3/17/2021

Hands On Exercise

Chapter 4

Configuring Group Policies

(Part 1)

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

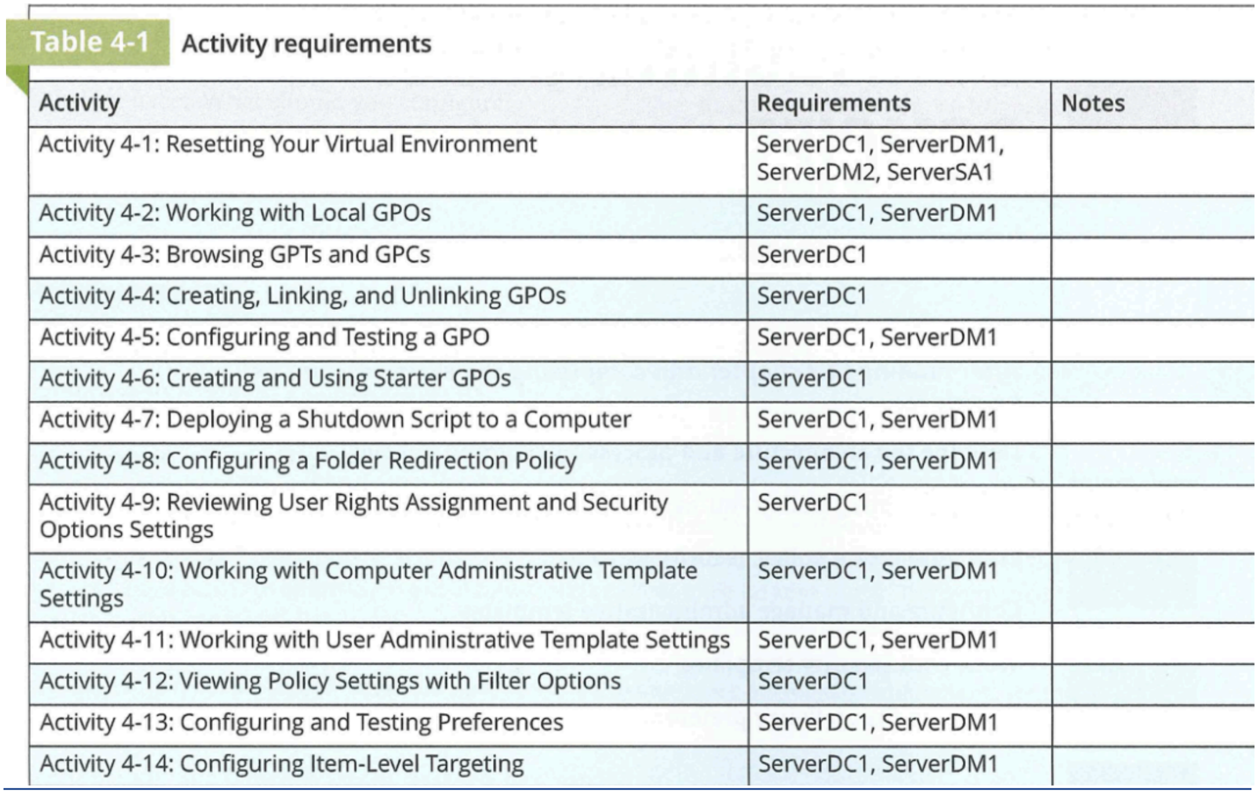


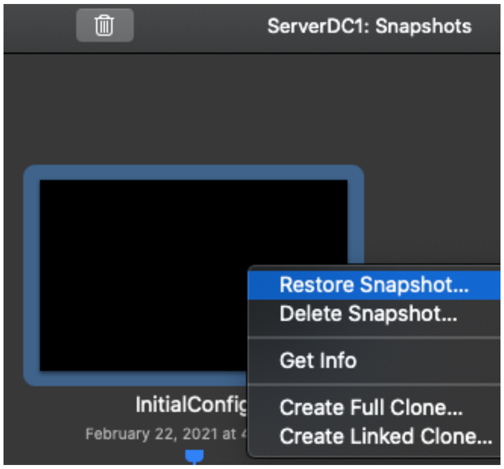
Table 4-1 Activity requirements

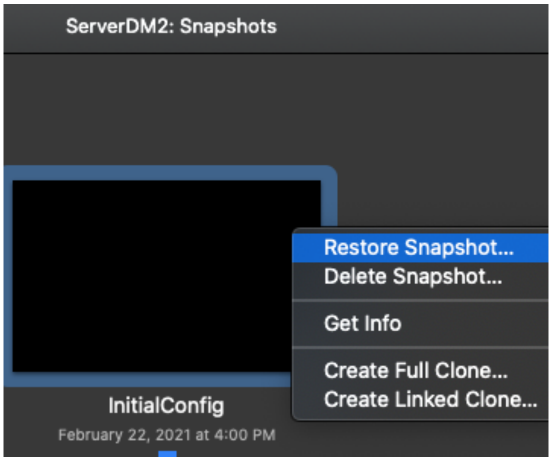
Activity	Requirements	Notes
Activity 4-1: Resetting Your Virtual Environment	ServerDC1, ServerDM1, ServerDM2, ServerSA1	
Activity 4-2: Working with Local GPOs	ServerDC1, ServerDM1	
Activity 4-3: Browsing GPTs and GPCs	ServerDC1	
Activity 4-4: Creating, Linking, and Unlinking GPOs	ServerDC1	
Activity 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	

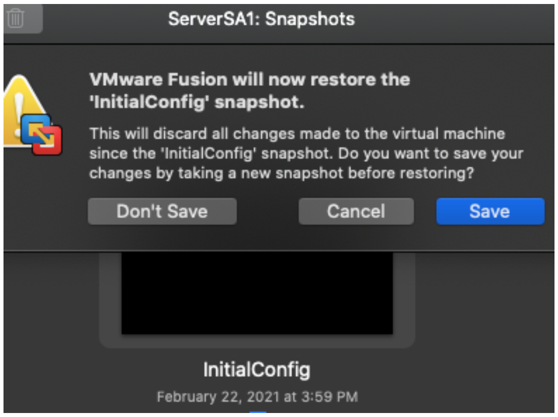
Activity 4-1: Resetting Your Virtual Environment

Description: Apply the lnitialConfig checkpoint or snapshot to ServerDC1, ServerDM1, ServerDM2, and ServerSA1.

- **4-1-1:** Be sure the servers are shut down. In your virtualization program, apply the lnitialConfig checkpoint or snapshot to ServerDC1, ServerDM1, ServerDM2, and ServerSA1.

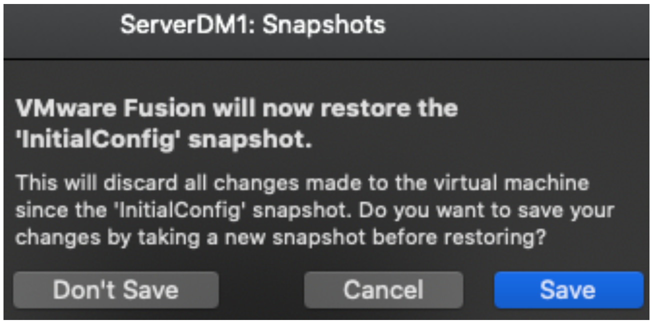






VMware Fusion will now restore the 'InitialConfig' snapshot.

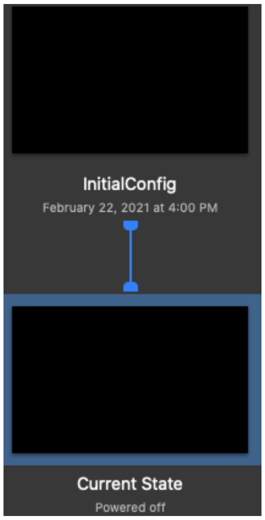
This will discard all changes made to the virtual machine since the 'InitialConfig' snapshot. Do you want to save your changes by taking a new snapshot before restoring?



VMware Fusion will now restore the 'InitialConfig' snapshot.

This will discard all changes made to the virtual machine since the 'InitialConfig' snapshot. Do you want to save your changes by taking a new snapshot before restoring?

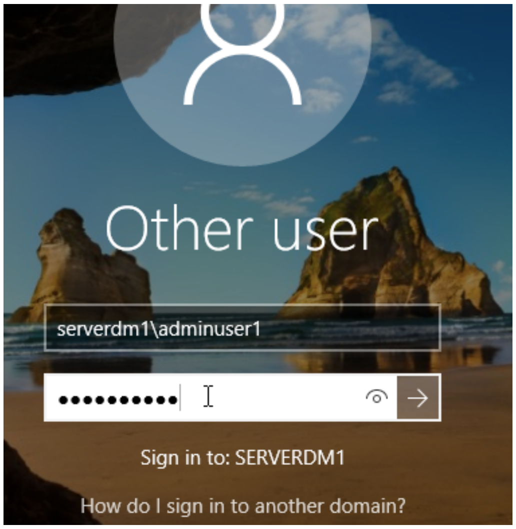
- 4-1-2: When the snapshot or checkpoint has finished being applied, continue to the next activity.



Activity 4-2: Working with Local GPOs

Description: n this activity, you sign in to ServerDM1 with the local Administrator account, configure some local GPOs, and create a local user account. Then you see how local GPOs can affect different users.

- 4-2-1: Sign in to **ServerDM1** with the adminuser1 account. To do so, on the sign in screen, click **Other user,** and then type **serverdm1\adminuser1** in the User name box and **Password01** in the Password box. You must specify that you are signing in to the local computer instead of the domain by prefacing the user name with the name of the computer unless you are signing in as Administrator.



Other user

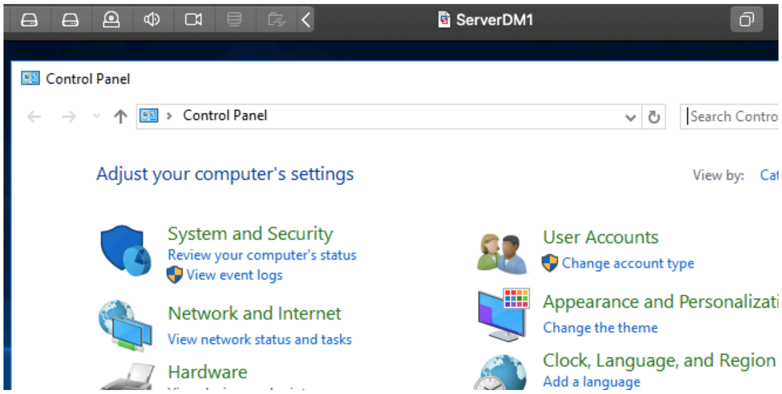
serverdm1\adminuser1

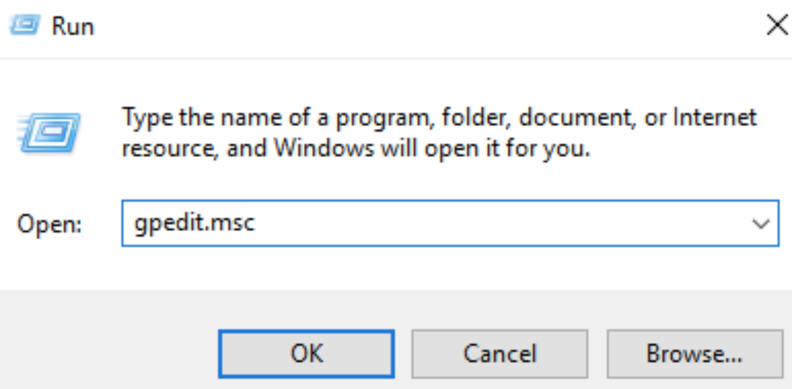
••••••••••

Sign in to: SERVERDM1

How do I sign in to another domain?

- 4-2-2: Right-click **Start** and click **Control Panel** to verify you have access to it, and then close Control Panel. Right- click **Start**, click **Run**, type **gpedit.msc** in the Open text box, and press **Enter** to open the Local Group Policy Editor for the Local Computer Policy GPO.

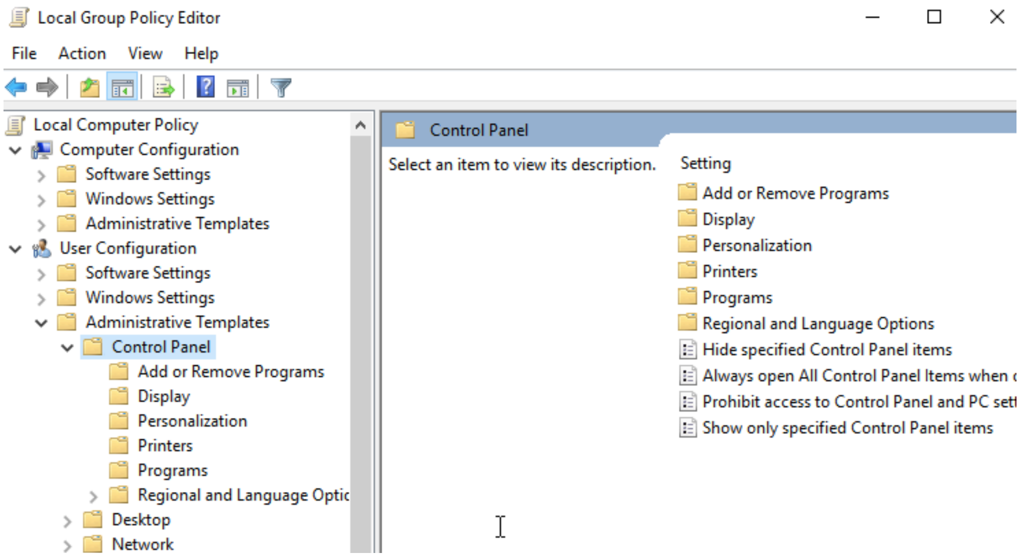




Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

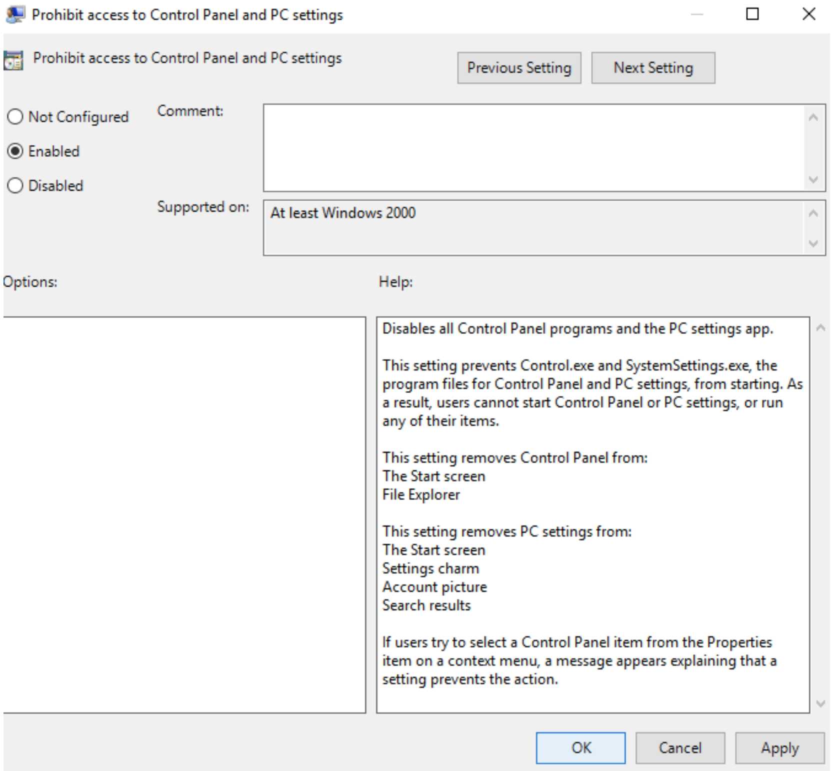
Open: gpedit.msc

- 4-2-3: Click to expand **User Configuration**, **Administrative Templates**, and then click the **Control Panel** node.



Select an item to view its description.

- 4-2-4: In the right pane, double-click **Prohibit access to Control Panel and PC settings**. In the Prohibit access to Control Panel and PC settings dialog box, click **Enabled** (see Figure 4-9) and then click **OK**. Close the Local Group Policy Editor.


Prohibit access to Control Panel and PC settings
Prohibit access to Control Panel and PC settings
Previous Setting
Next Setting
Options:
Help:
OK
Cancel
Apply

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000

Disables all Control Panel programs and the PC settings app.

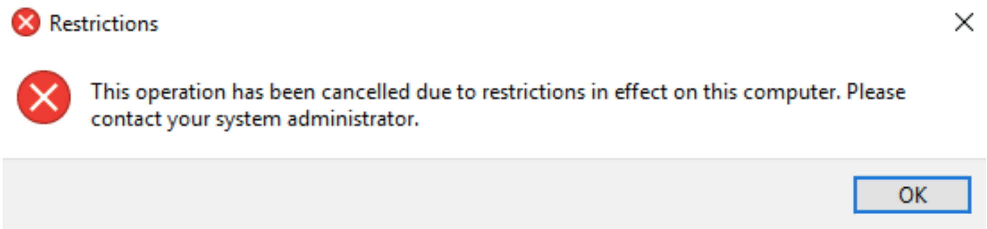
This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.

This setting removes Control Panel from:
The Start screen
File Explorer

This setting removes PC settings from:
The Start screen
Settings charm
Account picture
Search results

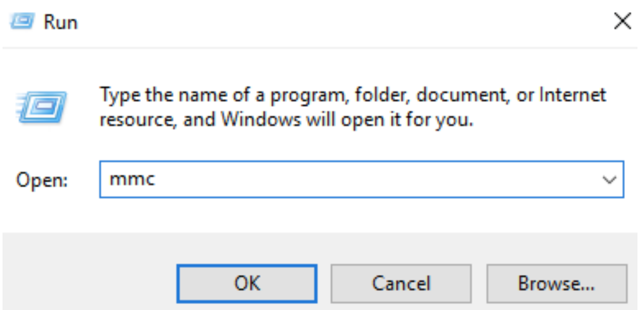
If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a setting prevents the action.

- 4-2-5: Right-click **Start** and click **Control Panel**. You see a message indicating that the action has been canceled because of restrictions in effect on the computer so click **OK**. Close Local Group Policy Editor.



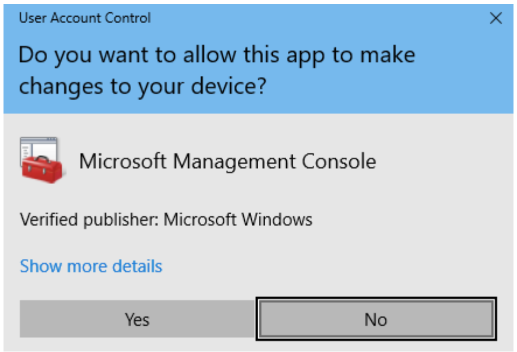
This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.

- 4-2-6: Right-click **Start**, click **Run**, type **mmc** in the Open text box, and press **Enter**.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

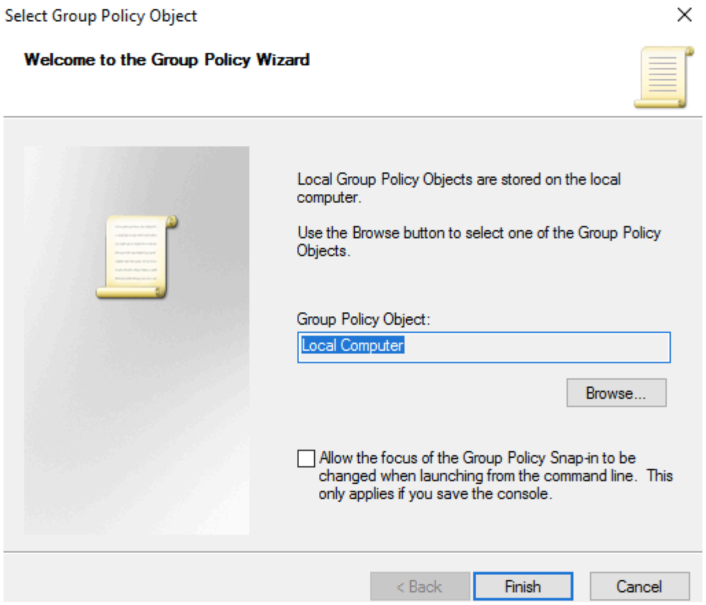


Do you want to allow this app to make changes to your device?

Microsoft Management Console

Verified publisher: Microsoft Windows

- **4-2-7:** In the MMC window, click **File**, **Add/Remove Snap-in** from the menu. In the Available snap-ins list box, click **Group Policy Object Editor**, and then click **Add**. The Group Policy Wizard starts.



Welcome to the Group Policy Wizard

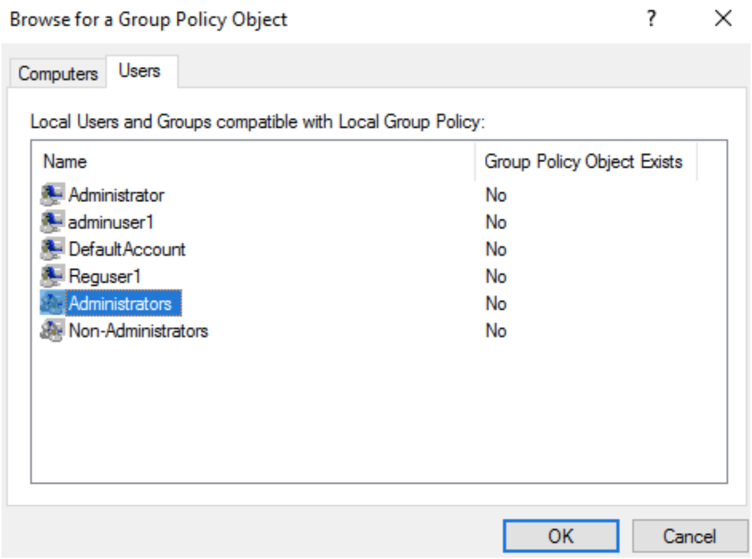
Local Group Policy Objects are stored on the local computer.

Use the Browse button to select one of the Group Policy Objects.

Group Policy Object: Local Computer

□ Allow the focus of the Group Policy Snap-in to be changed when launching from the command line. This only applies if you save the console.

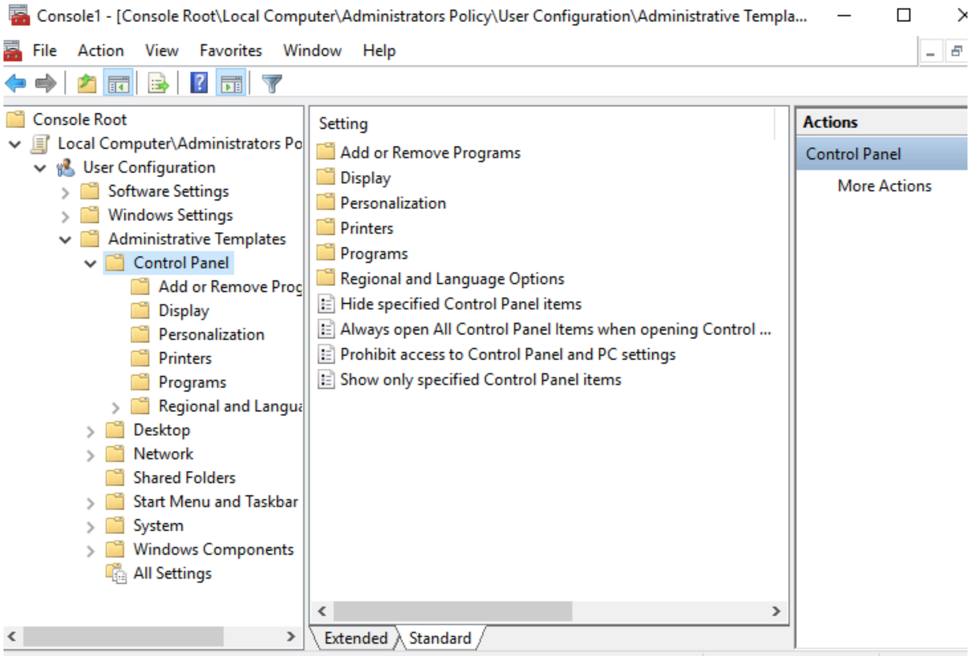
- **4-2-8:** In the Select Group Policy Object window, click **Browse**. In the Browse for a Group Policy Object dialog box, click the **Users** tab. Click **Administrators** (make sure you click the Administrators group, not the Administrator user account), and then click **OK**. Click Finish and then **OK**.



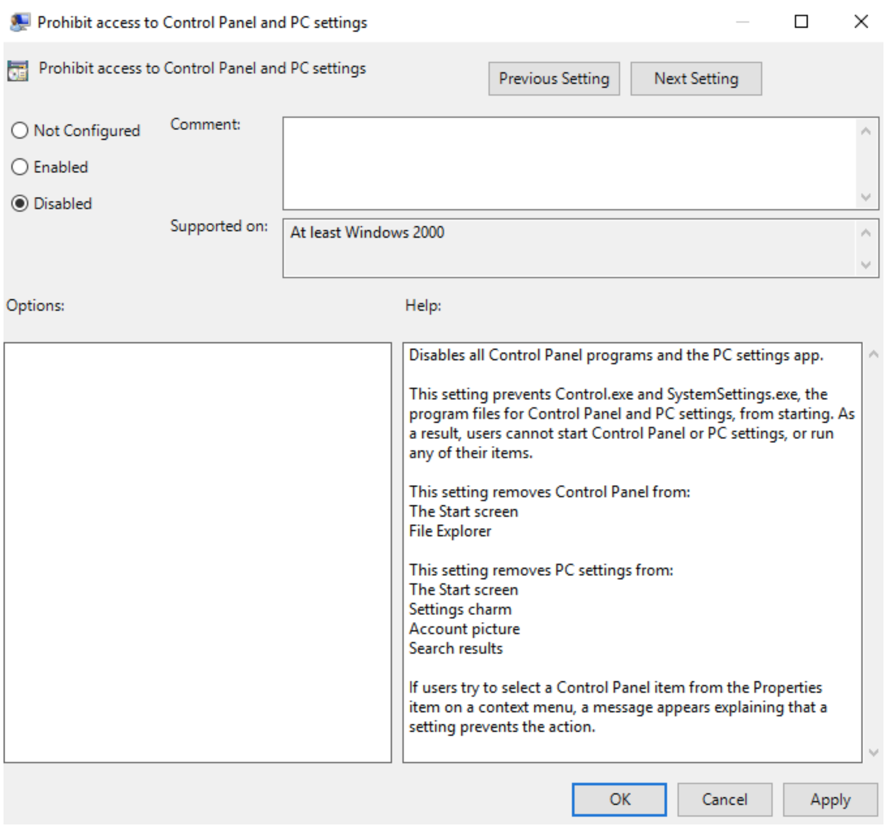
Local Users and Groups compatible with Local Group Policy:

Name	Group Policy Object Exists
Administrator	No
adminuser1	No
DefaultAccount	No
Reguser1	No
Administrators	No
Non-Administrators	No

- **4-2-9:** Click to expand **Local Computer\Administrators Policy**. Click to expand **User Configuration** and **Administrative Templates**, and then click the **Control Panel** node. *(Hint:* You might want to click the Standard tab at the bottom so that you can see the policy setting descriptions better.)



- **4-2-10:** In the right pane, double-click **Prohibit access to Control Panel and PC settings**. In the dialog box for configuring the policy, click **Disabled**, and then click **OK**. Close the MMC window and click No when prompted to save the console settings.



Prohibit access to Control Panel and PC settings

Prohibit access to Control Panel and PC settings

○ Not Configured
○ Enabled
● Disabled

Comment:

Supported on: At least Windows 2000

Options:

Help:

Disables all Control Panel programs and the PC settings app.

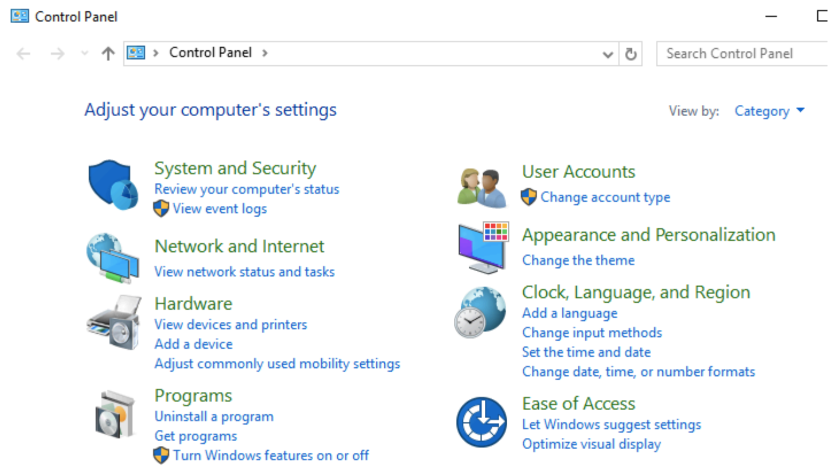
This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.

This setting removes Control Panel from:
The Start screen
File Explorer

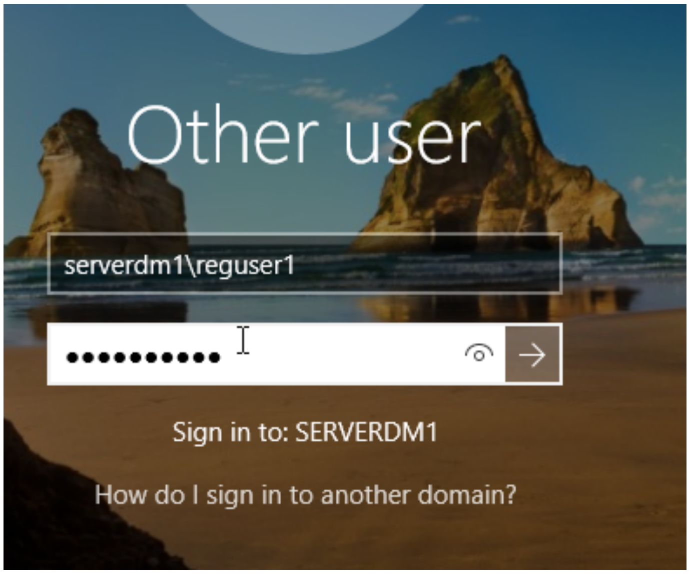
This setting removes PC settings from:
The Start screen
Settings charm
Account picture
Search results

If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a setting prevents the action.

- **4-2-11:** Right-click **Start** and click **Control Panel**, which opens. The Administrators local GPO overrode the Local Computer Policy (because you're signed in as adminuser1, which is a member of the Administrators group). Close Control Panel.



- 4-2-12: Sign out of ServerDM1 and sign back in as **reguser1** with **Password01**. Be sure to enter the user name as **serverdm1\reguser1** so that Windows knows you're signing in to the local computer.


Other user

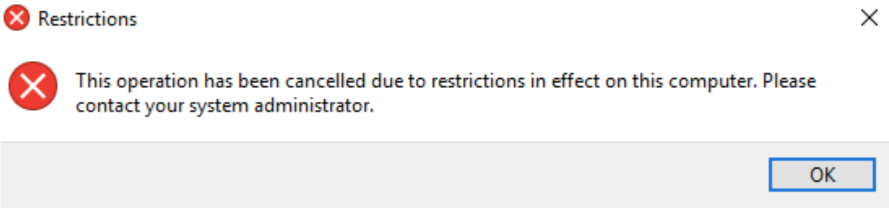
serverdm1\reguser1

●●●●●●●●●●●

Sign in to: SERVERDM1

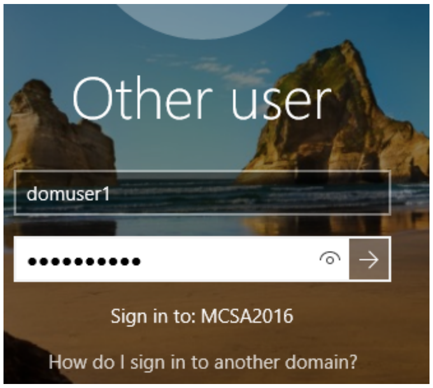
How do I sign in to another domain?

- 4-2-13: Right-click **Start** and click **Control Panel**. You see the same message as you did in Step 5. Click **OK**. Because reguser1 isn't an administrator and doesn't have a user-specific GPO configured, the default Local Computer Policy, which prohibits access to Control Panel, takes effect.


Restrictions

This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.

- 4-2-14: Sign out of ServerDM1, and sign in to the domain as **domuser1** using password **Password01**.

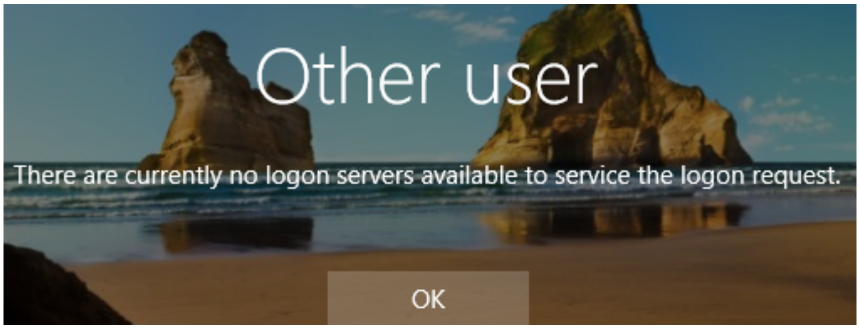

Other user

domuser1

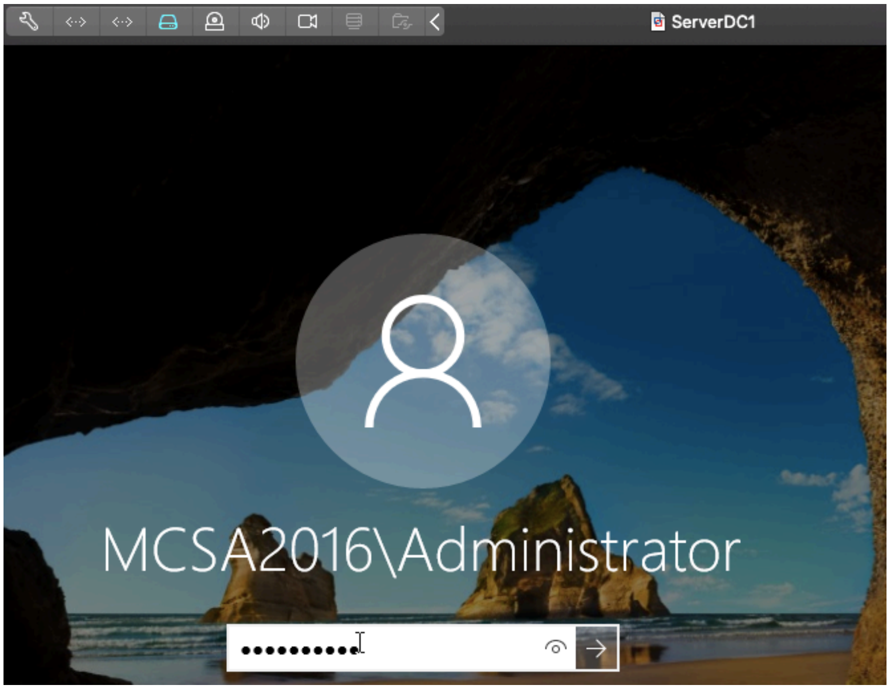
●●●●●●●●●●

Sign in to: MCSA2016

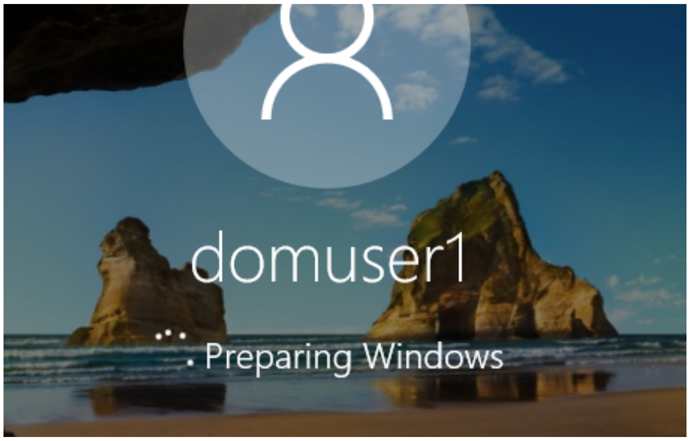
How do I sign in to another domain?



There are currently no logon servers available to service the logon request.

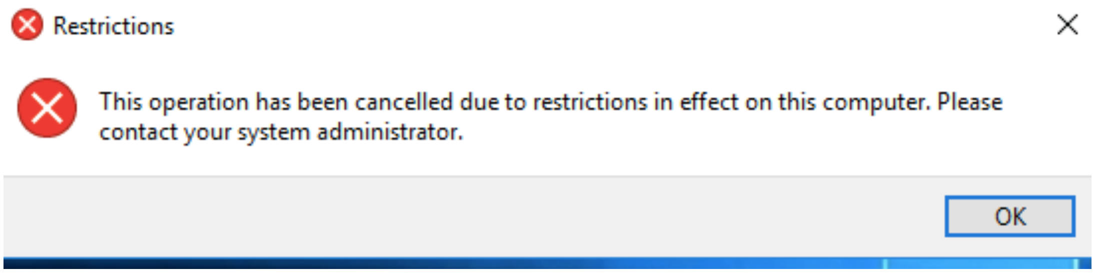


I had to turn on ServerDC1 first



Preparing Windows

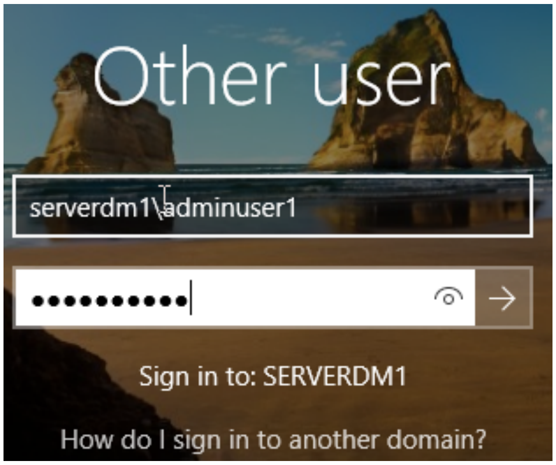
- **4-2-15:** Right-click **Start** and click **Control Panel**. You see the same message as you did in Steps 5 and 13; it demonstrates that the Local Computer Policy affects domain users as well as local users. The only local GPO that doesn't affect domain users is the user-specific GPO. Click **OK**.



Restrictions

This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.

- **4-2-16:** Sign out and sign in to ServerDM1 as **adminuser1**. (Remember to sign in as ServerDM1\adminuser1.) Open the Group Policy Object Editor for the Local Computer Policy (gpedit.msc). Change the Prohibit access to the Control Panel policy back to **Not Configured**, and then click **OK**. Close the Local Group Policy Editor. Sign out of ServerDM1.

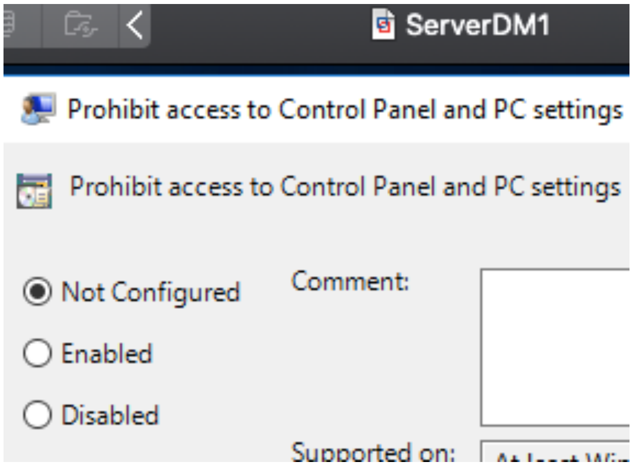


Other user

serverdm1\adminuser1

●●●●●●●●●●●

Sign in to: SERVERDM1



ServerDM1

Prohibit access to Control Panel and PC settings

Prohibit access to Control Panel and PC settings

● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on:

- **4-2-17:** Continue to the next activity.

Press Ctrl+Alt+Delete to unlock.

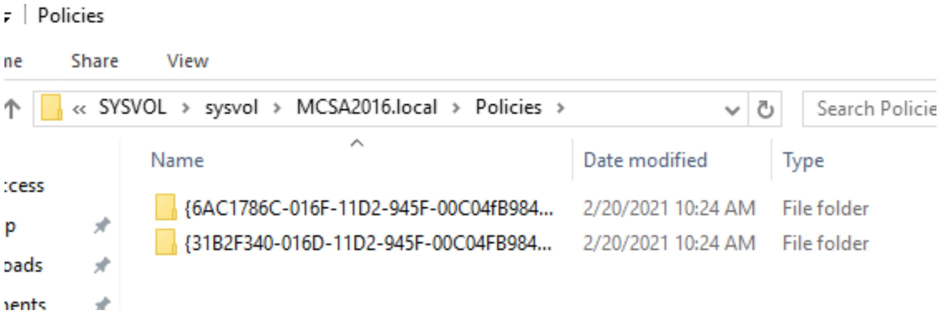
8:10

Friday, March 19

Activity 4-3: Browsing GPTs and GPCs

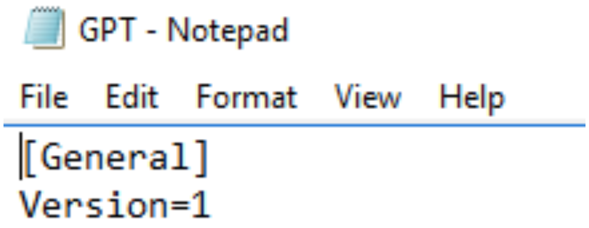
Description: In this activity, you explore the folders where the GPT component of GPOs is located and then you investigate the GPC component in Active Directory.

- 4-3-1: On ServerDC1, open File Explorer, and navigate to **C:\Windows\SYSVOL\sysvol\MCSA2016.local\Policies**, where you should see a list of folders similar to those in Figure 4-3 shown previously.



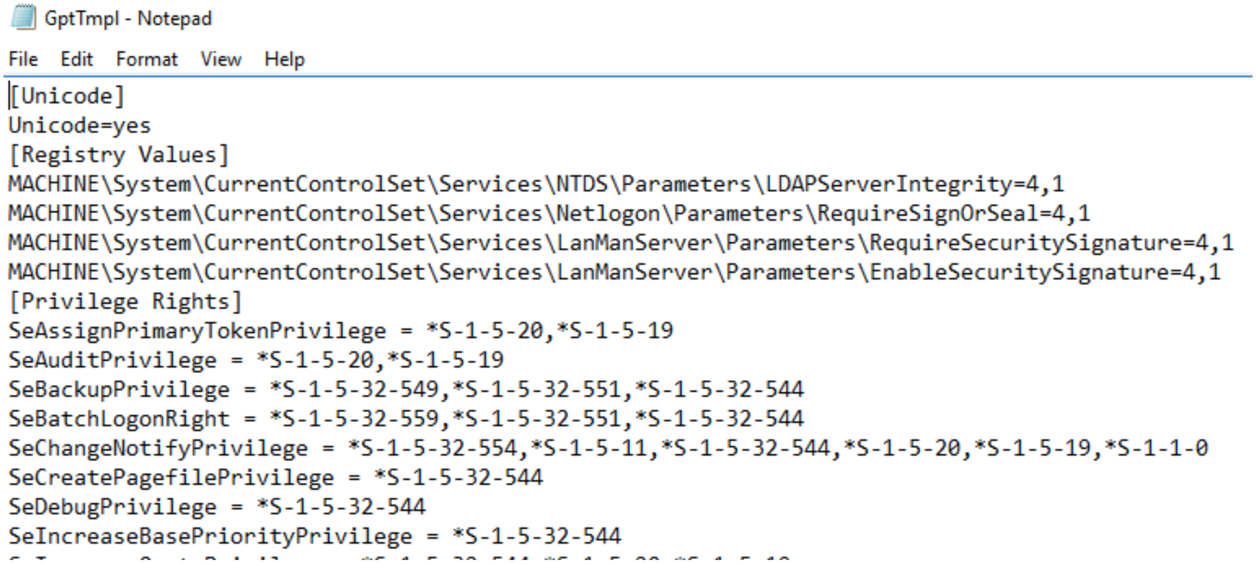
Name	Date modified	Type
{6AC1786C-016F-11D2-945F-00C04fB984...	2/20/2021 10:24 AM	File folder
{31B2F340-016D-11D2-945F-00C04FB984...	2/20/2021 10:24 AM	File folder

- 4-3-2: Double-click the folder starting with **6AC1**, which is the Default Domain Controllers Policy GPT. Double- click the **GPT.ini** file to open it in Notepad. Notice the version number, which changes each time the GPO is modified. Exit Notepad.



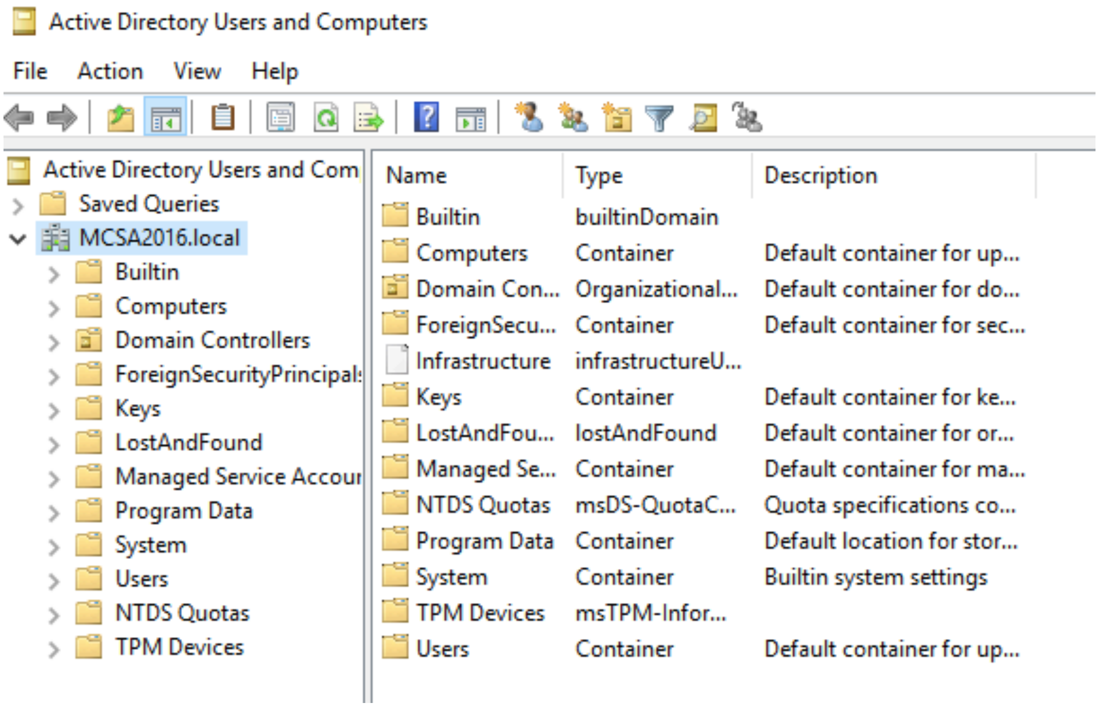
```
[General]
Version=1
```

- **4-3-3:** Click to expand the **MACHINE\Microsoft\Windows NT\SecEdit** folder and double-click the **GptTmpl.inf** file to open it in Notepad. Knowing the details of what's in this and other GPT files isn't important; you just need to know that they exist and how to find them. Exit Notepad.



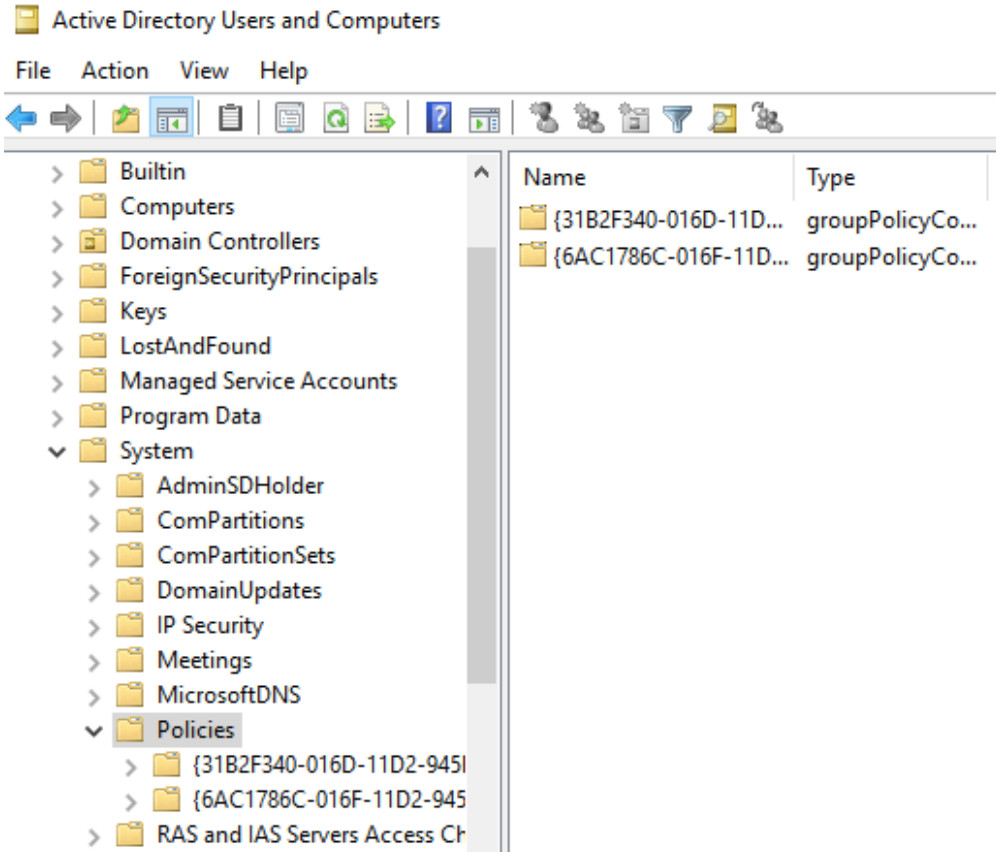
```
[Unicode]
Unicode=yes
[Registry Values]
MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\LDAPServerIntegrity=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
[Privilege Rights]
SeAssignPrimaryTokenPrivilege = *S-1-5-20,*S-1-5-19
SeAuditPrivilege = *S-1-5-20,*S-1-5-19
SeBackupPrivilege = *S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeBatchLogonRight = *S-1-5-32-559,*S-1-5-32-551,*S-1-5-32-544
SeChangeNotifyPrivilege = *S-1-5-32-554,*S-1-5-11,*S-1-5-32-544,*S-1-5-20,*S-1-5-19,*S-1-1-0
SeCreatePagefilePrivilege = *S-1-5-32-544
SeDebugPrivilege = *S-1-5-32-544
SeIncreaseBasePriorityPrivilege = *S-1-5-32-544
```

- **4-3-4:** Open Active Directory Users and Computers. Click **View** on the menu bar and click **Advanced Features** to enable the advanced features option for Active Directory Users and Computers. You'll see a few more folders.



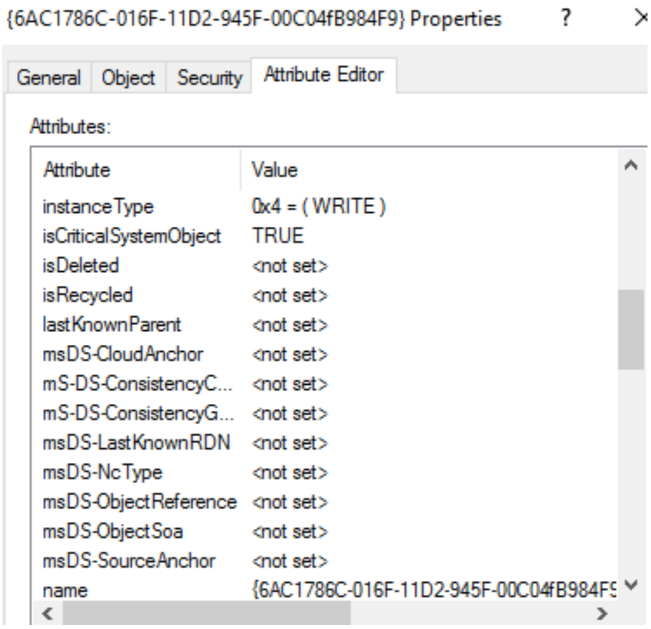
Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Infrastructure	infrastructureU...	
Keys	Container	Default container for ke...
LostAndFou...	lostAndFound	Default container for or...
Managed Se...	Container	Default container for ma...
NTDS Quotas	msDS-QuotaC...	Quota specifications co...
Program Data	Container	Default location for stor...
System	Container	Builtin system settings
TPM Devices	msTPM-Infor...	
Users	Container	Default container for up...

- 4-3-5: Click to expand the **System** folder and then click the **Policies** folder to see the list of GPC folders shown in Figure 4-10.



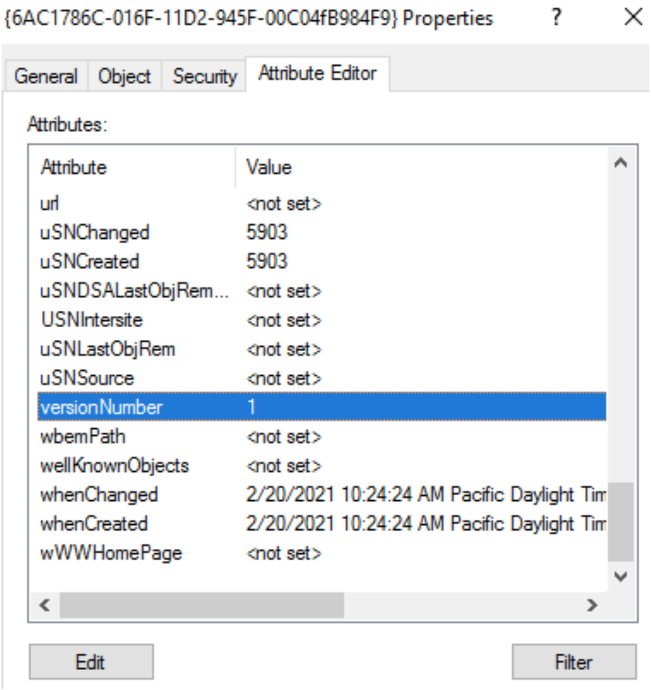
Name	Type
{31B2F340-016D-11D...	groupPolicyCo...
{6AC1786C-016F-11D...	groupPolicyCo...

- 4-3-6: In the right pane, right-click the GPC folder associated with the Default Domain Controllers GPO (the one that starts with **6AC1**) and click **Properties**. In the Properties dialog box, click the **Attribute Editor** tab. Scroll down to view some attributes of the GPC; attributes are listed in alphabetical order. Although you can edit attributes here, it isn't recommended unless you're sure of the results.



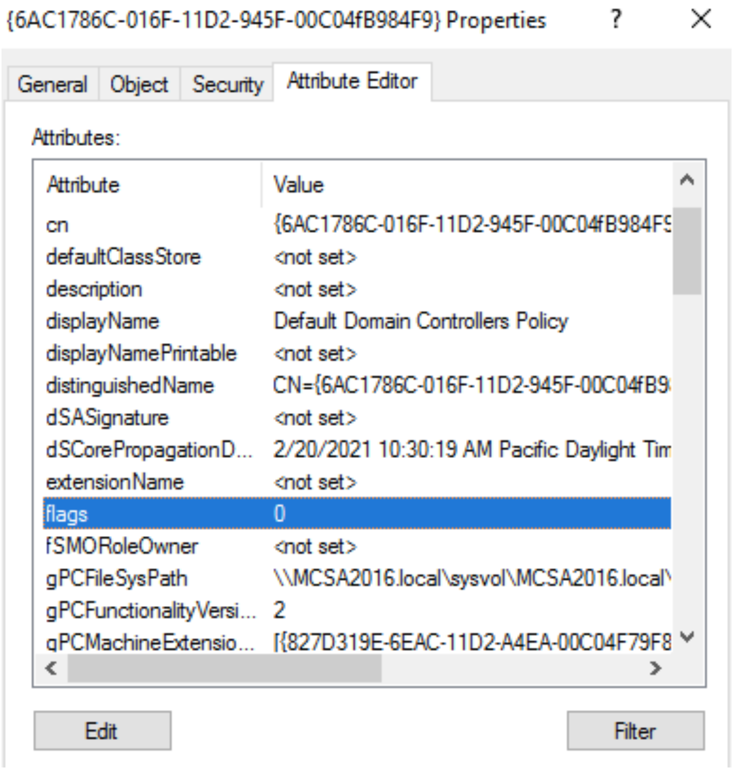
Attribute	Value
instanceType	0x4 = (WRITE)
isCriticalSystemObject	TRUE
isDeleted	<not set>
isRecycled	<not set>
lastKnownParent	<not set>
msDS-CloudAnchor	<not set>
mS-DS-ConsistencyC...	<not set>
mS-DS-ConsistencyG...	<not set>
msDS-LastKnownRDN	<not set>
msDS-NcType	<not set>
msDS-ObjectReference	<not set>
msDS-ObjectSoa	<not set>
msDS-SourceAnchor	<not set>
name	{6AC1786C-016F-11D2-945F-00C04fB984F9

- 4-3-7: Find the **versionNumber** attribute. It should have the same value you noted for the GPT.ini file in Step 2.



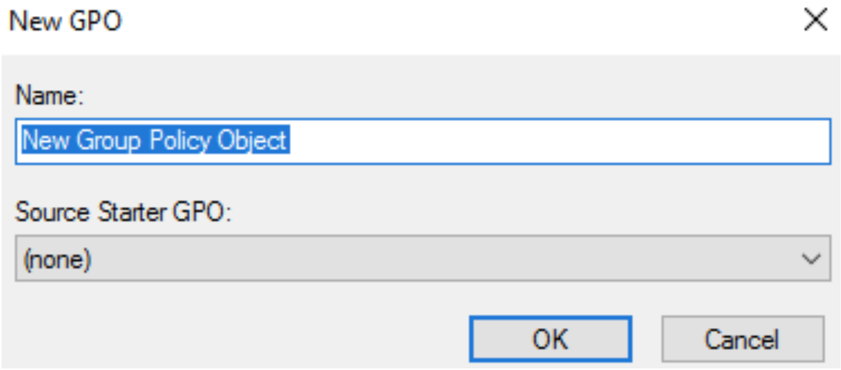
Attribute	Value
url	<not set>
uSNChanged	5903
uSNCreated	5903
uSNDSALastObjRem...	<not set>
USNIntersite	<not set>
uSNLastObjRem	<not set>
uSNSource	<not set>
versionNumber	1
wbemPath	<not set>
wellKnownObjects	<not set>
whenChanged	2/20/2021 10:24:24 AM Pacific Daylight Tim
whenCreated	2/20/2021 10:24:24 AM Pacific Daylight Tim
wWWHomePage	<not set>

- **4-3-8:** Find the **flags** attribute. Its value should be 0, indicating that the GPO is enabled. Click **Cancel.**



Attribute	Value
cn	{6AC1786C-016F-11D2-945F-00C04fB984F9
defaultClassStore	<not set>
description	<not set>
displayName	Default Domain Controllers Policy
displayNamePrintable	<not set>
distinguishedName	CN={6AC1786C-016F-11D2-945F-00C04fB9
dSASignature	<not set>
dSCorePropagationD...	2/20/2021 10:30:19 AM Pacific Daylight Tim
extensionName	<not set>
flags	0
fSMORoleOwner	<not set>
gPCFileSysPath	\\MCSA2016.local\sysvol\MCSA2016.local\
gPCFunctionalityVersi...	2
gPCMachineExtensio...	[{827D319E-6EAC-11D2-A4EA-00C04F79F8

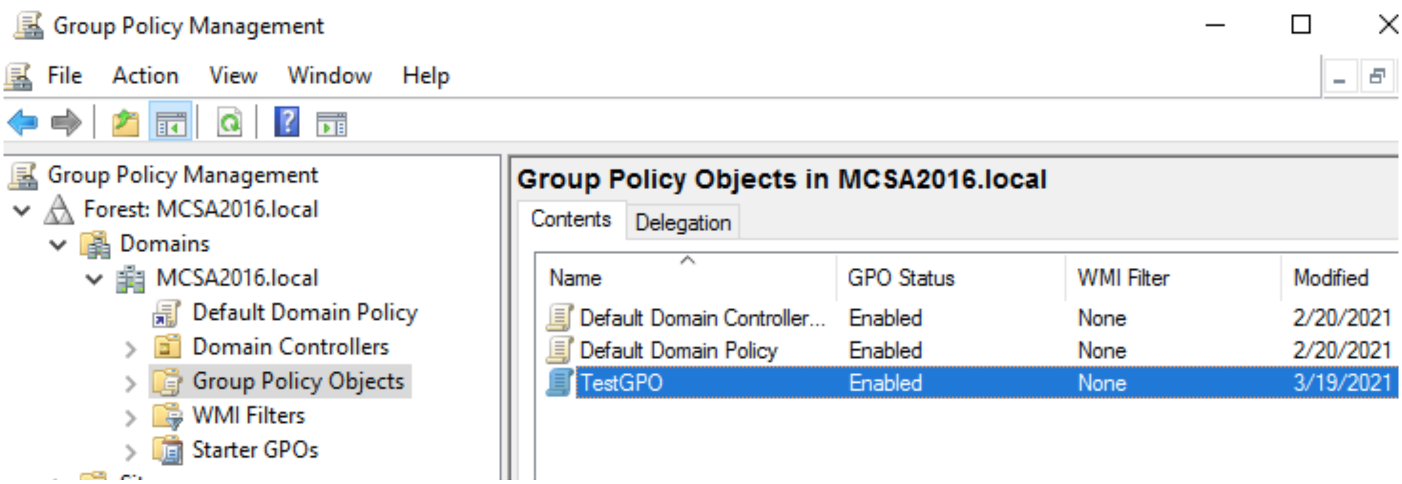
- **4-3-9:** Open the Group Policy Management console from the **Tools** menu in Server Manager. In the left pane, navigate to the **Group Policy Objects folder.** Right-click the **Group Policy Objects** folder and click **New.**



Name: New Group Policy Object

Source Starter GPO: (none)

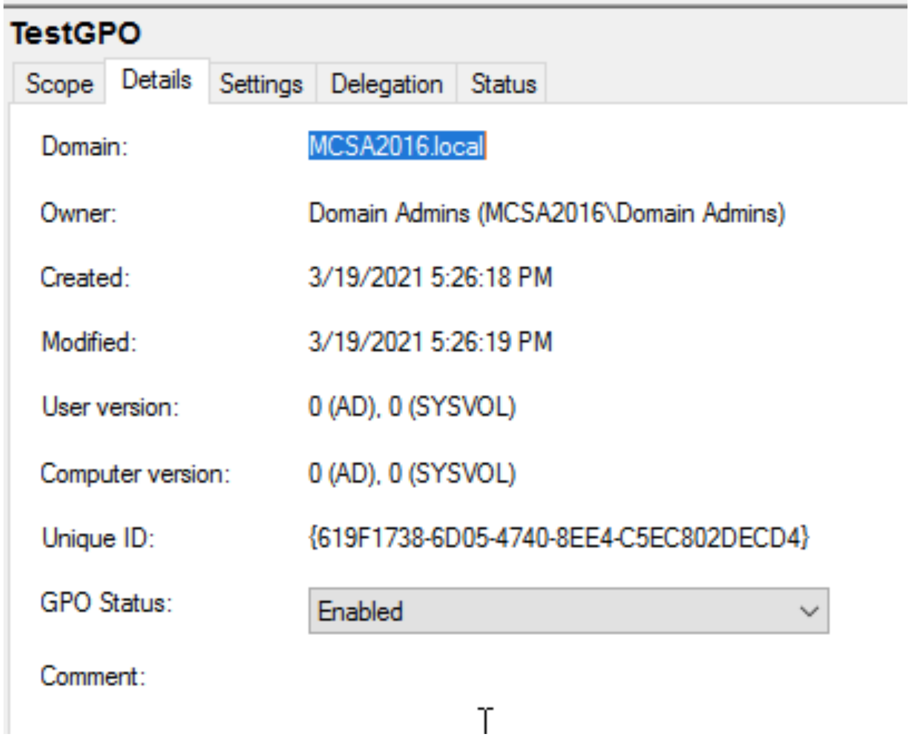
- **4-3-10:** In the New GPO dialog box, type **TestGPO** in the Name box and click **OK.**



Group Policy Objects in MCSA2016.local

Name	GPO Status	WMI Filter	Modified
Default Domain Controller...	Enabled	None	2/20/2021
Default Domain Policy	Enabled	None	2/20/2021
TestGPO	Enabled	None	3/19/2021

- **4-3-11:** Click **TestGPO** in the left pane, and in the right pane, click the **Details** tab.



Domain: MCSA2016.local

Owner: Domain Admins (MCSA2016\Domain Admins)

Created: 3/19/2021 5:26:18 PM

Modified: 3/19/2021 5:26:19 PM

User version: 0 (AD), 0 (SYSVOL)

Computer version: 0 (AD), 0 (SYSVOL)

Unique ID: {619F1738-6D05-4740-8EE4-C5EC802DECD4}

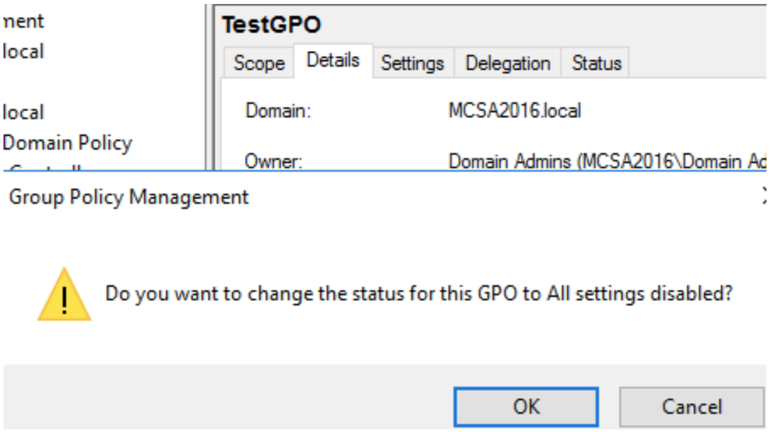
GPO Status: Enabled

Comment:

- **4-3-12:** Click the **GPO Status** list arrow, click **All settings disabled** (see Figure 4-11), and then click **OK.**

In Active Directory Users and Computers, click the **Refresh** icon to see that a new folder has been added under Policies. Open the Properties dialog box of the GPC folder associated with TestGPO (the folder that does *not* start with 6AC1 or 31

B2). Click the **Attribute Editor** tab and then view the value of the flags attribute. It's 3, indicating that the GPO is disabled.



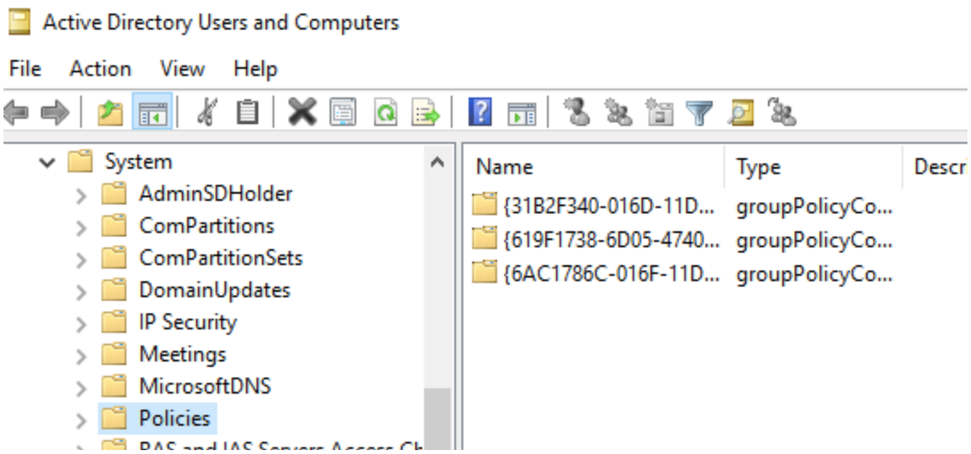
TestGPO

Domain: MCSA2016.local

Owner: Domain Admins (MCSA2016\Domain Ad

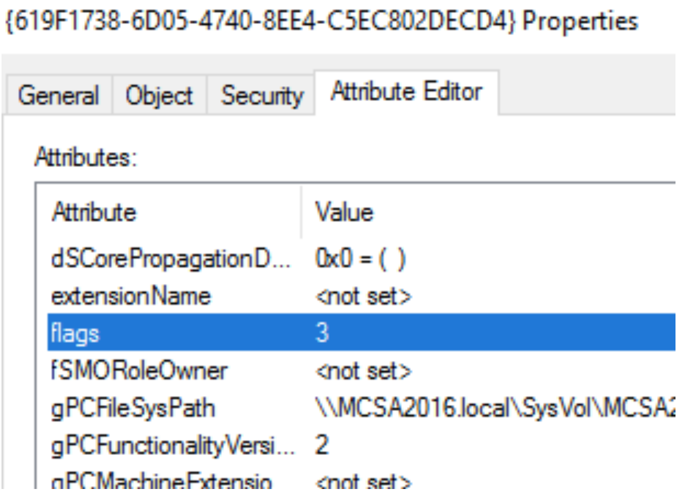
Group Policy Management

Do you want to change the status for this GPO to All settings disabled?



Active Directory Users and Computers

Name	Type	Descr
{31B2F340-016D-11D...	groupPolicyCo...	
{619F1738-6D05-4740...	groupPolicyCo...	
{6AC1786C-016F-11D...	groupPolicyCo...	

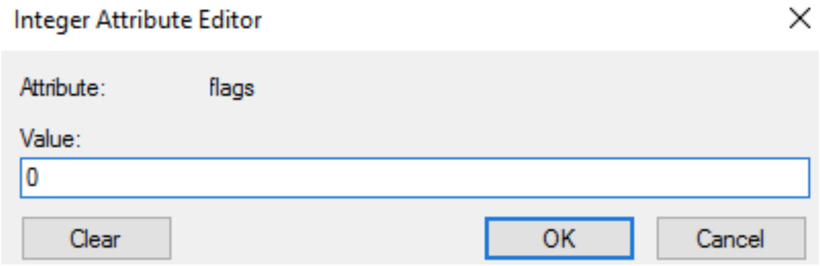


{619F1738-6D05-4740-8EE4-C5EC802DECD4} Properties

Attributes:

Attribute	Value
dSCorePropagationD...	0x0 = ( )
extensionName	<not set>
flags	3
fSMORoleOwner	<not set>
gPCFileSysPath	\\MCSA2016.local\SysVol\MCSA2
gPCFunctionalityVersi...	2
gPCMachineExtensio	<not set>

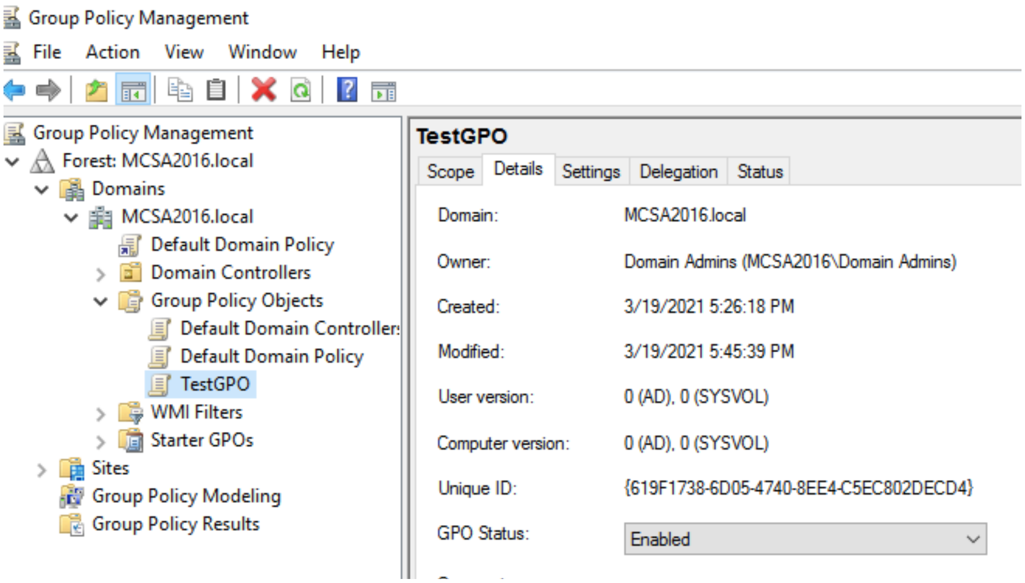
- 4-3-13: Click the **flags** attribute and click the Edit button. Type **0,** and then click **OK** twice. Close Active Directory Users and Computers.



Attribute: flags

Value: 0

- 4-3-14: In the Group Policy Management console, click the **Refresh** icon. The GPO status changes to Enabled because you changed the flag's attribute to 0. Close the Group Policy Management console.



Domain: MCSA2016.local

Owner: Domain Admins (MCSA2016\Domain Admins)

Created: 3/19/2021 5:26:18 PM

Modified: 3/19/2021 5:45:39 PM

User version: 0 (AD), 0 (SYSVOL)

Computer version: 0 (AD), 0 (SYSVOL)

Unique ID: {619F1738-6D05-4740-8EE4-C5EC802DECD4}

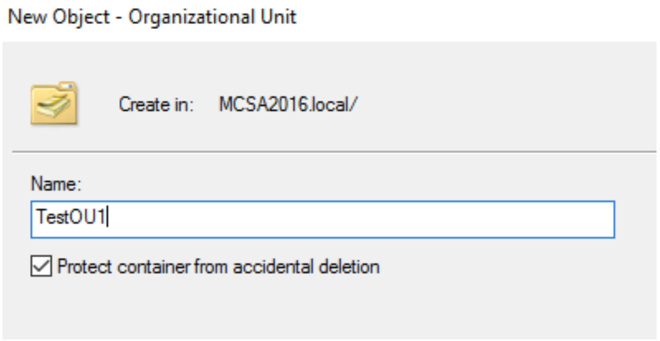
GPO Status: Enabled

- 4-3-15: Continue to the next activity.

Activity 4-4: Creating, Linking, and Unlinking GPOs

Description: In this activity, you create an OU and GPO and work with GPO links.

- **4-4-1:** On ServerDC1, open Active Directory Users and Computers, and create an OU named **TestOU1** under the domain node.



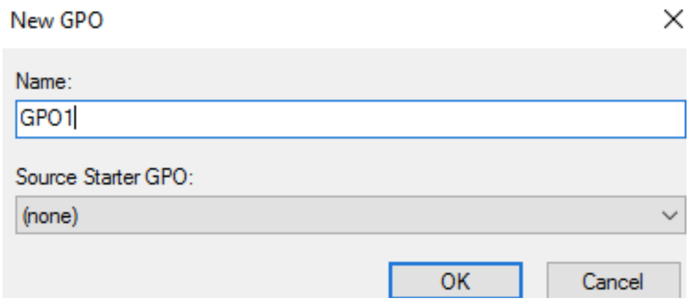
New Object - Organizational Unit

Create in: MCSA2016.local/

Name: TestOU1

☑ Protect container from accidental deletion

- **4-4-2:** Open the Group Policy Management console. Right-click **TestOU1** and click **Create a GPO in this domain, and Link it here.** In the New GPO dialog box, type GPO1 in the Name text box, and then click **OK**.

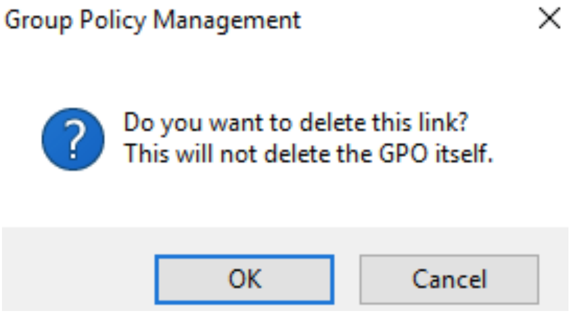


New GPO

Name: GPO1

Source Starter GPO: (none)

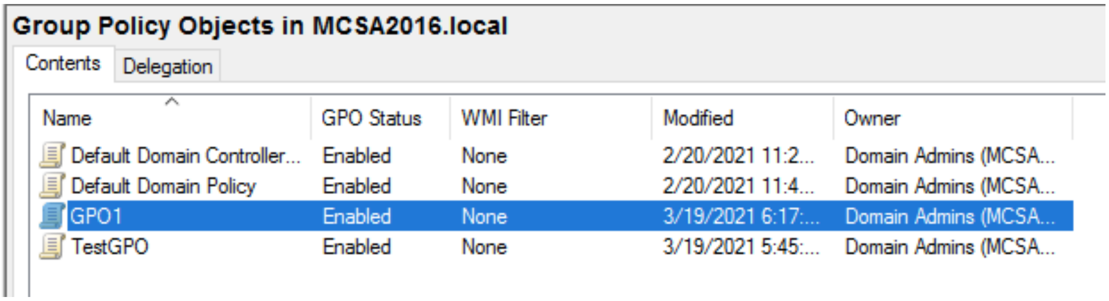
- **4-4-3:** In the right pane, notice that GPO1 is listed as Enabled. Changes you make to GPO1 affect any user or computer accounts that might be in TestOU1. Right-click **GPO1** and click **Delete**. Click **OK**. This action deletes only the link to the GPO, not the GPO itself.



Group Policy Management

Do you want to delete this link?
This will not delete the GPO itself.

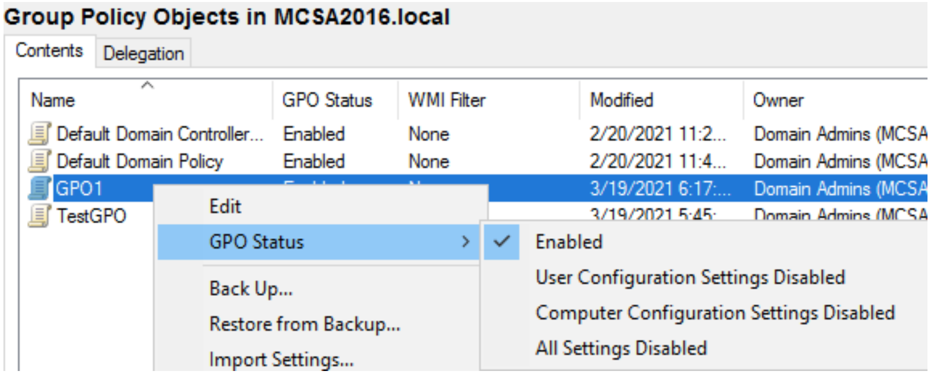
- 4-4-4: Click the **Group Policy Objects** folder to see all your GPOs, including the default GPOs.



Group Policy Objects in MCSA2016.local

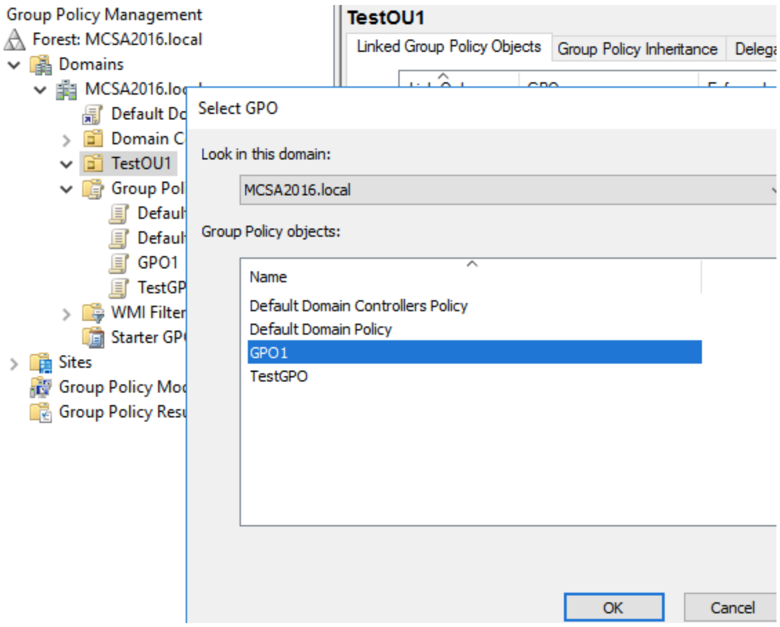
Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controller...	Enabled	None	2/20/2021 11:2...	Domain Admins (MCSA...
Default Domain Policy	Enabled	None	2/20/2021 11:4...	Domain Admins (MCSA...
GPO1	Enabled	None	3/19/2021 6:17:...	Domain Admins (MCSA...
TestGPO	Enabled	None	3/19/2021 5:45:...	Domain Admins (MCSA...

- 4-4-5: Right-click **GPO1** and point to **GPO Status**. You can enable or disable a GPO or just disable the Computer Configuration or User Configuration settings.



Group Policy Objects in MCSA2016.local

- 4-4-6: Right-click the **TestOU1** OU and click **Link an Existing GPO**. In the Select GPO dialog box, click GPO1, and then click **OK.**

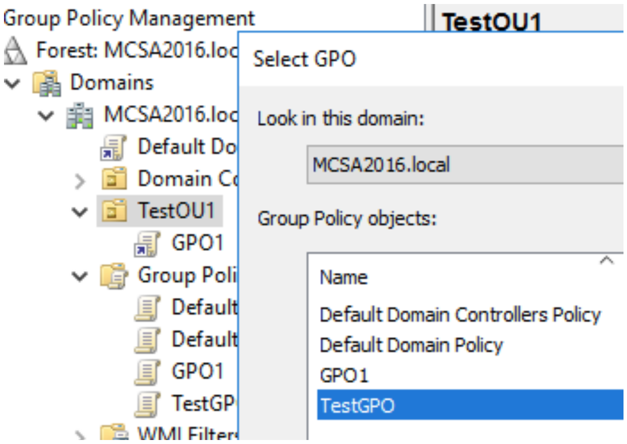


Look in this domain: MCSA2016.local

Group Policy objects:

Name
Default Domain Controllers Policy
Default Domain Policy
GPO1
TestGPO

- 4-4-7: To link another GPO to test **TestOU1**, right-click **TestOU1** and click **Link an Existing GPO**. Click **TestGPO** and then click **OK.**



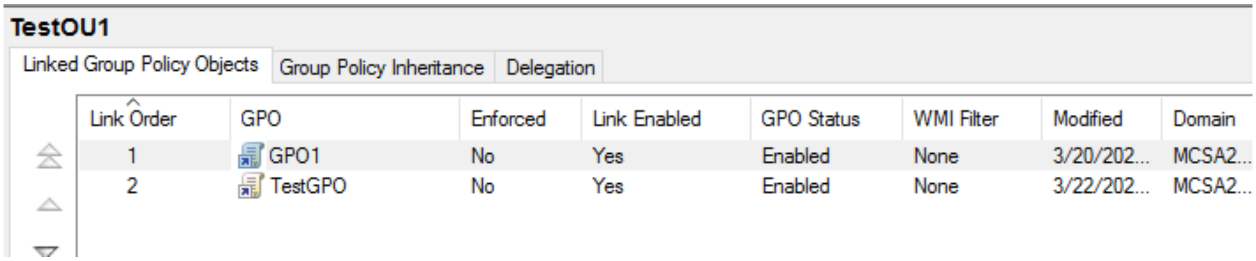
Select GPO

Look in this domain: MCSA2016.local

Group Policy objects:

Name
Default Domain Controllers Policy
Default Domain Policy
GPO1
TestGPO

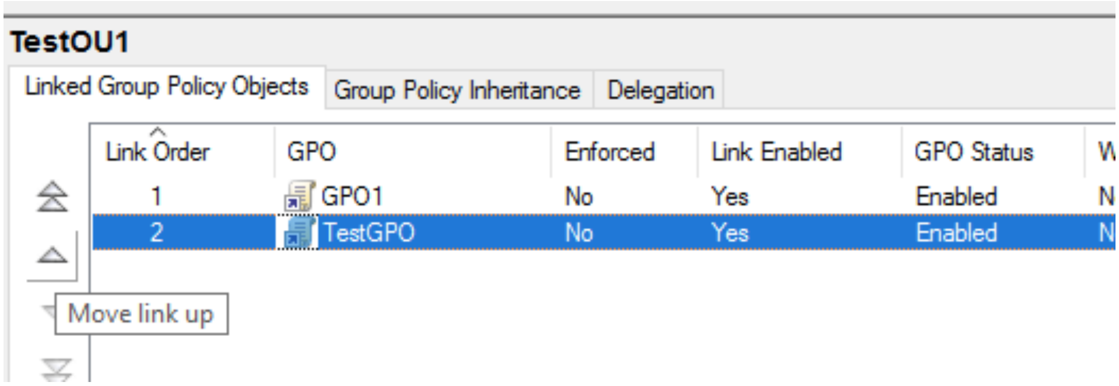
- 4-4-8: Click **TestOU1**. Notice that both GPO1 and TestGPO are linked to TestOU1. If both GPOs had the same policy setting configured but with different values, the value of the policy setting in GPO1 would take precedence because it would be applied last.



TestOU1

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	GPO1	No	Yes	Enabled	None	3/20/202...	MCSA2...
2	TestGPO	No	Yes	Enabled	None	3/22/202...	MCSA2...

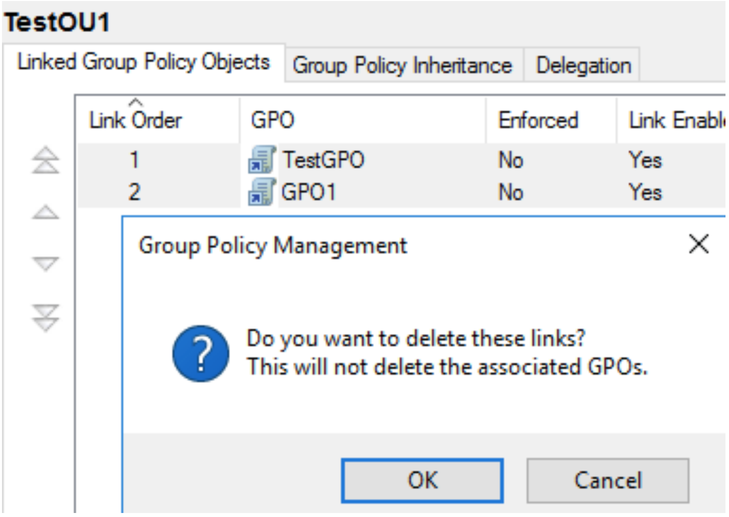
- 4-4-9: Click **TestGPO** in the right pane and click the **up arrow** to the left of the Link Order column. TestGPO now has link order 1, and GPO1 has link order 2, so TestGPO takes precedence if any settings conflict.



TestOU1

Link Order	GPO	Enforced	Link Enabled	GPO Status	W
1	GPO1	No	Yes	Enabled	N
2	TestGPO	No	Yes	Enabled	N

- **4-4-10:** Right-click **TestGPO** and click **Delete**. Click **OK** in the message box asking you to confirm the deletion. Next, right-click **GPO1** and click **Delete**, and then click **OK**. No policies should be linked to TestOU1 now.



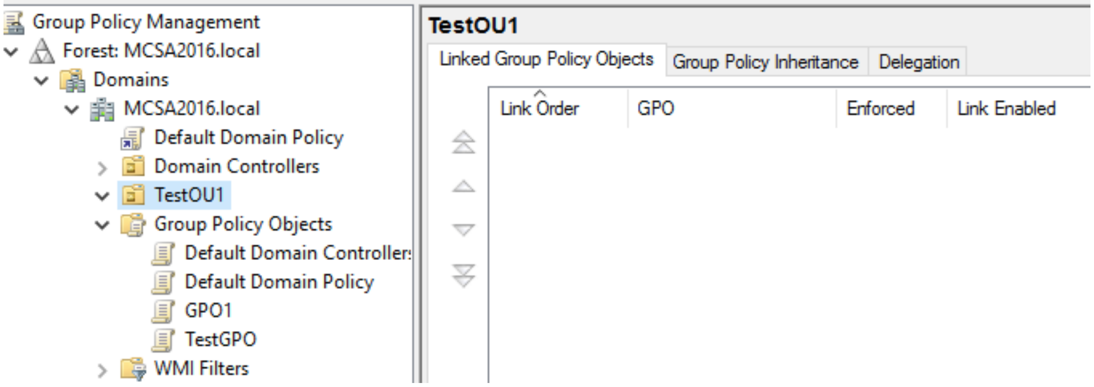
TestOU1

Link Order	GPO	Enforced	Link Enabl
1	TestGPO	No	Yes
2	GPO1	No	Yes

Group Policy Management

Do you want to delete these links?
This will not delete the associated GPOs.

- **4-4-11:** Continue to the next activity.



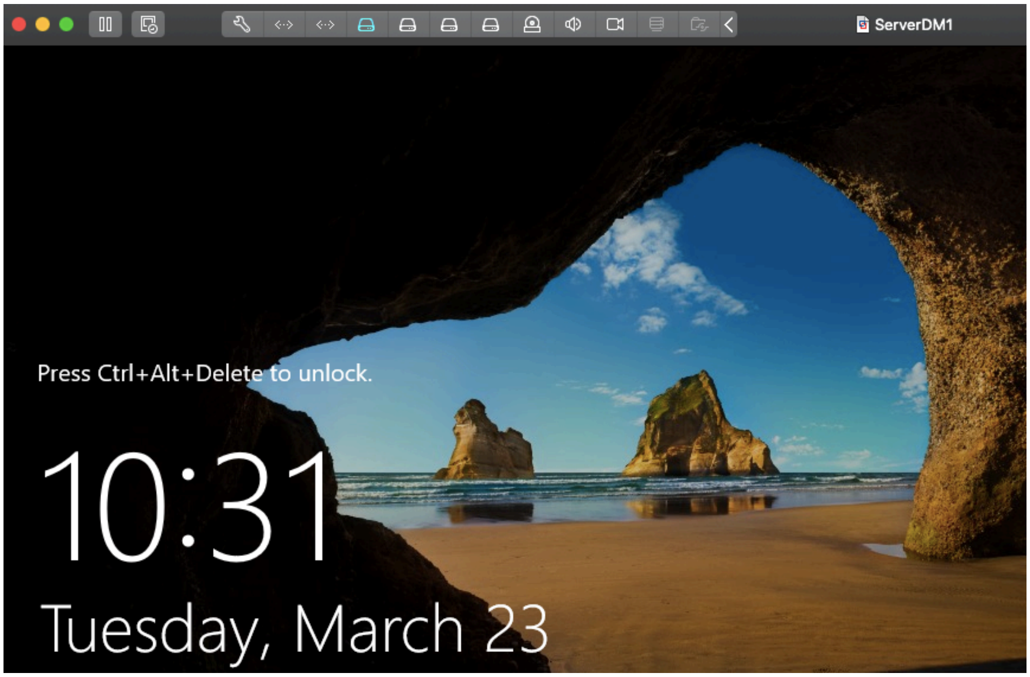
TestOU1

Link Order	GPO	Enforced	Link Enabled

Activity 4-5: Configuring and Testing a GPO

Description: In this activity, you move the ServerDM1 computer account to TestOU1 and test some computer settings by configuring GPO1.

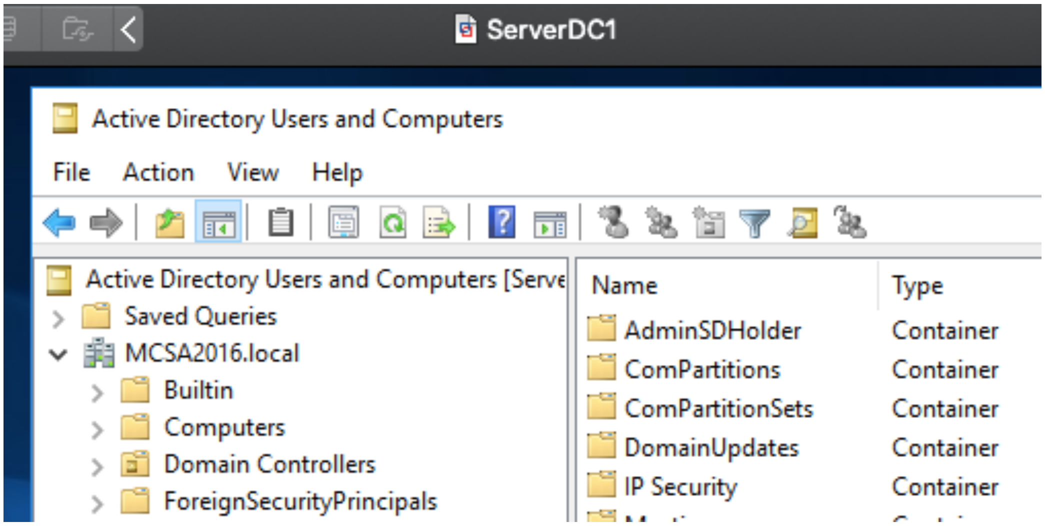
- 4-5-1: Start ServerDM1. On ServerDC1, open Active Directory Users and Computers, if necessary.


ServerDM1

Press Ctrl+Alt+Delete to unlock.

10:31

Tuesday, March 23

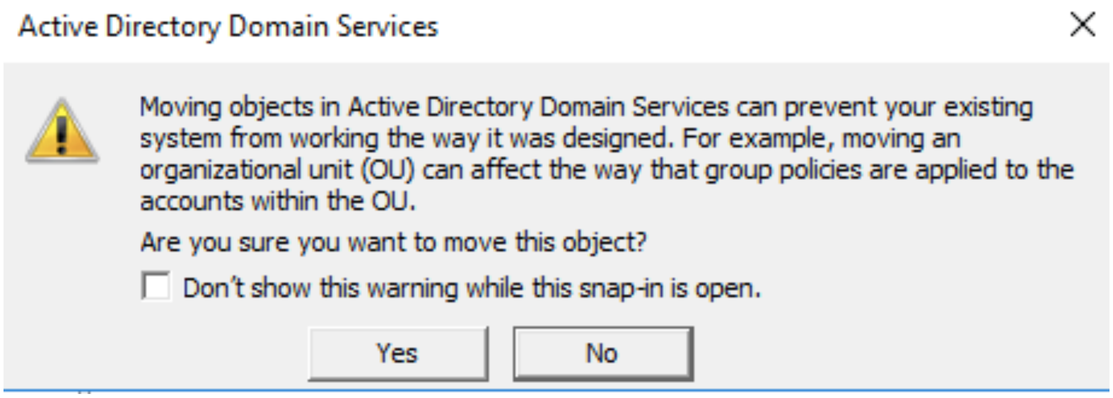

ServerDC1

Active Directory Users and Computers

Active Directory Users and Computers [Serve
- Saved Queries
- MCSA2016.local
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals

Name	Type
AdminSDHolder	Container
ComPartitions	Container
ComPartitionSets	Container
DomainUpdates	Container
IP Security	Container

- 4-5-2: Click the **Computers** folder and drag the **ServerDM1** computer account to the **TestOU1** OU. If necessary, click **Yes** in the warning message about moving Active Directory objects.



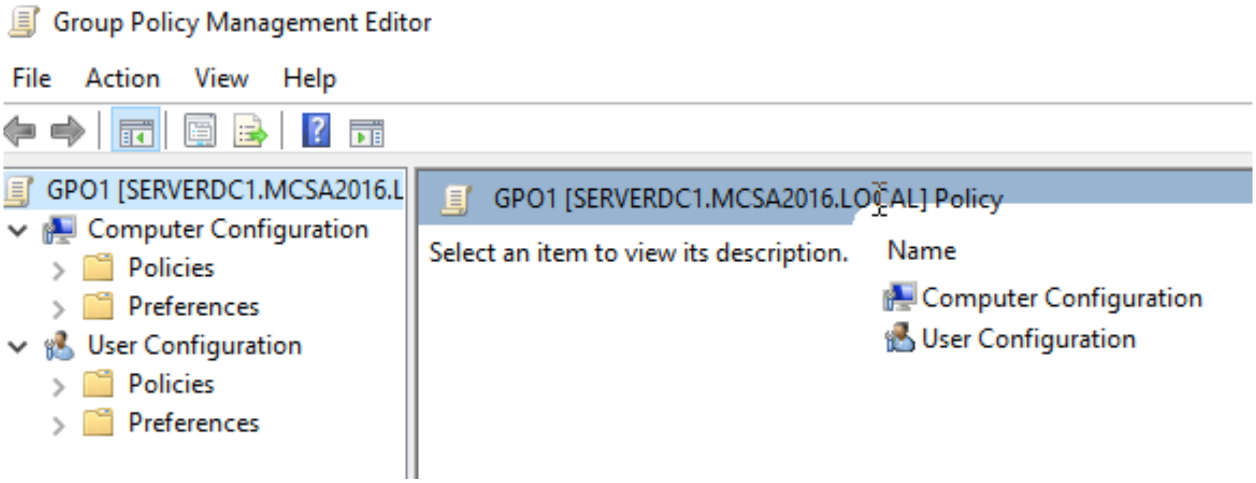
Active Directory Domain Services

Moving objects in Active Directory Domain Services can prevent your existing system from working the way it was designed. For example, moving an organizational unit (OU) can affect the way that group policies are applied to the accounts within the OU.

Are you sure you want to move this object?

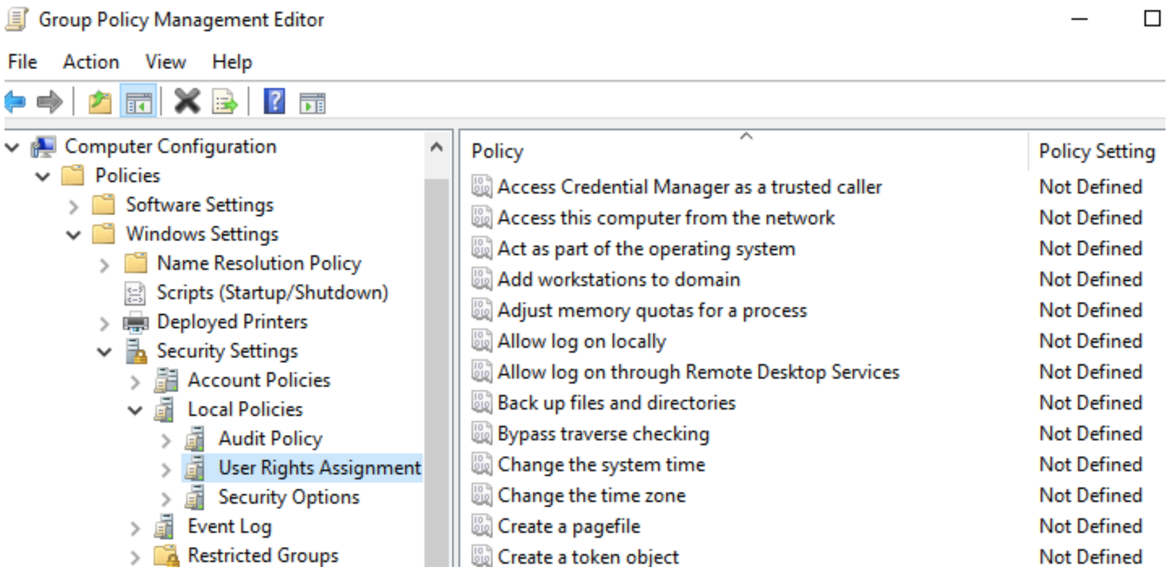
□ Don't show this warning while this snap-in is open.

- **4-5-3:** Open the Group Policy Management console, if necessary. Right-click **TestOU1** and click **Link an Existing GPO**. Click **GPO1** and then click **OK**. Right-click **GPO1** and click **Edit** to open it in the Group Policy Management Editor.



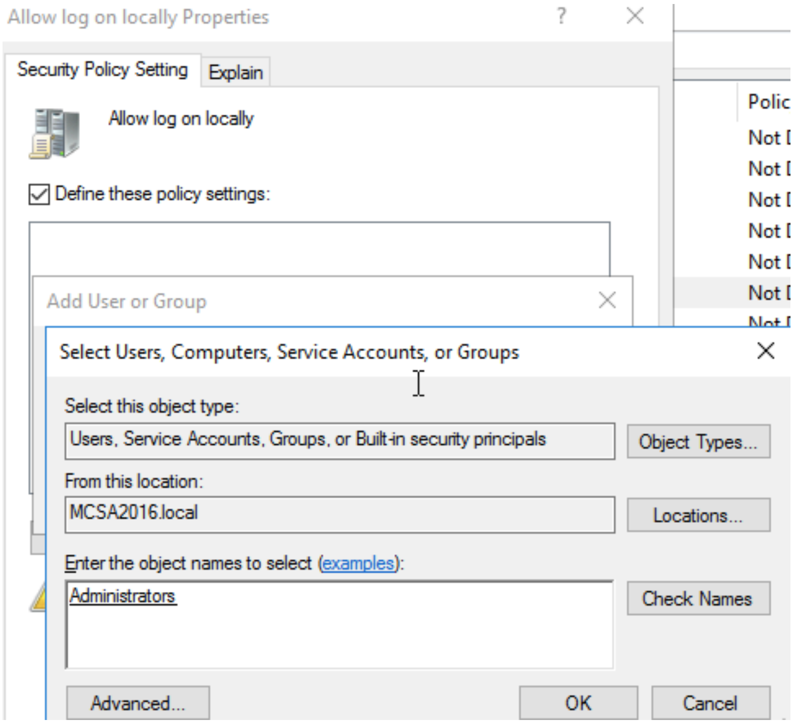
Select an item to view its description.

- **4-5-4:** Click to expand **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, and **Local Policies**, and then click **User Rights Assignment**.



Policy	Policy Setting
Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	Not Defined
Act as part of the operating system	Not Defined
Add workstations to domain	Not Defined
Adjust memory quotas for a process	Not Defined
Allow log on locally	Not Defined
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Not Defined
Bypass traverse checking	Not Defined
Change the system time	Not Defined
Change the time zone	Not Defined
Create a pagefile	Not Defined
Create a token object	Not Defined

- **4-5-5:** In the right pane, double-click **Allow log on locally** to open its Properties dialog box. Notice that the policy setting is currently not defined. Click the **Define these policy settings** check box, and then click **Add User or Group**. In the Add User or Group dialog box, click **Browse**. Type **Administrators** in the *Enter the object names to select* text box and click **Check Names**. Click **OK** three times.



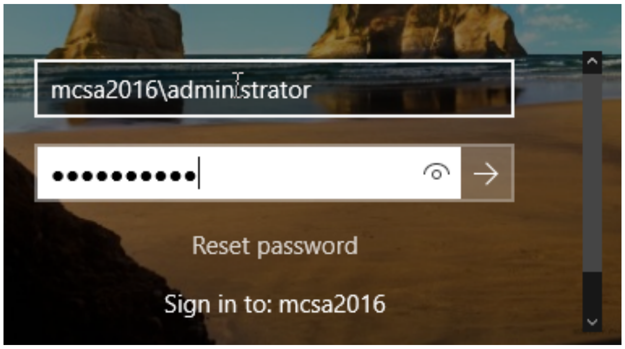
☑ Define these policy settings:

Select this object type:
Users, Service Accounts, Groups, or Built-in security principals

From this location:
MCSA2016.local

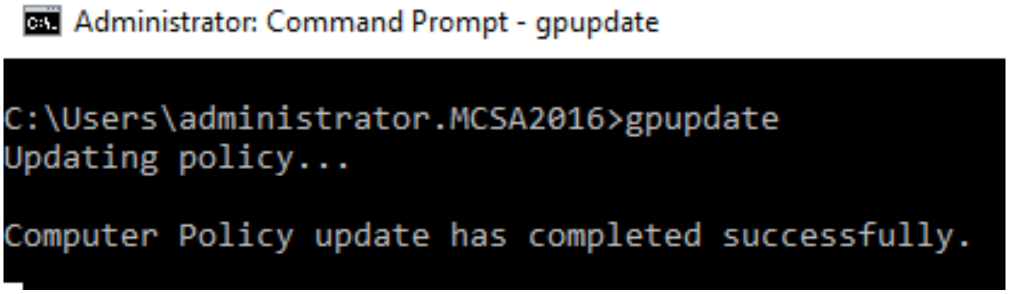
Enter the object names to select (examples):
Administrators

- 4-5-6: On ServerDM1, sign in to the domain as **Administrator.** To update the policies on ServerDM1, open a command prompt and type **gpupdate** and press **Enter.** Close the command prompt.



mcsa2016\administrator

••••••••••

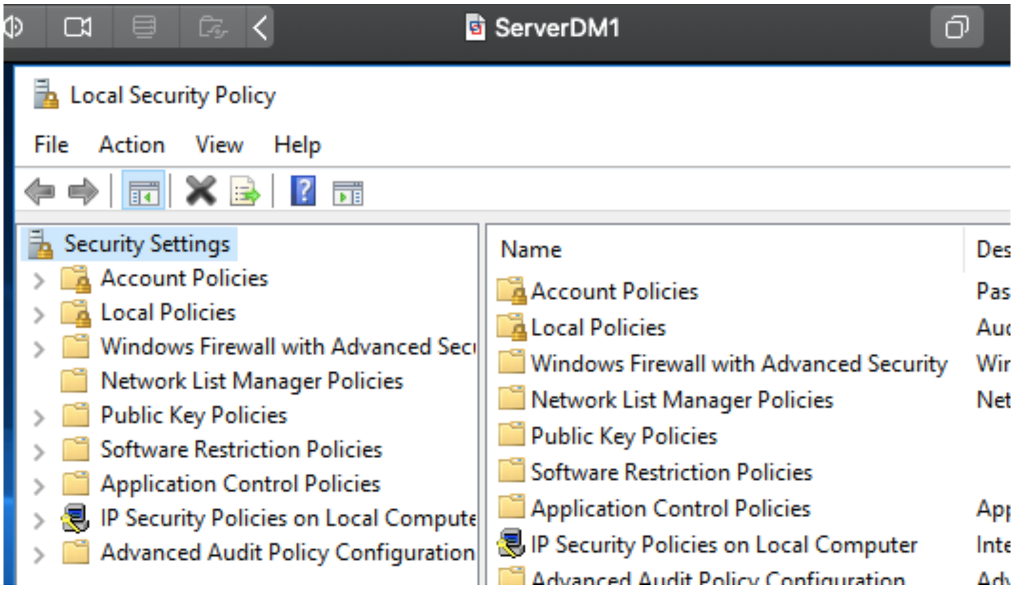


Administrator: Command Prompt - gpupdate

```
C:\Users\administrator.MCSA2016>gpupdate
Updating policy...

Computer Policy update has completed successfully.
```

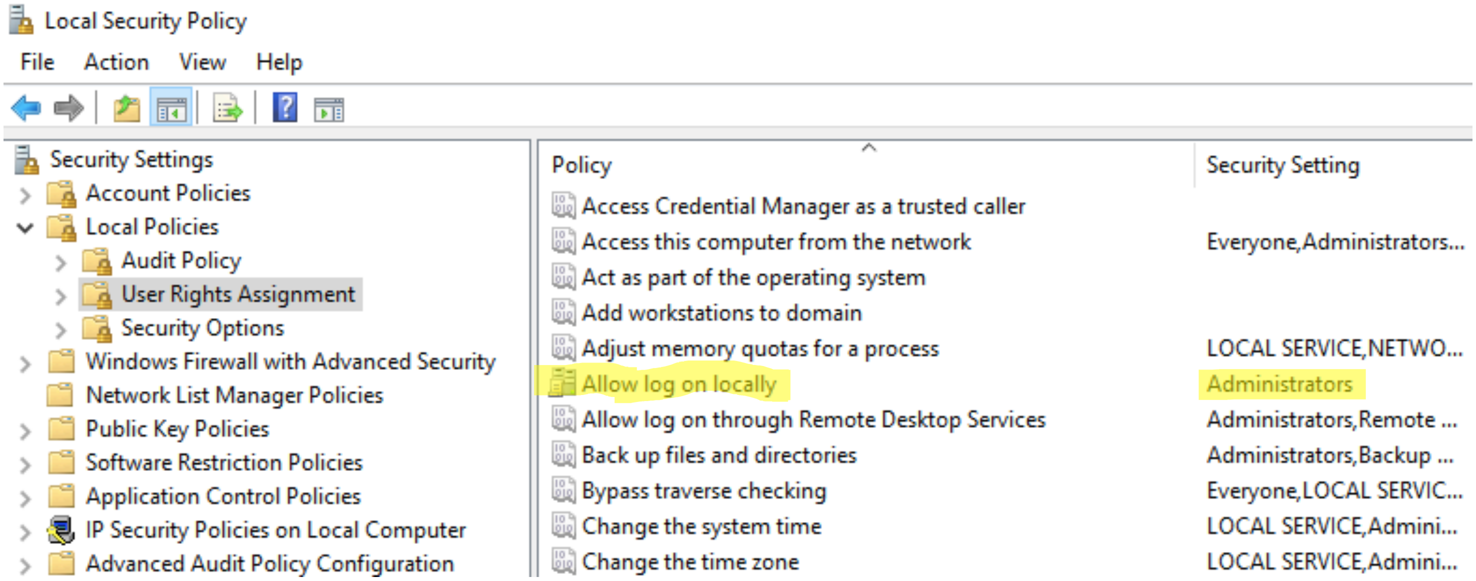
- 4-5-7: Right-click **Start**, click Run, type **secpol.msc** in the Open dialog box, and press **Enter** to open the Local Security Policy console. The Local Security Policy console contains only the security settings for the local computer.



ServerDM1
Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Name	Des
Account Policies	Pas
Local Policies	Auc
Windows Firewall with Advanced Security	Wir
Network List Manager Policies	Net
Public Key Policies	
Software Restriction Policies	
Application Control Policies	App
IP Security Policies on Local Computer	Inte
Advanced Audit Policy Configuration	Adv

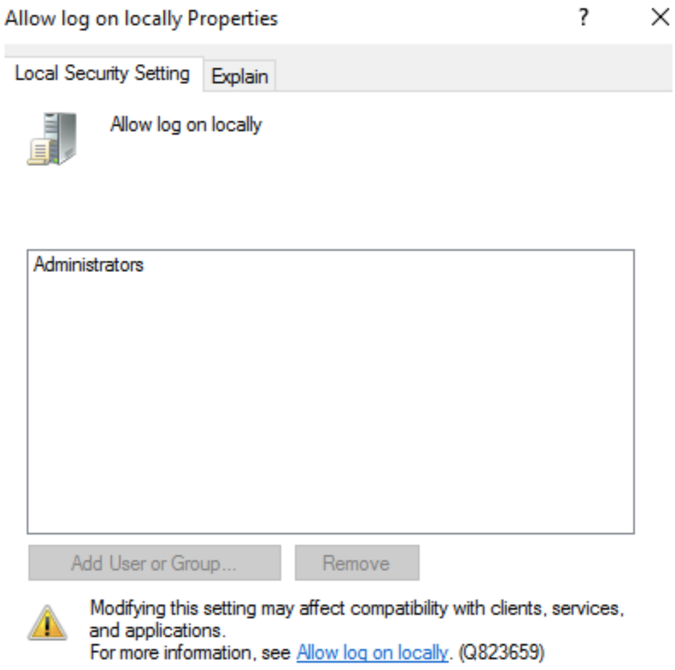
- 4-5-8: Click to expand **Local Policies**, and then click **User Rights Assignment**. Notice in Figure 4-12 that the icon next to the *Allow log on locally* policy looks like two towers and a scroll instead of the torn-paper icon next to the other policies. This icon indicates that the policy is defined by a domain GPO.



Security Settings
- Account Policies
- Local Policies
  - Audit Policy
  - User Rights Assignment
  - Security Options
- Windows Firewall with Advanced Security
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Computer
- Advanced Audit Policy Configuration

Policy	Security Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	Everyone,Administrators...
Act as part of the operating system	
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWO...
Allow log on locally	Administrators
Allow log on through Remote Desktop Services	Administrators,Remote ...
Back up files and directories	Administrators,Backup ...
Bypass traverse checking	Everyone,LOCAL SERVIC...
Change the system time	LOCAL SERVICE,Admini...
Change the time zone	LOCAL SERVICE,Admini...

- 4-5-9: In the right pane, double-click **Allow log on locally**. In the list box of users and groups, click **Administrators**. Neither the Add User or Group nor the Remove button is active because no users, not even administrators, can override domain polices on the local computer. Click **Cancel**.

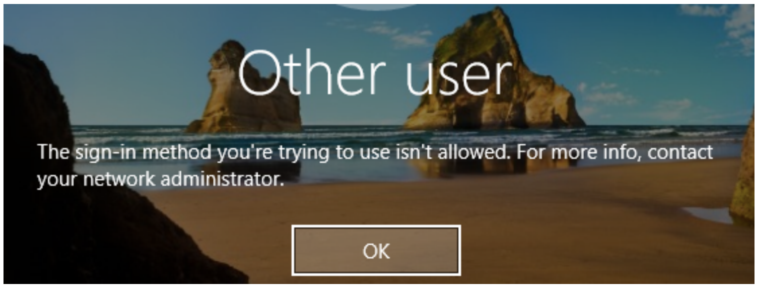


Allow log on locally

Administrators

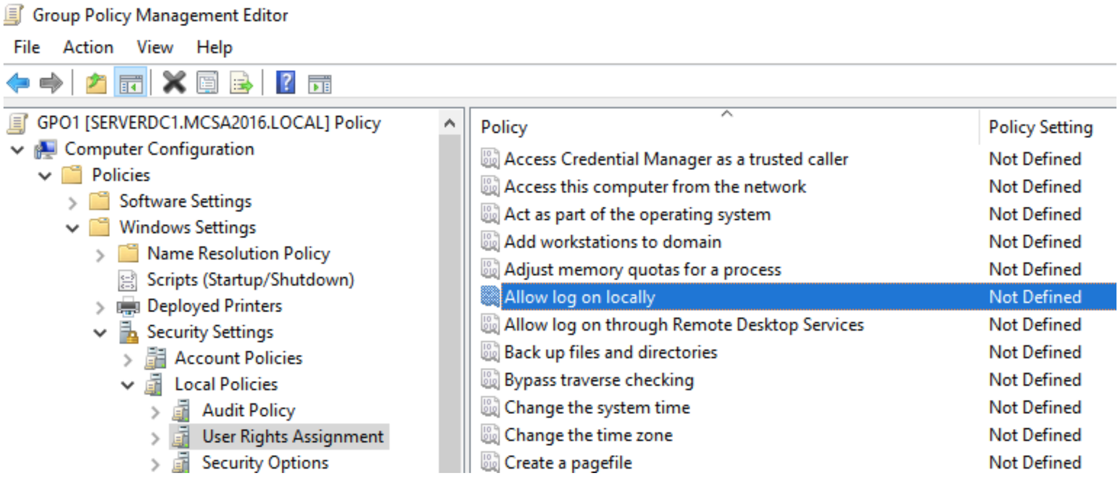
Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Allow log on locally. (Q823659)

- **4-5-10:** Sign out of ServerDM1, and then try to sign back in as **domuser1** using **Password01**. Because you have restricted local logon to Administrators only, you'll see the following message: "The sign-in method you're trying to use isn't allowed. For more info, contact your network administrator." The sign-in method referred to in the message is interactive logon or local logon. Click **OK.**



The sign-in method you're trying to use isn't allowed. For more info, contact your network administrator.

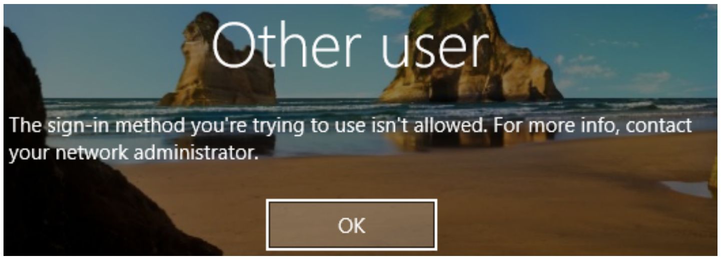
- **4-5-11:** On ServerDC1, change the **Allow log on locally** policy on GP01 to Not Defined by clearing the **Define these policy settings** check box, and then click **OK.** Close the Group Policy Management Editor.



- GPO1 [SERVERDC1.MCSA2016.LOCAL] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Deployed Printers
        - Security Settings
          - Account Policies
          - Local Policies
            - Audit Policy
            - User Rights Assignment
            - Security Options

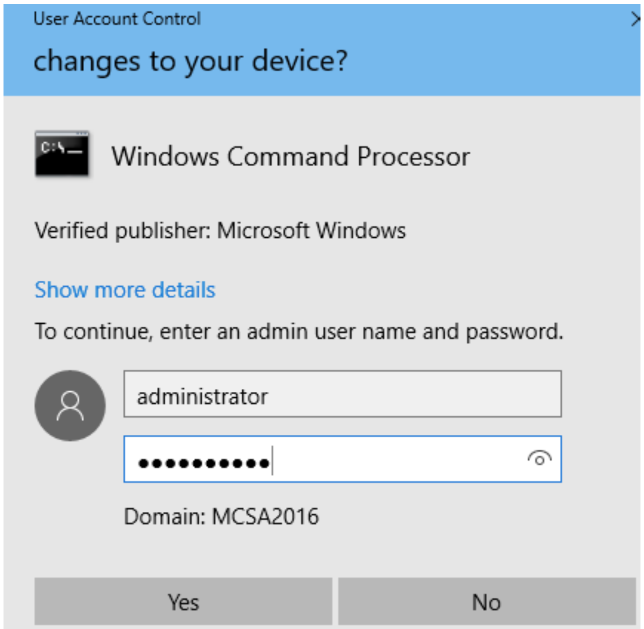
Policy	Policy Setting
Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	Not Defined
Act as part of the operating system	Not Defined
Add workstations to domain	Not Defined
Adjust memory quotas for a process	Not Defined
Allow log on locally	Not Defined
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Not Defined
Bypass traverse checking	Not Defined
Change the system time	Not Defined
Change the time zone	Not Defined
Create a pagefile	Not Defined

- **4-5-12:** On ServerDM1, try again to sign in as **domuser1.** You'll probably get the same message about not being able to sign in because the policy hasn't been updated yet. Click **OK.** Sign in as administrator, run **gpupdate** at a command prompt, and sign out again.



The sign-in method you're trying to use isn't allowed. For more info, contact your network administrator.

- 4-5-13: Sign in to ServerDM1 as **domuser1.** Only an administrator can run the Local Security Policy MMC, but there's a workaround if you start it from an elevated command prompt. Right-click **Start** and click **Command Prompt (Admin).** When prompted, type the Administrator account credentials and click **Yes**.



User Account Control

changes to your device?

Windows Command Processor

Verified publisher: Microsoft Windows

Show more details

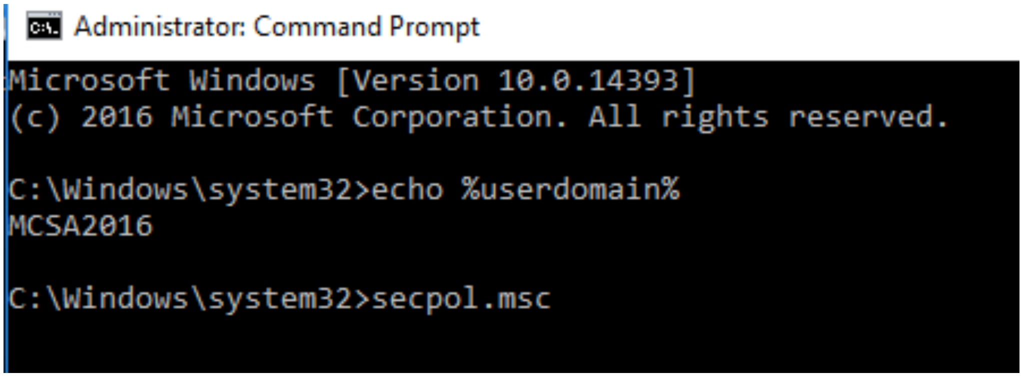
To continue, enter an admin user name and password.

administrator

••••••••••

Domain: MCSA2016

- 4-5-14: At the command prompt, type **secpol.msc** and press **Enter.**



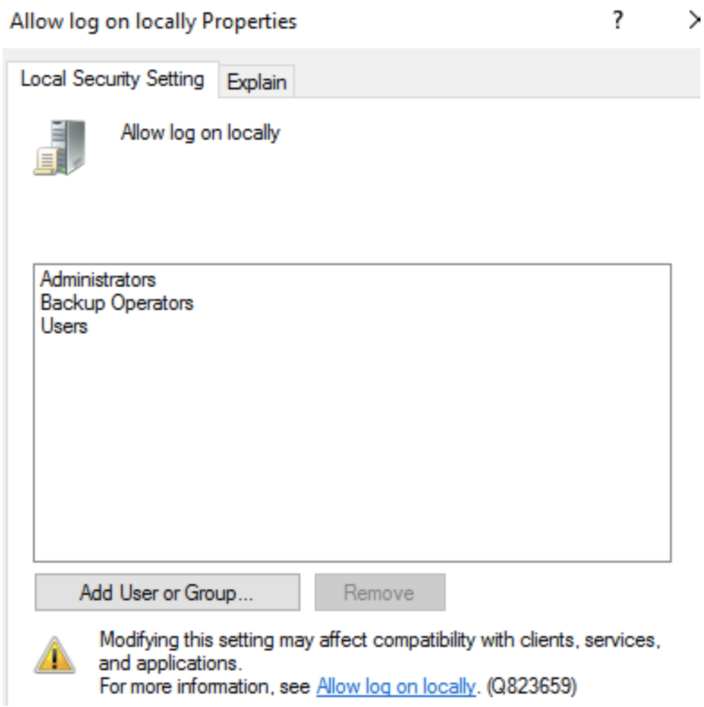
Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>echo %userdomain%
MCSA2016

C:\Windows\system32>secpol.msc
```

- 4-5-15: In the Local Security Policy console, click to expand **Local Policies** and **User Rights Assignment.** In the right pane, double-click **Allow log on locally** to view the list of users and groups assigned this permission. Notice that this right is now assigned from a local GPO rather than a domain GPO, so you can make changes if needed. Click **Cancel.**



Allow log on locally Properties

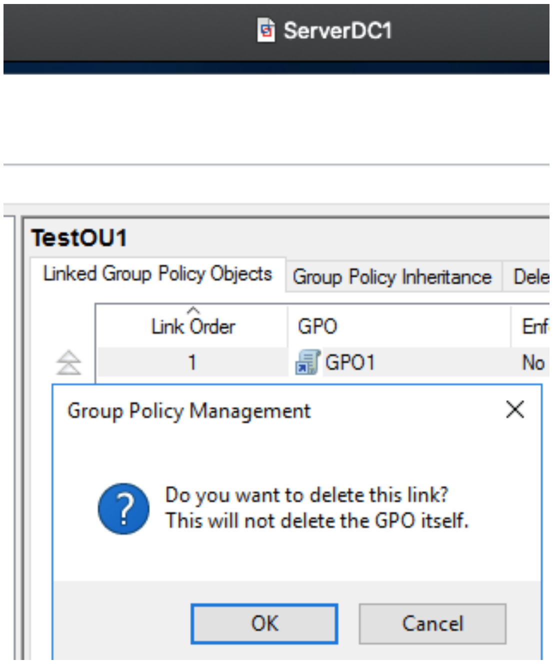
Local Security Setting | Explain

Allow log on locally

Administrators
Backup Operators
Users

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Allow log on locally. (Q823659)

- **4-5-16:** On ServerDC1, from the Group Policy Management console, unlink GPO1 from TestOU1 by right-clicking **GP01** under TestOU1 and clicking **Delete**. Click **OK**.



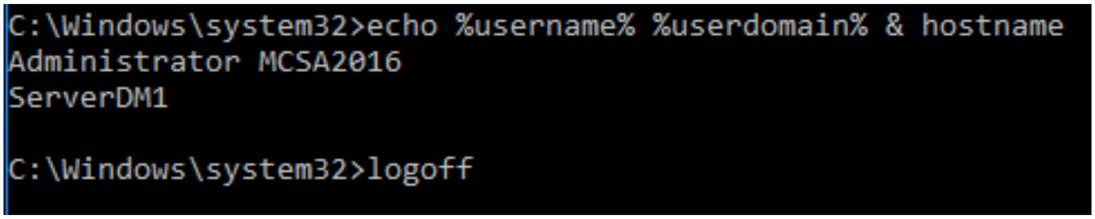
TestOU1

Link Order	GPO	Enf
1	GPO1	No

Group Policy Management

Do you want to delete this link?
This will not delete the GPO itself.

- **4-5-17:** Sign out of ServerDM1. Continue to the next activity.



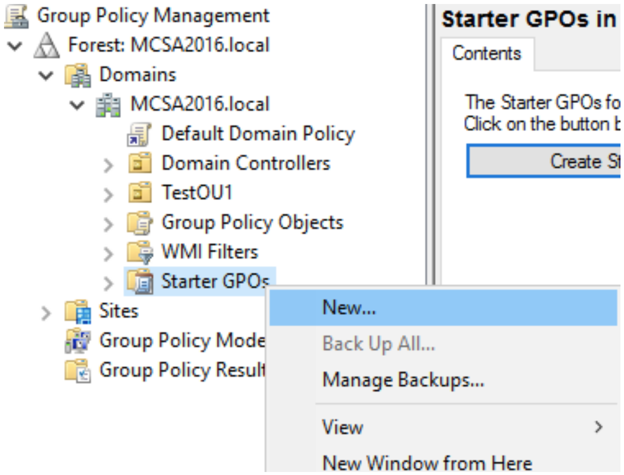
```
C:\Windows\system32>echo %username% %userdomain% & hostname
Administrator MCSA2016
ServerDM1

C:\Windows\system32>logoff
```

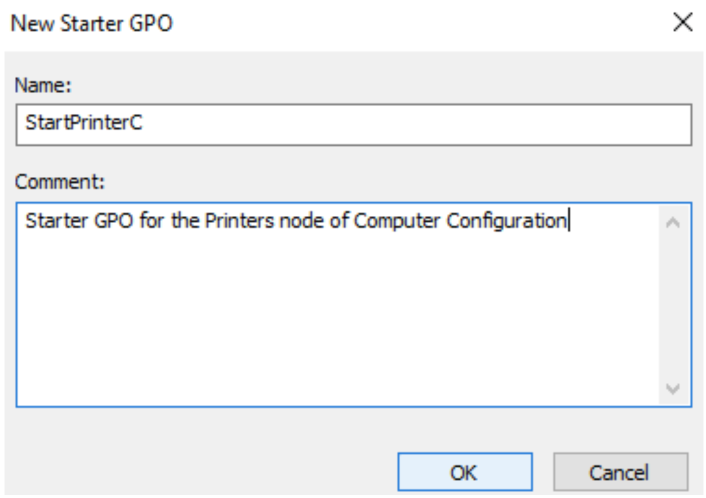
Activity 4-6: Creating and Using Starter GPOs

Description: In this activity, you create some Starter GPOs for creating new GPOs. You create two: one in the Computer Configuration node for configuring printers and one in the User Configuration node for configuring Start menu options.

- **4-6-1:** On ServerDC1, open the Group Policy Management console. Right-click the **Starter GPOs** folder and click **New.**



- **4-6-2:** In the New Starter GPO dialog box, type **StartPrintersC** in the Name text box. (*Start* stands for Starter GPO, *Printers* refers to the Printers node, and *C* refers to the Computer Configuration node of the GPO.) In the Comment text box, type **Starter GPO for the Printers node of Computer Configuration,** and then click **OK.**

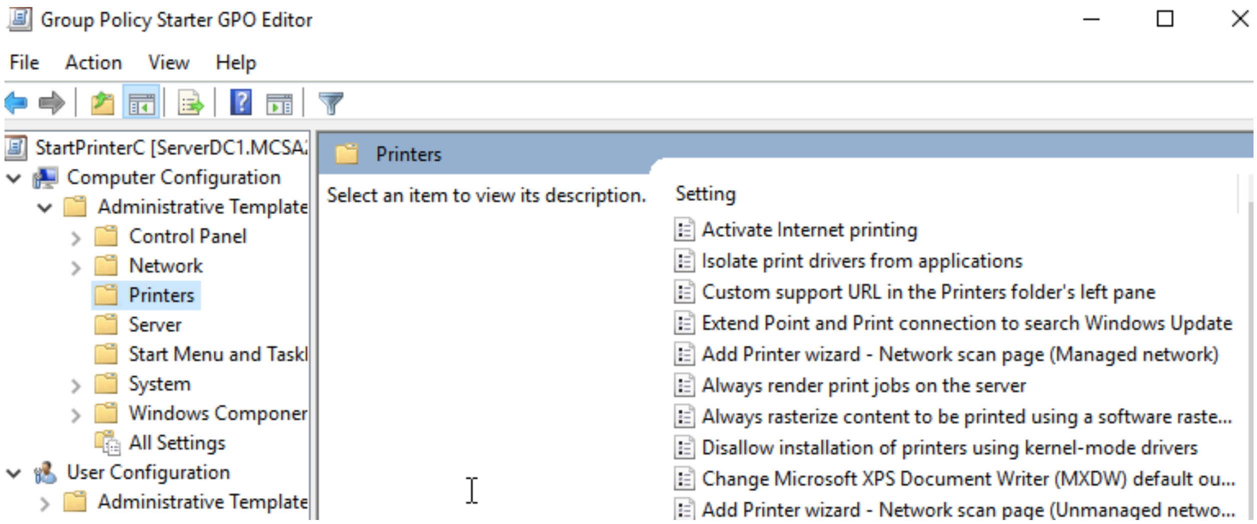


New Starter GPO

Name: StartPrinterC

Comment: Starter GPO for the Printers node of Computer Configuration

- **4-6-3:** Right-click the **StartPrintersC** GPO and click **Edit.** In the Group Policy Starter GPO Editor, click to expand **Computer Configuration** and **Administrative Templates,** and then click **Printers.**

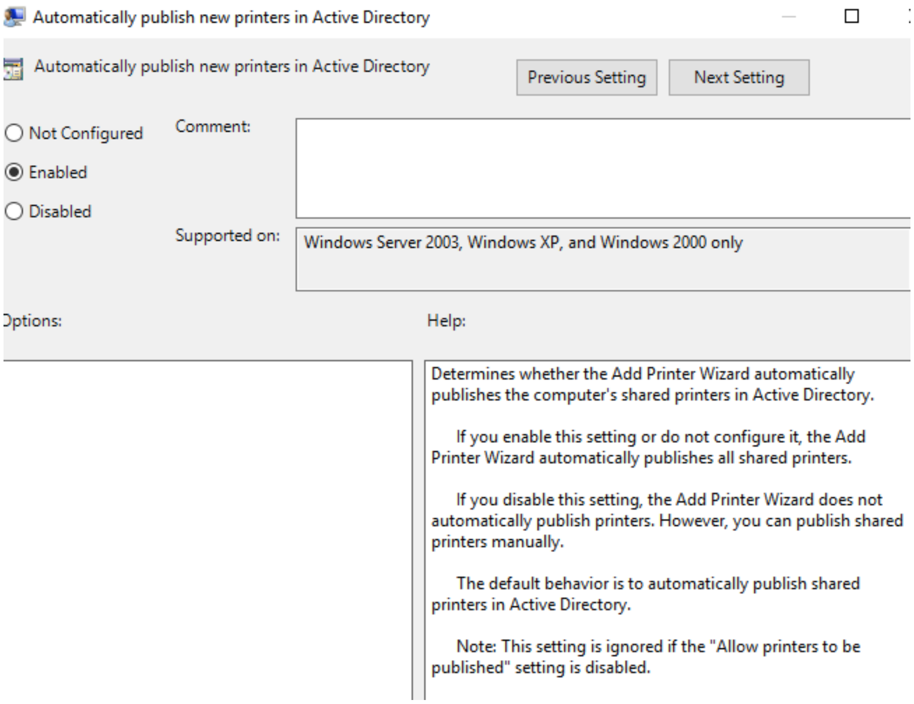


Group Policy Starter GPO Editor

Select an item to view its description.

Setting
Activate Internet printing
Isolate print drivers from applications
Custom support URL in the Printers folder's left pane
Extend Point and Print connection to search Windows Update
Add Printer wizard - Network scan page (Managed network)
Always render print jobs on the server
Always rasterize content to be printed using a software raste...
Disallow installation of printers using kernel-mode drivers
Change Microsoft XPS Document Writer (MXDW) default ou...
Add Printer wizard - Network scan page (Unmanaged netwo...

- **4-6-4:** In the right pane, double-click **Automatically publish new printers in Active Directory.** In the Properties dialog box, click **Enabled.** Read the explanation of this policy setting, and then click **OK.**


Automatically publish new printers in Active Directory
Automatically publish new printers in Active Directory
Previous Setting
Next Setting
Comment:
Supported on:
Options:
Help:

○ Not Configured

● Enabled

○ Disabled

Supported on: Windows Server 2003, Windows XP, and Windows 2000 only

Determines whether the Add Printer Wizard automatically publishes the computer's shared printers in Active Directory.

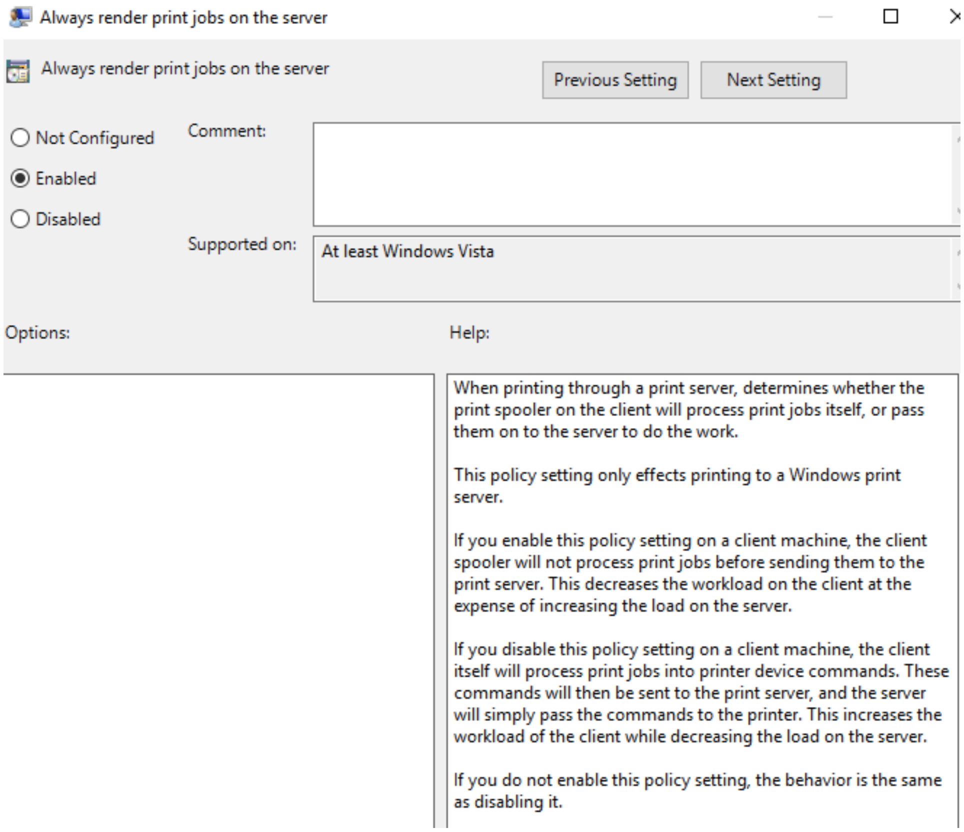
If you enable this setting or do not configure it, the Add Printer Wizard automatically publishes all shared printers.

If you disable this setting, the Add Printer Wizard does not automatically publish printers. However, you can publish shared printers manually.

The default behavior is to automatically publish shared printers in Active Directory.

Note: This setting is ignored if the "Allow printers to be published" setting is disabled.

- 4-6-5: Double-click **Always render print jobs on the server.** In the Properties dialog box, click **Enabled.** Read the explanation of this policy setting, and then click **OK.**


Always render print jobs on the server
Always render print jobs on the server
Previous Setting
Next Setting
Comment:
Supported on:
Options:
Help:

○ Not Configured

● Enabled

○ Disabled

Supported on: At least Windows Vista

When printing through a print server, determines whether the print spooler on the client will process print jobs itself, or pass them on to the server to do the work.

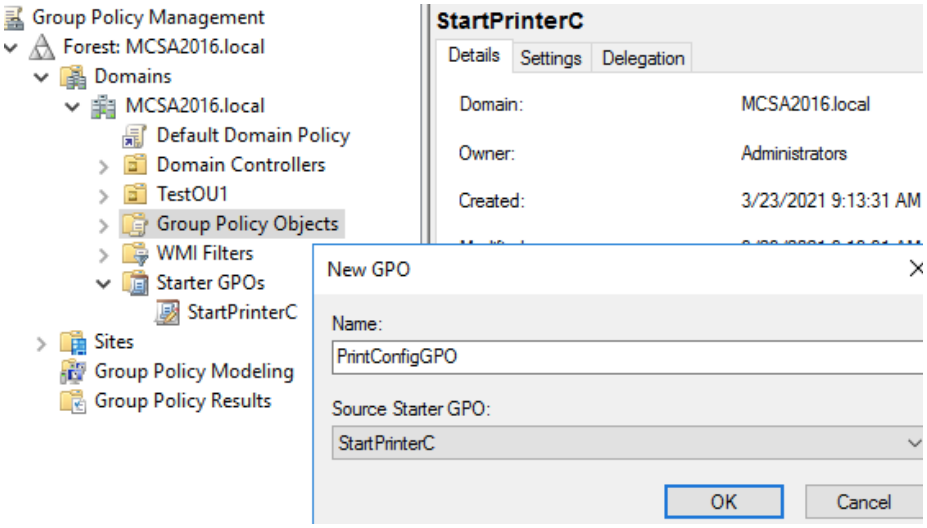
This policy setting only effects printing to a Windows print server.

If you enable this policy setting on a client machine, the client spooler will not process print jobs before sending them to the print server. This decreases the workload on the client at the expense of increasing the load on the server.

If you disable this policy setting on a client machine, the client itself will process print jobs into printer device commands. These commands will then be sent to the print server, and the server will simply pass the commands to the printer. This increases the workload of the client while decreasing the load on the server.

If you do not enable this policy setting, the behavior is the same as disabling it.

- **4-6-6:** Close the Group Policy Starter GPO Editor. In the Group Policy Management console, right-click the **Group Policy Objects** folder and click **New.** In the New GPO dialog box, type **PrintConfigGPO** in the Name text box, click **StartPrintersC** in the Source Starter GPO list box, and then click **OK.**



Domain: MCSA2016.local

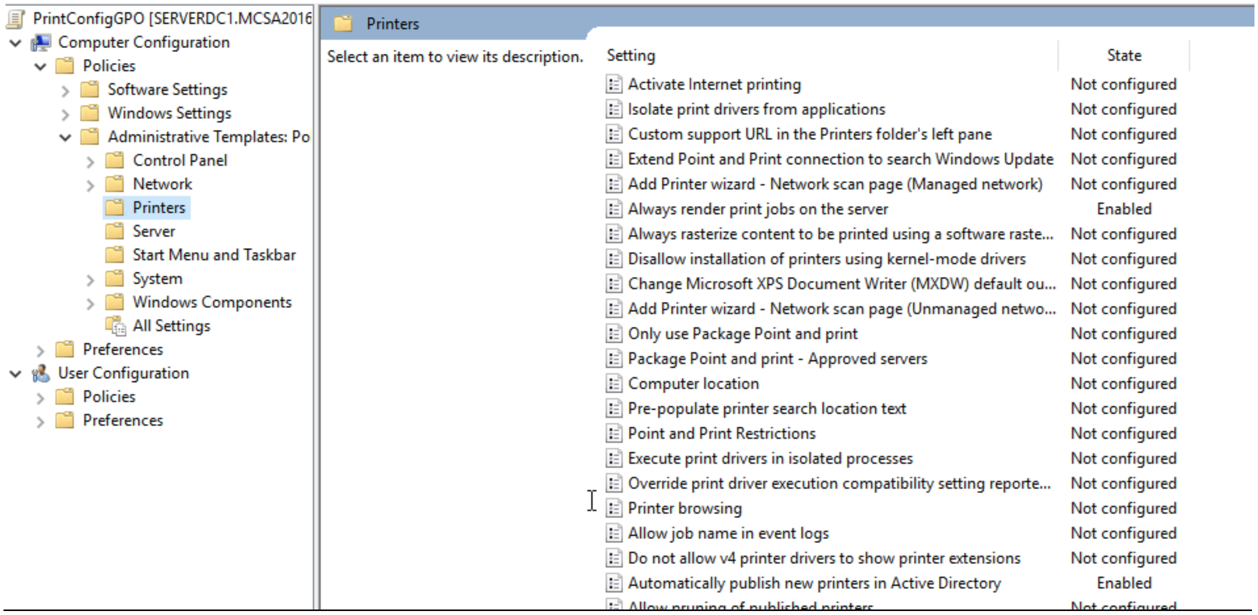
Owner: Administrators

Created: 3/23/2021 9:13:31 AM

Name: PrintConfigGPO

Source Starter GPO: StartPrinterC

- **4-6-7:** Right-click **PrintConfigGPO** and click **Edit.** In the Group Policy Management Editor, expand and navigate to the **Computer Configuration, Policies, Administrative Templates, Printers** to verify that your Starter GPO settings are there. Now you can link this new GPO to a container with computer accounts that have print servers installed, and the printer policies will be in effect on these servers. Close the Group Policy Management Editor.



Setting	State
Activate Internet printing	Not configured
Isolate print drivers from applications	Not configured
Custom support URL in the Printers folder's left pane	Not configured
Extend Point and Print connection to search Windows Update	Not configured
Add Printer wizard - Network scan page (Managed network)	Not configured
Always render print jobs on the server	Enabled
Always rasterize content to be printed using a software raste...	Not configured
Disallow installation of printers using kernel-mode drivers	Not configured
Change Microsoft XPS Document Writer (MXDW) default ou...	Not configured
Add Printer wizard - Network scan page (Unmanaged netwo...	Not configured
Only use Package Point and print	Not configured
Package Point and print - Approved servers	Not configured
Computer location	Not configured
Pre-populate printer search location text	Not configured
Point and Print Restrictions	Not configured
Execute print drivers in isolated processes	Not configured
Override print driver execution compatibility setting reporte...	Not configured
Printer browsing	Not configured
Allow job name in event logs	Not configured
Do not allow v4 printer drivers to show printer extensions	Not configured
Automatically publish new printers in Active Directory	Enabled
Allow pruning of published printers	Not configured