Active Directory Basics:

Vocabulary/Definitions:

Authentication: the process of verifying your identity before allowed access to use a resource.

Authorization: the process of verifying whether the authenticated user is authorized to use the resource.

Accounting: the process of documenting the authenticated and authorized person has accessed the resource.

Central Authentication: A certain type of authentication that allows authentication to users by logging in to the database.

Domain: A group of computers, networks and users that share the same Active Directory database.

Domain Controller: A server that takes care of managing active directory; hosting the database, handling authorization and authentication and accounting (AAA protocol).

Forest: A collection of domains inside the active directory database.

Local Authentication: A certain type of authentication that only works on that resource. (i.e. Username/pass to an account or car keys.)

Organizational Unit: A container (folder) within active directory that holds users, groups and computers. It is the smallest unit to which an admin can assign permissions to.

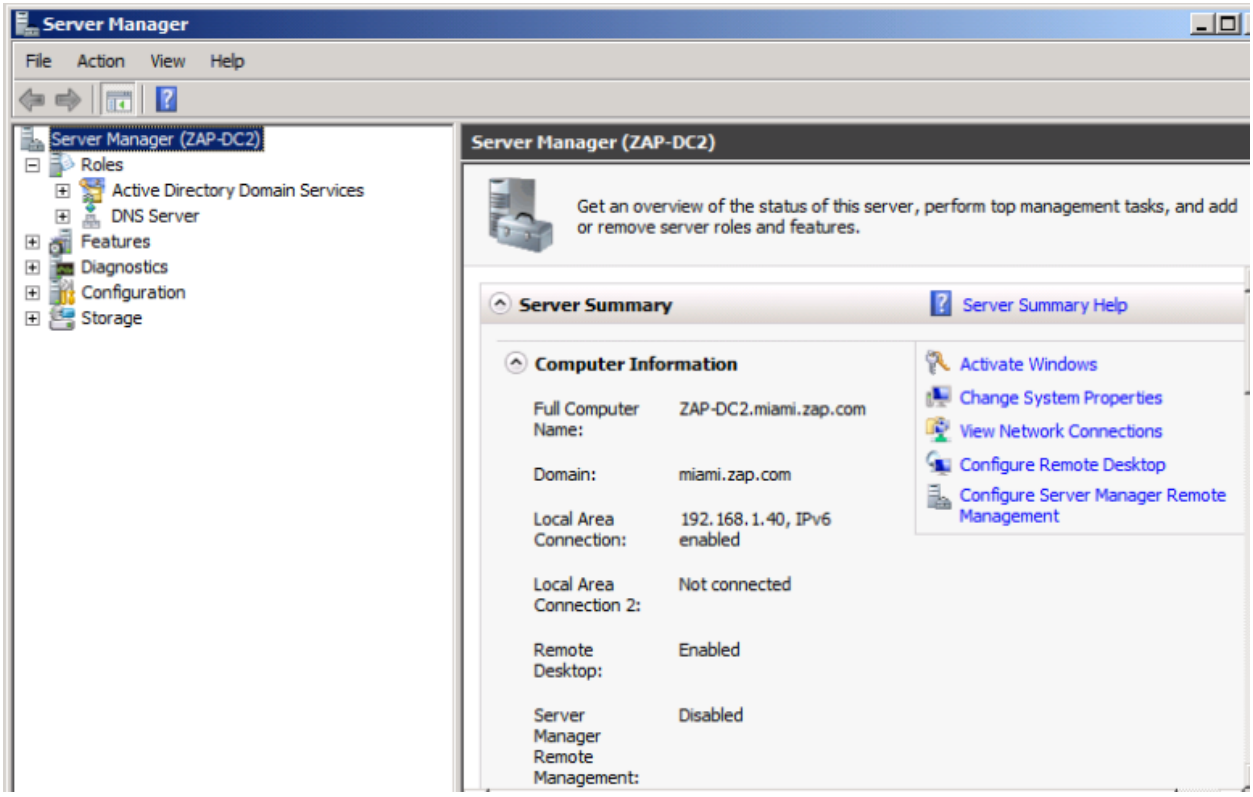
Server: A computer that manages access to a centralized resource.

What is Active Directory:

Active Directory is a central database that contains people's information that will be used to authenticate them when logging in.

Many businesses and organizations use active directory to store employee information. Employees that want to use company resources must authenticate to Active Directory before going any further. IT administrators use Active Directory to maintain order in the organization.

Every active directory structure has one domain controller. Domain controllers started in Windows Server 2003, but now companies use Windows Server 2012 R2. To make a server a domain controller, it must have Active Directory Domain Services installed as a role, as the screenshot below demonstrates.

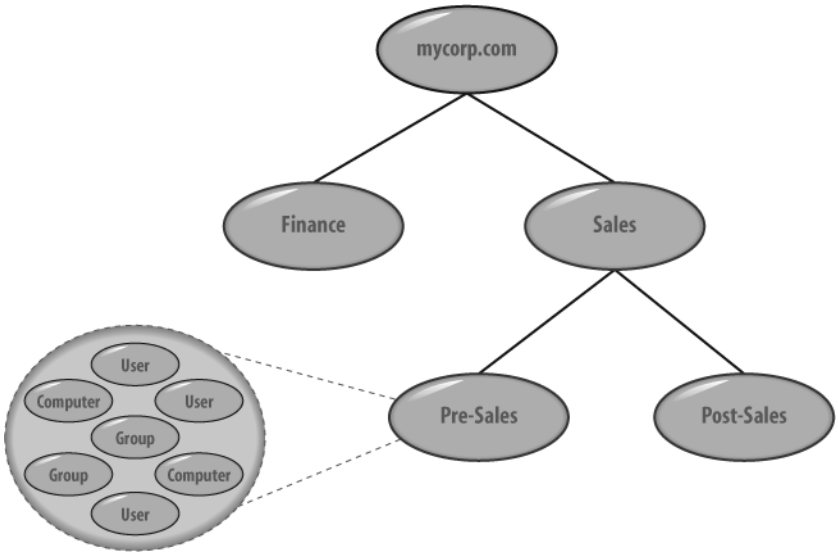


Forests and Domains:

In general IT terminology, a **domain** is a collection of resources. Let's say you were the founder of Facebook and you started with 100 employees and 100 computers, 1 website and 1 email server. All of those resources would belong inside Facebook.com. That is the **domain name**.

Using the same example above, your Facebook.com would be the **FOREST** name, or **top-level domain**. Because Active Directory lets you create **domains inside domains** and a collection of domains is called a **FOREST.**

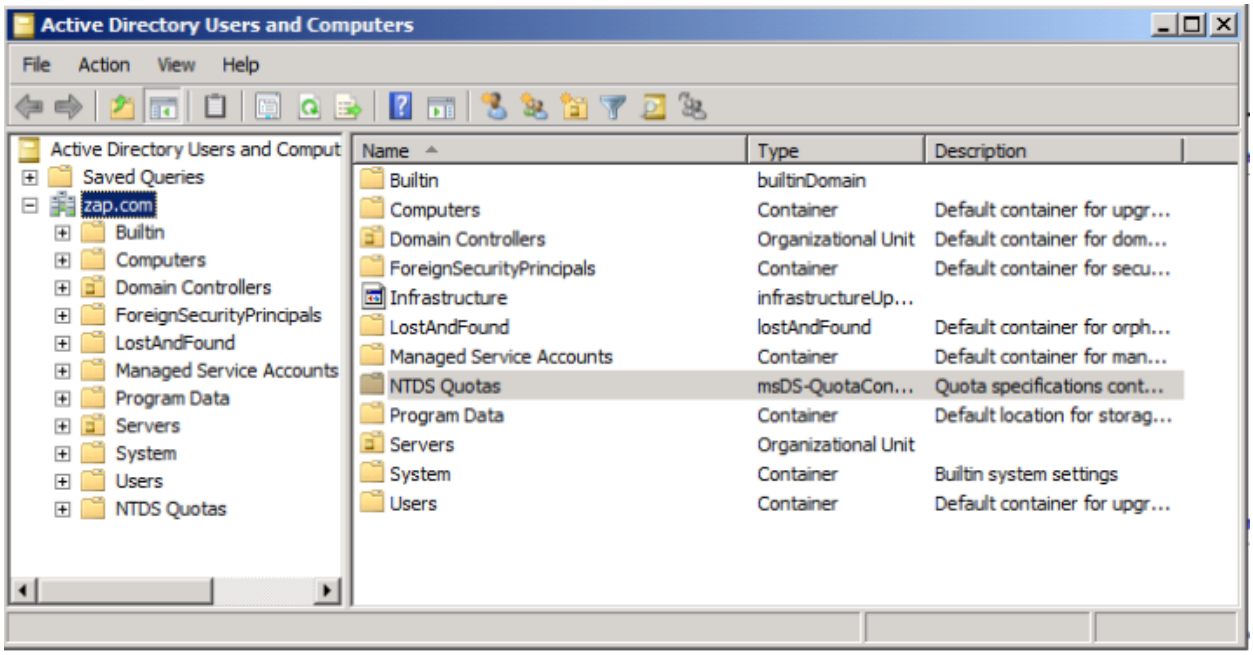
Let's say you expand Facebook to Europe and EU law requires you to have all European employees records physically stored in Europe, not in the US. So with Active Directory, you can create a **domain** inside Facebook.com and call it Europe.Facebook.com – then assign **servers**, computers and users inside this "Europe" domain, and the **domain controller** for the European domain would be physically stored in Europe.



<---Example of a forest

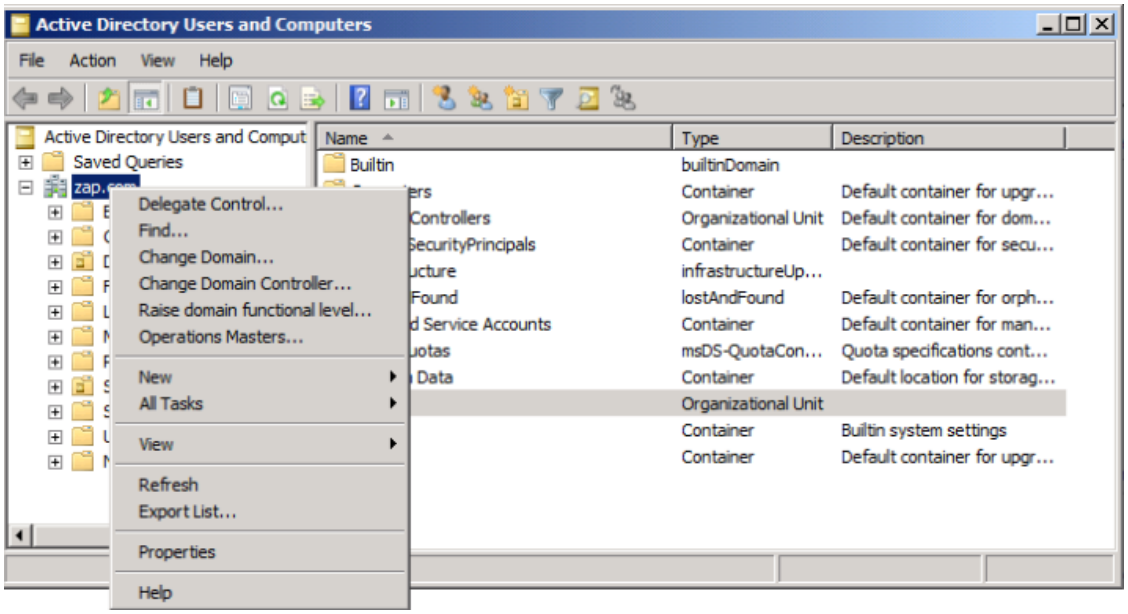
Active Directory Users and Computers:

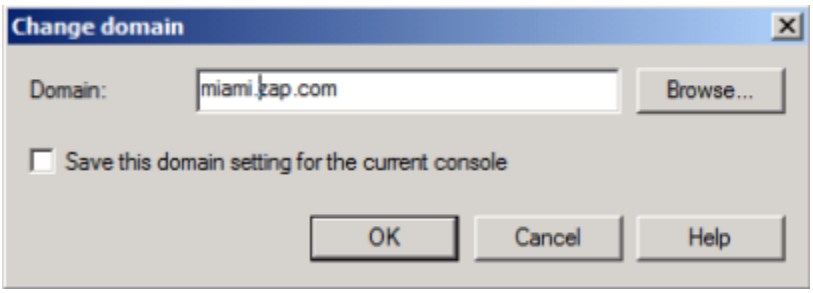
ADUC is a snap-in tool that manages active directory.

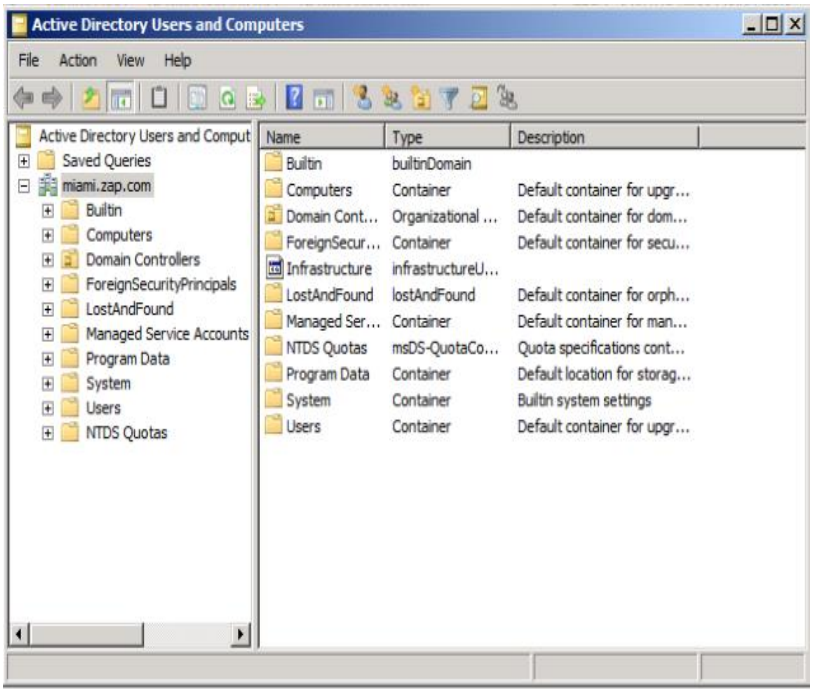


The folders under zap.com are called organizational units (OU's). They are an extreme and essential part in active directory. An active directory administrator has the option to split his organization in geographic locations, it is because of OU's. They are nested inside the domain.

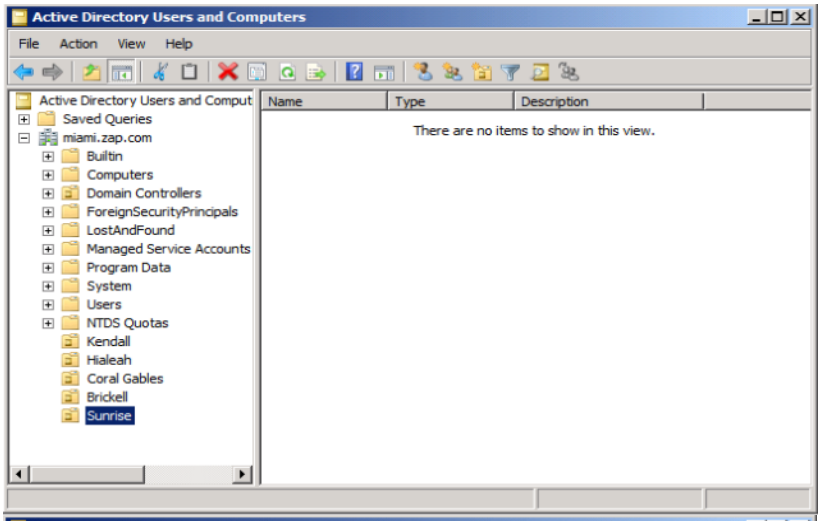
You can create a domain in your forest that is reserved only for employees of a certain location, and within that domain, create OUs that are for each department or each area inside that location. Once the domain has been created, from Users and Computers, you can just change domains.



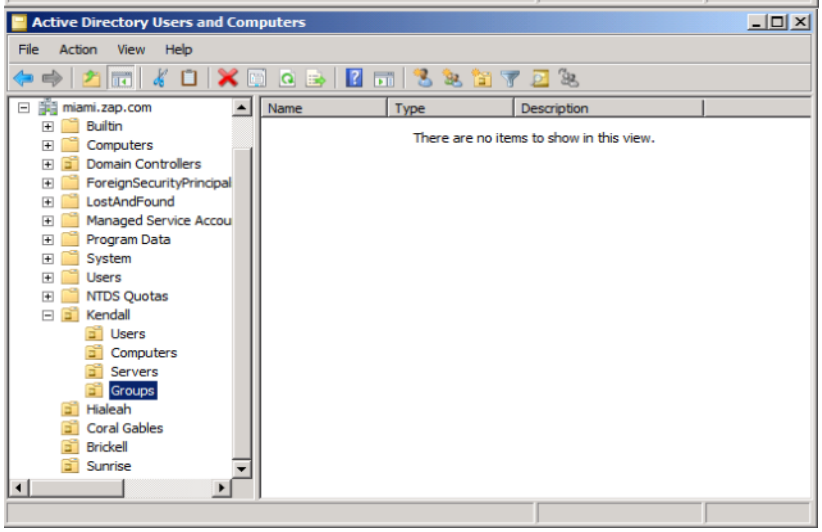




I am now inside MIAMI.ZAP.COM – a domain created only for MIAMI employees of ZAP corporation. Now, let's create OUs for every location in MIAMI where there is a ZAP office.

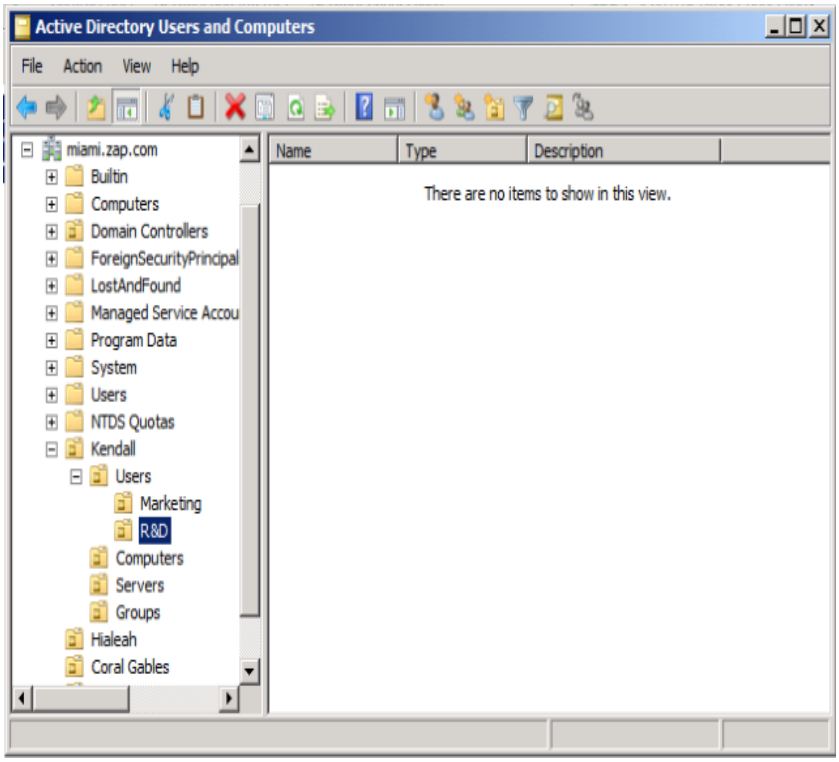


So now I've created 5 OUs for each of my Miami sites of ZAP corporation (Kendall, Hialeah, Coral Gables, Brickell, Sunrise). But they are empty.

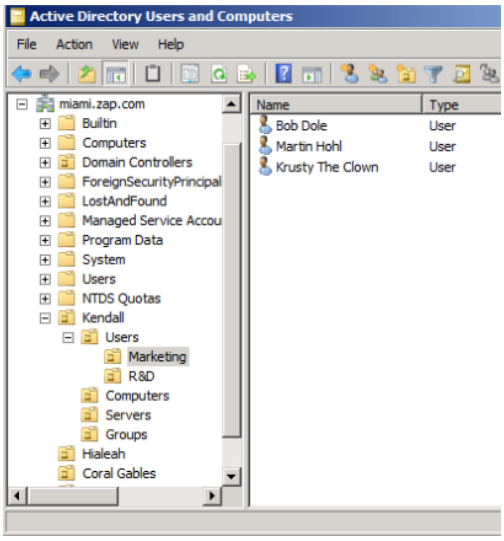


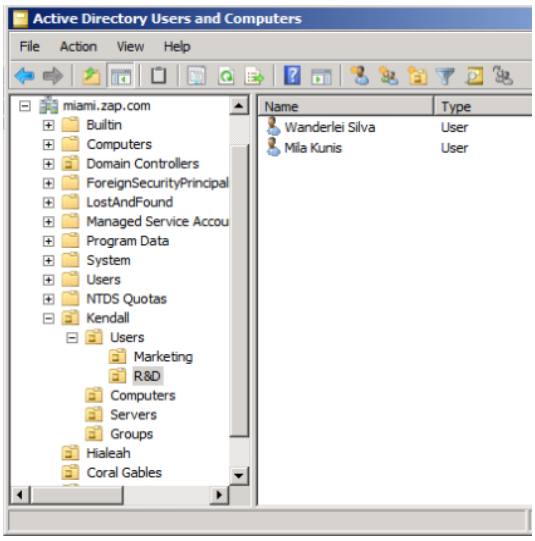
So I have created four more OUs inside of Kendall: one for users, one for computers (my users will be using), one for servers and one for groups.

Groups in Active Directory allow you to implement the AAA protocol a lot easier. Example: my Kendall office has 3 Marketing and 2 Research and Development employees working in there, so I will create two more OUs inside Users – Marketing and R&D.

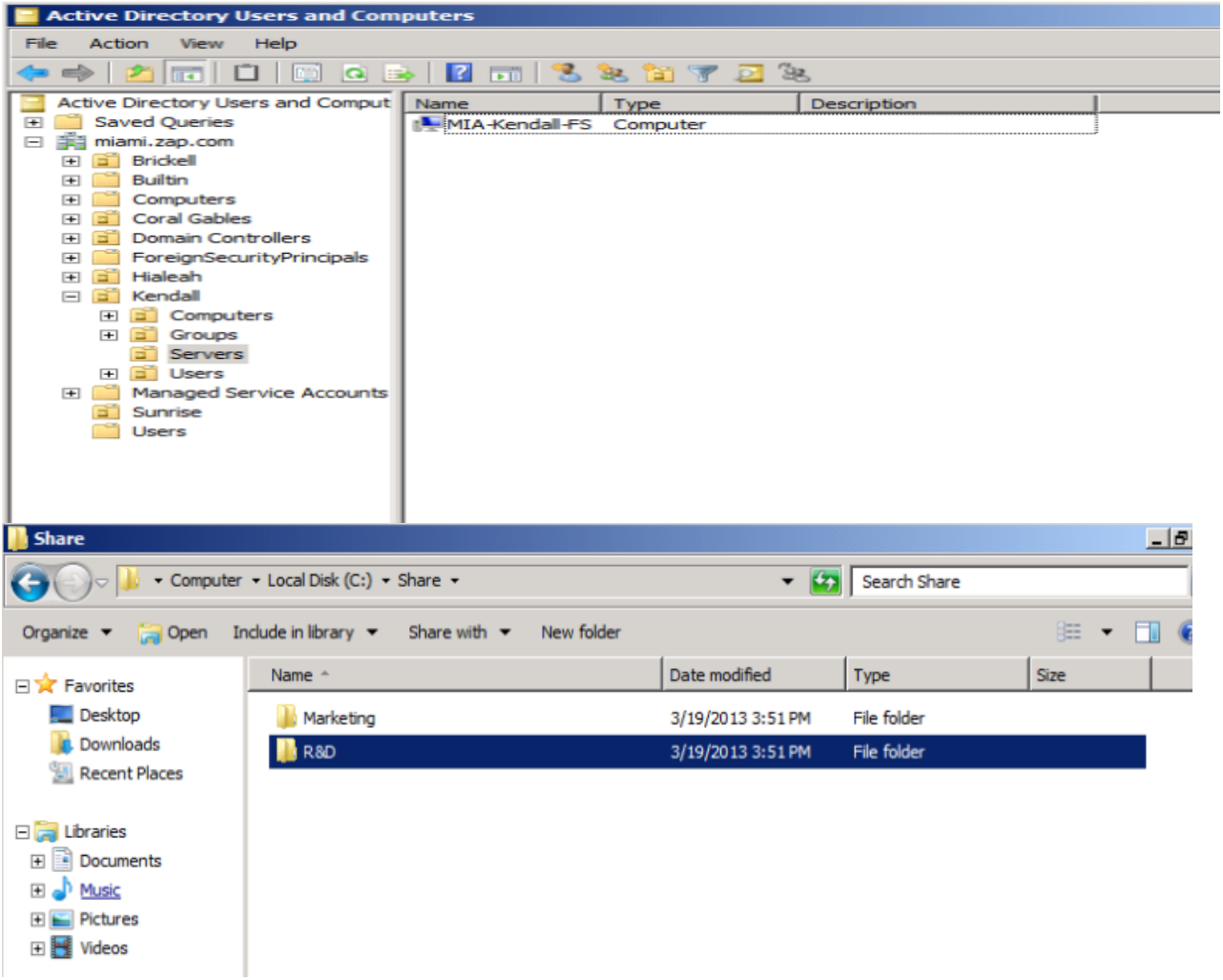


Now, I want to create the users inside the Marketing and R&D OUs.

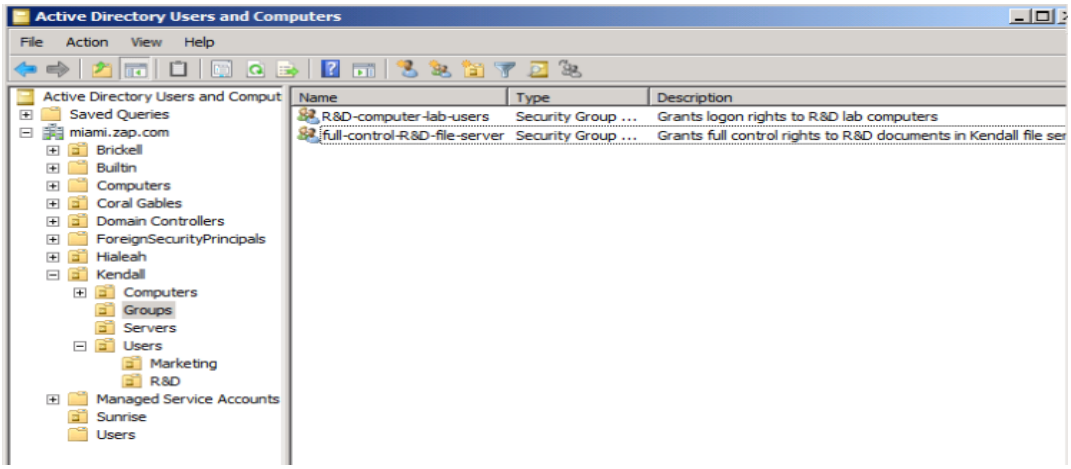




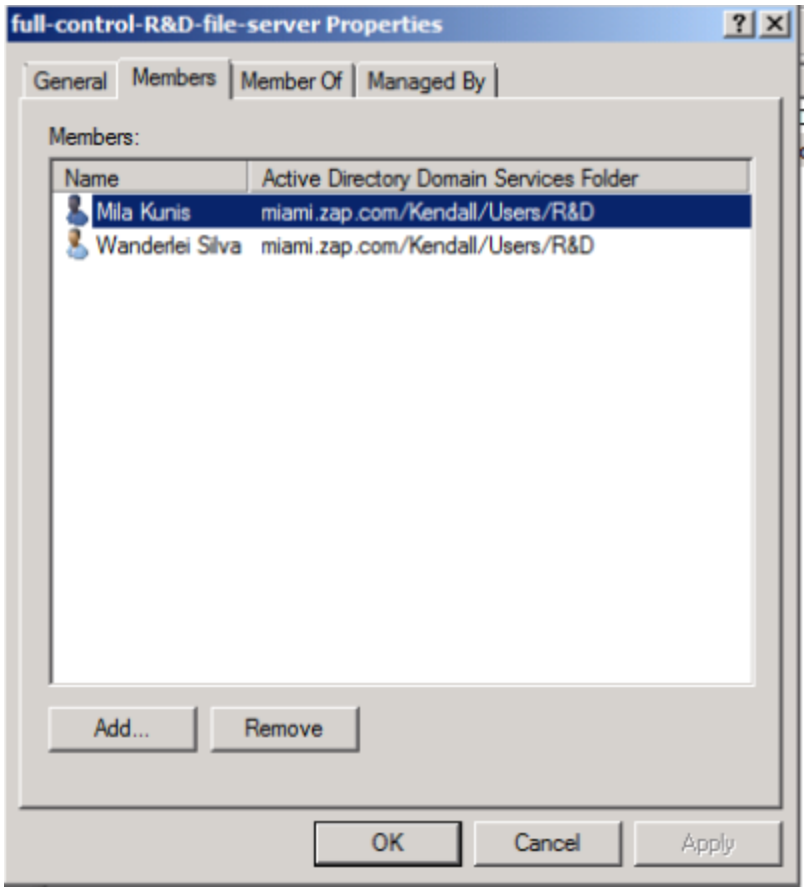
To demonstrate what groups are for, let's pretend the company has a file server where all of the Kendall work documents are stored.



We want to make sure the users in R&D department can only read documents in the R&D folder. So if Bob Dole from Marketing goes into the file server, he will NOT be able to access the R&D folder since he is not in the R&D department. For this, I have to create a group that grants access to R&D users only.

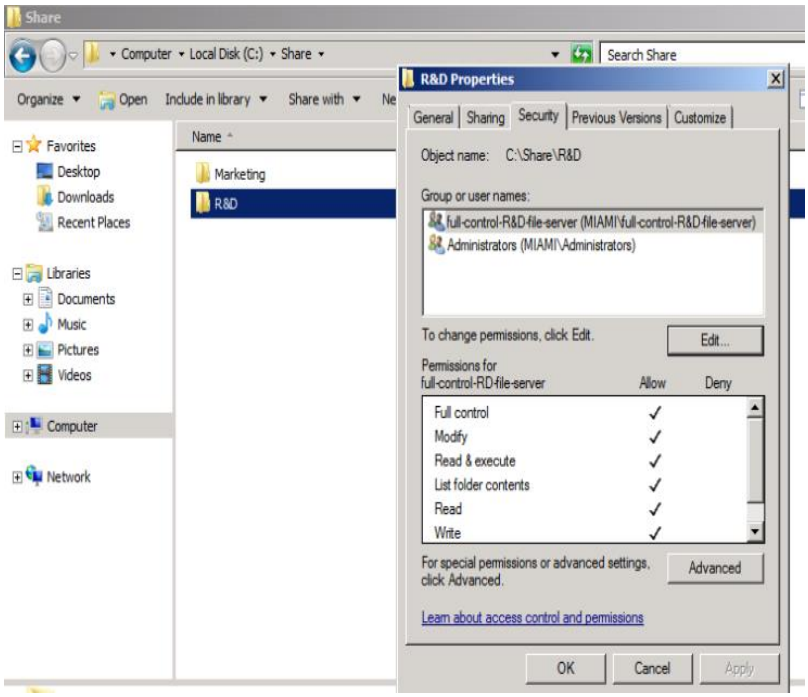


Group created…now it's time to add R&D people into the group.



Note the name of the group – it is always important to be very descriptive of what the group is for on its name. Now users from R&D OU have been added to the group that lets them in the R&D folder in the file server.

Now we have to go to the file server and bind the folder to the group we've just created.



There it is…it's showing that for the R&D folder, anyone that belongs inside the "full-control-R&D-file-server group" is allowed and has full control of the documents inside.

Conclusion:

OUs let us be more granular with the organization – and place users, computers, groups in them. They let us organize things in a certain way so we can then apply policies and protocols to the OUs.

As you just saw, different groups and locations have different business needs, and Active Directory allows an administrator to provide to these business needs.

The best way to learn Active Directory is to use it. Plain and simple, but one of the issues with getting hands on experience on Active Directory is finding a job where entry-level IT professionals are allowed to touch it, which are not too many.

YouTube videos:

https://www.youtube.com/watch?v=lFwek_OuYZ8

https://www.youtube.com/watch?v=J8uw3GNZxzQ

https://www.youtube.com/watch?v=qkN4bvqWqvo