

Module 2

Managing objects in AD DS

Module Overview

- Managing user accounts
- Managing groups in AD DS
- Managing computer objects in AD DS
- Using Windows PowerShell for AD DS administration
- Implementing and managing OUs

Lesson 1: Managing user accounts

- Creating user accounts
- Configuring user account attributes
- Demonstration: Managing user accounts
- Creating user profiles
- 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

Demonstration: Managing user accounts

In this demonstration, you will see how to use Active Directory Administrative Center to:

- Create a new user account
- Delete a user account
- Move a user account
- Configure user attributes:
 - Change department
 - Change group membership

Creating user profiles

The Profile section of the User Properties window

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile		COM+
General	Address	Account	Profile
Telephones			
Organization			

User profile

Profile path:

Logon script:

Home folder

☐ Local path:

☒ Connect: To:

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

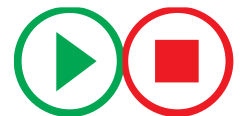


Group memberships
Home directory path
Profile path
Logon scripts
Password settings
Department
Manager

Template account



New user
account



Demonstration: Using templates to manage accounts

In this demonstration, you will see how to:

- Create a template account
- Create a new user based on the template

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

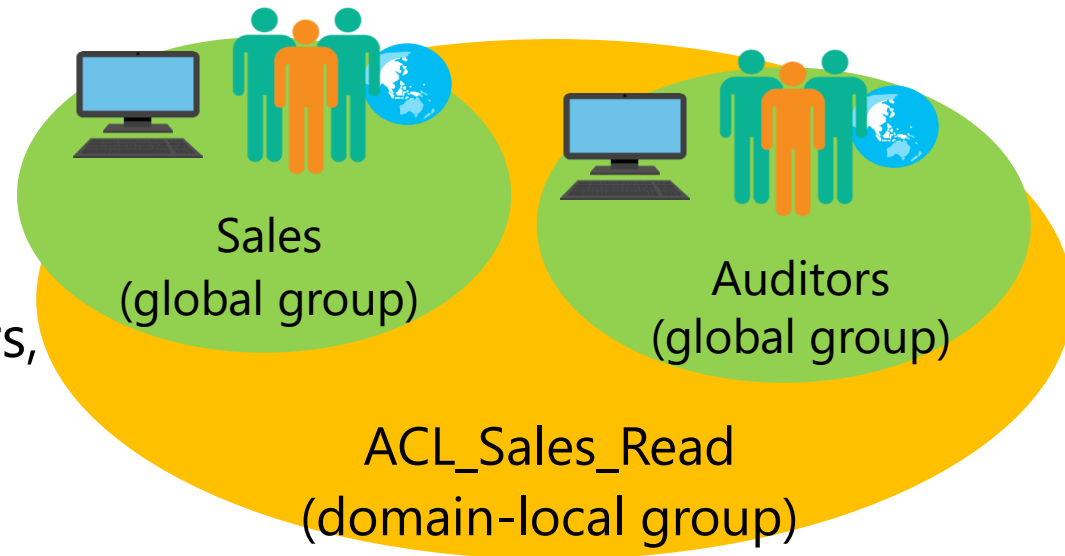
This best practice for nesting groups is known as IGDLA

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

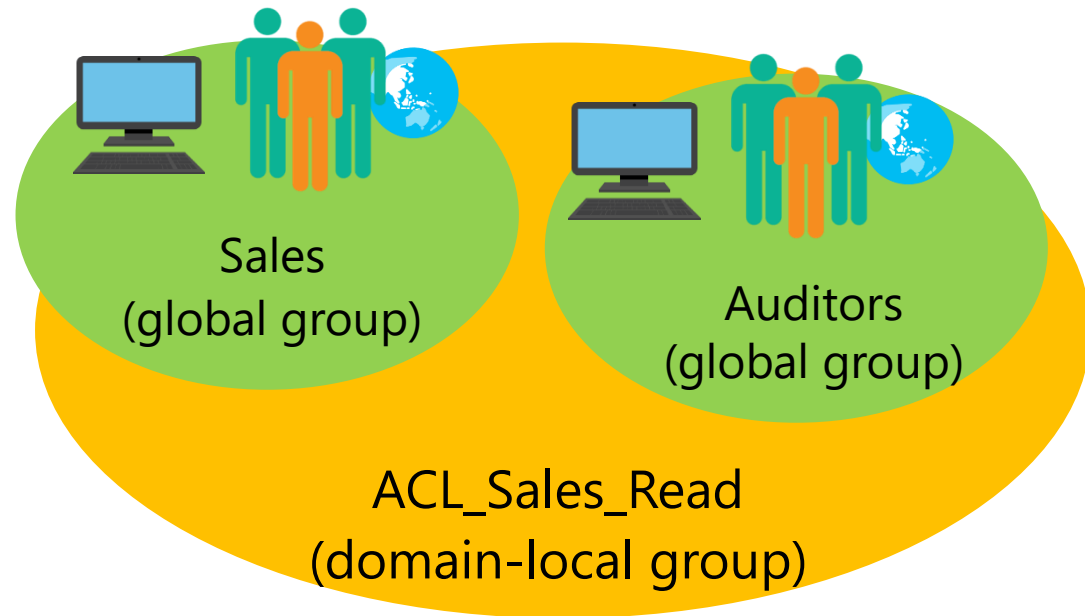


Implementing group management

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



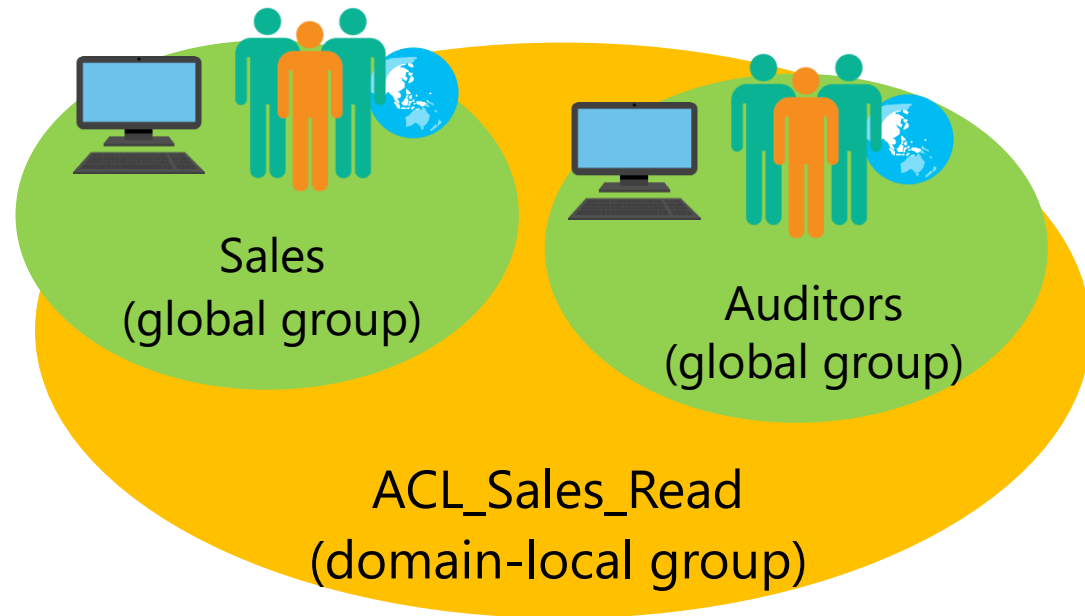
Implementing group management

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

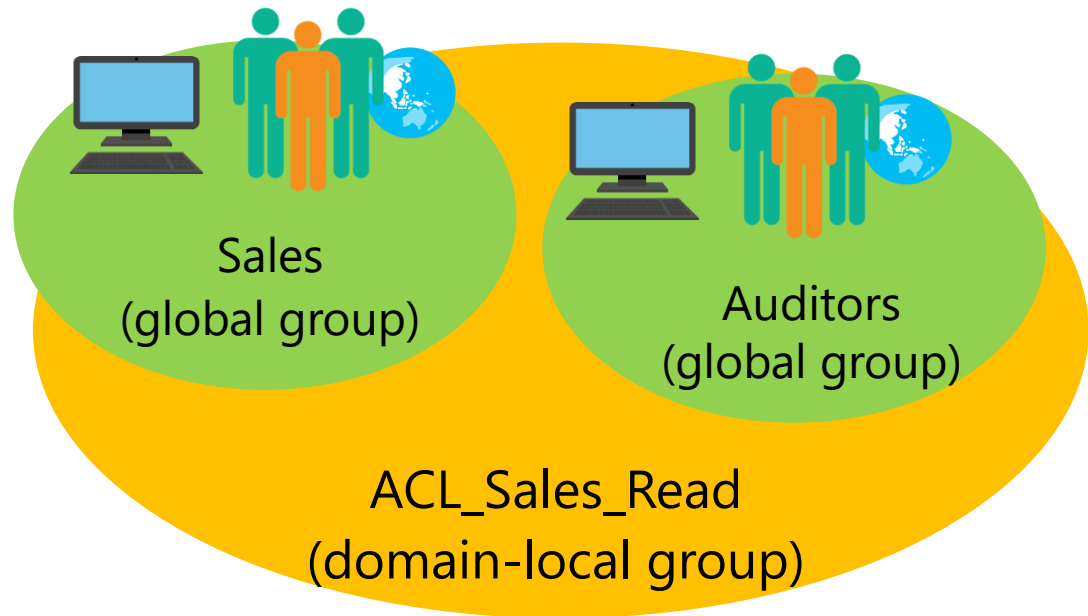
This best practice for nesting groups is known as IGDLA

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

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

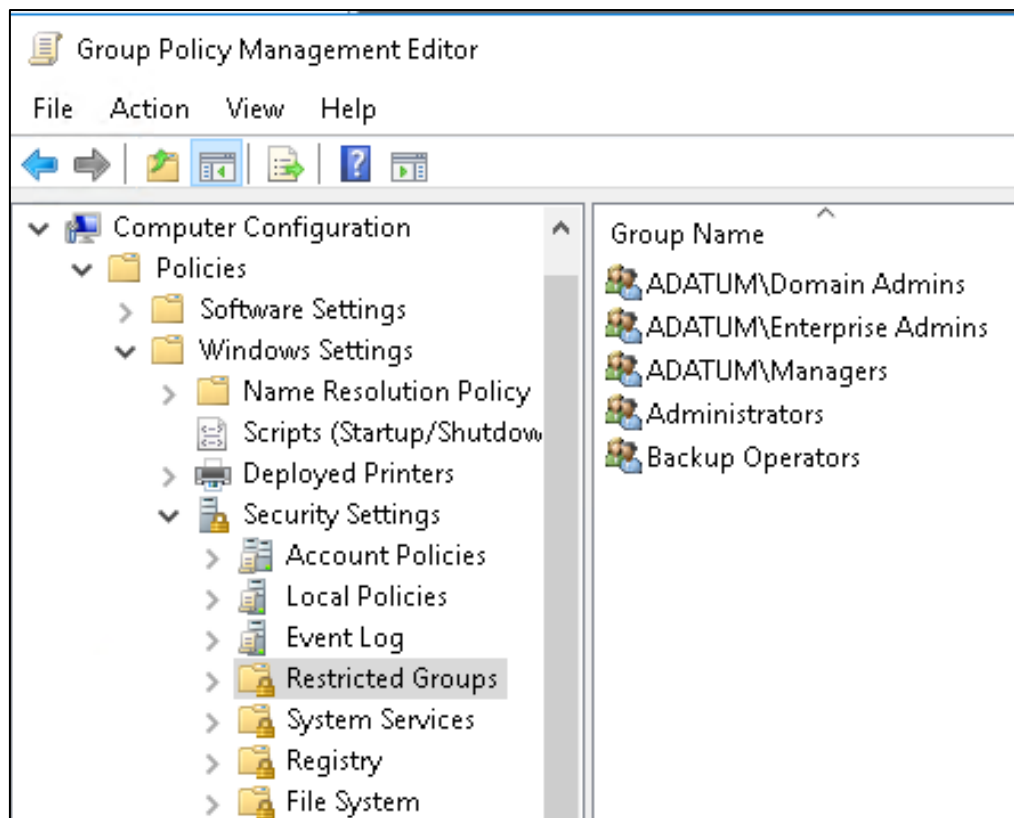
DL: Domain-local groups, which provide management such as resource access which are

A: Assigned access to a resource



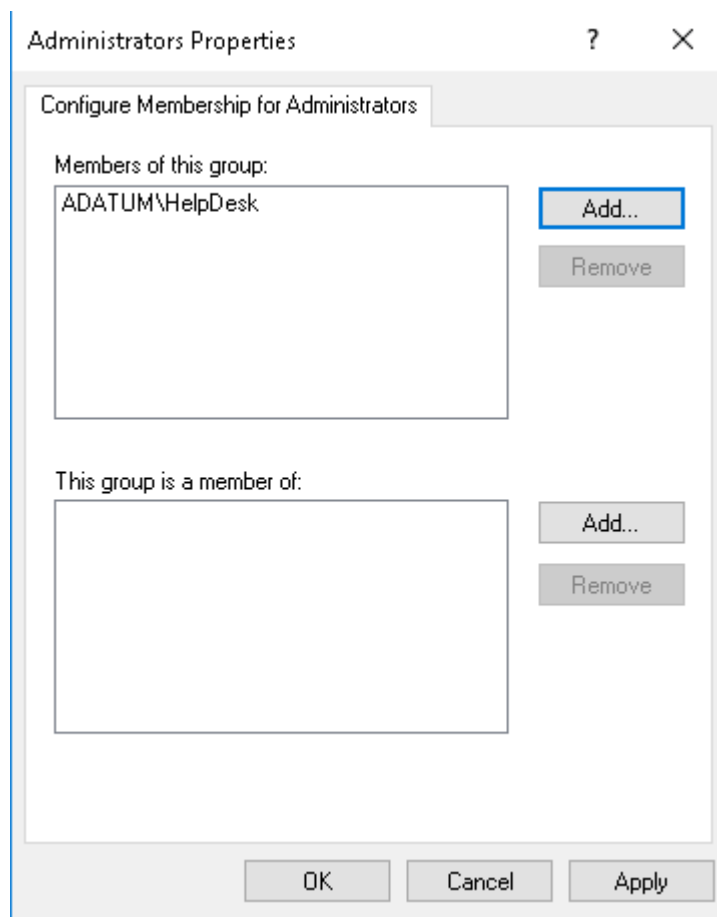
Managing group membership by using Group Policy

- 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

Demonstration: Managing groups in Windows Server

In this demonstration, you will see how to:

- Create a new group and add members to the group
- Add users to the group
- Change the group type and scope
- Configure a manager for the group

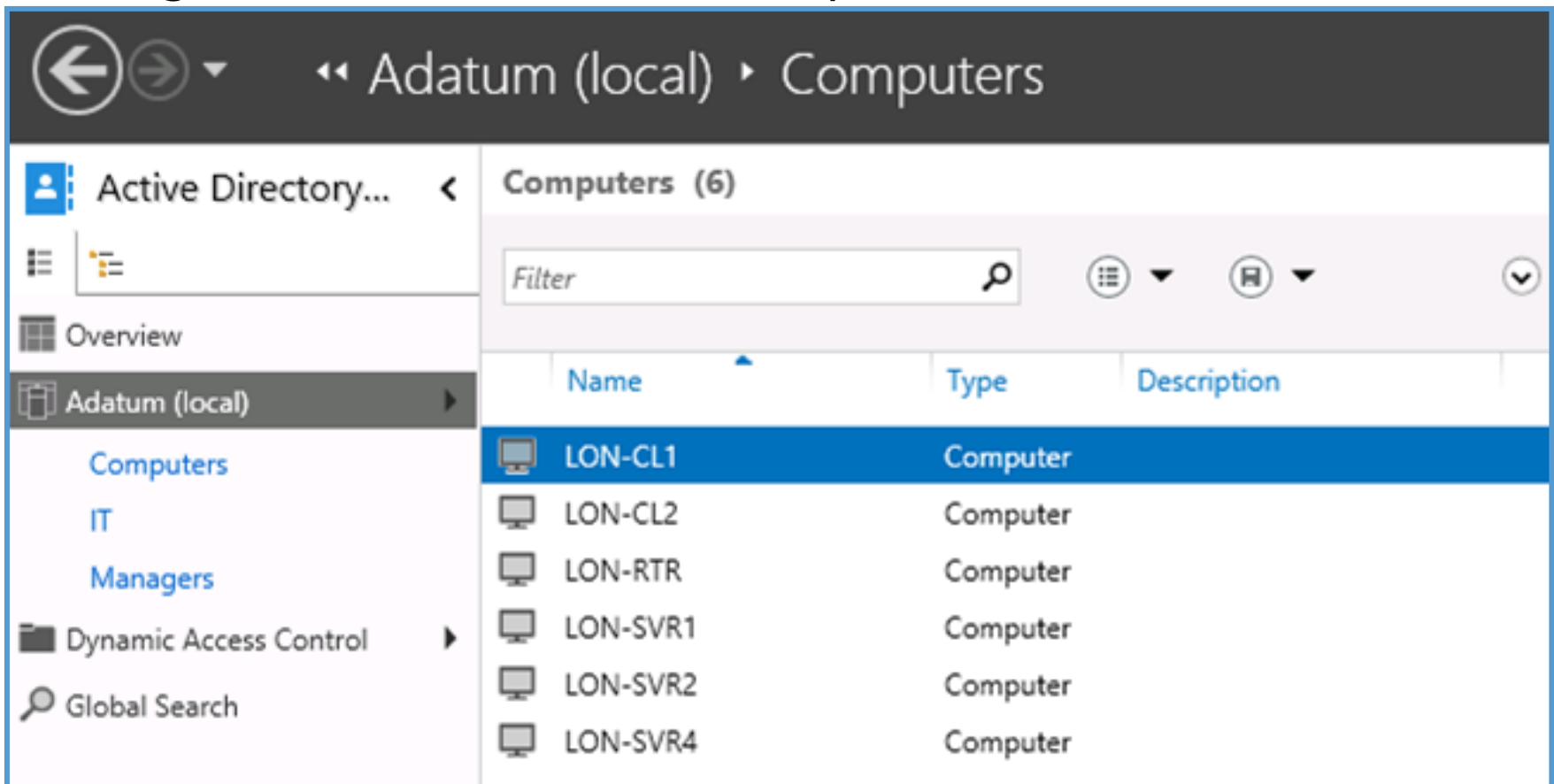
Lesson 3: Managing computer objects in AD DS

- 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
- Performing an offline domain join

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

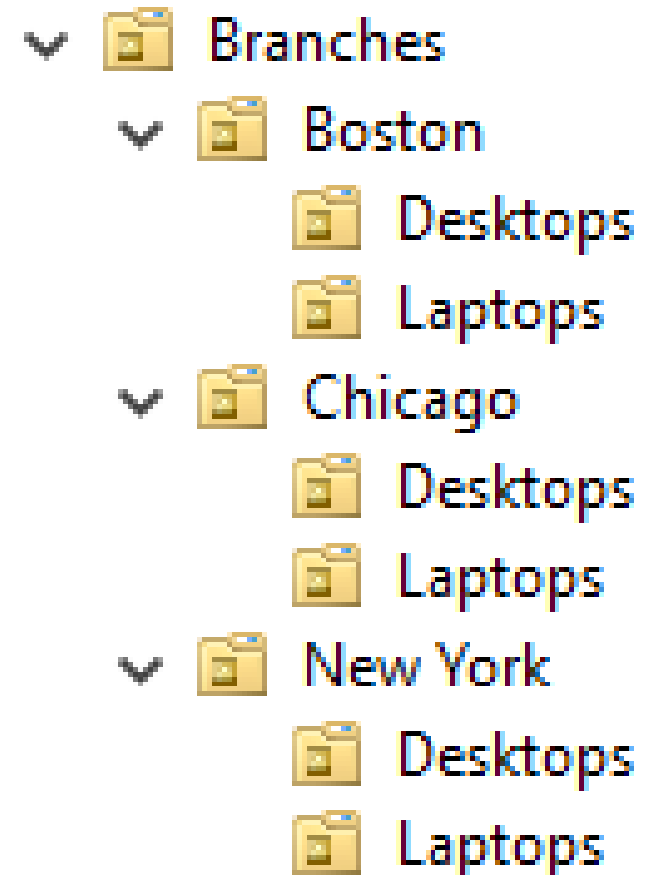


The screenshot shows the Active Directory Administrative Center interface. The breadcrumb navigation at the top indicates the path: Adatum (local) > Computers. The left-hand navigation pane shows the 'Adatum (local)' container selected, with sub-items for 'Computers', 'IT', and 'Managers'. The main content area displays a table of computers in the 'Computers (6)' container.

Name	Type	Description
LON-CL1	Computer	
LON-CL2	Computer	
LON-RTR	Computer	
LON-SVR1	Computer	
LON-SVR2	Computer	
LON-SVR4	Computer	

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

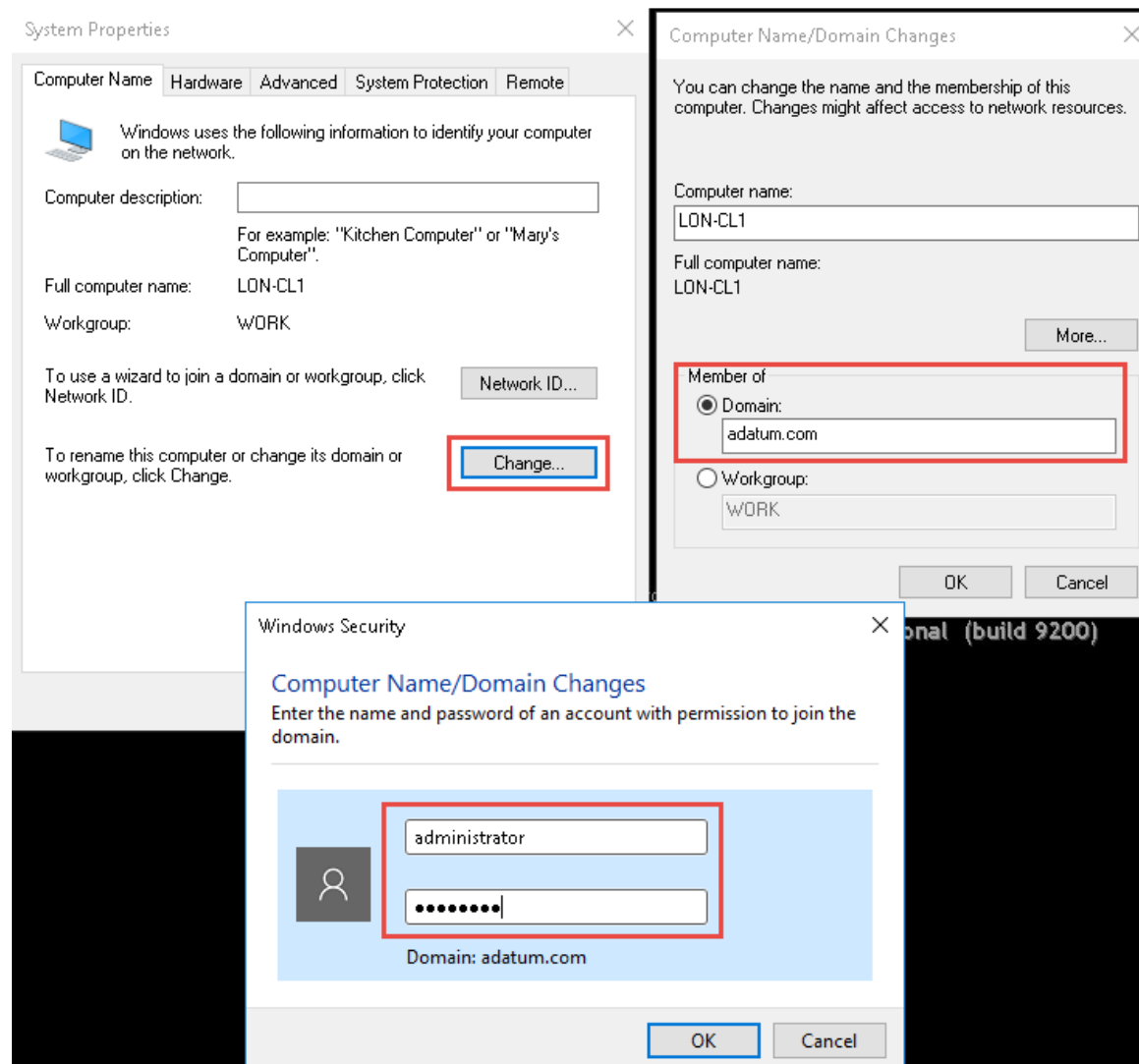


Controlling permissions to create computer accounts

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**

Performing an offline domain join

Use offline domain join to join computers to a domain when they cannot contact a domain controller

- Create a domain-join file by using:

```
djoin.exe /Provision /Domain <DomainName>  
/Machine <MachineName> /SaveFile <filepath>
```

- Import the domain join file by using:

```
djoin.exe /requestODJ /LoadFile <filepath>  
/WindowsPath <path to the Windows directory of  
the offline image>
```


Lab A: Managing AD DS objects

- Exercise 1: Creating and managing groups in AD DS
- Exercise 2: Creating and configuring user accounts in AD DS
- Exercise 3: Managing computer objects in AD DS

Logon Information

Virtual machines:

20742B-LON-DC1

20742B-LON-CL1

User name:

Adatum\Administrator

Password:

Pa55w.rd

Estimated Time: 45 minutes

Lab Scenario

You have been working for A. Datum Corporation as a desktop support specialist and have visited desktop computers to troubleshoot app and network problems. You recently accepted a promotion to the server support team. One of your first assignments is to configure the infrastructure service for a new branch office.

To begin deployment of the new branch office, you are preparing AD DS objects. As part of this preparation, you need to create users and groups for the new branch office that will house the Research department. Finally, you need to reset the secure channel for a computer account that has lost connectivity to the domain in the branch office.

Lab Review

- What types of objects can be members of global groups?
- What credentials are necessary for any computer to join a domain?

Lesson 4: Using Windows PowerShell for AD DS administration

- Using Windows PowerShell cmdlets to manage user accounts
- Using Windows PowerShell cmdlets to manage groups
- Using Windows PowerShell cmdlets to manage computer accounts
- Using Windows PowerShell cmdlets to manage OUs
- What are bulk operations?
- Demonstration: Using graphical tools to perform bulk operations
- Querying objects with Windows PowerShell
- Modifying objects with Windows PowerShell
- Working with CSV files
- Demonstration: Performing bulk operations with Windows PowerShell

Using Windows PowerShell cmdlets to manage user accounts

Cmdlet	Description
New-ADUser	Creates user accounts
Set-ADUser	Modifies properties of user accounts
Remove-ADUser	Deletes user accounts
Set-ADAccountPassword	Resets the password of a user account
Set-ADAccountExpiration	Modifies the expiration date of a user account
Unlock-ADAccount	Unlocks a user account after it has become locked after too many incorrect sign in attempts
Enable-ADAccount	Enables a user account
Disable-ADAccount	Disables a user account

```
New-ADUser "Sten Faerch" -AccountPassword (Read-Host -AsSecureString "Enter password") -Department IT
```

Using Windows PowerShell cmdlets to manage groups

Cmdlet	Description
New-ADGroup	Creates new groups
Set-ADGroup	Modifies properties of groups
Get-ADGroup	Displays properties of groups
Remove-ADGroup	Deletes groups
Add-ADGroupMember	Adds members to groups
Get-ADGroupMember	Displays membership of groups
Remove-ADGroupMember	Removes members from groups
Add-ADPrincipalGroupMembership	Adds group membership to objects
Get-ADPrincipalGroupMembership	Displays group membership of objects
Remove-ADPrincipalGroupMembership	Removes group membership from an object

```
New-ADGroup -Name "CustomerManagement" -Path  
"ou=managers,dc=adatum,dc=com" -GroupScope Global  
-GroupCategory Security
```

```
Add-ADGroupMember -Name "CustomerManagement"  
-Members "Joe"
```

Using Windows PowerShell cmdlets to manage computer accounts

Cmdlet	Description
New-ADComputer	Creates new computer accounts
Set-ADComputer	Modifies properties of computer accounts
Get-ADComputer	Displays properties of computer accounts
Remove-ADComputer	Deletes computer accounts
Test-ComputerSecureChannel	Verifies or repairs the trust relationship between a computer and the domain
Reset-ComputerMachinePassword	Resets the password for a computer account

```
New-ADComputer -Name "LON-SVR8" -Path  
"ou=marketing,dc=adatum,dc=com" -Enabled $true
```

```
Test-ComputerSecureChannel -Repair
```

Using Windows PowerShell cmdlets to manage OUs

Cmdlet	Description
New-ADOrganizationalUnit	Creates OUs
Set-ADOrganizationalUnit	Modifies properties of OUs
Get-ADOrganizationalUnit	Views properties of OUs
Remove-ADOrganizationalUnit	Deletes OUs

```
New-ADOrganizationalUnit -Name "Sales"  
-Path "ou=marketing,dc=adatum,dc=com"  
-ProtectedFromAccidentalDeletion $true
```


What are bulk operations?

- A bulk operation is a single action that changes multiple objects
- Sample bulk operations:
 - Create user accounts based on data in a spreadsheet
 - Disable all accounts not used in six months
 - Rename the department for many users
- You can perform bulk operations by using:
 - Graphical tools
 - Command-line tools
 - Scripts

Demonstration: Using graphical tools to perform bulk operations

In this demonstration, you will see how to use Active Directory Users and Computers to change the **Office** attribute for users in the Research OU as a bulk operation

Querying objects with Windows PowerShell

Parameter	Description
SearchBase	Defines the AD DS path to begin searching
SearchScope	Defines at what level below the SearchBase a search should be performed
ResultSetSize	Defines how many objects to return in response to a query
Properties	Defines which object properties to return and display
Filter	Defines a filter by using Windows PowerShell syntax
LDAPFilter	Defines a filter by using LDAP query syntax

Descriptions of operators:

-eq Equal to

-ne Not equal to

-lt Less than

-le Less than or equal to

-gt Greater than

-ge Greater than or equal to

-like Uses wildcards for pattern matching



Querying objects with Windows PowerShell

Show all the properties for a user account:

```
Get-ADUser -Name "Administrator" -Properties *
```

Show all the user accounts in the Marketing OU and all its subcontainers:

```
Get-ADUser -Filter * -SearchBase  
"ou=Marketing,dc=adatum,dc=com" -SearchScope subtree
```

Show all of the user accounts with a last sign in date before a specific date:

```
Get-ADUser -Filter {lastlogondate -lt "January 1, 2016"}
```

Show all of the user accounts in the Marketing department that have a last sign in date before a specific date:

```
Get-ADUser -Filter {(lastlogondate -lt "January 1,  
2016")} -and (department -eq "Marketing")}
```



Modifying objects with Windows PowerShell

Use the pipe character (|) to pass a list of objects to a cmdlet for further processing

```
Get-ADUser -Filter {company -notlike "*"} |  
Set-ADUser -Company "A. Datum"
```

```
Get-ADUser -Filter {lastlogondate -lt "January 1,  
2016"} | Disable-ADAccount
```

```
Get-Content C:\users.txt | Disable-ADAccount
```

Working with CSV files

The first line of a .csv file defines the names of the columns:

```
FirstName, LastName, Department  
Greg, Guzik, IT  
Robin, Young, Research  
Qiong, Wu, Marketing
```

A **foreach** loop processes the contents of a .csv file that have been imported into a variable:

```
$users=Import-CSV -LiteralPath "C:\users.csv"  
foreach ($user in $users) {  
    Write-Host "The first name is:"  
    $user.FirstName  
}
```

Demonstration: Performing bulk operations with Windows PowerShell

In this demonstration, you will see how to:

- Create a new global group in the IT department
- Add all users in the IT department to the group
- Set the address attributes for all users in the Research department
- Create a new OU
- Run a script to create new users from a .csv file
- Verify the accounts were modified and new accounts were created

Lesson 5: 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	<ul style="list-style-type: none">• Static• Delegation can be complicated
Organization-based strategy	<ul style="list-style-type: none">• Not static• Easy to categorize
Resource-based strategy	<ul style="list-style-type: none">• Not static• Easy to delegate administration
Multitenancy-based strategy	<ul style="list-style-type: none">• 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 policies 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

Demonstration: Delegating administrative permissions on an OU

In this demonstration, you will see how to:

- Create a new OU
- Use the Delegation of Control Wizard to assign a task
- Use advanced OU security to assign granular permissions to the Research Managers group

Lab B: Administering AD DS

- Exercise 1: Delegating administration for OUs
- Exercise 2: Creating and modifying AD DS objects with Windows PowerShell

Logon Information

Virtual machines:	20742B-LON-DC1 20742B-LON-SVR1 20742B-LON-CL1
User name:	Adatum\Administrator
Password:	Pa55w.rd

Estimated Time: 45 minutes

Lab Scenario

You have been working for the A. Datum Corporation as a desktop support specialist and have performed troubleshooting tasks on desktop computers to resolve application and network problems. You recently accepted a promotion to the server support team. One of your first assignments is to configure the infrastructure service for a new branch office.

To begin the deployment of the new branch office, you are preparing AD DS objects. As part of this preparation, you need to create an OU for the branch office and delegate permission to manage it. Also, you need to evaluate Windows PowerShell to manage AD DS more efficiently.

Lab Review

- Why are the users that this script created enabled?
- What is the status of accounts that the New-ADUser cmdlet creates?

Module Review and Takeaways

- Real-world Issues and Scenarios
- Tools
- Best Practice
- Common Issues and Troubleshooting Tips