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.

Properties for Multiple Items	?	×					
General Account Address Profile	Organization						
To change a property for multiple objects, first select the checkbox to enable the change, and then select the change.							
UPN suffix:	@MCSA2016.local	\sim					
Logon hours:	Logon hours						
Computer restrictions:	Log On To						
Account options:							
 Store password using reversible encryption Account is disabled Smart card is required for interactive logon Account is sensitive and cannot be delegated 							
Account expires							
 Never ○ End of: Sunday , April 11, 2021 							
ОК	Cancel 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 ? ×								\times
General	Account	Address	Profile	Organ	ization			
To change a property for multiple objects, first select the checkbox to enable the change, and then type the change.								
🗹 Job	Title:	Marketing A	ssociate					
🗌 Dep	artment:							
Com	ipany:							
Ma	nager							
Na	me:							
		Change		Proper	ties	C	lear	
		[ОК		Car	ncel	Арр	ly

• 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 Pers	on1 Pro	perties			?	×	Marketing P	erson2 Pro	perties			?	×
Member Of		Dial-in	Envi	ronment	Sessions		Member	Of	Dial-in	Enviro	onment	Sessio	ns
Remote con	itrol	Remote [Deskton Se	rvices Profile	COM+		Remote of	control	Remote D	esktop Sen	vices Profile	CO	M+
General Ad	ddress	Account	Profile	Telephones	Organizati	ion	General	Address	Account	Profile	Telephones	Organi	zation
						1	Job Title:	Marke	eting Associate				
Job litle:	Marke	eting Associate	e]	Departmen	t: Marke	eting				
Department:	Marke	ting					Company:	All Ab	out Computer I	Vetworks			
Company:	All Ab	out Computer	Networks]	Manager						
Manager							Name:]
Name:	Ch	2002	Properti		logr		Marketing P	erson3 Pr	roperties				?
	u	lange	Порен	65 0	ical		Member	Of	Dial-in	E	nvironment		Sessions
							Remote	control	Remote	Desktop	Services Profi	ile	COM+
							General	Address	Account	Profile	Telephor	nes (Organizati
							Job Title:	Mark	keting Associa	ate			
							Departmer	nt: Mark	keting				
							Company:	AII A	bout Compute	er Network	s		
							Manager						
							Name:						
								C	hange	Prop	erties	Clear	r

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 - Group	
New Object - Organizational Unit		Create in: MCSA	2016.local/TestOU1
Create in: MCSA2016.local/		Group name: Group 1-G	
Name:		Group name (pre-Windows 200 Group 1-G	00):
Protect container from accidental deletion		Group scope Domain local Global Universal	Group type Security Distribution
New Object - Group		New Object - Group	
Create in: MCSA2016.lo	cal/TestOU1	Create in: MCSA20	16.local/TestOU1
Group name:			
Group2-G		Group name:	
Group name (pre-Windows 2000):		Group1-DL	
Group2-G		Group name (pre-Windows 2000)	:
Group scope	Group type	Group 1-DL	
O Domain local	 Security 	Group scope	Group type
 Global 	ODistribution		Security
○ Universal		() Global	ODistribution
		OUniversal	

New Object - Group	New Object - Group
Create in: MCSA2016.local/TestOU1	Create in: MCSA2016.local/TestOU1
Group name:	Group name:
Group2-DL	Group 1-U
Group name (pre-Windows 2000):	Group name (pre-Windows 2000):
Group2-DL	Group1-U
Group scope	Group scope Group type O Domain local O Global O Universal Group type O Security O Distribution
Group name:	
Group2-U	
Group name (pre-Windows 2000):	
Group2-U	
Group scope Group type O Domain local Security O Global Distribution	
 Universal 	

• 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					?	\times
General	Members	Member Of	Managed By			
88	Group 1	I-G				
Group r	name (pre-W	/indows 2000): Group 1-	G		
Descrip	tion: [
E-mail:	[
Group	scope		Group	type		
OD	Domain local Security					
Global O Distribution						
OU	niversal					
00	niversal					

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

Group1-G Properties	?	\times	
Select Users, Contacts, Computers, Service Accounts, or	Groups		>
Select this object type:			
Users, Service Accounts, Groups, or Other objects		Objec	t Types
From this location:			
MCSA2016.local		Loca	ations
Enter the object names to select (<u>examples</u>):			
Group2-G		Chec	k Names
Advanced	ОК	(Cancel

• **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**.

Group1-G Properties ?		<
Select Users, Contacts, Computers, Service Accounts, or Gro	ups	×
Name Not Found		×
An object named "group 1-dl" cannot be found. Check the select accuracy and ensure that you typed the object name correctly, or selection.	ed object r remove	types and location for this object from the
Correct this object information and search again		
Select this object type:		
Users, Service Accounts, Groups, or Other objects		Object Types
From this location:		
MCSA2016.local		Locations
Enter the object name:		_
broup 1-dl		
Remove "group 1-dl" from selection		
Г	ОК	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**.



• **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.

Group1-DL Properties						×
General	Members	Member Of	Managed By			
88	Group 1-DL					
Group name (pre-Windows 2000): Group 1-DL						
Descript	tion:					
E-mail:	[
Group	scope		Group	type		
٥D	omain local		O Se	curity		
G	obal		ODi	stribution		
OU	niversal					

• 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.

Group1-DL Properties	?	×	
Select Users, Contacts, Computers, Service Accounts,	or Groups		×
Select this object type:			
Users, Service Accounts, Groups, or Other objects		Object 7	Types
From this location:			
MCSA2016.local		Locati	ons
Enter the object names to select (<u>examples</u>):			
Group 1-G		Check	Names
Advanced	OK		ancel
Advanced	UN		nicer

• 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.

6	Group1-U Properties ? ×			
ſ	Select Users, Contacts, Computers, Service Accounts, or Groups	×		
	Name Not Found	>	×	
	An object named "group 1-dl" cannot be found. Check the selected object ty accuracy and ensure that you typed the object name correctly, or remove th selection.	ypes and location fo nis object from the	Group1-U Properties	?
	Correct this object information and search again		General Members Member Of Managed By	
	Select this object type: Users, Service Accounts, Groups, or Other objects	Object Types	es Members:	
	From this location: MCSA2016.local	Locations	Name Active Directory Domain Services	Folder
ľ	Enter the object name:		Group 1-G MCSA2016.local/TestOU1 MCSA2016.local/TestOU1 MCSA2016.local/TestOU1	
	Remove "group 1-di" from selection			
	ОК	Cancel	el	

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

Active Directory Users and Co	Active Directory Users and Computers							
File Action View Help								
	← ⇒ 2 □ □ □ 2 □ 2 □ 3 3 2 7 2 3							
 Active Directory Users and (Saved Queries MCSA2016.local Administration Builtin Computers Domain Controllers ForeignSecurityPrinc Managed Service Ac Marketing Operations Research and Develc 	Name Administration Builtin Computers Domain Controllers ForeignSecurityPrincip Managed Service Acc Marketing Operations Research and Develop Users	Type Organizational U builtinDomain Container Organizational U Container Organizational U Organizational U Organizational U Container	Description Default container for up Default container for do Default container for sec Default container for ma					
Users TestOU1	TestOU1	Organizational U						

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.

Active Directory Users and Comp File Action View Help		a a a		
 Active Directory Users and Com Saved Queries TestDomain.local Builtin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accour TestOU1 Users 	Name Builtin Computers Domain Con ForeignSecu Managed Se TestOU1 Users	Type builtinDomain Container Organizational Container Organizational Container	Description Default container for up Default container for do Default container for sec Default container for ma Default container for up	

• 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.

Administrators Properties ?						×		
General	Members	Member Of Managed By						
88	Administrators							
Group n	Group name (pre-Windows 2000): Administrators							
Descript	tion:	Administrators	have complete	e and unrest	ricted acce	ss to		
E-mail:	[
Group	scope		Group	type				
Bu	uiltin local		Se	Security				
G	Global Distribution							
O Universal								
Notes:								

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

Administrators Proper	ties	?	\times				
General Members	lember Of Managed By						
Members:	Members:						
Name	Active Directory Domain Services Folder						
시 Administrator	MCSA2016.local/Users						
گ domadmin 1	MCSA2016.local/Users						
👗 domadmin2	MCSA2016.local/Users						
🍇 Domain Admins	MCSA2016.local/Users						
🍇 Enterprise Ad	MCSA2016.local/Users						

• 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.

Guests Properties		?	×	Users Pro	operties			?
General Members	Member Of Managed By			General	Members	Member Of	Managed By	
Members:				Membe	ers:			
Name	Active Directory Domain Services Folder	r		Name	•	Active Dir	ectory Domain	Services Folder
& Domain Guests	MCSA2016.local/Users			👥 👷 Al	uthenticated	NT AUTH	IORITY	
🛃 Guest	MCSA2016.local/Users			8 D	omain Users	MCSA20	6.local/Users	
				👏 IN	ITERACTIV	E NT AUTH	IORITY	
				l l				

• 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**.

Domain Admins Pro	operties	? Domain /	Admins Pro	operties		
General Members	Member Of Managed By	General Membe	Members rs:	Member Of	Managed By	
Group name (pre-W Description:	Vindows 2000): Domain Admins Designated administrators of the domain	Name	ministrator	Active Dir MCSA201	ectory Domain 6.local/Users	Services Folder
E-mail: Group scope	Group type					
 Domain local Global Universal 	 Security Distribution 					

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.

Do	main l	Users Prope	erties		?
G	eneral	Members	Member Of	Managed By	
	Membe	rs:			
	Name	•	Active Dir	ectory Domain Services Folde	er
	<u>_</u>	larketing T	. MCSA201	6.local/Marketing	
	🙎 Ad	Iministrator	MCSA201	6.local/Users	
	🐁 De	efaultAccour	t MCSA201	6.local/Users	
	💄 do	madmin 1	MCSA201	6.local/Users	
	🙎 do	madmin2	MCSA201	6.local/Users	
	🙎 do	muser1	MCSA201	6.local/Users	
	🙎 do	muser2	MCSA201	6.local/Users	
	🙎 Jo	e Tech1	MCSA201	6.local/Operations	
	🐁 krt	otgt	MCSA201	6.local/Users	
	🙎 🔏	arketing Per.	MCSA201	6.local/Marketing	
	🙎 Ma	arketing Per.	MCSA201	6.local/Marketing	
	🙎 Ma	arketing Per.	MCSA201	6.local/Marketing	
	🙎 Te	est User1	MCSA201	6.local/Operations	

• 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

Ge	neral	Members	Member Of	Managed By				
Μ	lembe	rs:						
	Name		Active Dir	Active Directory Domain Services Folder				
ESERVERDM1 MCSA2016.local/Com			6.local/Compu	ters				
	💻 SE	SERVERDM2 MCSA2016.local/Computers						

• **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.

:\Users\Administrator>whoami/groups							
SROUP INFORMATION							
Group Name	Туре	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.

C1 🗏 🕼 🖌	🖻 ServerSA1						
nternet Protocol Version 4 (TCP/IPv4)	Properties X						
General							
You can get IP settings assigned autor this capability. Otherwise, you need to for the appropriate IP settings. Obtain an IP address automatical	natically if your network supports ask your network administrator ly						
Ouse the following IP address:							
IP address:	192.168.0.4						
Subnet mask:	255.255.255.0						
Default gateway:	192.168.0.2						
Obtain DNS server address auton	natically						
• Use the following DNS server add	resses:						
Preferred DNS server:	192.168.0.1						
Alternate DNS server:	1 . 1 . 1 . 1						
Validate settings upon exit	Advanced						

• 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**.

System Properties

Computer Name/Domain	Changes	×	
You can change the name ar computer. Changes might affe	computer		
Computer name:			
ServerSA1			
Full computer name: ServerSA1			
		More	ange
Member of			
O Domain:			
Workgroup:			
WORKGROUP			
	ОК	Cancel	
	ОК	Cancel	Apply

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

	2	System Properties						
Dash	bc	Computer Name/Domain Ch	anges	×				
Wir	Windows Security X							
Сс	om	outer Name/Doma	in Changes					
Enter the name and password of an account with permission to join the domain.								
	Q	User name						
Password								
Domain: MCSA2016.local								
		OK	Cancel					

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: ServerSA1	poration. All righ	Computer Name/Domain Changes		
Full computer name: ServerSA1 Member of ① Domain: [MCSA2016.local	Computer Name/Domain Changes X	1	You must restart your computer to apply these changes Before restarting, save any open files and close all programs.	
WORKGROUP	OK Cancel		ОК	

• 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.

	e c. <	ServerDC1		
	Active Directory Users an	d Computers		_
	File Action View Help)		
	🗢 喇 🖄 📊 📋 🖾	0 🗟 🛛 🖬 🗏 🝇	🛅 🍸 🗾 🐍	
Microsoft Windows X	Active Directory Users Saved Queries Saved Queries MCSA2016.local	Name Administration	Type Organizational U	D
You must restart your computer to apply these changes	> 🖆 Administration > 🖆 Builtin > 🖆 Computers > 🖆 Domain Contro	Builtin Computers Domain Controllers ForeignSecurityPrincip	builtinDomain Container Organizational U Container	Di Di Di
Before restarting, save any open files and close all programs.	> 🛗 ForeignSecurit > 🛗 Managed Servi	Managed Service Acc	Container Organizational U	Di
Restart Now Restart Later	> ☐ Marketing > ☐ Operations	Operations Research and Develop	Organizational U Organizational U	

 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.M	ACSA2016> systeminfo
Host Name:	SERVERSA
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 РМ
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:	<pre>VMware, Inc. VMW71.00V.16722896.B64.2008100651, 8/10/202</pre>
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:	2,04/ MB
Available Physical Memory:	484 MB
Virtual Memory: Max Size:	/,SII MB
Virtual Memory: Available:	5,030 MB
Virtual Memory: In Use:	1,8/0 MB
Page File Location(s):	C:\pagetile.sys
Domain:	MCSA2016.Tocal
Logon Server:	\\SERVERDC1
HOTTIX(S):	4 HOTTIX(S) INSTALLED.
	[UI]: KB319213/
	[U2]: KB321132U [02], KB5001079
	[U3]: KB3UUIU/0 [04], kp4102720
Natural Cand(a)	[U4]: KB41U5/2U 2 NTC(c) Thetallod
Network Card(s):	2 NIC(S) INStalled. [01], Instal(D) 92574, Cigabit Natural Connection
	[01]: Inter(R) 623/4L Gigabit Network Connection
	DUCP Enabled: No
	TP address (es)
	$[011] \cdot 102 168 0 4$
	$[01] \cdot 192.100.0.4$ $[02] \cdot f_{0}80 \cdot \cdot 507c \cdot h205 \cdot a0h1 \cdot 3a06$
	[02]: Intel(R) 82574L Gigabit Network Connection
	Connection Name: Ethernet1

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

PS C:\Users\administrator.MCS	SA2016> 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.loćal
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	:
LinkedGroupPolicvObjects	: {CN={31B2F340-016D-11D2-945F-00C04FB984F9}.CN=Policie
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.

Administrator	이 C1 🗏 🖙 🄇 🖻 ServerSA1
Administrator: Windows PowerShell	
BIOS Version: Windows Directory: System Directory: Boot Device: System Locale: Input Locale: Time Zone: Total Physical Memory: Available Physical Memory: Virtual Memory: Max Size: Virtual Memory: Max Size: Virtual Memory: Available: Virtual Memory: In Use: Page File Location(s): Domain: Logon Server: Hotfix(s):	<pre>[02]: Intel64 Family 6 Model 61 Steppi VMware, Inc. VMW71.00V.16722896.B64.20 C:\Windows C:\Windows\system32 \Device\HarddiskVolume2 en-us;English (United States) en-us;English (United States) (UTC-08:00) Pacific Time (US & Canada) 2,047 MB 845 MB 3,199 MB 1,920 MB 1,279 MB C:\pagefile.sys WORKGROUP SERVERSA1 4 Hotfix(s) Installed.</pre>

 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.

Active Directory Users and Computers		🗙 🗐 🖸 📑 🛛 🦉 🧊	🐍 🗽 🛅 🍸 🏅
File Action View Help ←	* * 7 2 4	Name	Туре
Active Directory Users A Saved Queries MCSA2016.local Saved Administratior Builtin Computers Computers	rpe De omputer omputer omputer	IN SERVERDM1	Computer Computer Computer

	ServerDC1	ð				
Active Directory Users an	d Computers		- (<i>≣</i> , <	ServerDC1	
File Action View Help)					
🗢 🄿 🖄 🖬 🖌 📋	🗙 🗐 🖬 🗟 🗐	🐮 🗽 🛅 🍸 🗾 🍇	4	Active Directory Users an	d Computers	
Active Directory Users	Name	Type Descrip	_{ot} ile	Action View Help)	
> Carlos Saved Queries	I SERVERDM1	Computer Computer		🔌 🗖 📰 🗟 🛛 🖉	🖬 🗏 🐮 🗑 🖉 🖉	٤.
> C Administration	SERVERSA1	Computer	A	ctive Directory Users 🔺	Name	Туре
Active Directory Domain Se	vivices	× rnamed 'SERVERSA1'?		Saved Queries MCSA2016.local Administration Builtin Computers	SERVERDM1	Computer Computer
-	Ye	s No				

 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.

New Object - Computer	\times
Create in: MCSA2016.local/Computers	
Computer name:	
ServerSA1	
Computer name (pre-Windows 2000):	
SERVERSA1	
The following user or group can join this computer to a domain.	
User or group:	
Default: Domain Admins Change	
Assign this computer account as a pre-Windows 2000 computer	
OK Cancel Help	

 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.

PS C:\Users\Administrator> Add-Computer MCSA cmdlet Add-Computer at command pipeline posi	2016.local -Res tion 1	tart		
supply values for the following parameters:	cmdlet Add-Comp	uter at command pip	? X	
			1 P	
	Supply values for th	ne following parameters:		
	<u>U</u> ser name:	🕵 jtech1	~ _	
	Password:	•••••		
		ОК	Cancel]
mdlet Add-Computer at command pipeline pos Supply values for the following parameters Add-Computer : Computer 'ServerSA1' failed WORKGROUP' with following error message: , At line:1 char:1 Add-Computer MCSA2016.local -Restart	sition 1 : to join domair Access is denie	'MCSA2016.local ed.	' from its	current wo
+ CategoryInfo : OperationSto + FullyQualifiedErrorId : FailToJoinDo	oped: (Server5A mainFromWorkgro	1:String) [Add-Co oup,Microsoft.Pow	omputer], erShell.Co	InvalidOper mmands.AddO

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.



• 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.



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.



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.

🔿 🖉 📶			2 ·88
Active Directo	ory Users and Compute	ers [S Name	Туре
MCSA201	eries 6 local	🐁 AdminUser1	User
	istration		
> 📔 Builtin			
S 📑 Comp	uters		
> 📓 Doma	in Controllers		
> 📔 Foreig	nSecurityPrincipals		
> 📔 Manag	ged Service Accounts		
✓ ☑ Marke	ting		
Ad 🔝	vertising		
> Decay	tions		
> TestOl	In and Development		
> I Users			
> 📔 Users			
> 📔 Users	_	2	~
> 🦳 Users	25	?	×
> 🦳 Users minG Propertie eneral Member	s Member Of Manage	? ed By	×
> 🚆 Users minG Propertie eneral Members:	s Member Of Manage	? ed By	×
> 🚆 Users minG Propertie eneral Members Members: Name	s Member Of Manage Active Directory Do	? ed By omain Services Folder	×
> 🚆 Users minG Propertie eneral Members Members: Name & AdminUser1	8 Member Of Manage Active Directory Do MCSA2016.local/1	? ed By omain Services Folder Marketing/Advertising	×
> 🚆 Users minG Propertie eneral Members Members: Name & AdminUser1	s Member Of Manage Active Directory Do MCSA2016.local/I	? ed By omain Services Folder Marketing/Advertising	×
> 📔 Users minG Propertie eneral Members Members: Name & AdminUser1	s Member Of Manage Active Directory Do MCSA2016.local/1	? ed By omain Services Folder Marketing/Advertising	×
> 🗋 Users minG Propertie eneral Members Members: Name & AdminUser1	8 Member Of Manage Active Directory Do MCSA2016.local/1	? ed By omain Services Folder Marketing/Advertising	×
> 🚆 Users minG Propertie eneral Members Members: Name & AdminUser1	s Member Of Manage Active Directory Do MCSA2016.local/I	? ed By omain Services Folder Marketing/Advertising	×
> 🔛 Users minG Propertie eneral Members Members: Name & AdminUser1	s Member Of Manage Active Directory Do MCSA2016.local/1	? ed By omain Services Folder Marketing/Advertising	×

- 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.

```
ivadd-Notepad - C ×
File Edit Format View Help
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 Administratio n -ln User1 -upn AdminUser1@MCSA2016.local -pwd Password01 -memberof "CN=AdminG,OU=Administration, DC=MCSA 2016, 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 (1 % % 11 7 2 %	5	
 Active Directory Users and Computers [S Saved Queries MCSA2016.local Administration Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accounts 	Name AdminG AdminUser1	Type Security Group User	Descrip

• 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 A	dministration User3
C:\Users\Administrator>dsadd user "CN=AdminUser2,OU=Administration,D n -ln User2 -upn AdminUser2@MCSA2016.local -pwd Password01 -memberof 2016, DC=local" -mustchpwd yes -disabled yes dsadd succeeded:CN=AdminUser2,OU=Administration,DC=MCSA2016,DC=local	C=MCSA2016,DC=loc "CN=AdminG,OU=Ad	al" -fn Administratio Ministration, DC=MCSA
C:\Users\Administrator>dsadd user "CN=AdminUser3,OU=Administration,D n -ln User3 -upn AdminUser3@MCSA2016.local -pwd Password01 -memberof 2016, DC=local" -mustchpwd yes -disabled yes dsadd succeeded:CN=AdminUser3,OU=Administration,DC=MCSA2016,DC=local	C=MCSA2016,DC=loc "CN=AdminG,OU=Ad	al" -fn Administratio ministration, DC=MCSA
Active Directory Users and Computers		
File Action View Help		
🗢 🄿 📶 💼 🗎 🗐 🗟 🗟 🖬 🖏 🐮 🝸 💆 🎕		
Active Directory Users and Computers [S Name	Туре	Description

AdminG 🎎

🛃 AdminUser1

🛃 AdminUser2

🛃 AdminUser3

Security Group - ...

User

User

User

Saved Queries

MCSA2016.local

📋 Builtin

> Computers

Administration

> Domain Controllers

ForeignSecurityPrincipals
Managed Service Accounts

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 gr dsadd succeeded:CN=SalesG,OU=Ma	roup CN=SalesG,OU=Ma arketing,DC=MCSA2016	rketing,DC=MCSA2016,DC=local ,DC=local
C:\Users\Administrator> Active Directory Users and Computers File Action View Help (= (+)) (2) ((+)) ((+)) ((+)) ((+)) ((+)) ((+)) ((+)) ((+))) ((+)) ((+)) ((+))) ((+)) ((+)) ((+)) ((+))) ((+)) 🛛 📷 🐍 🔌 🛅 🎙	7 🔁 强
 Active Directory Users and Computers [S Saved Queries MCSA2016.local Administration Builtin Computers Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accounts Marketing 	Name Marketing Template Advertising Marketing Person1 Marketing Person2 Marketing Person3 MarketingG SalesG	Type User Organizational User User User Security Group Security Group

• 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. Sales G Properties ? >

General	Members	Member	Of	Managed By
Membe	rs:			
Name			Acti	ve Directory Domain Services Folder
<u>_</u> _N	Marketing Te	mplate	MC	SA2016.local/Marketing
🙎 Ma	arketing Per	son1	MC	SA2016.local/Marketing
🛛 🤱 Ma	arketing Pers	son2	MC	SA2016.local/Marketing
🛛 🤱 Ma	arketing Per	son3	MC	SA2016.local/Marketing

 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.

dened even ded. ON Administration ON Users DO NOCADOLO DO legal	
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=1	ocal
dsmod succeeded:CN=Marketing Person1,OU=Marketing,DC=MCSA2016,DC=loc	al
dsmod succeeded:CN=Marketing Person2,OU=Marketing,DC=MCSA2016,DC=loc	al
dsmod succeeded:CN=Marketing Person3,OU=Marketing,DC=MCSA2016,DC=loc	al
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.



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.



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\Administra	tor> Search-ADAccount -AccountDisabled -SearchBase "OU=Administration,DC=MCSA2016,DC=local"
AccountExpirationDate	
DistinguishedName	. CN-Administrantion DC-NCEA2016 DC-local
Enabled	Ch-Administration, DC-MCSA2010, DC-TOCA1
	: False
LastLogonDate	;
Lockedout	
Name	Adminuseri
ObjectClass	
ObjectGUID	: 6a2T11a9-2027-4004-D526-TC61T2D0900D
PasswordExpired	- False
PasswordNeverExpires	: Irue
SamAccountName	: AdminUser1
SID	: 5-1-5-21-3906145736-3692421193-1951280030-1625
UserPrincipalName	: AdminUser1@MC5A2016.local
AccountExpirationDate	
DistinguishedName	CN=AdminUser2.0U=Administration.DC=MCSA2016.DC=local
Enabled	: False
LastLogonDate	
LockedOut	False
Name	Adminuser2
ObjectClass	
ObjectGUTD	47b2b674-5df8-4ad3-ab24-a1a1157d4cb0
PasswordExpired	False
PasswordNeverExpires	· True
SamAccountName	· Adminiser2
STD	- Salar 10521-3906145736-3692421193-1951280030-1626
UserPrincipalName	• Administer2000542016 local
user Principaritaile	· Auminiosci zencsazoto, iocat
AccountExpirationDate	:
DistinguishedName	: CN=AdminUser3,OU=Administration,DC=MCSA2016,DC=local
Enabled	: False
LastLogonDate	:
Locked0ut	: False
Name	: AdminUser3
ObjectClass	: user
ObjectGUID	: 3ff3cdcc-5949-4f99-a4f1-8af019156db3
PasswordExpired	: False
PasswordNeverExpires	: True
SamAccountName	: AdminUser3
SID	: 5-1-5-21-3906145736-3692421193-1951280030-1627
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

csvusers.csv - Notepad -
 File Edit Format View Help

 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.

🧾 Save As			>
< > · 1	→ This PC → Local Disk (C:) →	✓ ³ Search Local Disk	c (C:)
Organize 🔻 🛛 Ne	ew folder		== • ?
 ✓ Quick access ✓ Desktop ✓ Downloads ✓ Documents 	Name PerfLogs Program Files Program Files (x86) Users	Date modified Type 7/16/2016 9:23 AM File fol 2/19/2021 6:09 PM File fol 7/16/2016 9:23 AM File fol 2/19/2021 5:59 PM File fol	der der der der
File name: Save as type:	<pre>* v < "C:\csvusers.csv" Text Documents (*.txt)</pre>		>
∧ Hide Folders	Encoding: ANSI	✓ Save	Cancel

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.



• **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 Idfide 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

```
Initial - 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.

Save As					×
$\leftarrow \rightarrow \cdot \cdot \uparrow$	> This PC $$ > Local Disk (C:) $$ >	~	ල් Search L	.ocal Disk (C:)	م
Organize 🔻 Ne	w folder			:==	- ?
Documents	🖈 ^ Name	Date	e modified	Туре	Siz
Pictures	PerfLogs	7/10	5/2016 9:23 AM	File folder	
🏪 Local Disk (C:	Program Files	2/19	9/2021 6:09 PM	File folder	
System32	Program Files (x86)	7/10	5/2016 9:23 AM	File folder	
💻 This PC	Users	2/19	9/2021 5:59 PM	File folder	
	V <	-			>
File name:	"C:\ldfusers.ldf"	I			`
Save as type:	Text Documents (*.txt)				`
∧ Hide Folders	Enc	oding: ANSI	∼ Sa	ive Ca	incel

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.

