Practical 2B – Implementing and Using Group Policy

Lab Requirements:

a) Windows Server NYP-DC1
b) Windows Client NYP-CL1 that has joined the domain.
c) File required - gpmc.msi located in ________________.

Common commands:
Open Group Policy Management: **Server Manager → Tools → Group Policy Management**
Start Active Directory Users and Computers: **Server Manager → Tools → Active Directory Users and Computers**

Practice 1

Objectives:

1. Create a GPO (Group Policy Object) in the Group Policy Objects container (folder).

Tasks:

1. On NYP-DC1, log on with your Administrator account.
2. Open **Group Policy Management**.
3. Expand frontier.net (if necessary) until you see the **Group Policy Objects** folder.
4. Right-click Group Policy Objects and select New.
5. Under Name, type **Test Policy** and hit **OK**.
6. To configure the Testing GPO, right-click Testing and select **Edit** (we shall not configure it now).
7. Close the Group Policy Management window.

You have created a GPO and this can be linked to the OUs (Organizational Unit)

Practice 2

Objectives:

1. Create new OUs and then move existing user accounts into those OUs.

Tasks:

1. On NYP-DC1, log on with your Administrator account.
2. Start Active Directory Users and Computers and create the following new OU under ***frontier.net*** domain:
    a. Marketing
    b. Information Technology

    c. Sales
3. Click the ***NYPmcp*** OU,
    a. Move ***User1 Marketing*** and ***User2 Marketing*** to ***Marketing OU***
    b. Move ***User1 IT*** to ***Information Technology OU***
4. Close Active Directory Users and Computers.

Practice 3

Objectives:

1. Use Group Policy Management to create a GPO.

Tasks:

1. On **NYP-DC1**, log on with your Administrator account.
2. Open Group Policy Management. Right-click the Marketing OU and click "Link an Existing GPO…".
3. Click "**Test Policy**" (created in Practice 1) and click **OK**. Notice that the GPO named Test Policy now appears in the list of Link Group Policy Object for Marketing.
4. Right click the Marketing OU and click "Create a GPO in this domain, and Link it here…". Type "**Marketing Policy**" and click **OK** to create a new GPO. This new GPO is now linked to the Marketing OU.
5. Right click the Marketing Policy and click **Edit**. The Group Policy Object Editor opens to allow the configuration settings of the Marketing Policy to be viewed and configured.
6. In the **User Configuration** section, click the plus sign (+) next to **Policies** and click the plus sign (+) next to **Administrative Templates** to expand its contents, and then click the **Start Menu and Taskbar** icon.
7. Double-click **Remove Documents icon from Start Menu**. Notice that the configuration settings include Not Configured, Enable, and Disabled. Do not change any configuration settings at this point.
8. Read the Help section on the purpose and notes associated with this setting. Click **OK** to close the window.
9. As time permits, browse through additional Group Policy settings in both the User Configuration and Computer Configuration sections. Do not configure any settings during this Practice.
10. Close the Group Policy Object Editor window when you are finished, along with the properties of the Marketing OU. Leave Active Directory Users and Computers open.

Practice 4

Objectives:

1. Use Group Policy Management to delete a GPO.

Tasks:

1. On NYP-DC1, log on with your Administrator account.
2. In Group Policy Management, click on the Marketing OU.
3. Select the **Test Policy** GPO and press the **Delete** button. Click **OK**.
4. Read the dialog box carefully.
5. Go to the **Group Policy Management Objects** folder to check if the **Test Policy** GPO has been deleted. Notice that the Test Policy GPO is still in the list.
6. Close all the windows except the Group Policy Management.

Practice 5

Objectives:

1. Configure and test the application of Group Policy settings.

Tasks:

1. On NYP-DC1, log on with your Administrator account.
2. Using Group Policy Management, edit the settings of the Marketing Policy GPO (right-click Marketing Policy and select Edit).
3. Under the **User Configuration → Policies** settings section, click the plus sign (+) next to **Administrative Templates** to view its contents.
4. Click the **Desktop** folder to view its contents. Double-click the **Remove Recycle Bin** icon from Desktop item to view its properties.
5. Click the **Enabled** radio button and click **OK**.
6. Click the **Start Menu and Taskbar** folder to view its contents. Double-click the **Remove Run menu from Start Menu** item to view its properties.
7. Click the **Enabled** radio button and click **OK**.
8. Click the **Control Panel** folder to view its contents. Double-click the **Prohibit access to the Control Panel** item to view its properties.
9. Click the **Enabled** radio button and click **OK**.
10. Close the Group Policy Management Editor window and the Group Policy Management window.
11. Open a Command Prompt (Admin) and run this command:

    ```
    gpupdate /force
    ```
12. On **NYP-CL1**, log on as the **user1-marketing** (which is a member of Marketing OU), using the password Pa$$w0rd.
13. Confirm that the Recycle bin does not appear on the user desktop. Click Start to confirm that both the Run command and access to Control Panel are unavailable.
14. Log off from NYP-CL1.

Practice 6

Objectives:

1. Use Group Policy settings to configure a logon banner for domain users.

Tasks:

1. On NYP-DC1, log on with your Administrator account.
2. Open Group Policy Management and edit the settings of the **Default Domain Policy** GPO.
3. In the **Computer Configuration** section, enter the **Policies** folder, click the plus signs (+) next to **Windows Settings**, **Security Settings**, and **Local Policies** to expand them.
4. Click **Security Options** to view its settings.
5. Double-click **Interactive logon: Message text for users attempting to log on** to view its properties.
6. Click the Define this policy setting in the template check box. In the text box, type “Only authorized users of Frontier.net are permitted to log on”. Click **OK**.
7. Double-click **Interactive logon: Message title for users attempting to log on** to view its properties.
8. Click the Define this policy setting check box. In the text box, type “Frontier.net Corporate Security Policy” and click **OK.**
9. Close the Group Policy Object Editor window, as well as the properties of frontier.net.
10. Open a Command Prompt (Admin) and run this command:

    gpupdate /force

11. Restart **NYP-CL1** if necessary.
12. Start **NYP-CL1**, press Ctrl-Alt-Delete (or VMware equivalent) to begin the logon process. The Frontier.net Corporate Security Policy window opens. Click **OK**.
13. Log on using your Administrator or other user account.

Practice 7

Objectives:

1. Use GPOs to assign logon scripts to domain users.

Tasks:

1. On NYP-DC1, log on with your Administrator account.
2. Open File Explorer**.** Click **View →Options → Change folder and search options**.
3. Click the **View** tab. In the **Advanced** settings section, ensure that the **Hide extensions for known file types** check box is unchecked, and click **OK**.

4. Create a **shared** folder name ***shared*** on Drive C. Set **Authenticated users** to have **Read** permission.
5. On drive C: create a new folder called ***Scripts***.
6. Open the ***Script*** folder and create a new text document.
7. Double-click **New Text Document**.txt to open it.
8. In the first line of the file, type

   net use x: \\NYP-DC1\shared

   Save the file and then close it.
9. Rename ***New Text Document.txt*** to ***logon.bat***.
10. Right-click the ***logon.bat*** file and click Copy. Close My Computer.
11. Open **Group Policy Management** and access the configuration settings of the **Marketing Policy** GPO.
12. Under **User Configuration→Policies**, click the plus sign (+) next to **Windows Settings** to expand it and then click **Scripts** (Logon/Logoff).
13. Double-click **Logon** to access its properties. Click the **Show Files** button.
14. In the new window that opens, right-click an area of free space, click **Paste**, and then close the window (the logon.bat is pasted here).
15. In the **Logon Properties** window, click **Add**. In the Add a Script window, click **Browse** and then double-click **logon.bat**. Click **OK** to close the window, and then click **OK** again to close the Logon Properties window.
16. Close the Group Policy Object Editor window.
17. Close the Group Policy Management window.
18. Open a Command Prompt (Admin) and run this command:
    gpupdate /force

19. On **NYP-CL1**, log on as the user **user1-marketing** using the password Pa$$w0rd.
20. Open **Computer** and verify that drive X has been mapped to the ***\\NYP-DC1\shared*** folder. Close **Computer**.
21. On NYP-CL1, log off and then log back on using your Administrator account. Open **Computer** to verify that drive X has not been mapped because the Administrator account does not fall under the scope of the Marketing Policy GPO.
22. Close Computer.

Practice 8

Objectives:

1. Link a single GPO to multiple containers. Create a policy to "Remove Run menu from Start Menu" and apply it to IT OU and Sales OU.

Tasks:

1. On NYP-DC1, log on with your Administrator account.
2. Create a new GPO for Information Technology OU named: ***Remove Run Command***.
3. Right click the policy and click **Edit** to access the properties of the ***Remove Run Command*** GPO.
4. Under ***User Configuration→Policies***, click the plus sign (+) next to ***Administrative Templates*** to expand it, and then click **Start Menu and Taskbar** to view its settings.
5. Enable ***Remove Run menu from Start Menu*** policy.
6. Close the Group Policy Management Editor window.
7. Link the same ***Remove Run menu from Start Menu*** policy to **Sales OU** by right clicking the Sales OU and select **Link an Existing GPO**... You will see the ***Remove Run Command*** GPO. Select it.
8. The ***Remove Run Command GPO*** is now linked to both the Information Technology OU as well as the Sales OU.
9. Close the Group Policy Management window.

Practice 9

Objectives:

1. Configure Group Policy inheritance settings. We shall enable the "Remove Run menu from Start Menu" for all domain users by linking it to the domain.

Tasks:

1. On **NYP-DC1**, log on with your Administrator account.
2. Link the "**Remove Run Command**" (created in practice 8) policy to the domain.
   - Right click **frontier.net** domain and select **Link an Existing GPO**. Select the "**Remove Run Command**" policy and click **OK**.
   - Notice the policy is now under the Default Domain Policy.
   - Now all domain users will be affected by the policy (ie. Run command disabled)
3. Close the Group Policy Management Editor window.
4. Enable **Marketing** users to be able to use the **Run** command:
   a) Access the configuration settings of the **Marketing Policy GPO** (created previously)

b) Under the **User Configuration→Policies** settings section, click the plus sign (+) next to **Administrative Templates** to expand it, and then click **Start Menu and Taskbar** to view its settings.

c) ***Disable*** the ***Remove Run menu from Start Menu*** policy. This will stop the removal of the Run command for all users in the Marketing OU.

5. Execute the following command on NYP-DC1:
   gpupdate /force
6. Log on **NYP-CL1** as **user1-IT.** Notice that the **Run** command is no longer available. Log off user1-IT.
7. Log on **NYP-CL1** as **user1-marketing**. Note that the **Run** command is available because OU-level policies are applied after domain-level policies.
8. Log off from NYP-CL1.
9. We shall enforce the "**Remove Run Command**" policy at the domain level so that it will override the Marketing policy
   a) On **NYP-DC1**, login in as **Administrator** and open the **Group Policy Management**.
   b) Right-click the "**Remove Run Command" Policy** and click on **Enforced**.
   This will prevent settings in it from being overridden by policy settings applied at the OU level. Run the **gpupdate /force** command on NYP-DC1 (and if necessary on NYP-CL1).
10. Log on **NYP-CL1** as user **user1-marketing**. Verify that the **Run** command no longer appears. Why is this so?
11. On **NYP-DC1**, remove the **Enforced** setting from the **"Remove Run Command" Policy** GPO. Close all open windows.

Practice 10

Objectives:

1. Use security permissions to filter and control the application of Group Policy settings. Block the Marketing policy from applying to user1-marketing.

Tasks:

1. Log in to NYP-DC1 as Administrator. We shall exclude user1-marketing from the Marketing Policy.
2. Open **Group Policy Management**, and click on the **Marketing Policy** under the **Marketing OU**. (Note: click in the **LEFT** panel)
3. The right panel will show four tabs – Scope, Details, Settings, Delegation.
4. Click the **Delegation** tab, and review the permissions associated with the Authenticated Users group. Note that this group has only the **Read** permission allowed.
5. Click **Add**. In the Enter the object names to select text box, type **User1-marketing → Check Names → OK → OK**. The user1-marketing has **Read** permission.

6. Click on the **Advanced** button at the bottom right corner (maximize the window if you cannot see the Advanced button).
7. Click to select **User1 Marketing** user account and note the Permissions for user1-marketing. Check the **Deny** check box for the Full Control permission setting. This will stop settings in the Marketing Policy GPO from applying to User1 Marketing. Click **OK**. Click **Yes** in the Windows Security dialog box.
8. Close all open windows and log off.
9. On **NYP-CL1**, log on as the user **user2-marketing** with the password Pa$$w0rd. Click the Start menu to confirm that the Run command is available for user2-marketing as per the Marketing Policy GPO setting. Log off.
10. Log on **NYP-CL1** as user **user1-marketing** with the password Pa$$w0rd. Click the Start menu to confirm that the Run command is **not** available for user1-marketing because the Marketing Policy GPO does not apply due to permission filtering. As such, the policy settings applied by the "Remove Run Command" Policy are applied to the user1-marketing user account.
11. Log off from NYP-CL1.

Practice 11

Objectives:

1. Publish an application using Group Policy settings.

Tasks:

1. On NYP-DC1, log on with your Administrator account.
2. Create a new folder in C:\ called **source**
3. Copy **gpmc.msi** to NYP-DC1 **C:\source** in the virtual server. Your instructor will inform you where gpmc.msi is located.
4. Open the ***C:\Source*** folder. Copy the files named ***gpmc.msi*** to the ***C:\shared*** folder (*shared* was created in Practice 7).
5. Open **Group Policy Management** and create a new GPO named ***GPMC Publishing.*** Link it to the Information Technology OU.
6. Click Edit to access the configuration settings of the ***GPMC Publishing*** Group Policy Object.
7. Under **User Configuration→Policies**, click the plus sign (+) next to **Software Settings** to expand it.
8. Right-click **Software installation**, click **New**, and then click **Package**.
9. In the Open dialog box, type \\NYP-DC1\shared \gpmc.msi in the File name text box and click **Open**.
10. In the Deploy Software dialog box, ensure that the **Published** radio button is selected and click **OK**. Click on the Software installation icon. Notice that the ____________****,*** version, deployment state and source information is now listed.

11. Run **gpupdate /force** on both NYP-DC1 and NYP-CL1 with administrator account.
12. On **NYP-CL1**, log on as **user1-it** using the password Pa$$w0rd.
13. Click **Start**, click **Control Panel → Programs and Features → Install a program from the network.** Notice that the ________* is now available for installation by the user1-it user account.
14. You can try installing it.

* *Write down the software title displayed*

Practice 12

Objectives:

1. Use RSoP to determine effective Group Policy settings.

Tasks:

1. On NYP-DC1, log on with your Administrator account.
2. Open **Group Policy Management.**
3. Access the configuration settings of the **Default Domain Policy** GPO.
4. Under the **User Configuration→Policies** settings section, click the plus sign (+) next to **Administrative** Templates to expand it, and then click **Start Menu and Taskbar** to view its settings.
5. Double-click **Remove Run menu from Start Menu**, click the **Disabled** radio button, and then click **OK**. This will once again enable the Run command for all domain users.
6. Close the Group Policy Management window.
7. Run the **gpudpdate /force** command.
8. Open a new **MMC** and add the **Resultant Set of Policy** (RSoP) snap-in.
9. Right-click the Resultant Set of Policy icon and click **Generate RSoP Data**.
10. At the Resultant Set of Policy Wizard welcome screen, click **Next**.
11. At the Mode Selection window, ensure that the **Logging mode** radio button is selected and click **Next.**
12. At the Computer Selection window, ensure that the **This computer** radio button is selected, and click **Next**.
13. At the User Selection window, click the Select a specific user radio button. Click the **Frontier\administrator** user account and then click **Next**.
14. At the Summary of Selections window, click **Next** to begin the analysis process.
15. Click **Finish** to complete the Resultant Set of Policy Wizard.
16. Click the sign next to ***Administrator on NYP-DC1 – RSOP***. Under the Computer Configuration section, click the plus signs (+) next to **Windows Settings**, **Security Settings**, and **Local Policies** to expand them. Click **Security Options** to view its settings.
17. Scroll through the list to view the Security Options that are applied to the Administrator user account as a result of Group Policy settings.

18. If time permits, browse through additional sections to view other policies that have been applied to the Administrator user account via GPO settings.
19. Close the MMC without saving changes.

Note:
You can also try the gpresult command.
Open a Command Prompt (Admin) and type **gpresult /R > c:\rsop.txt**
Try also: **gpresult /V > c:\rsop_verbose.txt**
Examine the 2 text files. Type gpresult /? to see all the options.

Practice 13

Objectives:

1. Install the Group Policy Management Console.
2. Create a linked GPO.
3. Back up and restore a GPO.
4. Use Group Policy reporting to view the settings in a GPO and save the report.
5. Create a Group Policy Results report.

Tasks:

1. On NYP-DC1, log in as Administrator.
2. Launch Group Policy Management from the Administrative start menu.
3. Right-click the **Marketing** OU, and click **Create and Link a GPO Here**.
4. In the **New GPO** dialog box, type **Lockdown** and click **OK**.
5. In the left panel, click on **Group Policy Objects** to expand it.
6. Right-click the **Lockdown** GPO, and click **Back up**.
7. In the **Backup Group Policy Object** dialog box, click **Browse** and click onto **C:** drive. Click **Make New Folder** and name it as **GPO Backup**. Click **OK**.
8. Click **Back Up** and click **OK**.
9. Delete the **Lockdown** GPO from the Group Policy Objects folder.
10. Right-click the **Group Policy Objects** folder, and click **Manage Backups**.
11. Select the **Lockdown** GPO, and click **Restore**.
12. Click **OK** twice and click **Close**. Notice that the **Lockdown** GPO has been restored.
13. Expand the **Group Policy Objects** folder.
14. In the left console pane, click the **Marketing Policy** GPO.
15. In the right pane, click the **Settings** tab.
16. View the settings of the GPO.
17. Right-click anywhere on the report and select **Save Report** from the shortcut menu.
18. Save the report as an HTML file in C:\.
19. Browse to C:\ and open the **Marketing Policy.htm** file. Click **Allow block content** at the **Information Bar** prompt.
20. View the report.
21. Go back to **Group Policy Management**.

22. Right-click the **Group Policy Results** folder and then click **Group Policy Results Wizard**.
23. In the **Group Policy Results Wizard**, click **Next**.
24. In the **Computer Selection** page, accept the default, which is **This Computer**, and then click **Next**.
25. In the **User Selection** page, accept the default and then click **Next**.
26. In the **Summary of Selections** page, click **Next**.
27. Click **Finish**.
28. Browse through the report information.
29. Close all windows and log off.

[End]