**NE259 – Windows Server – Lab3**

**\*\*\*UPDATE: New Lab 2 with revised Account Names & Departments!!! Check the Week2 folder.**

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

As previously demonstrated, users gain access to the Active Directory network by authenticating with valid domain user accounts. Once a user authenticates, the user will need to access resources within the domain such as files, folders and even applications. To provide security in the domain, these resources are protected by Permissions which are held in Access Control Lists on each protected resource. While it is possible to provide access to resources by entering individual user account information into each Access Control List, this would be prohibitively inefficient except in the smallest of Active Directory network. To make access control efficient, permissions are granted to entities called Groups with have user accounts as members. As will be seen, it is far simpler to grant a specific level of access (permission) to a large number of users by employing groups than assigning permissions to each individual account.

While the concept of groups is very simple (containers holding membership lists) the proper use of different types and scopes of groups can be confusing. The two different types of groups (Security and Distribution) are easily dealt with: Only Security groups can be used for assigning permissions, so those are they only type we will consider here. The real difficulty come in the understanding and proper use of the three scopes that are possible within the Security group type, Global groups, Domain Local groups and Universal groups.

* **Domain Local** Groups

Protect Resources within the local domain with permissions

* **Global** Groups

Collect users within the local domain

* **Universal** Groups

Collect Global groups from different domains in the forest

* **System** Groups (Special Identities)

Collect users based on Authentication method or status

Microsoft’s recommended best practice for using groups is represented by the acronyms **A-G-DL-P** and **A-G-U-DL-P**. For single domain forests and even many multiple domain forests, the A-G-DL-P is the only form needed. User Accounts (A) are members of Global groups (G) which are members of Domain Local groups (DL). Permissions (P) to access resources are given only to Domain Local Groups. In larger forests where Universal Groups may be employed, Global groups are members of Universal groups (U) which are members of Domain Local groups.

**\*\*\*LOOK AT THIS IMAGE FOR A GOOD ILLUSTRATION OF GROUP LAYOUT\*\*\***



**Required Materials:**

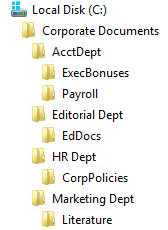
Server 2016 image as prepared in the previous lab exercises.

Permissions will be demonstrated in subsequent labs. In this lab you will work with different groups and place user accounts in appropriate groups.

**REMEMBER!! Accounts (user accounts) -> Global Groups -> Domain Local Groups -> Permissions.**

**You’ve already created the Accounts** at the end of Lab 2; you’ll **now create Global Groups** reflecting the **Departments** within the AVERY.PRI organization.

Preliminary Task:

  
**Create the folder structure below on the SRV16 system.**

\Corporate-Documents

\AcctDept

\ExecBonuses

\Payroll

\EditorialDept

\EdDocs

\HRDept

\CorpPolicies

\MarketingDept

\Literature

* On **SRV16**, **create the folder structure shown above.** First create the **Corporate-Documents** folder directly under the C:\ drive, then create the four departmental folders under the **Corporate-Documents** folder. Finally, create the appropriate departmental subfolders as shown.

Part 1: Global Groups

**Global** groups contain membership lists of user accounts (and computer accounts) from the local domain that have similar security access requirements and restrictions. The membership list that a Global group contains can only include users and computers that are members of the domain where that Global group exists. While the membership list of a Global group is very restricted, a Global group can be a member of a Domain Local group in any domain in the forest. It can also be used to access resources in any domain in the forest directly, although that is not the preferred method.

Creating Global groups for AVERY will be simple; you can organize users into Global groups based on their departments or titles. Plan your groups below. One example is provided to give you guidance. You will not need to use all the spaces provided.

Finish ompleting the form below

Group Scope Group Name\_\_\_\_\_\_\_\_ Members \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Global **HRManagers** **Woodrow Webb**

Global **HRStaff** **Julio Watkins, Ivan Grant**

Global \_\_**AcctDeptMan**\_\_\_\_\_ \_\_**Alyssa Cox**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Global \_\_**AcctDeptStaff**\_\_\_\_\_ \_\_**Lewis Pearson, Raymond Sullivan**\_\_\_\_\_

Global \_\_**MarketMan**\_\_\_\_ Cassondra moran, melody beck

Global \_\_MarketStaff\_\_\_\_\_\_\_ lavern keller

Global \_\_MISSrAdmin\_\_\_\_\_\_ misty burns

Global \_\_MISAdmin\_\_\_\_\_\_ tracy oliver

Global \_\_MISHelpStaff\_\_\_\_\_\_\_ pat berry, sean santiago

Global EdStaffInterns Edward Ortiz, nick perkins

Global editorialstaff Sheryl hale

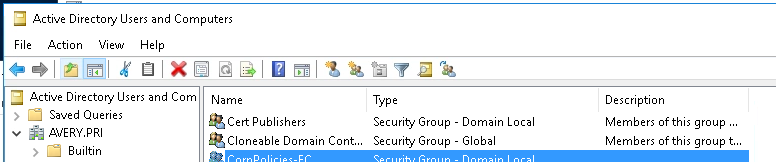
Global senioreditor jasmine adams

Global \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Global \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**In the next section you will create Global groups for AVERY as you described on the previous page.**

* Start **SRV16** and log on with your personal administrative account.
* Using the Tools menu in Server Manager, open Active Directory Users and Computers (ADUC).
* In the left pane **expand** the AVERY.pri domain to show the subfolders.
* Left click on the Users folder (container) and examine the contents in the right pane.
* Expand the width of the Type column header so you can read the full names of the types of objects, then click on the Type column header to sort the entries by type.



What different types of group scopes do you find in the Users container?

**Domain local, global, universal**

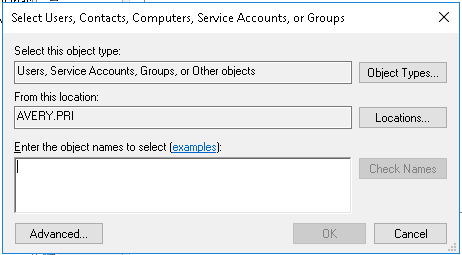
* Right click on the Users container in the left pane and select New then Group from the cascading menus.
* Give the group the name of **HRManagers** that will be a Global security group.

What are the default radio button settings for Group Scope and Type?

Scope: Global Type: Security

* Now create another Global security group for **HRStaff**.
* In the right pane of ADUC **now double click on the HRManagers group** to open the Properties page for this group.
* Click on the Members tab at the top.
* In the Members section, click the Add button. This will take you to the place where you can put users (or other groups) into this group.

This windows has three main sections, Object Type, Locations and Check Names.



* Click on the  
  Object Types button and examine the options
* **Uncheck all the boxes except for the Users box and click OK.**
* Rather than try to remember the user names, click on the **Advanced** button at the bottom of the window.
* Although you could perform a detailed search, just click on **Find Now** for a simple search.
* You should now see a list of all the users in your domain. **Locate** the **user** who is the **HRManager**, click on the name and then click OK.

What is this user full object name entry shown in the Enter the object names field?

**WWebb@AVERY.PRI**

* Click OK to return to the Members tab of the **HRManagers** Properties window and click OK.

**As you can tell if you examine the options in various screens there are variations on how you can search for and add users to groups. In the next step you will see a variation of the process.**

* In the Users container, locate the account for Julio Watkins and double click on it to open the user’s properties window.
* Click on the **Member Of** tab.

What group or groups is **Julio Watkins** a member of?

**Domain Users**

* Click the Add button.
* This time, instead of using the Advanced button, type in **HRStaff** in the Enter field and click on Check Names.
* When you do this, if the name is found the system will underline the name of the group for you to verify the spelling and existence of the group, then click OK.
* Click OK again to save the change to the account.
* You have just learned two different ways to add users to group. Now using any method you prefer, Create the remaining Global Groups and add the appropriate uses from the previous lab to those groups.

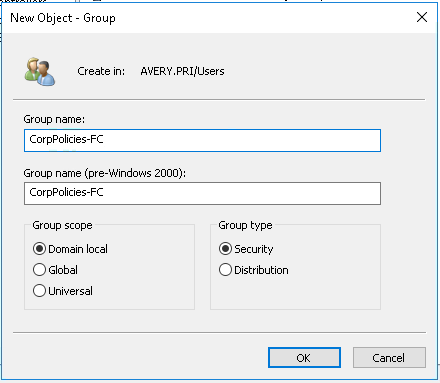
Part 2: Domain Local Groups

A **Domain Local** group is used to control access (assign permissions) to resources within the local domain that contains that particular Doman Local group. A Domain Local group cannot be used to access resources outside its own domain. Domain Local Groups have membership lists that can contain accounts or groups from any domain in the forest. A given resource (such as a file or folder) may have multiple Domain Local groups in its Access Control list. It is a common practice to include and abbreviation of the permission level in the name of a Domain Local group. This will be demonstrated later.

The Human Resources (HR) Department at AVERY is responsible for administering corporate policies and benefits. The HR Department routinely publishes company policy information and information on benefits such as vacation, overtime and healthcare policies. To accomplish this, they post documents on corporate servers that all employees can access. While all employees need to be able to read the documents, only HR managers are allowed to modify the documents, while HR staff can only read them. MIS Department members need to have full control of the folder. To simplify the control of these documents the documents are put in a folder called Corporate Policies that will be protected by permissions. To simplify the application of permissions, Domain Local groups will be used. Following are the groups that the MIS department will create for this purpose.

***In the next steps you will create these Domain Local groups and then put the appropriate Global groups into them.***

* On **SRV16** in ADUC create a group in the Users container called **CorpPolicies-FC** and give it the **Domain Local Scope** and **Security** Type.



* After the DL group has been created, click the Members tab and add the Domain Admins group.
* Now create DL security groups that will have the Modify permission and the Read permission as shown above. Then add the appropriate Global groups to them.

Now that the Accounts and Global Groups are created along with the proper memberships and the above folder construct is made it’s time to create the Domain Local Groups and add the Global Group to them. Below is a list of the Domain Local (DL) groups and their memberships. Using ADUC, create these Domain Local Groups and add the Global Groups from above to them. Follow the format below.

Resource (Folder) Name: **\HRDept\CorpPolices**

Scope Permission Group Name \_\_ Membership\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DL Full Control (FC) CorpPolicies-FC Doman Admins (built-in Global group)

DL Modify (M) CorpPolicies-M HRManagers (Global group)

DL Read CorpPolicies-R HRStaff (Global group)

Resource (Folder) Name: **[**EditorialDept**\EdDocs**

Scope Permission Group Name \_\_\_\_\_ Membership (Global Group Name)\_

DL \_\_\_FC\_\_\_\_ \_\_\_EdDocs-FC\_\_\_\_\_\_\_ \_Senior Editors, All **MIS** Global Groups

DL \_\_\_M\_\_\_\_\_\_ \_\_\_EdDocs-M\_\_\_\_\_\_\_\_ \_\_\_\_\_Editorial Staff \_\_\_\_\_\_\_\_

DL \_\_\_RW\_\_\_ \_\_\_EdDocs-RW\_\_\_\_\_\_\_ \_\_\_Editorial Staff Interns\_\_\_\_\_\_\_

DL \_\_\_\_R\_\_\_ \_\_\_EdDocs-R\_\_\_\_\_\_ \_\_\_\_\_\_Marketing Managers\_\_\_\_\_

Resource (Folder) Name: **\MarketingDept\Literature**

Scope Permission Group Name \_\_ Membership\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DL\_ Full Control MarketLit-FC\_ Marketing Dept Manger, Domain Admins

DL\_ Modify MarketLit-M\_ Marketing Dept. Staff (Global group)

DL\_ Read MarketLit-R\_ Everyone (Special Identities Group)

Resource (Folder) Name: \_\_\**AcctDept**\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Scope Permission DL Group Name \_\_\_\_\_ Membership (Global Group Name)\_

DL \_FC\_\_\_\_\_\_ \_\_AcctDept-FC\_\_\_\_\_\_\_\_ \_\_Acct Managers, **MIS Senior Admins**

Resource (Folder) Name: \_\_\_\AcctDept\**Payroll**\_\_\_\_\_\_

Scope Permission DL Group Name \_\_\_\_\_ Membership (Global Group Name)\_

DL \_\_M\_\_\_\_\_ \_\_ AcctDept-Payroll-M \_ \_\_Accounting Staff\_\_\_\_\_\_

DL \_\_FC\_\_\_\_\_ \_\_\_AcctDeptPayroll-FC \_MIS Admin, Domain Admins

* Add the appropriate Global groups into the proper Domain Local the groups.
* Answer the following questions:
* What Global group or groups is Julio Watkins a member of?

**Domain Users, HRStaff**

* What Domain Local group or groups is the **HRStaff** group a member of?

**CorpPolicies-R**

* What **permission** is planned for the **CorpPolicies-R** security group for the contents of the CorpPolicies folder?

**Read**

* Given this information, what permission will Julio Watkins have for the contents of the CorpPolicies folder?

**Read only**

* Finally, apply the permissions listed below to the Domain Local groups created above. In the following sections of the lab you will use the indicated security requirements to add permissions to the proper domain local groups to protect the resources (folders) described. For simplicity we use only four different permission levels. **FC** for Full Control, **M** for Modify, **R** for Read and **RW** for Read and Write. You can use the special built-in Everyone group instead of a Domain Local group if appropriate.

EditorialDept

* **Marketing Managers and staff** need to be able to **read** **Editorial** department documents.

EditorialDept\**EdDocs**

* **Editorial Staff** need **Modify**, **Senior Editors & all of the MIS Dept** needs **Full Control**, **Interns** need **Read and Write** permission.

HRDept\**CorpPolicies** special documents requirements.

* **Domain Admins** need **full control** of all documents in the **CorpPolicies** folders.
* **HRManagers** need **Modify** control.
* **HRStaff** need **Read** control.

MarketingDept\**Literature**

* **Everyone** (*special identity group*) in the company needs to be able to read the contents.
* **MIS Administrators & Marketing department managers** need **full control**.  
  **Marketing Staff** need to be able to **modify** documents.

AcctDept special documents requirements.

* **Accounting Managers & MIS Senior Administrators** need **full control** of all documents in the **AccDept** folders.

AcctDept**\Payroll**

* **Accounting Staff** need to be able to **modify** [AcctDept\**Payroll]** data but should **not** have any access to Executive bonus documents
* **MIS Domain Administrators** should have **full control** of [AcctDept\**Payroll]** documents but not [AcctDept\**Executive Bonuses]**. They should have **no** access to bonus information

You should plan one Domain Local group for each permission level that will be needed.

***Note: When you use System groups like Everyone, Authenticated Users or Creator Owner, you set permissions for those groups directly on the resource; you don’t put system groups into Domain Local groups.***