Lab Overview

Lab Objectives
• Configure GPO Scope
• Configure GPO Link Order, Inheritance and Enforcement
• Delegate Group Policy Management Tasks
• Generate GPO Settings Reports
• Backup and Restore GPOs
• Generate Group Policy Results
• Copy GPOs in the Same and Cross-domain
• Execute scripts to manage Group Policy

Lab Audience

Lab Scenario

Estimated Lab Time
Lab Setup

Virtual PC 2004 Overview
This lab makes use of Virtual PC 2004, an application that allows you to run multiple virtual computers on the same physical hardware. During the labs you will work with two virtual PC sessions, each of which contains a separate virtual computer running Windows Server 2003 Enterprise Edition (the window for one of these virtual machines will be minimized for the full duration of the lab). These images are fully functional images running as domain controllers - see the Virtual Lab Machines section for more details.

Setting the Focus:
In order for a virtual PC to have the focus (e.g. for you to actually work with it) you must **single click** inside of it, as with any other application running on the “host machine”.

Unsetting the Focus:
To move your cursor outside of the virtual PC, simply move the mouse outside the boundaries of the virtual machine and click a different application.

Right-Alt Key
Note that some commands for Virtual PC 2004 require that the Alt key on the right hand side of the keyboard be used (the Alt key on the left hand side of the keyboard is not available for this purpose)

Logging on to a virtual PC
To enter user credentials at a logon prompt, press **Right Alt+Delete**. This will prompt you for a username and password and is your first step when running the labs.

Toggling between a Window and Full Screen
At any time you can switch a virtual PC screen between being visible in a window and running full screen. To toggle back and forth, press **Right Alt+Enter**.

Lab Virtual Machines

<table>
<thead>
<tr>
<th>Machine Name</th>
<th>Purpose</th>
<th>Domain</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPMC</td>
<td>Production Domain DC</td>
<td>GPMCDemo.com</td>
<td>192.168.0.1</td>
</tr>
<tr>
<td>Test</td>
<td>Test Domain DC</td>
<td>Test1.GPMCDemo.com</td>
<td>192.168.0.2</td>
</tr>
</tbody>
</table>
To start the lab

Log onto the Host machine and start the Virtual PC Console:
A. If you are not already logged onto the Host machine, do so using the supplied credentials. See a Hands-on-Lab proctor if you need assistance with this (typically a host machine will already be logged on when you sit down at that machine).
B. On the Host, start the Virtual PC 2004 console.

Start the GPMCDemo virtual PC:
A. Highlight the GPMCDemo virtual machine (within the Virtual PC 2004 console) and click Start.
B. After the GPMCDemo virtual machine starts, minimize the virtual PC. You do not need to log on to this virtual session and it should remain minimized for the duration of the lab.

**Important:** You will not perform any additional steps in the GPMCDemo virtual PC. All work in this lab is now performed in the Test1.GPMCDemo virtual PC (which will now be referred to as Test1).
The GPMCDemo virtual PC needs to be running since you’ll be communicating with it over the virtual network between the two virtual PC’s.

Start the Test1.GPMCDemo virtual machine
A. Select the Test1.GPMCDemo virtual machine and click Start.
B. After the Test1.GPMCDemo virtual machine starts, click anywhere inside the Test1.GPMCDemo virtual PC to ensure it has the focus.
C. Press Right Alt+Delete (this equals the traditional Ctrl-Alt-Del). The Log On to Windows dialog appears
D. Logon as Administrator, with a password of pass@word1

**Important Shutdown Steps**
When you complete this GPMC lab, you have to end the lab prematurely or you visit the machine with the previous users virtual PC’s session still running, please make sure you shut down both virtual machines. This ensures that the next person to use the lab starts afresh.
A. For each virtual machine:
   • Ensure the virtual machine has the focus.
   • Select Action menu and select the Close option.
Step # 1
Launch and Configure the GPMC

Scenario

You are an administrator in a large organization in charge of managing Group Policy. You will use the Group Policy Management Console (GPMC) to facilitate management of the Group Policy environment. Since you’re in a distributed environment, you also want to ensure you are talking to the correct domain controller for each domain because it is important to avoid replication conflicts. Replication conflicts might occur since there may be latency in the replication used to ensure domain controllers receive the same version of each GPO. If two administrators are simultaneously editing the same GPO on different domain controllers, it is possible for the changes written by one administrator to be overwritten by another administrator, depending on this replication latency.

For the purposes of the lab, you have already obtained and installed GPMC on your computer and will now launch and configure GPMC.

Note that, unless otherwise stated, all the steps described in the remainder of this lab are to be carried out in the Test1 Virtual PC session.

Goal

Launch and configure the GPMC console to show all domains in the forest and to view domain controller options.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Detailed Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Launch GPMC</td>
<td>a. Click Start, All Programs, Administrative Tools, Group Policy Management and maximize the resultant window. Note: You can also launch GPMC by typing GPMC.msc from the Start, Run dialog.</td>
</tr>
</tbody>
</table>
| 2. Configure the GPMC console | a. Once GPMC starts, expand the Domains node in GPMC (in the tree view on the left hand side). You will see that only the Test1.GPMCDemo.com domain is listed.  
                             | b. Right-click the Domains node, and select Show Domains... from the context menu.  
                             | c. Click the checkbox next to the GPMCDemo.com option and then click OK.  
                             | d. The GPMCDemo.com domain has now been added to the console. |
| 3. View Domain Controller options | a. Right-click the GPMCDemo.com domain node and select Change Domain Controller. This displays the Change Domain Controller dialog. Notice that you are able to specify which domain controller to use in order to avoid potential replication conflicts.  
                             | b. Click Cancel since we don’t want to make any changes. |
Step # 2  
Configure GPO Scope

Scenario
The value of implementing Group Policy for your organization can only be realized by properly scoping GPOs so that they apply to the desired users and computers within Organizational Units (OUs) that you want to manage. Using GPMC, you can scope GPOs based on three factors:

- Linking it to an OU, Domain, or Site
- Using Security filtering
- Using WMI Filters

Goal
Configure the scope of GPOs in your organization.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Detailed Steps</th>
</tr>
</thead>
</table>
| 1. Link an existing GPO to an Organizational Unit by drag and drop | a. Expand the GPMCDemo.com node.  
b. Expand the Engineering - Offsite OU which is in the GPMCDemo.com domain. Notice there is an existing GPO linked to this OU, called Common Managed Settings (the GPO Link appears under the OU as a separate icon).  
c. Expand the Group Policy Objects node in GPMCDemo.com domain, and then click on the LightlyManaged User Settings GPO.  
d. Drag the LightlyManaged User Settings GPO to the Engineering - Offsite OU. This links the LightlyManaged User Settings GPO to the Engineering - Offsite OU.  
e. Click OK at the link confirmation dialog.  
f. Refer back to the Engineering - Offsite OU node, notice the LightlyManaged User Settings GPO is now linked to this OU. Every object (users or computers) in the Engineering - Offsite OU will now have the LightlyManaged Users Settings GPO apply to it. |
| 2. Modify which user/groups will have the GPO apply to them by using Security Filtering | a. Click the LightlyManaged User Settings GPO, which is under the Group Policy Objects node.  
b. In the scope tab, within the Security Filtering Section, select the Authenticated Users group and click the Remove button. Click OK to the confirmation dialog.  
c. Click the Add button.  
d. In the Select User, Computer, or Group dialog box, enter the Mobile Users group then click OK. Now only members of this group, which are in an OU that has the LightlyManaged User Settings GPO linked to it, will have the GPO settings applied to them. |
3. Review targeting specific machines using a WMI Filter

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Review targeting specific machines using a WMI Filter</td>
</tr>
<tr>
<td></td>
<td>a. While still in the scope tab for the Lightly Managed User Settings GPO, under the WMI Filtering section, notice no WMI filters are currently linked to the GPO. This means the GPO is not scoped based on attributes of a target computer. Even though you don’t need to use a WMI Filer at this time, click on the WMI Filter drop-down and review the available WMI Filters. Make sure you do not select a WMI Filter.</td>
</tr>
</tbody>
</table>

4. Create a new GPO and Link it to an Organizational Unit (OU)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>Create a new GPO and Link it to an Organizational Unit (OU)</td>
</tr>
<tr>
<td></td>
<td>a. Expand the Corp Headquarters\ Servers\Terminal Servers OU.</td>
</tr>
<tr>
<td></td>
<td>b. Right-click the Terminal Servers OU and select Create and link a GPO here from the context menu.</td>
</tr>
<tr>
<td></td>
<td>c. Name the new GPO TS Security and press OK.</td>
</tr>
<tr>
<td></td>
<td>d. Notice that the TS Security GPO has been created under the Group Policy Objects node.</td>
</tr>
<tr>
<td></td>
<td>e. Expand the Terminal Servers OU. Notice the TS Security GPO has also been linked to the Terminal Servers OU. Also notice that the icon for the TS Security GPO link is different from the icon for the TS Security GPO.</td>
</tr>
</tbody>
</table>
Step # 3
Edit an Existing GPO

Scenario
Now that you have properly scoped the TS Security GPO to the Terminal Servers OU, you need to configure settings within the GPO.

Goal
Use GPMC to launch the Group Policy Object Editor to configure a setting within a GPO.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Detailed Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Edit an existing GPO</td>
<td>a. Right-click the TS Security GPO link, which is under the Corp Headquarters</td>
</tr>
</tbody>
</table>
Step # 4
Configure GPO Link Order and Inheritance

Scenario
You have received multiple change requests to fine-tune how GPOs apply and are inherited in your Group Policy infrastructure. These changes include changing GPO link order and inheritance for an OU.

Goal
Understand how GPO link order and GPO inheritance can be used in your organization.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Detailed Steps</th>
</tr>
</thead>
</table>
| 1. Configure the order in which GPOs are linked to a node | a. Click on the GPMCDemo.com node.  
   b. Under the Linked Group Policy Objects tab, notice that three GPOs are linked to the GPMCDemo.com node and will apply according to their link order.  
   Note: The GPO with the lowest link order has the highest precedence since it will apply last to a user or computer.  
   c. To ensure the WW EFS Recovery Policy has higher precedence than the WW ITG Policy, click on the WW EFS Recovery Policy and click the Move Link Up Arrow (single arrow). |
| 2. Review the order in which GPOs are inherited by child OUs from a parent OU | a. Click on the Corp Headquarters\Servers\Terminal Servers OU.  
   b. Select the Group Policy Inheritance tab.  
   c. Review the list of GPOs that are inherited by and linked to the Terminal Servers OU from its parent. |
| 3. Block GPO inheritance for the Terminal Servers OU | a. Right-click the Terminal Servers OU and select Block Inheritance from the context menu.  
   b. Now review the list of GPOs under the Group Policy Inheritance tab. Notice only one GPO is now applied to the OU - the TS Security GPO linked to this OU. All GPOs that would normally be inherited from parent OUs have been blocked and will no longer apply to objects in this OU or children OUs. Also notice the blue exclamation mark on the Terminal Servers OU which visually denotes that the OU has block inheritance set.  
   Note: If an Enforced GPO was linked to a parent OU, it will always be inherited even if Block Inheritance is set on a child OU. Enforced GPOs take precedence over any GPOs that are linked to child containers. Enforcing a GPO link works by moving that GPO to the end of the processing order. |
Step # 5
Delegate Group Policy Management Tasks

Scenario
Due to the size of your corporation’s infrastructure, a number of Group Policy management tasks are performed by multiple administrators. Using GPMC, you will delegate the following Group Policy management tasks:

- The ability to create GPOs in a domain by users in the same or in external domains.
- Permissions on an individual GPO (for example, read access).
- Permissions on an individual Site, Domain or Organizational Unit (SOM).
- The ability to create WMI filters in a domain.
- Permissions on an individual WMI filter (for example, edit access)

Goal
Understand how GPMC allows administrators to delegate various Group Policy management tasks.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Detailed Steps</th>
</tr>
</thead>
</table>
| 1. Delegate GPO Creation to a user in the same domain | a. Click on the Group Policy Object node in the GPMCDemo.com domain then select the Delegation tab.  
   b. Review the list of groups and users - these have permission to create GPOs in the GPMCDemo.com domain.  
   c. Double-click on the Group Policy Creator Owners (GPMCDemo\Group Policy Creator Owners) group then select the Members tab.  
   d. Click the Add button.  
   e. In the Select User Computer, or Group dialog, the location should already default to the GPMCDemo.com domain. This means you are adding a user or group from the GPMCDemo.com domain.  
   f. While still in the Select User Computer, or Group dialog, enter AnthonyC. Click Ok.  
   g. Click OK again to exit the dialog. GPMCDemo\AnthonyC has now been added to the GPMCDemo\Group Policy Creator Owners group and now has the ability to create a GPO in the GPMCDemo.com domain.  |

Note: Adjusting the membership of the Group Policy Creators Owners (GPCO) group is the same mechanism that existed in Windows 2000. This is just a different UI for performing the same task. However, since the GPCO group is a domain global group, it cannot contain members from outside the domain. Thus, prior to GPMC, this task could not be delegated to members outside the domain. It is recommended that for users and groups within the domain that you continue to use the
2. Delegate GPO Creation to a user in an external domain
   a. While still in the **Delegation** tab for the **Group Policy Objects** node, click the **Add** button.
   b. In the Select User Computer, or Group dialog, enter **GPCO X-Domain** and click **OK**.
   c. Double-click on the **GPCO X-domain** (GPMCDemo\GPCO X-Domain) group then select the **Members** tab and click **Add**. Note that this is a domain local group, so you can add members to it from other domains.
   d. In the Select User Computer, or Group dialog, click the **Locations** button. In the locations dialog, expand the **GPMCDemo.com** domain then select the **Test1.GPMCDemo.com** domain (you may need to scroll down to locate this domain). Click **OK** to close the **Locations** dialog.
   e. While still in the Select User Computer, or Group dialog, enter **BrianV**. Click **Ok**.
   f. Click **OK** again to exit the dialog. **Test1\BrianV**, who is in the **Test1.GPMCDemo.com** domain, now has the ability to create GPOs in the **GPMCDemo.com** domain.

3. Delegate Permissions on an Individual GPO
   a. Under the **Group Policy Objects** node, click on the **TS Security GPO**
   b. Click on the **Delegation** tab
   c. To grant users/groups permission on this GPO, click the **Add** button.
   d. In the Select User Computer, or Group dialog, enter **Dave Thompson** then click **OK**.
   e. In the Add Group or User dialog, select the **Edit settings, delete, modify security Permissions and click OK**

4. Delegate Permissions on a SOM (Scope of Management)
   a. Select the **GPMCDemo.com node**.
   b. Click on the **Delegation** tab.
   c. Review the three delegation options by selecting each permission from the drop down (Link GPOs, Perform Group Policy Modeling Analyses, Read Group Policy Results Data) and note that the list of groups and users changes for each option.
   d. Select the **Read Group Policy Results data** option in the Permission drop-down box.
   e. Click the **Add** button.
   f. In the Select User Computer, or Group dialog, enter **HelpDesk** then click **OK**.
   g. In the Add Group or User dialog, select **This Container and all Child Containers** permission. Then click **OK**.

5. Delegate WMI Filter Creation
   a. Click on the **WMI Filters** node (a child of the **GPMCDemo.com** node) then select the **Delegation** tab
   b. Review the existing groups and users that have permission to create WMI filters in the **GPMCDemo.com** domain.
c. Click the Add button
d. In the Select User Computer, or Group dialog, enter **GPAdmins** then click OK.
e. In the Add Group or User dialog, select **Full control** permission. Then click OK. The users in the GPAdmins group now have full control over all WMI Filters in the GPMCDemo.com domain including those that they didn’t create.

| 6. Delegate Individual WMI Filter Permissions | a. Expand the **WMI Filters** node, click on the WinXP WMI Filter then select the **Delegation** tab.  
b. Review the existing groups and users that have permissions on the WinXP WMI Filter.  
c. Click the **Add** button  
d. In the Select User Computer, or Group dialog, enter **Delegated Admins** then click **OK**  
e. In the Add Group or User dialog, select **Full control** permission. Then click **OK**. The users in the Delegated Admins group now have full control over the WinXP WMI Filter in the GPMCDemo.com domain.  
d. Click on the **General** tab.  
e. Review the description of the WMI Filter and the WMI query that will be executed on the targeted client once the WMI Filter is linked to a GPO. |
Step # 6  
GPO Settings Reporting

Scenario

One of the biggest problems that you encountered as an administrator managing your corporation’s Group Policy infrastructure prior to using GPMC is obtaining a comprehensive report of all settings within a particular GPO. Fortunately, the settings tab of a GPO or GPO link pane in GPMC now shows an HTML report that displays all the defined settings in a GPO. This report can be generated by any user with read access to the GPO.

Goal

Understand GPMC’s reporting abilities.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Detailed Steps</th>
</tr>
</thead>
</table>
| 1. Generate a GPO Settings Report          | a. Click on the Default Domain Policy GPO link under the GPMCDemo.com domain. Click OK to the confirmation dialog.  
                                          | b. Click on the Settings tab. Clicking this tab will generate a report of the settings for the GPO.  
                                          | c. Once the report is generated, click on the Show All link.  
                                          | d. Review the various settings contained within the GPO settings report.  
                                          | e. You can also expand individual sections in the report by clicking each heading.                                                              |
| 2. Save the GPO Settings Report to the local file system | a. Right-click anywhere in the actual report to display the report’s context menu and select the Save Report option. Give the report a name, select HTML as the file type and save it to the local drive.  
                                          | Note that you could have also saved the report as XML.  |
| 3. View a GPO Settings Report outside of GPMC | a. Using file explorer, navigate to the location where you saved the GPO settings report.  
                                          | b. Double-click on the report to view the report in Internet Explorer.  
                                          | c. Click on the Show All link.  
                                          | d. Close IE and File Explorer.  
                                          | Note: If you view a GPO Settings report outside of GPMC, the report will also contain information from the Scope, Details and Delegation tabs. This information is not shown in the report in GPMC because it is redundant. |
Step # 7
Backing up GPOs

Scenario
As part of standard operating procedures, administrators at your corporation backup any GPO prior to modifying its settings. Furthermore, all GPOs are backed up on a regular basis as part of a larger disaster recovery plan. Backing up GPOs ensures that a GPO can be restored to a prior known state.

When you backup a GPO, all relevant GPO data is copied into a specified file system location. The relevant data includes:

- The GPO GUID and domain.
- GPO Settings.
- The Discretionary Access Control List (DACL) on the GPO.
- WMI filter link (but not the filter itself).

The backup operation does not capture items stored outside the GPO, such as WMI filters, links to a Site or OU to that GPO, and IP Security policy data.

Goal
Use GPMC to backup GPOs.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Detailed Steps</th>
</tr>
</thead>
</table>
| 1. Backup a GPO        | a. From the Group Policy Objects node in the Test1.GPMDemo.com domain (note the change of domain), right-click on the WW ITG Policy GPO and select Back up... from the context menu.  
   b. For location, type c:\GPOBackups and type a meaningful backup Description. Then click Backup.  
   c. After the backup succeeds, click OK to close the backup window.  
   Note: You can backup all GPOs in a domain at once by choosing the “Backup all...” option which is available by right-clicking the Group Policy Objects node and selecting Backup All... from the context menu. This will backup all GPOs to the same file system location. In the interest of time, you won’t do this in this lab. |
| 2. Manage your Backups | a. Right-click on the Domains Node and select Manage Backups from the context menu. This will show all backed up GPOs regardless of the domain.  
   b. Ensure that the Manage Backup dialog is pointing to c:\GPOBackups for backup location.  
   c. Review the list of backed up GPOs that are displayed for the specified file system location.  
   Note: When viewing a list of backed up GPOs from the |
| Manage Backup dialog, you can view the settings contained within each backed up GPO by clicking the View Settings button. Also, if you have multiple backups of a GPO, select the Show only the latest version of each GPO check box to view only the latest backup of each GPO.

d. Close the Manage Backups dialog. |
Step # 8
Restoring GPOs

Scenario
You recently made multiple settings changes to a GPO which worked fine in your test environment, but appears not he working as expected in production. Fortunately, you backed up the GPO prior to making these changes and you will now restore it to its prior state. When you restore the GPO, the following components of the GPO will be restored:

- GPO Settings
- ACLs on the GPO
- WMI filter links (but not the filters themselves)

The restore operation will not restore GPO links, but if an existing GPO link is present, the GPO link will continued to be used.

Goal
Restore a GPO back to a prior state.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Detailed Steps</th>
</tr>
</thead>
</table>
| 1. Restore a GPO | a. From the Group Policy Objects node in the Test1.GPMCDemo.com domain, right-click on the WW ITG Policy GPO and select Restore from Backup from the context menu.  
b. The Restore Group Policy Object Wizard dialog appears. Click Next.  
c. Ensure the backup location is c:\GPOBackups then click Next.  
d. Select the WW ITG Policy that you previously backed up then click Next.  
e. Click Finish to restore the GPO.  
f. After the restore succeeds, click OK.  
Note: You can also restore a GPO via the Manage Backup Dialog if a GPO was previously deleted. |
Step # 9
Copy GPO - Same Domain

Scenario
Due to the recent acquisition of a small sales company that will now be integrated into your corporation, you need to create a GPO to properly manage these new users and computers. But instead of creating a new GPO from scratch, you can copy an existing GPO and use it as a template to build the new GPO.

Goal
Use the copy features of GPMC to create a GPO in the same domain and across domains.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Detailed Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Copy a GPO in the same domain</td>
<td>a. From the Group Policy Objects node in the Test1.GPMCDemo.com domain, right-click on the Common Managed Settings GPO and select Copy from the context menu.</td>
</tr>
<tr>
<td></td>
<td>b. Right-click the Group Policy Objects node and select paste.</td>
</tr>
<tr>
<td></td>
<td>c. For the Copy GPO dialog, select the Use default permissions for new GPOs option and click OK.</td>
</tr>
<tr>
<td></td>
<td>d. Once the copy is successfully completed, click OK.</td>
</tr>
<tr>
<td></td>
<td>e. Since a GPO with the same name already exists, the new GPO is named “Copy of Common Managed Settings”.</td>
</tr>
<tr>
<td></td>
<td>f. Right-click on “Copy of Common Managed Settings” and select rename from the context menu.</td>
</tr>
<tr>
<td></td>
<td>g. Rename the GPO Remote Sales Settings.</td>
</tr>
<tr>
<td>2. Link the new GPO to the Sales and Marketing OU</td>
<td>a. Right-click on the Sales and Marketing OU in the Test1.GPMCDemo.com domain and select Link an existing GPO from the context menu.</td>
</tr>
<tr>
<td></td>
<td>b. Ensure you are looking in the Test1.GPMCDemo.com domain then select the Remote Sales Settings GPO and click OK.</td>
</tr>
</tbody>
</table>
Step # 10  
Generating Group Policy Results

Scenario
You want to start aggressively managing users in your production domain but you want to first verify the impact of the new GPO in your test environment prior to deploying it to production. So in the Test1.GPMCDemo.com domain, you have already created a new OU called Highly Managed and located it under the Corp Headquarters\User Accounts OU. You have also created a new GPO called Highly Managed Users and have linked it to the Highly Managed OU (if you expand the Highly Managed OU, you will see the GPO link as a child node).

Your next step is to see the impact of this new GPO by logging into the test environment as a user that is in the targeted Highly Managed OU. When you log into the test environment, you notice a deployment error. To investigate this error, you will use Group Policy Results to determine the resultant set of policy that was applied to this user.

Goal
Use Group Policy Results to review the settings actually applied to a user.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Detailed Steps</th>
</tr>
</thead>
</table>
| 1. Show user experience in test environment | a. Minimize GPMC.  
b. From the Test1 virtual machine, double-click the BrianV-Test.rdp icon which is on the desktop (be careful to distinguish this from the BrianV-Prod.rdp icon, which is also on the desktop).  
You have now started a terminal server session by logging in as BrianV into the Test1.GPMCDemo.com domain.  
Note: The password for Test1\BrianV is pass@word2 and has been saved as part of the session in order to speed up the lab. Occasionally, the screen background for the terminal server session may not fully refresh when first displayed - if this occurs, press F5 to complete the background.  
c. Now click on Start. Notice the RUN menu item is available.  
This is a deployment error and it is your task to identify the cause of the problem. The run command shouldn’t be available to BrianV, who is in the highly managed users OU.  
d. Click Start, Log Off BrianV, to end BrianV’s session.  
e. Click Log off to the confirmation dialog. |
| 2. Run Group Policy Results to find why the deployment error is occurring | a. Maximize GPMC.  
b. Right-click the Group Policy Results node (you might have to scroll down) and select the Group Policy Results Wizard... option from the context menu.  
c. Click Next.  
d. Select the default This Computer option and click Next.  
e. Select the Select a specific user: option, then select |
Test1\BrianV. Click Next.
f. Click Next again to gather policy settings for BrianV.
g. Click Finish.
h. Press Enter to save the generated report using the default name.
i. Click on the generated report, and then select the Settings tab.
j. Click the Show link next to the User Configuration\Administrative Templates\Start Menu and Taskbar report heading. Scroll down to the Remove Run menu from Start Menu setting - notice that it is Disabled and that the winning GPO is the WW ITG Policy GPO! You did not expect this result because your new Highly Managed Users GPO had enabled this setting and you expected this GPO to be the winning GPO. For some reason, it is not applying.

Note: Click on the setting name to view the explain text for that setting.
k. From within the Test1.GPMCDemo.com domain, click on the Corp Headquarters\User Accounts\Highly Managed OU and select the Group Policy Inheritance tab. Notice that the WW ITG Policy has higher precedence than the Highly Managed Users GPO because it is marked as Enforced. This is the deployment error. The WW ITG Policy should not be enforced. To correct this, the enforcement property of the WW ITG Policy needs to be removed.

Note: Now that you understand the deployment error, you will now copy this GPO to the production domain in the next step. To expedite the lab, the Enforced property of the WW ITG Policy has already been removed in the GPMCDemo.com domain. You may resolve this in the Test1 domain by right-clicking the WW ITG Policy GPO link (under the Test1 domain node) and unchecking the Enforced option from the context menu.
Step # 11
Copy GPO - Cross Domain

Scenario
After you have identified and “fixed” the GPO deployment error in the test environment, it's now time to deploy the Highly Managed Users GPO into the production environment. GPMC allows you to quickly do this by supplying a cross-domain copy wizard.

Note that when copying GPOs across domains, some information in the GPO may be specific to the domain where the GPO is defined. Items that can be specific to a domain include references to security principals such as users, groups, and computers as well as UNC paths. When copy the GPO to a new domain, it may not always be desirable, or even possible, to use the same references. The solution is to modify these domain-specific references in the GPO, during the import or copy operation, so that the settings in the destination GPO are written with the appropriate information for the destination domain. GPMC supports this capability using a concept called migration tables. You can create migration tables using the Migration Table Editor (MTE), which is part of GPMC.

Since the Highly Managed Users GPO contains both UNC paths and security principals, you will use the MTE to map these to new values in the destination GPO. This mapping is necessary because the references to UNCs or security principals in the GPO’s source domain are not valid in the domain of the destination GPO.

Goal
Use GPMC to copy a GPO from one domain to another.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Detailed Steps</th>
</tr>
</thead>
</table>
| 1. Copy the Highly Managed Users GPO from Test to Production | a. From the Group Policy Objects node in the Test1.GPMCDemo.com domain, right-click on the Highly Managed Users GPO and select Copy from the context menu.  
b. Right-click the Group Policy Objects node in the GPMC Demo.com domain (note the change of domain) and select Paste from the context menu.  
Note: You can also copy a GPO by dragging and dropping a GPO from a source Group Policy Objects node to a destination Group Policy Objects node. Do not drag the source to a domain or OU - that creates a cross-domain GPO link, which is generally not advised.  
c. The cross-domain copying wizard appears. Click Next.  
d. On the Specifying Permissions page, leave the Use the default permissions for new GPOs option checked and click Next.  
e. The scan results will indicate that the GPO contains security principals or UNC paths. Click Next.  
f. On the Migrating References page in the wizard, select the Using this migration table option, then click the New button. |
g. The Migration Table Editor (MTE) appears. From the MTE menu, select Tools, Populate from GPO. Select the Test1.GPMCDemo.com domain, and then select the Highly Managed Users GPO. Click OK. This option extracts all security principals and UNC paths that are referenced in this GPO, and enters them into the migration table. By default, the destination is set to Same As Source. In the next 2 steps below, you will specify the destination values.

h. To modify the destination values for the security principals in the migration table, press and hold the ctrl button while clicking the cell handles for the first two rows. The first two rows should now be highlighted. Right-click the highlighted rows and select the Set Destination, Map by Relative Name from the context menu.

i. To modify destination values for UNC paths in the migration table, double-click in the Source Name cell for the third row. Copy the source value to the Destination Name cell. In the Destination Name cell, change the \Test1\FR path to \GPMCDemo\FR. Do the same for the fourth row.

j. From the MTE’s menu, select File, Save. Select and confirm overwriting of the existing HighlyManaged.migtable file (ordinarily this file would not exist and you would create a new file - it is placed there for convenience during this lab).

k. Close the MTE by selecting File, Exit.

l. The migration table path is now pre-filled in the wizard. Click Next.

m. Click Finish.

n. When the copy process is successful, click OK. The Highly Managed Users GPO has now been successfully copied from the test environment (Test1.GPMCDemo) to production environment (GPMCDemo) using a Migration Table.

2. Link Highly Managed Users

a. From the GPMCDemo.com domain, right-click on the Corp Headquarters\User Accounts\Highly Managed OU and choose Link an Existing GPO from the context menu.

b. Ensure you are looking in the GPMCDemo.com domain then select the Highly Managed Users GPO and click OK.

3. Show user experience in production environment

a. Minimize GPMC.

b. From the Test1 virtual machine, double-click the BrianV - Prod.rdp icon which is on the desktop.

You have now started a terminal server session by logging in as BrianV into the GPMCDemo.com domain.

Note: The password for GPMCDemo\BrianV is pass@word2 and has been saved as part of the session in order to speed up the lab.

c. Now click on Start. Notice the RUN menu item has been removed. The deployment error has been fixed and the GPO has been successfully deployed to production.

d. Click Start, Log Off BrianV, to end BrianV’s session.

e. Click Log off to the confirmation dialog
Step # 12  
GPMC Scripting  

Scenario  
As an administrator, you may prefer to use a script as opposed to a UI-based tool to perform specific tasks. For example, for those tasks that need to be performed on a periodic or nightly basis, you could use the Windows Task Scheduler to schedule jobs that execute scripts. Since the GPMC user interface is based on a set of scriptable COM interfaces practically anything you can do via the GPMC UI, you can do via script. The sample scripts provided by GPMC can be easily extended to suit your own needs.

You will now use GPMC’s scripting ability to extract a list of all GPOs in your domain, along with detailed information for a specific GPO. Furthermore, you have been asked to implement a recent change request in which you need to grant read access to all GPOs in your production domain to the HelpDesk group. This is so they can generate HTML reports of the settings in all of the GPOs in the domain. Using a GPMC sample script, you will configure multiple GPOs without using the GPMC UI.

Goal  
Understand GPMC’s scripting abilities, specifically its speed and ability to configure multiple GPOs in your organization.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Detailed Steps</th>
</tr>
</thead>
</table>
| 1. Open Command Window | a. From the Test1 machine, double-click the GPMC Scripts short-cut on the desktop.  
b. The command window should open along with the directory pointing to C:\Program Files\GPMC\Scripts.  
Note: The command window has already been configured so your default scripting environment is CScript. This is done by opening a command window and typing cscript //h:cscript. |
| 2. Execute the ListAllGPOs.wsf script to generate a list of all GPOs in the Test1 domain | a. At the command prompt, type ListAllGPOs.wsf /? to review the switches available for this script  
b. Execute the script by typing ListAllGPOs.wsf  
c. Review the output. |
| 3. Execute the DumpGPOInfo.wsf script to generate detailed information about a single GPO | a. Execute the script by typing DumpGPOInfo.wsf “Remote Sales Settings” /domain:Test1.GPMCDemo.com  
b. Review the output. |
| 4. Execute the GrantPermissionOnAllGPOs.wsf to give Read access to all GPOs in the GPMCDemo.com | a. Execute the script by typing GrantPermissionOnAllGPOs.wsf HelpDesk /Permission:Read  
b. Review the output and note that all GPOs in the domain have been updated with the read permission for the |
domain to the HelpDesk group

| 5. Review the list of 28 other available scripts | a. While still in the command window, type `dir/p` to review a list of all available sample scripts  
   b. Close the command window. |

This concludes the GPMC Lab.
Summary

- Launch and Configure the GPMC
- Configure GPO Scope
- Configure GPO Link Order, Inheritance and Enforcement
- Delegate Group Policy Management
- Generate GPO Settings Reports
- Backup GPOs
- Restore GPOs
- Generate Group Policy Results
- Copy GPO - Cross Domain and Same Domain
- Perform GPMC Scripting
Resources

GPMC Home Page

GPMC Whitepapers and Technical Articles

Download GPMC

Group Policy Home Page
http://www.microsoft.com/grouppolicy