3/17/2021

Hands On Exercise

Chapter 4

Configuring Group Policies

(Part 2)

El Adel, Taoufik
IT 416 - SPRING 2021 - OLD DOMINION UNIVERSITY

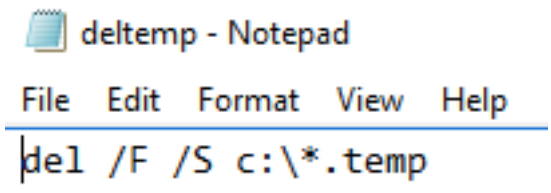
Table 4-1 Activity requirements

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	

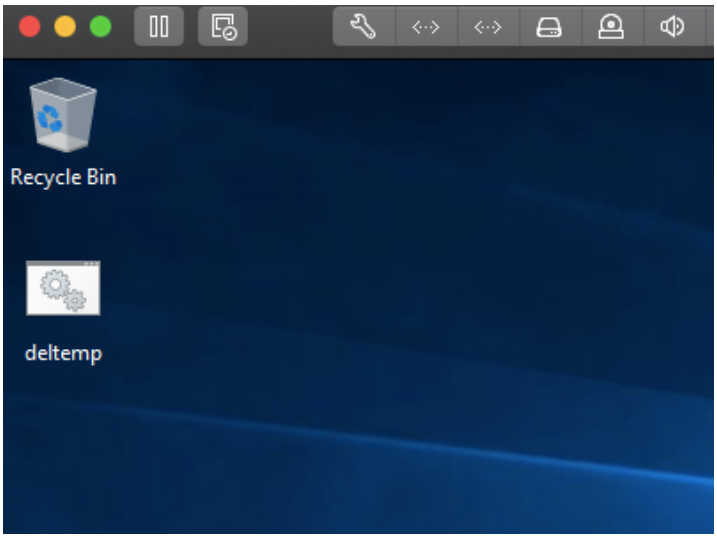
Activity 4-7: Deploying a Shutdown Script to a Computer

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

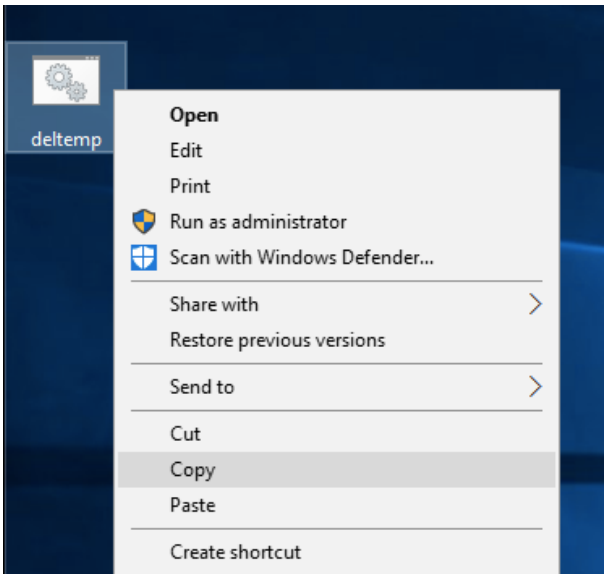
- **4-7-1:** On ServerDC1, start Notepad and type del / FIS c:*.temp. The /F option forces the deletion of read-only files, and the /s option deletes the file in the current directory and all subdirectories.



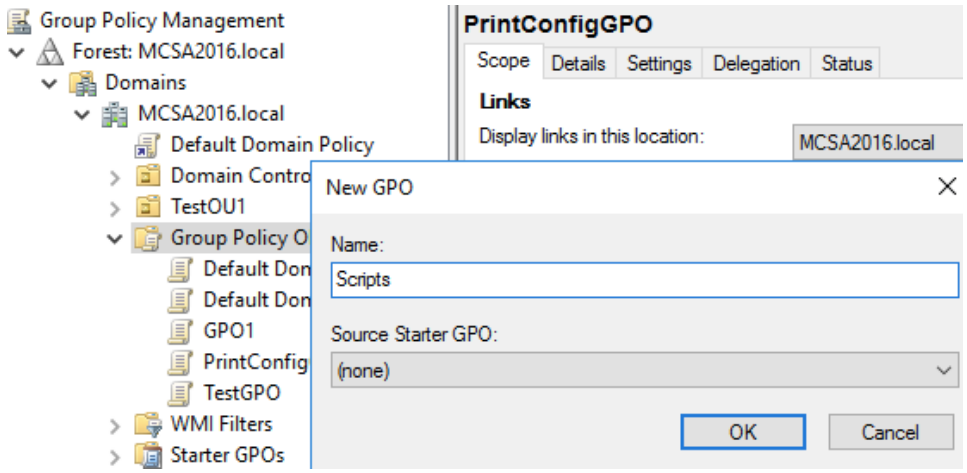
- **4-7-2:** Click File, Save As from the menu. Choose the desktop as the location for saving your file. In the Save as type list box, click All Files (*.*). Type deltemp.bat in the File name text box and click **Save**. Exit Notepad.



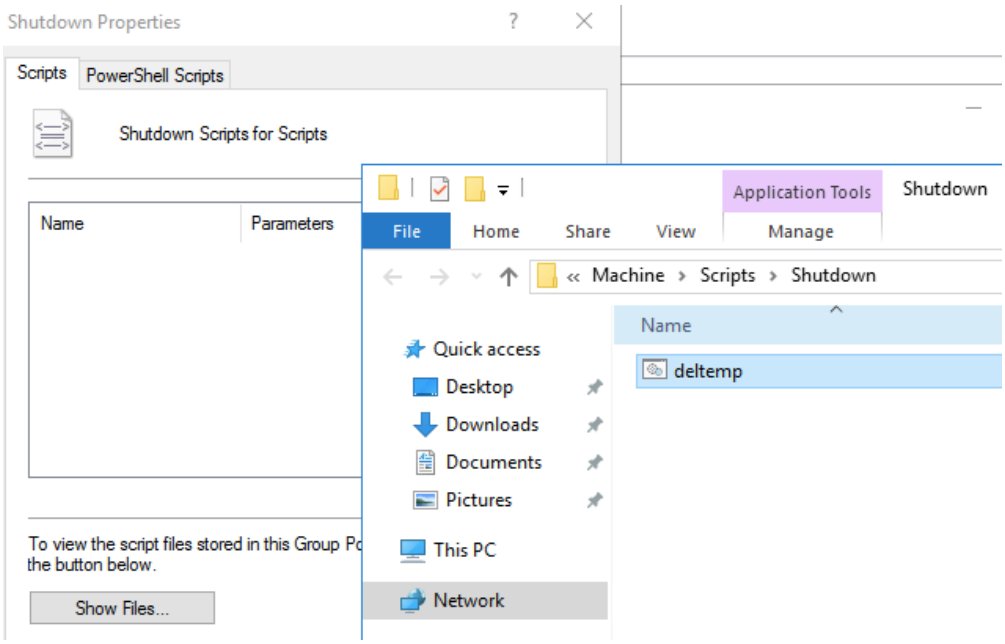
- **4-7-3:** Right-click **deltemp.bat** on your desktop and click **Copy.** (You paste the script into the SYSVOL share in a later step.)



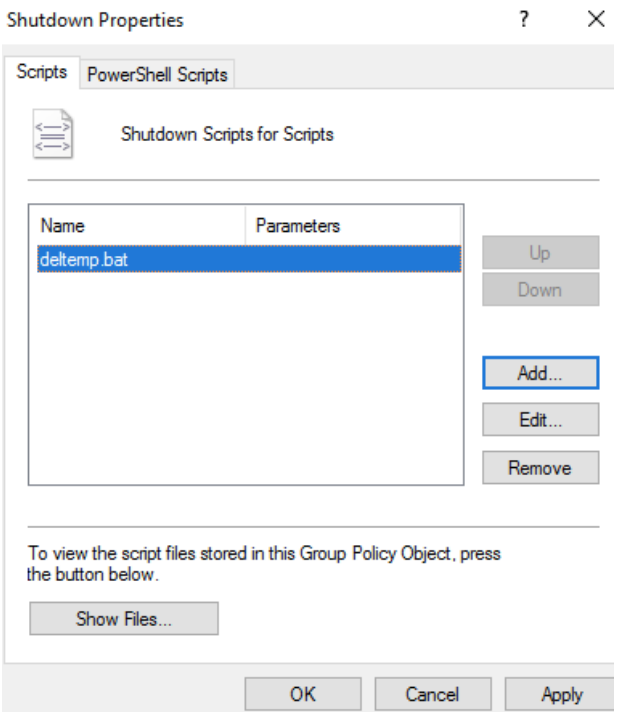
- **4-7-4:** Open the Group Policy Management console. Click the **Group Policy Objects** folder and create a GPO named **Scripts.**



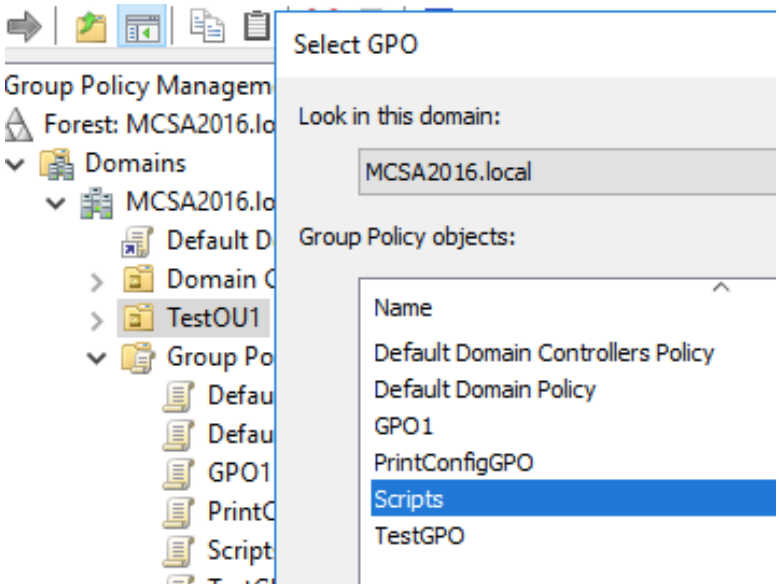
- 4-7-5: Right-click the **Scripts** GPO and click **Edit.** In the Group Policy Management Editor, click to expand **Computer Configuration, Policies,** and **Windows Settings,** and then click **Scripts (Startup/Shutdown).** Right-click **Shutdown** in the right pane and click **Properties.** In the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



- 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.

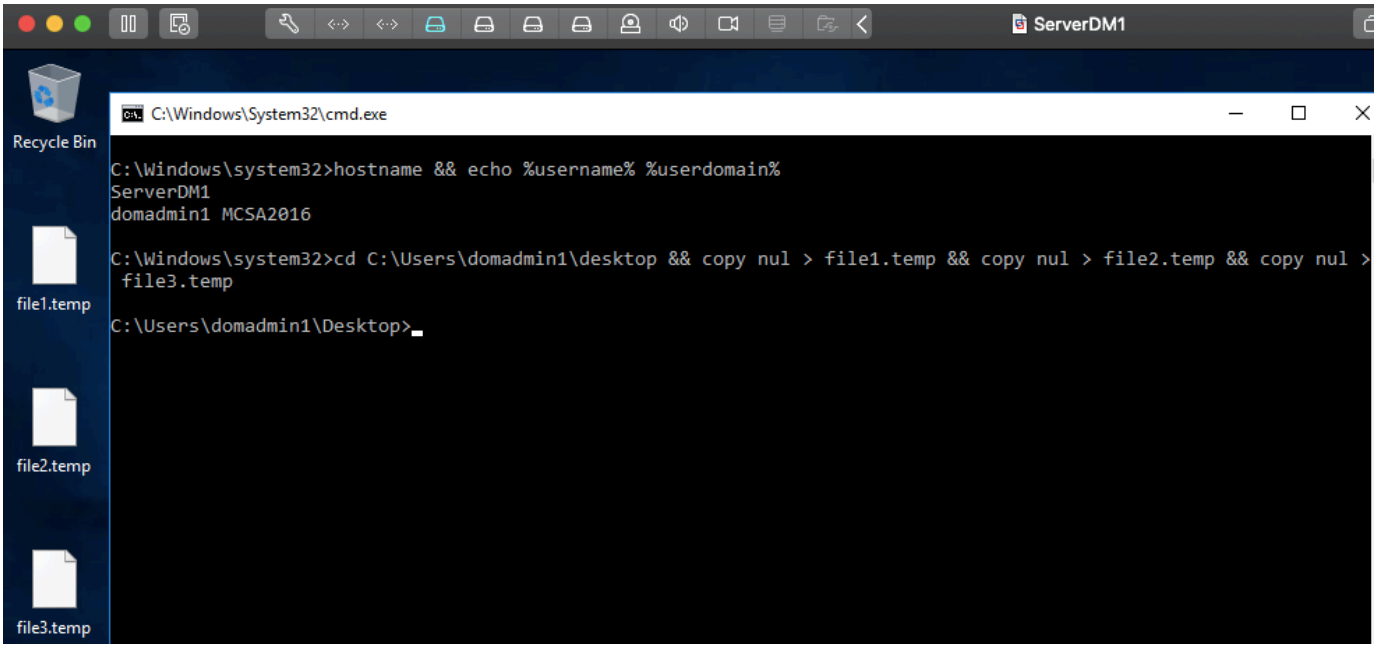


- **4-7-7:** Close the Group Policy Management Editor. Link **Scripts** to the **TestOU1** OU, which is where you moved the ServerDM1 account to earlier.

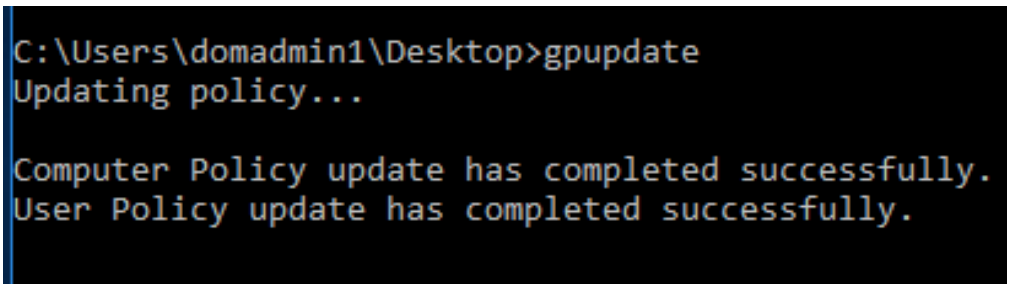


- **4-7-8:** Sign in to ServerDM1 as **domadmin1.** You're going to create a few files on your desktop that have the .temp extension. Open a command prompt window, then type **cd desktop,** and press **Enter.** Type **copy nul > file1.temp** and press **Enter** to create an empty file. Repeat the command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

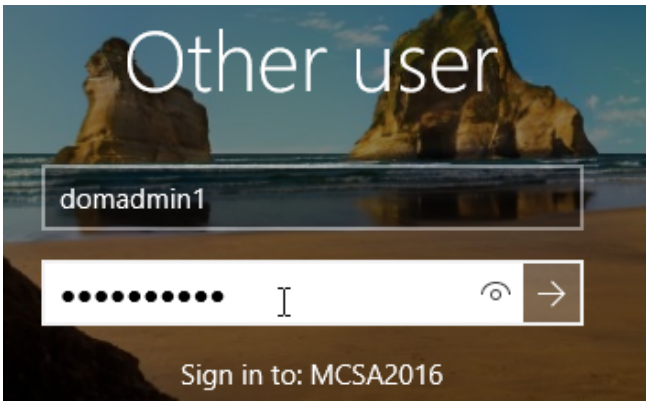
file1 to **file2** and then **file3.** You see the files on your desktop (you may have to minimize Server Manager and the command prompt to see the files).

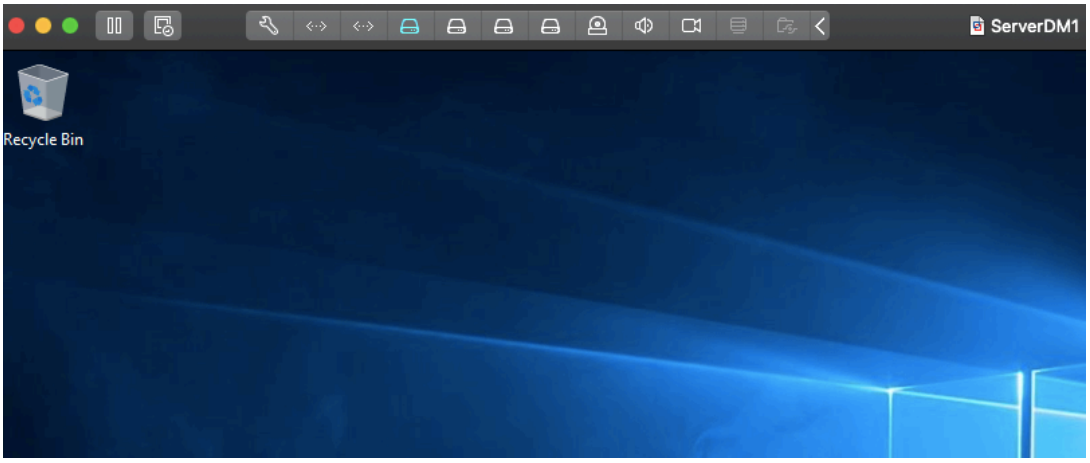


- 4-7-9: Type **gpupdate** and press **Enter.** After gpupdate is finished, restart ServerDM1. (If you don't run gpupdate, you have to restart the computer to load the policy and then shut it down again to make the shutdown script run.) The shutdown process will probably take a little longer than usual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

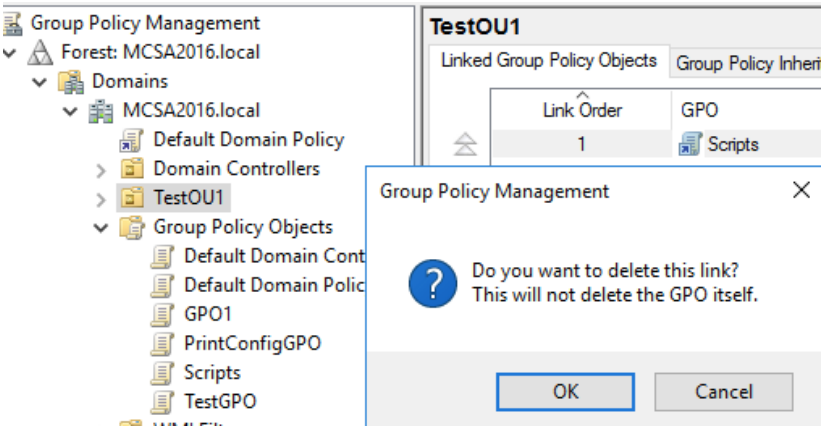


- 4-7-10: Sign in to ServerDM1 as **domadmin1** again and verify that the .temp files have been deleted. Sign out of ServerDM1.





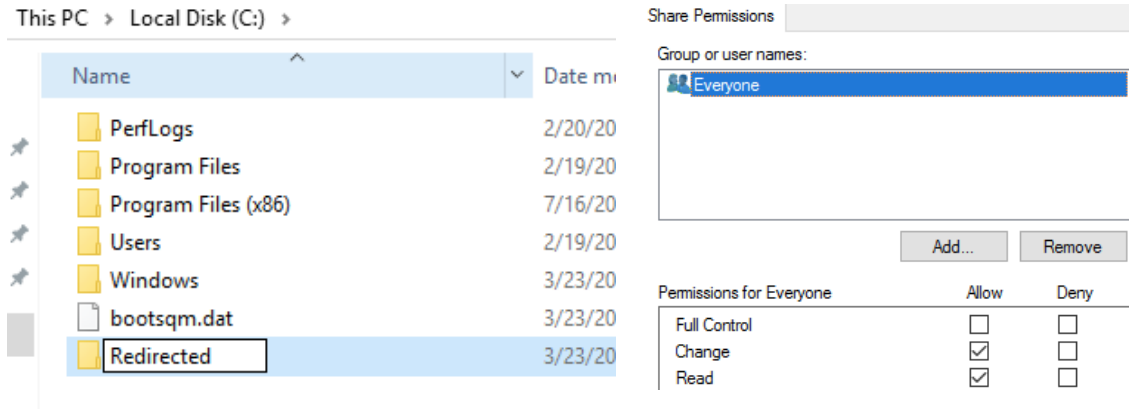
- 4-7-11: On ServerDC1, unlink the **Scripts** GPO from the **TestOU1** OU. Continue to the next activity.



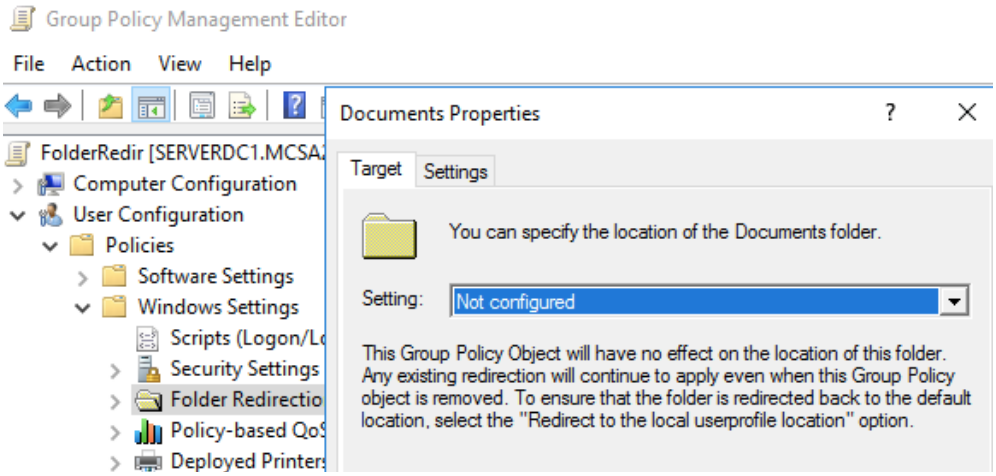
Activity 4-8: Configuring a Folder Redirection Policy

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.

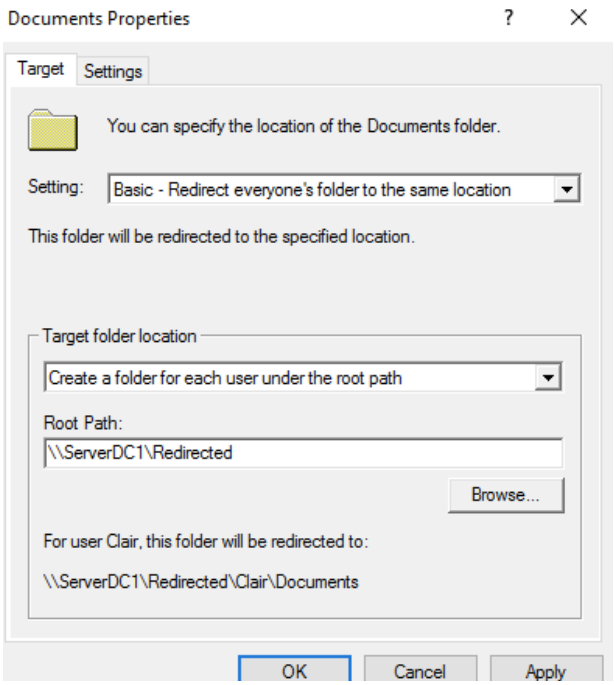


- 4-8-2: Open the Group Policy Management console and create a GPO named **FolderRedir** in the Group Policy Objects folder. Open **FolderRedir** in the Group Policy Management Editor. Expand **User Configuration, Policies, Windows Settings,** and **Folder Redirection.** Right-click the **Documents**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

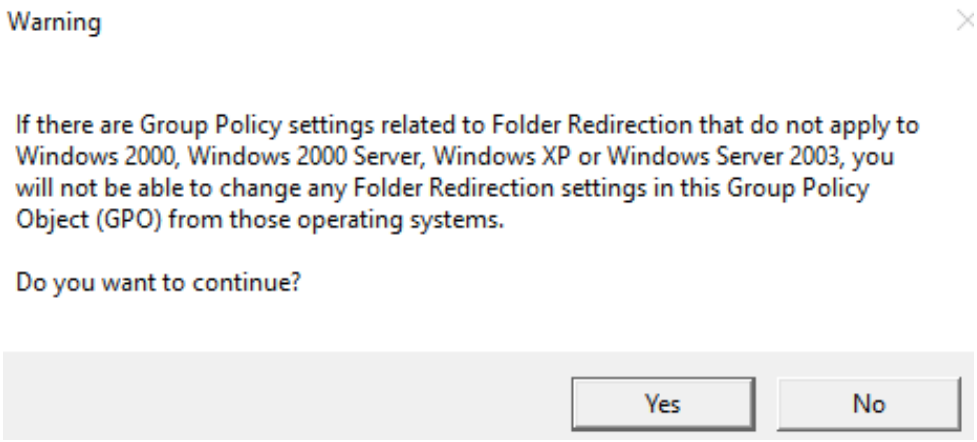


- 4-8-3: In the Documents Properties dialog box, click **Basic - Redirect everyone's folder to the same location** in the Setting drop-down list. Click the **Target folder**

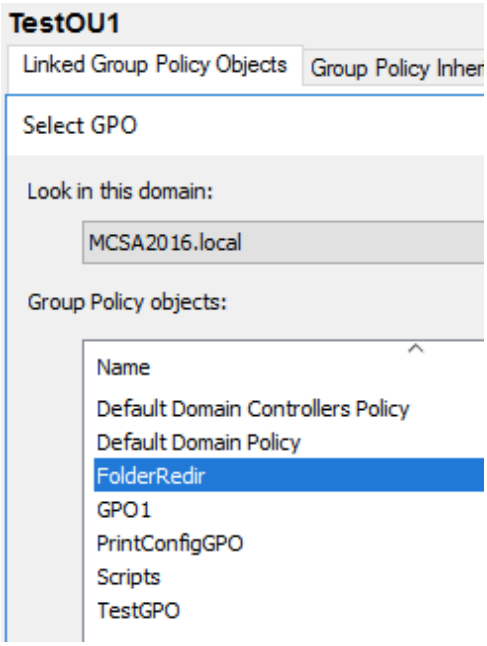
location list arrow to view the available options, and then, if necessary, click **Create a folder for each user under the root path** in the list. In the Root Path text box, type **\\ServerDC1\Redirected.**



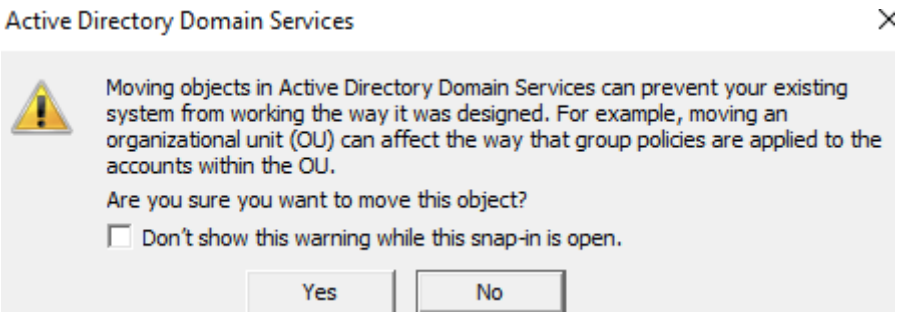
- **4-8-4:** Click the **Settings** tab and review the available options. Click to clear the **Grant the user exclusive rights to Documents** check box. Click **Redirect the folder back to the local userprofile location when policy is removed,** click **OK,** and in the warning message box, click **Yes.**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



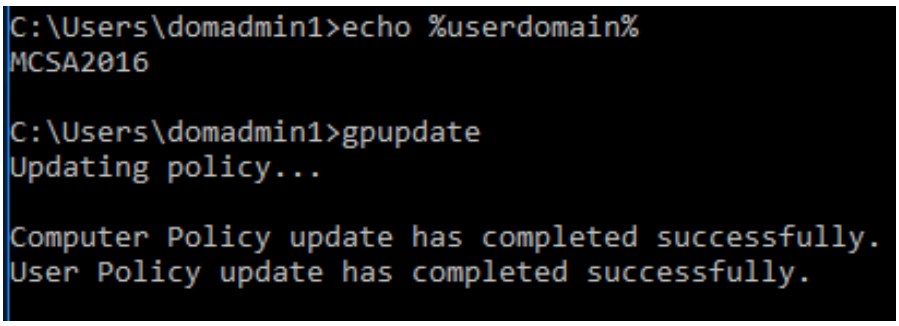
- **4-8-5:** In the Group Policy Management console, link the **FolderRedir** GPO to **Test0U1.**



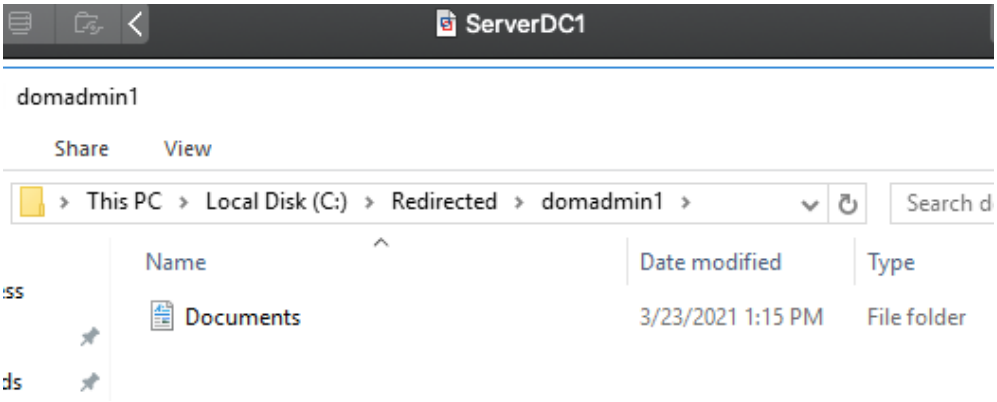
- **4-8-6:** Open Active Directory Users and Computers and move the user **domadmin1** (located in the Users folder) to TestOU1 by dragging and dropping the user account.



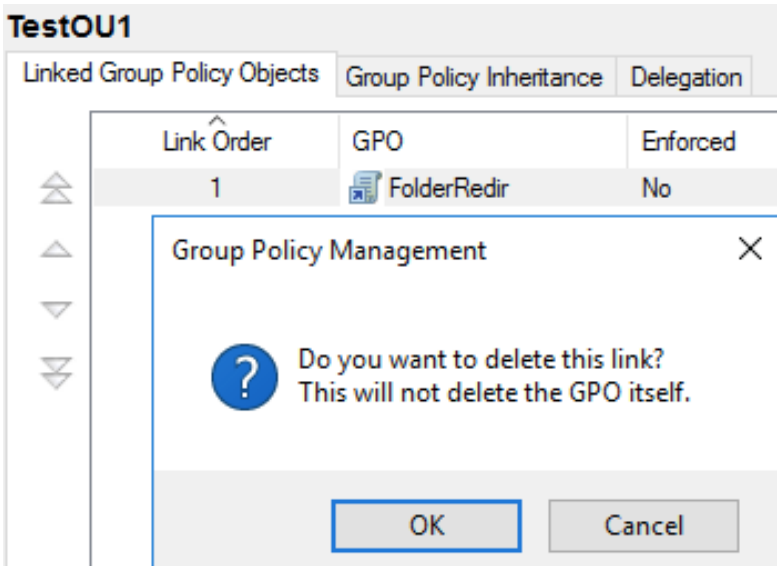
- **4-8-7:** On ServerDM1, sign in as **domadmin1** and run **gpupdate** from a command prompt. Then sign out of ServerDM1 and sign in again as **domadmin1.** You might see a message indicating that folder redirection is occurring.



- **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.



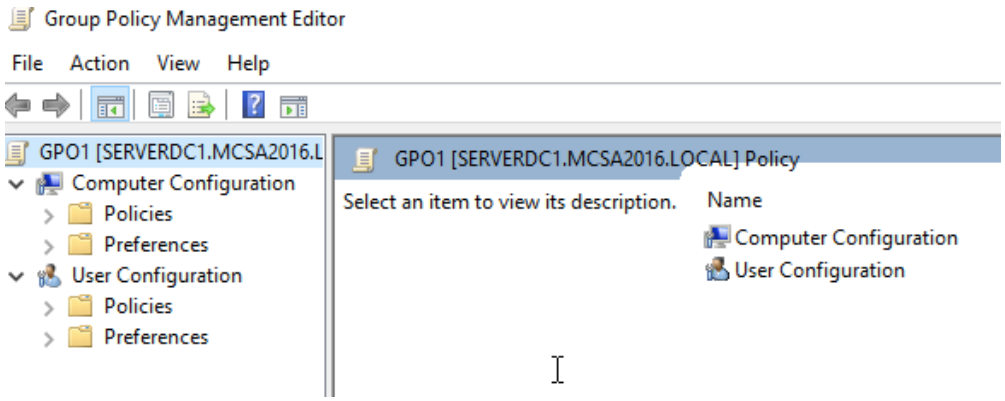
- **4-8-9:** Unlink the **FolderRedir** GPO from **Test0U1.** Continue to the next activity.



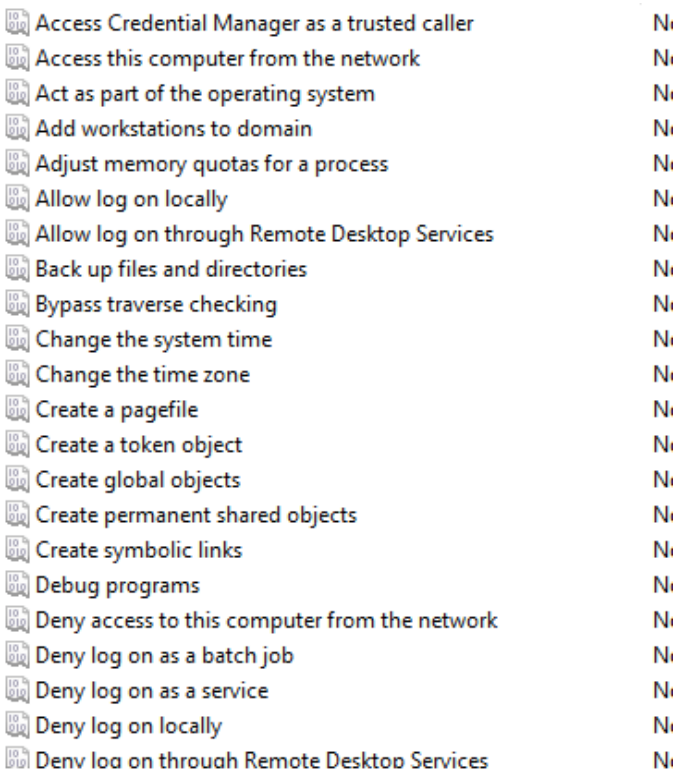
Activity 4-9: Reviewing User Rights Assignment and Security Options Settings

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

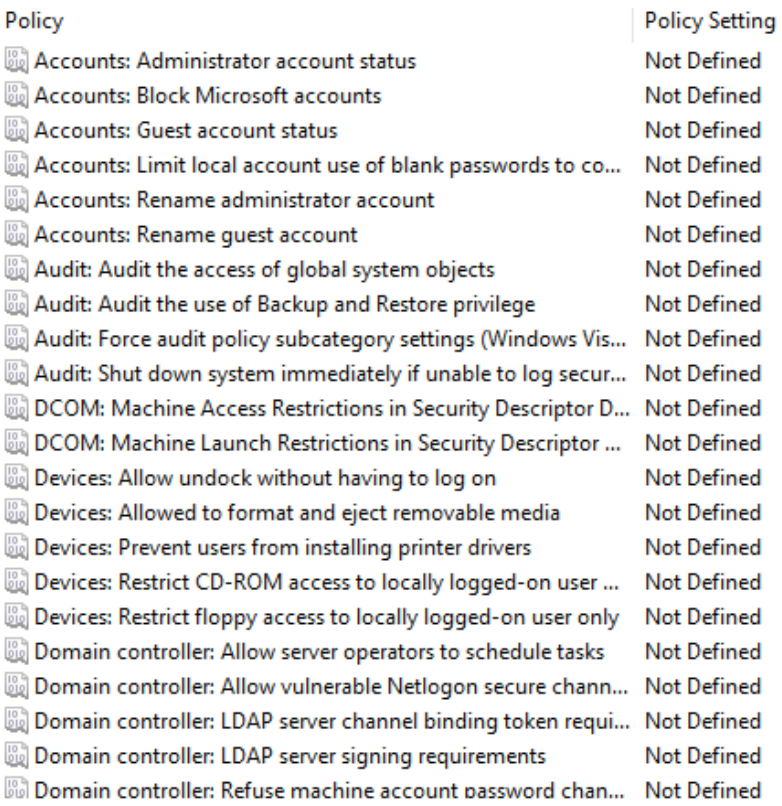
- **4-9-1:** On ServerDC1, open the Group Policy Management console, and then open **GP01** in the Group Policy Management Editor.



- **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.



- **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.



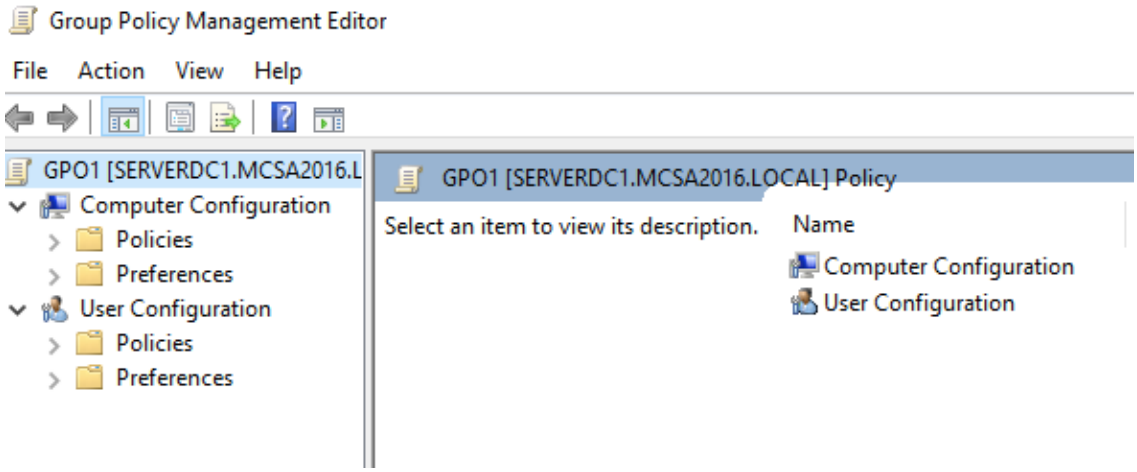
Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to co...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename 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.

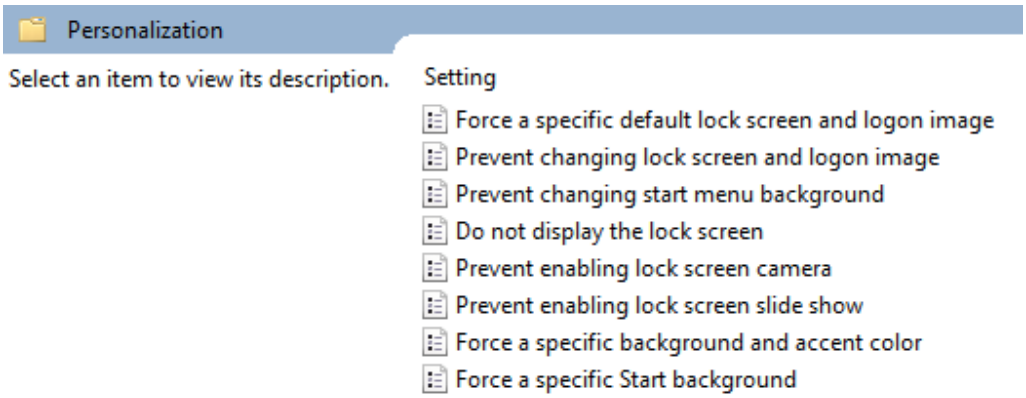
Activity 4-10: Working with Computer Administrative Template Settings

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.

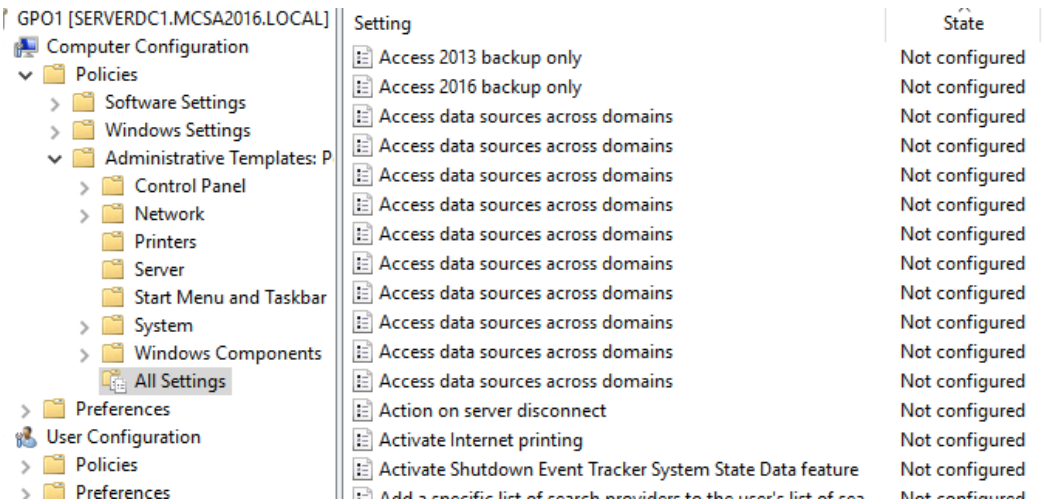
- **4-10-1:** On ServerDC1, open **GP01** in the Group Policy Management Editor.



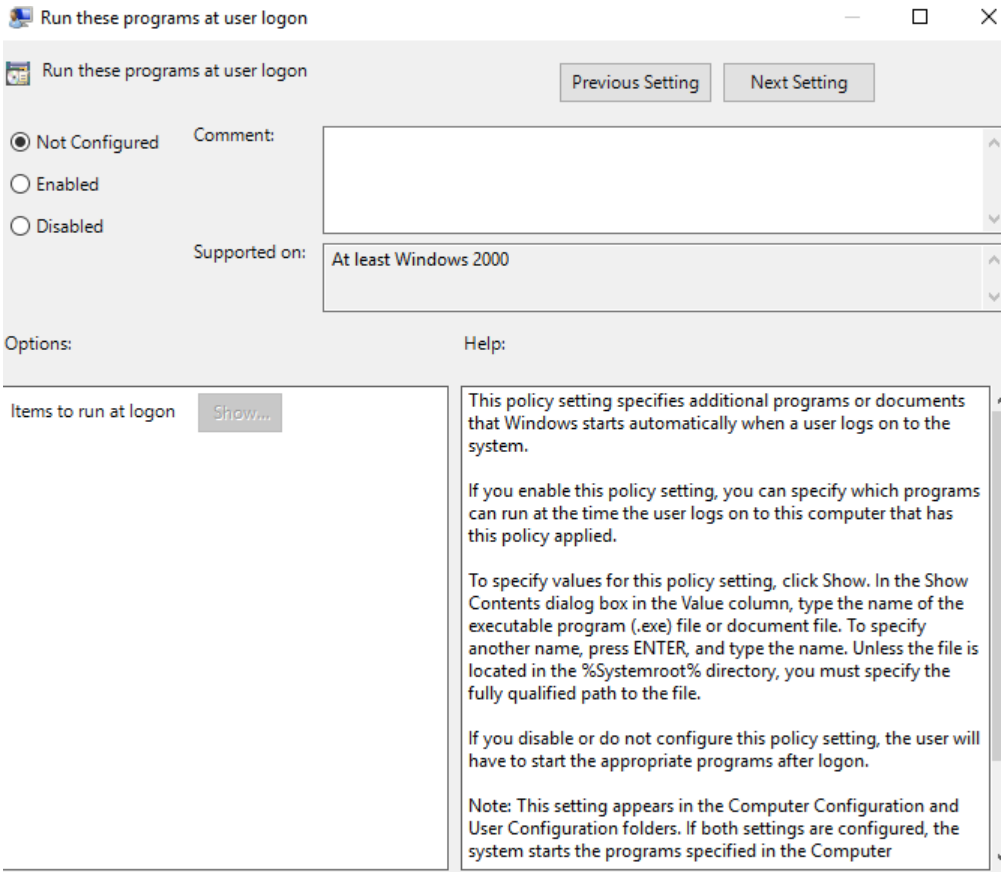
- **4-10-2:** Under Computer Configuration, click to expand **Policies** and **Administrative Templates**. Browse through the folders under Administrative Templates to see the settings and subfolders under each one. Take your time to get a good feel for the types of settings available in each main folder.



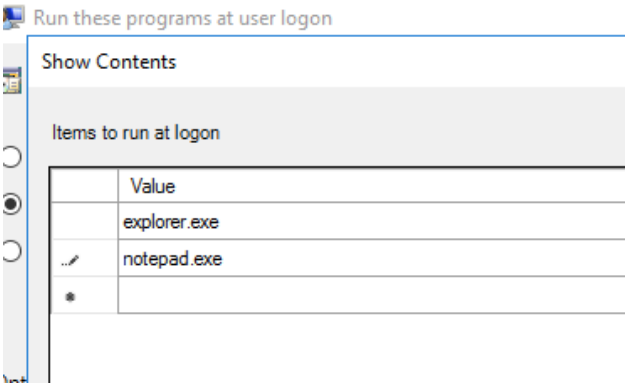
- **4-10-3:** Click the **All Settings** folder to see the full list of settings in Administrative Templates. The settings are arranged in alphabetic order by default. Click the **State** column to view the settings according to their state, which is Not configured, Enabled, or Disabled. Because GP01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



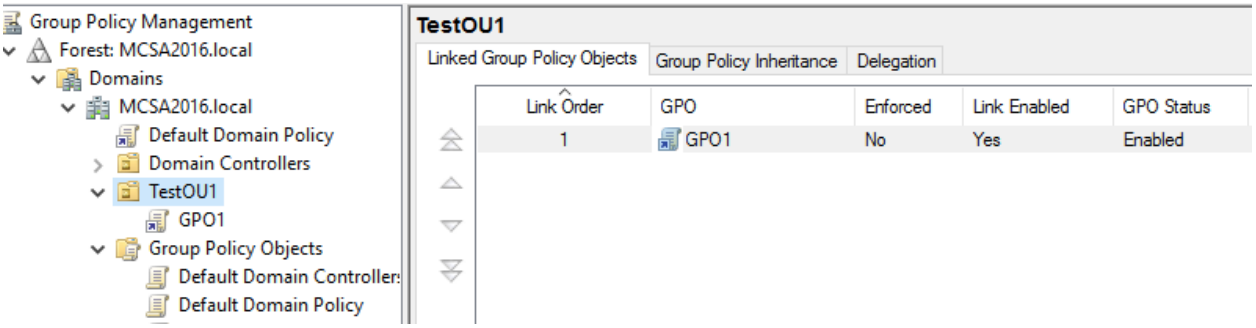
- **4-10-4:** In the left pane, click to expand the System folder, and then click **Logon**. In the right pane, click the **Setting** column header to arrange the setting in alphabetical order and then double-click **Run these programs at user logon**. This policy can be used in place of a logon script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



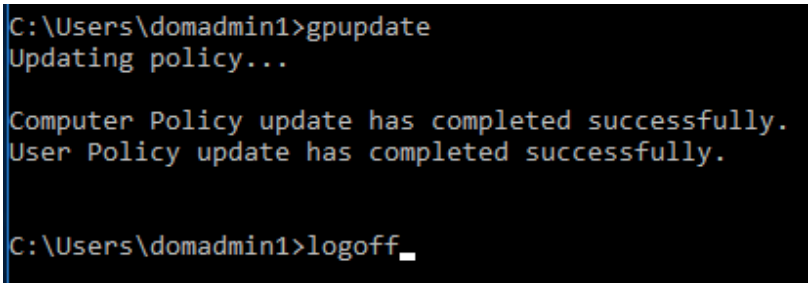
- **4-10-5:** In the Run these programs at user logon window, click **Enabled**, and then click **Show**. In the first row of the Show Contents dialog box, type **explorer.exe**, and in the second row, type **notepad.exe (**see Figure 4-27). Now all target computers run File Explorer and Notepad when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

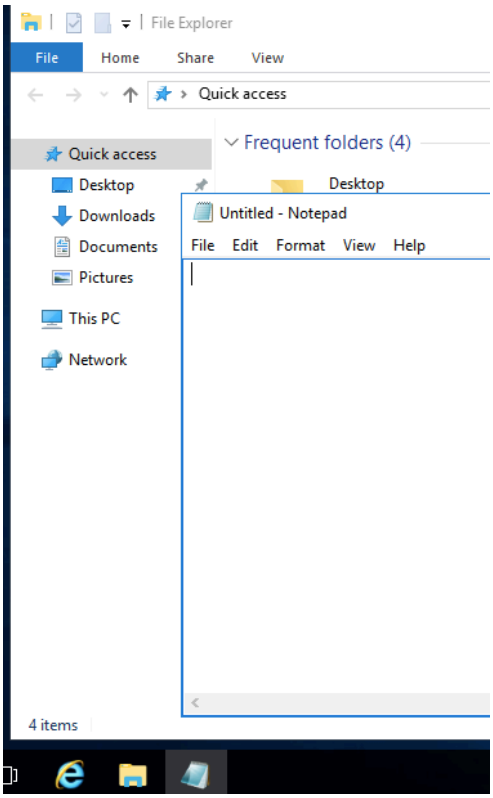


- **4-10-6:** Link **GPO1** to the **TestOU1** OU.

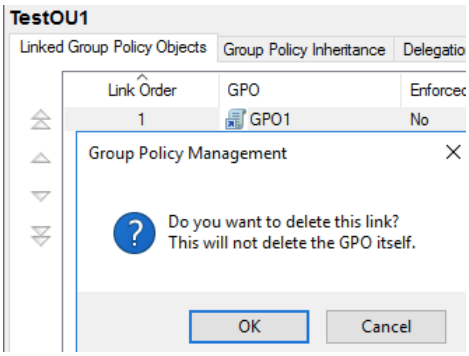


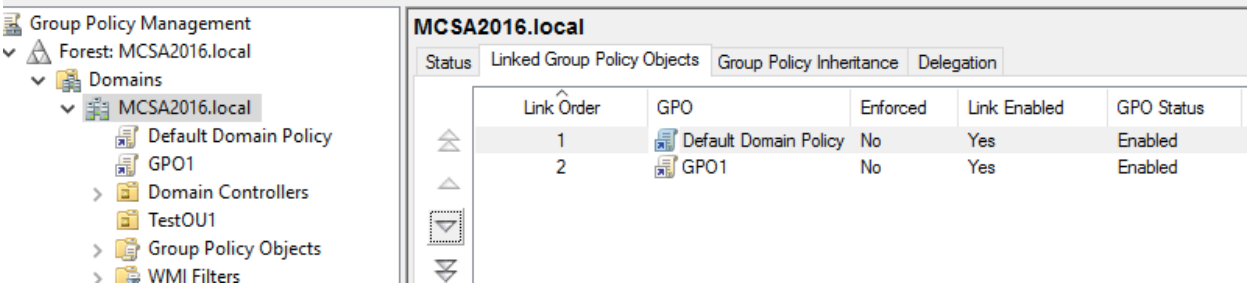
- **4-10-7:** On ServerDM1, sign in as **domadmin1** and run **gpupdate**. Then sign out of ServerDM1, and sign in again as **domadmin1**. After a few moments, File Explorer and Notepad open. Close File Explorer and Notepad.

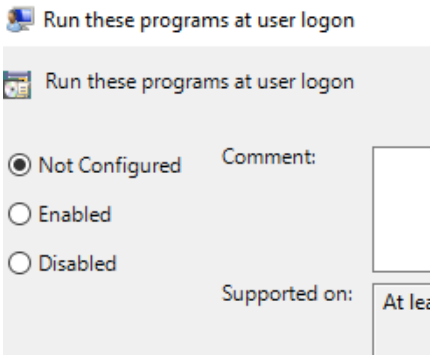




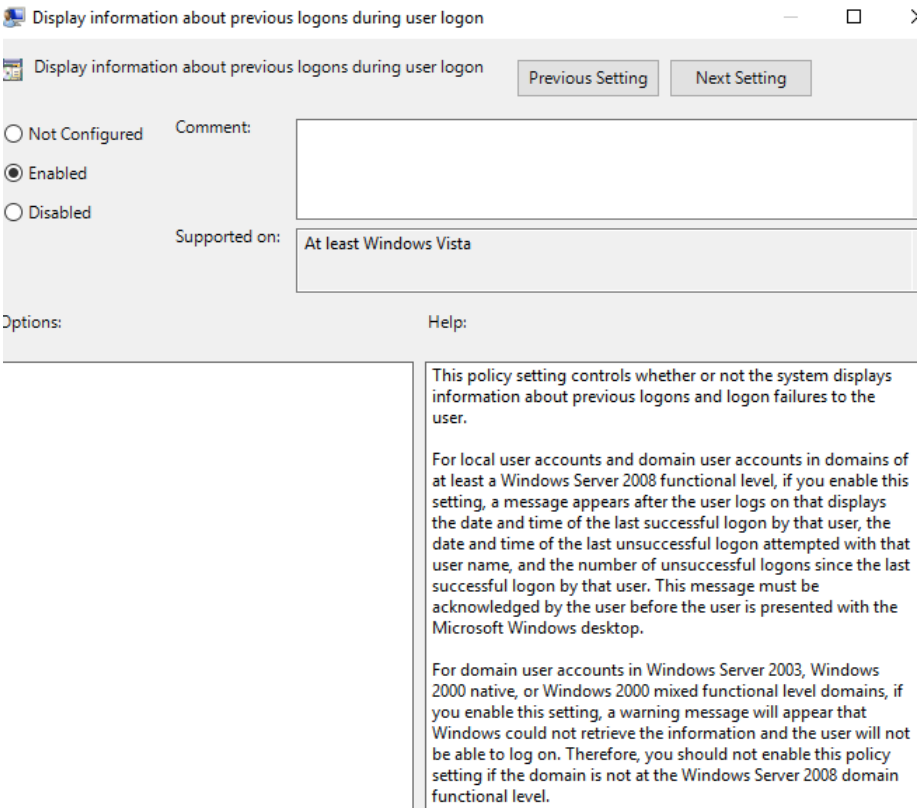
- **4-10-8:** On ServerDC1, unlink **GPO1** from **TestOU1** and link it to the domain node. Open GPO1 in the Group Policy Management Editor. Navigate to the **Run these programs at user logon** policy and set it to **Not Configured**.





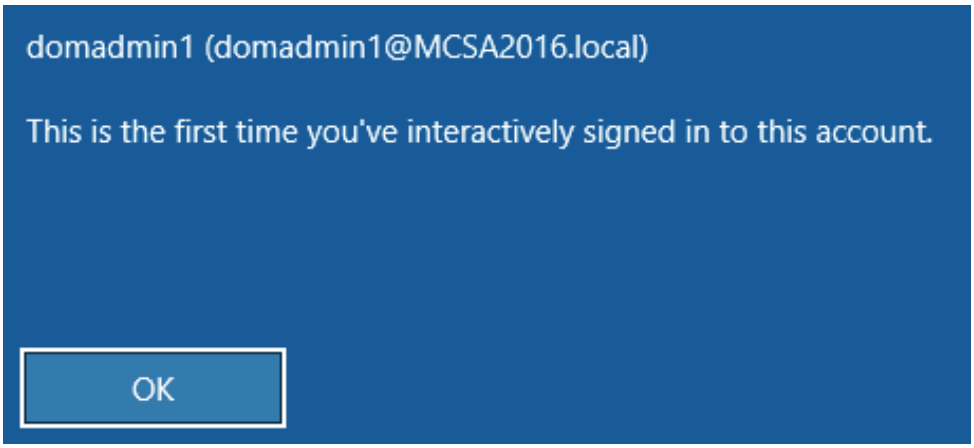


- **4-10-9:** Navigate to **Computer Configuration**, **Policies**, **Administrative Templates**, and **Windows Components**, and click **Windows Logon Options**. In the right pane, double-click **Display information about previous logons during user logon**. Read the Help information about this policy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

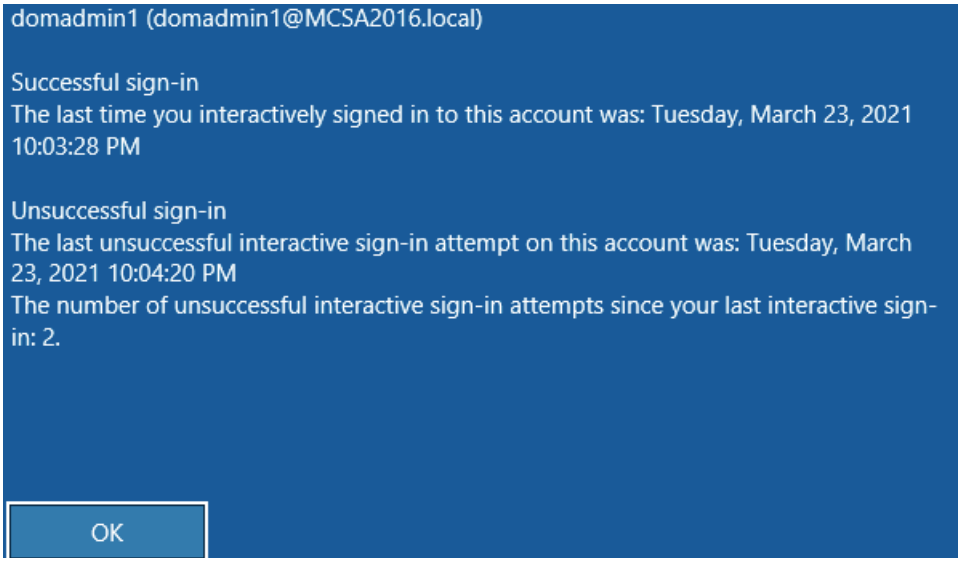


- **4-10-10:** On ServerDM1, run **gpupdate**, and then sign out and sign in again as **domadmin1**. You see a message stating that it's the first time you have signed in to the account. That's because this is the first time you have signed in since the policy was enabled. Click **OK**.

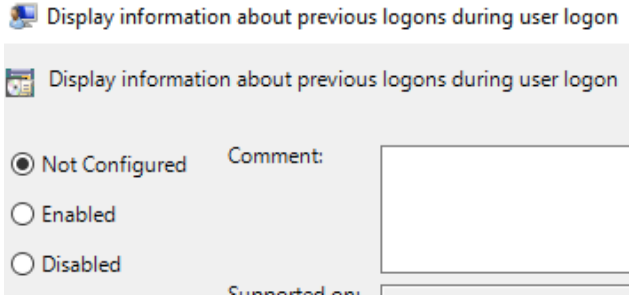
```
C:\Users\domadmin1>gpupdate
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.


C:\Users\domadmin1>logoff
```

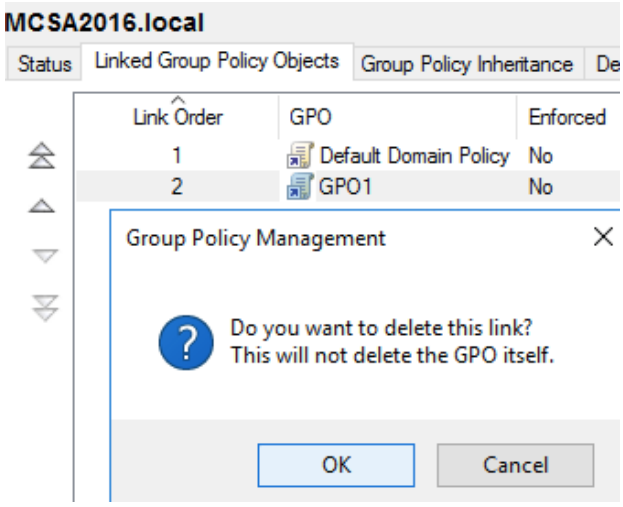


- **4-10-11:** Sign out of ServerDM1, and then try to sign in again, but with an incorrect password. Then sign in with the correct password. A window opens showing the last successful sign-in and an unsuccessful sign-in attempt (see Figure 4-28). This information is intended to let users know whether 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.



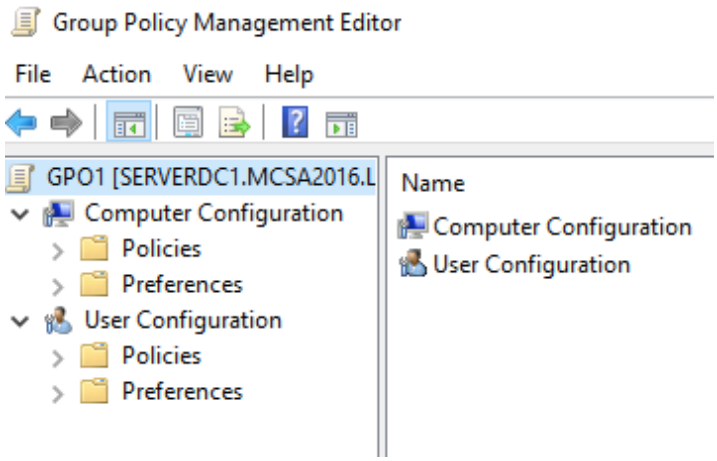


- **4-10-13:** Continue to the next activity.

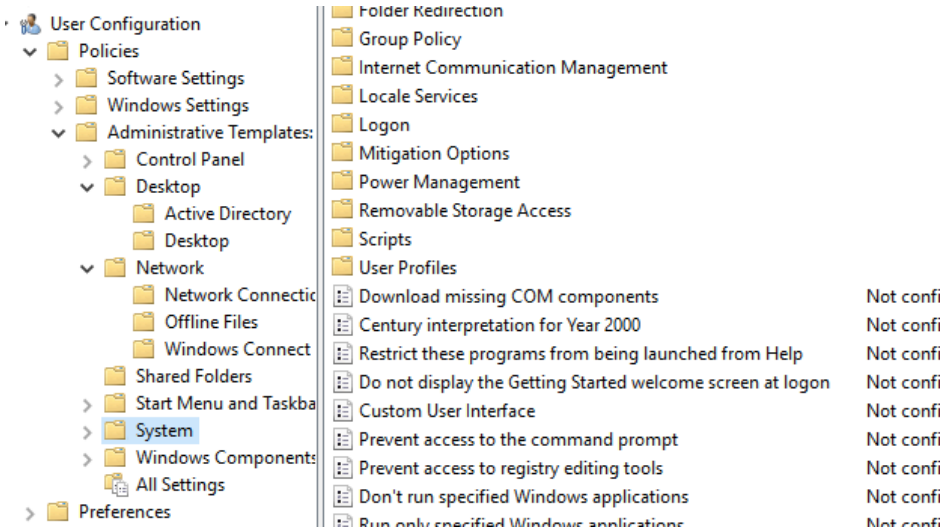
Activity 4-11: Working with User Administrative Template Settings

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.

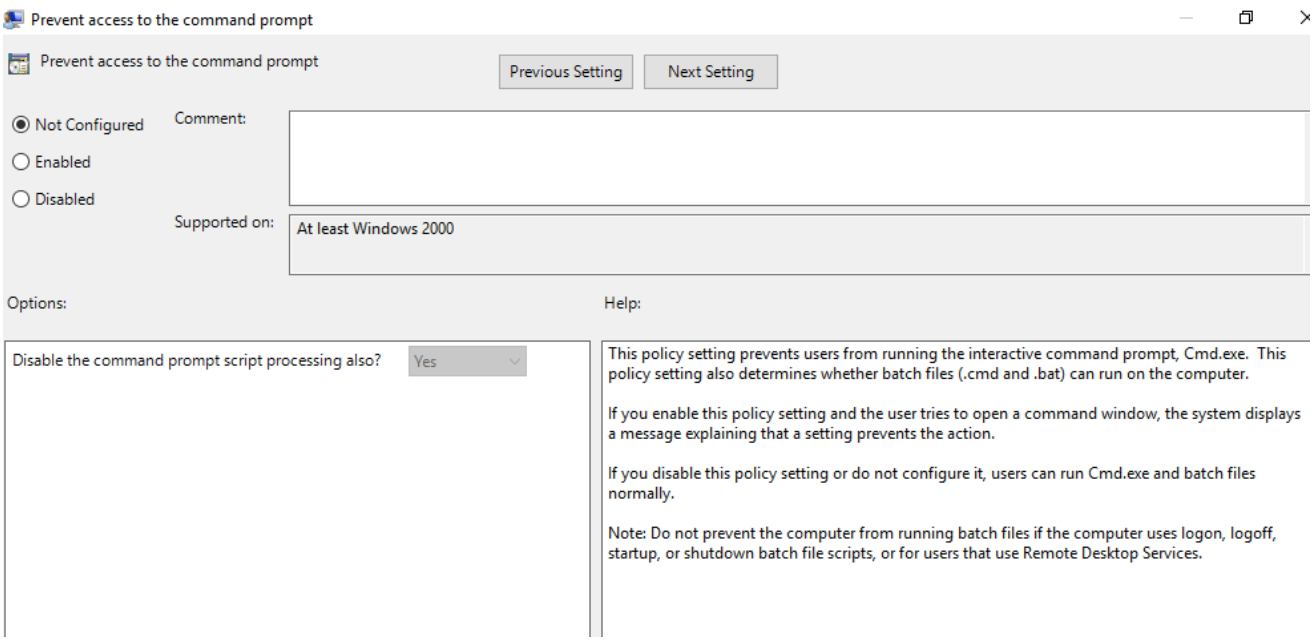
- **4-11-1:** On ServerDC1, open **GP01** in the Group Policy Management Editor.



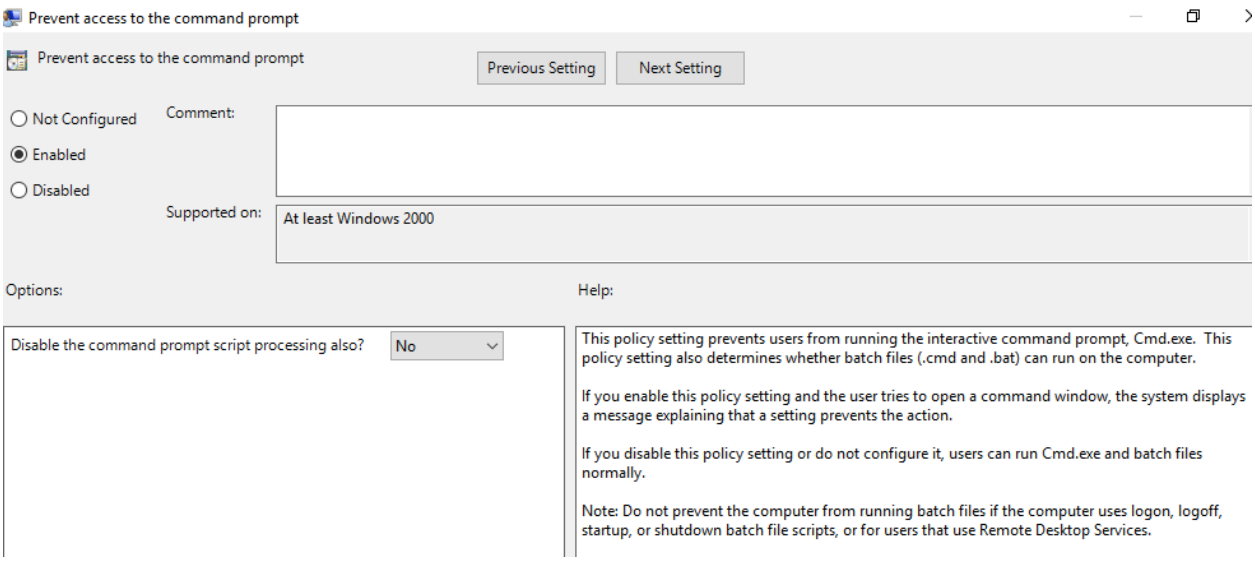
- **4-11-2:** Under User Configuration, click to expand **Policies** and **Administrative Templates**. Browse through the folders under Administrative Templates to see the settings and subfolders under each one. Take your time to get a good feel for the types of settings available in each main folder.



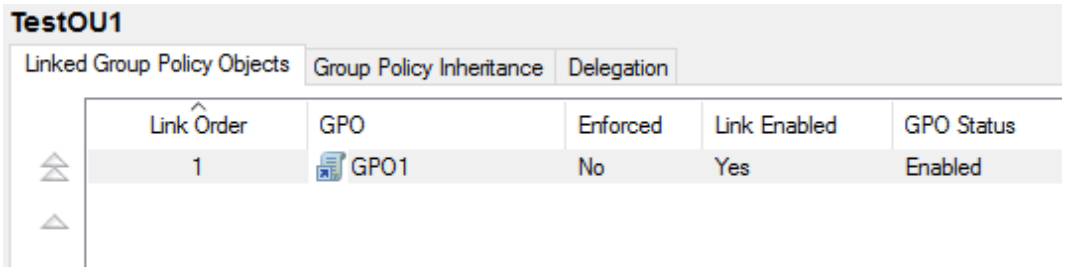
- **4-11-3:** In the left pane, click to expand the **System** folder, and then click to select the **System** folder. In the right pane, double-click **Prevent access to the command prompt**.



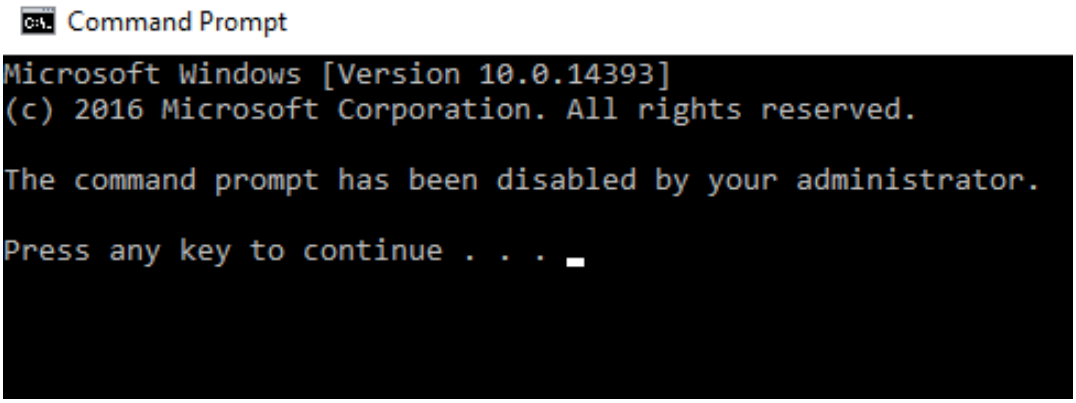
- 4-11-4: Read the policy help information. Click **Enabled**, and then click OK. Close the Group Policy Management Editor.



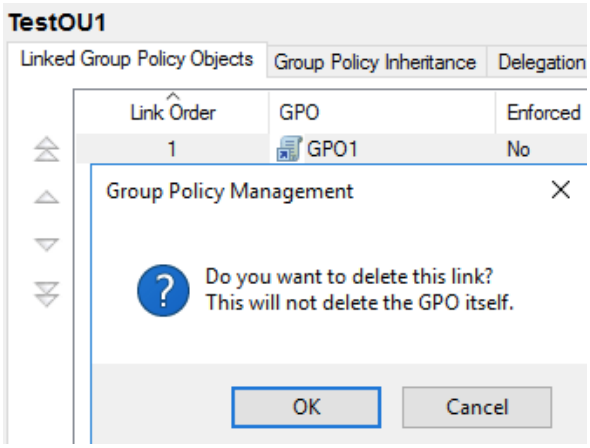
- 4-11-5: In Group Policy Management, link **GP01** to **TestOU1**.



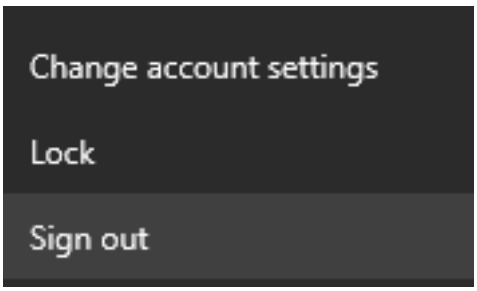
- **4-11-6:** On ServerDM1, sign in as **domadmin1**. Right-click **Start** and click **Command Prompt**. A command prompt window opens, but you see a message stating that the administrator has disabled it. Press any key to close the command prompt window**.**



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



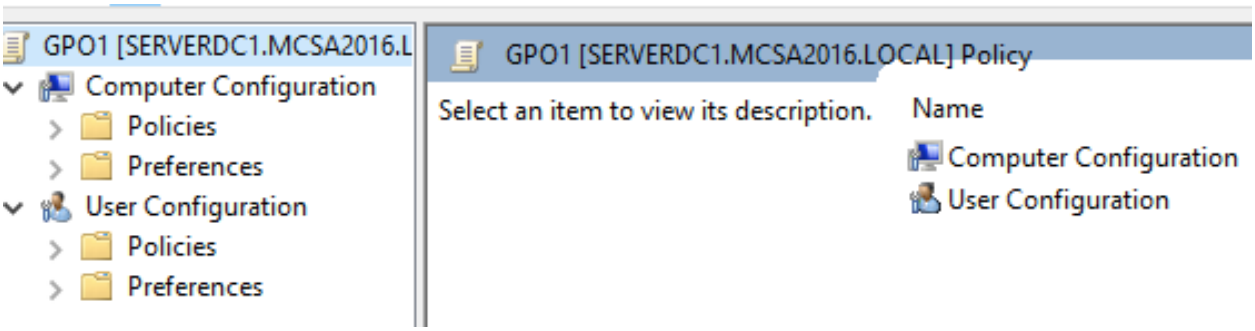
- **4-11-8:** Sign off ServerDM1. Continue to the next activity.



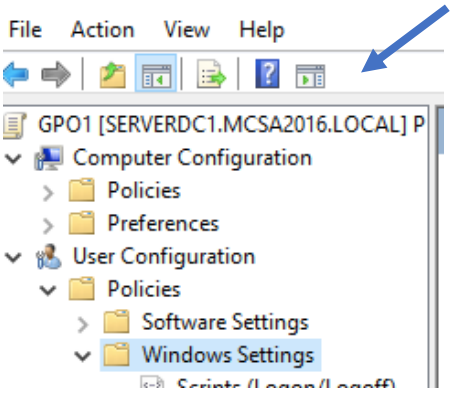
Activity 4-12: Viewing Settings with Filter Options

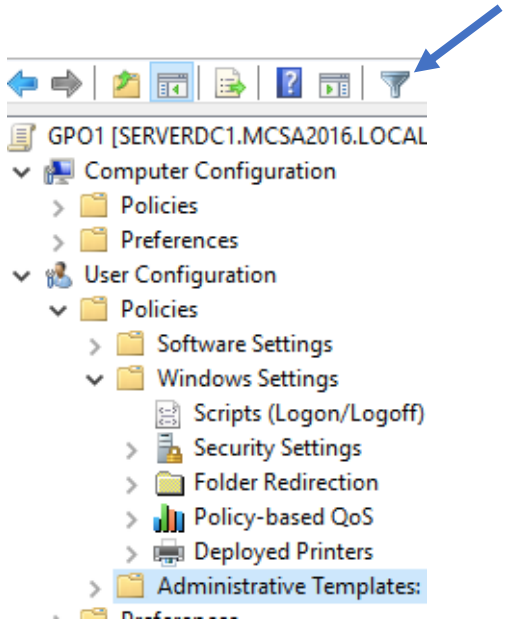
Description: In this activity, you want to configure the setting that displays the desktop instead of the Start screen when users sign in to Windows 8 computers. You can't remember the exact setting name, but you know it's in the User Configuration node of a GPO. You configure a filter to narrow down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

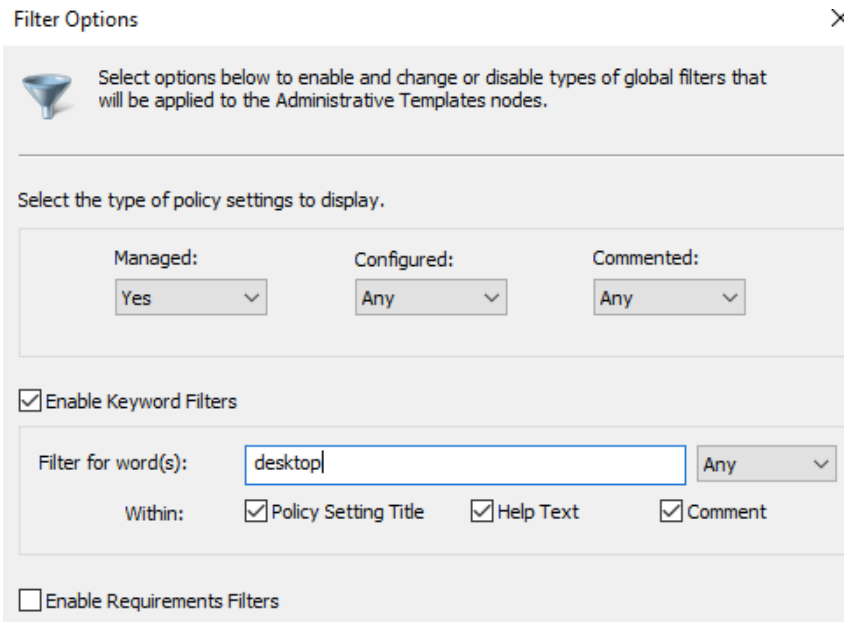


- **4-12-2:** Under User Configuration, click to expand **Policies,** and click **Windows Settings.** Notice that there's no Filter icon on the toolbar because you can't filter settings in Windows Settings. Click **Administrative Templates.** You see the Filter icon now.

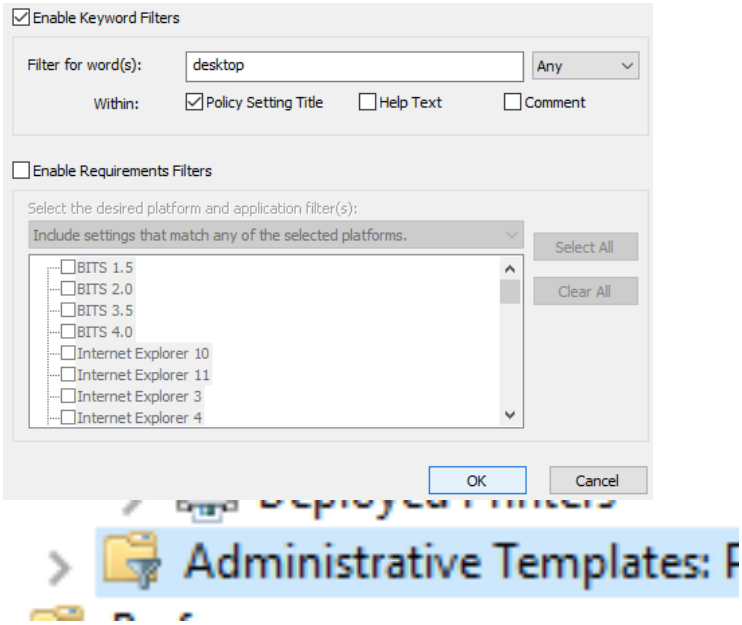




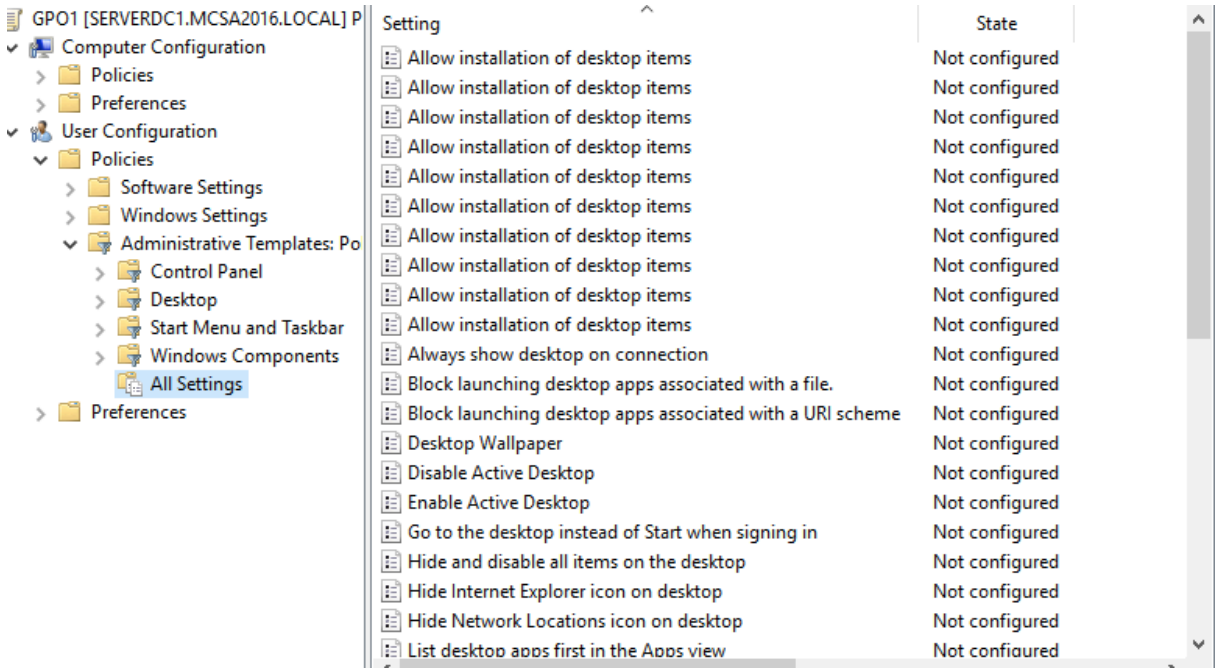
- 4-12-3: Click **Action, Filter Options.** In the Filter Options window, click the **Enable Keyword Filters** check box. You remember that the policy setting title has the word "desktop" in it, so type **desktop** in the Filter for words(s) text box. If necessary, click **Any** in the list box next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



- 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.

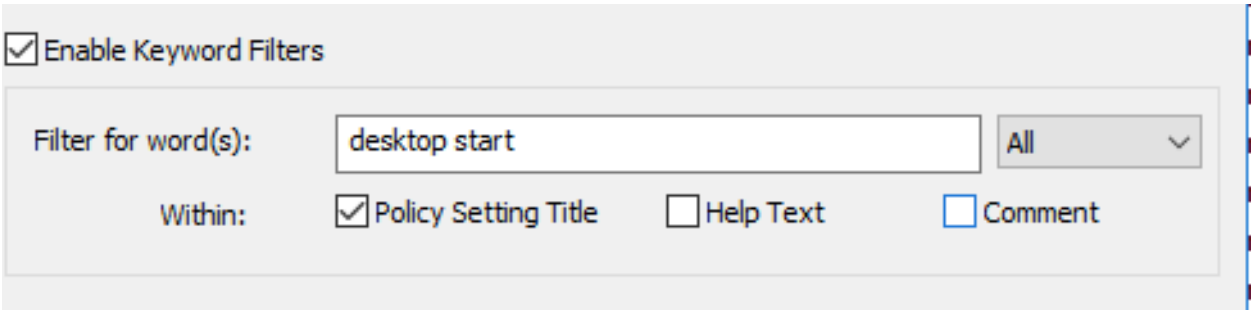


- **4-12-5:** Under User Configuration, click to expand **Administrative Templates,** and click **All Settings.** You see a list of policy settings with the word *desktop* in the title. That's still quite a few settings to sift through.

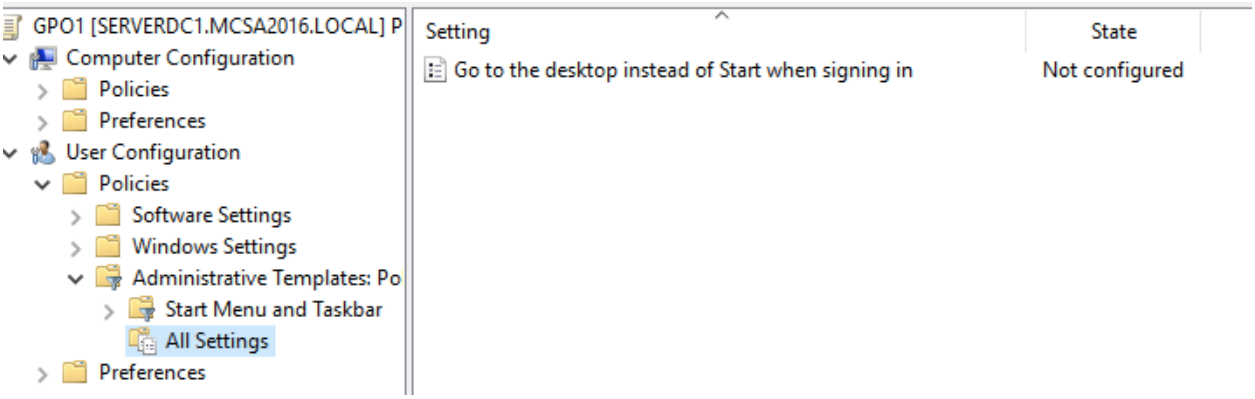


- **4-12-6:** Click **Action, Filter Options.** You remember that the word "start" was also in the title. In the Filter for words(s) text box, type the word *start* next to

"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.**



- **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.

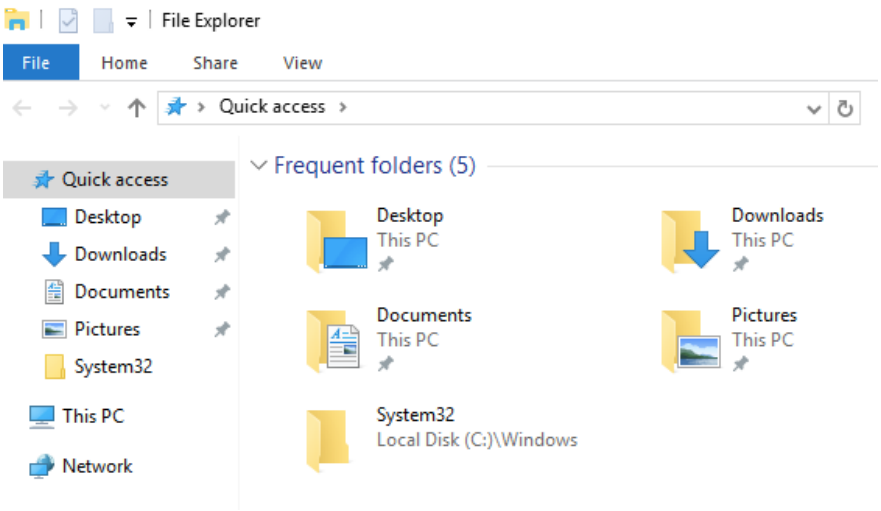


- **4-12-8:** Continue to the next activity.

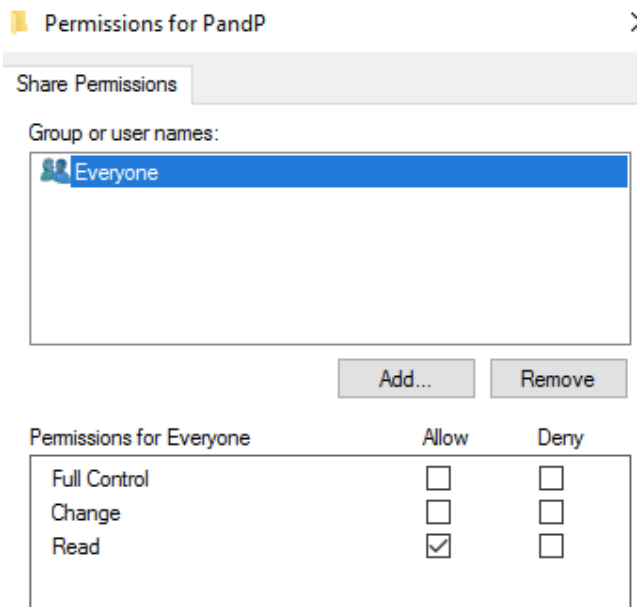
Activity 4-13: Configuring and Testing Preferences

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.

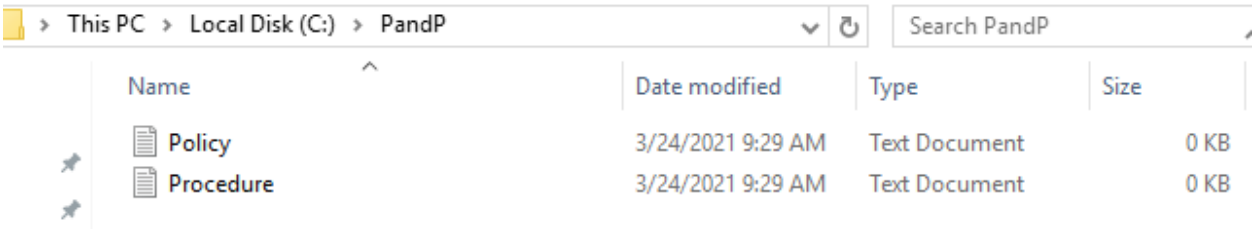
- **4-13-1:** To create a file preference in which a folder with files is distributed to all computers, first you create a share for the files to be copied in a preference. On ServerDC1, open **File Explorer.**



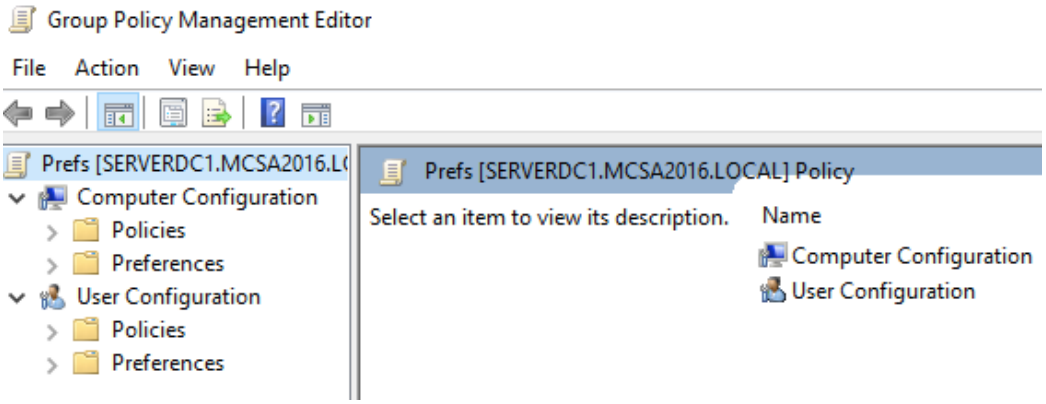
- **4-13-2:** Create a folder named **PandP** on the **C:** volume. Share this folder and give the **Everyone** group **Read** permission.



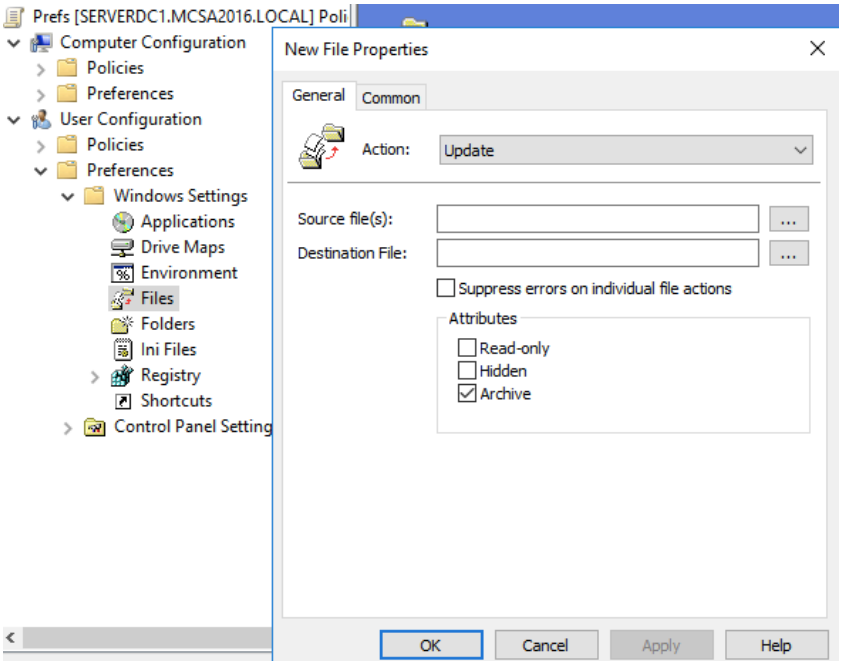
- **4-13-3:** In the PandP folder, create two text files: Name the first file **Policy.txt** and the second one **Procedure.txt.** Close File Explorer.



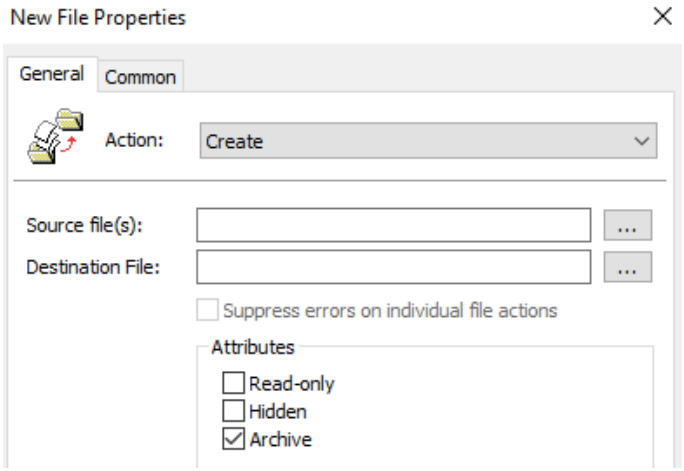
- **4-13-4:** Open the Group Policy Management console, if necessary. Create a GPO named **Prefs** in the Group Policy Objects folder and open it in the Group Policy Management Editor.



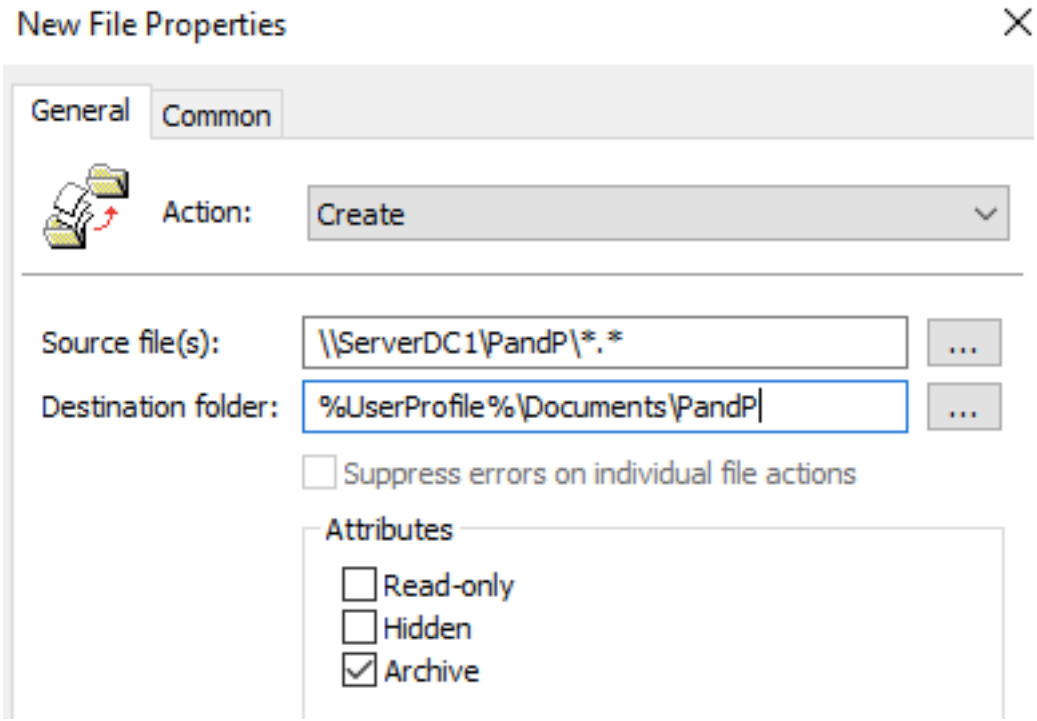
- **4-13-5:** Under User Configuration, click to expand **Preferences** and **Windows Settings.** Right-click **Files,** point to **New,** and click **File.**



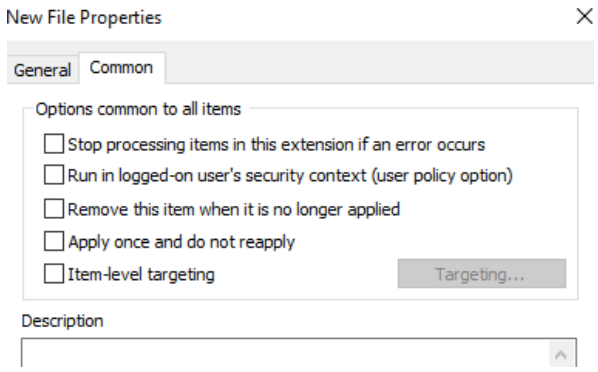
- **4-13-6:** In the Action list box, click **Create.**

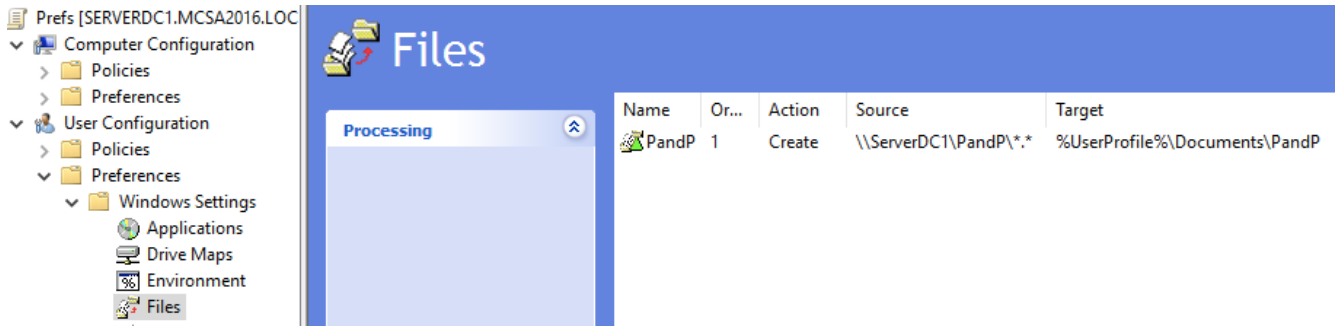


- **4-13-7:** In the Source file(s) text box, type **\\ServerDC1\PandP*.*.** Using a wildcard copies all files in the PandP folder. In the Destination folder text box, type **%UserProfile%\Documents\PandP.** The PandP folder is created automatically when the policy is applied. Leave the default **Archive**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

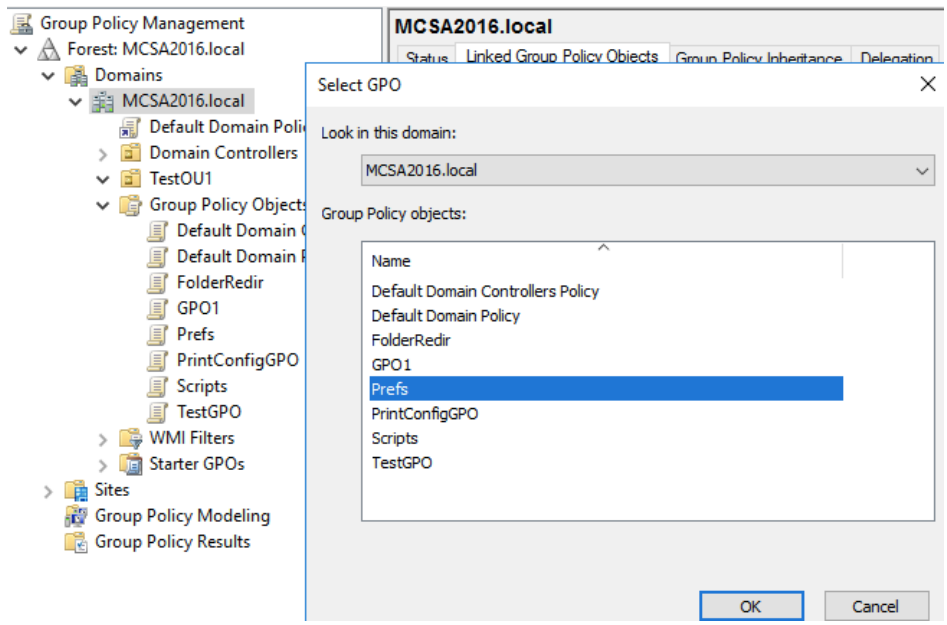


- **4-13-8:** Click the **Common** tab. Review the available options, and then click **OK.** Note that you can change the processing order of preferences, so if you need one preference to be processed before another, you can arrange them in the order you want. Close the Group Policy Management Editor.

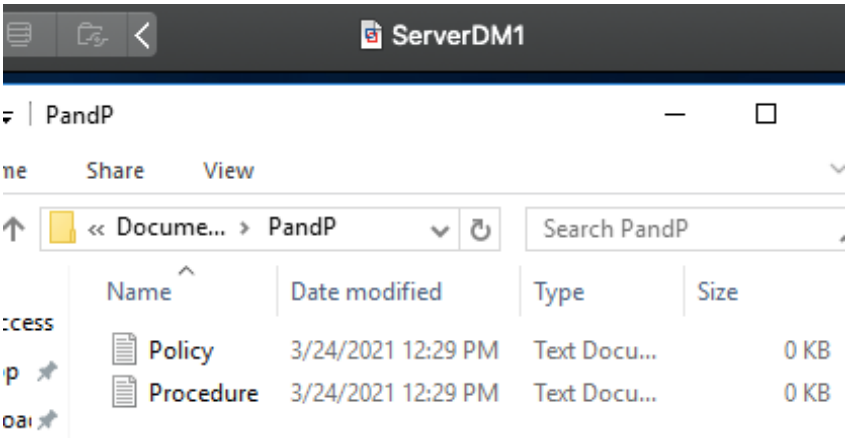




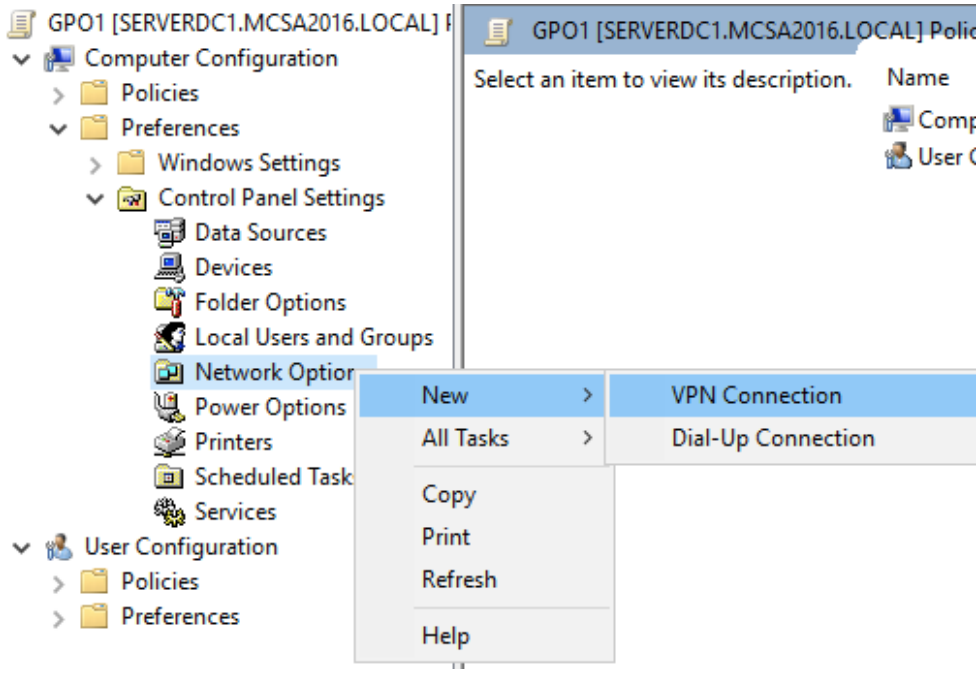
- **4-13-9:** In the Group Policy Management console, link the **Prefs** GPO to the domain object.



- **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.

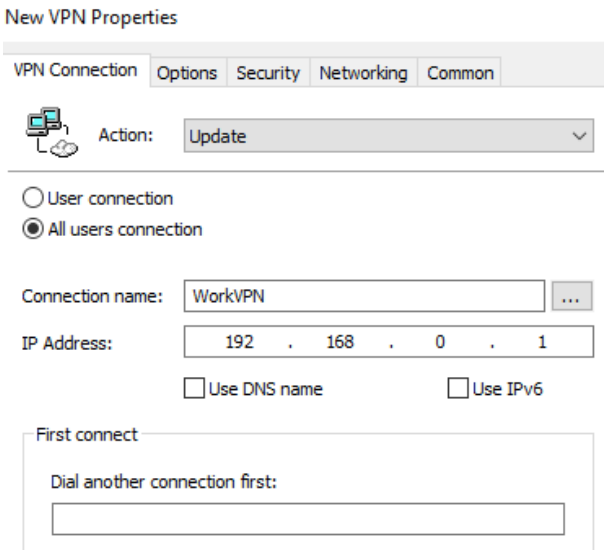


- **4-13-11:** Next, you'll create a Control Panel preference in which you deploy a VPN connection. On ServerDC1, open the **Prefs** GPO in the Group Policy Management Editor. Under Computer Configuration, click to expand **Preferences** and **Control Panel Settings.** Right-click **Network Options,**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

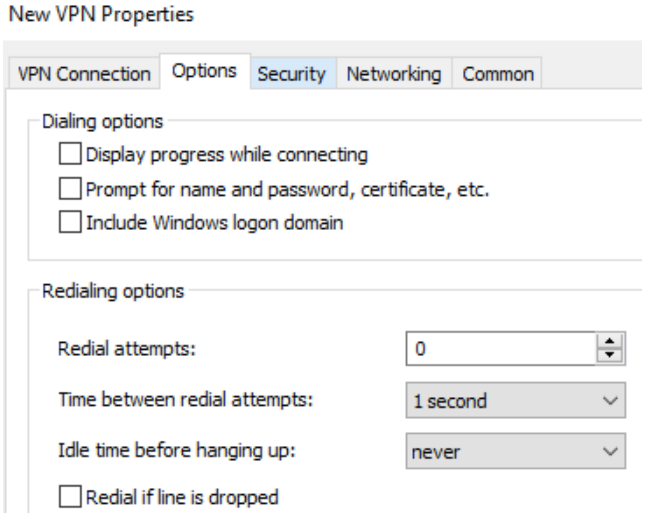


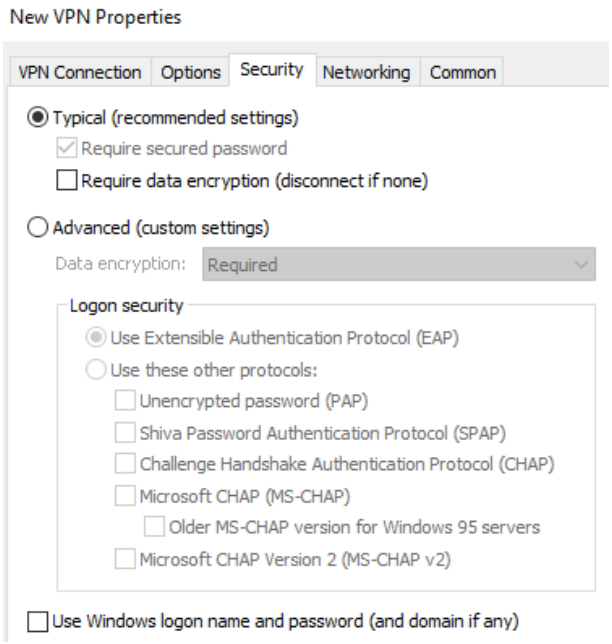
- **4-13-12:** In the Action drop-down list, leave the default setting **Update.** Click the **All users connection** option button so that all users logging on to target

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).

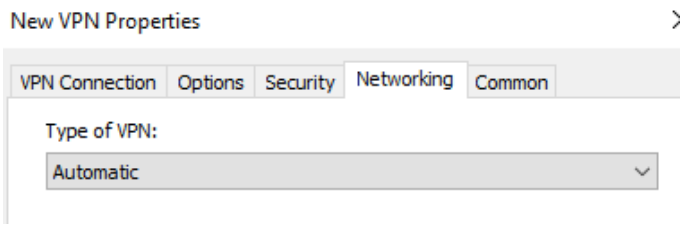


- **4-13-13:** Click the **Options** tab and review the available settings. Click the **Security** tab, which is where you set authentication options. Leave the settings at their defaults.

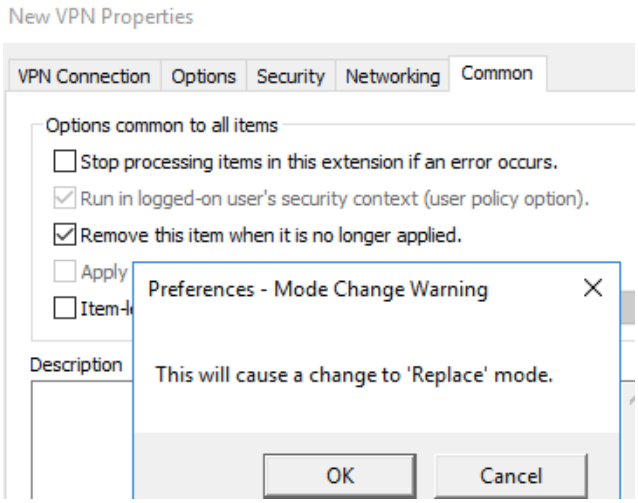




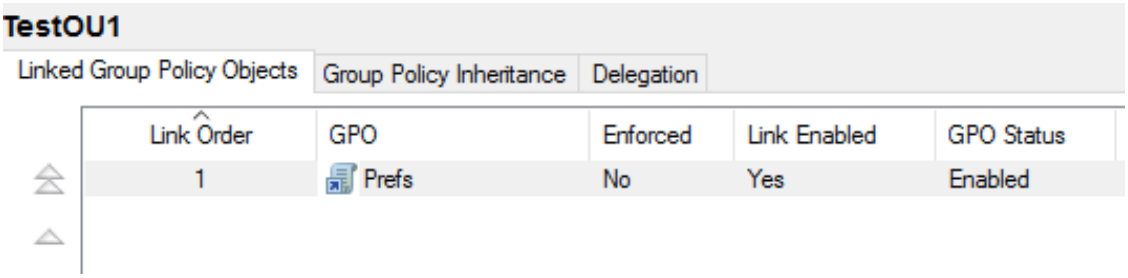
- **4-13-14:** Click the **Networking** tab where you can choose the VPN tunnel type. Leave the default setting **Automatic.**



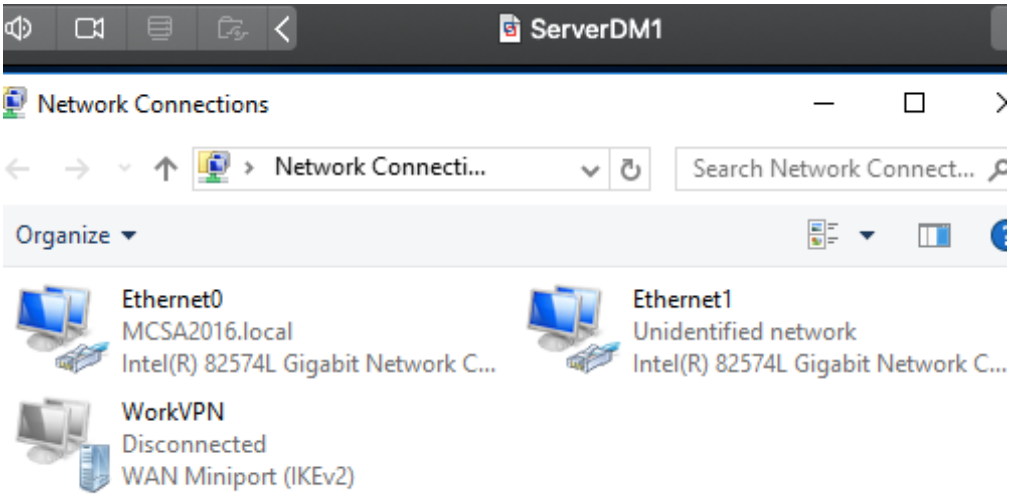
- **4-13-15:** Click the **Common** tab and click **Remove this item when it is no longer applied.** In the warning message stating that the preference will be set to Replace mode, click **OK**. Click **OK** again.



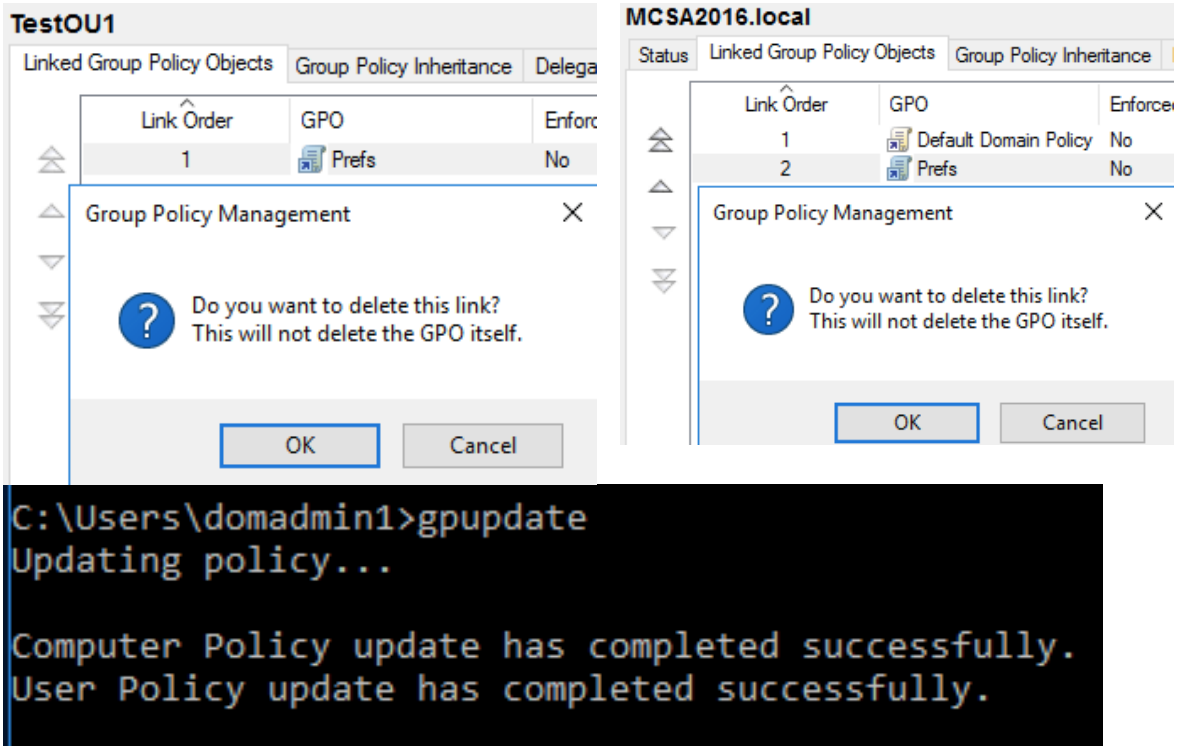
- **4-13-16:** Link the **Prefs** GPO to the **TestOU1** OU. Sign in to ServerDM1 as **domadmin1** . Because it's a Computer Configuration policy, you have to restart the computer or run gpupdate for it to be applied. Open a command prompt window, and then type **gpupdate** and press **Enter**.



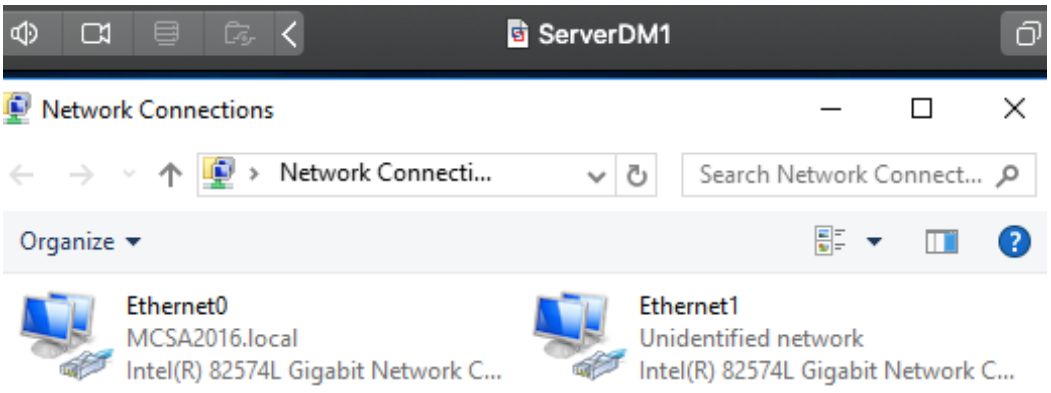
- **4-13-17:** Right-click **Start** and click **Network Connections**. You see the WorkVPN connection.



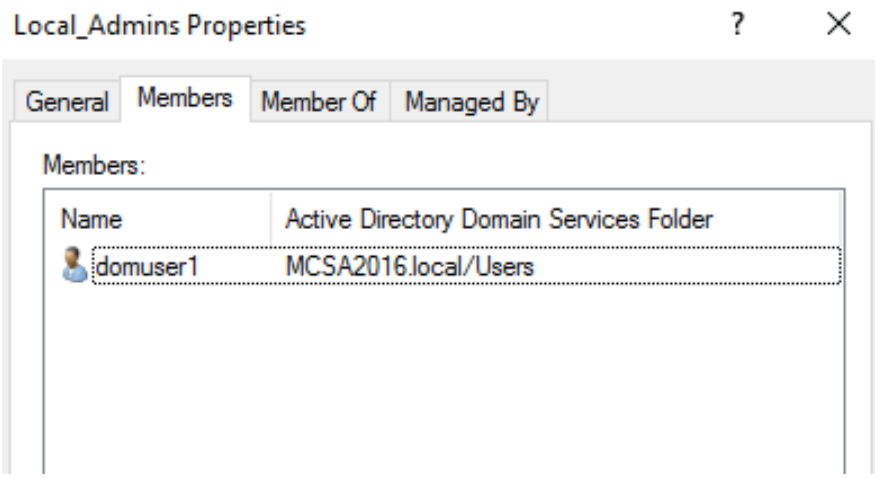
- **4-13-18:** Because you selected the *Remove this item when it is no longer applied* option, you should test that functionality. On ServerDC1, unlink **Prefs** from the domain. On ServerDM1, run **gpupdate** again.



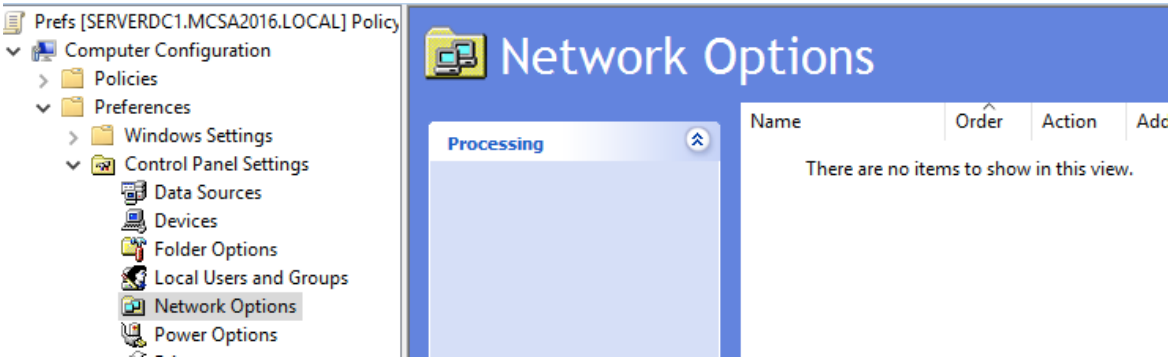
- **4-13-19:** Look in the Network Connections window to verify that the VPN connection has been removed. Sign out of ServerDM1.



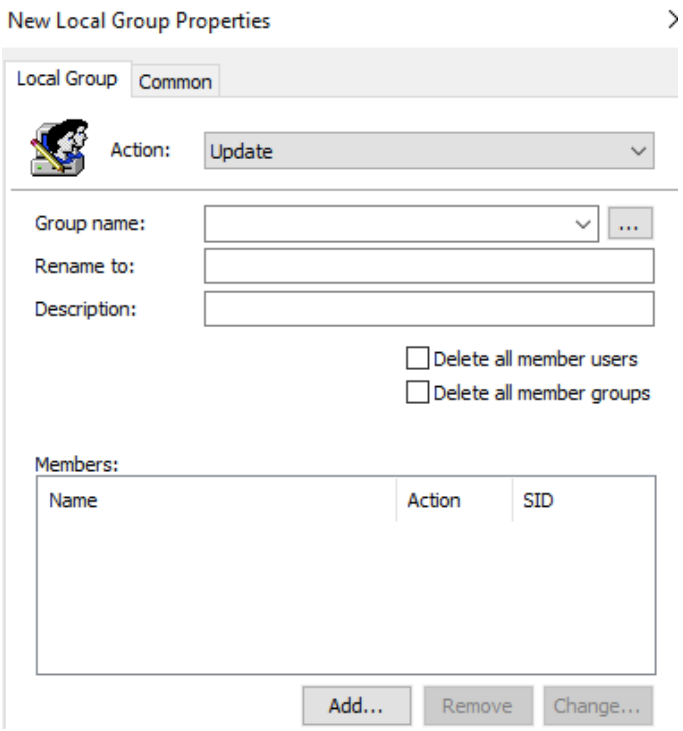
- **4-13-20:** Next, you'll create a preference that configures local groups on member computers. On ServerDC1, open Active Directory Users and Computers. Click the **Users** folder, and then create a global security group named **Local_Admins** in this folder. Add **domuser1** to this group.



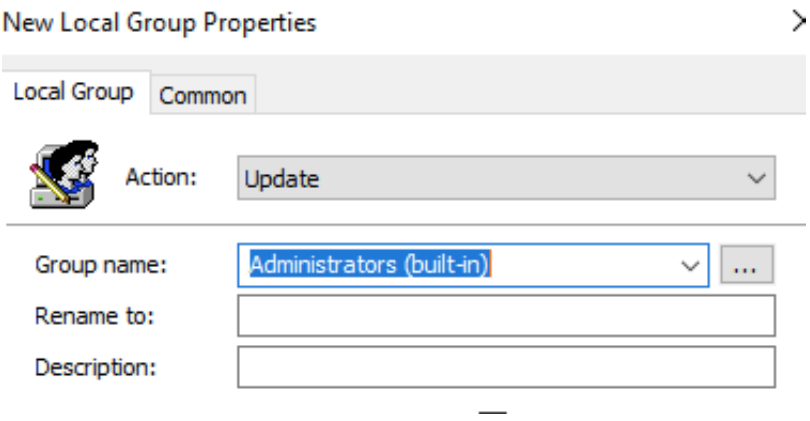
- **4-13-21:** Open the Group Policy Management console, and open the **Prefs** GPO in the Group Policy Management Editor. Delete the **Network Options** preference under the Computer Configuration\Control Panel Settings.



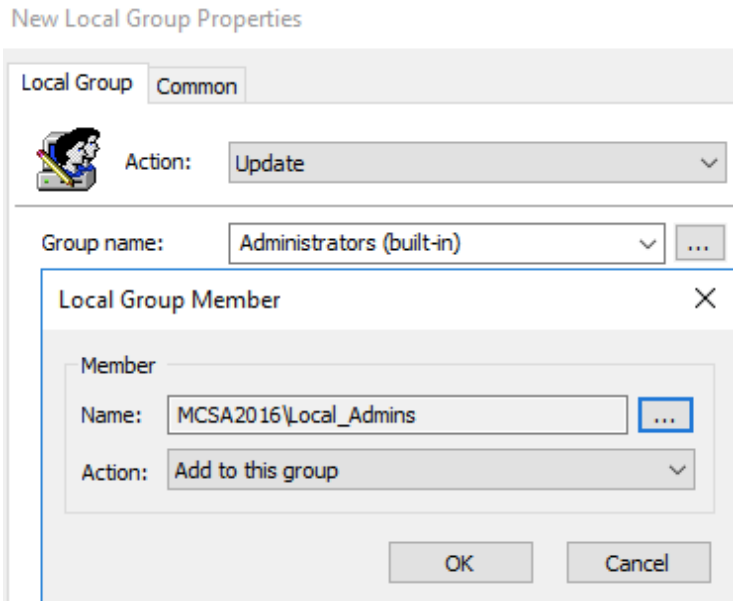
- **4-13-22:** Next, right-click **Local Users and Groups**, point to **New**, and click **Local Group**.



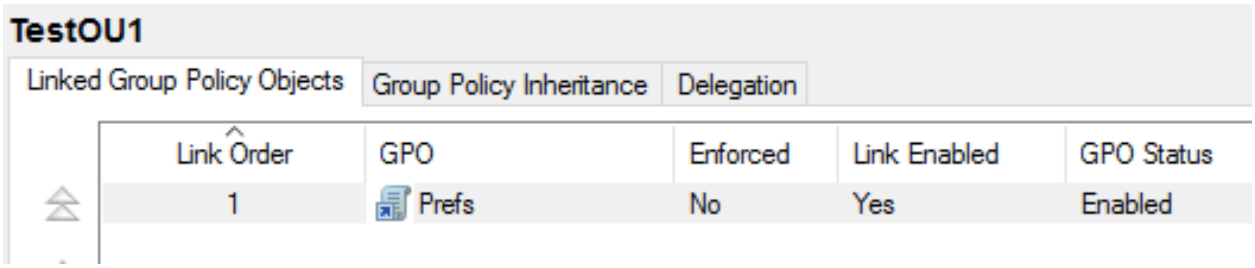
- **4-13-23:** Make sure Update is the selected action. Click the **Group name** list arrow, and click **Administrators** (**built-in**) in the list.



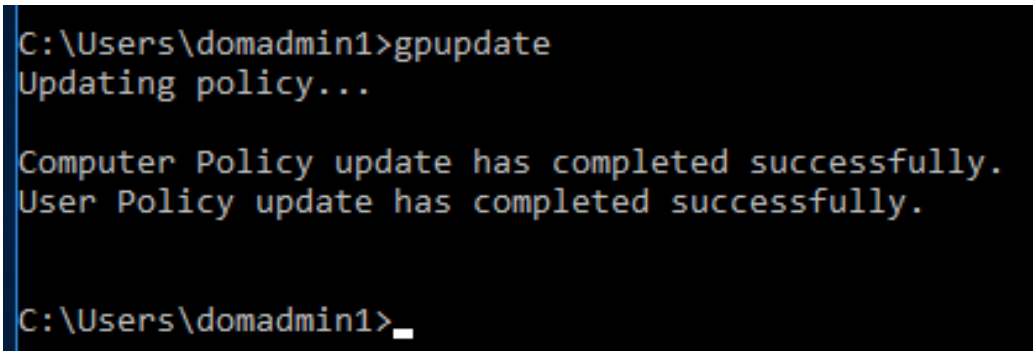
- **4-13-24:** Click the **Add** button, and then click the **browse** button next to the Name text box. In the Select User, Computer, or Group dialog box, type **Local_Admins**, click **Check Names**, and then click **OK**. Make sure the action is **Add to this group**, and then click **OK** twice.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



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

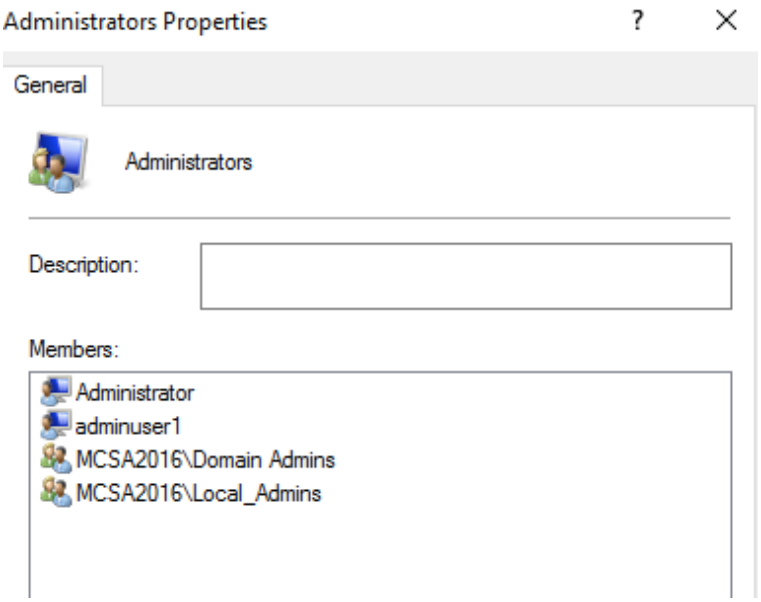


- **4-13-26:** Sign in to the domain from ServerDM1 as **domadmin1**. Open a command prompt window, type **gpupdate**, and press **Enter**. Close the command prompt window.

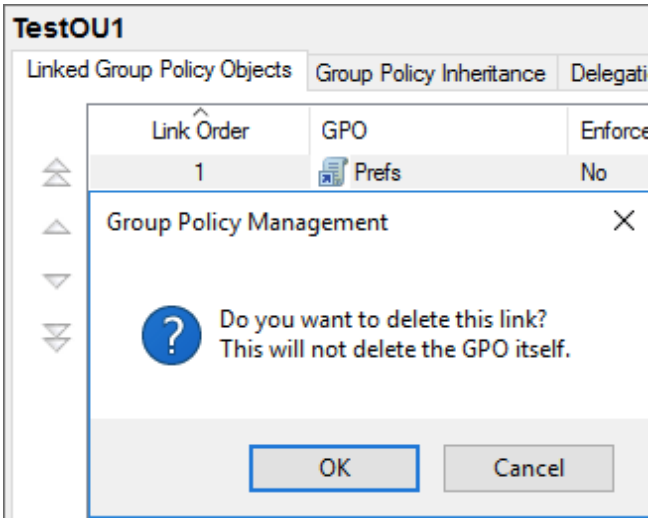


- **4-13-27:** Right-click **Start** and click **Computer Management**. Click to expand **Local Users and Groups**, click **Groups**, and then double-click **Administrators** to open the Properties dialog box. You should see Local_Admins in the Members

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.



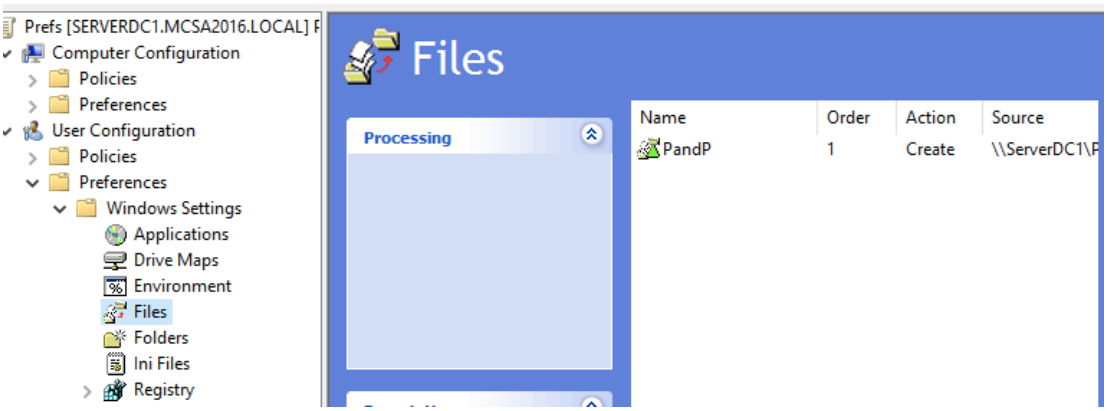
- **4-13-28:** On ServerDC1, unlink the **Prefs** GPO from the **TestOU1** OU. Continue to the next activity.



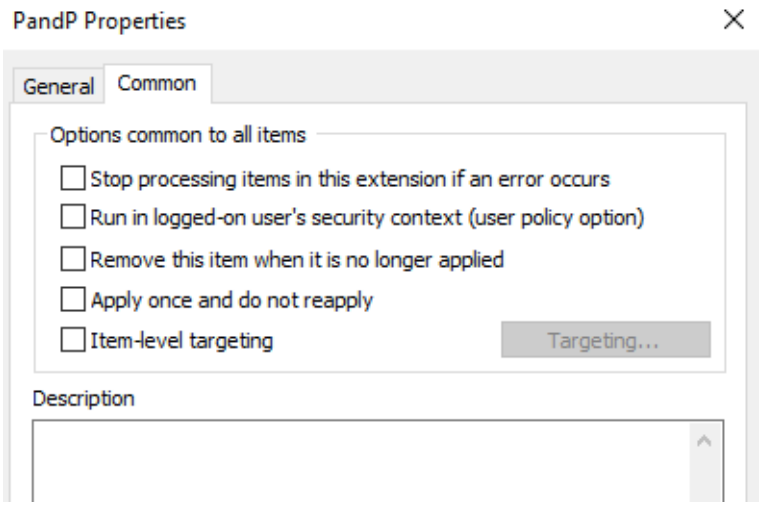
Activity 4-14: Configuring item-level Targeting

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.

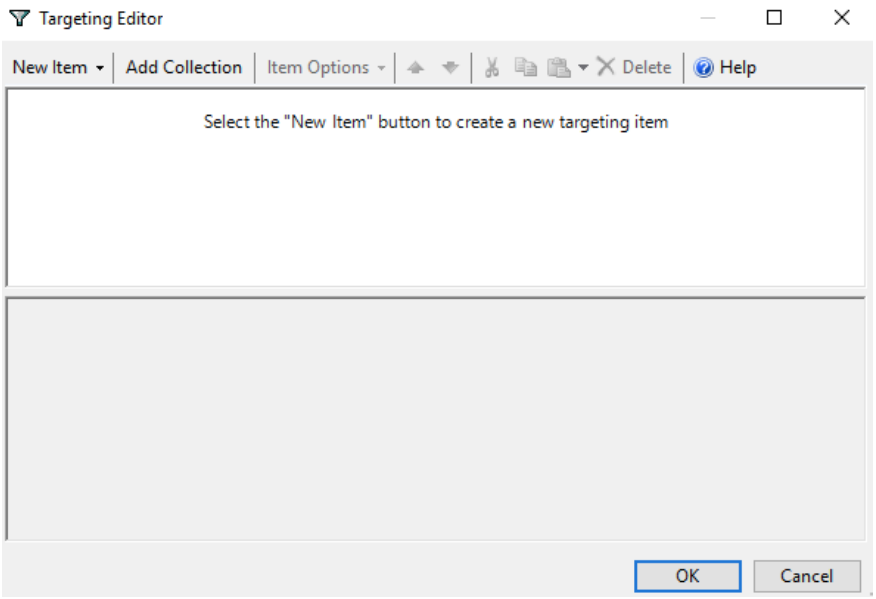
- **4-14-1:** On ServerDC1, open the Prefs GPO in the Group Policy Management Editor. Under User Configuration, expand **Preferences** and **Windows Settings**, and then click **Files.**



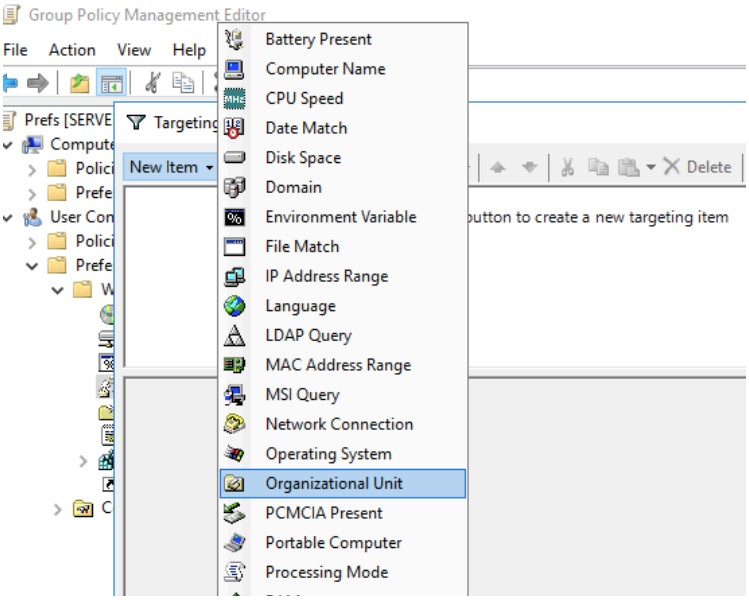
- **4-14-2:** Double-click the **PandP** file preference in the right pane. In the Properties dialog box, click the **Common** tab.



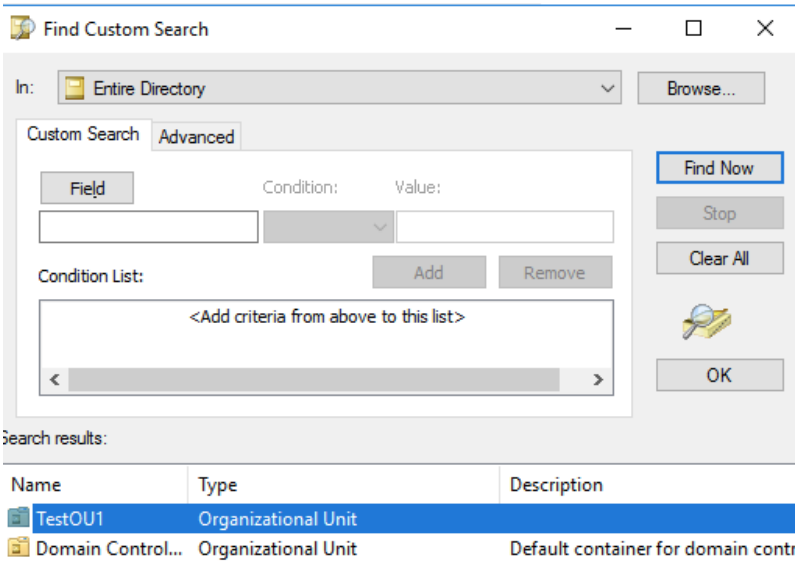
- 4-14-3: Click the **Item-level targeting** check box, and then click the **Targeting** button.



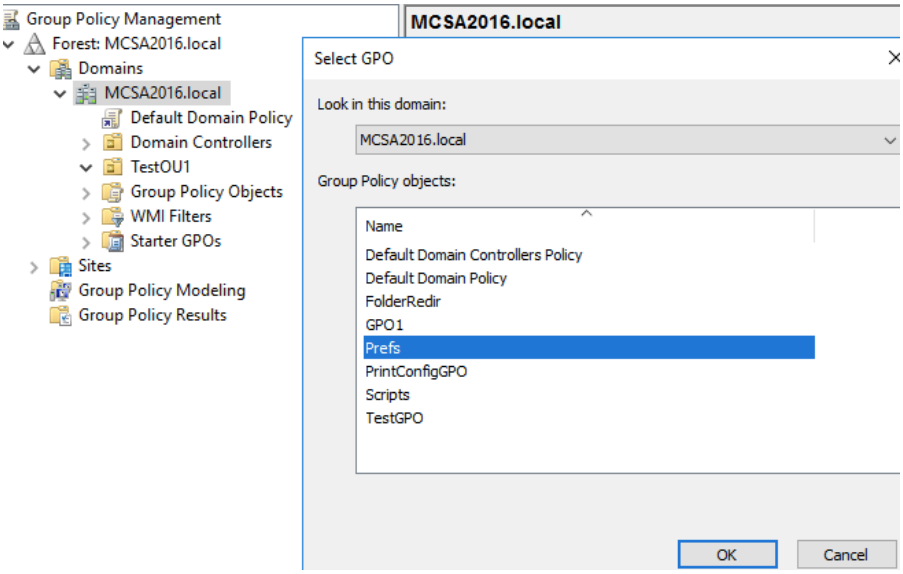
- 4-14-4: In the Targeting Editor window, click **New Item**, and then click **Organizational Unit**.



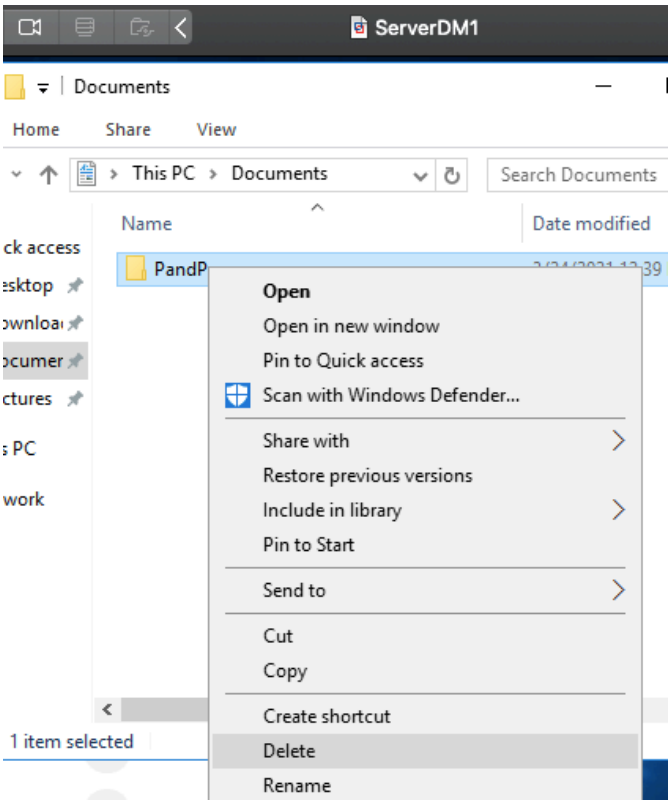
- 4-14-5: In the Organizational Unit text box, click the browse button, click **TestOU1**, and then click **OK**. Click **OK** twice to get back to the Group Policy Management Editor. This will limit the preference to only users in the TestOU1 organization unit, which in this case is only domadmin1.



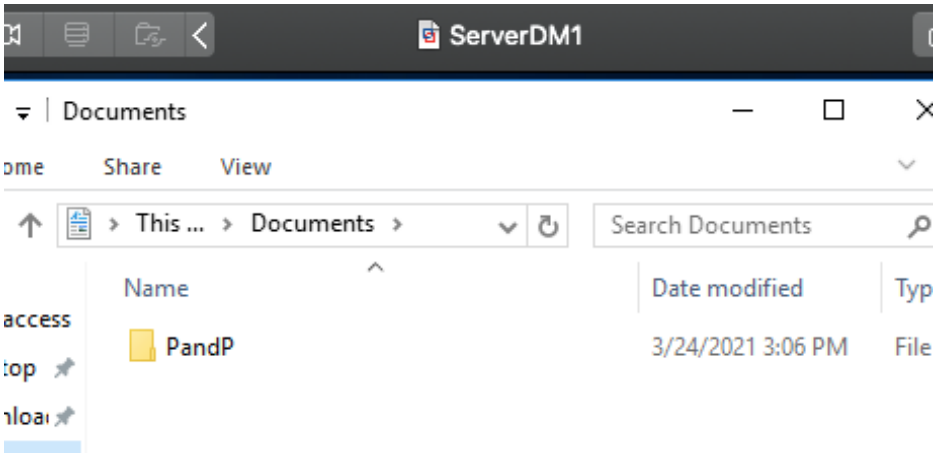
- 4-14-6: Close Group Policy Management Editor. Link the **Prefs** GPO to the domain.



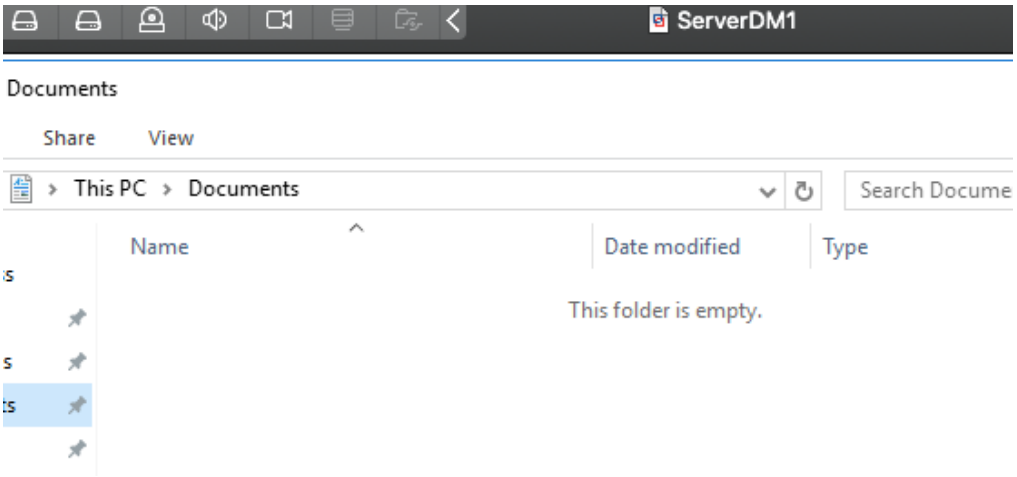
- 4-14-7: Sign in to ServerDM1 as **domadmin1**. Open File Explorer, click **Documents** in the left pane, and delete the **PandP** folder. Sign out of ServerDM1.



- **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.



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