**NE247 – Windows Server – Lab5**

**Points deducted if All Answers Are Not In: Ariel, 14pt, Bold, Red!**

Group polices are a mechanism that allows control of both users and computers in the Active Directory network. In this lab you will learn to work with OUs and Group Policy Objects (GPOs) for the Widgets organization.

Required Materials:

**SRV16** and **WIN10** images as prepared in previous lab exercises.

Part 1: Organizational Units

Organization units have several purposes. They allow users and computers to be grouped in a logical manner for administration, they allow delegation of control so certain individuals can provide administration to a subgroup of users and computers without having wider administrative capabilities and they provide the primary method of applying group policies to user and computer accounts.

Group Policies can be applied at the Site, Domain or OU level. Most polices are linked at the OU level because that give the most granular control of policy settings. Polices linked to the Site will be inherited by all users and computer in any domain contained in that site. Polices liked to the domain will be inherited by any uses and computers is OUs within that domain. Policies liked to an OU will be applied to all uses and computers in that OU and any child OUs under that OU.

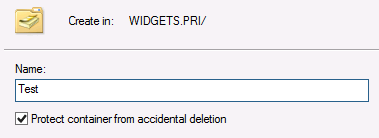
Therefore one of the important considerations in the design of a domain is the OU structure because that will determine how group polices can be linked and applied. There is no single preferred method of designing an OU hierarchy. Designing the OU hierarchy is part of the art of Active Directory design.

Widgets has chosen to design OUs based on departmental structure, with each department in the company given an individual branch of the OU hierarchy. Whether User and Computer objects are put the same OU or in separate OUs is another decision an administrator must make, and there is no single best option for all designs.

**In the following steps you will create an Organization Unit structure for Widgets and place user accounts in the appropriate OUs.**

* Start **SRV16** and log on with your personal administrative account.
* Open Active Directory Users and Computers (ADUC) from the Tools menu of Server Manager.

Under the Widgets.pri domain you will see a number of folder icons. Most of the icons you see here are not OUs but are simple containers. Simple containers have a blank folder icon. Organization Units have a folder icon that isn’t blank; you will see another small image within the folder icon. You cannot link GPOs directly to simple containers, and you cannot create sub containers under them, so they do not serve well for our GPO requirements. For that you need OUs.

* How many actual OUs are there in the default domain configuration? \_\_\_\_\_\_\_\_\_
* **Highlight** the Domain container (**WIDGETS.PRI**) then right click on it and select first **New** then **Organizational Unit** form the cascading menus.
* Give the OU the name of TEST and leave the check mark checked to protect the OU from accidental deletion.
* After creating the new OU, right click on it in the left pane of ADUC and click Delete.

When you try to delete the protected OU, what error message do you get?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

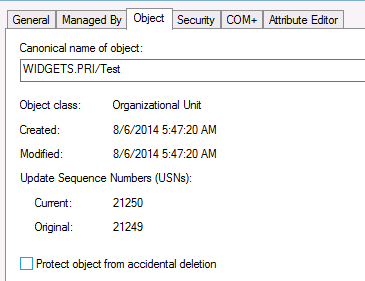
* Right click on the Test OU and select Properties. List the tabs you see.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

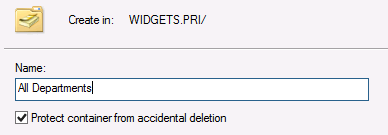
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Close the Properties window.
* Locate the Menu bar at the top of the ACUC window and click on the View title, then click on Advanced Features under View.
* Return to the Test OU, right click on it and select Properties again. You will see new tabs now that you are in Advanced View mode.
* Click on the Object tab and uncheck the box for Protect object from accidental deletion and then click OK.



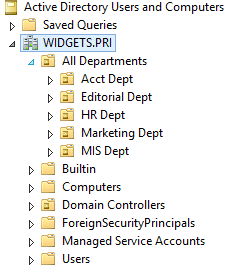
* Return to the left pane of ADUC and delete the Test OU. Don’t continue until you can delete the OU.
* Click on the View menu and uncheck the Advanced Features selection.
* Right click on the **WIDGETS.PRI** domain icon and create a new OU.
* Give the first OU the name All Departments.



* After creating the All Departments OU, right click on it and select New and then OU to create a child OU under All Departments. Name the new organizational unit **HR Dept**.
* Create child OUs under HR Department called **HR Users** and **HR Computers** as shown below.



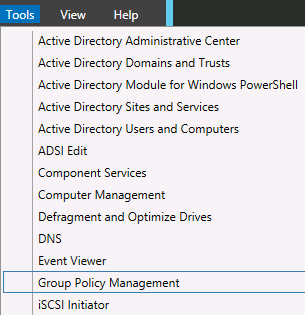
* In the Users container of the Widgets.pri domain (note that it is not an OU) locate the three member accounts of the HR Department and move them to the HR Users OU. You can use the mouse pointer to drag the user icons to the new OU, or you can right click on an account and select the Move… option form the menu. *[You can use the Ctrl or Shift keys to select multiple accounts to move at the same time.]*
* *This is exactly where the user ‘Description’ from Lab 2 comes in handy. You entered the ‘Description’ for each user right?? 😊. Oh No?? Welp, enjoy figuring them out…*
* Next create OUs directly under the **All Departments** OU in the Widgets organization. Create separate OUs under each departmental OU for **users** and **computers** as you did with the HR department. Shown below.



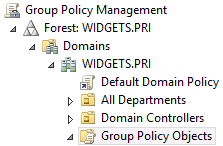
* Move the Widgets users to the appropriate OUs as you did with the HR department.
* Close ADUC
* Continue on to the next section …

Part 2: Group Policy Management Console

* Still on **SRV16** logged on as your personal account open the Group Policy Management Console (GPMC) from the Tools menu of Server Manager.



* Expand the Forest, Domains, widgets.pri and finally the Group Policy Objects containers in the left pane of the application.



* List the Group Policy Objects (GPOs) that exist by default in your domain. (There will be only two.)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Highlight (left click on) the widgets.pri icon. Below the icon you will see the **Default Domain Policy** icon. Note the small arrow in the icon in front of the printed name. The arrow indicates that this is a link to the policy, not the actual policy itself. Deleting the link will not delete the policy, but editing the link will cause the main policy to change.
* Left click on the Default Domain Policy link and read the notice that appears. You can check the box so you don’t see this message every time you click on a policy link.
* You should now see that the **Scope** tab is open in the right pane. Security filtering specifies the group membership needed for a user or computer to receive the settings from this policy (assuming the user or computer is in a container that receives the policy).

What group is listed under Security Filtering?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Remember that the Authenticated Users group contains all security principles that log on with a username and password. This includes computer accounts!
* Click on the Details tab.
* After examining the information offered in this section, click on the arrow to expose the alterntives for GPO Status.

List the four choices and put a check next to the default that is selected.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Next, click on the **Settings** tab.
* Click the **show all** link. This will show you all the settings in this policy. You should see that there are many settings in the Computer Configuration section

What do you see under the User Configuration settings?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If there are no settings in a GPO for one of the two sections (Computer and User Configurations) you can disable the unused section to improve system performance (if there are many GPOs)

* Under **Account Policies/Password Policy** settings record the defaults you see.

Enforce password history \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Maximum password age \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Minimum password age \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Minimum password length \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Password must meet complexity requirements \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Store passwords using reversible encryption \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* In the left pane of GPMC click on the **Domain Controllers** icon.
* In the right pane you should see three tabs. The first, Linked Group Policy Objects, should already be selected. This tab shows the polices linked directly to this container. List the policy that is linked here by default.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Next, open the **Group Policy Inheritance** tab.

This shows all policies that will have an effect on users and/or computers in this OU and their order of precedence. The higher the level of precedence (the lower the precedence number) the more powerful the policy will be. Any conflicting settings between policies will result in the policy with the lowest precedence number taking priority over all others.

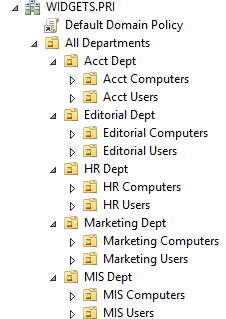
* List the two default policies and their precedence numbers

\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If there are any conflicts, which policy will win? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* In the left pane, **expand all the OUs under All Departments**. You should see all the OUs that you created in a previous lab exercise. If you do not see the correct OUs, many any necessary adjustments before proceeding.



* **Highlight on the OU for the HR Dept** and in the right pane click on Linked Group Policy Objects (the first tab).

Are there any GPOs linked directly to this container? **[ Y / N ]**

What GPO policy settings are inherited? (Group Policy Inheritance tab)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Linking a policy to this container will affect any users and/or computers in this container as well as any child containers (as long as none are set to Block Policy Inheritance).

Part 3: Preparation for GPOs

In the next section, you will create and work with GPOs. However, you first need to do some preparation. In the next steps, you will prepare a shared folder for desktop background images.

* On **SRV16** use File Explorer to navigate to the root of the C: drive and create a folder called **wallpaper**.
* **Share** the **wallpaper** folder with the **Everyone**, Allow **Read** share permission.
* The instructor will make image available to you either from the Canvas > Week 6 folder or on portable media. From within Skytap run IE and log onto Canvas then download and copy the **hr-wallpaper.jpg** image to the **wallpaper** folder.
* Enable IE Downloads. Internet Options > Security > Zone(Internet) > Custom Level > Downloads > File download > Enable > OK.

Part 4: Working with GPOs

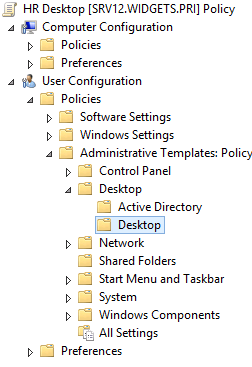
In the next section you will create and link GPOs

* Return to GPMC on **SRV16** and left click on the HR Users OU to highlight it.
* **Right click on the HR Users** container and select the option to Create a GPO in this domain….
* In the New GPO dialog box give the policy the name **HR Desktops** and click OK. You will not make any changes in the Source Starter GPO box.
* **Expand the HR Users OU** and you should see a link for the new policy name. Right click on the **HR Desktops** link and select **Edit** from the menu.

You will now be in the Group Policy Management Editor where you can make changes to the new policy. You should see two main sections, Computer Configuration and User Configuration. As you should know, setting placed in the Computer Configuration section apply to all computers no matter who is logged in to them. Settings in the User Configuration section apply to all users regardless of what computers they log onto.

You will also see separate folders for Policies and Preferences. Polices are always enforced and users cannot change them. Preferences can be changed by uses one they are in place.

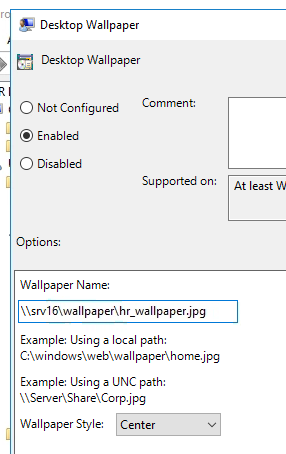
* In the left pane **expand User Configuration** > **Policies** > **Administrative Templates** > **Desktop** and then click on the **Desktop** folder underneath.



* In the right pane left click on the Desktop Wallpaper icon. You will see that the left pane is now divided onto two panes, one for explanations and one for settings. Near the bottom of the pane you will see two tabs. Click on the Standard tab to remove the explanation section.
* **Double click on the Desktop Wallpaper option**.
* You will need to make three choices in this window. First you will click the **Enabled** radio button near the top. This will activate the policy setting.
* In the Wallpaper Name box you will need to type in a network accessible location for the wallpaper file. You can’t use a designation like C: because this would point clients to their local C: drive. Instead you need to **use the UNC name and path**. You will use the following:

**\\SRV16\wallpaper\hr\_wallpaper.jpg**

* Leave the Wallpaper Style (orientation) to the default of Center.



* When finish, click on OK at the bottom of the window and close the GPM Editor.
* Open a CMD Prompt on the **SRV16** machine and run the **gpupdate /force** command to ensure the latest group policies are updated.

You have now created a user policy that will affect all users in the HR Users OU. In the next steps you will test the policy to see if it works.

* Switch to **WIN10**, log off your personal account and log on to an account that is a member of the HR Department, Cotton Malone.
* What desktop wallpaper do you get? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[If you get a black *screen instead of the desired wallpaper double check your permissions and the exact spelling in of the UNC path. If you still get a black screen after logging off and logging back on as cmalone, you may have to get the latest updates for your images.]*

* Log off **WIN10** as cmalone and log on as jstone.

What desktop wallpaper do you get? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Log off **WIN10**
* Return to **SRV16** and locate the jstone account in Active Directory Uses and Computers (ACUC).
* Move the jstone user icon to the HR Users OU
* Switch to **WIN10** and log on as jstone

What desktop does jstone get now?

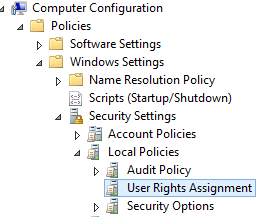
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If the wallpaper didn’t change, log off and log right back on as jstone. Don’t continue until you see the new wallpaper. You may find that if you don’t reboot the computer, the new wallpaper won’t show until the second logon.

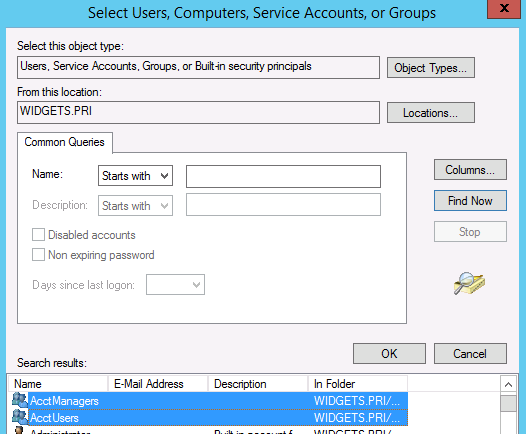
* Switch back to **SRV16** and move the jstone icon back to the Acct User OU.
* Switch back to **WIN10**.
* Did the desktop change without logging off? **[Y / N ]**
* Log off and log back on as jstone.
* Did the wallpaper change? **[Y / N]** (if not, log off an log back on.)
* You have now seen how a GPO containing user settings will affect all the users in any OU receiving the policy.

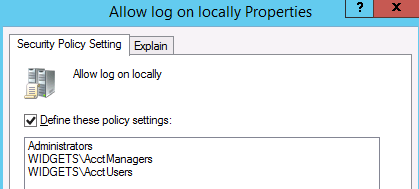
In the next steps, you will create a computer policy and see how it applies to computers, no matter who logs on.

* At **SRV16** open GPMC and locate the Acct Computers OU. Create and link a new GPO to this OU called **Restrict Acct Computers**.
* Edit the new policy and navigate under the **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**



* Locate the policy for **Allow Log on locally** and double click on the setting.
* Check the box to **Define these policy settings**: then click on the box for Add User or Group.
* Click **Browse** then at the next window click **Advanced** and then click **Find Now**.
* Locate the **two Global groups** you created for the **Accounting Department (Managers and Staff) and add them to the list.** (Your group name may be different than those shown below.)
* after adding the two global groups, add the Administrators group. (The system won’t let you finish unless you add the Administrators.)
* Open a CMD Prompt on the **SRV16** machine and run the **gpupdate /force** command to ensure the latest group policies are updated.





You have now created a policy that will only allow members of the Accounting Department and Administrators to log onto any computers in the Acct Computers OU. In the next steps, you will test the policy to see if it works.

* In **Active Directory Users and Computers**, locate the **WIN10** computer icon in the Computers container and **move it to the Acct Computers OU**.
* Restart the **WIN10** image. When it restarts, try to log on as the cmalone account. This should fail. Record the error message you get.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Now try to log on to **WIN10** with the jstone account. This should succeed because the jstone account should be a member of the AcctUsers group.
* Now try to logon with your personal account.
* Were you able to log on with your personal account?  **[Y / N ]**

Your personal account isn’t a member of the Accounting Department. Why were you able to logon?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Move **WIN10** back to the Computers container
* Run **gpupdate /force** on the **WIN10** computer
* Restart **WIN10** and try to logon with the cmalone account.
* Were you successful? [ Y / N ]
* Don’t finish until you can log on with any account.
* Shut down your images.

. . –End