8/5/2025

Lab 6

Managing Computer Objects and Organizational Units

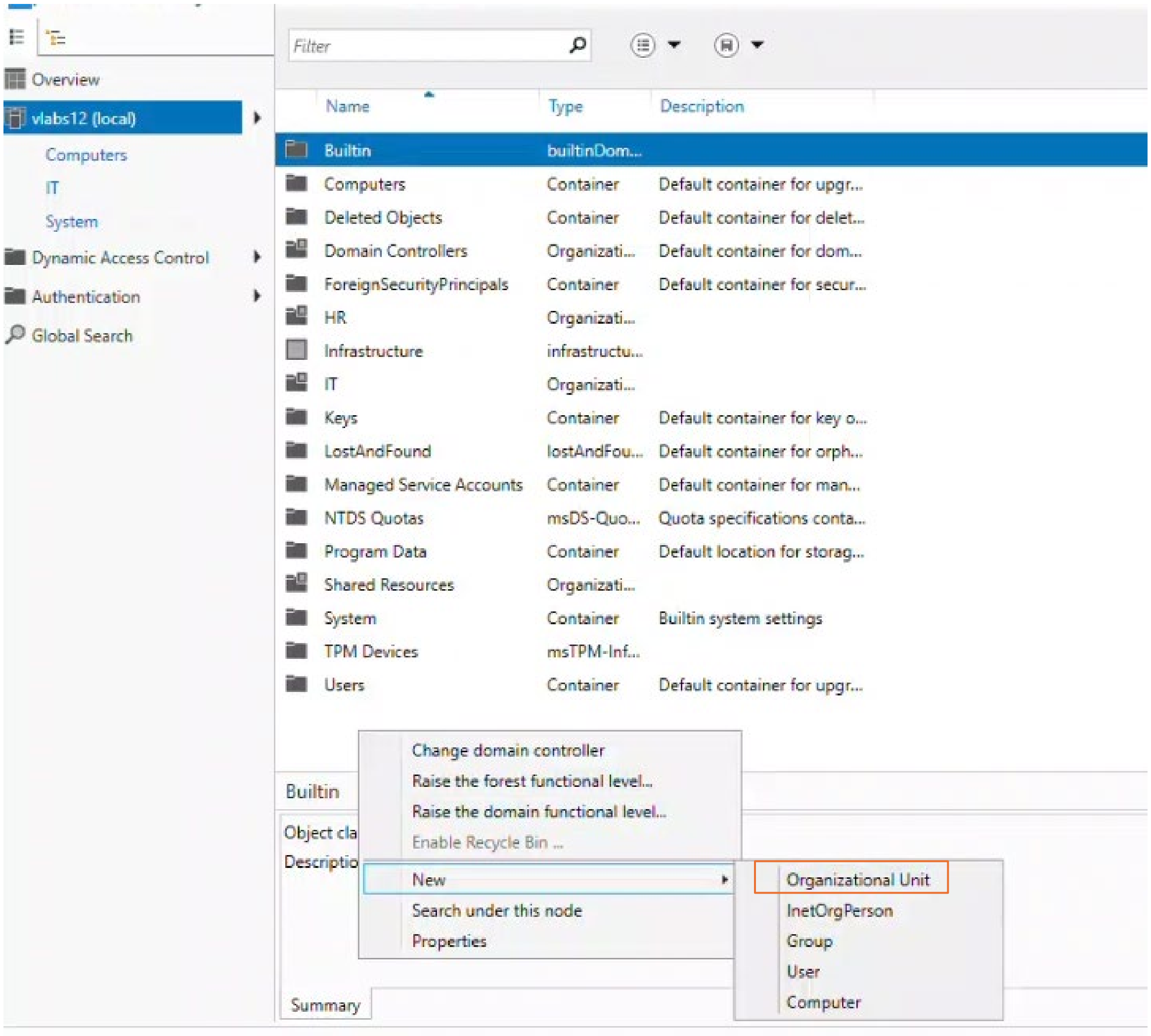
Mohammed, Laetitia, 0931512
NETWORK INSTALLATION AND ADMINISTRATION II

Contents

Lab Overview This lab is designed to help you practice managing computer objects and organizational units (OUs) in Active Directory using Active Directory Administrative Center (ADAC) and PowerShell. You will perform tasks related to creating, deleting, modifying, and delegating control over OUs, as well as managing computer objects.

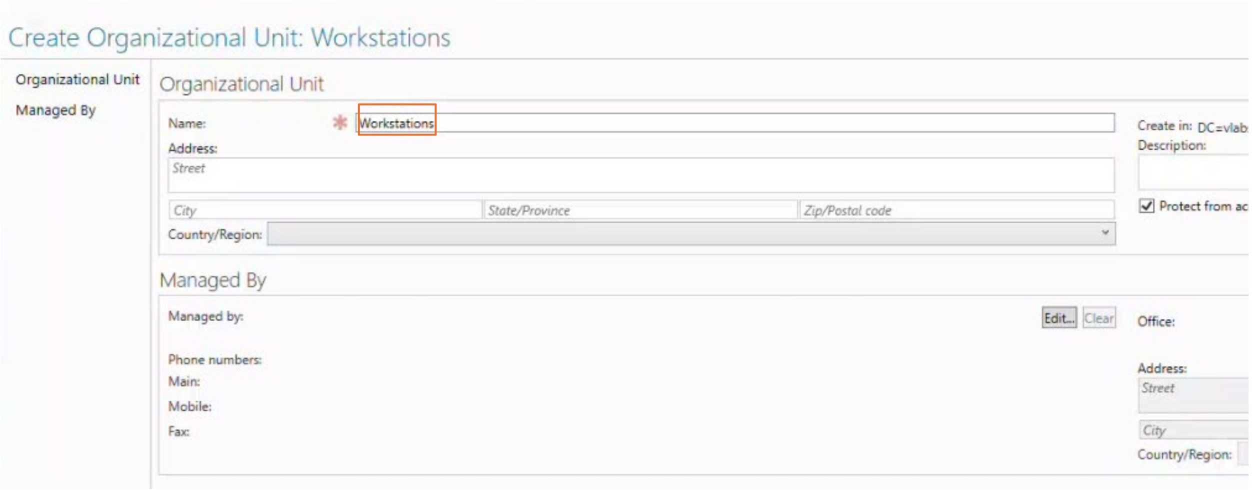
Task 1: Managing Computer Objects

Start by creating the OU “Workstations” in vlabs12 by right-clicking on vlabs12 → New → Organizational Unit



Name	Type	Description
Builtin	builtinDom...	
Computers	Container	Default container for upgr...
Deleted Objects	Container	Default container for delet...
Domain Controllers	Organizati...	Default container for dom...
ForeignSecurityPrincipals	Container	Default container for secur...
HR	Organizati...	
Infrastructure	infrastructu...	
IT	Organizati...	
Keys	Container	Default container for key o...
LostAndFound	lostAndFou...	Default container for orph...
Managed Service Accounts	Container	Default container for man...
NTDS Quotas	msDS-Quo...	Quota specifications conta...
Program Data	Container	Default location for storag...
Shared Resources	Organizati...	
System	Container	Builtin system settings
TPM Devices	msTPM-Inf...	
Users	Container	Default container for upgr...

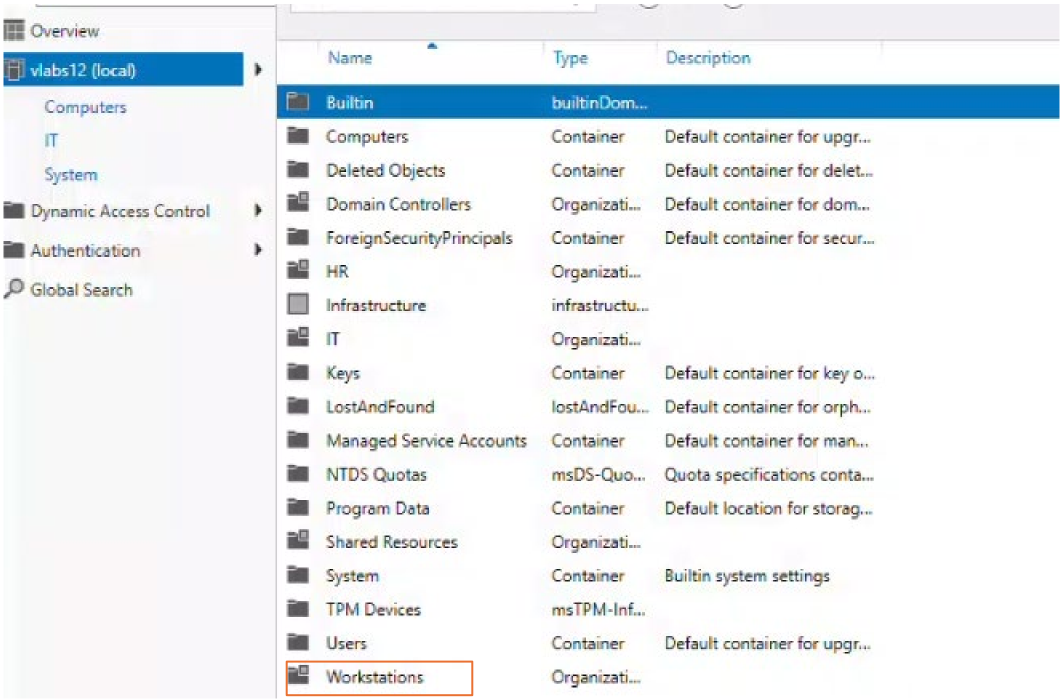
Name it and click OK


Create Organizational Unit: Workstations

Name: * Workstations

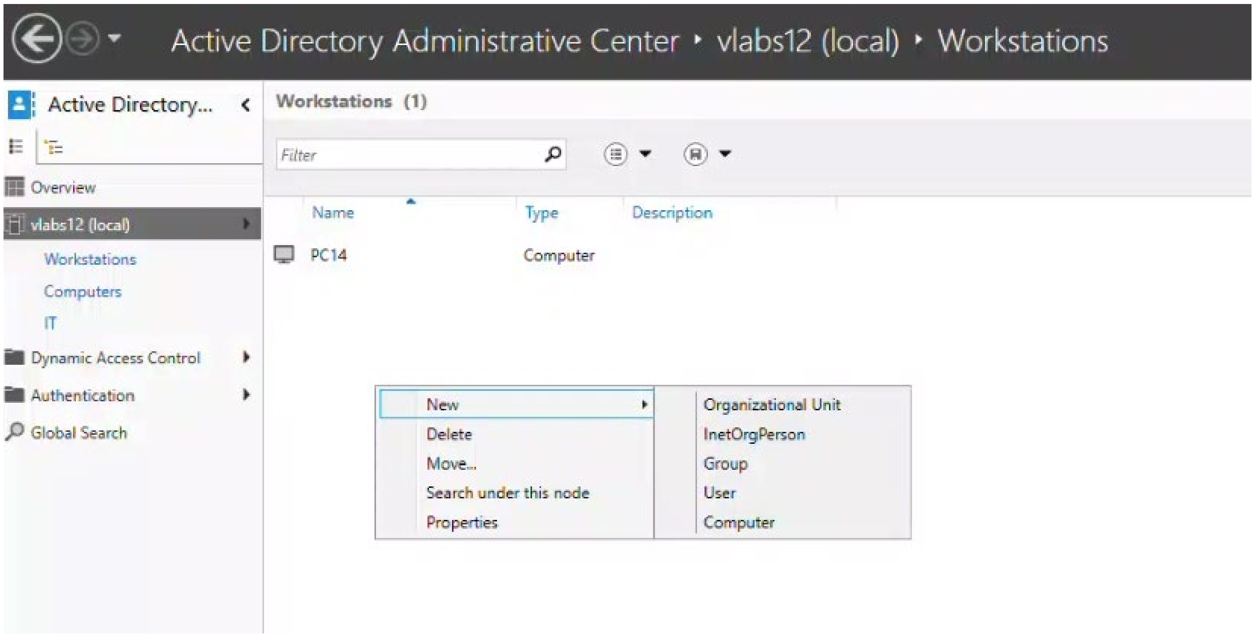
Create in: DC=vlab

☑ Protect from ac



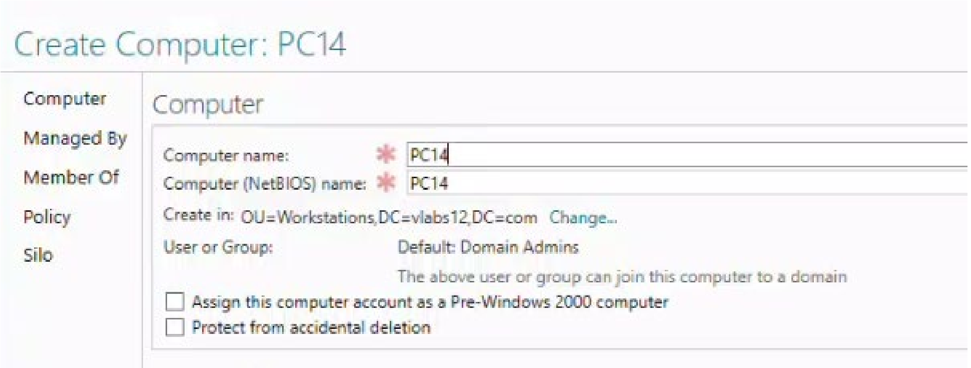
Name	Type	Description
Builtin	builtinDom...	
Computers	Container	Default container for upgr...
Deleted Objects	Container	Default container for delet...
Domain Controllers	Organizati...	Default container for dom...
ForeignSecurityPrincipals	Container	Default container for secur...
HR	Organizati...	
Infrastructure	infrastructu...	
IT	Organizati...	
Keys	Container	Default container for key o...
LostAndFound	lostAndFou...	Default container for orph...
Managed Service Accounts	Container	Default container for man...
NTDS Quotas	msDS-Quo...	Quota specifications conta...
Program Data	Container	Default location for storag...
Shared Resources	Organizati...	
System	Container	Builtin system settings
TPM Devices	msTPM-Inf...	
Users	Container	Default container for upgr...
Workstations	Organizati...	

In the Workstation OU, create a new computer object. New → Computer



Name	Type	Description
PC14	Computer	

Name it PC14. Press OK.



Create Computer: PC14

Computer

Computer name: * PC14

Computer (NetBIOS) name: * PC14

Create in: OU=Workstations,DC=vlabs12,DC=com Change...

User or Group: Default: Domain Admins

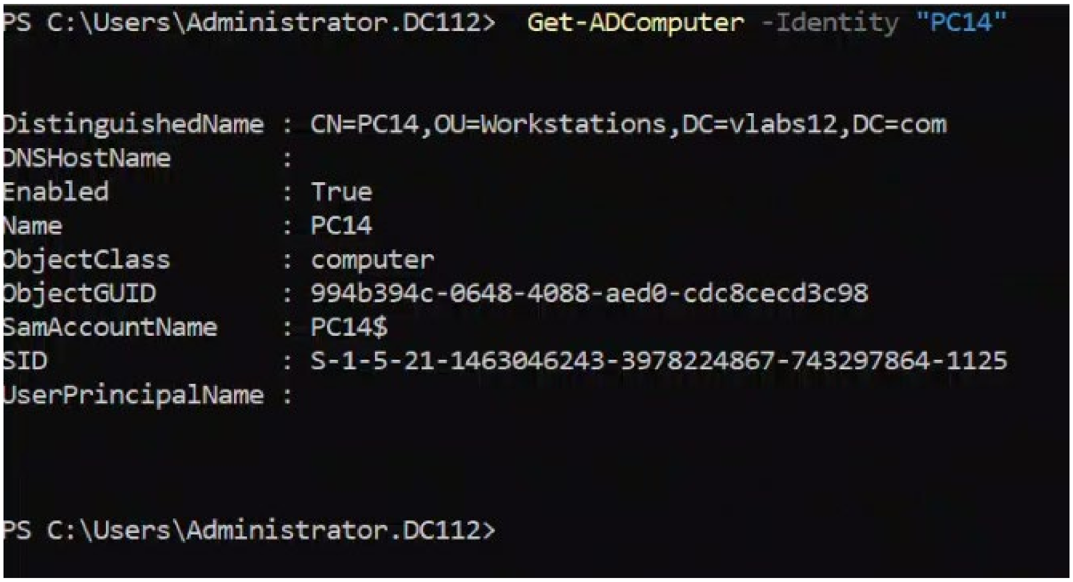
The above user or group can join this computer to a domain

□ Assign this computer account as a Pre-Windows 2000 computer

□ Protect from accidental deletion

Confirm it’s creation on PowerShell using

Get-ADComputer -Identity “PC14”

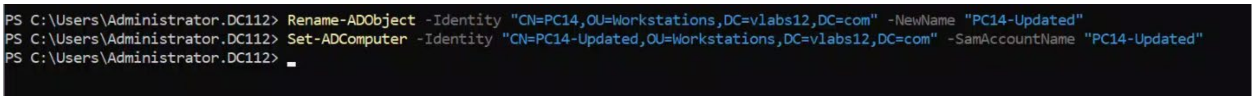


```
PS C:\Users\Administrator.DC112>  Get-ADComputer -Identity "PC14"


DistinguishedName : CN=PC14,OU=Workstations,DC=vlabs12,DC=com
DNSHostName       :
Enabled           : True
Name              : PC14
ObjectClass       : computer
ObjectGUID        : 994b394c-0648-4088-aed0-cdc8cecd3c98
SamAccountName    : PC14$
SID               : S-1-5-21-1463046243-3978224867-743297864-1125
UserPrincipalName :



PS C:\Users\Administrator.DC112>
```

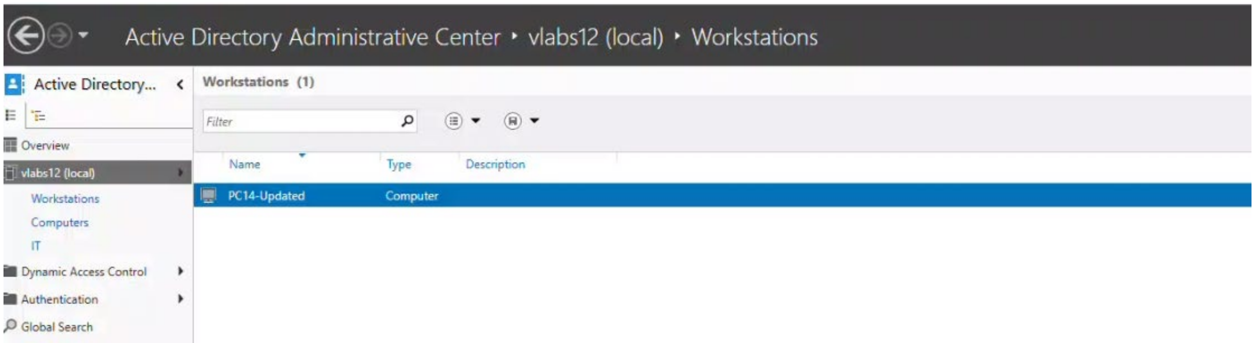
I could not find how to rename PC14 through ADAC. Everything I found online suggested only using PowerShell. There is apparently the option to “rename” on certain versions on ADAC.

Rename-ADObject -Identity "CN=PC14,OU=Workstations,DC=vlabs12,DC=local" -NewName "PC14-Updated"

Set-ADComputer -Identity "CN=PC14-Updated,OU=Workstations,DC=vlabs12,DC=com" -SamAccountName "PC14-Updated"



```
PS C:\Users\Administrator.DC112> Rename-ADObject -Identity "CN=PC14,OU=Workstations,DC=vlabs12,DC=com" -NewName "PC14-Updated"
PS C:\Users\Administrator.DC112> Set-ADComputer -Identity "CN=PC14-Updated,OU=Workstations,DC=vlabs12,DC=com" -SamAccountName "PC14-Updated"
PS C:\Users\Administrator.DC112> _
```

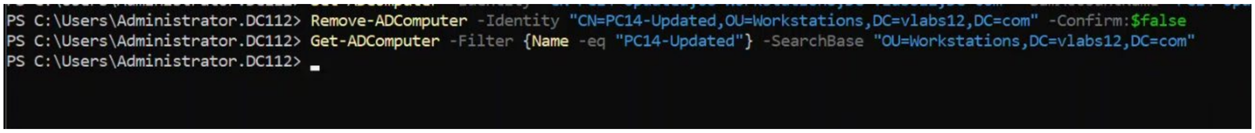


Name	Type	Description
PC14-Updated	Computer	

Remove PC14-Updated in PowerShell using the following commands:

Remove-ADComputer -Identity "CN=PC14-Updated,OU=Workstations,DC=vlabs12,DC=com" -Confirm:$false

Get-ADComputer -Filter {Name -eq "PC14-Updated"} -SearchBase "OU=Workstations,DC=vlabs12,DC=com"



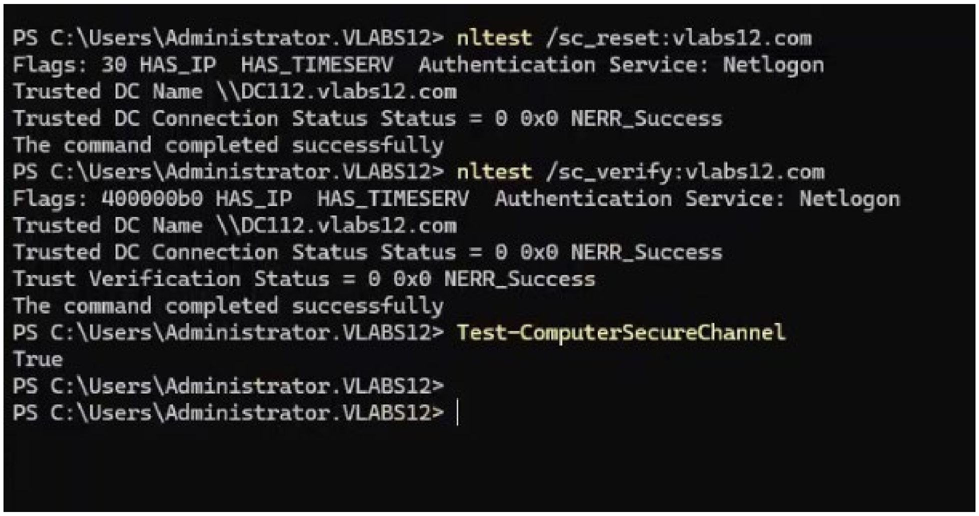
```
PS C:\Users\Administrator.DC112> Remove-ADComputer -Identity "CN=PC14-Updated,OU=Workstations,DC=vlabs12,DC=com" -Confirm:$false
PS C:\Users\Administrator.DC112> Get-ADComputer -Filter {Name -eq "PC14-Updated"} -SearchBase "OU=Workstations,DC=vlabs12,DC=com"
PS C:\Users\Administrator.DC112> _
```

Reset the secure channel for Client12 using PowerShell

Nltest /sc_reset:vlabs12.com

Test-ComputerSecureChannel

The return prompt “True” means the secure channel is restored



```
PS C:\Users\Administrator.VLABS12> nltest /sc_reset:vlabs12.com
Flags: 30 HAS_IP  HAS_TIMESERV  Authentication Service: Netlogon
Trusted DC Name \\DC112.vlabs12.com
Trusted DC Connection Status Status = 0 0x0 NERR_Success
The command completed successfully
PS C:\Users\Administrator.VLABS12> nltest /sc_verify:vlabs12.com
Flags: 400000b0 HAS_IP  HAS_TIMESERV  Authentication Service: Netlogon
Trusted DC Name \\DC112.vlabs12.com
Trusted DC Connection Status Status = 0 0x0 NERR_Success
Trust Verification Status = 0 0x0 NERR_Success
The command completed successfully
PS C:\Users\Administrator.VLABS12> Test-ComputerSecureChannel
True
PS C:\Users\Administrator.VLABS12>
PS C:\Users\Administrator.VLABS12> |
```

Task 2: Redirecting the Computers Container

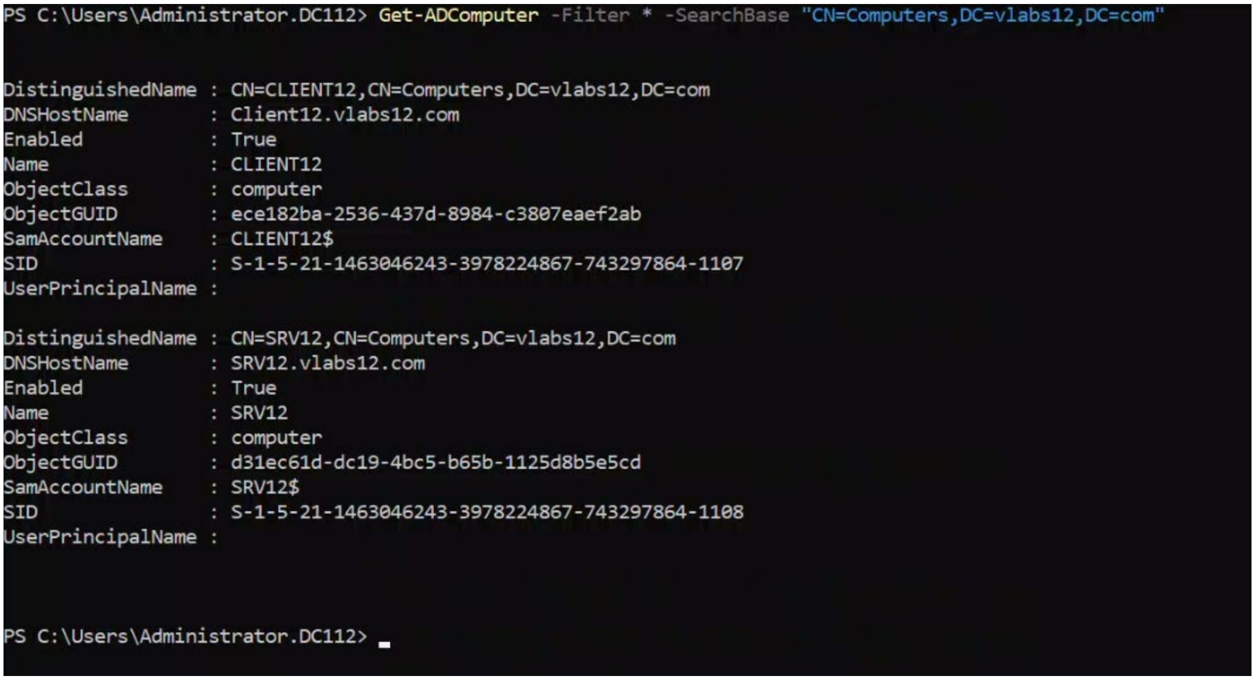
Verify the default Computers container location using PowerShell.

Redirect the default location of the Computers container to the Workstations OU using PowerShell.

Verify that the redirection was applied using PowerShell.

Verify the Computers container with the following command:

Get-ADComputer -Filter * -SearchBase "CN=Computers,DC=vlabs12,DC=com"

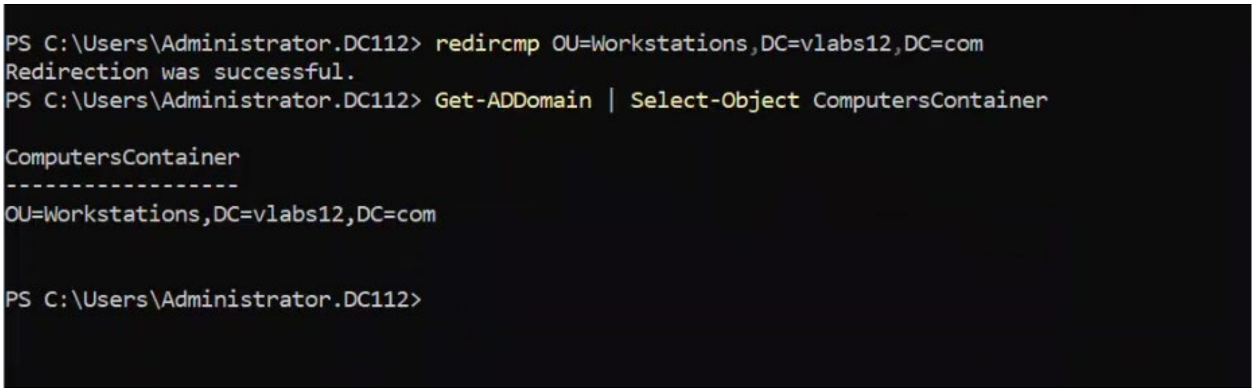


```
PS C:\Users\Administrator.DC112> Get-ADComputer -Filter * -SearchBase "CN=Computers,DC=vlabs12,DC=com"


DistinguishedName : CN=CLIENT12,CN=Computers,DC=vlabs12,DC=com
DNSHostName       : Client12.vlabs12.com
Enabled           : True
Name              : CLIENT12
ObjectClass       : computer
ObjectGUID        : ece182ba-2536-437d-8984-c3807eaef2ab
SamAccountName    : CLIENT12$
SID               : S-1-5-21-1463046243-3978224867-743297864-1107
UserPrincipalName :

DistinguishedName : CN=SRV12,CN=Computers,DC=vlabs12,DC=com
DNSHostName       : SRV12.vlabs12.com
Enabled           : True
Name              : SRV12
ObjectClass       : computer
ObjectGUID        : d31ec61d-dc19-4bc5-b65b-1125d8b5e5cd
SamAccountName    : SRV12$
SID               : S-1-5-21-1463046243-3978224867-743297864-1108
UserPrincipalName :



PS C:\Users\Administrator.DC112> _
```

Redirect the default Computers container to Workstation OU using the following:

redircmp OU=Workstations,DC=vlabs12,DC=com

Confirm the redirection with **Get-ADDomain | Select-Object ComputersContainer**



```
PS C:\Users\Administrator.DC112> redircmp OU=Workstations,DC=vlabs12,DC=com
Redirection was successful.
PS C:\Users\Administrator.DC112> Get-ADDomain | Select-Object ComputersContainer

ComputersContainer
------------------
OU=Workstations,DC=vlabs12,DC=com


PS C:\Users\Administrator.DC112>
```

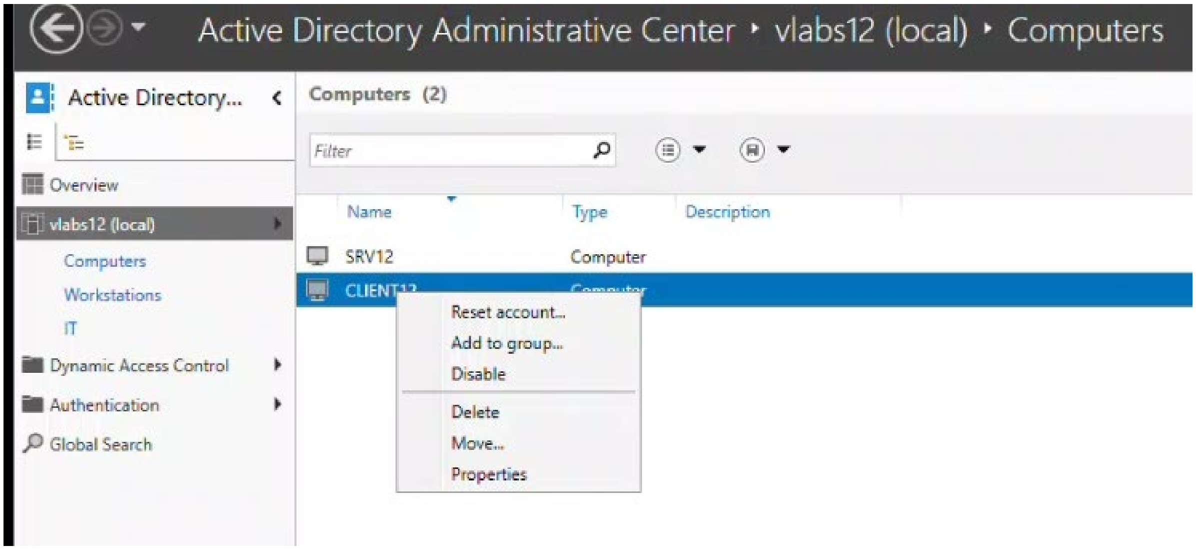
Task 3: Moving Computer Objects

Move ClientXX from Computers container to Workstations OU using ADAC.

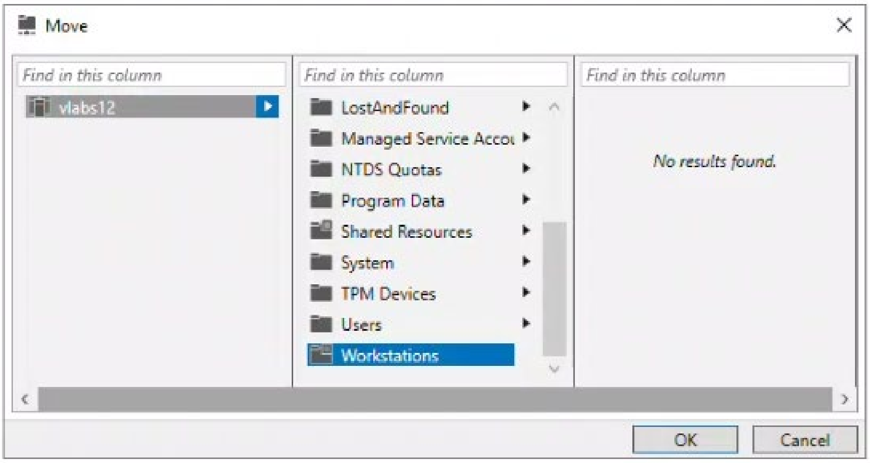
Create an OU named Servers using PowerShell.

Move SRVXX to the Servers OU using PowerShell.

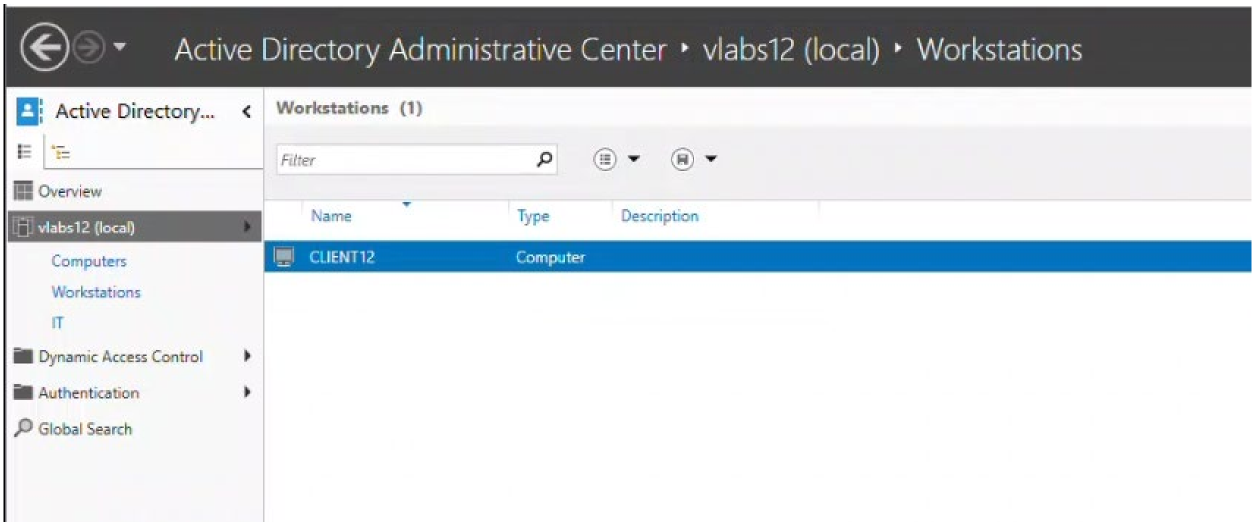
Move Client12 from the Computers container to the Workstation OU by right clicking → Move



Select Workstations and then click OK



Confrim Client12 has been moved to Workstations



This would be the PowerShell command:

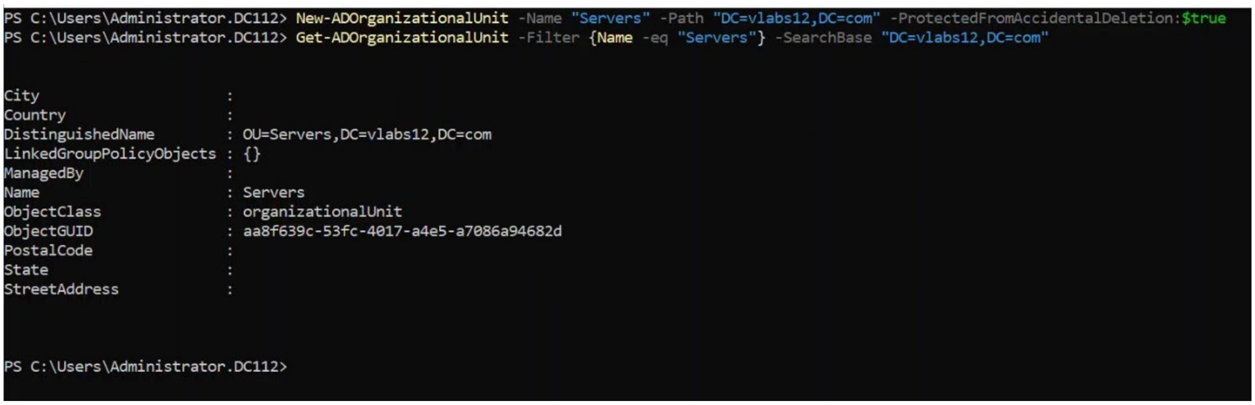
Get-ADComputer -Filter * -SearchBase "CN=Client12,CN=Computers,DC=vlabs12,DC=com" | Move-ADObject-TargetPath "OU=Workstations,DC=vlabs12,DC=com"

Get-ADComputer -Filter * -SearchBase “CN=Client12,OU=Workstations,DC=vlabs12,DC=com”

Create the OU “Servers” in PowerShell

New-ADOrganizationalUnit -Name "Servers" -Path "DC=vlabs12,DC=com" -ProtectedFromAccidentalDeletion:$true

Get-ADOrganizationalUnit -Filter {Name -eq "Servers"} -SearchBase "DC=vlabs12,DC=com"

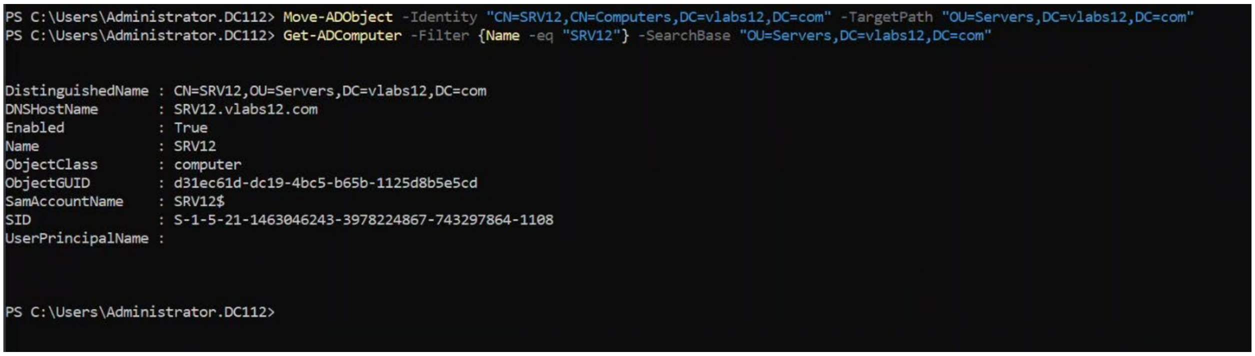


```
PS C:\Users\Administrator.DC112> New-ADOrganizationalUnit -Name "Servers" -Path "DC=vlabs12,DC=com" -ProtectedFromAccidentalDeletion:$true
PS C:\Users\Administrator.DC112> Get-ADOrganizationalUnit -Filter {Name -eq "Servers"} -SearchBase "DC=vlabs12,DC=com"


City                     :
Country                  :
DistinguishedName        : OU=Servers,DC=vlabs12,DC=com
LinkedGroupPolicyObjects : {}
ManagedBy                :
Name                     : Servers
ObjectClass              : organizationalUnit
ObjectGUID               : aa8f639c-53fc-4017-a4e5-a7086a94682d
PostalCode               :
State                    :
StreetAddress            :



PS C:\Users\Administrator.DC112>
```

Move SRV12 to Servers using the following PoweShell commands:

Move-ADObject -Identity "CN=SRV12,CN=Computers,DC=vlabs12,DC=com" -TargetPath "OU=Servers,DC=vlabs12,DC=com"

Get-ADComputer -Filter {Name -eq "SRV12"} -SearchBase "OU=Servers,DC=vlabs12,DC=com"



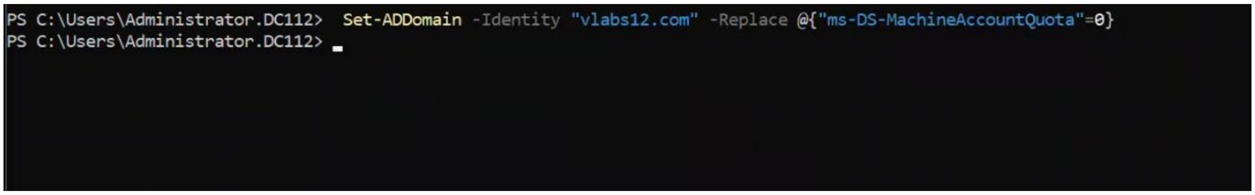
```
PS C:\Users\Administrator.DC112> Move-ADObject -Identity "CN=SRV12,CN=Computers,DC=vlabs12,DC=com" -TargetPath "OU=Servers,DC=vlabs12,DC=com"
PS C:\Users\Administrator.DC112> Get-ADComputer -Filter {Name -eq "SRV12"} -SearchBase "OU=Servers,DC=vlabs12,DC=com"


DistinguishedName : CN=SRV12,OU=Servers,DC=vlabs12,DC=com
DNSHostName       : SRV12.vlabs12.com
Enabled           : True
Name              : SRV12
ObjectClass       : computer
ObjectGUID        : d31ec61d-dc19-4bc5-b65b-1125d8b5e5cd
SamAccountName    : SRV12$
SID               : S-1-5-21-1463046243-3978224867-743297864-1108
UserPrincipalName :


PS C:\Users\Administrator.DC112>
```

Task 4: Changing the Default Quota for Creating Computer Objects

Change the Default Quota for creating Computer Objects to 0 using PowerShell.

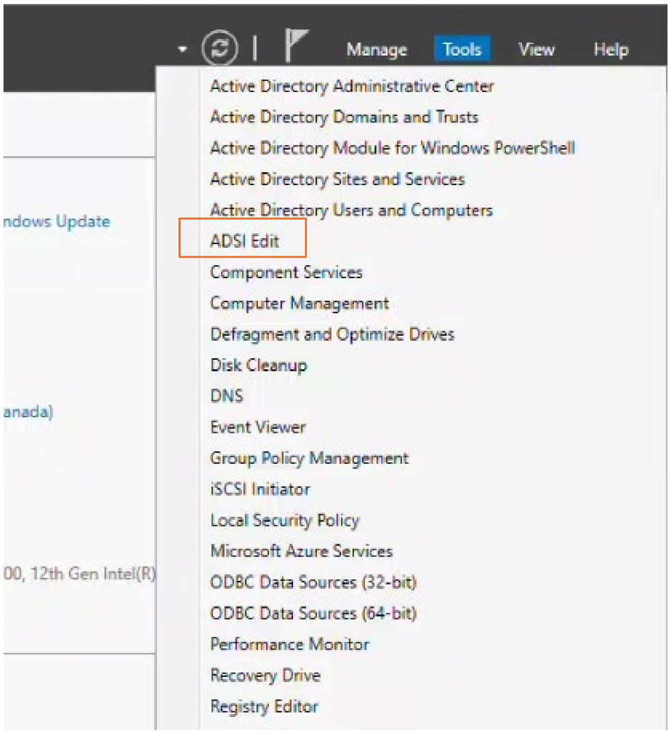
Verify the change using ADSI Edit.

Set-ADDomain -Identity "vlabs12.com" -Replace @{"ms-DS-MachineAccountQuota"=0}

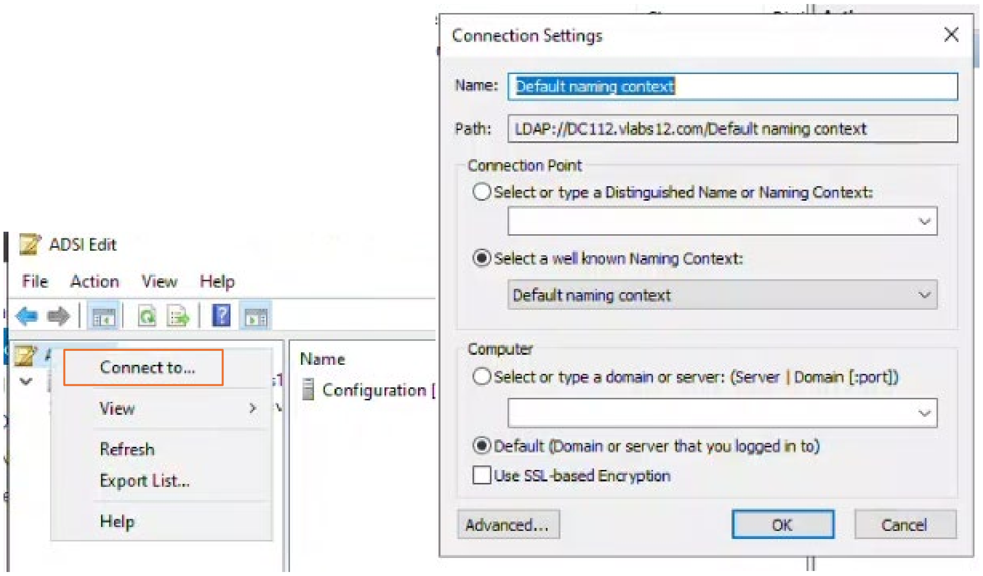


```
PS C:\Users\Administrator.DC112>  Set-ADDomain -Identity "vlabs12.com" -Replace @{"ms-DS-MachineAccountQuota"=0}
PS C:\Users\Administrator.DC112> _
```

Confirm graphically by using ADSI Edit in AD. Go to Tools → ADSI Edit


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Recovery Drive
Registry Editor
ndows Update
anada)
00, 12th Gen Intel(R)

Right-click and select "connect to.." → Name: Default naming context. Click OK


Connection Settings

Name: Default naming context

Path: LDAP://DC112.vlabs12.com/Default naming context

Connection Point

○ Select or type a Distinguished Name or Naming Context:

● Select a well known Naming Context: Default naming context

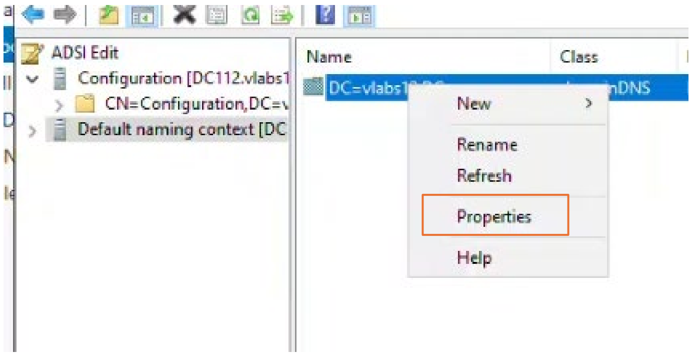
Computer

○ Select or type a domain or server: (Server | Domain [:port])

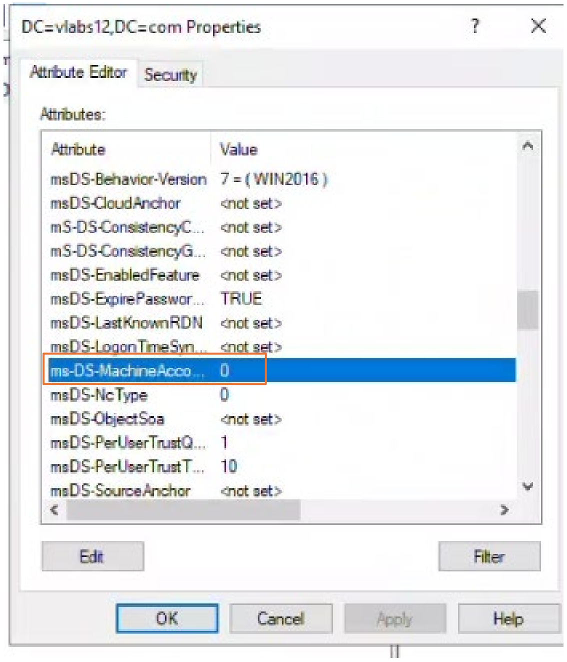
● Default (Domain or server that you logged in to)

□ Use SSL-based Encryption

Right-click on DC=vlabs12,DC=com and go to properties



Scroll down until you find ms-DS-MachineAccountQuota and verify it's set to 0, like we just configured in PowerShell



Attribute	Value
msDS-Behavior-Version	7 = (WIN2016)
msDS-CloudAnchor	<not set>
mS-DS-ConsistencyC...	<not set>
mS-DS-ConsistencyG...	<not set>
msDS-EnabledFeature	<not set>
msDS-ExpirePasswor...	TRUE
msDS-LastKnownRDN	<not set>
msDS-LogonTimeSyn...	<not set>
ms-DS-MachineAcco...	0
msDS-NcType	0
msDS-ObjectSoa	<not set>
msDS-PerUserTrustQ...	1
msDS-PerUserTrustT...	10
msDS-SourceAnchor	<not set>

Task 5: Managing Organizational Units (OUs)

Create IT Department OU under vlabs.com using ADAC:

Verify that IT Department OU has been created using PowerShell.

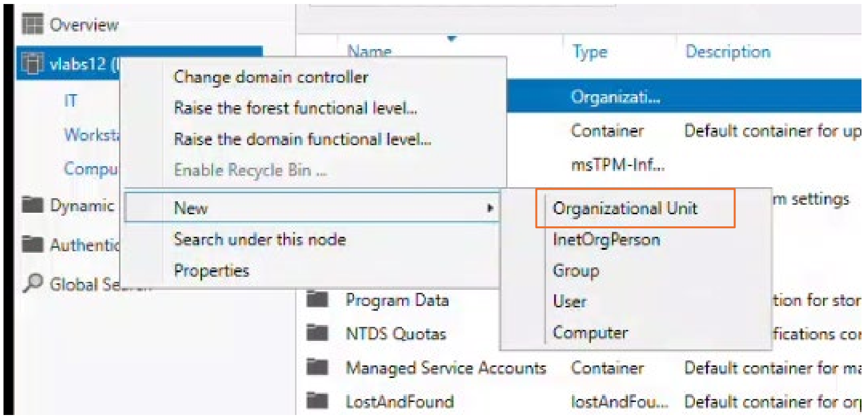
Add a description: "Handles IT operations and security" to the IT Department OU using PowerShell.

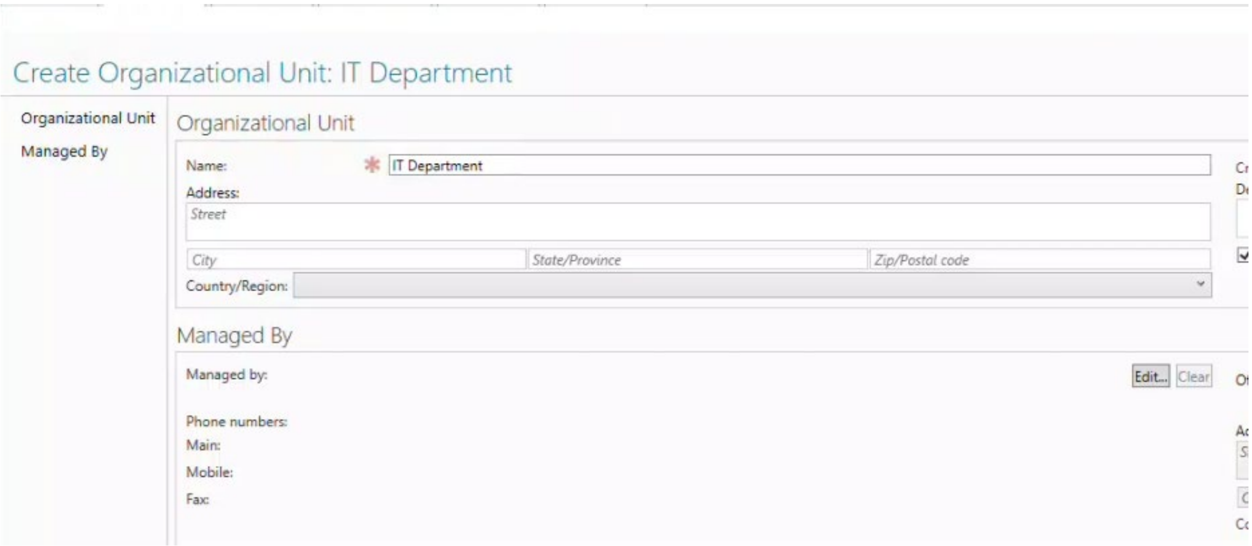
Rename IT Department to IT Services using ADAC.

Create Finance OU using ADAC and verify the creation using PowerShell.

Delete the Finance OU using PowerShell and verify the deletion in PowerShell.

Create the OU “IT Department”



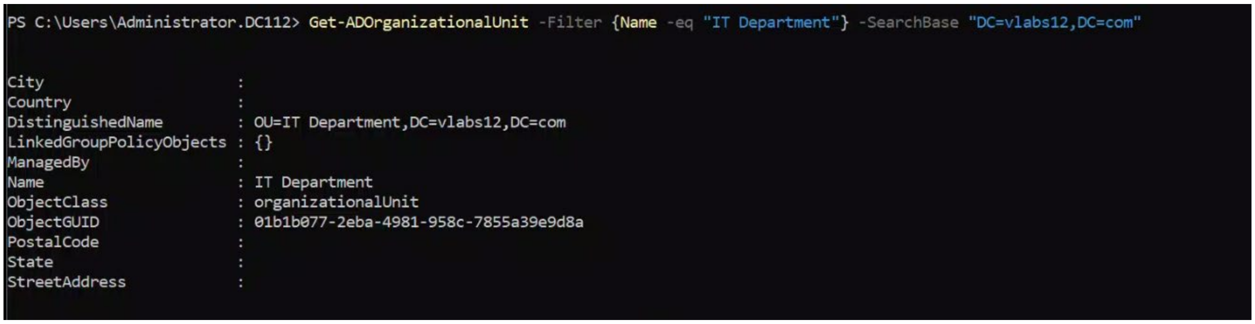


Create Organizational Unit: IT Department

Organizational Unit

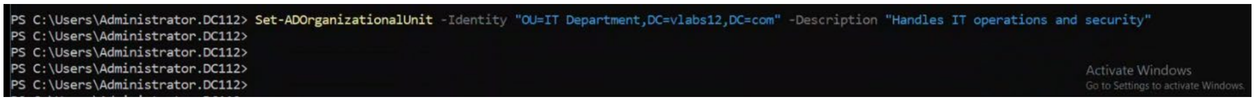
Name: * IT Department

```
Get-ADOrganizationalUnit -Filter {Name -eq "IT Department"} -SearchBase "DC=vlabs12,DC=com"
```



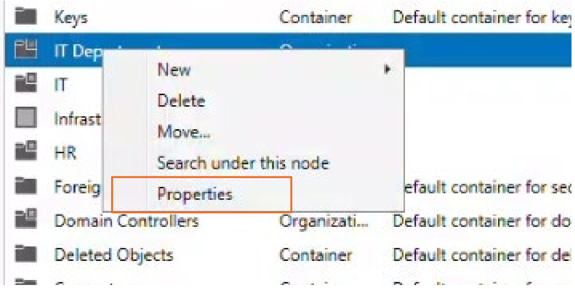
```
PS C:\Users\Administrator.DC112> Get-ADOrganizationalUnit -Filter {Name -eq "IT Department"} -SearchBase "DC=vlabs12,DC=com"


City                     :
Country                  :
DistinguishedName        : OU=IT Department,DC=vlabs12,DC=com
LinkedGroupPolicyObjects : {}
ManagedBy                :
Name                     : IT Department
ObjectClass              : organizationalUnit
ObjectGUID               : 01b1b077-2eba-4981-958c-7855a39e9d8a
PostalCode               :
State                    :
StreetAddress            :
```

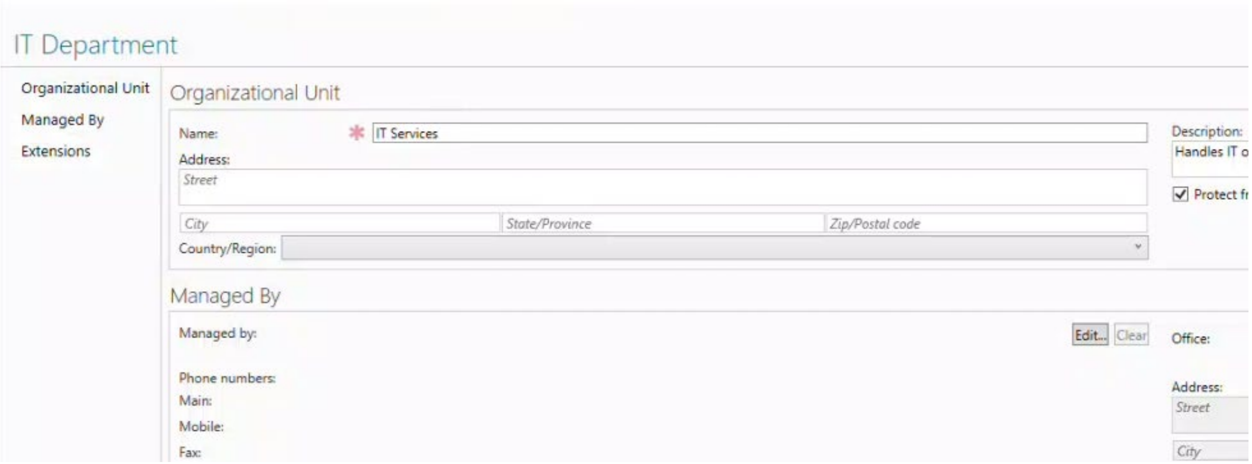
Set-ADOrganizationalUnit -Identity "OU=IT Department,DC=vlabs12,DC=com" -Description "Handles IT operations and security"



```
PS C:\Users\Administrator.DC112> Set-ADOrganizationalUnit -Identity "OU=IT Department,DC=vlabs12,DC=com" -Description "Handles IT operations and security"
PS C:\Users\Administrator.DC112>
PS C:\Users\Administrator.DC112>
PS C:\Users\Administrator.DC112>
PS C:\Users\Administrator.DC112>
```

Rename IT Department to IT Services by right clicking → Properties





Organizational Unit

Name: * IT Services

Address:

Street

City | State/Province | Zip/Postal code

Country/Region:

Description: Handles IT o

☑ Protect fr

Managed By

Managed by:

Office:

Phone numbers:

Main:

Mobile:

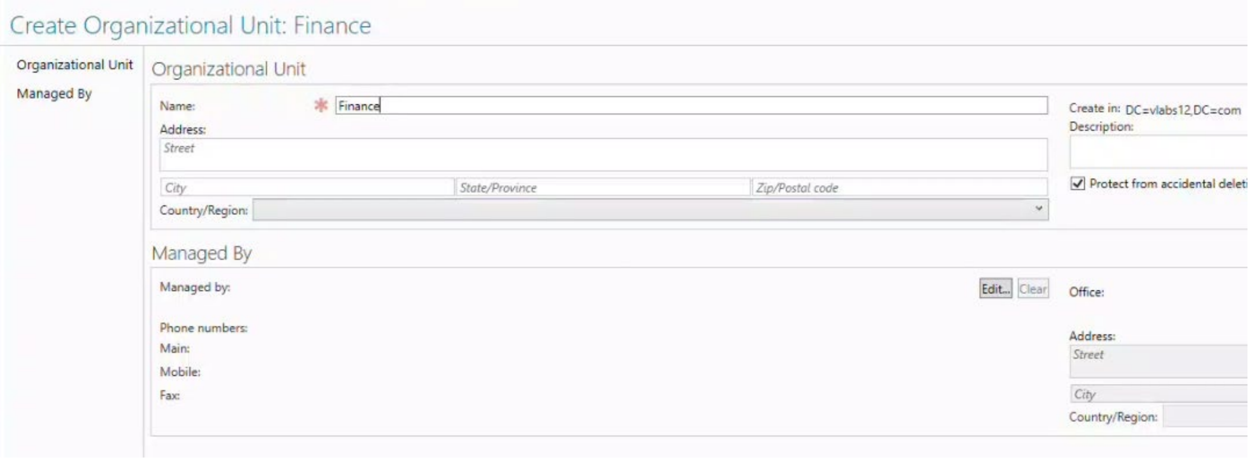
Fax:

Address:

Street

City

Create the Finance OU



Create Organizational Unit: Finance

Organizational Unit

Name: * Finance

Address:

Create in: DC=vlabs12,DC=com

Description:

☑ Protect from accidental deleti

Managed By

Managed by:

Phone numbers:

Main:

Mobile:

Fax:

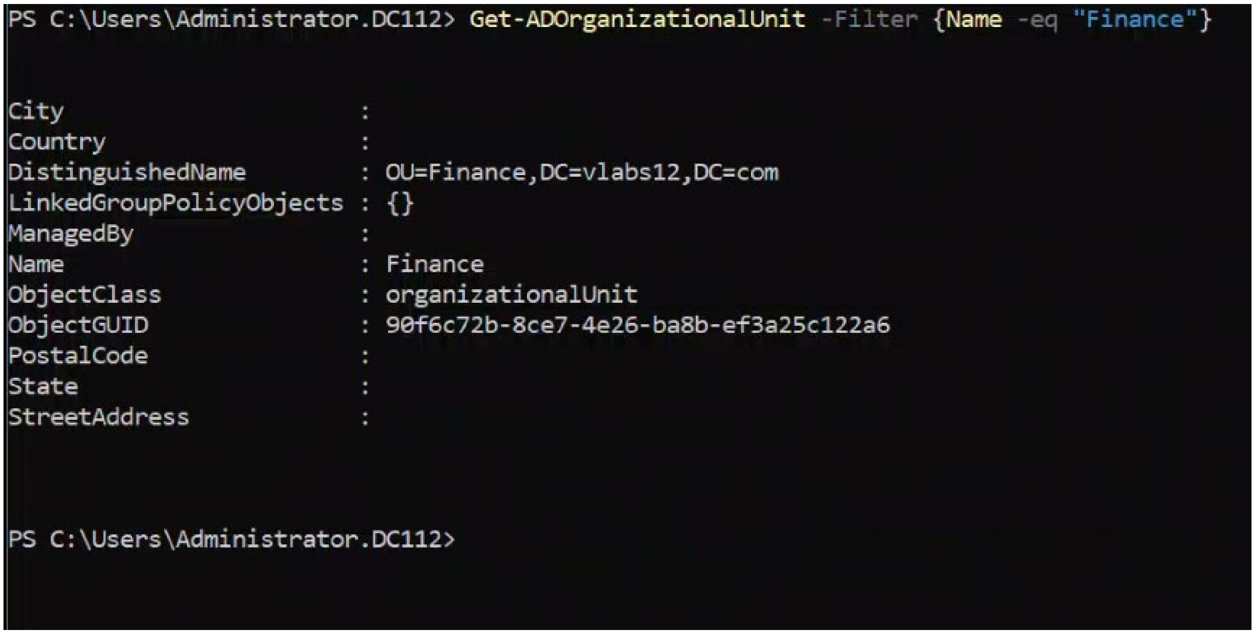
Office:

Address:

Country/Region:

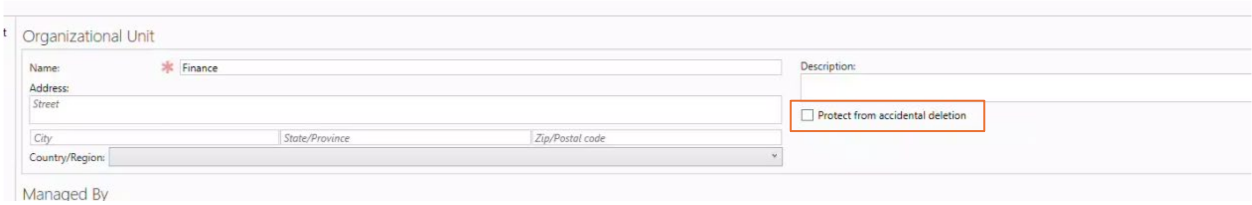
Confirm it’s creation with PowerShell using the following:

Get-ADOrganizationalUnit-Filter {Name -eq "Finance"}



```
PS C:\Users\Administrator.DC112> Get-ADOrganizationalUnit -Filter {Name -eq "Finance"}


City                     :
Country                  :
DistinguishedName        : OU=Finance,DC=vlabs12,DC=com
LinkedGroupPolicyObjects : {}
ManagedBy                :
Name                     : Finance
ObjectClass              : organizationalUnit
ObjectGUID               : 90f6c72b-8ce7-4e26-ba8b-ef3a25c122a6
PostalCode               :
State                    :
StreetAddress            :



PS C:\Users\Administrator.DC112>
```

To delete Finance, we have to first uncheck “Protect from accidental deletion”



Organizational Unit

Name: * Finance

Address:

Street

City | State/Province | Zip/Postal code

Country/Region:

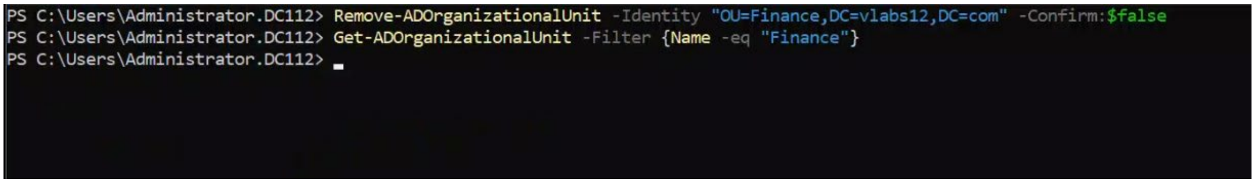
Description:

□ Protect from accidental deletion

Managed By

Remove-ADOrganizationalUnit -Identity "OU=Finance,DC=vlabs12,DC=com" -Confirm:$false

Get-ADOrganizationalUnit -Filter {Name -eq "Finance"}



```
PS C:\Users\Administrator.DC112> Remove-ADOrganizationalUnit -Identity "OU=Finance,DC=vlabs12,DC=com" -Confirm:$false
PS C:\Users\Administrator.DC112> Get-ADOrganizationalUnit -Filter {Name -eq "Finance"}
PS C:\Users\Administrator.DC112> _
```

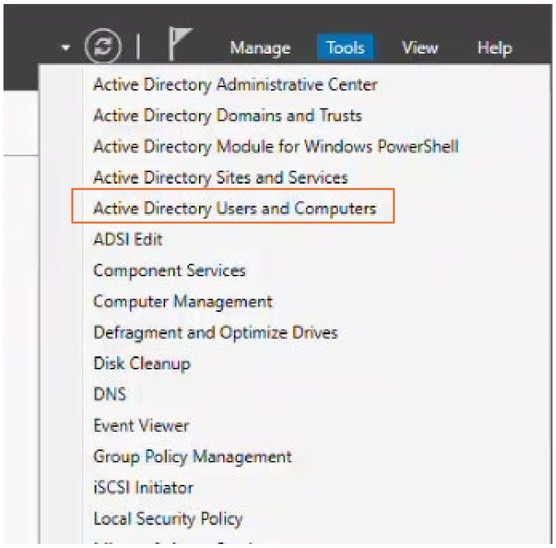
Task 6: Delegating Control of an OU

Use the Delegation of Control Wizard in AD Users and Computers to delegate Reset Password permissions to Sophie Lambert on the IT Services OU.

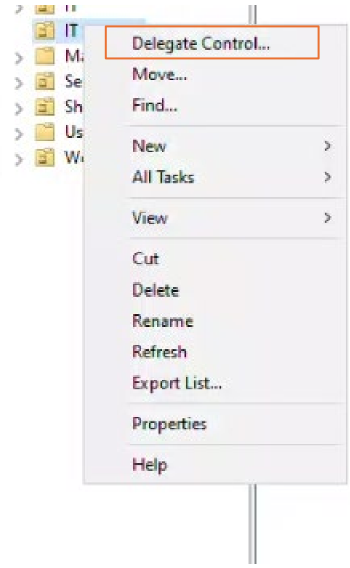
Check which users or groups have been delegated control over the IT Services OU using AD Users and Computers 3.

List the delegation permissions on the IT Services OU using PowerShell.

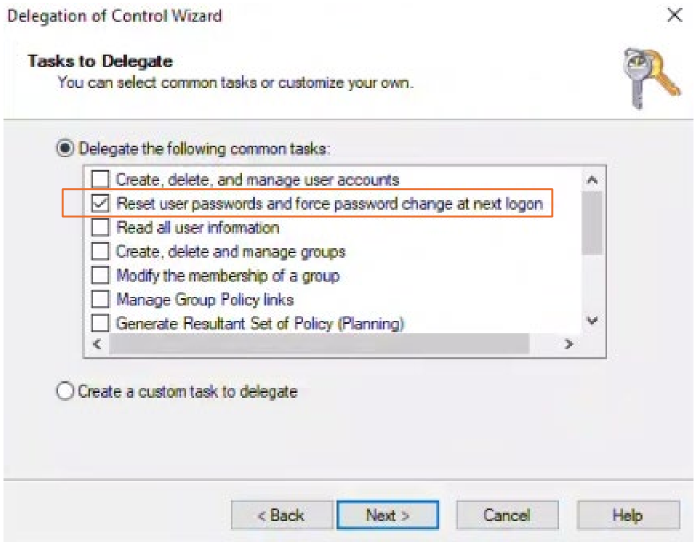
Delegate “Reset Password” permission to Sophie Lambert using AD Users and Computers. Go to Tools → Active Directory Users and Computers


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy

Right click on IT Services and click on Delegate Control



Check the box “Reset user passwords and force password change at next logon” → Next



Delegation of Control Wizard

Tasks to Delegate

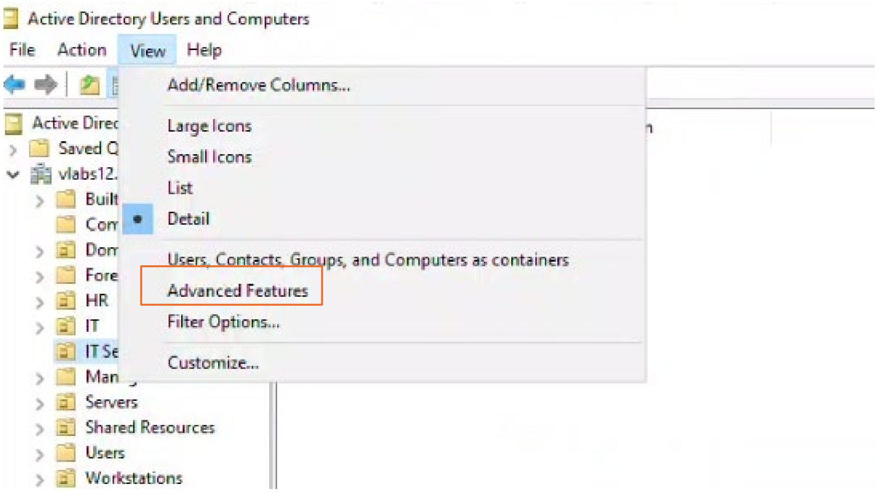
You can select common tasks or customize your own.

● Delegate the following common tasks:

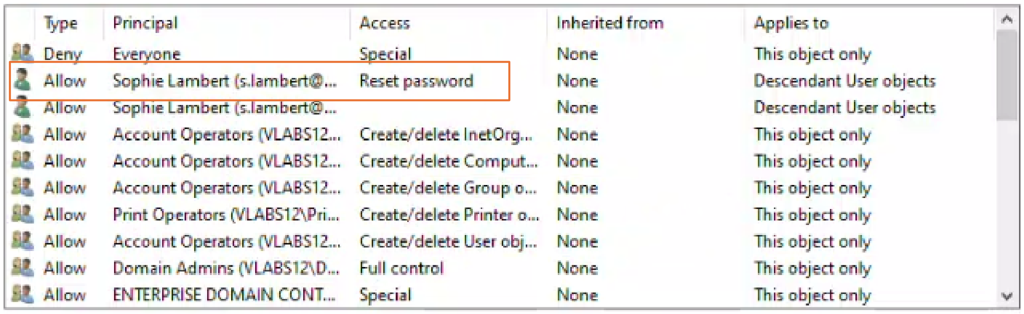
- □ Create, delete, and manage user accounts
- ☑ Reset user passwords and force password change at next logon
- □ Read all user information
- □ Create, delete and manage groups
- □ Modify the membership of a group
- □ Manage Group Policy links
- □ Generate Resultant Set of Policy (Planning)

○ Create a custom task to delegate

Once that's done, go to view at the top and select Advanced Feautures



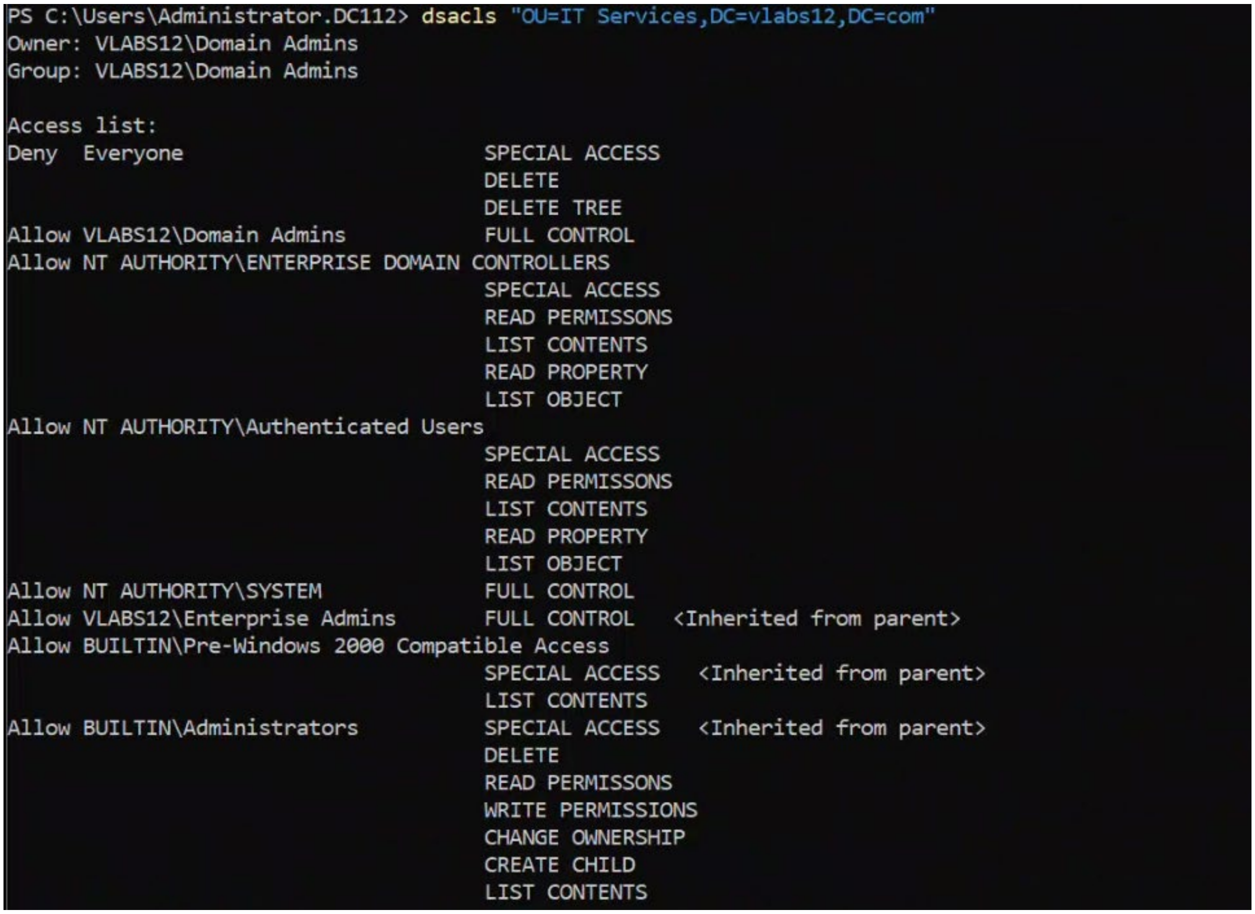
Right click on IT Services → Properties → Security → Advanced



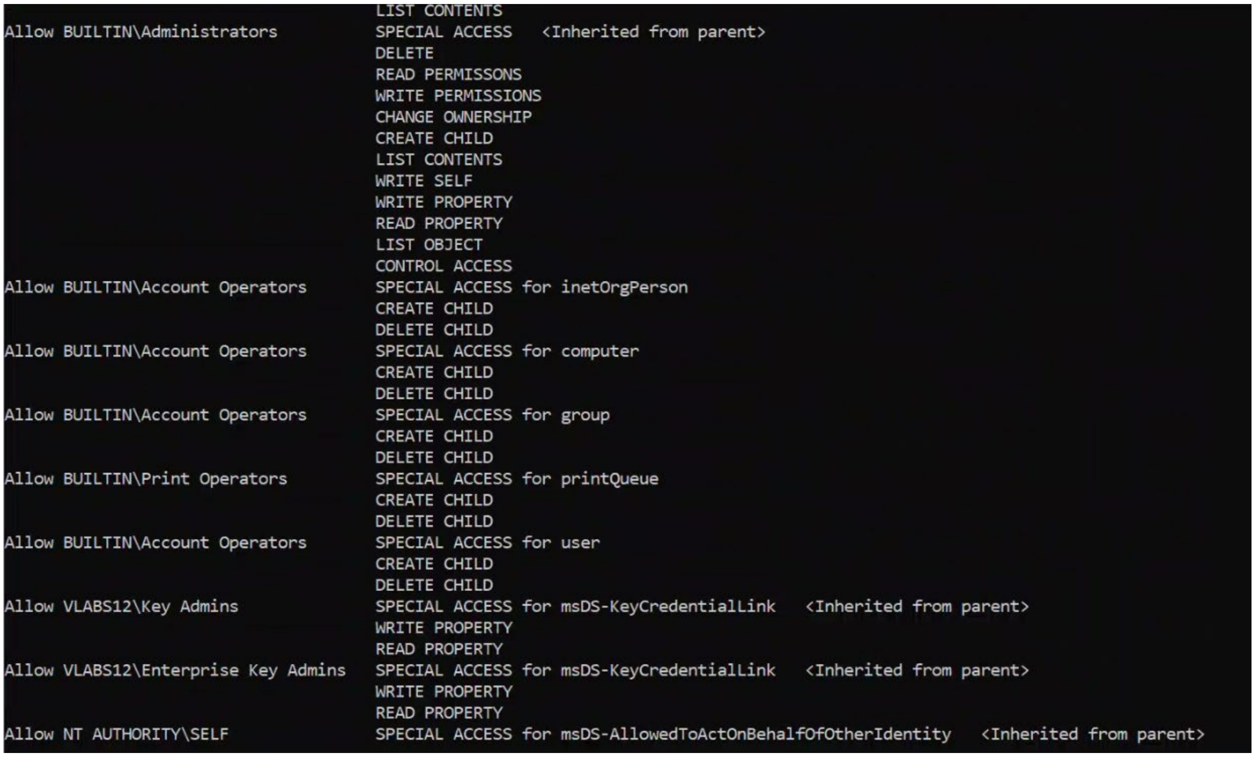
Type	Principal	Access	Inherited from	Applies to
Deny	Everyone	Special	None	This object only
Allow	Sophie Lambert (s.lambert@...	Reset password	None	Descendant User objects
Allow	Sophie Lambert (s.lambert@...		None	Descendant User objects
Allow	Account Operators (VLABS12...	Create/delete InetOrg...	None	This object only
Allow	Account Operators (VLABS12...	Create/delete Comput...	None	This object only
Allow	Account Operators (VLABS12...	Create/delete Group o...	None	This object only
Allow	Print Operators (VLABS12\Pri...	Create/delete Printer o...	None	This object only
Allow	Account Operators (VLABS12...	Create/delete User obj...	None	This object only
Allow	Domain Admins (VLABS12\D...	Full control	None	This object only
Allow	ENTERPRISE DOMAIN CONT...	Special	None	This object only

Verify the current permissions for IT Services using PowerShell

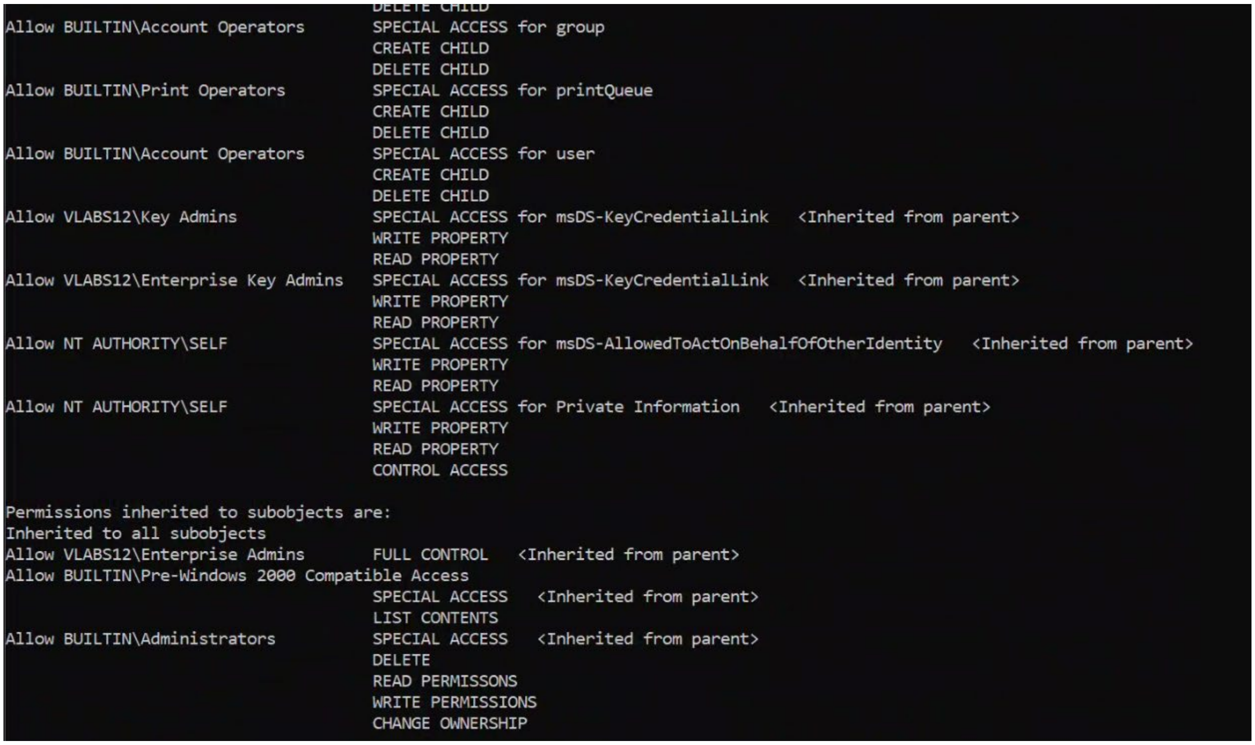
dsacls "OU=IT Services,DC=vlabs12,DC=com"



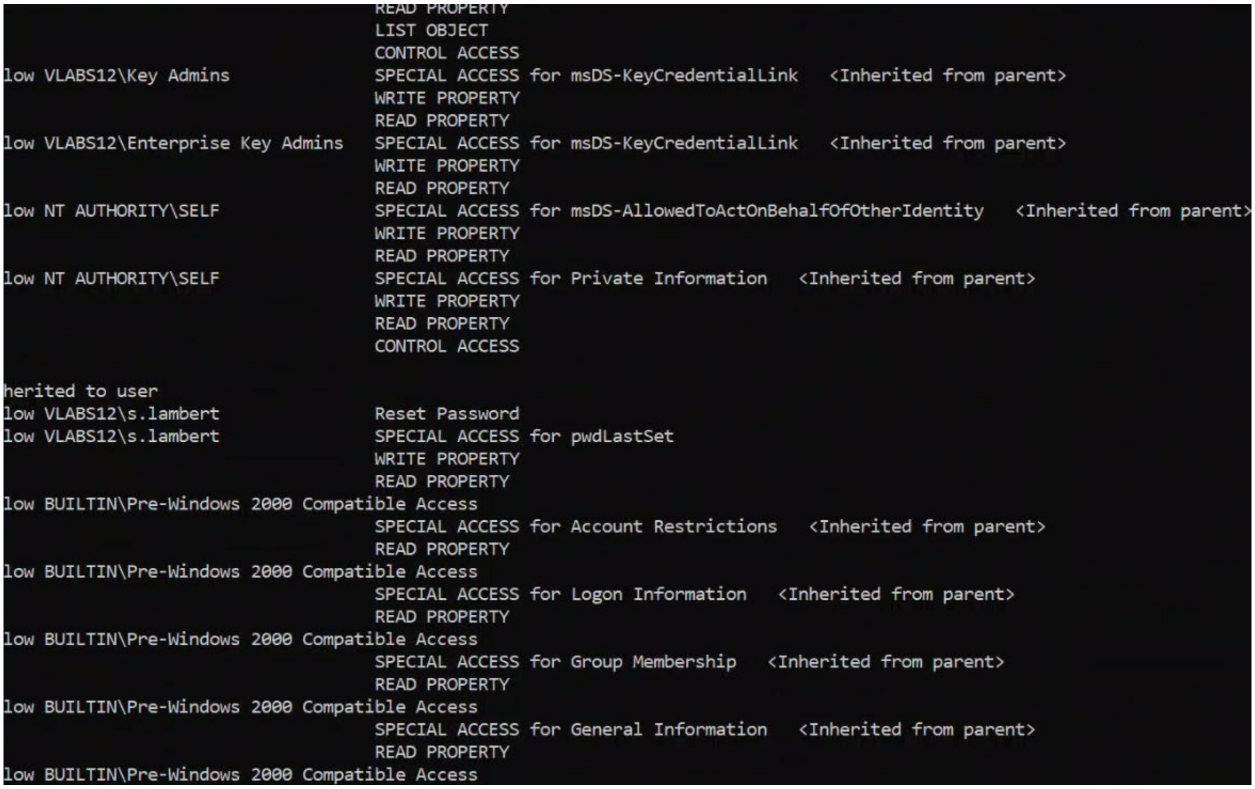
```
PS C:\Users\Administrator.DC112> dsacls "OU=IT Services,DC=vlabs12,DC=com"
Owner: VLABS12\Domain Admins
Group: VLABS12\Domain Admins

Access list:
Deny  Everyone                        SPECIAL ACCESS
                                      DELETE
                                      DELETE TREE
Allow VLABS12\Domain Admins           FULL CONTROL
Allow NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
                                      SPECIAL ACCESS
                                      READ PERMISSONS
                                      LIST CONTENTS
                                      READ PROPERTY
                                      LIST OBJECT
Allow NT AUTHORITY\Authenticated Users
                                      SPECIAL ACCESS
                                      READ PERMISSONS
                                      LIST CONTENTS
                                      READ PROPERTY
                                      LIST OBJECT
Allow NT AUTHORITY\SYSTEM             FULL CONTROL
Allow VLABS12\Enterprise Admins       FULL CONTROL   <Inherited from parent>
Allow BUILTIN\Pre-Windows 2000 Compatible Access
                                      SPECIAL ACCESS   <Inherited from parent>
                                      LIST CONTENTS
Allow BUILTIN\Administrators          SPECIAL ACCESS   <Inherited from parent>
                                      DELETE
                                      READ PERMISSONS
                                      WRITE PERMISSIONS
                                      CHANGE OWNERSHIP
                                      CREATE CHILD
                                      LIST CONTENTS
```



```
                                      LIST CONTENTS
Allow BUILTIN\Administrators          SPECIAL ACCESS   <Inherited from parent>
                                      DELETE
                                      READ PERMISSONS
                                      WRITE PERMISSIONS
                                      CHANGE OWNERSHIP
                                      CREATE CHILD
                                      LIST CONTENTS
                                      WRITE SELF
                                      WRITE PROPERTY
                                      READ PROPERTY
                                      LIST OBJECT
                                      CONTROL ACCESS
Allow BUILTIN\Account Operators       SPECIAL ACCESS for inetOrgPerson
                                      CREATE CHILD
                                      DELETE CHILD
Allow BUILTIN\Account Operators       SPECIAL ACCESS for computer
                                      CREATE CHILD
                                      DELETE CHILD
Allow BUILTIN\Account Operators       SPECIAL ACCESS for group
                                      CREATE CHILD
                                      DELETE CHILD
Allow BUILTIN\Print Operators         SPECIAL ACCESS for printQueue
                                      CREATE CHILD
                                      DELETE CHILD
Allow BUILTIN\Account Operators       SPECIAL ACCESS for user
                                      CREATE CHILD
                                      DELETE CHILD
Allow VLABS12\Key Admins              SPECIAL ACCESS for msDS-KeyCredentialLink   <Inherited from parent>
                                      WRITE PROPERTY
                                      READ PROPERTY
Allow VLABS12\Enterprise Key Admins   SPECIAL ACCESS for msDS-KeyCredentialLink   <Inherited from parent>
                                      WRITE PROPERTY
                                      READ PROPERTY
Allow NT AUTHORITY\SELF               SPECIAL ACCESS for msDS-AllowedToActOnBehalfOfOtherIdentity   <Inherited from parent>
```



```
                                      DELETE CHILD
Allow BUILTIN\Account Operators       SPECIAL ACCESS for group
                                      CREATE CHILD
                                      DELETE CHILD
Allow BUILTIN\Print Operators         SPECIAL ACCESS for printQueue
                                      CREATE CHILD
                                      DELETE CHILD
Allow BUILTIN\Account Operators       SPECIAL ACCESS for user
                                      CREATE CHILD
                                      DELETE CHILD
Allow VLABS12\Key Admins              SPECIAL ACCESS for msDS-KeyCredentialLink   <Inherited from parent>
                                      WRITE PROPERTY
                                      READ PROPERTY
Allow VLABS12\Enterprise Key Admins   SPECIAL ACCESS for msDS-KeyCredentialLink   <Inherited from parent>
                                      WRITE PROPERTY
                                      READ PROPERTY
Allow NT AUTHORITY\SELF               SPECIAL ACCESS for msDS-AllowedToActOnBehalfOfOtherIdentity   <Inherited from parent>
                                      WRITE PROPERTY
                                      READ PROPERTY
Allow NT AUTHORITY\SELF               SPECIAL ACCESS for Private Information   <Inherited from parent>
                                      WRITE PROPERTY
                                      READ PROPERTY
                                      CONTROL ACCESS

Permissions inherited to subobjects are:
Inherited to all subobjects
Allow VLABS12\Enterprise Admins       FULL CONTROL   <Inherited from parent>
Allow BUILTIN\Pre-Windows 2000 Compatible Access
                                      SPECIAL ACCESS   <Inherited from parent>
                                      LIST CONTENTS
Allow BUILTIN\Administrators          SPECIAL ACCESS   <Inherited from parent>
                                      DELETE
                                      READ PERMISSONS
                                      WRITE PERMISSIONS
                                      CHANGE OWNERSHIP
```



```
                                    READ PROPERTY
                                    LIST OBJECT
                                    CONTROL ACCESS
low VLABS12\Key Admins              SPECIAL ACCESS for msDS-KeyCredentialLink   <Inherited from parent>
                                    WRITE PROPERTY
                                    READ PROPERTY
low VLABS12\Enterprise Key Admins   SPECIAL ACCESS for msDS-KeyCredentialLink   <Inherited from parent>
                                    WRITE PROPERTY
                                    READ PROPERTY
low NT AUTHORITY\SELF               SPECIAL ACCESS for msDS-AllowedToActOnBehalfOfOtherIdentity   <Inherited from parent>
                                    WRITE PROPERTY
                                    READ PROPERTY
low NT AUTHORITY\SELF               SPECIAL ACCESS for Private Information   <Inherited from parent>
                                    WRITE PROPERTY
                                    READ PROPERTY
                                    CONTROL ACCESS

herited to user
low VLABS12\s.lambert               Reset Password
low VLABS12\s.lambert               SPECIAL ACCESS for pwdLastSet
                                    WRITE PROPERTY
                                    READ PROPERTY
low BUILTIN\Pre-Windows 2000 Compatible Access
                                    SPECIAL ACCESS for Account Restrictions   <Inherited from parent>
                                    READ PROPERTY
low BUILTIN\Pre-Windows 2000 Compatible Access
                                    SPECIAL ACCESS for Logon Information   <Inherited from parent>
                                    READ PROPERTY
low BUILTIN\Pre-Windows 2000 Compatible Access
                                    SPECIAL ACCESS for Group Membership   <Inherited from parent>
                                    READ PROPERTY
low BUILTIN\Pre-Windows 2000 Compatible Access
                                    SPECIAL ACCESS for General Information   <Inherited from parent>
                                    READ PROPERTY
low BUILTIN\Pre-Windows 2000 Compatible Access
```

Task 7: Managing Permissions on Ous

Use PowerShell to deny deletion of objects inside IT Services OU for Sophie Lambert.

Use PowerShell to grant Generic Read (GR) permissions on IT Services OU to Sophie Lambert.

Use PowerShell to grant write permissions for modifying the telephoneNumber attribute for all the users in the HR OU.

Use PowerShell to remove all permissions for Lucas Bernard on the HR OU.

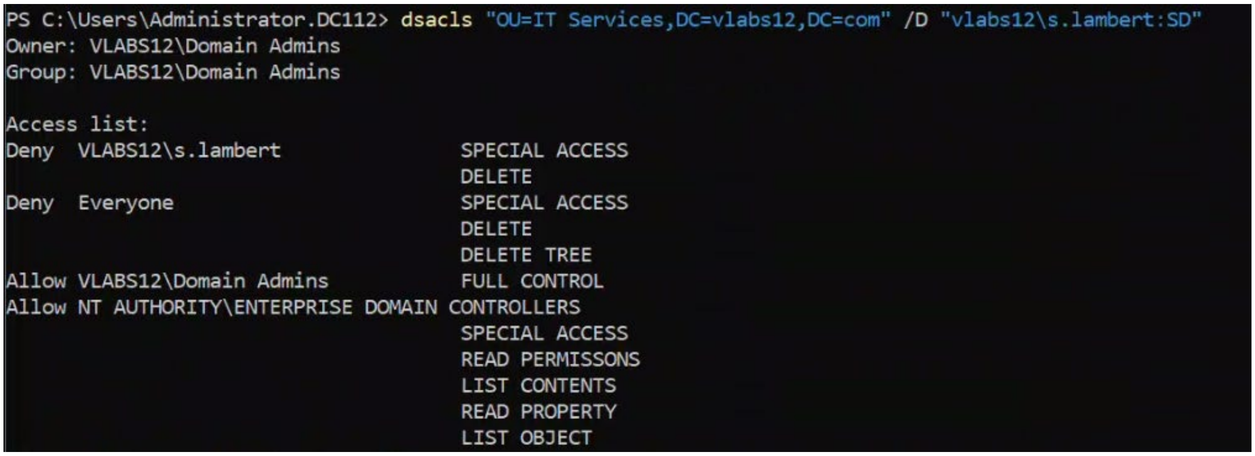
Check which users or groups have been delegated permission over the HR OU using AD Users and Computers.

Reset permissions of the IT Services OU to default using PowerShell.

Check that the permissions of the IT Services OU has been reset to default using AD Users and Computers.

Use the following to deny deletion of objects to Sophie Lambert in IT Services

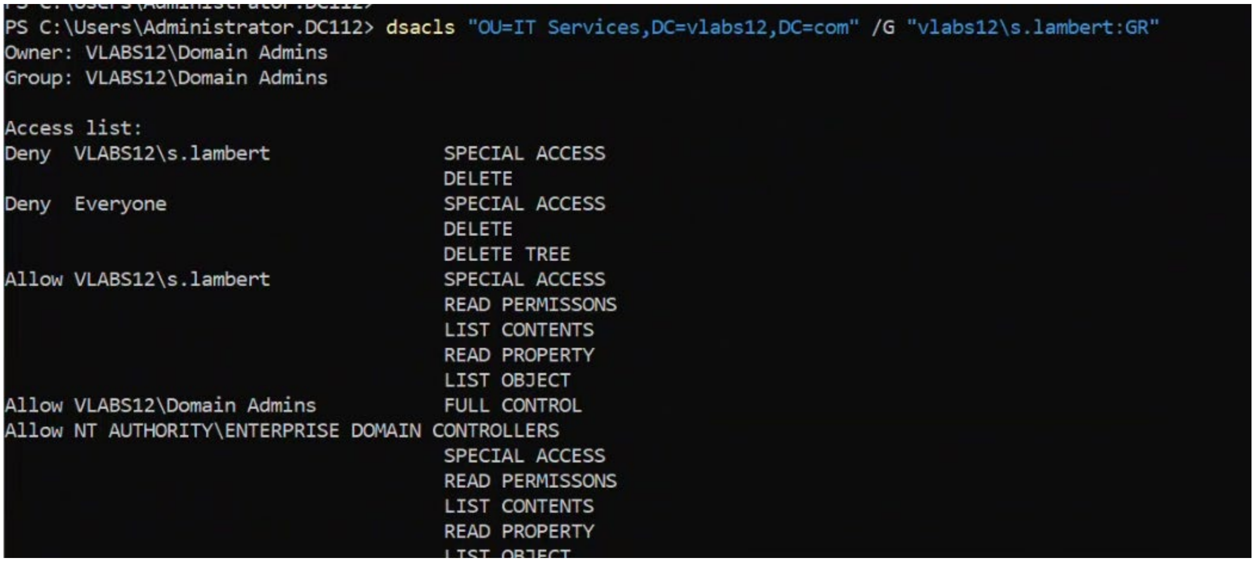
dsacls "OU=IT Services,DC=vlabs12,DC=com" /D "vlabs12\s.lambert:SD"



```
PS C:\Users\Administrator.DC112> dsacls "OU=IT Services,DC=vlabs12,DC=com" /D "vlabs12\s.lambert:SD"
Owner: VLABS12\Domain Admins
Group: VLABS12\Domain Admins

Access list:
Deny  VLABS12\s.lambert               SPECIAL ACCESS
                                      DELETE
Deny  Everyone                        SPECIAL ACCESS
                                      DELETE
                                      DELETE TREE
Allow VLABS12\Domain Admins           FULL CONTROL
Allow NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
                                      SPECIAL ACCESS
                                      READ PERMISSONS
                                      LIST CONTENTS
                                      READ PROPERTY
                                      LIST OBJECT
```

The following grants Sophie Lambert generic read permissions in IT Services

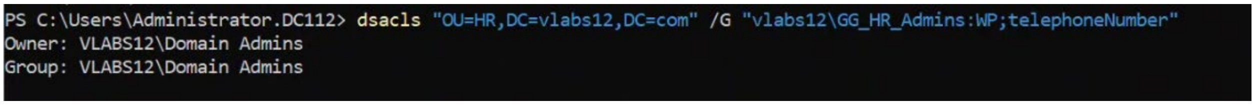
Dsacls “OU=IT Services,DC=vlabs12,DC=com” /G “vlabs12\s.lambert:GR”



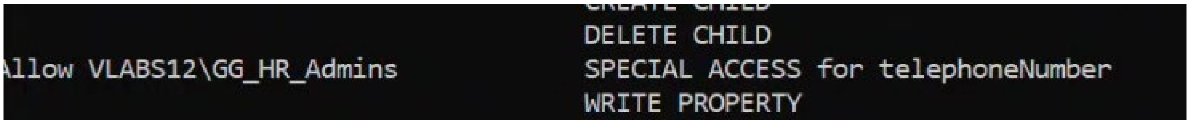
```
PS C:\Users\Administrator.DC112>
PS C:\Users\Administrator.DC112> dsacls "OU=IT Services,DC=vlabs12,DC=com" /G "vlabs12\s.lambert:GR"
Owner: VLABS12\Domain Admins
Group: VLABS12\Domain Admins

Access list:
Deny  VLABS12\s.lambert               SPECIAL ACCESS
                                      DELETE
Deny  Everyone                        SPECIAL ACCESS
                                      DELETE
                                      DELETE TREE
Allow VLABS12\s.lambert               SPECIAL ACCESS
                                      READ PERMISSONS
                                      LIST CONTENTS
                                      READ PROPERTY
                                      LIST OBJECT
Allow VLABS12\Domain Admins           FULL CONTROL
Allow NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
                                      SPECIAL ACCESS
                                      READ PERMISSONS
                                      LIST CONTENTS
                                      READ PROPERTY
                                      LIST OBJECT
```

Grant write permissions in HR OU for modifying the telephoneNumber

Dsacls"OU=HR,DC=vlabs12,DC=com"/G"vlabs12\GG_HR_Admins:WP;telephoneNumber"



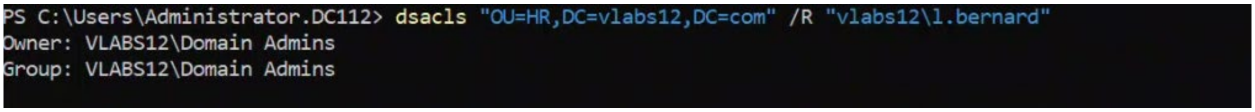
```
PS C:\Users\Administrator.DC112> dsacls "OU=HR,DC=vlabs12,DC=com" /G "vlabs12\GG_HR_Admins:WP;telephoneNumber"
Owner: VLABS12\Domain Admins
Group: VLABS12\Domain Admins
```



```
                                    CREATE CHILD
                                    DELETE CHILD
Allow VLABS12\GG_HR_Admins          SPECIAL ACCESS for telephoneNumber
                                    WRITE PROPERTY
```

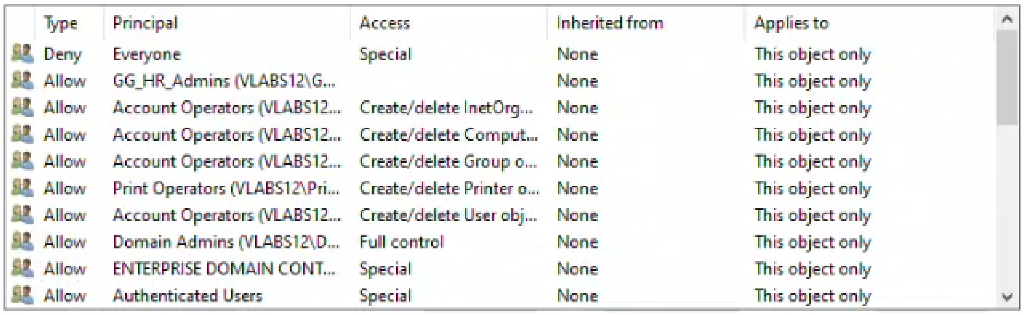
Remove all permissions for Lucas Bernard in HR OU

dsacls "OU=HR,DC=vlabs12,DC=com" /R "vlabs12\l.bernard"

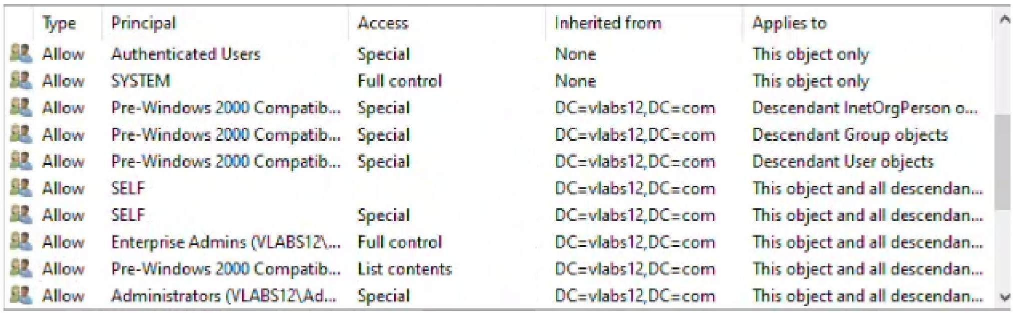


```
PS C:\Users\Administrator.DC112> dsacls "OU=HR,DC=vlabs12,DC=com" /R "vlabs12\l.bernard"
Owner: VLABS12\Domain Admins
Group: VLABS12\Domain Admins
```

In Active Directory Users and Computers, right click on HR → Properties → Security → Advanced and verify the permissions



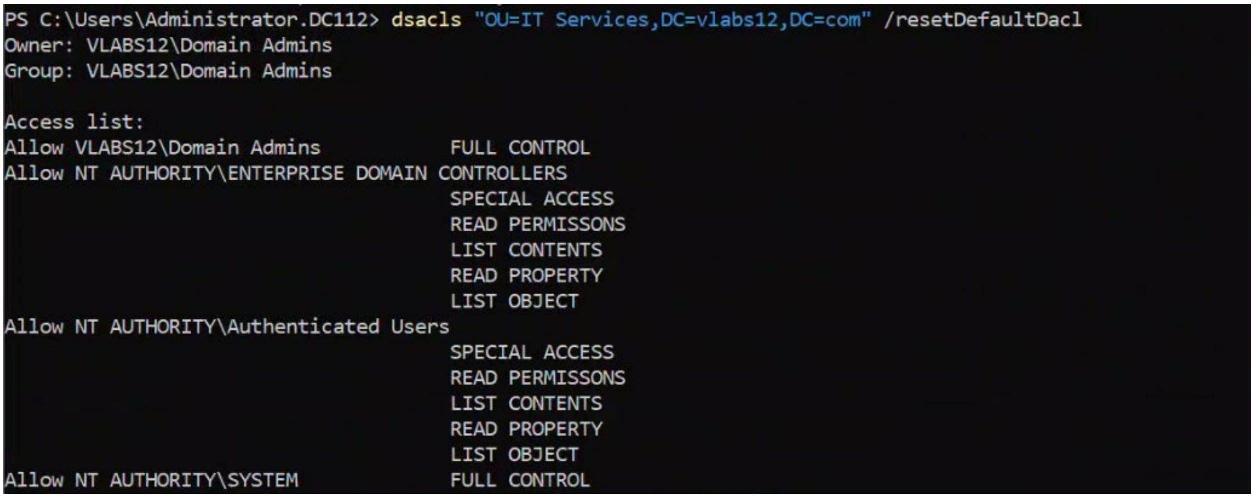
Type	Principal	Access	Inherited from	Applies to
Deny	Everyone	Special	None	This object only
Allow	GG_HR_Admins (VLABS12\G...		None	This object only
Allow	Account Operators (VLABS12...	Create/delete InetOrg...	None	This object only
Allow	Account Operators (VLABS12...	Create/delete Comput...	None	This object only
Allow	Account Operators (VLABS12...	Create/delete Group o...	None	This object only
Allow	Print Operators (VLABS12\Pri...	Create/delete Printer o...	None	This object only
Allow	Account Operators (VLABS12...	Create/delete User obj...	None	This object only
Allow	Domain Admins (VLABS12\D...	Full control	None	This object only
Allow	ENTERPRISE DOMAIN CONT...	Special	None	This object only
Allow	Authenticated Users	Special	None	This object only



Type	Principal	Access	Inherited from	Applies to
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	Pre-Windows 2000 Compatib...	Special	DC=vlabs12,DC=com	Descendant InetOrgPerson o...
Allow	Pre-Windows 2000 Compatib...	Special	DC=vlabs12,DC=com	Descendant Group objects
Allow	Pre-Windows 2000 Compatib...	Special	DC=vlabs12,DC=com	Descendant User objects
Allow	SELF		DC=vlabs12,DC=com	This object and all descendan...
Allow	SELF	Special	DC=vlabs12,DC=com	This object and all descendan...
Allow	Enterprise Admins (VLABS12\...	Full control	DC=vlabs12,DC=com	This object and all descendan...
Allow	Pre-Windows 2000 Compatib...	List contents	DC=vlabs12,DC=com	This object and all descendan...
Allow	Administrators (VLABS12\Ad...	Special	DC=vlabs12,DC=com	This object and all descendan...

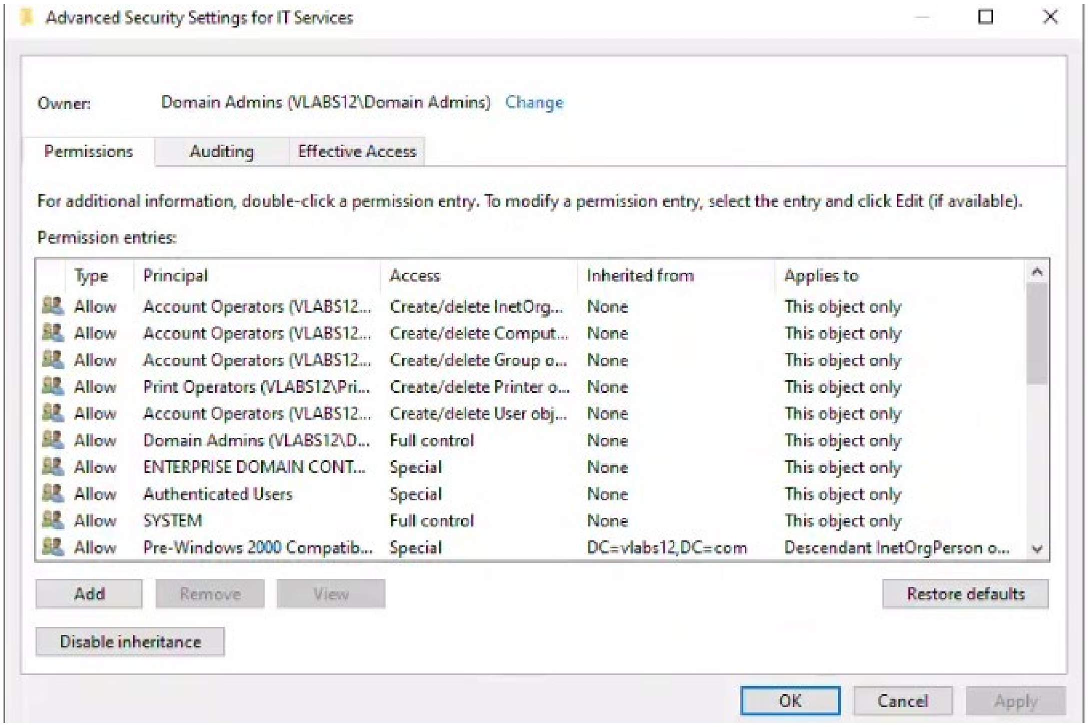
Reset all permissions in IT Services with the following:

dsacls "OU=IT Services,DC=vlabs12,DC=com" /resetDefaultDacl



```
PS C:\Users\Administrator.DC112> dsacls "OU=IT Services,DC=vlabs12,DC=com" /resetDefaultDacl
Owner: VLABS12\Domain Admins
Group: VLABS12\Domain Admins

Access list:
Allow VLABS12\Domain Admins           FULL CONTROL
Allow NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
                                      SPECIAL ACCESS
                                      READ PERMISSONS
                                      LIST CONTENTS
                                      READ PROPERTY
                                      LIST OBJECT
Allow NT AUTHORITY\Authenticated Users
                                      SPECIAL ACCESS
                                      READ PERMISSONS
                                      LIST CONTENTS
                                      READ PROPERTY
                                      LIST OBJECT
Allow NT AUTHORITY\SYSTEM             FULL CONTROL
```

Verify again in AD Users and Computers but with IT Services that all the permissions have been reset. Sophie Lambert’s deny/allow permissions are no longer listed so it was successful.



Advanced Security Settings for IT Services

Owner: Domain Admins (VLABS12\Domain Admins) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Account Operators (VLABS12...	Create/delete InetOrg...	None	This object only
Allow	Account Operators (VLABS12...	Create/delete Comput...	None	This object only
Allow	Account Operators (VLABS12...	Create/delete Group o...	None	This object only
Allow	Print Operators (VLABS12\Pri...	Create/delete Printer o...	None	This object only
Allow	Account Operators (VLABS12...	Create/delete User obj...	None	This object only
Allow	Domain Admins (VLABS12\D...	Full control	None	This object only
Allow	ENTERPRISE DOMAIN CONT...	Special	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	Pre-Windows 2000 Compatib...	Special	DC=vlabs12,DC=com	Descendant InetOrgPerson o...