



3/25/2021

Hands On Exercise

Chapter 5

Managing Group Policies

(Part2)



El Adel, Taoufik

IT 416 - SPRING 2021 - OLD DOMINION UNIVERSITY

Table 5-1 Activity requirements

Activity	Requirements	Notes
Activity 5-1: Resetting Your Virtual Environment	ServerDC1, ServerDM1	
Activity 5-2 Working with GPO Inheritance Blocking and Enforcement	ServerDC1, ServerDM1	
Activity 5-3: Using GPO Security Filtering	ServerDC1, ServerDM1	
Activity 5-4: Using GPO Security Filtering for a Computer Account	ServerDC1, ServerDM1	
Activity 5-5: Configuring Loopback Policy Processing	ServerDC1, ServerDM1	
Activity 5-6: Using Remote Group Policy Updates	ServerDC1, ServerDM1	
Activity 5-7: Using Group Policy Results and Group Policy Modeling	ServerDC1, ServerDM1	
Activity 5-8: Backing Up and Restoring a GPO	ServerDC1	

Activity 5-4: Using GPO Security Filtering for a Computer Account

Time Required: 15 minutes

Objective: Change the default security filtering on a GPO and examine the results.

Required Tools and Equipment: ServerDC1, ServerDM1

Description: In this activity, you change the security filtering on a GPO for a computer account.

1. On ServerDC1, open the Group Policy Management console, if necessary. Right-click the **Group Policy Objects** folder and click **New**. Type **GPO2** in the Name text box and click **OK**.
2. Click **GPO2** in the left pane. In the right pane, click the **Scope** tab, if necessary.
3. In the Security Filtering dialog box in the right pane, click the **Add** button. Click the **Object Types** button. By default, computer accounts aren't recognized in this dialog box. In the Object Types dialog box, click to select **Computers**. Click **OK**.

4. Type **ServerDM1**, click **Check Names**, and click **OK**.
5. Click the **Delegation** tab and then click **Advanced**. In the top pane of the GPO2 Security Settings dialog box, click **Authenticated Users**. In the bottom pane, scroll down and click to clear **Apply group policy**. Click **OK**. ServerDM1 is now the only security principal with Read and Apply Group Policy permissions for GPO2.
6. Open GPO2 in Group Policy Management Editor. Navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options**.
7. Find and double-click **Interactive logon: Message text for users attempting to log on**. Click **Define this policy setting in the template**. In the text box, type **Authorized users only may attempt to sign in to this computer!** Click **OK**.
8. Double-click **Interactive logon: Message title for users attempting to log on**. Click **Define this policy setting** and then type **Sign in Warning** in the text box. Click **OK**.
9. Close Group Policy Management Editor. Link GPO2 to the domain.
10. Sign in to ServerDM1 as domuser1. Since the policy you configured is a Computer policy, it is only applied when the computer restarts or if you run gpupdate. Open a command prompt and run **gpupdate**, then sign out of ServerDM1.

11. Attempt to sign in again to ServerDM1 (you usually need to press Ctrl+Alt+Delete to sign in; with a virtual machine, you probably need to press the Ctrl+Alt+Delete toolbar icon or alternate key sequence). You see the sign-in warning you just created. Click **OK**. You don't need to sign in right now.
12. On ServerDC1, run **gpupdate**. Because you linked the policy to the domain, it would normally affect ServerDC1 as well as ServerDM1. Sign out of ServerDC1, and try to sign in again as **Administrator**. You don't see the warning message because only ServerDM1 has permission to read and apply GPO2. Sign in to ServerDC1.
13. On ServerDC1, open Group Policy Management. Navigate to the **Group Policy Objects** folder and click **GPO2** in the left pane. Under Security Filtering, click **Add**. Type **Authenticate Users**, click **Check Names**, and click **OK**. Click **ServerDM1\$ (MCSA2016\ServerDM1\$)**, click **Remove**, and click **OK** to set Security Filtering back to the default.
14. Continue to the next activity.

GPO2

Scope | Details | Settings | Delegation | Status

Links

Display links in this location: MCSA2016.local

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
SERVERDM1\$ (MCSA2016\SERVERDM1\$)

GPO2

Scope | Details | Settings | Delegation | Status

These groups and users have the specified permission for this GPO

Groups and users:

Name	Allowed Permissions
Authenticated Users	Read
Domain Admins (MCSA2016\Domain Admins)	Edit settings, delete, modify security
Enterprise Admins (MCSA2016\Enterprise Admins)	Edit settings, delete, modify security
ENTERPRISE DOMAIN CONTROLLERS	Read
SERVERDM1\$ (MCSA2016\SERVERDM1\$)	Read (from Security Filtering)
SYSTEM	Edit settings, delete, modify security

- Interactive logon: Machine account lockout threshold Not Defined
- Interactive logon: Machine inactivity limit Not Defined
- Interactive logon: Message text for users attempting to log on Authorized users only may attempt to sign in to this computer!
- Interactive logon: Message title for users attempting to log on Sign in Warning
- Interactive logon: Number of previous logons to cache (in c... Not Defined

MCSA2016.local

Status | Linked Group Policy Objects | Group Policy Inheritance | Delegation

	Link Order	GPO	Enforced	Link Enabled	GPO Status
↑	1	Default Domain Policy	No	Yes	Enabled
↑	2	GPO2	No	Yes	Enabled

Sign in Warning

Authorized users only may attempt to sign in to this computer!

OK

Activity 5-5: Configuring Loopback Processing

Time Required: 20 minutes

Objective: Configure loopback policy processing.

Required Tools and Equipment: ServerDC1, ServerDM1

Description: In this activity, you configure loopback policy processing.

1. On ServerDC1, open Active Directory Users and Computers. Create an OU under the domain node named **MemberServers**. Click the **Computers** folder and drag and drop **ServerDM1** to the **MemberServers** OU. Click **Yes** to confirm. Close Active Directory Users and Computers.
2. Open the Group Policy Management console, if necessary. Create a GPO named **GPO3**, and open it in the Group Policy Management Editor.
3. Expand **User Configuration, Policies, and Administrative Templates**, and configure the following settings:
 - Desktop\Remove Recycle Bin icon from desktop: **Enabled**
 - Desktop\Desktop\DesktopWallpaper: **Enabled**
 - Wallpaper Name: **C:\windows\web\wallpaper\theme2\img7.jpg** (or another image file if you don't have img7.jpg)
 - Wallpaper Style: **Fill**
4. Link **GPO3** to the **MemberServers** OU. (If you don't see the MemberServers OU, click the **Refresh** icon.) Remember that these settings are User Configuration settings, so they don't normally have an effect on computer accounts, which is the only type of account in MemberServers.
5. Sign in to ServerDM1 as **domuser1**. Run **gpupdate**, sign out, and sign in again. The changes you made in GPO3 don't have any effect. The Recycle Bin is still on the desktop, and the wallpaper hasn't changed. Stay signed in to ServerDM1.
6. On ServerDC1, open **GPO3** in the Group Policy Management Editor, if necessary.
7. Expand **Computer Configuration, Policies, Administrative Templates, System, and Group Policy**. Double-click **Configure user Group Policy loopback processing mode**. Click **Enabled**, and in the Mode drop-down list box, click **Merge**. This option allows existing user settings that are normally applied to be applied as long as there's no conflict. Click **OK**.
8. On ServerDM1, run **gpupdate**. Sign out, and sign in again as **domuser1**. The settings made in the User Configuration node of GPO3 should now be applied. The wallpaper has changed, and the Recycle Bin is no longer on the desktop. Sign out of ServerDM1.
9. On ServerDC1, unlink **GPO3** from the **MemberServers** OU. Close Group Policy Management Editor.
10. Continue to the next activity.

	Name	Type
Active Directory Users and Com		
> Saved Queries		
MCSA2016.local		
> Builtin		
> Computers		
> Domain Controllers		
> ForeignSecurityPrincipal:		
> Managed Service Accour		
> TestOU1		
> Users		
MemberServers	SERVERDM1	Computer

Administrative Templates:		
> Control Panel		
> Desktop		
Active Directory		
Desktop		
> Network		
> Shared Folders		
> Start Menu and Taskbar		
> System		
	Remove Computer icon on the m...	Not configured
	Remove My Documents icon o...	Not configured
	Hide Network Locations icon o...	Not configured
	Remove Properties from the Co...	Not configured
	Remove Properties from the Do...	Not configured
	Do not add shares of recently o...	Not configured
	Remove Recycle Bin icon from ...	Enabled
	Remove Properties from the Re...	Not configured
	Don't save settings at exit	Not configured

Desktop Wallpaper

Desktop Wallpaper Previous Set

Not Configured Comment:
 Enabled
 Disabled

Supported on:

Options:

Wallpaper Name:

Example: Using a local path: C:\windows\web\wallpaper\home.jpg

Example: Using a UNC path: \\Server\Share\Corp.jpg

Wallpaper Style:

MemberServers

Link Order	GPO	Enforced	Link Enabled	GPO Status
1	GPO3	No	Yes	Enabled

Configure user Group Policy loopback processing mode

Not Configured Comment:

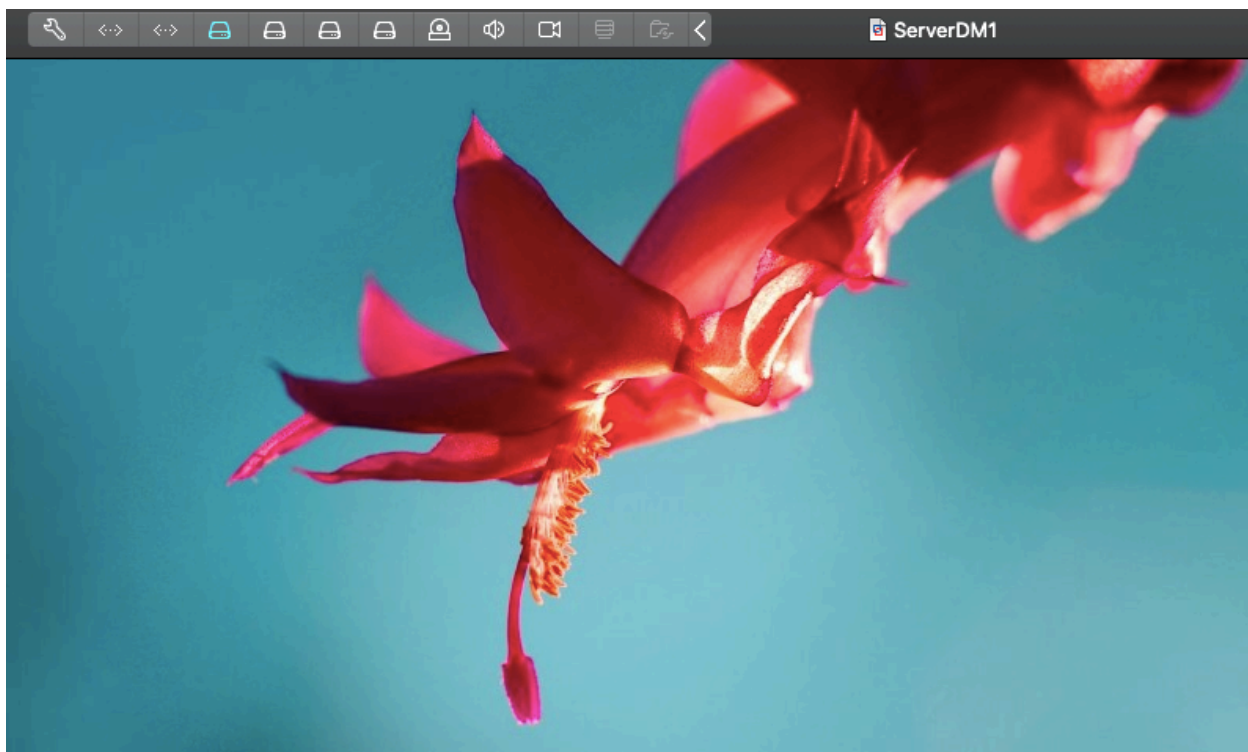
Enabled

Disabled

Supported on:

Options:

Mode:



Activity 5-6: Using Remote Group Policy Updates

Time Required: 10 minutes

Objective: Configure the firewall and perform a remote group policy update.

Required Tools and Equipment: ServerDC1, ServerDM1

Description: Configure the firewall for a remote group policy update on ServerDM1.

1. On ServerDM1, sign in as the domain **Administrator**. Open the Network and Sharing Center, and click **Windows Firewall** at the lower left.
 2. In the Windows Firewall window, click **Advanced settings**. In the Windows Firewall with Advanced Security window, click **Inbound Rules**.
 3. In the Actions pane, click **Filter by Profile** and click to select **Filter by Domain Profile**. Right-click the following settings and click **Enable Rule** for each one: **Remote Scheduled Tasks Management (RPC)**, **Remote Scheduled Tasks Management (RPC-EPMAP)**, and **Windows Management Instrumentations (WMI-In)**. Close Windows Firewall with Advanced Security and Windows Firewall.
 4. On ServerDC1, open the Group Policy Management console, if necessary. Right-click the **MemberServers** OU and click **Group Policy Update**. You'll see a message indicating that one computer will be updated because the ServerDM1 account is in the MemberServers OU. Click **Yes**.
-

- In the Remote Group Policy update results window, you should see ServerDM1 in the list of computers (see Figure 5-16). Click **Close**. On ServerDM1, a command prompt window opens after a while, and the `gpupdate` command runs.

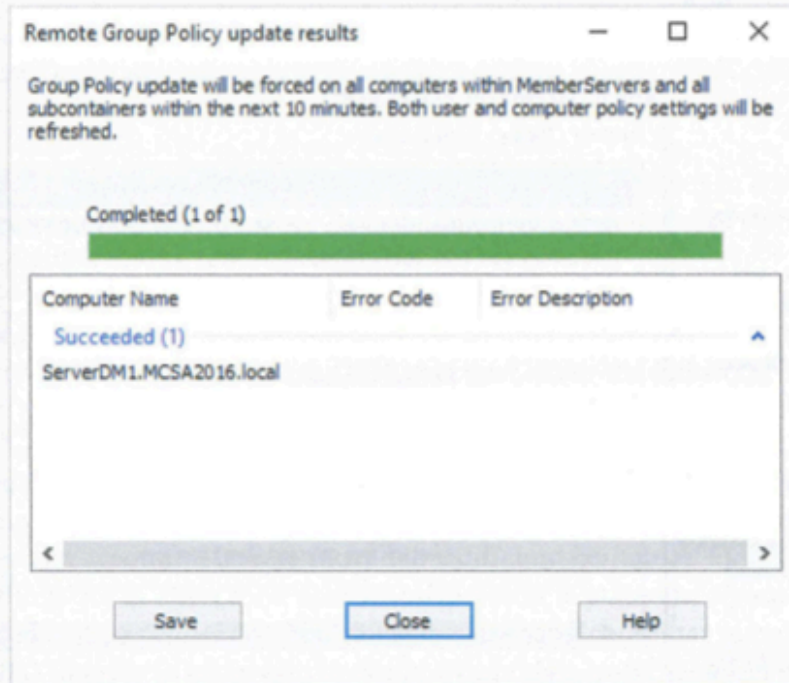
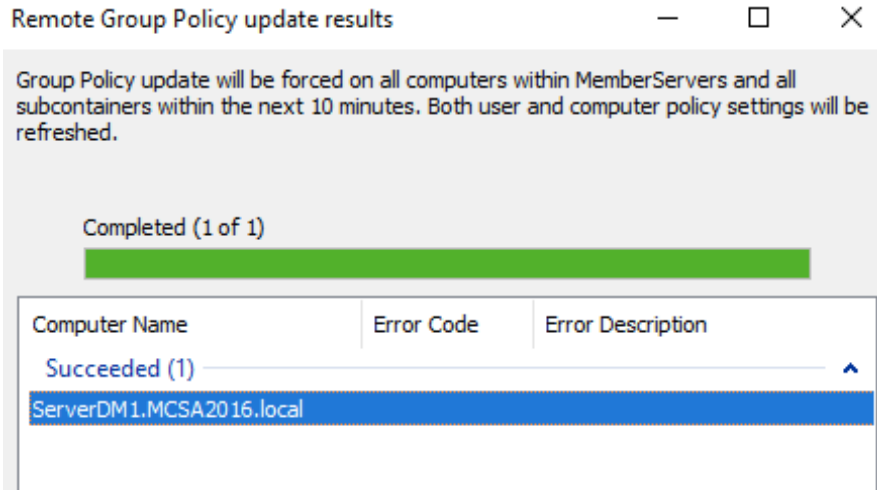


Figure 5-16 Results of a remote group policy update

- To perform a remote Group Policy update using PowerShell, open a PowerShell prompt on ServerDC1. Type **`Invoke-GPUUpdate -Computer ServerDM1 RandomDelayInMinutes 0`** and press **Enter**. A command prompt window opens immediately on ServerDM1. On ServerDC1, close the PowerShell prompt.
- Sign out of ServerDM1 but stay signed in to ServerDC1 and continue to the next activity.

Inbound Rules Filtered by: Domain Profile					
Name	Group	Profile	Enabled	Action	
Network Discovery (WSD-In)	Network Discovery	Domai...	No	Allow	
Performance Logs and Alerts (DCOM-In)	Performance Logs and Alerts	Domain	No	Allow	
Performance Logs and Alerts (TCP-In)	Performance Logs and Alerts	Domain	No	Allow	
Remote Desktop - Shadow (TCP-In)	Remote Desktop	All	No	Allow	
Remote Desktop - User Mode (TCP-In)	Remote Desktop	All	No	Allow	
Remote Desktop - User Mode (UDP-In)	Remote Desktop	All	No	Allow	
Remote Event Log Management (NP-In)	Remote Event Log Manage...	All	No	Allow	
Remote Event Log Management (RPC)	Remote Event Log Manage...	All	No	Allow	
Remote Event Log Management (RPC-EP...	Remote Event Log Manage...	All	No	Allow	
Remote Event Monitor (RPC)	Remote Event Monitor	All	No	Allow	
Remote Event Monitor (RPC-EPMAP)	Remote Event Monitor	All	No	Allow	
✔ Remote Scheduled Tasks Management (...)	Remote Scheduled Tasks M...	All	Yes	Allow	
✔ Remote Scheduled Tasks Management (...)	Remote Scheduled Tasks M...	All	Yes	Allow	
Remote Service Management (NP-In)	Remote Service Management	All	No	Allow	
Remote Service Management (RPC)	Remote Service Management	All	No	Allow	



```
PS C:\Users\Administrator> Invoke-GPUUpdate -Computer ServerDM1 -RandomDelayInMinutes 0
PS C:\Users\Administrator>
```



Activity 5-7: Using Group Policy Results and Group Policy Modeling

Time Required: 25 minutes

Objective: Use the Group Policy Results and Group Policy Modeling tools.

Required Tools and Equipment: ServerDC1, ServerDM1

Description: In this activity, you use the Group Policy Results Wizard to see how user and computer accounts are affected by group policy settings. Then you use the Group Policy Modeling Wizard to create a what-if scenario to see how accounts are affected if they're moved to a different OU.

1. On ServerDC1, open the Group Policy Management console. Link **GPO3** to the **TestOU1** OU (this is where domuser1 is located). On ServerDM1, sign in as **domuser1**. This ensures that the latest policies are applied to domuser1 on ServerDM1.
2. Right-click **Group Policy Results** and click **Group Policy Results Wizard**. In the welcome window, click **Next**.
3. In the Computer Selection window, click the **Another computer** option button, and type **ServerDM1** in the text box. Click **Next**.
4. In the User Selection window, click **MCSA2016\domuser1**, and then click **Next**.
5. In the Summary of Selections window, click **Next**, and then click **Finish**.
6. Click **domuser1 on serverdm1** in the left pane, if necessary. In the report generated in the right pane, examine the Summary and Details tabs. In the Details tab, click the **show all** link to see all applied settings. Pay particular attention to the User Details section. Click the **Policy Events** tab. You won't see the events unless you enable all three Remote Event Log Management rules in Windows Firewall on ServerDM1.
7. In the left pane of the Group Policy Management console under Group Policy Results, you see the icon domuser1 on serverdm1. You can right-click the icon to save the report, rerun the query, and see an advanced view. Right-click **domuser1 on serverdm1** and click **Advanced View**. The policy information opens in the Resultant Set of Policy (RSOP) snap-in. You can browse through the policies to see all the policies that are currently configured. Close the RSOP console. When prompted to save the console, click **No**.

- In Group Policy Management, right-click **Group Policy Modeling** and click **Group Policy Modeling Wizard**. In the welcome window, click **Next**.
- In the Domain Controller Selection window, click the **This domain controller** option button, and then click **Next**.
- In the User and Computer Selection window, click the **User** option button and type **mcsa2016\domuser1**. Click the **Computer** option button, type **mcsa2016\serverdm1** (see Figure 5-19), and click **Next**.

Group Policy Modeling Wizard

User and Computer Selection

You can view simulated policy settings for a selected user (or a container with user information) and computer (or a container with computer information).

Example container name: CN=Users,DC=MCSA2016,DC=local
Example user or computer: MCSA2016\Administrator

Simulate policy settings for the following:

User information

Container: Browse...

User: Browse...

Computer information

Container: Browse...

Computer: Browse...

Skip to the final page of this wizard without collecting additional data

< Back Next > Cancel

Figure 5-19 Selecting the user and computer for Group Policy Modeling

- In the Advanced Simulated Options window, accept the defaults, and click **Next**.
- In the Alternate Active Directory Paths window in the User location text box, change TestOU1 to **MemberServers**. This change simulates the policies that would be applied to domuser1 if the user were in the MemberServers OU. Click **Next**.
- Click **Next** in the User Security Groups window, the Computer Security Groups window, the WMI Filters for Users window, and the WMI Filters for Computers window.
- In the Summary of Selections window, click **Next**, and then click **Finish**.
- The report is displayed in the right pane. Click the **Details** tab, and scroll down until you see User Details. Under the General section, notice that the User container shows mcsa2016.local/MemberServers to indicate that the results are based on domuser1 being located in MemberServers. Also notice that GPO3 is not shown as an applied GPO as it was in the Group Policy Results report. That's because GPO3 would not be applied to the user account if the user was in the MemberServers OU.
- Continue to the next activity.

Group Policy Results Wizard



Summary of Selections

The list contains the selections you made in this wizard.



To make changes to your selections, click Back. To gather the policy settings, click Next.

Selection	Settings
User name	MCSA2016\domuser1
Display user policy settings	Yes
Computer name	ServerDM1
Display computer policy settings	Yes

Group Policy Modeling Wizard



Summary of Selections

The list contains the selections you made in this wizard.



To make changes to your selections, click Back. To process the simulation, click Next.

Selection	Settings
User name	mcsa2016\domuser1
Computer name	mcsa2016\serverdm1
Slow network simulation	No
Loopback mode	(None)
Site name	(None)
User Location	OU=MemberServers,DC=MCSA2016,DC=local
Computer location	(Not specified)
User security groups	(Not specified)
Computer security groups	(Not specified)

Processing the simulation on this domain controller:

ServerDC1.MCSA2016.local

< Back

Next >

Cancel

domuser1 on serverdm1		
Summary	Details	Query
None		
User Details		
General		
User name	mcsa2016\domuser1	
User container	MCSA2016.local/MemberServers	
Domain	MCSA2016.local	
Slowlink processing	No	
Loopback processing	No loopback mode	
Component Status		
Component Name	Status	
Group Policy Infrastructure	Success	
Registry	Success	



Activity 5-8: Backing up and Restoring a GPO

Time Required: 10 minutes

Objective: Back up and restore a GPO.

Required Tools and Equipment: ServerDC1

Description: In this activity, you use PowerShell cmdlets to back up and restore a GPO.

1. On ServerDC1, create a directory named **C:\backupgpo** to store backed-up GPOs.
2. Open a PowerShell prompt. Type **Backup-GPO -Name GPO1 -Path C:\backupgpo** and press **Enter**.
3. In the Group Policy Management console, open **GPO1** in the Group Policy Management Editor.
4. Expand **Computer Configuration, Policies, Windows Settings, Security Settings, Local Policies, and User Rights Assignment**. Double-click the **Add workstations to domain** policy.
5. Click **Define these policy settings**. Click the **Add User or Group** button, and type **Domain Users** in the User or group names text box. Click **OK** twice, and close the Group Policy Management Editor.
6. In the PowerShell window, type **Restore-GPO -Name GPO1 -Path C:\backupgpo** and press **Enter**.
7. In the Group Policy Management console, open **GPO1** in the Group Policy Management Editor.
8. Expand **Computer Configuration, Policies, Windows Settings, Security Settings, Local Policies, and User Rights Assignment**. Double-click the **Add workstations to domain** policy.
9. Verify the policy has been restored to its original setting, Not Defined.
10. Shut down all servers.

```
PS C:\Users\Administrator> Backup-GPO -Name GP01 -Path C:\backuppgo
```

```

DisplayName      : GP01
GpoId            : 7ac2ee3d-6ecf-4728-a499-20296aff509d
Id              : 5ae55a0e-43f7-4652-a989-3333432df1a6
BackupDirectory : C:\backuppgo
CreationTime     : 3/26/2021 9:59:28 AM
DomainName      : MCSA2016.local
Comment         :

```


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	MCSA2016\Domain Users
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

```
PS C:\Users\Administrator> Restore-GPO -Name GP01 -Path C:\backuppgo
```

```

DisplayName      : GP01
DomainName      : MCSA2016.local
Owner           : MCSA2016\Domain Admins
Id              : 7ac2ee3d-6ecf-4728-a499-20296aff509d
GpoStatus       : AllSettingsEnabled
Description     :
CreationTime    : 3/25/2021 9:32:53 AM
ModificationTime : 3/26/2021 10:03:37 AM
UserVersion     : AD Version: 2, SysVol Version: 2
ComputerVersion : AD Version: 3, SysVol Version: 3
WmiFilter      :

```

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
Add workstations to domain Properties ? X	
Security Policy Setting Explain	
 Add workstations to domain	
<input type="checkbox"/> Define these policy settings:	