



3/3/2021

Active Directory Hands On Exercise

Chapter 2

Managing OUs and Active Directory Accounts

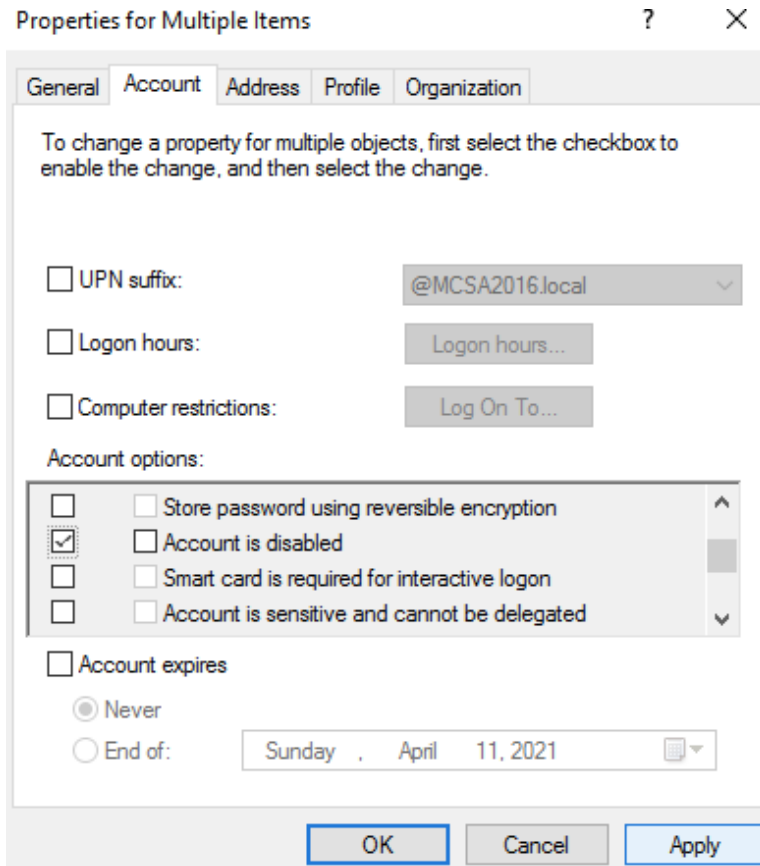
(Part2)



El Adel, Taoufik

IT 416 - SPRING 2021 - OLD DOMINION UNIVERSITY

- **2-7-6:** Click the **Account** tab. Scroll down in the Account options list box and click to select the **Account is disabled** check box on the far left (see Figure 2-18). Click **Apply**.



- **2-7-7:** Click the **Address** and **Profile** tabs to review which attributes you can change. Click the **Organization** tab. Click the **Job Title** check box, type **Marketing Associate** in the text box, and then click **OK**.

Properties for Multiple Items ? X

General Account Address Profile Organization

To change a property for multiple objects, first select the checkbox to enable the change, and then type the change.

Job Title:

Department:

Company:

Manager

Name:

Change... Properties Clear

OK Cancel Apply

- 2-7-8: Open the Properties dialog box for each Marketing Person account to verify that the changes were made for all. When you're finished with each one, click **OK**.

Marketing Person1 Properties ? X

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

Job Title:

Department:

Company:

Manager

Name:

Change... Properties Clear

Marketing Person2 Properties ? X

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

Job Title:

Department:

Company:

Manager

Name:

Marketing Person3 Properties ? X

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

Job Title:

Department:

Company:

Manager

Name:

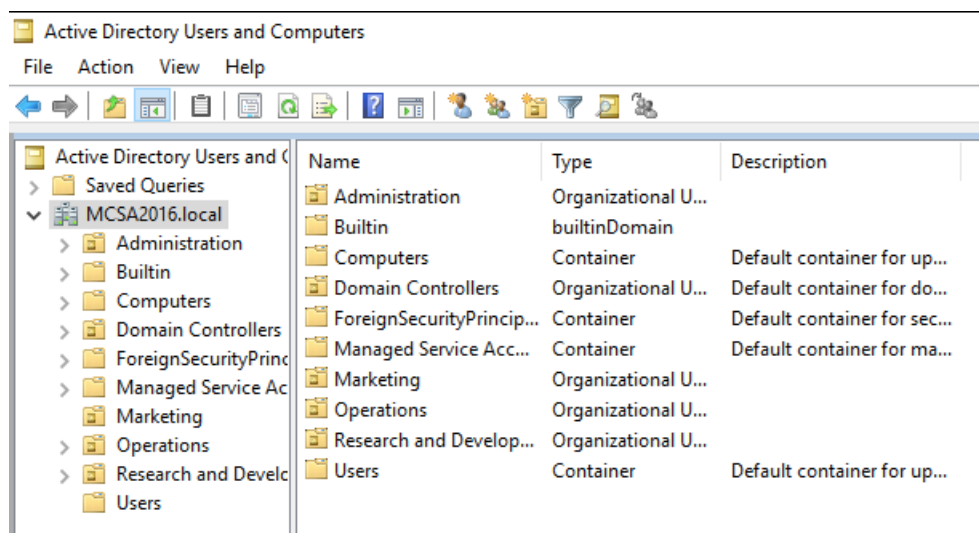
Change... Properties Clear

- **2-7-9:** Continue to the next activity.

Activity 2-8: Creating Groups with Different Scopes


Description: In this activity, you work with groups and see how nesting groups and converting group scope work.

- **2-8-1:** On ServerDC1, open Active Directory Users and Computers.



- **2-8-2:** Create a new OU named **TestOU1**. Click **Test0U1** and create the following security groups with the indicated scope: **Group1-G** (global), **Group2-G** (global), **Group1-DL** (domain local), **Group2-DL** (domain local), **Group1-U** (universal), and **Group2-U** (universal).


New Object - Organizational Unit

 Create in: MCSA2016.local/

Name:

Protect container from accidental deletion

New Object - Group

 Create in: MCSA2016.local/TestOU1

Group name:

Group name (pre-Windows 2000):


Group scope

Domain local
 Global
 Universal

Group type

Security
 Distribution

New Object - Group

 Create in: MCSA2016.local/TestOU1

Group name:

Group name (pre-Windows 2000):


Group scope

Domain local
 Global
 Universal

Group type

Security
 Distribution

New Object - Group

 Create in: MCSA2016.local/TestOU1

Group name:

Group name (pre-Windows 2000):

Group scope

Domain local
 Global
 Universal

Group type

Security
 Distribution

New Object - Group

Create in: MCSA2016.local/TestOU1

Group name:
Group2-DL

Group name (pre-Windows 2000):
Group2-DL

Group scope

Domain local
 Global
 Universal

Group type

Security
 Distribution

New Object - Group

Create in: MCSA2016.local/TestOU1

Group name:
Group1-U

Group name (pre-Windows 2000):
Group1-U

Group scope

Domain local
 Global
 Universal

Group type

Security
 Distribution

New Object - Group

Create in: MCSA2016.local/TestOU1

Group name:
Group2-U

Group name (pre-Windows 2000):
Group2-U

Group scope

Domain local
 Global
 Universal

Group type

Security
 Distribution

- **2-8-3:** In the right pane of Active Directory Users and Computers, double-click **Group1-G** to open its Properties dialog box. In the Group scope section, notice that the Domain local option is disabled because converting from global to domain local isn't allowed.

Group1-G Properties ? X

General Members Member Of Managed By

Group1-G

Group name (pre-Windows 2000): Group1-G

Description:

E-mail:

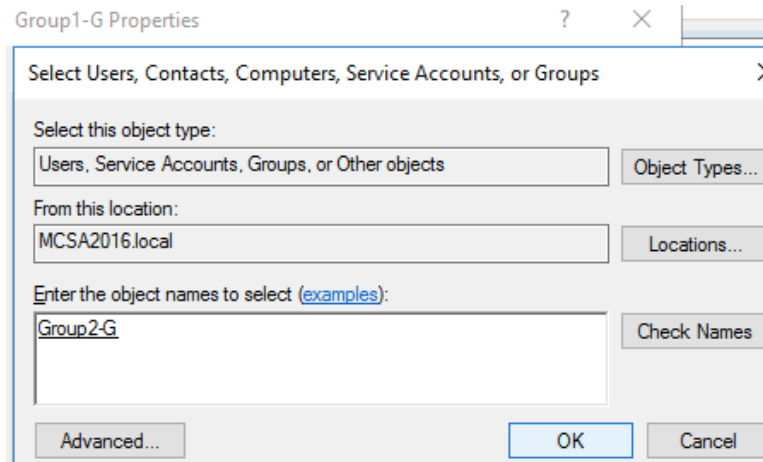
Group scope

Domain local
 Global
 Universal

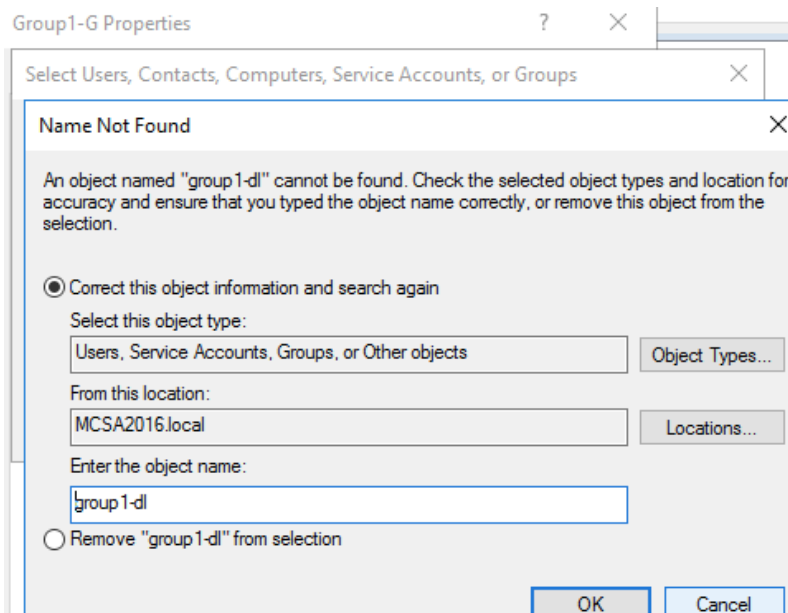
Group type

Security
 Distribution

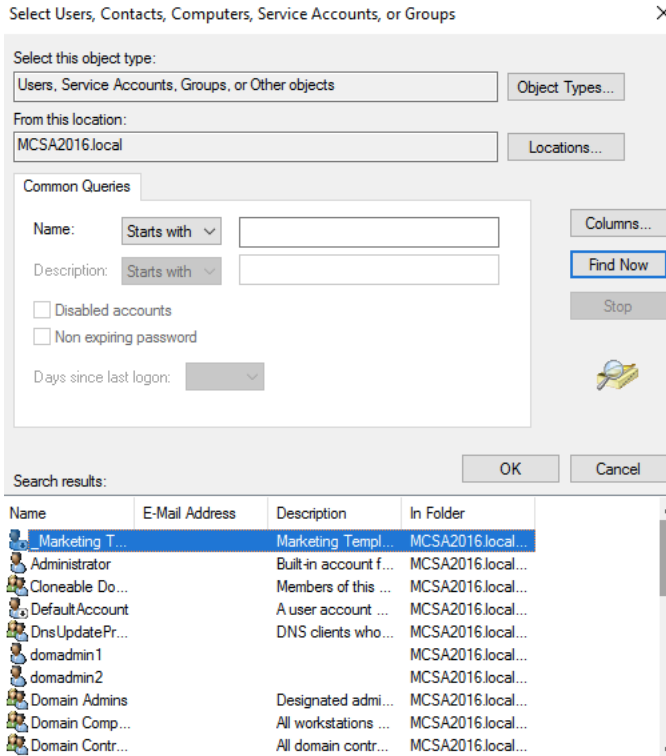
- **2-8-4:** Click the **Members** tab, and then click **Add**. Type **Group2-G**, click **Check Names**, and then click **OK**.



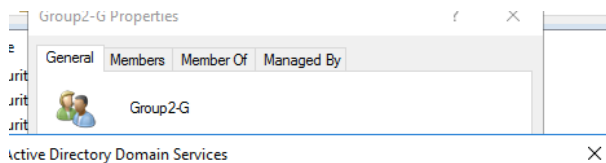
- **2-8-5:** Click **Add**. Type **Group1-DL** and click **Check Names**. The Name Not Found message box is displayed because domain local groups can't be members of global groups. Click **Cancel**.



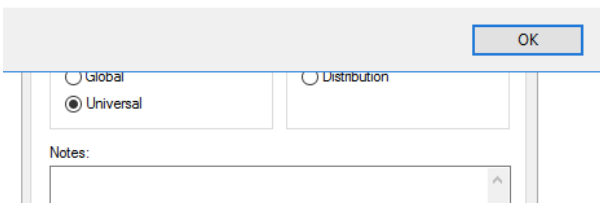
- 2-8-6:** Click **Advanced**, and then click **Find Now**. Active Directory displays only valid objects that can be made a group member, so no domain local or universal groups are listed. Click **Cancel** twice, and then click **OK**.



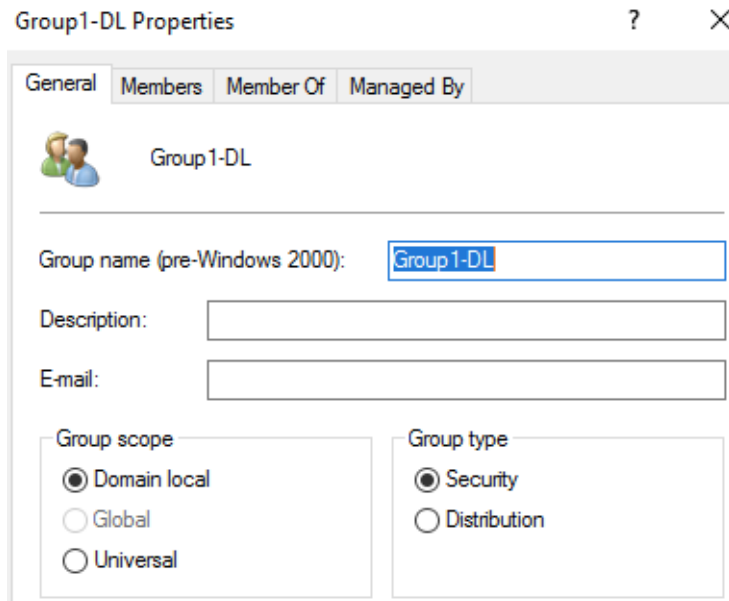
- 2-8-7:** Double-click **Group2-G** to open its Properties dialog box. In the Group scope section, click the **Universal** option button, and then click **OK**. You should get an error message stating that a global group can't have a universal group as a member. Because Group2-G is a member of Group1-G, attempting to convert it to universal violates that rule. Click **OK**, and then click **Cancel**.



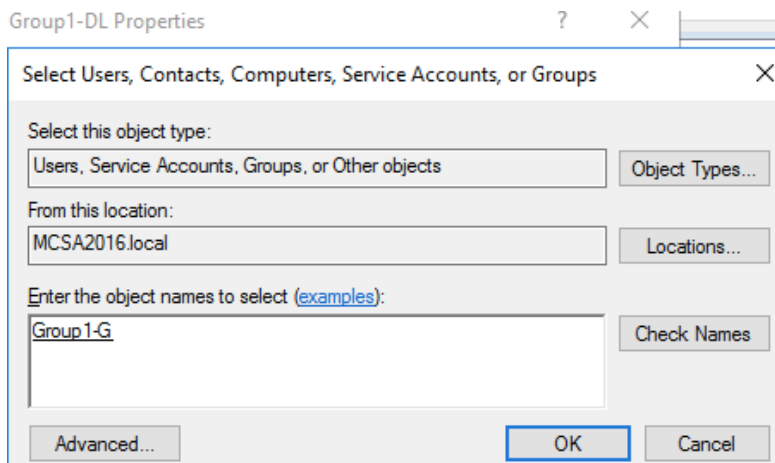
! The following Active Directory Domain Services error occurred: A global group cannot have a universal group as a member.



- **2-8-8:** Double-click **Group1-DL** to open its Properties dialog box. In the Group scope section, the Global option is disabled because you can't convert a domain local group to a global group.

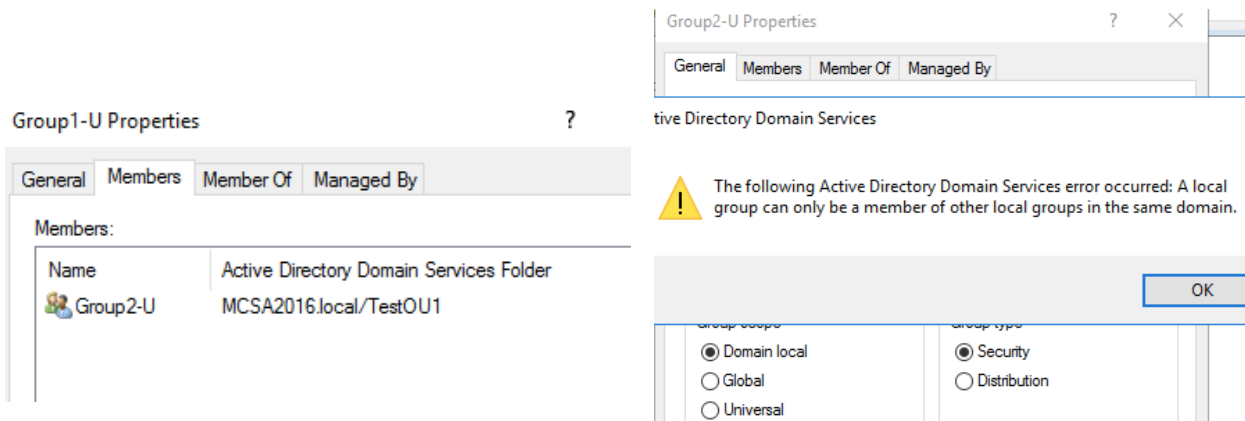


- **2-8-9:** Click the **Members** tab and add **Group1-G** as a member. Adding a global group as a member of a domain local group is in line with the AGDLP best practice. Click **OK** twice.

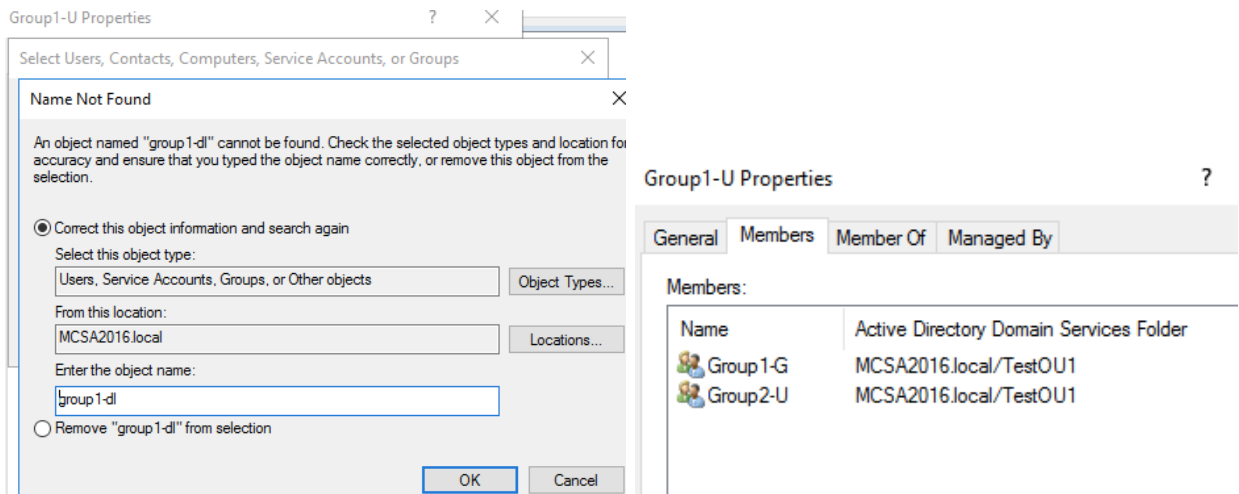


- **2-8-10:** Double-click **Group1-U** to open its Properties dialog box. Add **Group2-U** as a member, and then click **OK** twice. Double-click **Group2-U** to open its

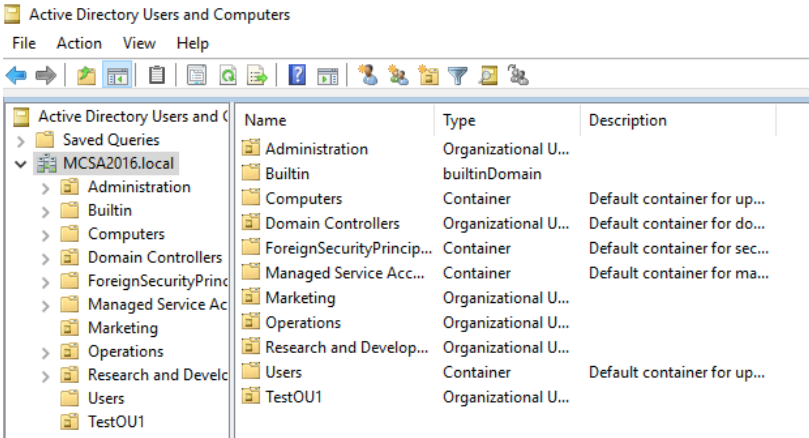
Properties dialog box. In the Group scope section, click **Domain local**, and then click **OK**. You get an error message, which reinforces the rule that universal groups can be converted to domain local groups only if they're not already a member of another universal group. Click **OK**, and then click **Cancel**.



- 2-8-11:** Double-click **Group1-U** to open its Properties dialog box. Try to add **Group1-DL** as a member. Nesting domain local groups in universal groups isn't permitted. Add **Group1-G** as a member. Success! Global groups can be members of universal groups. Close all open dialog boxes.



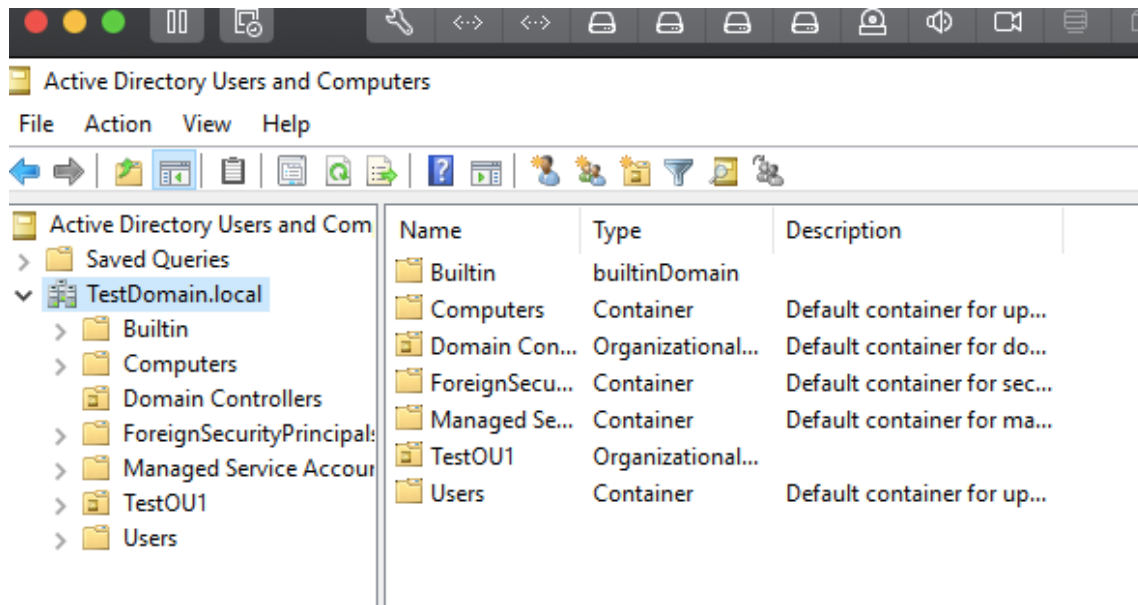
- 2-8-12:** Leave Active Directory Users and Computers open for the next activity.



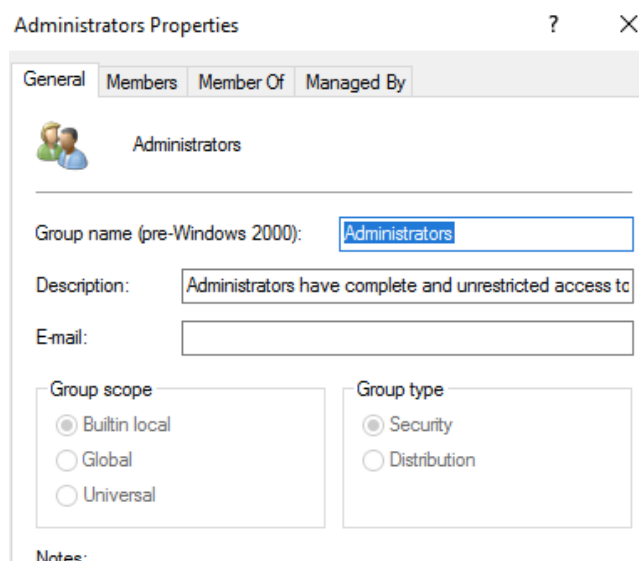
Activity 2-9: Working with Default Groups

Description: In this activity, you examine the properties of default groups to see their scope and default membership.

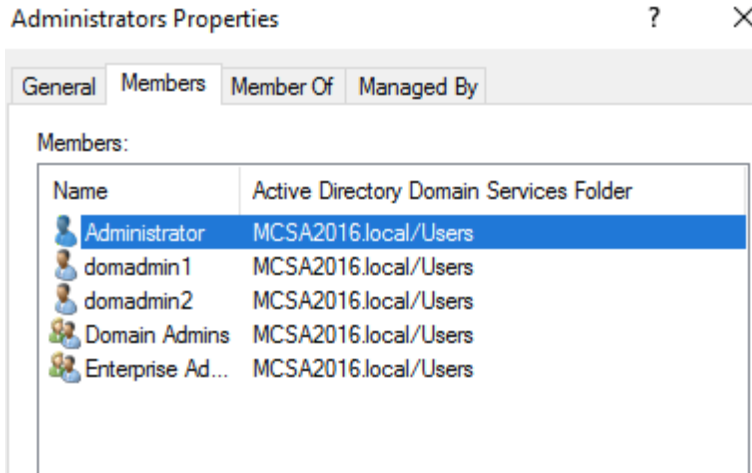
- **2-9-1:** On ServerDC1, open Active Directory Users and Computers, if necessary.



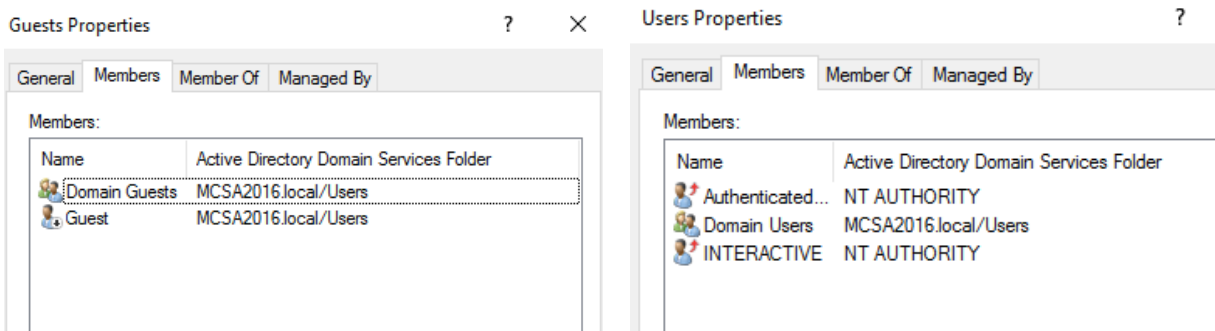
- 2-9-2: Click the **Builtin** folder. Double-click the **Administrators** group to open its Properties dialog box. The options in the Group scope and Group type sections are disabled because you can't change the scope or type of groups in the Builtin folder. Notice that the selected scope is Builtin local. These groups are considered domain local, but there are some differences between Builtin local and other domain local groups, as you'll see.



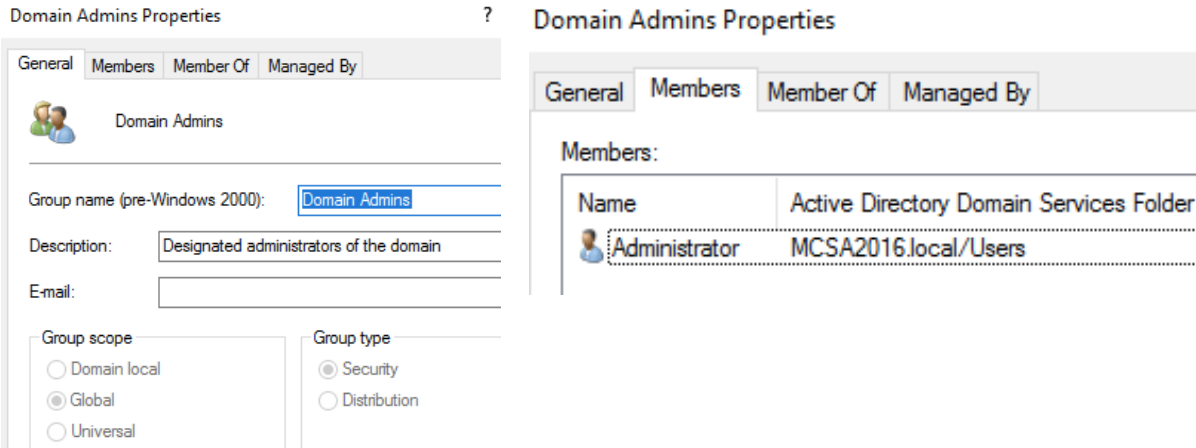
- 2-9-3: Click the **Members** tab to see this group's members, and then click **Cancel**.



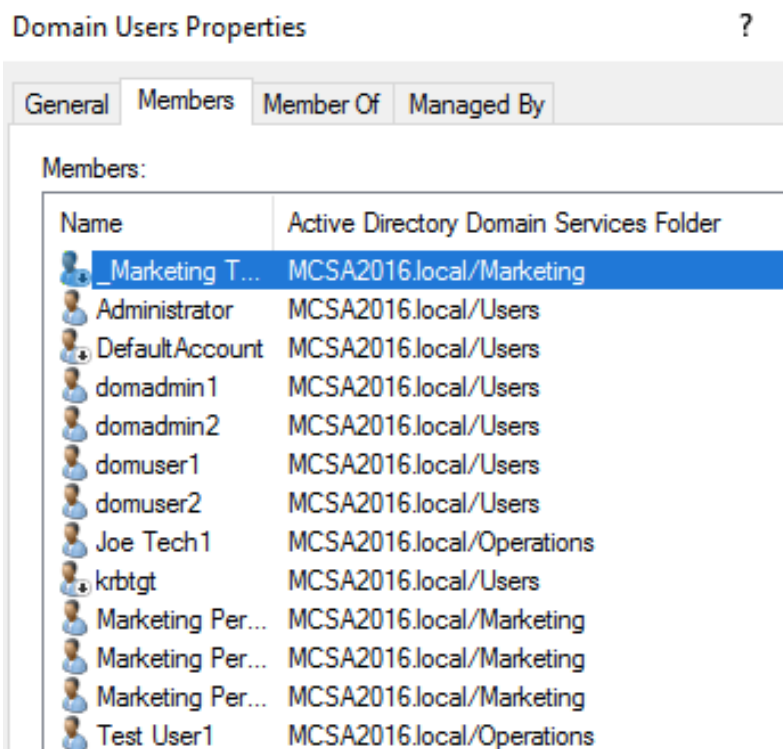
- 2-9-4:** Next, view the membership of the **Guests** and **Users** groups. Notice that the Users group has two special identities as members: Authenticated Users and Interactive. In addition, Domain Users is a member. Close both Properties dialog boxes.



- 2-9-5:** Click the **Users** folder. Double-click **Domain Admins** to open its Properties dialog box. Notice that you can't change this group's scope or type. Click the **Members** tab to view the group membership, and then click **Cancel**.

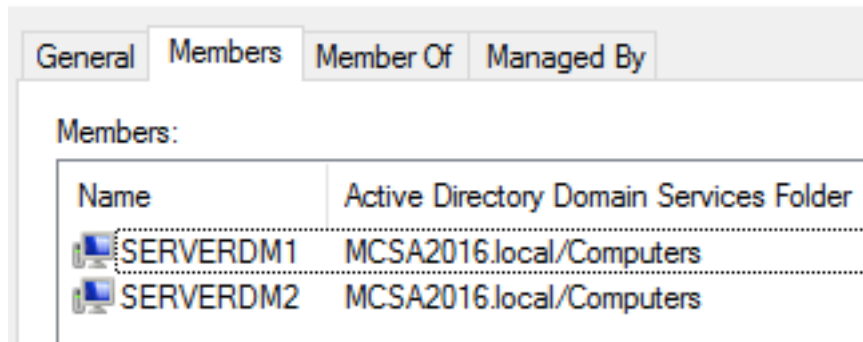


- 2-9-6: Next, view the membership of the **Domain Users** group. Notice that all the users you have created became members of this group automatically. Close this properties dialog box.



- 2-9-7: View the membership of the **Domain Computers** group. Currently, ServerDM1 and ServerDM2 are both members. When a computer is joined to the domain, the computer account is added to this group.

Domain Computers Properties



- **2-9-8:** To see the groups your currently logged-on account is a member of, open a command prompt window. Type **whoami /groups** and press **Enter**. You see a long list of groups the domain administrator is a member of, including several special identity groups, such as Everyone, Interactive, Authenticated Users, and Local. In the output, these groups are identified as well-known groups. Close the command prompt window.

```
C:\Users\Administrator>whoami /groups

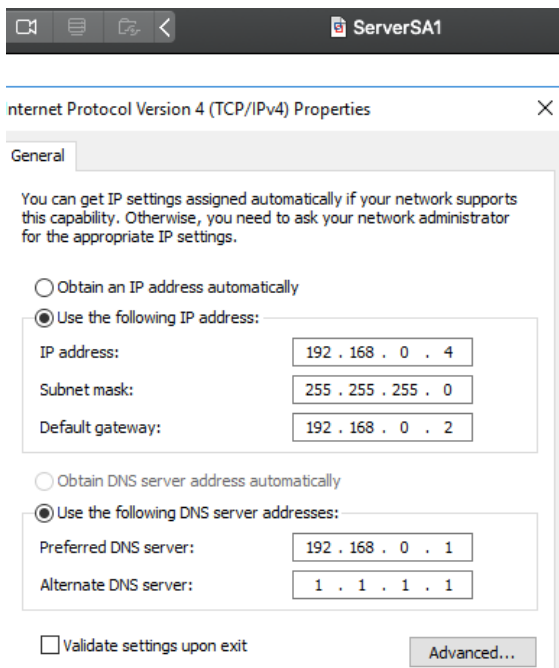
GROUP INFORMATION
-----
Group Name                                     Type                SID                  Attributes
-----
Everyone                                       Well-known group    S-1-1-0              Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                       Alias               S-1-5-32-544         Mandatory group, Enabled by default, Enabled group, Group owner
BUILTIN\Users                                Alias               S-1-5-32-545         Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access    Alias               S-1-5-32-554         Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                     Well-known group    S-1-5-4              Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                                Well-known group    S-1-2-1              Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users             Well-known group    S-1-5-11             Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization                Well-known group    S-1-5-15             Mandatory group, Enabled by default, Enabled group
LOCAL                                         Well-known group    S-1-2-0              Mandatory group, Enabled by default, Enabled group
MCSA2016\Group Policy Creator Owners          Group               S-1-5-21-3906145736-3692421193-1951280030-520 Mandatory group, Enabled by default, Enabled group
MCSA2016\Domain Admins                       Group               S-1-5-21-3906145736-3692421193-1951280030-512 Mandatory group, Enabled by default, Enabled group
MCSA2016\Schema Admins                       Group               S-1-5-21-3906145736-3692421193-1951280030-518 Mandatory group, Enabled by default, Enabled group
MCSA2016\Enterprise Admins                   Group               S-1-5-21-3906145736-3692421193-1951280030-519 Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity    Well-known group    S-1-18-1             Mandatory group, Enabled by default, Enabled group
MCSA2016\Denied RODC Password Replication Group Alias               S-1-5-21-3906145736-3692421193-1951280030-572 Mandatory group, Enabled by default, Enabled group, Local Group
Mandatory Label\High Mandatory Level         Label               S-1-16-12288
```

- **2-9-9:** Continue to the next activity.

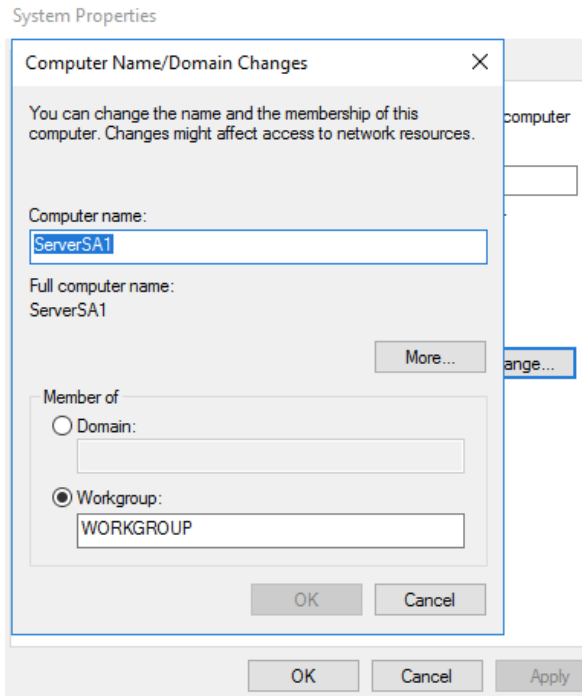
Activity 2-10: Joining a Computer to the Domain

Description: In this activity, you join the ServerSA1 computer to the domain using the GUI. Then, you remove the computer from the domain and join it again using PowerShell. Finally, you remove the computer from the domain again.

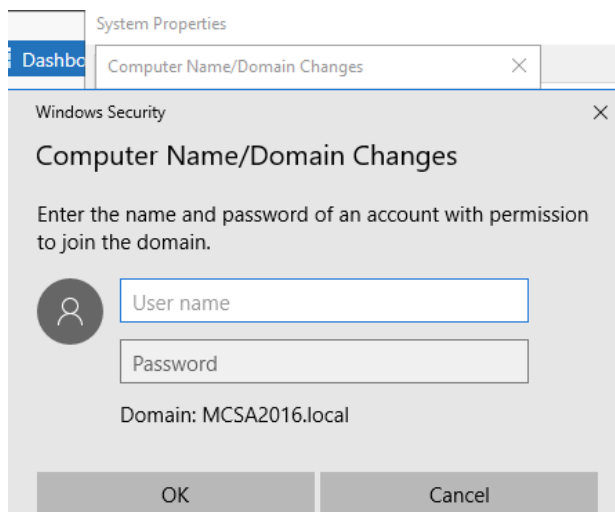
- **2-10-1:** Ensure that ServerDC1 is running. Sign in to ServerSA1. ServerSA1's DNS configuration must point to ServerDC1. Verify that ServerSA1's DNS server is 192.168.0.1 and if it isn't, change it.



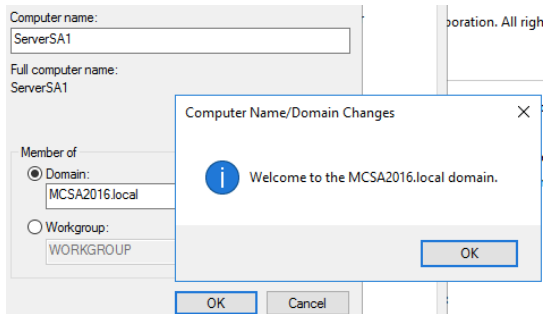
- **2-10-2:** On ServerSA1, right-click **Start** and click **System**. In the System control panel, click **Change settings** next to Computer name. The System Properties dialog box opens. In the Computer Name tab, click **Change**.



- **2-10-3:** Click the **Domain** option button, type **MCSA2016.local**, and then click **OK**. You're prompted for credentials.



- **2-10-4:** Type **jtech1** (you created jtech1 earlier, in Activity 2-2) in the User name text box and **Password01** in the Password text box. Click **OK**. You see a message welcoming you to the domain. Click **OK**. In the message stating that you need to restart the computer to apply the changes, click **OK** and then click **Close**.



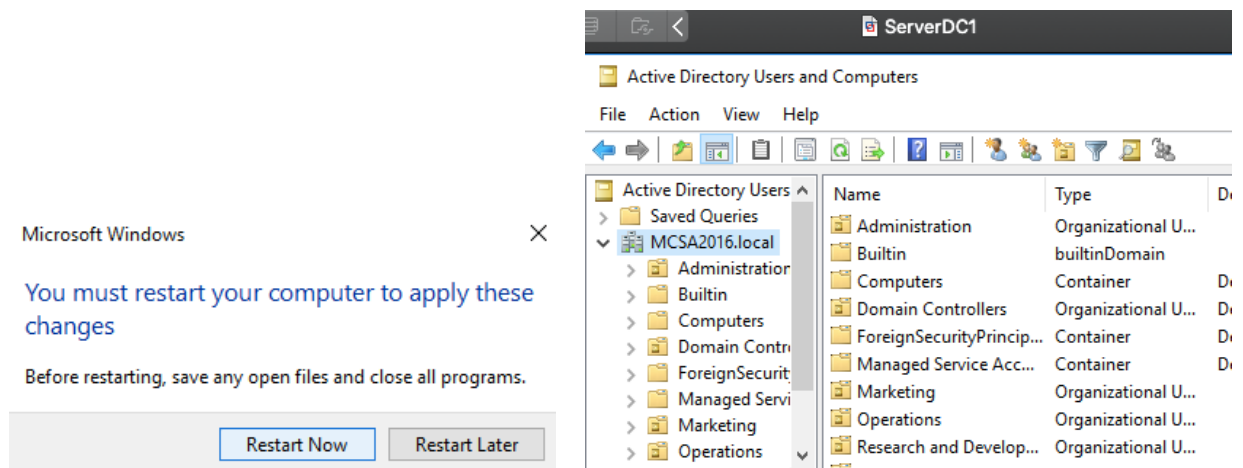
Computer Name/Domain Changes

i You must restart your computer to apply these changes

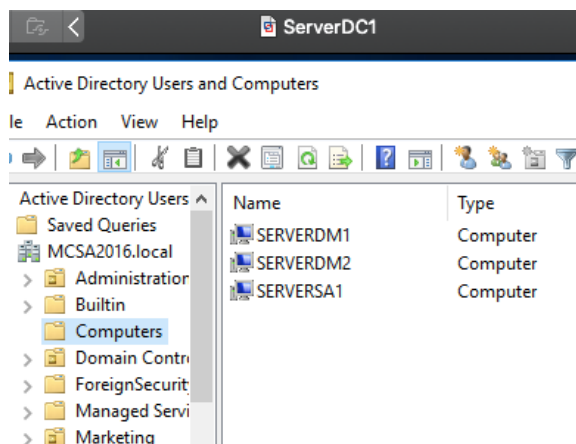
Before restarting, save any open files and close all programs.

OK

- 2-10-5:** When prompted to restart your computer, click **Restart Now**. While ServerSA1 is restarting, sign in to ServerDC1, and open Active Directory Users and Computers.



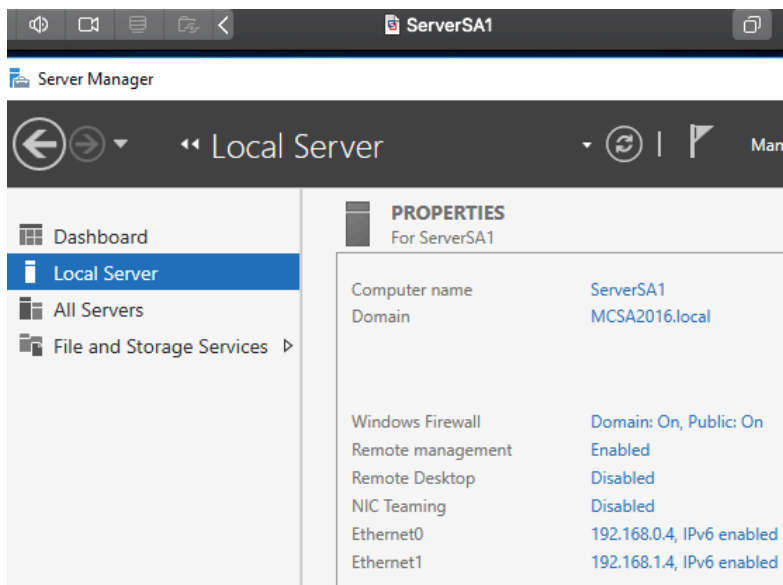
- 2-10-6:** Click the **Computers** folder, and you see a computer object named ServerSA1. It was created automatically when you joined ServerSA1 to the domain. (If you don't see the object, click the **Refresh** icon in Active Directory Users and Computers.)



- **2-10-7:** When ServerSA1 restarts, click **Other user** on the sign in screen and sign in to the domain as **mcsa2016\administrator**. (Note: When you sign in to the domain as administrator from a member server, you must preface the user name with the domain name as in mcsa2016\administrator; to sign in to the domain as any other user, you do not need to enter the domain name.)



- **2-10-8:** On ServerSA1 in Server Manager, click Local Computer. Under Computer name, it now says Domain instead of Workgroup.



- **2-10-9:** Open a PowerShell window. Type **systeminfo** and press **Enter**, Information about the computer is displayed, including the domain membership and which DC logged you on (see Figure 2-23). Type **Get-ADDomain** and press **Enter** to list information about the domain the computer is a member of.

```
PS C:\Users\administrator.MCSA2016> systeminfo

Host Name:                SERVERSAL
OS Name:                  Microsoft Windows Server 2016 Datacenter Evaluation
OS Version:               10.0.14393 N/A Build 14393
OS Manufacturer:        Microsoft Corporation
OS Configuration:        Member Server
OS Build Type:            Multiprocessor Free
Registered Owner:        Windows User
Registered Organization:
Product ID:                00377-10000-00000-AA360
Original Install Date:    2/19/2021, 3:26:26 PM
System Boot Time:         3/12/2021, 11:24:01 AM
System Manufacturer:      VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                          [01]: Intel64 Family 6 Model 61 Stepping 4 GenuineIntel
                          [02]: Intel64 Family 6 Model 61 Stepping 4 GenuineIntel
BIOS Version:             VMware, Inc. VMW71.00V.16722896.B64.2008100651, 8/10/2021
Windows Directory:        C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:              en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     2,047 MB
Available Physical Memory: 484 MB
Virtual Memory: Max Size:  7,511 MB
Virtual Memory: Available: 5,636 MB
Virtual Memory: In Use:    1,875 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    MCSA2016.local
Logon Server:              \\SERVERDC1
Hotfix(s):                  4 Hotfix(s) Installed.
                          [01]: KB3192137
                          [02]: KB3211320
                          [03]: KB5001078
                          [04]: KB4103720
Network Card(s):           2 NIC(s) Installed.
                          [01]: Intel(R) 82574L Gigabit Network Connection
                              Connection Name: Ethernet0
                              DHCP Enabled:    No
                              IP address(es)
                              [01]: 192.168.0.4
                              [02]: fe80::597c:b295:e9b1:3e06
                          [02]: Intel(R) 82574L Gigabit Network Connection
                              Connection Name: Ethernet1
```

```
PS C:\Users\administrator.MCSA2016> Install-WindowsFeature RSAT-AD-PowerShell
```

```

PS C:\Users\administrator.MCSA2016> Get-ADDomain

AllowedDNSSuffixes      : {}
ChildDomains            : {}
ComputersContainer      : CN=Computers,DC=MCSA2016,DC=local
DeletedObjectsContainer : CN=Deleted Objects,DC=MCSA2016,DC=local
DistinguishedName       : DC=MCSA2016,DC=local
DNSRoot                 : MCSA2016.local
DomainControllersContainer : OU=Domain Controllers,DC=MCSA2016,DC=local
DomainMode              : Windows2016Domain
DomainSID               : S-1-5-21-3906145736-3692421193-1951280030
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=MCSA2016,DC=local
Forest                  : MCSA2016.local
InfrastructureMaster    : ServerDC1.MCSA2016.local
LastLogonReplicationInterval :
LinkedGroupPolicyObjects : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policy
LostAndFoundContainer   : CN=LostAndFound,DC=MCSA2016,DC=local
ManagedBy              :
Name                    : MCSA2016
NetBIOSName             : MCSA2016
ObjectClass              : domainDNS
ObjectGUID               : 36fcc4c8-ba2c-47f9-bc96-569c3f95a6f7
ParentDomain            :
PDCEmulator             : ServerDC1.MCSA2016.local
PublicKeyRequiredPasswordRolling : True
QuotasContainer         : CN=NTDS Quotas,DC=MCSA2016,DC=local
ReadOnlyReplicaDirectoryServers : {}
ReplicaDirectoryServers : {ServerDC1.MCSA2016.local}
RIDMaster               : ServerDC1.MCSA2016.local
SubordinateReferences   : {DC=ForestDnsZones,DC=MCSA2016,DC=local, DC=DomainDns
SystemsContainer       : CN=System,DC=MCSA2016,DC=local
UsersContainer          : CN=Users,DC=MCSA2016,DC=local

```

- **2-10-10:** Next, you'll remove the computer from the domain. Type **Remove-Computer** and press **Enter**. Press **Enter** to confirm. Note that the changes take effect only after you restart the computer. Type **Restart-Computer** and press **Enter**.

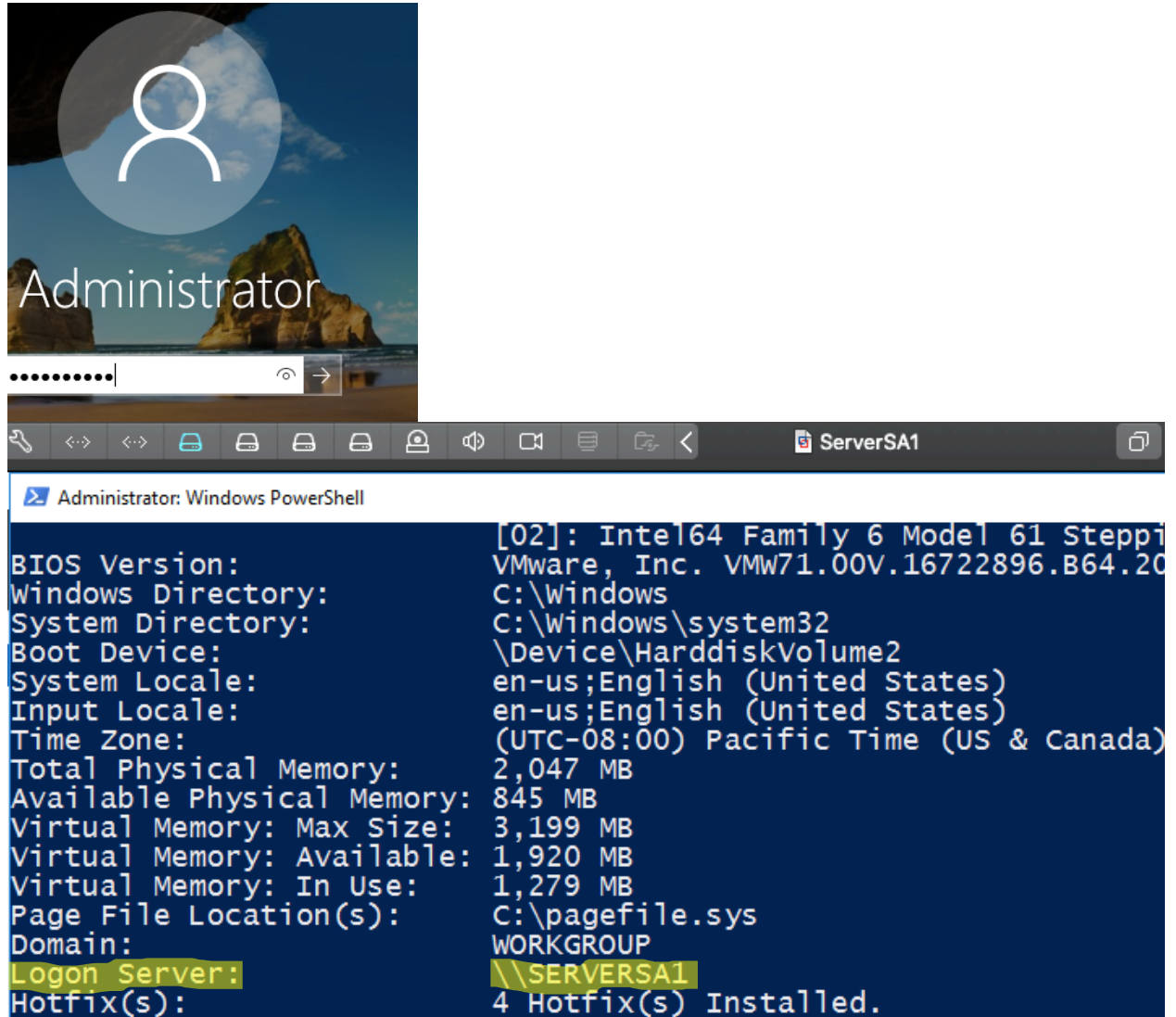
```

PS C:\Users\administrator.MCSA2016> Remove-Computer

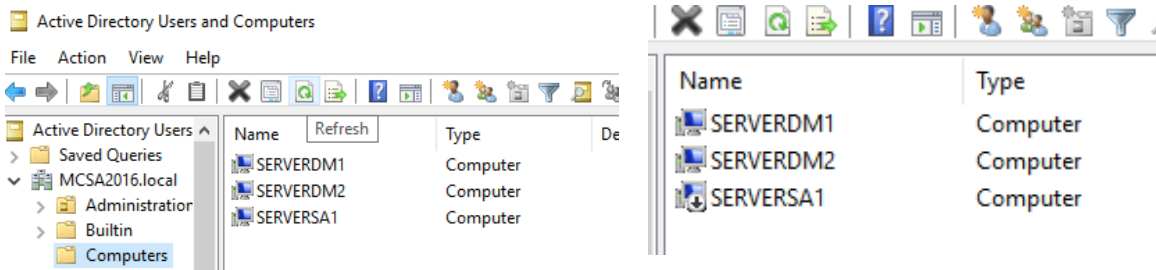
Confirm
After you leave the domain, you will need to know the password of the local Administrator
computer. Do you wish to continue?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"):
WARNING: The changes will take effect after you restart the computer ServerSA1.
PS C:\Users\administrator.MCSA2016>

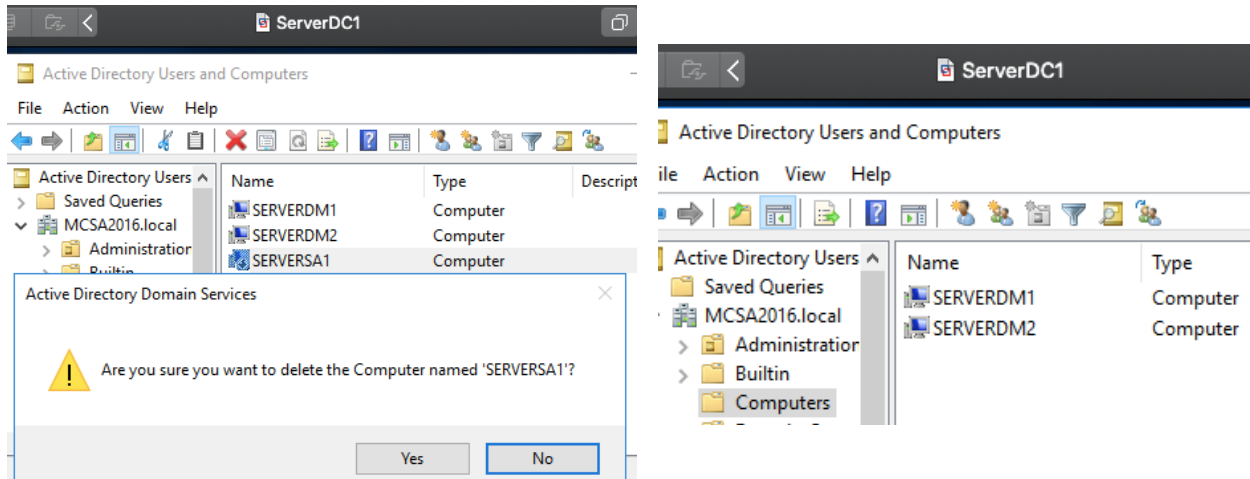
```

- **2-10-11:** When ServerSA1 restarts, sign in as the local administrator. Open a PowerShell window and type **systeminfo** and press **Enter**. Notice that the Logon Server is now **\\SERVERSA1**.

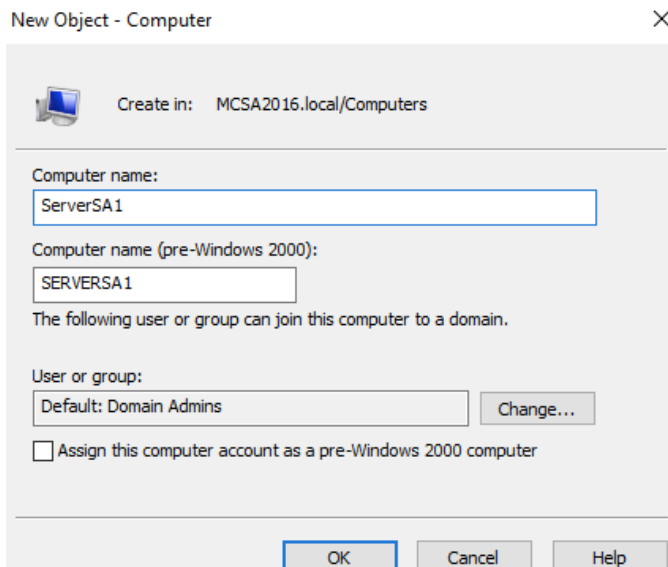


- 2-10-12:** On ServerDC1, in ADUC, click the **Computers** folder. Click the **Refresh** icon and you should see that the ServerSA1 computer account has a down arrow, which means that it's disabled. Right-click **ServerSA1**, click **Delete**, and then click **Yes** to confirm. Click **Yes** again.



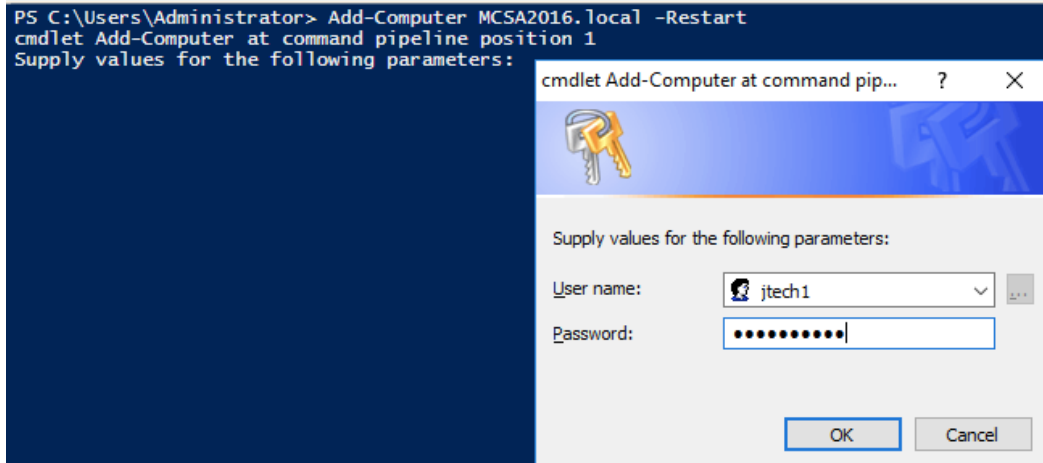


- 2-10-13:** Right-click in the **Computers** OU, point to **New**, and click **Computer**. In the New Object - Computer dialog box, type **ServerSA1** in the Computer name box. Notice that the default setting in User or group is Domain Admins, which means that only members of that group can join the computer to the domain. Click **OK**.



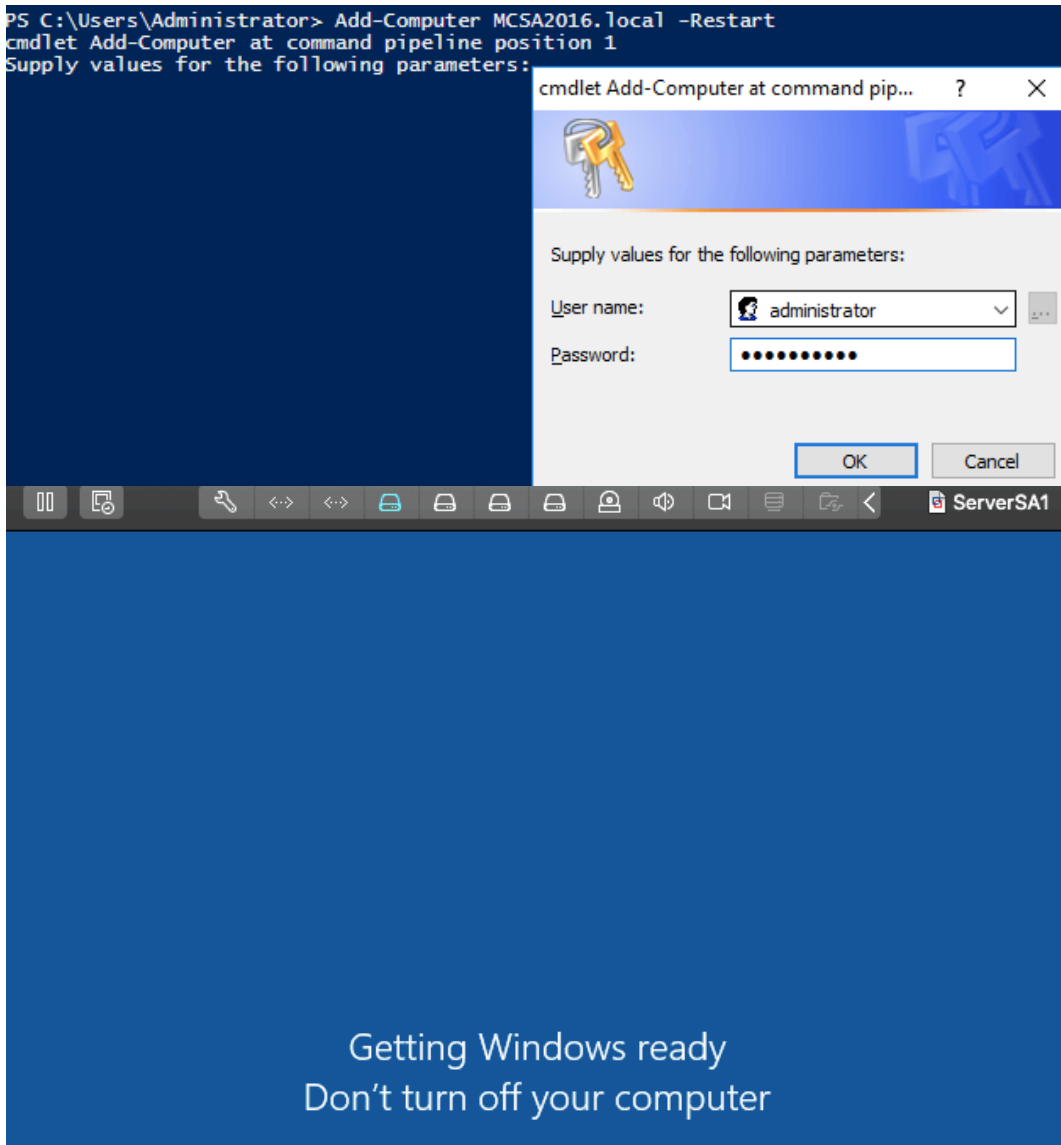
- 2-10-14:** On ServerSA1, in the PowerShell window, type **Add-Computer MCSA2016.local -Restart** and press **Enter**. When prompted for credentials, type **jtech1** and **Password01** and click **OK**. You see a message stating that the computer failed to join the domain because access was denied. That's because

when you created the computer account, you specified that only Domain Admins had the right to join the computer to the domain and jtech1 is not a member of Domain Admins.

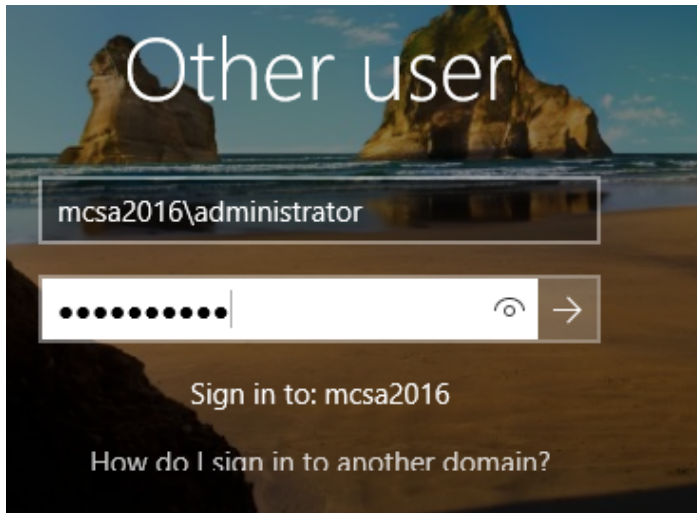


```
cmdlet Add-Computer at command pipeline position 1
Supply values for the following parameters:
Add-Computer : Computer 'ServerSA1' failed to join domain 'MCSA2016.local' from its current workgroup
'WORKGROUP' with following error message: Access is denied.
At line:1 char:1
+ Add-Computer MCSA2016.local -Restart
+ ~~~~~
+ CategoryInfo          : OperationStopped: (ServerSA1:String) [Add-Computer], InvalidOperationException
+ FullyQualifiedErrorId : FailToJoinDomainFromWorkgroup,Microsoft.PowerShell.Commands.AddComputerCommand
```

- **2-10-15:** Type `Add-Computer MCSA2016.local -Restart` and press **Enter**. When prompted for credentials, type **administrator** and **Password01** and click **OK**. The computer restarts.



- **2-10-16:** When ServerSA1 restarts, click **Other user** and sign in as **mcsa2016\administrator**.



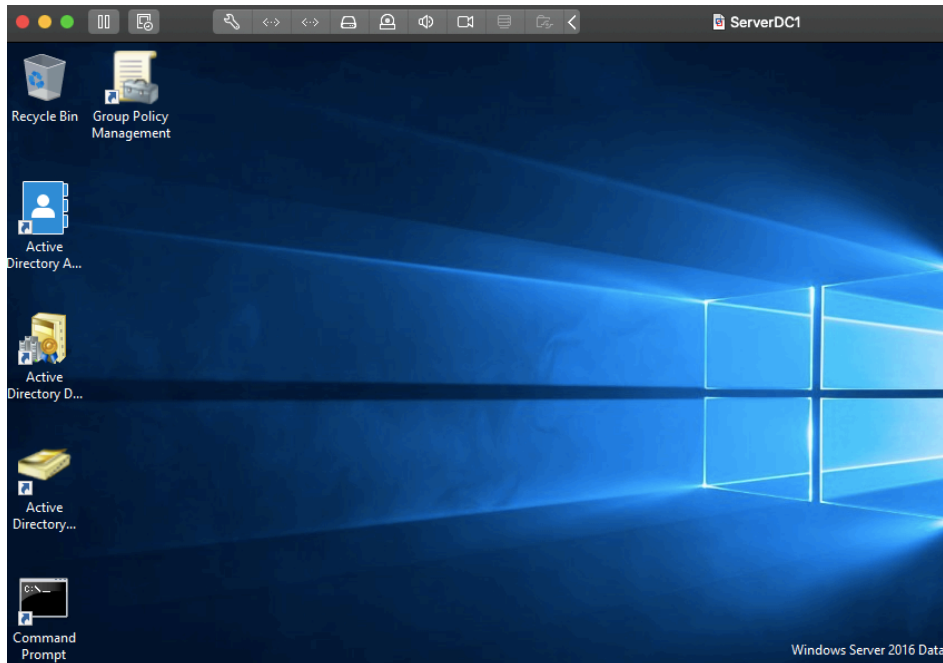
- **2-10-17:** Open a PowerShell window, type **Remove-Computer** and press **Enter**. Press **Enter** to confirm. Type **Stop-Computer** and press **Enter** to shut down ServerSA1.

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\administrator.MCSA2016> Remove-Computer

Confirm
After you leave the domain, you will need to know the password of the
local Administrator account to log onto this computer. Do you wish
to continue?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"):
WARNING: The changes will take effect after you restart the computer
ServerSA1.
PS C:\Users\administrator.MCSA2016> Stop-Computer
PS C:\Users\administrator.MCSA2016>
```

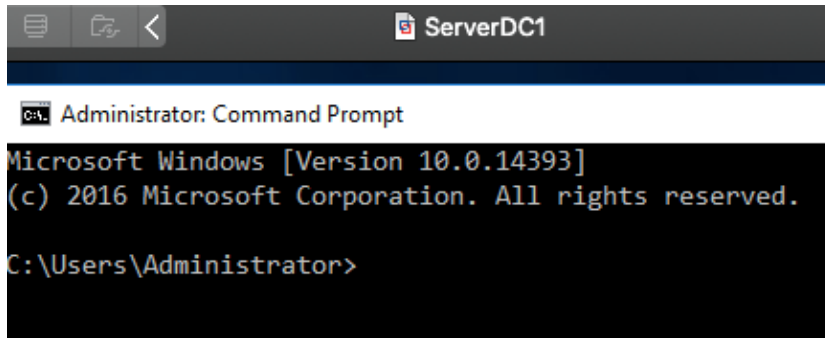
- **2-10-18:** Leave ServerDC1 running for the next activity.



Activity 2-11: Creating a Batch File for the dsadd Command

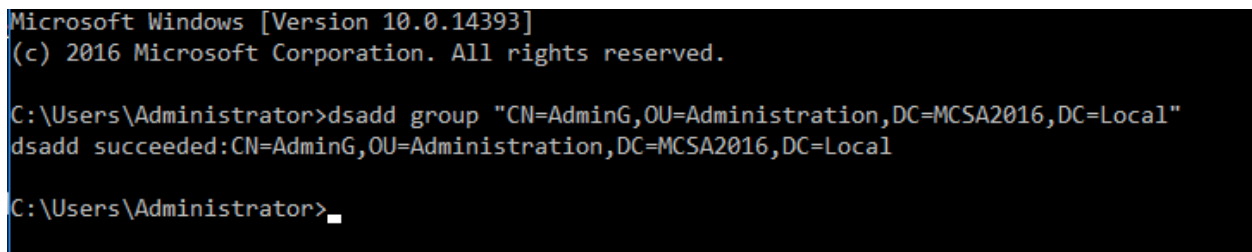
Description: In this activity, you create a batch file for the dsadd command. First you create a new group in the Administration OU, and then you create the batch file to allow you to easily create users and add them to the group.

- **2-11-1:** If necessary, sign in to ServerDC1 as Administrator, and open a command prompt window.



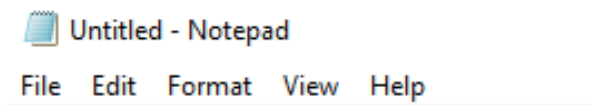
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>
```

- **2-11-2:** To create a security group called **AdvertG** with global scope, type **dsadd group "CN=AdminG,OU=Administration,DC=MCSA2016,DC=Local"** and press **Enter**. If you typed it correctly, you'll see a message starting with "dsadd succeeded." You don't need to specify the scope because global is the default.



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>dsadd group "CN=AdminG,OU=Administration,DC=MCSA2016,DC=Local"
dsadd succeeded:CN=AdminG,OU=Administration,DC=MCSA2016,DC=Local
C:\Users\Administrator>
```

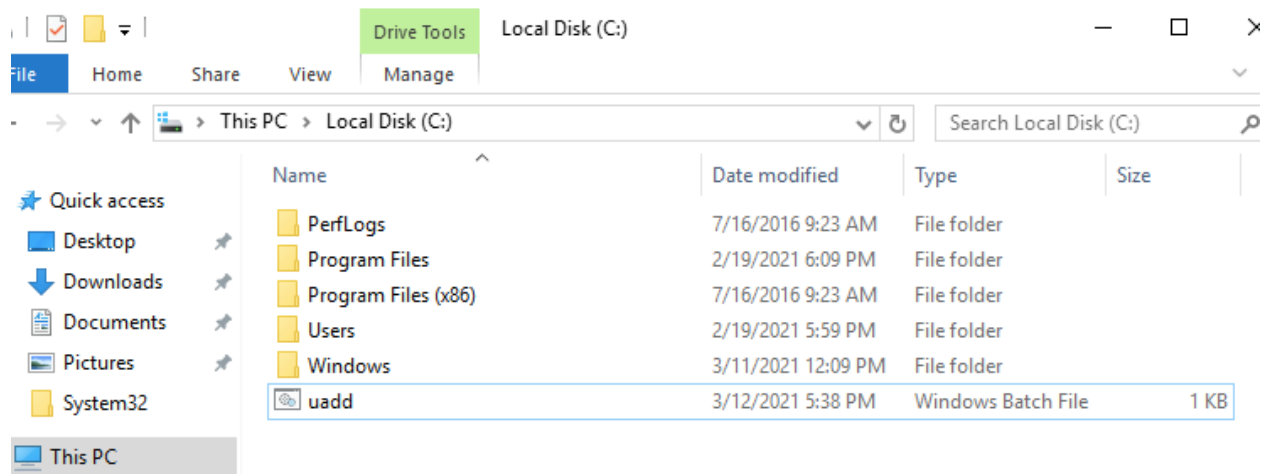
- **2-11-3:** Open Notepad by typing **notepad** and pressing **Enter**.



- **2-11-4:** In Notepad, type the following on one line: **dsadd user "CN=%1,OU=Advertising,OU=Marketing,DC=MCSA2016,DC=local" -fn %2 -ln %3 -upn %1@MCSA2016.local -pwd Password01 -memberof "CN=AdminG, OU=Administration, DC=MCSA2016, DC=local" -mustchpwd yes -disabled yes.**

```
dsadd user "CN=
%1,OU=Advertising,OU=Marketing,DC=MCSA2016,DC=local" -fn %2
-ln %3 -upn %1@MCSA2016.local -pwd Password01 -memberof
"CN=AdminG,OU=Administration, DC=MCSA2016, DC=local" -
mustchpwd yes -disabled yes
```

- **2-11-5:** Save the file as "**C:\uadd.bat**". Because Notepad adds the .txt extension automatically, enclose the filename in quotation marks to preserve the .bat extension. Exit Notepad.



- **2-11-6:** At the command prompt, type **C:\uadd AdminUser1 Administration User1** and press **Enter**. The last line of the command output should start with "dsadd succeeded." If dsadd failed, check the syntax in the uadd.bat file. Make sure there's a space between the option name and the option value; for example, make sure there's a space between -fn and %2

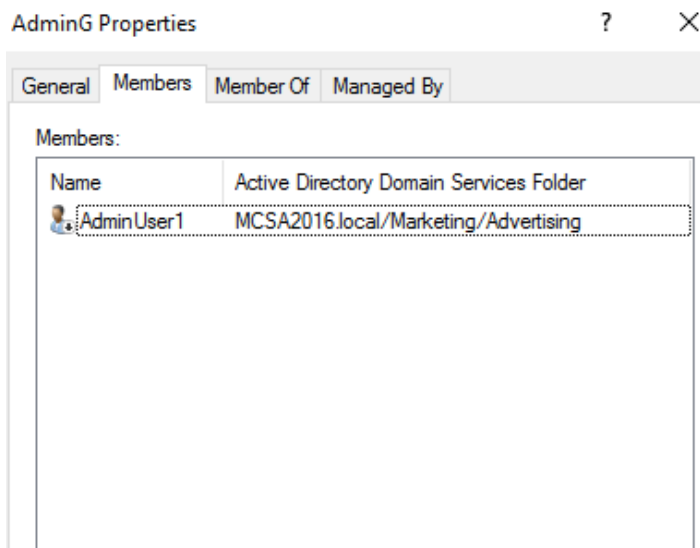
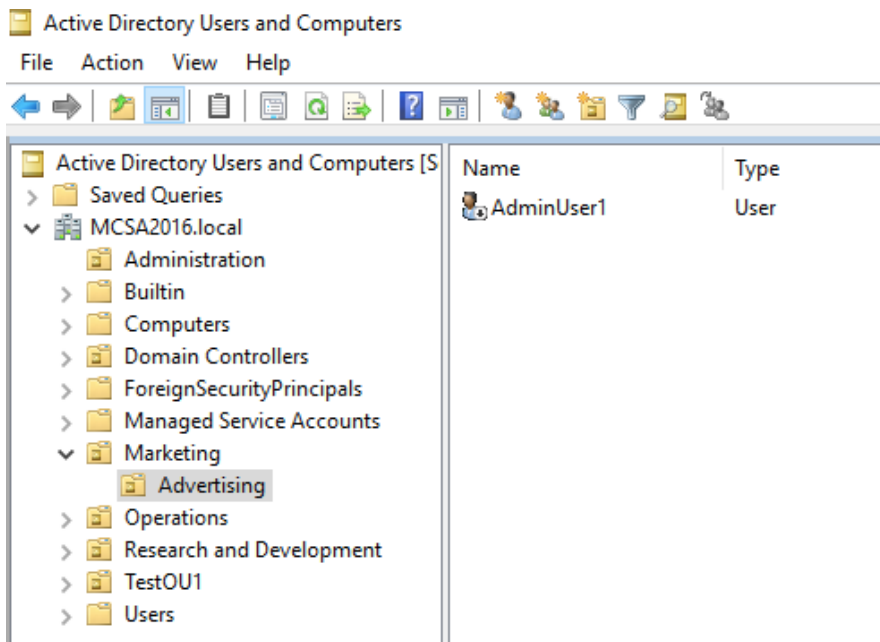
```
C:\Users\Administrator>c:\uadd AdminUser1 Administration User1

C:\Users\Administrator>dsadd user "CN=AdminUser1,OU=Advertising,OU=Marketing,DC=MCSA2016,DC=local" -fn Adm
inistration -ln User1 -upn AdminUser1@MCSA2016.local -pwd Password01 -memberof "CN=AdminG,OU=Administratio
n, DC=MCSA2016, DC=local" -mustchpwd yes -disabled yes
dsadd succeeded:CN=AdminUser1,OU=Advertising,OU=Marketing,DC=MCSA2016,DC=local

C:\Users\Administrator>
```

- **2-11-7:** Refresh the view in Active Directory Users and Computers by clicking **Action, Refresh** from the menu or clicking the **Refresh** toolbar icon. The user

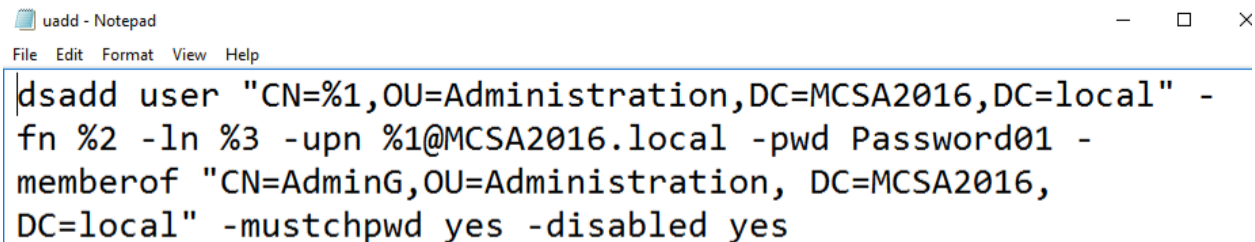
you just created should appear in the Administration OU and be a member of the AdminG group.



- I have noticed there is a discrepancy in the command offered by the book. As we can see, the new created user **AdminUser1** shows up in the **OU Advertising** (nested inside the **OU Marketing**) instead of **Administration** (the writer has also missed instructing to **create the OU Advertising, without creating it, the command does not execute**).
- To **solve** this issue, I have modified the script in the batch file “uadd.bat” as follow:

```
dsadd user "CN=%1,OU=Administration,DC=MCSA2016,DC=local" -fn %2 -ln %3 -upn %1@MCSA2016.local -pwd Password01 -memberof "CN=AdminG,OU=Administration, DC=MCSA2016, DC=local" -mustchpwd yes -disabled yes
```

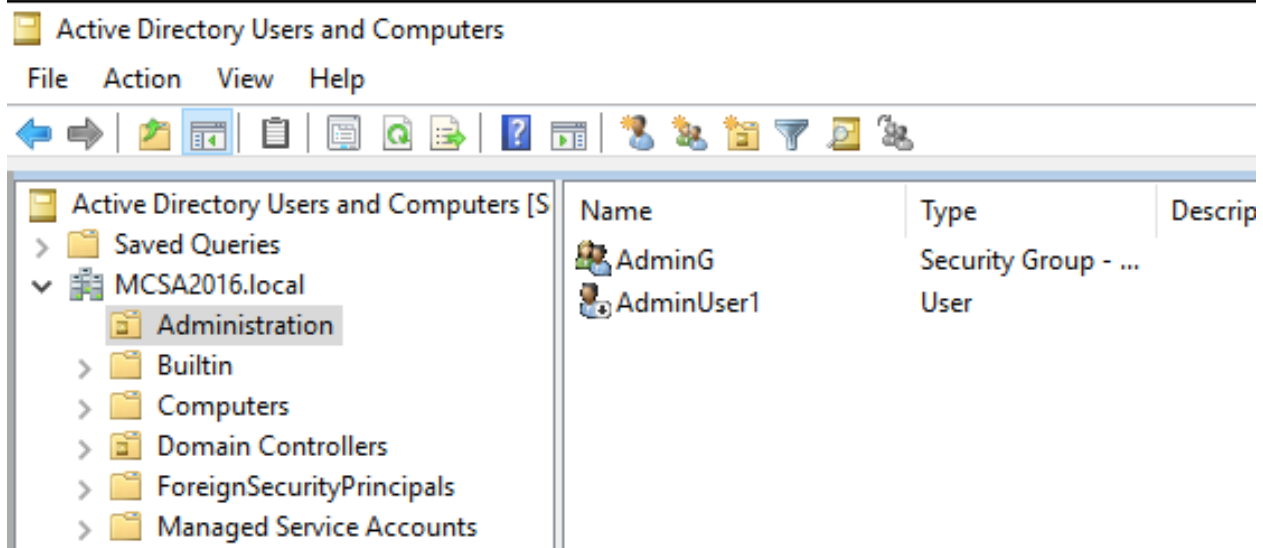
- This way, when we type “C:\uadd AdminUser1 Administration User1”, the variables %1, %2, and %3 will respectively be replaced by **AdminUser1**, **Administration**, and **User1**. **AdminUser1** will be created and added to the **Administration OU** with **Administration** as a **first name** and **User1** as a **last name**. **AdminUser1** will also be placed in the **AdminG** group that is in the **Administration OU**.



```
dsadd user "CN=%1,OU=Administration,DC=MCSA2016,DC=local" -fn %2 -ln %3 -upn %1@MCSA2016.local -pwd Password01 -memberof "CN=AdminG,OU=Administration, DC=MCSA2016, DC=local" -mustchpwd yes -disabled yes
```

```
C:\Users\Administrator>C:\uadd AdminUser1 Administration User1

C:\Users\Administrator>dsadd user "CN=AdminUser1,OU=Administration,DC=MCSA2016,DC=local" -fn Administration -ln User1 -upn AdminUser1@MCSA2016.local -pwd Password01 -memberof "CN=AdminG,OU=Administration, DC=MCSA2016, DC=local" -mustchpwd yes -disabled yes
dsadd succeeded:CN=AdminUser1,OU=Administration,DC=MCSA2016,DC=local
```



Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers [S]

- > Saved Queries
- ▼ MCSA2016.local
 - Administration
 - > Builtin
 - > Computers
 - > Domain Controllers
 - > ForeignSecurityPrincipals
 - > Managed Service Accounts

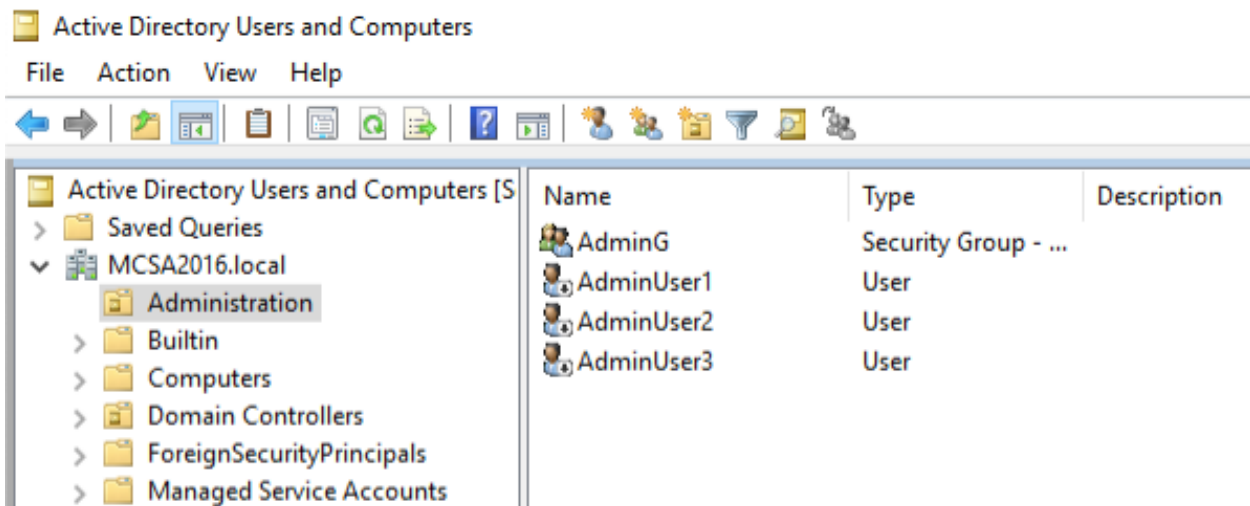
Name	Type	Descrip
AdminG	Security Group - ...	
AdminUser1	User	

- **2-11-8:** Create two more users named **AdminUser2** and **AdminUser3** using the batch file (with first names and last names in the format shown in Step 6). Leave Active Directory Users and Computers and the command prompt window open and continue to the next activity.

```
C:\Users\Administrator>C:\uadd AdminUser2 Administration User2 & C:\uadd AdminUser3 Administration User3

C:\Users\Administrator>dsadd user "CN=AdminUser2,OU=Administration,DC=MCSA2016,DC=local" -fn Administration -ln User2 -upn AdminUser2@MCSA2016.local -pwd Password01 -memberof "CN=AdminG,OU=Administration, DC=MCSA2016, DC=local" -mustchpwd yes -disabled yes
dsadd succeeded:CN=AdminUser2,OU=Administration,DC=MCSA2016,DC=local

C:\Users\Administrator>dsadd user "CN=AdminUser3,OU=Administration,DC=MCSA2016,DC=local" -fn Administration -ln User3 -upn AdminUser3@MCSA2016.local -pwd Password01 -memberof "CN=AdminG,OU=Administration, DC=MCSA2016, DC=local" -mustchpwd yes -disabled yes
dsadd succeeded:CN=AdminUser3,OU=Administration,DC=MCSA2016,DC=local
```



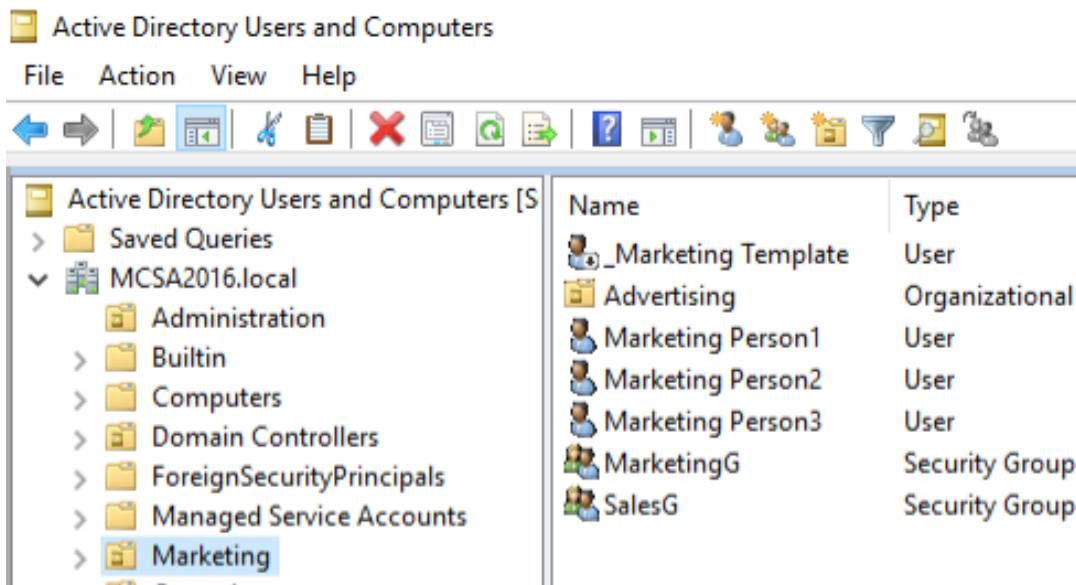
Activity 2-12: Using Pipes

Description: In this activity, you use dsquery and dsmod to assign group memberships. Then, you use PowerShell to find disabled users and use a pipe to enable those users.

- **2-12-1:** First, you'll create a new group in the Marketing OU. On ServerDC1, at the command prompt, type **dsadd group "CN=SalesG, OU=Marketing, DC=MCSA2016, DC=local"** and press **Enter**.

```
C:\Users\Administrator>dsadd group CN=SalesG,OU=Marketing,DC=MCSA2016,DC=local
dsadd succeeded:CN=SalesG,OU=Marketing,DC=MCSA2016,DC=local

C:\Users\Administrator>
```



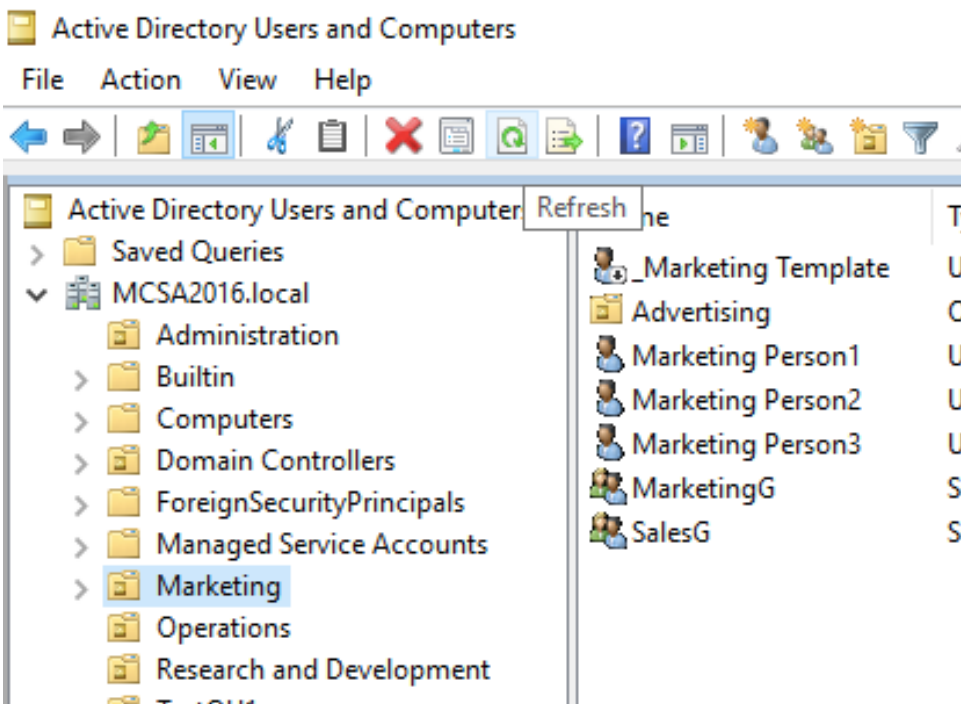
- **2-12-2:** Type **dsquery user "OU=Marketing,DC=MCSA2016,DC=local"** and press **Enter**. The output should be a list of all users, shown in DN format, in the Marketing OU. This data is what's piped to the dsmod command in the next step. (Note: If there were OUs nested under the Marketing OU, users in those OUs would also be listed.)

```
C:\Users\Administrator>dsquery user OU=Marketing,DC=MCSA2016,DC=local
"CN=_Marketing Template,OU=Marketing,DC=MCSA2016,DC=local"
"CN=Marketing Person1,OU=Marketing,DC=MCSA2016,DC=local"
"CN=Marketing Person2,OU=Marketing,DC=MCSA2016,DC=local"
"CN=Marketing Person3,OU=Marketing,DC=MCSA2016,DC=local"
```

- **2-12-3:** Type `dsquery user "OU=Marketing,DC=MCSA2016,DC=local" | dsmod group "CN=SalesG,OU=Marketing,DC=MCSA2016,DC=local" -addmbr` and press **Enter**.

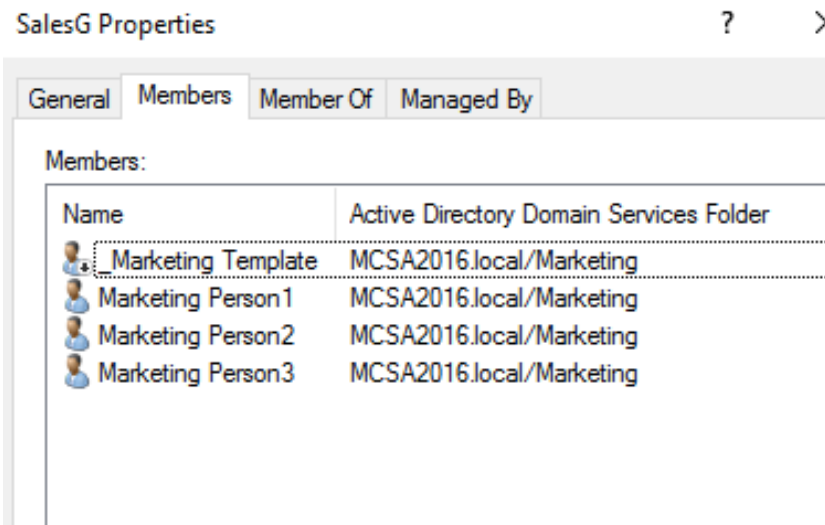
```
C:\Users\Administrator>dsquery user OU=Marketing,DC=MCSA2016,DC=local | dsmod group CN=SalesG,OU=Marketing,DC=MCSA2016,DC=local -addmbr
dsmod succeeded:CN=SalesG,OU=Marketing,DC=MCSA2016,DC=local
```

- **2-12-4:** If you get a message indicating that dsmod was successful, open Active Directory Users and Computers, if necessary. If you get an error, check the syntax and spelling, and make sure there are no spaces between DN components.



- **2-12-5:** In Active Directory Users and Computers, double-click the **SalesG** group in the Marketing OU. (You might need to refresh the view before you can see this group.) Click the **Members** tab. You should see all the users the dsquery

command displayed in Step 3. Close the Properties dialog box.



- **2-12-6:** At some point, the passwords of some users you have created will expire. To set their passwords to never expire, type `dsquery user | dsmod user -pwdneverexpires yes` and press **Enter**.

```
C:\Users\Administrator>dsquery user | dsmod user -pwdneverexpires yes
dsmod succeeded:CN=Administrator,CN=Users,DC=MCSA2016,DC=local
dsmod succeeded:CN=Guest,CN=Users,DC=MCSA2016,DC=local
dsmod succeeded:CN=DefaultAccount,CN=Users,DC=MCSA2016,DC=local
dsmod succeeded:CN=krbtgt,CN=Users,DC=MCSA2016,DC=local
dsmod succeeded:CN=domuser1,CN=Users,DC=MCSA2016,DC=local
dsmod succeeded:CN=domuser2,CN=Users,DC=MCSA2016,DC=local
dsmod succeeded:CN=domadmin1,CN=Users,DC=MCSA2016,DC=local
dsmod succeeded:CN=domadmin2,CN=Users,DC=MCSA2016,DC=local
dsmod succeeded:CN=Joe Tech1,OU=Operations,DC=MCSA2016,DC=local
dsmod succeeded:CN=Test User1,OU=Operations,DC=MCSA2016,DC=local
dsmod succeeded:CN=Test User2,OU=Operations,DC=MCSA2016,DC=local
dsmod succeeded:CN=Test User3,OU=Operations,DC=MCSA2016,DC=local
dsmod succeeded:CN= Marketing Template,OU=Marketing,DC=MCSA2016,DC=local
dsmod succeeded:CN=Marketing Person1,OU=Marketing,DC=MCSA2016,DC=local
dsmod succeeded:CN=Marketing Person2,OU=Marketing,DC=MCSA2016,DC=local
dsmod succeeded:CN=Marketing Person3,OU=Marketing,DC=MCSA2016,DC=local
dsmod succeeded:CN=AdminUser1,OU=Administration,DC=MCSA2016,DC=local
dsmod succeeded:CN=AdminUser2,OU=Administration,DC=MCSA2016,DC=local
dsmod succeeded:CN=AdminUser3,OU=Administration,DC=MCSA2016,DC=local
```

- **2-12-7:** Next, you'll use PowerShell to work with users. Close the command prompt and open a PowerShell window.

Windows PowerShell ISE

Loading...

- **2-12-8:** Find all accounts that are disabled. Type **Search-ADAccount -AccountDisabled** and press **Enter**. You see a number of accounts in the list, including the Guest account and some other accounts you probably don't want to enable.

```
PS C:\Users\Administrator> Search-ADAccount -AccountDisabled

AccountExpirationDate :
DistinguishedName     : CN=Guest,CN=Users,DC=MCSA2016,DC=local
Enabled               : False
LastLogonDate         :
LockedOut             : False
Name                  : Guest
ObjectClass           : user
ObjectGUID            : 0604e291-631e-4e2d-9c28-326e8d18dc96
PasswordExpired       : False
PasswordNeverExpires : True
SamAccountName        : Guest
SID                   : S-1-5-21-3906145736-3692421193-1951280030-501
UserPrincipalName     :

AccountExpirationDate :
DistinguishedName     : CN=DefaultAccount,CN=Users,DC=MCSA2016,DC=local
Enabled               : False
LastLogonDate         :
LockedOut             : False
Name                  : DefaultAccount
ObjectClass           : user
ObjectGUID            : bfd6d4b5-3190-4bf9-bc52-c870722ee3d8
PasswordExpired       : False
PasswordNeverExpires : True
SamAccountName        : DefaultAccount
SID                   : S-1-5-21-3906145736-3692421193-1951280030-503
UserPrincipalName     :

AccountExpirationDate :
DistinguishedName     : CN=krbtgt,CN=Users,DC=MCSA2016,DC=local
Enabled               : False
LastLogonDate         :
LockedOut             : False
Name                  : krbtgt
```

- **2-12-9:** To narrow the search to just those users in the Administration OU, type **Search-ADAccount Account- Disabled -SearchBase "OU=Administration,DC=MCSA2016,DC=local"** and press **Enter**. You see the list of users you created in the previous activity.

```

PS C:\Users\Administrator> Search-ADAccount -AccountDisabled -SearchBase "OU=Administration,DC=MCSA2016,DC=local"

AccountExpirationDate :
DistinguishedName     : CN=AdminUser1,OU=Administration,DC=MCSA2016,DC=local
Enabled               : False
LastLogonDate         :
LockedOut             : False
Name                  : AdminUser1
ObjectClass           : user
ObjectGUID            : 6a2f11a9-2d27-4dd4-b526-fc61f2bd9ddb
PasswordExpired       : False
PasswordNeverExpires : True
SamAccountName        : AdminUser1
SID                   : S-1-5-21-3906145736-3692421193-1951280030-1625
UserPrincipalName     : AdminUser1@MCSA2016.local

AccountExpirationDate :
DistinguishedName     : CN=AdminUser2,OU=Administration,DC=MCSA2016,DC=local
Enabled               : False
LastLogonDate         :
LockedOut             : False
Name                  : AdminUser2
ObjectClass           : user
ObjectGUID            : 47b2b674-5df8-4ad3-ab24-a1a1157d4cb0
PasswordExpired       : False
PasswordNeverExpires : True
SamAccountName        : AdminUser2
SID                   : S-1-5-21-3906145736-3692421193-1951280030-1626
UserPrincipalName     : AdminUser2@MCSA2016.local

AccountExpirationDate :
DistinguishedName     : CN=AdminUser3,OU=Administration,DC=MCSA2016,DC=local
Enabled               : False
LastLogonDate         :
LockedOut             : False
Name                  : AdminUser3
ObjectClass           : user
ObjectGUID            : 3ff3cdcc-5949-4f99-a4f1-8af019156db3
PasswordExpired       : False
PasswordNeverExpires : True
SamAccountName        : AdminUser3
SID                   : S-1-5-21-3906145736-3692421193-1951280030-1627
UserPrincipalName     : AdminUser3@MCSA2016.local

```

- 2-12-10:** To enable the disabled accounts, press the up arrow to repeat the previous command and at the 'end of the command, type | **Set-ADUser -Enabled \$true** and press **Enter**. Press the up arrow twice to repeat the command from Step 9 and press **Enter**. You should not see any output since none of the accounts is disabled now.

```

PS C:\Users\Administrator> Search-ADAccount -AccountDisabled -SearchBase "OU=Administration,DC=MCSA2016,DC=local" | Set-ADUser -Enabled $true
PS C:\Users\Administrator>

```

- 2-12-11:** Continue to the next activity.

Activity 2-13: Using a csvde to Create Users

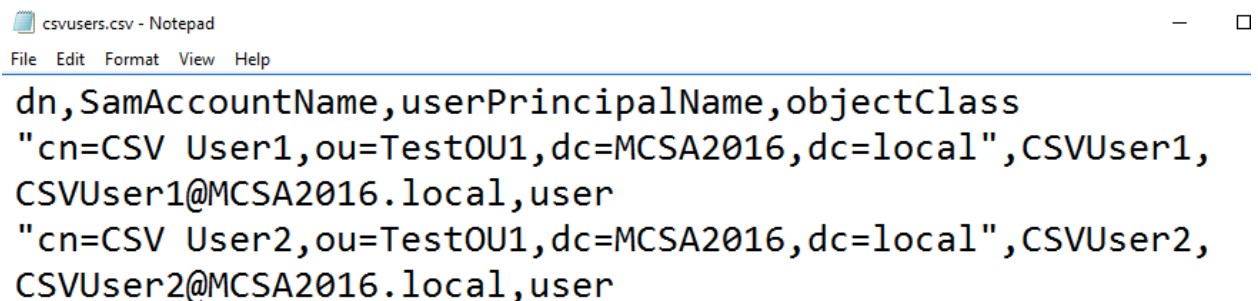
Description: In this activity, you use the csvde command to bulk create users. You will manually add users to the input file, but in practice, you would export users from a database program to create the file.

- **2-13-1:** Start Notepad and type the following, pressing Enter after each line:

dn,SamAccountName,userPrincipalName,objectClass

**"cn=CSV User1,ou=TestOU1,dc=MCSA2016,dc=local",CSVUser1,
CSVUser1@MCSA2016.local,user**

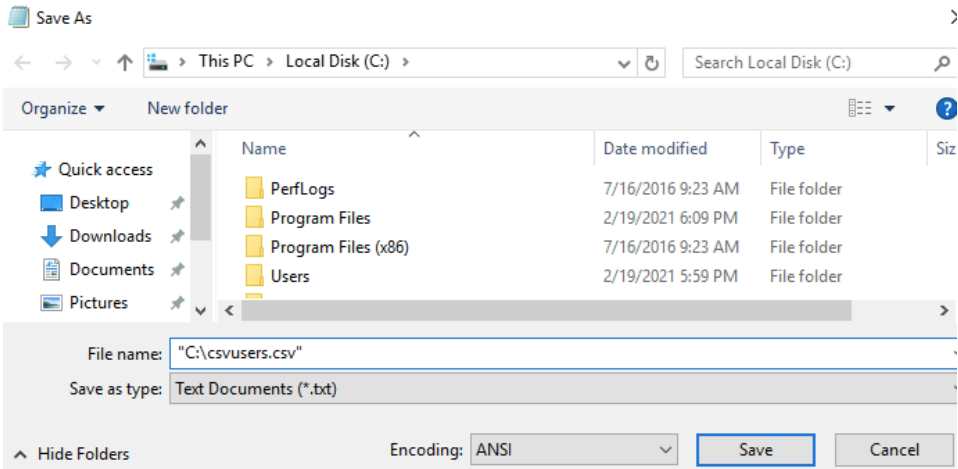
**"cn=CSV User2,ou=TestOU1,dc=MCSA2016,dc=local ",CSVUser2,
CSVUser2@MCSA2016.local,user**



The screenshot shows a Notepad window titled 'csvusers.csv - Notepad'. The menu bar includes 'File', 'Edit', 'Format', 'View', and 'Help'. The text content of the file is as follows:

```
dn,SamAccountName,userPrincipalName,objectClass
"cn=CSV User1,ou=TestOU1,dc=MCSA2016,dc=local",CSVUser1,
CSVUser1@MCSA2016.local,user
"cn=CSV User2,ou=TestOU1,dc=MCSA2016,dc=local",CSVUser2,
CSVUser2@MCSA2016.local,user
```

- **2-13-2:** Click **File, Save As** from the menu. In the File name text box, type **"C:\csvusers.csv"**, and then click **Save**. Exit Notepad.



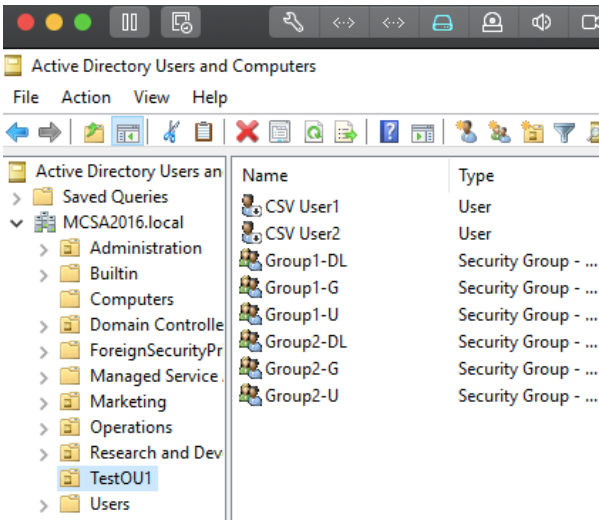
- **2-13-3:** Open a command prompt window. Type `cd \` and press **Enter** to move to the root of the C drive where you saved the file. Type `csvde -i -f csvusers.csv` and press **Enter**. You should see a message stating that two entries were modified successfully, and the command was successful.

```
C:\>csvde -i -f csvusers.csv
Connecting to "(null)"
Logging in as current user using SSPI
Importing directory from file "csvusers.csv"
Loading entries...
2 entries modified successfully.

The command has completed successfully

C:\>
```

- **2-13-4:** Close the command prompt window, and open Active Directory Users and Computers. Click the **TestOU1** OU and verify that the users were created. You'll see that the accounts are disabled.



- **2-13-5:** Continue to the next activity.

Activity 2-14: Using Ldifde to Create Users

Description: In this activity, you use the `ldifde` command to bulk create users. You will manually add users to the input file, but in practice, you would export users from a database program to create the file.

- **2-14-1:** Start Notepad and type the following, pressing **Enter** after each line:

dn: cn=LDF User1,ou=TestOU1,dc=MCSA2016,dc=local

changetype: add

ObjectClass: user

SamAccountName: LDFUser1

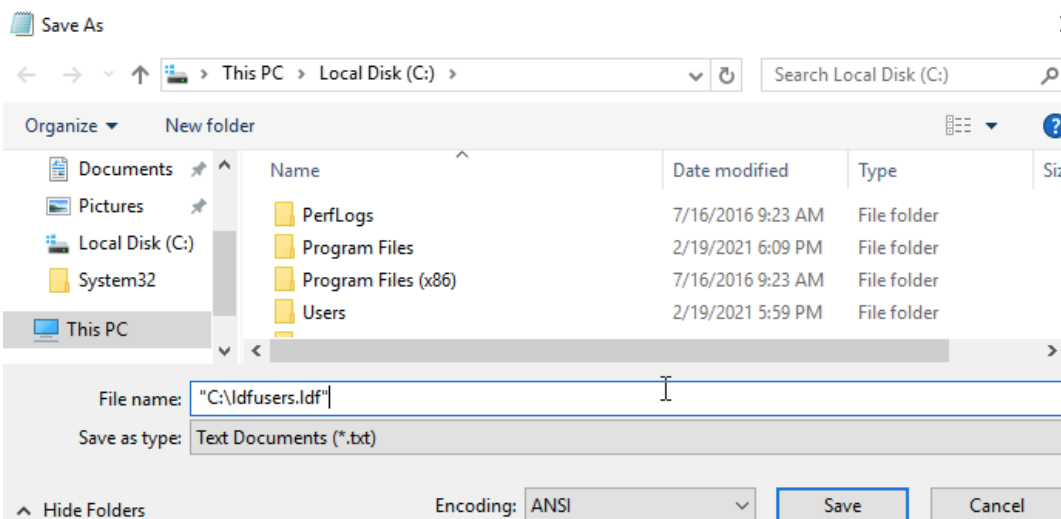
UserPrincipalName: LDFUser1@MCSA2016.local

Untitled - Notepad

File Edit Format View Help

```
dn: cn=LDF User1,ou=TestOU1,dc=MCSA2016,dc=local
changetype: add
ObjectClass: user
SamAccountName: LDFUser1
UserPrincipalName: LDFUser1@MCSA2016.local
```

- **2-14-2:** Click **File, Save As** from the menu. In the File name text box, type "**C:\ldfusers.ldf**", and then click **Save**. Exit Notepad.

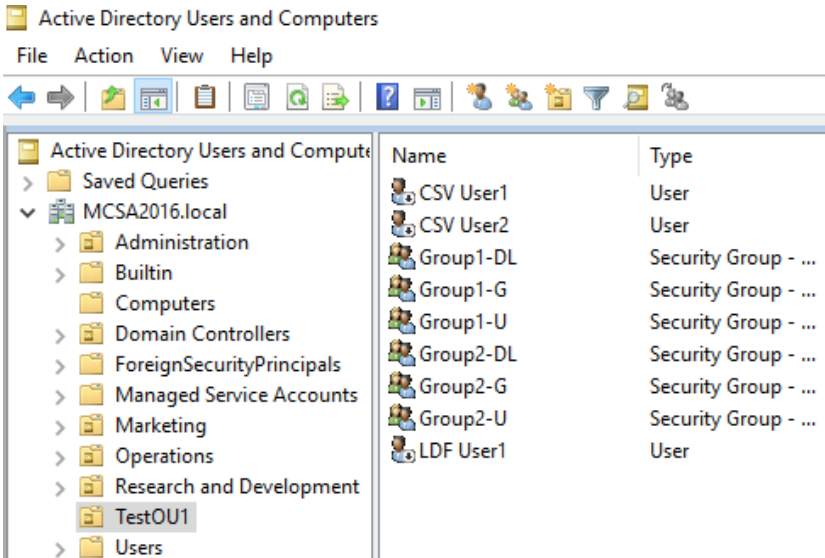


- **2-14-3:** Open a command prompt window. Type **cd ** and press **Enter**. Type **ldifde -i -f ldfusers.ldf** and press **Enter**. You should see a message stating that the command was successful.

```
C:\>ldifde -i -f ldfusers.ldf
Connecting to "ServerDC1.MCSA2016.local"
Logging in as current user using SSPI
Importing directory from file "ldfusers.ldf"
Loading entries..
1 entry modified successfully.

The command has completed successfully
```

- **2-14-4:** Close the command prompt window, and open Active Directory Users and Computers, if necessary. Click the **TestOU1** OU and verify that LDFUser1 was created. If necessary, refresh the view so that you can see this user.



- **2-14-5:** Sign out or shut down ServerDC1.

