

Supporting Group Policy

Lab 01: Group Policy Introduction



V1.0 Released: February 17, 2014

# Exercise 1 Creating new Group Policy Objects

You are the Administrator for the contoso.com domain. One of your responsibilities is to create a new Group Policy object. This object will be applied to an Organizational Unit for your Sales division.

## Goal

In this exercise, you will create a new Group Policy Object, define its’ settings, and link it to the Sales Organizational unit.

Note: Install GPMC on Domain Controller if OS is Windows Server 2003.

Download: <http://www.microsoft.com/en-us/download/details.aspx?id=21895>

|  |  |
| --- | --- |
| **Tasks** | **Detailed Steps** |
| 1. Open Active Directory Users and computers. 2. Create an Organizational Unit Sales, and two children OUs, Users and Computers. 3. Move your computer account into the Sales\Computers OU. 4. Create a new user account in the Sales\Users OU. | 1. On your Domain Controller, click Start, Run, and type **dsa.msc.** Press OK. This will launch the Active Directory Users and Computers console. 2. Right click the Domain object, and select **New**, **Organizational Unit**. Name this new OU **Sales.** Click OK 3. Next, right click the Sales OU. Select **New, Organizational Unit.** Call this new OU **Users**. 4. Finally, right click the Sales OU once more. Select **New, Organizational Unit.** Call the new OU Computers. 5. The OU structure should look like this:      1. Next, move the workstation account for your client machine to the Sales\Computers OU. To do this, click on the Computers folder. Select the machine account, right click it, and select **Move.** Then browse to the Sales\Computers OU, and click OK. 2. Click on the Sales\Users OU. Right click the OU, and select **New**, **User.** Name the user **PolicyTest.** Assign the user a password, and click OK. User logon name: policytest@aphra.local |
| 1. Create a New Group Policy Object for the Sales OU. 2. Define settings for the Group Policy. | 1. On your Domain Controller, click Start, Run, and type **gpmc.msc.** Press OK. 2. Right click the Sales OU, and select **Create a GPO in this domain, and Link it here**. Then name the new policy **Sales Policy.** 3. Highlight the Sales Policy, and select **Edit**. This will launch the Group Policy editor. 4. For the Sales Users, we want to Hide all Items on their desktops. To configure this policy, click on User Configuration\Administrative Templates\Desktop\**Hide and Disable all items on the desktop.** Double click this policy, and enable it. Click OK. 5. For all the computers in the Sales OU, we want to enable the policy setting to rename the Administrator account. To do this, apply the policy Computer Configuration\Security Settings\Local Policies\Security Options\**Accounts: Rename administrator account.** Enable this policy, and set the Administrator account name to Bob. 6. Close the Group Policy editor. Reboot the client machine, and log onto the machine with the PolicyTest user account you created earlier. 7. If the policy has successfully applied, no desktop icons will appear on the desktop. 8. If the previous test was successful, attempt to log off the client machine, and Log in with the Administrator account. This should fail. Attempt to logon with the user name Bob. This should now be the Administrator account. 9. Re-open the Sales policy object you created earlier. Disable the Rename Administrator account policy setting. 10. Reboot the client workstation. You should now be able to log in again with the Administrator account (as Administrator). |

# Exercise 2 Block Policy Inheritance and No Override

First you will create a policy at the domain level, that will enforce settings against all machines in the domain, including the Sales OU.

Next, you will take the role of the local Sales admin, and configure the **Block Policy Inheritance** flag on your Sales OU. This will prevent the policy from being applied from the Domain level.

Finally, you will take the role of the domain administrator, who decides that all users will get this policy, regardless of the wishes of the OU administrators.

## Goal

In this exercise, you will learn how to apply the **Block Policy Inheritance** flag. The second part of the exercise will have you applying the **No Override** setting to a domain level policy to ensure its enforcement.

|  |  |
| --- | --- |
| **Tasks** | **Detailed Steps** |
| 1. Create a domain level policy with the setting **Do not display last user name** defined. | 1. On your Domain Controller, click Start, Run, and type **gpmc.msc**. Press OK. 2. Right click the domain icon, and select **Create a GPO in this domain, and Link it here**. Then name the new policy **Interactive Logon Policy**. 3. Click **Edit** to open the policy. This will launch the Group Policy Editor. 4. Navigate to Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\**Interactive Logon: Do not display last user name.** 5. Double click the policy, and set it to **Enabled.** 6. Close GPMC on the Domain Controller. |
| 1. Restart the Workstation machine. Verify that the User Name field is blank, as expected. 2. Now, you wish to prevent this policy from applying to the Sales OU. 3. Restart the client machine again to verify that the domain policy is now blocked. 4. Now, we need to set the domain policy to **Link Enabled**, to ensure that it is in fact applied to all child OUs. | 1. Restart the client workstation. On reboot, and after hitting Ctrl-Alt-Delete, the User Name field should be blank. 2. Re-open GPMC. Right click the Sales OU, and select Block Inheritance. 3. Restart the client machine once more. The policy restricting the Last logon name should no longer apply. 4. Re-open GPMC. Right click the GPO **Interactive Logon Policy**, and select **Enforced**. Close all windows on the Domain Controller. 5. Restart the client machine a third time. After reboot, the Last user name setting should again be in effect. |

# Exercise 3 GPO Filtering based on ACL settings

As the administrator of the Sales OU, you need to create a new policy, this time one designed to lockdown a group of trainees that will be in your department for a short time.

## Goal

In this exercise, you will use security filtering to apply a lockdown policy only to those users that need to apply it.

|  |  |
| --- | --- |
| **Tasks** | **Detailed Steps** |
| 1. Create a new global group **Trainees.** Create a new user **Newbie**, and add Newbie to the Trainees group. | 1. On the domain controller, click Start, Run, dsa.msc. This will open Active Directory Users and Computers. Drill down into the Sales OU, into the Users OU. 2. Right click the Users OU, and select New, Group. Specify the group as a domain global group called **Trainees**. Click OK. 3. Next, right click the Users OU, select New, User. Name the new user **Newbie.** Specify a password for the new user, and click OK. 4. Right click Newbie, and select **Add to Group.** In the popup box, specify the Trainees group. Click OK. |
| 1. Create a New lockdown policy on the Sales OU. 2. Configure the ACLs for the new policy to only apply to the Trainees group. | 1. Create a new GPO named **Trainee Policy**, linked to the Sales OU. Highlight this policy and click **Edit.** 2. Once inside the Group Policy Editor, enable the following settings: User Configuration\Administrative Templates\Control Panel\**Prohibit access to the Control Panel,** User Configuration\Administrative Templates\System\**Prevent access to the command prompt**, User Configuration\Administrative Templates\System\**Prevent access to registry editing tools**, and User   Close the Group Policy Editor.   1. Highlight the Trainee Policy GPO, and click Properties. Click the Security Tab. 2. Highlight the Authenticated Users group, and remove the **Apply Group Policy** Access Control Entry. Click Apply. 3. Next, click Add. Enter the Group Name Trainees in the popup box. Click OK. 4. This should result in the Trainees group being added to the Aceess Control List for this policy, with Read permission. Add the **Apply Group Policy** permission for the Trainees group. 5. Click Apply. Close all windows on the Domain Controller. 6. Logon to your client computer (which should still be a member of the Sales OU), as the Newbie user account. After logon completes, examine the start menu, attempt to run registry editing tools, or the command prompt. Log off as Newbie, and log back on as the PolicyTest user. That user should not receive any of these settings. |