Lab 6 – Active Directories, Organizational Units, Groups, Users and Security Policies

In this lab we will learn about components of Active Directory: Organizational Units (OUs), users, groups and related security issues and policies. We will explore password policies and learn how to set these up on Windows Server 2016. We will create Active Directory users and groups and learn how to set up associated accounts. We will see how to use OUs to delegate administration and manage group policies.

Discussion

As we saw in the previous lab, Active Directory (AD) is a part of Windows Server operating systems and is what makes a particular server a domain controller. AD is both a database where we keep information about identities of objects in our network and is also where we would go to check if something "belongs" to our network.

Security is integrated with Active Directory (AD) through logon authentication and also through access control to objects in the directory. With a single network logon, administrators can manage directory data and organization throughout their network, and authorized network users can access resources anywhere on the network. Policy-based administration eases the management of even the most complex network.

AD provides protected storage of user account and group information by using access control on objects and user credentials. Because AD stores not only user credentials but also access control information, users who log on to the network obtain both authentication and authorization to access system resources.

AD allows administrators to manage system security efficiently. For example, by setting a file's properties, an administrator can permit all users in a group to read that file. Access to objects in AD is based on group membership. In addition, users belonging to a given OU may be prevented from performing certain tasks on one or more systems.

Active Directory Objects

Some common components that make up an Active Directory are:

- Resources (computers, files, etc.)
- Users
- Groups
- Organizational Unit
- Domains
- Trees and Forests
- A global catalog

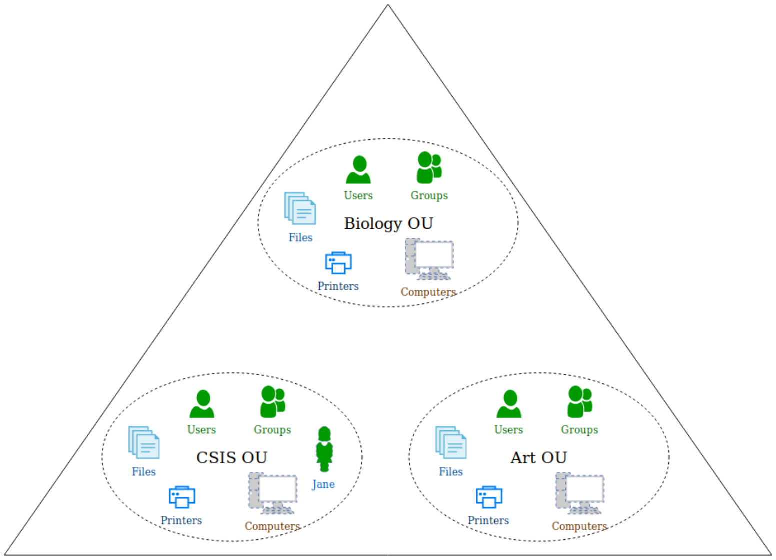
Groups

We can place users with similar needs in a “container” called a **group.** A user group allows us to grant secure access to resources to many users in one step. Resources with similar purpose, like computers or printers, can also be placed in a group and access to a group of resources can be given to a single user or a group of users. We can even create groups of groups!

Organizational Units

An Organizational Unit (**OU**) is an Active Directory container used to organize related objects in a single domain. For example, we can use an OU to organize users, groups, computers, and printers in a department of our business or organization. This way, we can assign an administrator the responsibility of supervising all objects in an OU. We could also assign policies to an OU to lock down users and computers from performing certain tasks. For example, we can prevent users in a group from activating the screen saver.

The following example has three OUs within the uwrf.edu domain. The CSIS OU contains individual CSIS students as well as groups along with resources like computers and printers assigned to the CSIS department. Jane is assigned the task of administering the CSIS OU, authorizing her to add/remove/change any of the objects with the OU. Jane may add a new printer to the OU and allow only the user hnajafi to print to that printer. Jane may also create a group policy preventing hnajafi from starting the task manager, or change the background on his computer and remove the user hnajafi from the OU when he retires. Users in the other OUs are not affected by these changes.



uwrf.edu domain

Active Directory Replication

A domain controller (**DC**) is a server that runs AD in order to manage and secure objects in a network. As such, it is a critical service on that network domain: a failure in a DC will bring down the network of computers in that domain. Although individual computers will continue running, users may not be able to access them if, for example, users cannot be authenticated to connect to a computer or a service like a print service running on these computers.

For this reason, it is important to have one or more replicas of the primary controller on the network. The controllers will be copies of each other and maintain the same AD through periodic replication of their active directories. This way, if the primary controller dies, the secondary controller can automatically take over.

Active Directory Structure

Directory replication between domain controllers can lead to performance problems if the physical connectivity of the network is not properly configured. For example, if we have a domain replicated across a ***slow*** network connection, replication can bring network performance down and potentially render the network useless. To remedy this problem, the Windows Server 2016 uses **sites** and **site links**.

A “site” represents domain controllers connected via ***high speed*** network connections. Replication within a site takes place based on a change notification process. Any changes in an AD will lead to the server waiting for 15 seconds and then announcing the change to the other domain controllers with the site. A **site link** connects two sites and offers the ability to manage the replication process across the slow links. For example, you can indicate how often or when replication should take place across a link.

Finding Directory Information

Active Directory is designed to provide information to queries about directory objects from both users and programs. Administrators and users can easily search for and find information in the directory by using the Search command on the Start menu. Client programs can access information in AD by using Active Directory Service Interfaces (ADSI).

One of the main benefits of AD is its rich store of information on network objects. Information published in AD about users, computers, files, and printers is available to network users. This availability is controlled by security permissions to view information.

Everyday tasks on a network involve communication with other users and connection to published resources. These tasks require finding names and addresses to send mail or connect to shared resources. In this respect, AD functions as a shared address book for the enterprise. For example, you can find a user by first name, last name, e-mail name, office location, or other properties of that person's user account. Finding information is optimized by use of the global catalog, as explained earlier in this manual.

Efficient Search Tools

Administrators can use the advanced Find dialogs in the “Active Directory Users and Computers” snap-in to perform management tasks with greater efficiency and to easily customize and filter data retrieved from the directory. In addition, administrators can add objects to groups quickly and with minimal network impact by utilizing browse-less queries to help find likely members.

Active Directory Communication standards

AD uses the DNS naming standards for IP name resolution. For example, if you need to locate the server csis.uwrf.edu, a DNS lookup is used to resolve the IP address. Once the IP is discovered, a direct communication session can take place. The Lightweight Directory Access Protocol (LDAP) is then used to query and update the Active Directory Database.

Password Policies

Active Directory provides several security mechanisms to help protect your system. Perhaps the most fundamental security mechanism is password protection. However, because password protection is so fundamental, it is often given little thought. Yet it is a weak password policy that makes your directory most vulnerable to break-ins.

A password policy is a set of rules that govern how passwords are used in a given system. The password policy mechanism provided by the directory server allows you to dictate such things as the minimum length a password must be and whether users can reuse passwords. When users attempt to logon to your system, the directory server compares the password with the value in the password attribute of the user's directory entry to make sure they match. The directory server also uses the rules defined by the password policy to ensure that the password is valid before binding the user to the directory.

The following are examples of policies that may be associated with passwords:

- Password Expiration (Maximum Age): We can set our password policy to have users use the same passwords indefinitely by having the passwords never expire. Or, we can set our policy so that passwords expire every 1 to 24,855 days. In general, the longer a password is in use, the more likely it is to be discovered. On the other hand, if passwords expire too often, users may have trouble remembering them and resort to writing their passwords down. A common policy is to have passwords expire every 30 to 90 days.
- Password Forced Validation (Minimum Age): We can set our password policy so that users cannot change the password for a period of time. For example, if policy is set to have a minimum age of 1 day, it would force a newly changed password to not be changed for at least one day.
- Password History: We can set our password policy to store from 2 to 24 previous passwords. Or, we can disable password history, thus allowing users to reuse passwords. Password history refers to whether users are allowed to reuse passwords. If a password policy enables password history, the directory stores a specific number of old passwords and when a user attempts to reuse one of the passwords the directory server has stored, the reused password will be rejected. This feature can increase system security by preventing users from using the same password every time it is changed.
- Password Length: The directory server allows us to specify a minimum length for user passwords. In general, shorter passwords are easier to crack. We can require passwords that are from 2 to 512 characters. A good length for passwords is 8 characters. This is long enough to be difficult to crack, but short enough that users can remember the password without writing it down.
- Password Complexity Requirements and Syntax Checking: The password policy establishes some syntax guidelines for password strings, such as using numbers and characters. This ensures that the password is not a "trivial" word.
- Password Storage Scheme: The password storage scheme specifies the type of encryption used to store directory server passwords within the directory. Although passwords stored in the directory can be protected through the use of access control information (ACI) instructions, it is still not a good idea to store clear text passwords in the directory.

Users and groups

User account objects represent all the information that define a physical user with access permissions to the network. Having user accounts assists in the administration and security of the network by making it possible to:

- Require authentication of anyone connecting to the network
- Control access to network resources such as shared folders or printers
- Monitor access to resources by auditing actions performed by a user logged on with a specific account

When creating user accounts, it is important to set standards on the various elements of a user object. Some of these standards may include:

- **Establishing a naming convention:** For example, LastnameFirstInitial
- **Controlling password ownership:** This is the password policy described earlier
- **Including additional required attributes:** For example, should you store an email address or a phone number? Keep in mind every piece of information requires storage and replication in the Active Directory.

<u>Group objects</u> are used to organize collections of users, or other groups into a single security principal. This would simplify administration by allowing assignment of rights and resource permissions to a group rather than to individual users. Groups in Active Directory belonging to a single domain can be assigned a **domain local** scope. Global and Universal scopes are also available when more than one domain is involved (Outside the scope of this course).

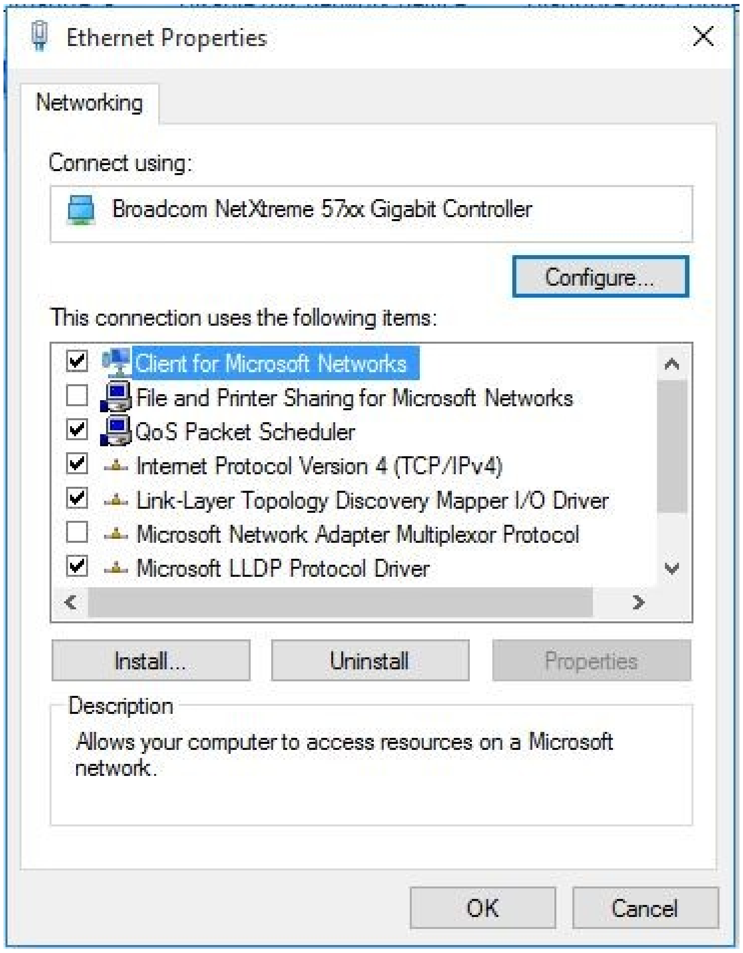
Activities

Disable file sharing on each workstation

- From **Control Panel** select **Network and Internet → Network and Sharing Center → Change adapter settings** → right click **Local Area Connection → Properties**. Make sure **File and Printer Sharing for Microsoft Networks** is unchecked as shown here and click OK.

- Restart the workstations.

- Once all workstations are restarted, connect to your server and view the network by opening file explorer, then selecting Network. You should not see the workstation shared folders (if not restart the server.)



Ethernet Properties

Networking

Connect using:

Broadcom NetXtreme 57xx Gigabit Controller

This connection uses the following items:

☑ Client for Microsoft Networks
□ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
□ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver

Description

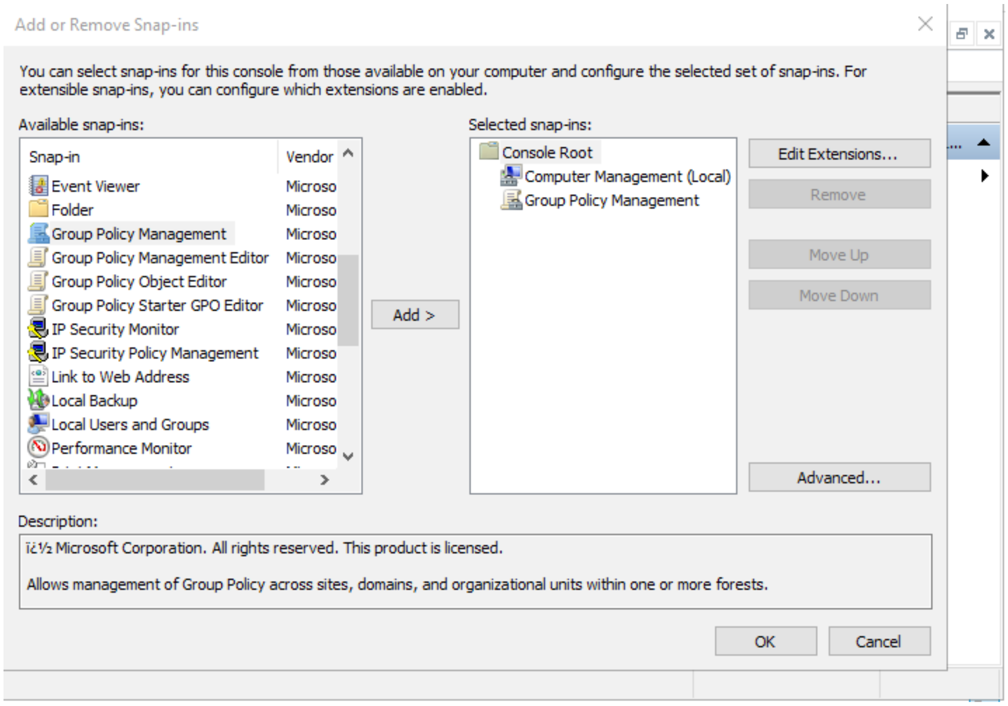
Allows your computer to access resources on a Microsoft network.

CONTACT ME AT THIS POINT AND SHOW ME THE TREE. YOU WILL NEED A SIGN OFF ON THIS.

Set up a password policy on Server

- Remote desktop into your server. You can use the computer name, “Server__” or the IP address of your server to connect.

- Open your previously created mmc console (or else start MMC using **Start**→**Run** and type **mmc**) and add the snap-in **Group Policy Management** as shown here and select OK.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Event Viewer	Microso
Folder	Microso
Group Policy Management	Microso
Group Policy Management Editor	Microso
Group Policy Object Editor	Microso
Group Policy Starter GPO Editor	Microso
IP Security Monitor	Microso
IP Security Policy Management	Microso
Link to Web Address	Microso
Local Backup	Microso
Local Users and Groups	Microso
Performance Monitor	Microso

Selected snap-ins:

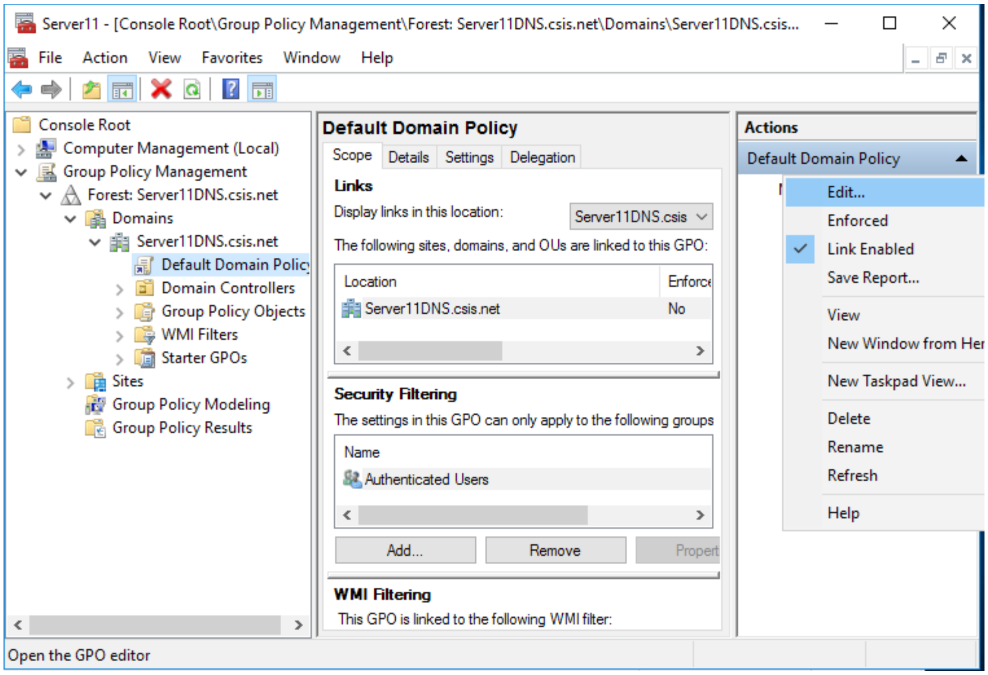
Console Root
Computer Management (Local)
Group Policy Management

Description:

ï¿½ Microsoft Corporation. All rights reserved. This product is licensed.

Allows management of Group Policy across sites, domains, and organizational units within one or more forests.

- Expand the **Group Policy Management**, **Forest: yourservername.csis.net**, then **Domains**, then **yourservername.csis.net**. Select **Default Domain Policy** and on the right side of the screen click on **More** Actions→**Edit**.



Server11 - [Console Root\Group Policy Management\Forest: Server11DNS.csis.net\Domains\Server11DNS.csis...

Default Domain Policy

Links

Display links in this location: Server11DNS.csis

The following sites, domains, and OUs are linked to this GPO:

Location	Enforce
Server11DNS.csis.net	No

Security Filtering

The settings in this GPO can only apply to the following groups

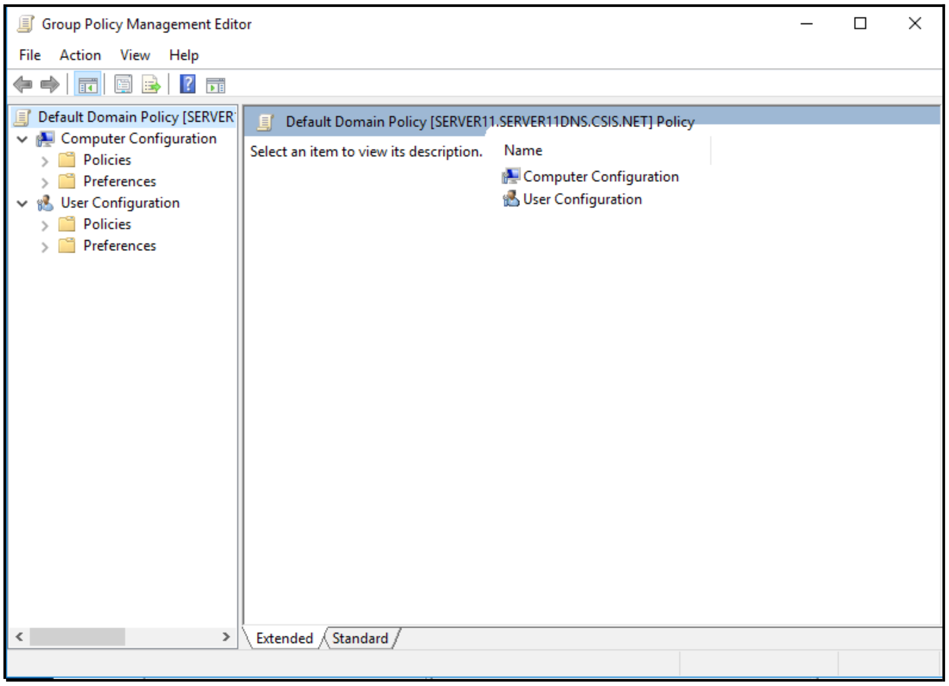
Name
Authenticated Users

WMI Filtering

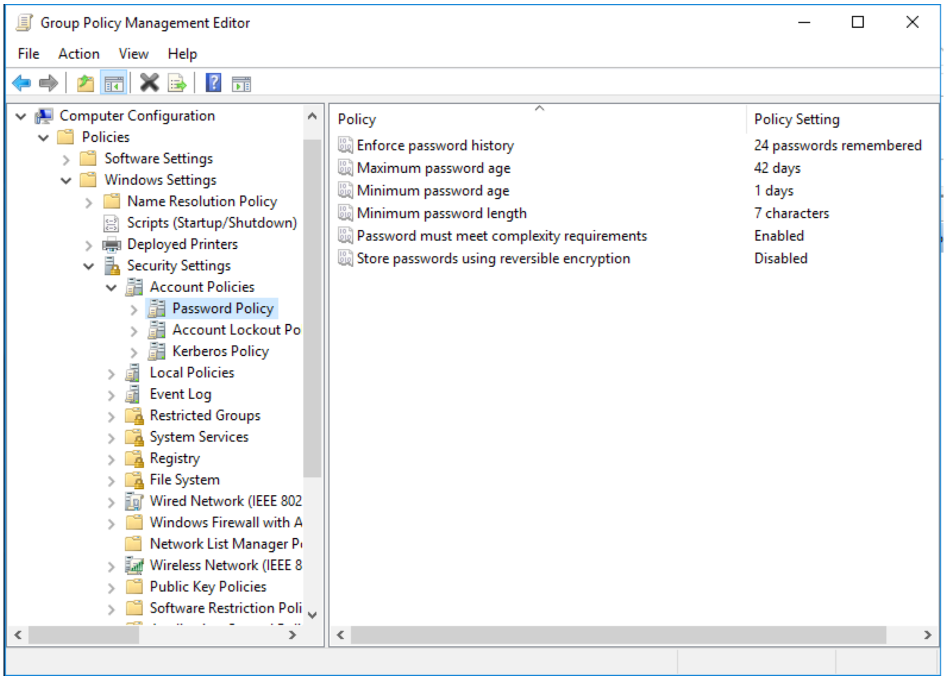
This GPO is linked to the following WMI filter:

Open the GPO editor

- This should bring up the following window:


Group Policy Management Editor
File
Action
View
Help
Default Domain Policy [SERVER
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences
Default Domain Policy [SERVER11.SERVER11DNS.CSIS.NET] Policy
Select an item to view its description.
Name
Computer Configuration
User Configuration
Extended
Standard

- Expand, **Computer configuration**→**Policies**→**Windows Settings** →**Security Settings** →**Account Policies** →**Password Policy** as shown here:



Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

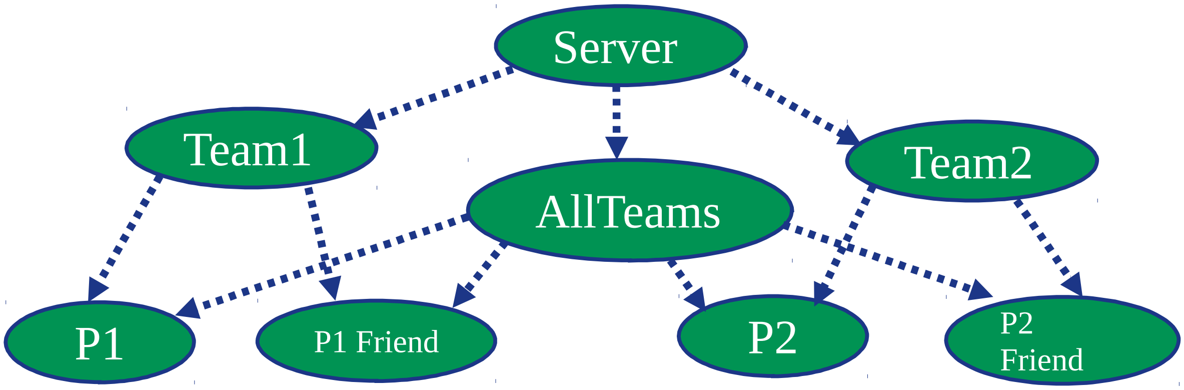
- This is where we can setup our password policies. Search online for the meaning of each of these policies and explain them in your report.

- We will remove all of these restrictions to make life easier for us in this experimental lab. However, in a real network scenario, we would have to make sure these are defined by our supervisors and enforced using this tool.

- Double click each of the policies and set the numeric values to **0** (in effect disabling them) and **Disable** the **Password must meet complexity requirements**. Close the window.

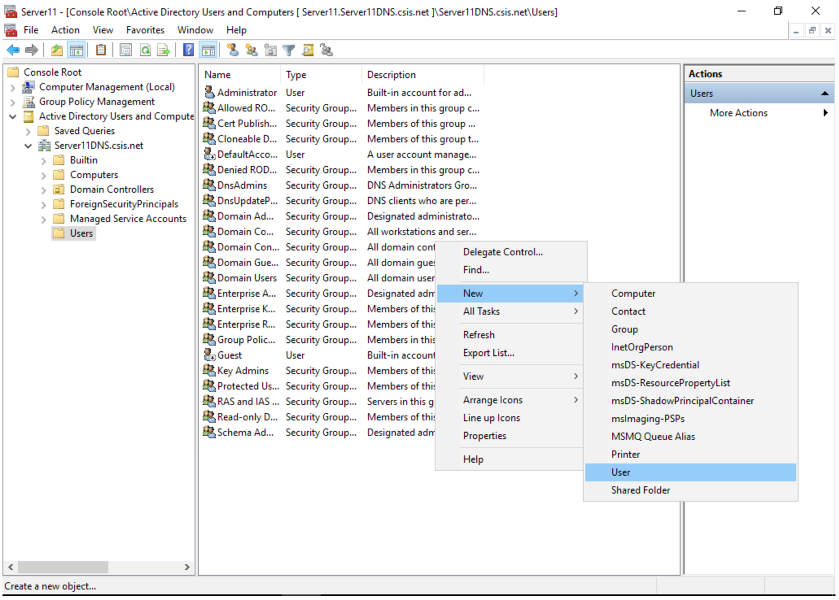
Create users and groups on the server:

- Now that we have a password policy, we can start creating users and groups. We will create a group that represents the Server team, one group for each workstation and two users for each of workstation group. We will organize this so that the server group is composed of workstation groups and workstation groups will be composed of the corresponding members. In this way, access to shared resources can be assigned to the server team members, members of a workstation team or individual members. The following diagram demonstrates this setup. Partner 1 and two represent you and your partner. P1 friend and P2 friend represent someone you know or an imaginary friend.



- Install the **Active directory users and computers snap-in** in **MMC** from the **Add/Remove Snap-in** menu.

- After you have added this snap in, select the **Users** folder. Right click in the pane area (or on the Users Folder) and select **New**→**User** (shown here) to create each user.



Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
DefaultAcco...	User	A user account manage...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain cont
Domain Gue...	Security Group...	All domain gue:
Domain Users	Security Group...	All domain user
Enterprise A...	Security Group...	Designated adm
Enterprise K...	Security Group...	Members of thi:
Enterprise R...	Security Group...	Members of thi:
Group Polic...	Security Group...	Members in thi:
Guest	User	Built-in account
Key Admins	Security Group...	Members of thi:
Protected Us...	Security Group...	Members of thi:
RAS and IAS ...	Security Group...	Servers in this g
Read-only D...	Security Group...	Members of thi:
Schema Ad...	Security Group...	Designated adm

Create a new object...

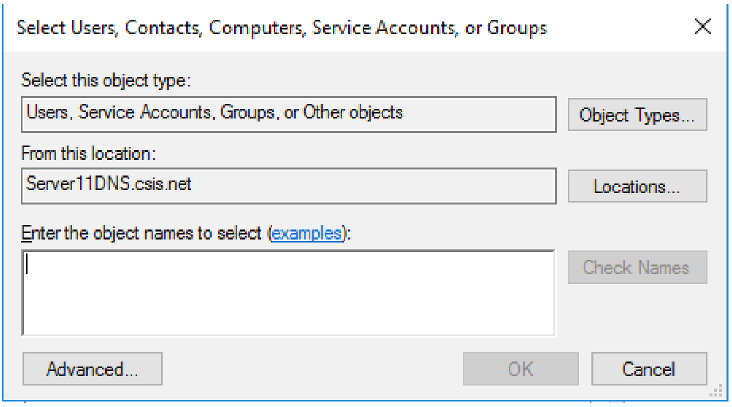
- For each user, enter first and last name and a user logon name. We will follow the policy of making user logon name be the user's last name, followed by first and middle initials. For example Fiona Apple McAfee should have the username McafeeFA. Once this information is entered, click **Next**→enter **network** for password, make sure the **User must change password** is **not** checked→**Next** →**Finish**. Do this for every user (partner1, partner2, p1 friend and p2 friend). <u>In your report, note the other available checkboxes, research them online, and include your findings.</u>

- Once the users are created, double click one of them in the MMC pane and note all the additional information that can be saved for the user. In a real implementation, it would be a good idea to enter some of this information. In your lab report, write down the names of the tabs in the same row as the **General** tab.

- Once you have examined the user information, create your groups the same way you created your users, except select **New group** instead of new user. Use the name **AllTeams** for the server group and make sure that **Domain Local** is selected for the Group Scope. Use **Team1** and **Team2** for each workstation team and set the group scope to be **Global**.

- Now that your groups are created, we will need to add members to each group.

- Start with the **AllTeams** group. Double click this group's icon, select the **Members** tab and click **Add**. You should see the following



Select Users, Contacts, Computers, Service Accounts, or Groups

Select this object type:
Users, Service Accounts, Groups, or Other objects

From this location:
Server11DNS.csis.net

Enter the object names to select (examples):

- Enter the first few characters of each team name in the **Enter the object names to select** text area, click **Check Names**, select the corresponding group from the displayed list, and click **OK**. Do this for all members.

- Now add each team member to the corresponding team group.

- At this point we have a number of users placed in groups that are, in turn, grouped by the server team. To test this, authenticate each of the users you created with the domain controller by logging into your workstations as these users. (Note: no need to restart the computer – just logout and log back in as a different user. Also, keep in mind that to remote desktop to the server you need to use the administrator account and not the new user accounts).

CONTACT ME AT THIS POINT AND DEMO YOUR SETUP. YOU WILL NEED A SIGN OFF ON THIS.

Although you now have an account on the server and you can log onto it, you do not have rights and permission to do much. In the next lab we will learn how to provide users and groups such rights and permissions.

In this part of the lab, we will experiment with OUs to delegate administrative responsibilities.

- Go back to the **mmc** and select GPM (group policy management).
- Drill down (→Forest→Domain) to get your domain (… .csis.net)
- Right click the domain and create a new OU called **team1OU**
- Refresh the window by pressing F5.
- Go to **Users** under **Active Directory Users and Computers**, right click Team1 group→move→team1ou. Do the same for the corresponding users that you created earlier in

the lab.

- Complete the previous steps to create and populate team2OU.
- Create a new user called "team1admin" and move it to the **team1OU**.
- Within **Active Directory Users and Computers**, right-click the team1OU → Delegate Control. Add the team1admin. Check all of the boxes. Note all the options and especially pay attention to the ability to add and remove users and groups.
- Next we have to give team1admin rights to remote login to the server with administrative rights to be able to perform tasks from any workstation.
    - Open the Control Panel → System and security → System → Change settings → Remote tab, click Select users and add team1admin and Administrator to the list.
- Now access Group policy management from the mmc. Expand the forest, domains, domain controller and you should see the default domain controllers policy. Make sure this is the one under the Domain Controllers folder. Right click on the default domain controllers policy → Edit, expand Computer configuration → Policies → Windows settings → Security settings → Local policies → User Rights Assignments.
    - Double click **Allow logon Locally**. If **Define These Policy Settings** is not checked, go ahead and check it. Now click **Add User or Group**, browse, then add team1admin.
    - Double click on **Allow logon through remote desktop services**. If **Define These Policy Settings** is not checked, go ahead and check it. Now add team1admin and Administrators.
    - Now to be sure that the group policy is updated, click the Windows Icon and in the search area type **`gpupdate`**. Wait for it to indicate that it was successful.
- From one of your workstations, remote desktop to the server as the team1admin user.
- Open mmc. If it cannot be found through the search feature click the Windows icon → run → mmc.exe.
    - Note: If prompted to login in to access the mmc, use the credentials for the user you are logged in as. For example, if you are using the team1admin account to login to the server, you would use the team1admin credentials **not** the administrator.
- Create a **new** mmc with the snap-ins: Group Policy Management and Active Directory User and Computers. Save it to the desktop.
- Go to Active Directory, then team1OU and try to edit the name of one of your user and create a new user in team1 group called testuser. If you did everything correctly, you should be able to do this since team1admin has been delegated this responsibility for the team1OU.
- Go to the team2OU and try to do the same actions as in the above steps. You should not be able to do this as team1admin had not been given administrative rights to the team2OU.

CONTACT ME AT THIS POINT AND DEMO YOUR SETUP. YOU WILL NEED A SIGN OFF ON THIS.

- Exercise: Performs the above steps for team2OU.

CONTACT ME AT THIS POINT AND DEMO YOUR SETUP. YOU WILL NEED A SIGN OFF ON THIS.

In this part of the lab, we will experiment with using OUs to enforce group policies.

- Remote login with the administrator account.
- Go back to the mmc and now select Group policy management.
- Drill down to get your domain (…com)
- Right click Group Policy Objects → New. Give the policy object the name **team1OUGP**
- Next, we need to set the security permissions for the team1OU. Right click team1OUGP → Edit, look around in the computer configuration policies and see what is available. In your

report, list three of them.

- Explore all other settings under the Computer and user configuration settings.
- Under User Configuration, Policies, Administrative Template Policy … → All Settings → find Remove Task Manager. Double click it and select Enabled.
- Now we need to link the team1OUto this group policy. To do this, right click team1OU in **Group Policy Management** → Link an Existing GPO → select team1OUGP.
  - Group policies can be created, configured, and managed using PowerShell. The link below shows how to configure group policies:
  - https://sid-500.com/2017/08/25/configuring-group-policies-by-using-windows-powershell/
- Now login as a user from team1 on a workstation and try to run the task manager. You should not be able to do this.

CONTACT ME AT THIS POINT AND DEMO YOUR SETUP. YOU WILL NEED A SIGN OFF ON THIS.

- Exercise: Performs the above steps for team2OU.

CONTACT ME AT THIS POINT AND DEMO YOUR SETUP. YOU WILL NEED A SIGN OFF ON THIS.

Before you leave, save your MMC setting, close all applications, and shut down the server and your workstations.

CSIS 247 Lab #6 Active Directory *Lab* Sign-offs Due: 9:00 am Oct. 21st

1 sheet per team – print this sheet and bring it to the lab.

Your Names: ____ *Server/Team #:* ____

Date: __________

Sign-offs:

Network tree

Login from workstation

team1admin changes to team2OU

team2OU changes

Run task manager as user from team1

team2 changes

CSIS 247 Lab #6 **Report**

Active Directories, Organizational Units, Groups, Users and Security Policies

Your Names:

Enter the information you gathered in the lab into this work document and submit it using the D2L Dropbox.

Make sure to submit the original copies of my sign-off.

As in the previous lab, Falcon Inc. has three divisions connected via a network:

- The Minneapolis division connects to London and Amsterdam via a slow 256Kbps link that is not very reliable.
- The London division connects to Amsterdam via a dedicated and reliable fiber optics line.
- Each division has an HR, Accounting, Engineering, and a Sales department.
- Each department is composed of user, group, computer and printer objects.
- Each department is responsible for management of their own objects and they have a corresponding administrative user.
- The HR department should not have the ability to start the task manager or install any new applications on their computers.
- Each user of a division would need to be given access to their personal resources such as files and printers. Also, members of each department would need to have access to a departmental shared folder where they can exchange documents.
- Each division will also have a plotter that will be accessed by all employees of that division.
- In addition, Sales and Engineering departments belonging to all divisions will need to have a shared area for exchange of documents.

A) What group and user structures would you recommend for this organization?

B) What kind of Active Directory Structure would you recommend for Falcon Inc?
Provide a diagram – a graphical representation of your recommended Active Directory Structure including users, groups, computers, printers, plotters, domains, OU(s), OU(s) delegation, site(s) and sitelink(s) and group policies.

Use a site like www.draw.io or software like Word, LibreOffice, or Visio to create the diagram – hand-drawn or hand-lettered diagrams will not be accepted.