3/17/2021

Hands On Exercise

Chapter 4 Configuring Group Policies

(Part 2)

El Adel, Taoufik IT 416 - SPRING 2021 - OLD DOMINION UNIVERSITY Table 4-1 Activity requirements

Activity	Requirements	Notes
Activity 4-1: Resetting Your Virtual Environment	ServerDC1, ServerDM1, ServerDM2, ServerSA1	
Activity 4-2: Working with Local GPOs	ServerDC1, ServerDM1	
Activity 4-3: Browsing GPTs and GPCs	ServerDC1	
Activity 4-4: Creating, Linking, and Unlinking GPOs	ServerDC1	
Activity 4-5: Configuring and Testing a GPO	ServerDC1, ServerDM1	
Activity 4-6: Creating and Using Starter GPOs	ServerDC1	
Activity 4-7: Deploying a Shutdown Script to a Computer	ServerDC1, ServerDM1	
Activity 4-8: Configuring a Folder Redirection Policy	ServerDC1, ServerDM1	
Activity 4-9: Reviewing User Rights Assignment and Security Options Settings	ServerDC1	
Activity 4-10: Working with Computer Administrative Template Settings	ServerDC1, ServerDM1	
Activity 4-11: Working with User Administrative Template Settings	ServerDC1, ServerDM1	
Activity 4-12: Viewing Policy Settings with Filter Options	ServerDC1	
Activity 4-13: Configuring and Testing Preferences	ServerDC1, ServerDM1	
Activity 4-14: Configuring Item-Level Targeting	ServerDC1, ServerDM1	-

Activity 4-7: Deploying a Shutdown Script to a Computer

Description: In this activity, you write a shutdown script that deletes all files with a .temp extension, and deploy this script using group policies.

• 4-7-1: On ServerDC1, start Notepad and type del / FIS c:*.temp. The /F option forces the deletion of read-only files, and the /s option deletes the file in the current directory and all subdirectories.

4-7-2: Click File, Save As from the menu. Choose the desktop as the location for saving your file. In the Save as type list box, click All Files (*.*). Type deltemp.bat in the File name text box and click Save. Exit Notepad.



• 4-7-3: Right-click **deltemp.bat** on your desktop and click **Copy.** (You paste the script into the SYSVOL share in a later step.)

Q .,		
494	Open	
deltemp	Edit	
	Print	
	😌 Run as administrator	
	🚼 Scan with Windows Defender	
	Share with >	
	Restore previous versions	
	Send to >	
	Cut	
	Сору	
	Paste	
	Create shortcut	

 4-7-4: Open the Group Policy Management console. Click the Group Policy Objects folder and create a GPO named Scripts.

Group Policy Management		PrintCo	onfigG	PO			
Forest: MCSA2016.local		Scope	Details	Settings	Delegation	Status	
V B Domains		Links					
MCSA2016.local							
🛒 Default Domain	Policy	Display	links in th	is location:		MCSA201	6.local
🔉 💼 Domain Contro	New GPO						×
> 📓 TestOU1	New or o						~
🗸 📑 Group Policy O	Name:						
🧾 Default Don	Scripts						
🧾 Default Don							
🗐 GPO1	Source Starter	GPO:					
PrintConfig	(none)						~
TestGPO	. ,						
> 🕞 WMI Filters					ОК	Ca	ancel
> 🛅 Starter GPOs							

 4-7-5: Right-click the Scripts GPO and click Edit. In the Group Policy Management Editor, click to expand Computer Configuration, Policies, and Windows Settings, and then click Scripts (Startup/Shutdown). Right-click Shutdown in the right pane and click Properties. In the Shutdown Properties dialog box, click Show Files.

In the File Explorer window that opens, right-click the right pane and click **Paste**. Note the path where the script is stored-a folder in the SYSVOL share on your DC. Close the File Explorer window.

Shutdown Properties	?	×			
Scripts PowerShell Scripts					
Shutdown Scripts for Scripts					_
	📊 🛃 📊 🛨			Application Tools	Shutdown
Name Parameters	File Home	Share	View	Manage	
	$\leftarrow \rightarrow \land \uparrow$	« Ma	achine > Sc	ripts > Shutdown	
			Name	^	
	📌 Quick access				
	Desktop	*	leiter	np	
	Downloads	*			
	Documents	*			
	Pictures	*			
To view the script files stored in this Group Po the button below.	💻 This PC				
Show Files	💣 Network				

• 4-7-6: In the Shutdown Properties dialog box, click Add. In the Add a Script dialog box, click Browse. Click deltemp, and then click Open. Click OK twice.

Shutdown Properties			?	\times
Scripts PowerShell Scripts				
Shutdown Scrip	ots for Scripts			
Name	Parameters			
deltemp.bat			Up	
			Dowr	n
			Add	
			Edit	
			Remov	/e
To view the script files store the button below. Show Files	d in this Group P	olicy Object, pr	ess	
	ОК	Cancel	Ap	oply

4-7-7: Close the Group Policy Management Editor. Link **Scripts** to the **TestOU1** OU, which is where you moved the ServerDM1 account to earlier.



4-7-8: Sign in to ServerDM1 as domadmin1. You're going to create a few files on your desktop that have the .temp extension. Open a command prompt window, then type cd desktop, and press Enter. Type copy nul > file1.temp and press Enter to create an empty file. Repeat the command two more times, changing

file1 to file2 and then file3. You see the files on your desktop (you may have to minimize Server Manager and the command prompt to see the files).



4-7-9: Type **gpupdate** and press **Enter.** After gpupdate is finished, restart ServerDM1. (If you don't run gpupdate, you have to restart the computer to load the policy and then shut it down again to make the shutdown script run.) The shutdown process will probably take a little longer than usual because the script has to run.



4-7-10: Sign in to ServerDM1 as **domadmin1** again and verify that the .temp files have been deleted. Sign out of ServerDM1.





4-7-11: On ServerDC1, unlink the **Scripts** GPO from the **TestOU1** OU. Continue to the next activity.



Activity 4-8: Configuring a Folder Redirection Policy

Description: In this activity, you configure a folder redirection policy for the Documents folder and apply it to ServerDM1.

• 4-8-1: On ServerDC1, open File Explorer and create a folder named **Redirected** in the **C** volume. Share the folder, giving the **Everyone** group **Read/Write** sharing permission, and leave the remaining permissions at their default settings. Close File Explorer.

Thi	s PC > Local Disk (C:) >		Share Permissions		
	Name	✓ Date me	Group or user names:		
*	PerfLogs	2/20/20			
*	Program Files	2/19/20			
*	Users	2/19/20		Add	Remove
*	Windows	3/23/20	Permissions for Everyone	Allow	Deny
	📄 bootsqm.dat	3/23/20	Full Control		
	Redirected	3/23/20	Change Read	$\mathbf{\nabla}$	

4-8-2: Open the Group Policy Management console and create a GPO named FolderRedir in the Group Policy Objects folder. Open FolderRedir in the Group Policy Management Editor. Expand User Configuration, Policies, Windows Settings, and Folder Redirection. Right-click the Documents folder and click Properties.



4-8-3: In the Documents Properties dialog box, click **Basic - Redirect everyone's folder to the same location** in the Setting drop-down list. Click the **Target folder**

location list arrow to view the available options, and then, if necessary, click **Create a folder for each user under the root path** in the list. In the Root Path text box, type **ServerDC1\Redirected.**

Documents	Properties	?	×
Target Se	ettings		
	You can specify the location of the Documents folde	er.	
Setting:	Basic - Redirect everyone's folder to the same locat	tion	•
This folde	r will be redirected to the specified location.		
Target f	older location a folder for each user under the root path		•
Root Pa	ath:		
\\Serv	erDC1\Redirected		
	Br	owse	
For use	Clair, this folder will be redirected to:		
\\Serve	rDC1\Redirected\Clair\Documents		
	OK Cancel	Ар	ply

4-8-4: Click the Settings tab and review the available options. Click to clear the Grant the user exclusive rights to Documents check box. Click Redirect the folder back to the local userprofile location when policy is removed, click OK, and in the warning message box, click Yes. Close the Group Policy Management Editor.

Warning		\times
If there are Group Policy settings related to Folde Windows 2000, Windows 2000 Server, Windows X will not be able to change any Folder Redirection Object (GPO) from those operating systems.	r Redirection that do not apply to P or Windows Server 2003, you settings in this Group Policy	
Do you want to continue?		
	Yes No	

• 4-8-5: In the Group Policy Management console, link the FolderRedir GPO to Test0U1.

TestO	001	
Linked	Group Policy Objects	Group Policy Inher
Select	: GPO	
Look i	n this domain:	
	MCSA2016.local	
Group	Policy objects:	
	Name	^
	Default Domain Contr	ollers Policy
	Default Domain Policy	
	FolderRedir	
	GPO1	
	PrintConfigGPO	
	Scripts	
	TestGPO	

• **4-8-6:** Open Active Directory Users and Computers and move the user **domadmin1** (located in the Users folder) to TestOU1 by dragging and dropping the user account.

Active Di	rectory Domai	n Services			×
Â	Moving objects system from w organizational accounts withir	in Active Direct orking the way i unit (OU) can af n the OU.	tory Domain it was design ffect the way	Services can prevent red. For example, mo y that group policies :	t your existing oving an are applied to the
	Are you sure y	ou want to mov	e this object	?	
	Don't show	this warning wh	nile this snap	-in is open.	
		Yes	No		

4-8-7: On ServerDM1, sign in as domadmin1 and run gpupdate from a command prompt. Then sign out of ServerDM1 and sign in again as domadmin1. You might see a message indicating that folder redirection is occurring.



• 4-8-8: On ServerDC1, open File Explorer and navigate to C:\redirected. You see a folder there named domadmin1 and in that folder is folder named Documents.

₿	Ē.	<	화 ServerDC1
do	madmii	1	
	Share	View	
	→ Thi	s PC → Local Disk (C:) → I	edirected > domadmin1 > 🗸 💆 Search d
		Name	Date modified Type
55	*	Documents	3/23/2021 1:15 PM File folder
ds	*		

4-8-9: Unlink the **FolderRedir** GPO from **Test0U1.** Continue to the next activity.

lestOU1			
Linked Group F	Policy Objects	Group Policy Inheritance	Delegation
li	nk Order	GPO	Enforced
2	1	🛒 FolderRedir	No
	Group Policy Management		×
$\overline{\nabla}$? Do Thi	you want to delete this I s will not delete the GPC	ink?) itself.
	OK Cancel		

Activity 4-9: Reviewing User Rights Assignment and Security Options Settings

Description: In this activity, you open the Group Policy Management Editor and explore the User Rights Assignment and Security Options policies.

4-9-1: On ServerDC1, open the Group Policy Management console, and then open **GP01** in the Group Policy Management Editor.



4-9-2: Click to expand **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, and **Local Policies**, and then click **User Rights Assignment**. Browse the list of policies and double-click any that look interesting or that aren't self-explanatory. Click the **Explain** tab and read the detailed description. Suggested policies to view in detail include Add workstations to domain, Back up files and directories, Bypass traverse checking, Allow log on locally, Deny log on locally, Load and unload device drivers, Shut down the system, and Take ownership of files or other objects.

Access Credential Manager as a trusted caller	N
Access this computer from the network	N
Act as part of the operating system	N
🔯 Add workstations to domain	N
🔯 Adjust memory quotas for a process	N
🔯 Allow log on locally	N
🔯 Allow log on through Remote Desktop Services	N
🔯 Back up files and directories	N
🔯 Bypass traverse checking	N
👸 Change the system time	N
🔯 Change the time zone	N
📖 Create a pagefile	N
🔯 Create a token object	N
🔯 Create global objects	N
🔯 Create permanent shared objects	N
👸 Create symbolic links	N
🔯 Debug programs	N
🔯 Deny access to this computer from the network	N
📖 Deny log on as a batch job	N
🔯 Deny log on as a service	N
🔯 Deny log on locally	N
🕅 Denv loa on throuah Remote Desktop Services	N

4-9-3: Browse the **Security Options** node in a similar manner. Suggested policies to view in detail include Accounts: Administrator account status, Accounts: Rename administrator account, Accounts: Limit local account use of blank passwords to console logon only, Audit: Force audit policy subcategory settings, Devices: Prevent users from installing printer drivers, Interactive logon: Do not display last user name, Interactive logon: Message text for users attempting to log on, Interactive logon: Prompt user to change password before expiration, Network access: Shares that can be accessed anonymously, Network security: Force logoff when logon hours expire, Shutdown: Clear virtual memory pagefile, User Account Control: Behavior of the elevation prompt for standard users, and User Account Control: Run all administrators in Admin Approval Mode.

Policy	Policy Setting
🔯 Accounts: Administrator account status	Not Defined
🔯 Accounts: Block Microsoft accounts	Not Defined
🔯 Accounts: Guest account status	Not Defined
🔯 Accounts: Limit local account use of blank passwords to co	Not Defined
🔯 Accounts: Rename administrator account	Not Defined
🔯 Accounts: Rename guest account	Not Defined
🔯 Audit: Audit the access of global system objects	Not Defined
🔯 Audit: Audit the use of Backup and Restore privilege	Not Defined
🔯 Audit: Force audit policy subcategory settings (Windows Vis	Not Defined
🔯 Audit: Shut down system immediately if unable to log secur	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor D	Not Defined
🔯 DCOM: Machine Launch Restrictions in Security Descriptor	Not Defined
🔯 Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
🔯 Devices: Prevent users from installing printer drivers	Not Defined
🔯 Devices: Restrict CD-ROM access to locally logged-on user	Not Defined
🔯 Devices: Restrict floppy access to locally logged-on user only	Not Defined
🔯 Domain controller: Allow server operators to schedule tasks	Not Defined
🔯 Domain controller: Allow vulnerable Netlogon secure chann	Not Defined
🔯 Domain controller: LDAP server channel binding token requi	Not Defined
🔯 Domain controller: LDAP server signing requirements	Not Defined
🕅 Domain controller: Refuse machine account password chan	Not Defined

• **4-9-4:** When you have time, you should explore these nodes more thoroughly to become more familiar with the settings. Close Group Policy Management Editor and continue to the next activity.

Activity 4-10: Working with Computer Administrative Template Settings

Description: In this activity, you explore Administrative Templates settings under Computer Configuration and configure some settings to see the effect they have on the computer operating environment.

4-10-1: On ServerDC1, open GP01 in the Group Policy Management Editor.



4-10-2: Under Computer Configuration, click to expand **Policies** and **Administrative Templates**. Browse through the folders under Administrative Templates to see the settings and subfolders under each one. Take your time to get a good feel for the types of settings available in each main folder.

Personalization	
Personalization Select an item to view its description.	Setting Force a specific default lock screen and logon image Prevent changing lock screen and logon image Prevent changing start menu background Do not display the lock screen Prevent enabling lock screen camera Prevent enabling lock screen slide show Force a specific background and accent color
	Force a specific Start background

 4-10-3: Click the All Settings folder to see the full list of settings in Administrative Templates. The settings are arranged in alphabetic order by default. Click the State column to view the settings according to their state, which is Not configured, Enabled, or Disabled. Because GP01 has no configured settings, the view doesn't change.

GPO1 [SERVERDC1.MCSA2016.LOCAL]	Setting	State
 Computer Configuration Policies Software Settings Windows Settings Administrative Templates: P Control Panel Network 	Access 2013 backup only Access 2016 backup only Access 2016 backup only Access data sources across domains Access data sources across domains	Not configured Not configured Not configured Not configured Not configured Not configured
 Network Printers Server Start Menu and Taskbar System Windows Components All Settings 	Access data sources across domains	Not configured Not configured Not configured Not configured Not configured Not configured
 Preferences User Configuration Policies Preferences 	Action on server disconnect Activate Internet printing Activate Shutdown Event Tracker System State Data feature Add a specific list of soarch providers to the user's list of soarch	Not configured Not configured Not configured

 4-10-4: In the left pane, click to expand the System folder, and then click Logon. In the right pane, click the Setting column header to arrange the setting in alphabetical order and then double-click Run these programs at user logon. This policy can be used in place of a logon script if you want more programs to run when any user logs on to certain computers.

Run these program	ns at user logon					_		\times
📷 Run these prograr	ns at user logon			Previous Setting	Next Setti	ng		
Not Configured	Comment:							^
○ Enabled								
O Disabled	_							~
	Supported on:	At least Window	ws 2000					Ô
Options:			Help:					*
Items to run at logon	Show		This policy that Windo system. If you enab can run at t this policy a To specify v Contents di executable another nan located in t fully qualifi If you disab have to stan Note: This s User Config system star	setting specifies add ws starts automatica le this policy setting he time the user log applied. yalues for this policy ialog box in the Valu program (.exe) file o me, press ENTER, an he %Systemroot% d ed path to the file. le or do not configu t the appropriate pro- setting appears in th juration folders. If bo ts the programs spe	litional program ally when a use , you can speci s on to this con setting, click S e column, type r document fil d type the nam irectory, you n ure this policy s ograms after lo e Computer Co th settings are cified in the Co	ify which ify which mputer show. In the the na e. To sp ne. Unlik nust sp setting, oggon. onfigur configur configur	locument on to the ch progra that has n the Sho ime of the becify ess the file ess the file the user v ation and gured, the r	s / ms w e e is will

4-10-5: In the Run these programs at user logon window, click Enabled, and then click Show. In the first row of the Show Contents dialog box, type explorer.exe, and in the second row, type notepad.exe (see Figure 4-27). Now all target computers run File Explorer and Notepad when a user logs on. Click OK twice and close the Group Policy Management Editor.

Ņ	Run these programs at user logon						
	S	how Co	ontents				
C		Items to	run at logon				
			Value				
9			explorer.exe				
С			notepad.exe				
		*					
) mt							

4-10-6: Link GPO1 to the TestOU1 OU.



4-10-7: On ServerDM1, sign in as domadmin1 and run gpupdate. Then sign out of ServerDM1, and sign in again as domadmin1. After a few moments, File Explorer and Notepad open. Close File Explorer and Notepad.



🐂 🖸 📑 🖛 File	Explorer
File Home	Share View
$\leftarrow \rightarrow \cdot \uparrow $	> Quick access
- Ouisk accord	✓ Frequent folders (4)
	- Deskton
	Untitled - Notenad
	File Edit Format View Help
Pictures	
	'
This PC	
💣 Network	
4 items	<
) 🥭 🥫	4

4-10-8: On ServerDC1, unlink **GPO1** from **TestOU1** and link it to the domain node. Open GPO1 in the Group Policy Management Editor. Navigate to the **Run these programs at user logon** policy and set it to **Not Configured**.



Run these program	Run these programs at user logon					
Run these program	ns at user logon					
Not Configured	Comment:					
○ Enabled						
 Disabled 						
	Supported on:	At lea				

 4-10-9: Navigate to Computer Configuration, Policies, Administrative Templates, and Windows Components, and click Windows Logon Options. In the right pane, double-click Display information about previous logons during user logon. Read the Help information about this policy setting. Click Enabled, and then click OK.

E Display information about previous logons during user logon – D >								
Display information about previous logons during user logon Previous Setting Next Setting								
O Not Configured	Comment:							
Enabled								
 Disabled 								
	Supported on:	At least Window	vs Vista					
Options:			Help:					
			This policy information user. For local us at least a W setting, a m the date an date and tir user name, successful I acknowledd Microsoft V For domain 2000 native, you enable Windows cu be able to Il setting if th functional I	setting controls whet a about previous logo er accounts and dom indows Server 2008 fn assage appears after d time of the last suc me of the last unsucci and the number of u logon by that user. Th ged by the user befor Vindows desktop. In user accounts in Win , or Windows 2000 m this setting, a warnin ould not retrieve the log on. Therefore, you e domain is not at th evel.	her or not the ins and logon i lain user accou unctional level the user logs of cessful logon at essful logon at nsuccessful lo nis message m e the user is pr ndows Server 2 ixed functiona g message win information ar u should not er e Windows Ser	system of failures t unts in du , if you e on that d by that u ttempted gons sin ust be resented 2003, Wir I level do I appear nd the us nable thi rver 2008	displays to the omains of mable the lisplays user, the d with the with the mains, in that er will n s policy d domain	of iis at ist ot

4-10-10: On ServerDM1, run **gpupdate**, and then sign out and sign in again as **domadmin1**. You see a message stating that it's the first time you have signed in to the account. That's because this is the first time you have signed in since the policy was enabled. Click **OK**.



4-10-11: Sign out of ServerDM1, and then try to sign in again, but with an incorrect password. Then sign in with the correct password. A window opens showing the last successful sign-in and an unsuccessful sign-in attempt (see Figure 4-28). This information is intended to let users know whether somebody has been trying to use their accounts to log on. Click OK.



 4-10-12: Sign out of ServerDM1. On ServerDC1, in Group Policy Management Editor, set the Display information about previous logons during user logon policy to Not Configured. Unlink GP01 from the domain node.



4-10-13: Continue to the next activity.

Activity 4-11: Working with User Administrative Template Settings

Description: In this activity, you explore Administrative Templates settings under User Configuration, and then configure some settings to see the effect they have on a user's environment.

• 4-11-1: On ServerDC1, open **GP01** in the Group Policy Management Editor.

Group Policy Management Editor



 4-11-2: Under User Configuration, click to expand Policies and Administrative Templates. Browse through the folders under Administrative Templates to see the settings and subfolders under each one. Take your time to get a good feel for the types of settings available in each main folder.

 Viser Configuration Policies Software Settings Windows Settings Administrative Templates: Control Panel Control Panel Desktop Active Directory Desktop Network Network Offline Files Windows Connectic Shared Folders Start Menu and Taskba System Windows Components 	 Folder Kedirection Group Policy Internet Communication Management Locale Services Logon Mitigation Options Power Management Removable Storage Access Scripts User Profiles Download missing COM components Century interpretation for Year 2000 Restrict these programs from being launched from Help Do not display the Getting Started welcome screen at logon Custom User Interface Prevent access to the command prompt Prevent access to registry editing tools 	Not confi Not confi Not confi Not confi Not confi Not confi Not confi
> C System > Windows Components	Prevent access to the command prompt Prevent access to registry editing tools	Not confi Not confi
All Settings Preferences	 Don't run specified Windows applications Run only specified Windows applications 	Not confi

• 4-11-3: In the left pane, click to expand the **System** folder, and then click to select the **System** folder. In the right pane, double-click **Prevent access to the command prompt**.

Prevent access to t	he command pro	mpt				đ	×
Prevent access to	the command pro	ompt	Previous Se	etting Next Setting			
Not Configured	Comment:						Т
O Enabled							
O Disabled	c						
	Supported on:	At least Windows 2	2000				
Options:				Help:			
Disable the command	l prompt script pro	ocessing also? Ye	es 🗸 🗸	This policy setting prevents users from running the interactive command promp policy setting also determines whether batch files (.cmd and .bat) can run on the	t, Cmd.e compu	exe. This iter.	
				If you enable this policy setting and the user tries to open a command window, a message explaining that a setting prevents the action.	he syste	m displa	ys
				If you disable this policy setting or do not configure it, users can run Cmd.exe ar normally.	d batch	files	
				Note: Do not prevent the computer from running batch files if the computer use startup, or shutdown batch file scripts, or for users that use Remote Desktop Sen	s logon, /ices.	logoff,	
1							

• 4-11-4: Read the policy help information. Click **Enabled**, and then click OK. Close the Group Policy Management Editor.

💭 Prevent access to the command prompt	
Prevent access to the command prompt Previous Se	tting Next Setting
O Not Configured Comment:	
Enabled	
O Disabled	
Supported on: At least Windows 2000	
Options:	Help:
Disable the command prompt script processing also? No ~	This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determines whether batch files (.cmd and .bat) can run on the computer.
	If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.
	If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally.
	Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop Services.

• 4-11-5: In Group Policy Management, link **GP01** to **TestOU1**.

Те	stO	U1				
Li	Linked Group Policy Objects		Group Policy Inheritance	Delegation		
		Link Order	GPO	Enforced	Link Enabled	GPO Status
	\cong	1	🛒 GPO1	No	Yes	Enabled

 4-11-6: On ServerDM1, sign in as domadmin1. Right-click Start and click Command Prompt. A command prompt window opens, but you see a message stating that the administrator has disabled it. Press any key to close the command prompt window.





4-11-7: On ServerDC1, unlink GP01 from TestOU1.



4-11-8: Sign off ServerDM1. Continue to the next activity.

Change account settings
Lock
Sign out

Activity 4-12: Viewing Settings with Filter Options

Description: In this activity, you want to configure the setting that displays the desktop instead of the Start screen when users sign in to Windows 8 computers. You can't remember the exact setting name, but you know it's in the User Configuration node of a GPO. You configure a filter to narrow down the search. (You don't actually configure the policy; you only use the filter option to find the policy.)

4-12-1: On ServerDC1, open GP01 in the Group Policy Management Editor.



4-12-2: Under User Configuration, click to expand **Policies**, and click **Windows Settings.** Notice that there's no Filter icon on the toolbar because you can't filter settings in Windows Settings. Click **Administrative Templates.** You see the Filter icon now.



Þ 🔿 📶 🗟 🛛 🖬 🔻
GPO1 [SERVERDC1.MCSA2016.LOCAL
🗸 👰 Computer Configuration
> 🧮 Policies
> 📔 Preferences
🗸 💰 User Configuration
🗸 🚞 Policies
> 📔 Software Settings
🗸 📔 Windows Settings
Scripts (Logon/Logoff)
> 🚡 Security Settings
> 📄 Folder Redirection
> 🎳 Policy-based QoS
> 譨 Deployed Printers
> 📔 Administrative Templates:
- 🦰 D

4-12-3: Click Action, Filter Options. In the Filter Options window, click the Enable Keyword Filters check box. You remember that the policy setting title has the word "desktop" in it, so type desktop in the Filter for words(s) text box. If necessary, click Any in the list box next to the Filter for words(s) text box.

Filter Options 2						
Select options b will be applied to	Select options below to enable and change or disable types of global filters that will be applied to the Administrative Templates nodes.					
Select the type of policy s	ettings to disp	blay.				
Managed:		Configured:		Comme	nted:	
Yes	~	Any	~	Any	~	
Enable Keyword Filters	5					
Filter for word(s):	desktop				Any	~
Within:	Policy Set	tting Title	Help Text		Comment	
Enable Requirements F	Filters					

•

4-12-4: Click the **Policy Setting Title** check box, and if necessary, click to clear the **Help Text** and **Comment** check boxes. Click **OK**. You see a filter icon on the Administrative Templates folder.

Enable Keyword Filters				
Filter for word(s):	desktop		Any	\sim
Within:	Policy Setting Title	Help Text	Commen	t
Enable Requirements Fi	ilters			
Select the desired platfo	orm and application filter(s):		
Include settings that ma	atch any of the selected	platforms.	∼ Sele	ect All
BITS 1.5 BITS 2.0 BITS 3.5 BITS 4.0 Internet Explore Internet Explore Internet Explore 	r 10 r 11 r 3 r 4		 Cle V 	ar All
-			ок	Cancel
> 📑	Admini	strative	e Tem	plates:

4-12-5: Under User Configuration, click to expand **Administrative Templates**, and click **All Settings.** You see a list of policy settings with the word *desktop* in the title. That's still quite a few settings to sift through.

GPO1 [SERVERDC1.MCSA2016.LOCAL] P	Setting	State	^
Computer Configuration	E Allow installation of desktop items	Not configured	
> Policies	E Allow installation of desktop items	Not configured	
> Preferences	E Allow installation of desktop items	Not configured	
Policies	Allow installation of desktop items	Not configured	
Software Settings	Allow installation of desktop items	Not configured	
> Windows Settings	E Allow installation of desktop items	Not configured	
🗸 📑 Administrative Templates: Po	Allow installation of desktop items	Not configured	
> 🕞 Control Panel	E Allow installation of desktop items	Not configured	
> 嬦 Desktop	Allow installation of desktop items	Not configured	
> 📑 Start Menu and Taskbar	E Allow installation of desktop items	Not configured	
> 📑 Windows Components	E Always show desktop on connection	Not configured	
🖺 All Settings	Block launching desktop apps associated with a file.	Not configured	
> 📔 Preferences	🗄 Block launching desktop apps associated with a URI scheme	Not configured	
	🖹 Desktop Wallpaper	Not configured	
	🗄 Disable Active Desktop	Not configured	
	Enable Active Desktop	Not configured	
	Go to the desktop instead of Start when signing in	Not configured	
	Hide and disable all items on the desktop	Not configured	
	🗄 Hide Internet Explorer icon on desktop	Not configured	
	Hide Network Locations icon on desktop	Not configured	
	E List desktop apps first in the Apps view	Not configured	*

• **4-12-6:** Click **Action, Filter Options.** You remember that the word "start" was also in the title. In the Filter for words(s) text box, type the word *start* next to

"desktop," making sure to leave a space between them. In the list box, click **All** so that the filter shows only policy settings with both words in them. Click **OK**.

Enable Keyword Filters						
Filter for word(s):	desktop start		All	\sim		
Within:	Policy Setting Title	Help Text	Comment			

4-12-7: Now you see only one policy setting, and it's the one you are looking for. Click the filter icon on the tool bar to remove the filter. You see all settings again. Close the Group Policy Management Editor.



4-12-8: Continue to the next activity.

Activity 4-13: Configuring and Testing Preferences

Description: In this activity, you configure a number of Group Policy preferences. You create a file preference, deploy a VPN connection, and configure local groups. • 4-13-1: To create a file preference in which a folder with files is distributed to all computers, first you create a share for the files to be copied in a preference. On ServerDC1, open File Explorer.



• 4-13-2: Create a folder named **PandP** on the C: volume. Share this folder and give the **Everyone** group **Read** permission.

Permissions for PandP		>
Share Permissions		
Group or user names:		
	Add	Remove
Permissions for Everyone	Allow	Deny
Full Control		
Read	\leq	

 4-13-3: In the PandP folder, create two text files: Name the first file Policy.txt and the second one Procedure.txt. Close File Explorer.

<mark>,</mark> → Th	is PC → Local Disk (C:) → PandP	~ (✓ O Search PandP		
	Name	Date modified	Туре	Size	
	Policy	3/24/2021 9:29 AM	Text Document	0 KB	
*	Procedure	3/24/2021 9:29 AM	Text Document	0 KB	

4-13-4: Open the Group Policy Management console, if necessary. Create a GPO named **Prefs** in the Group Policy Objects folder and open it in the Group Policy Management Editor.



 4-13-5: Under User Configuration, click to expand Preferences and Windows Settings. Right-click Files, point to New, and click File.

Prefs [SERVERDC1.MCSA2016.]	OCAL1 Poli	
 Ecomputer Configuration Deliving 	New File Properties	×
 Policies Preferences User Configuration Policies Preferences Prefere	General Common Action: Update Source file(s): Destination File: Suppress errors on individual file actions Attributes Read-only Hidden	×
Kegistry If Shortcuts Control Panel Setting	Archive	
<	OK Cancel Apply H	Help

• 4-13-6: In the Action list box, click **Create**.

New File	Properties		×
General	Common		
P	Action:	Create	~
Source f	file(s): tion File:	Suppress errors on individual file actions Attributes Read-only Hidden Archive]

4-13-7: In the Source file(s) text box, type \\ServerDC1\PandP*.*. Using a wildcard copies all files in the PandP folder. In the Destination folder text box, type %UserProfile%\Documents\PandP. The PandP folder is created automatically when the policy is applied. Leave the default Archive attribute selected (see Figure 4-35)

New File Properties					
General	Common				
F	Action:	Create	~		
Source file(s): Destination folder:		\\ServerDC1\PandP*.* %UserProfile%\Documents\PandP Suppress errors on individual file actions			
		☐ Read-only ☐ Hidden ☑ Archive			

 4-13-8: Click the Common tab. Review the available options, and then click OK. Note that you can change the processing order of preferences, so if you need one preference to be processed before another, you can arrange them in the order you want. Close the Group Policy Management Editor.



4-13-9: In the Group Policy Management console, link the **Prefs** GPO to the domain object.



4-13-10: Sign in to ServerDM1 as domadmin1. Open File Explorer, and in the left pane, click Documents under This PC. Double-click the PandP folder, and you should see the two files you created. Sign out of ServerDM1.



4-13-11: Next, you'll create a Control Panel preference in which you deploy a VPN connection. On ServerDC1, open the Prefs GPO in the Group Policy Management Editor. Under Computer Configuration, click to expand Preferences and Control Panel Settings. Right-click Network Options, point to New, and click VPN Connection.



 4-13-12: In the Action drop-down list, leave the default setting Update. Click the All users connection option button so that all users logging on to target computers have access to the connection. In the Connection name text box, type **WorkVPN**. In the IP Address text box, type **192.168.0.1** (see Figure 4-36).

New VPN Propertie	s					
VPN Connection O	ptions	Security	Netwo	rking	Common	1
Log Action:	Upda	ite				~
OUser connection	tion					
Connection name:	Work	kvpn				
IP Address:	:	192 .	168		0.	. 1
	Us	e DNS na	me		Us	e IPv6
First connect						
Dial another co	nnection	n first:				

 4-13-13: Click the Options tab and review the available settings. Click the Security tab, which is where you set authentication options. Leave the settings at their defaults.

New VPN Properties



New VPN Properties

VPN Connection Options Security Networking Common Typical (recommended settings) Require secured password Require data encryption (disconnect if none)						
O Advanced (c	stom settings)					
Data encryp	on: Required	\sim				
Logon sec	ity					
Use E	tensible Authentication Protocol (EAP)					
🔾 Use t	ese other protocols:					
U	Unencrypted password (PAP)					
Shiva Password Authentication Protocol (SPAP)						
Challenge Handshake Authentication Protocol (CHAP)						
Microsoft CHAP (MS-CHAP)						
Older MS-CHAP version for Windows 95 servers						
Microsoft CHAP Version 2 (MS-CHAP v2)						

 4-13-14: Click the Networking tab where you can choose the VPN tunnel type. Leave the default setting Automatic.



• 4-13-15: Click the Common tab and click Remove this item when it is no longer applied. In the warning message stating that the preference will be set to Replace mode, click OK. Click OK again.

New VPN Prop	perties				
VPN Connectio	on Options	Security	Networking	Common	
Options co	mmon to all it	ems			
Stop p	rocessing iter	ns in this e	xtension if an	error occur	s.
🗹 Run in	logged-on us	er's securi	ty context (us	ser policy op	tion).
Remov	e this item w	hen it is no	longer applie	d.	
Apply	Preference	s - Mode	Change War	ning	×
Description This will cause a change to 'Replace' mode.					
		(Ж	Cancel	

 4-13-16: Link the Prefs GPO to the TestOU1 OU. Sign in to ServerDM1 as domadmin1. Because it's a Computer Configuration policy, you have to restart the computer or run gpupdate for it to be applied. Open a command prompt window, and then type gpupdate and press Enter.

TestO	001				
Linked	Group Policy Objects	Group Policy Inheritance	Delegation		
	Link Order	GPO	Enforced	Link Enabled	GPO Status
\geq	1	🛒 Prefs	No	Yes	Enabled

4-13-17: Right-click **Start** and click **Network Connections**. You see the WorkVPN connection.



4-13-18: Because you selected the *Remove this item when it is no longer applied* option, you should test that functionality. On ServerDC1, unlink **Prefs** from the domain. On ServerDM1, run **gpupdate** again.



• **4-13-19:** Look in the Network Connections window to verify that the VPN connection has been removed. Sign out of ServerDM1.



4-13-20: Next, you'll create a preference that configures local groups on member computers. On ServerDC1, open Active Directory Users and Computers. Click the **Users** folder, and then create a global security group named **Local_Admins** in this folder. Add **domuser1** to this group.

Local_Admins Properties

General	Members	Member Of Managed By	
Membe	rs:		_
Name		Active Directory Domain Services Folder	
👗 do	muser1	MCSA2016.local/Users	1

 4-13-21: Open the Group Policy Management console, and open the Prefs GPO in the Group Policy Management Editor. Delete the Network Options preference under the Computer Configuration\Control Panel Settings.

?

×



4-13-22: Next, right-click Local Users and Groups, point to New, and click Local Group.

New Local Group Properties

Local Group Commo	n			
Action:	Update			~
Group name:				~
Rename to:				
Description:				
			Delete all	member users member groups
Members:				
Name			Action	SID
		Add	Remove	Change

• 4-13-23: Make sure Update is the selected action. Click the **Group name** list arrow, and click **Administrators** (built-in) in the list.

>

New Local Group Pr	operties	>
Local Group Commo	n	
Action:	Update	~
Group name:	Administrators (built-in)	~
Rename to:		
Description:		

 4-13-24: Click the Add button, and then click the browse button next to the Name text box. In the Select User, Computer, or Group dialog box, type Local_Admins, click Check Names, and then click OK. Make sure the action is Add to this group, and then click OK twice. Close Group Policy Management Editor. New Local Group Properties

Local Group Common	
Action: Update	~
Group name: Administrators (built-in)	×
Local Group Member	×
Member	
Name: MCSA2016\Local_Admins	
Action: Add to this group	~
ОК	Cancel

4-13-25: Link the Prefs GPO to the TestOU1 OU.

TestO	0U1				
Linked	Group Policy Objects	Group Policy Inheritance	Delegation		
	Link Order	GPO	Enforced	Link Enabled	GPO Status
\cong	1	🛒 Prefs	No	Yes	Enabled

4-13-26: Sign in to the domain from ServerDM1 as domadmin1. Open a command prompt window, type gpupdate, and press Enter. Close the command prompt window.



 4-13-27: Right-click Start and click Computer Management. Click to expand Local Users and Groups, click Groups, and then double-click Administrators to open the Properties dialog box. You should see Local_Admins in the Members text box. Click **OK**. Now any domain user you add to the Local_Admins group has local administrator access to all computers in the scope of the Prefs GPO. Sign out of ServerDM1.

Administrators Prop	erties	?	×
General			
Administr	ators		
Description:			
Members:			
Moministrator Reference Momental Mathematica	omain Admins ocal_Admins		

4-13-28: On ServerDC1, unlink the **Prefs** GPO from the **TestOU1** OU. Continue to the next activity.



Activity 4-14: Configuring item-level Targeting

Description: h this activity, you configure item-level targeting for the file preference so that you can still have the policy linked to the domain, and other preferences affect all users.

4-14-1: On ServerDC1, open the Prefs GPO in the Group Policy Management Editor. Under User Configuration, expand **Preferences** and **Windows Settings**, and then click **Files**.



4-14-2: Double-click the **PandP** file preference in the right pane. In the Properties dialog box, click the **Common** tab.



• 4-14-3: Click the Item-level targeting check box, and then click the Targeting button.

			\times
New Item - Add Collection Item Options - 🍝 🗢 🐰 🗈 🛍 - 🗙 Delete	🕜 Hel	р	
Select the "New Item" button to create a new targeting item			
,	or	6	
	UK	Cano	el

• 4-14-4: In the Targeting Editor window, click New Item, and then click Organizational Unit.

Group Policy Management	ditor	
File Action View Help	Battery Present	
	Computer Name	
	CPU Speed	
Prefs [SERVE Targeting	🖁 🛛 Date Match	
Compute Dolici New Item -	Disk Space	A - X B R - X Delete
> Prefe	Domain	
🗸 🕵 User Con	Environment Variable	outton to create a new targeting item
> 📔 Polici	File Match	
V 🎽 Prefe	IP Address Range	
× • •	Sanguage	
	A LDAP Query	
	MAC Address Range	
<u> 4</u>	MSI Query	
	Network Connection	
	Operating System	
	Organizational Unit	
> 🐼 C 🔤	S PCMCIA Present	
	Portable Computer	
	Processing Mode	
	A	

4-14-5: In the Organizational Unit text box, click the browse button, click
 TestOU1, and then click OK. Click OK twice to get back to the Group Policy
 Management Editor. This will limit the preference to only users in the TestOU1 organization unit, which in this case is only domadmin1.

📡 Find Custom Sea	rch		_	
In: 📃 Entire Direct	ory		~	Browse
Custom Search Adv	vanced			
Field	Condition:	Value:		Find Now Stop
				Clear All
Condition List:		Add	Remove	
<add above="" criteria="" from="" list="" this="" to=""></add>				9 7
<			>	OK
Search results:				
Name	Туре		Description	
TestOU1	Organizational Unit			
道 Domain Control	Organizational Unit		Default contair	ner for domain contr

• 4-14-6: Close Group Policy Management Editor. Link the **Prefs** GPO to the domain.

MCSA0016 Joopl	
INC SA20 16.10Cal	
Select GPO Look in this domain: MCSA2016.local Group Policy objects: Name Default Domain Controllers Policy Default Domain Policy FolderRedir GPO1 Prefs PrintConfigGPO Scripts TestGPO	~
Scripts TestGPO	Cancel
	Select GPO Look in this domain: MCSA2016.local Group Policy objects: Name Default Domain Controllers Policy Default Domain Policy FolderRedir GPO1 Prefs PrintConfigGPO Scripts TestGPO OK

4-14-7: Sign in to ServerDM1 as domadmin1. Open File Explorer, click
 Documents in the left pane, and delete the PandP folder. Sign out of ServerDM1.



•

4-14-8: Sign in again to ServerDM1 as **domadmin1** and verify that the PandP folder and the two files were created again.



4-14-9: Sign out of ServerDM1, and sign in as **domuser1**, (This user account is in the Users folder in Active Directory.) Open File Explorer, and in the left pane, click **Documents** under This PC. You don't see the PandP folder because item-level targeting limited this preference to user accounts in TestOU1. Sign out of ServerDM1.

	6	• @ @		ថ្មី ServerDM1		
Do	cumen	ts				
	Share	View				
	> Th	is PC → Docum	nents	✓ Ö Search Docume		
		Name	^	Date modified Type		
s				This folder is empty		
_	*			This folder is empty.		
s	7					
.s	*					

• 4-14-10: On ServerDC1, unlink the **Prefs** GPO from the domain.

MCSA	2016.local						
Status	Linked Group Policy O)bjects	Group Policy Inheritance		De		
	Link Order	GPO		Enforc	ed		
≳	1	🗊 Default Domain Policy		No			
	2	🗊 Prefs		No			
~	Group Policy Management						
ኞ	Do you want to delete this link? This will not delete the GPO itself.						
		ОК	Cancel				