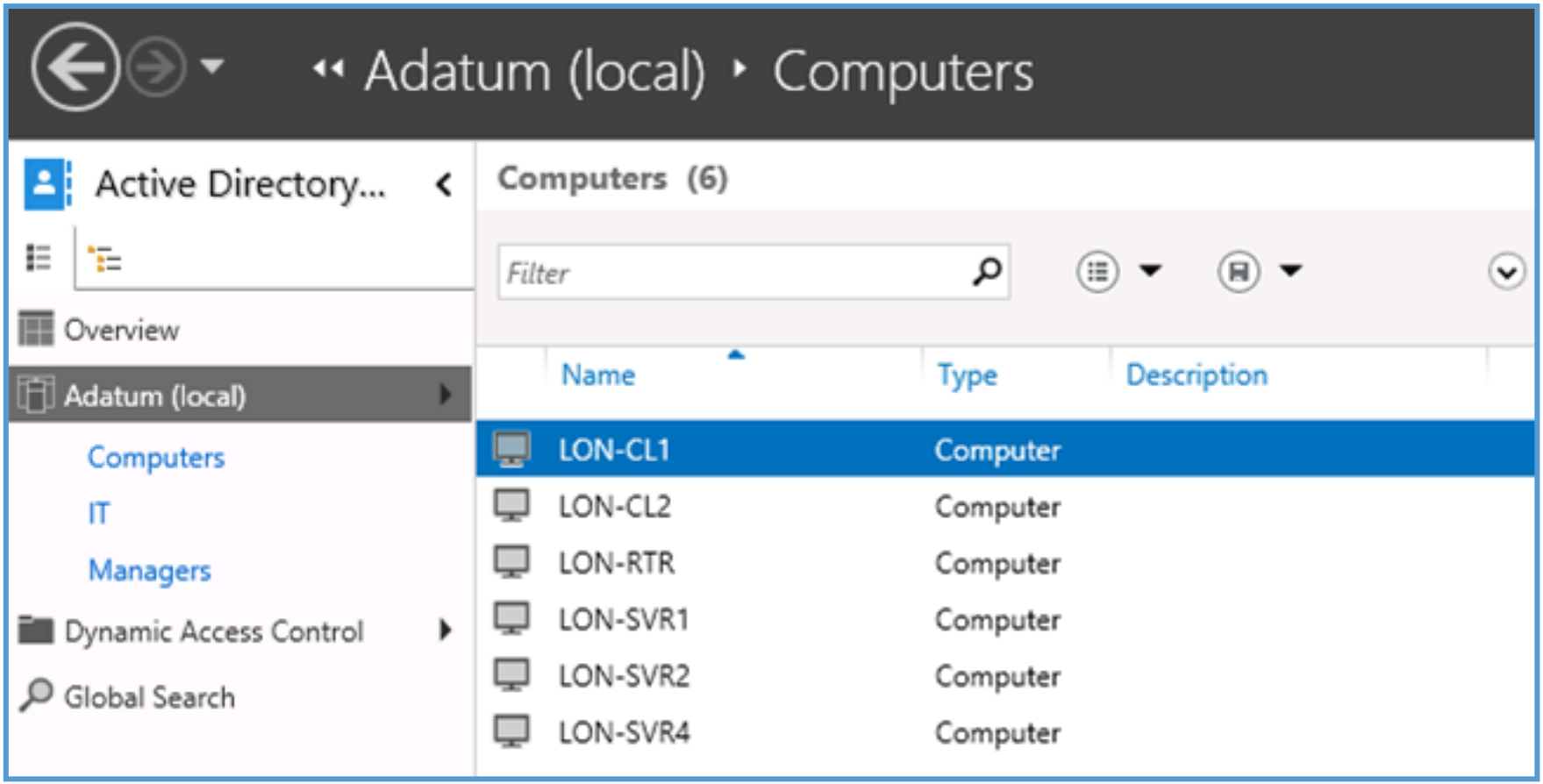
Lesson 3: Managing computer objects in AD DS

- What is the Computers container?
- Specifying the location of computer accounts
- Controlling permissions to create computer accounts
- Joining a computer to a domain
- Computer accounts and secure channels
- Resetting the secure channel

What is the Computers container?

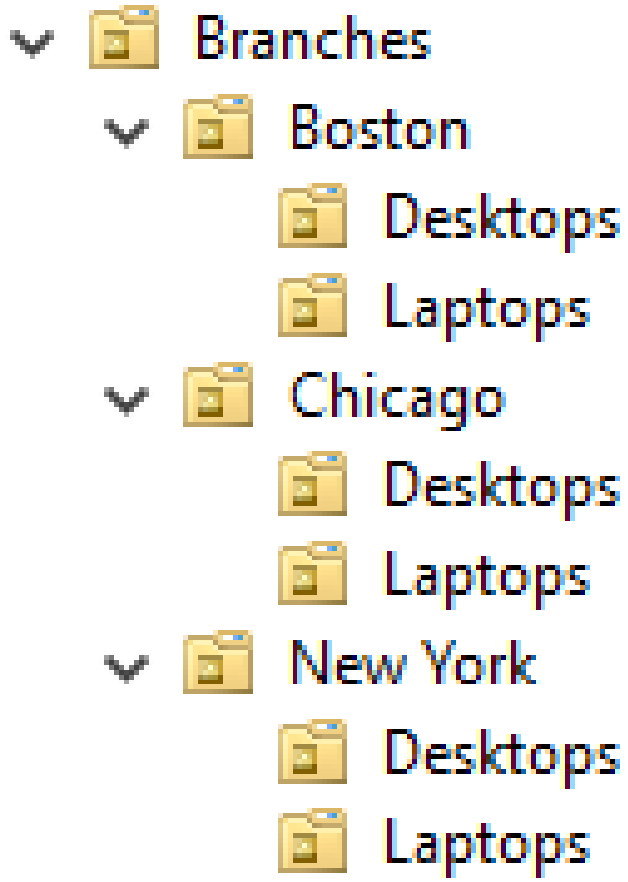
Active Directory Administrative Center is opened to the Adatum (local)\Computers container

Distinguished Name is CN=Computers,DC=Adatum,DC=com



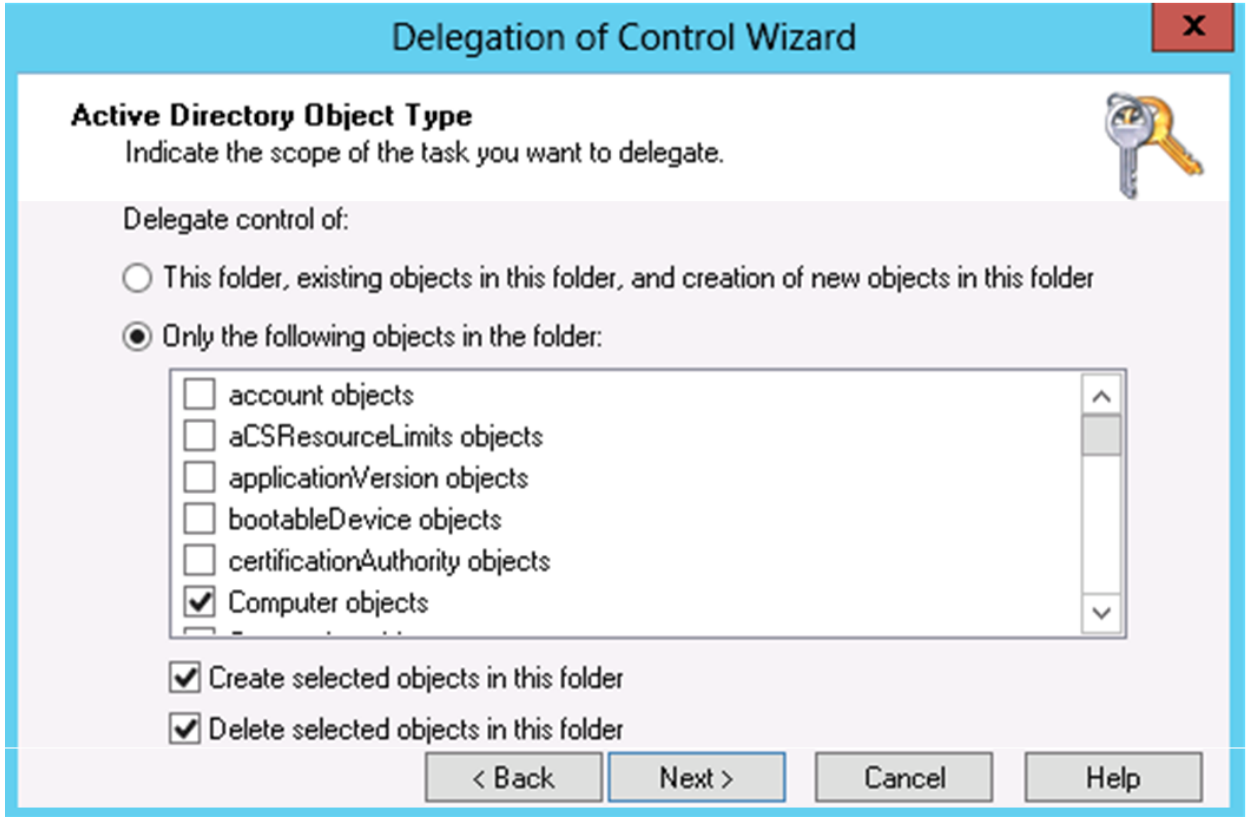
Specifying the location of computer accounts

- Best practice is to create OUs for computer objects
  - Servers are typically subdivided by server role
  - Client computers are typically subdivided by region
- Divide OUs:
  - By administration
  - To facilitate configuration with Group Policy

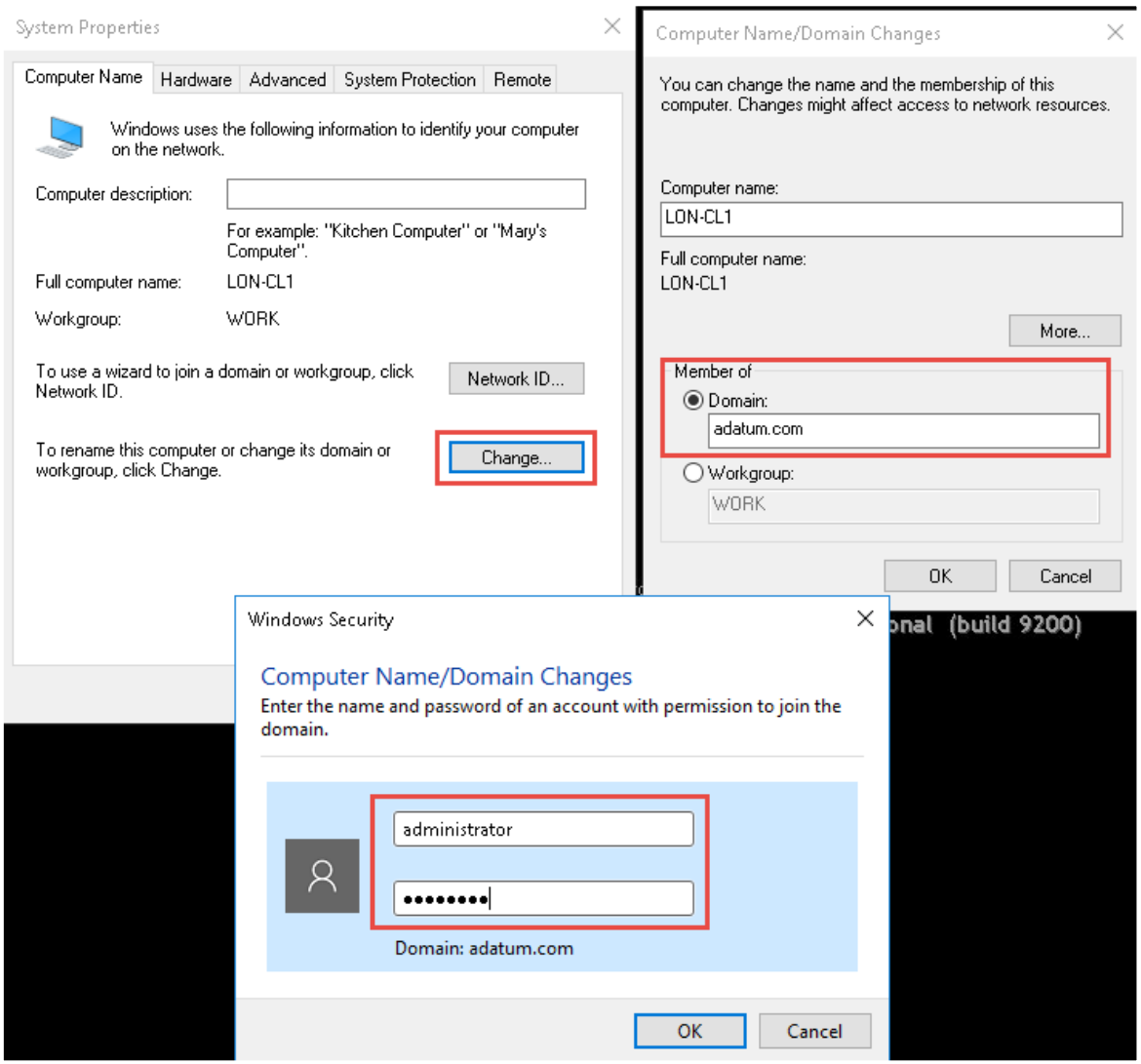


Controlling permissions to create computer accounts

In the Delegation of Control Wizard window, the administrator is creating a custom delegation for computer objects



Joining a computer to a domain



Computer accounts and secure channels

- Computers have accounts:
  - SAMAccountName and password
  - Used to create a secure channel between the computer and a domain controller
- Scenarios in which a secure channel might be broken:
  - Reinstalling a computer, even with same name, generates a new SID and password
  - Restoring a computer from an old backup or rolling back a computer to an old snapshot
  - The computer and domain disagreeing about what the password is

Resetting the secure channel

- Do not delete a computer from the domain and then rejoin it; this creates a new account, resulting in a new SID and lost group memberships
- Options for resetting the secure channel:
  - **nltest**
  - **netdom**
  - Active Directory Users and Computers
  - Active Directory Administrative Center
  - Windows PowerShell
  - **dsmod**

Lesson 4: Implementing and managing OUs

- Planning OUs
- OU hierarchy considerations
- Considerations for using OUs
- AD DS permissions
- Delegating AD DS permissions
- Demonstration: Delegating administrative permissions on an OU

Planning OUs

Location-based strategy	• Static • Delegation can be complicated
Organization-based strategy	• Not static • Easy to categorize
Resource-based strategy	• Not static • Easy to delegate administration
Multitenancy-based strategy	• Static • Easy to delegate administration • Easy to include and separate new tenants
Hybrid strategy	

OU hierarchy considerations

Align OU strategy to administrative requirements, not the organizational chart, because organizational charts are more subject to change than your IT administration model

AD DS inheritance behavior can simplify Group Policy administration because it allows group polices to be set on an OU and flow down to lower OUs in the hierarchy

Plan to accommodate changes in the IT administration model

Considerations for using OUs

- OUs can be created using AD DS graphical tools or command-line tools
- New OUs are protected from accidental deletion by default
- When objects are moved between OUs:
  - Directly assigned permissions remain in place
  - Inherited permissions will change
- Appropriate permissions are required to move objects between OUs

AD DS permissions

- Users receive their token (list of SIDs) during sign in
- Objects have a security descriptor that describes:
  - Who (SID) has been granted or denied access
  - Which permissions (Read, Write, Create or Delete child)
  - What kind of objects
  - Which sublevels
- When users browse the Active Directory structure, their token is compared to the security descriptor to evaluate their access rights

Delegating AD DS permissions

- Permissions on AD DS objects can be granted to users or groups
- Permission models are usually object-based or role-based
- The Delegation of Control Wizard can simplify assigning common administrative tasks
- The OU advanced security properties allow you to grant granular permissions