**CSIS 2260 - Lab #9**

20

***Windows Server 2019 - Active Directory and Group Policies***

Due date: 20:59 March 26, 2021 (Pacific Time)

**Name: Stephen Joy Student No.: 300329148 Section: 012**

**Objectives:** To learn about Active Directory, Domain Controllers, Group Policy and setting User Rights in Windows Server 2019.

**Insert the required screenshots in the Word file. Do not submit the screenshots separately.**

**You may not use the numeric keypad on your keyboard in the Windows Server 2019 virtual machine, especially when you enter the password. It is turned off by default.**

**Write down your answers in the highlighted areas.**

**Equipment Required:**

A Windows 10 PC with VirtualBox installed and a Windows Server 2019 VM created.

**Introduction:**

***AD DS*** is a directory service that enables you to create organizational divisions called ***domains***. A domain is a logical container of network components, hosted by at least one server designated as domain controller. The primary functions of AD DS are to provide authentication and authorization services for hardware and software resources on the network. Users joined to an AD DS domain can log on to the domain, as opposed to an individual computer, and can access any resources in that domain for which administrators have granted them permissions.

In AD DS, you can subdivide a domain into organizational units (***OU***) and populate it with ***objects***, each of which represents a logical or physical resource such as user, group, computer, printer, etc. Every ***object*** consists of ***attributes***, which store information about the object. For example, a user object can have attributes such as user’s name, address, and phone number. An OU is part of a domain and inherits policies and permissions from its parent objects. One can also apply separate Group Policy settings to an OU.

An organization can have multiple domains which can be joined together as a ***forest***. The first domain created on an Active Directory network is the ***forest root domain***. Active Directory services are implemented in the network’s ***domain controllers***. Each domain controller hosts one domain, storing domain’s objects in a database. Users and computers access domain controller frequently as they log on to the domain and access domain resources.

1. **Installing the Active Directory Domain Service (AD DS) [\_\_\_\_\_/4]**
2. Start the Windows Server 2019 VM in VirtualBox.
3. Use ***right Ctrl*** + ***Del*** to log in as administrator. Ensure that the Windows Server VM is connected to the Internet. You MUST connect to the network before installing the AD DS.
4. Install AD DS Role
5. From ***Server******Manager***, select ***Manage*** > ***Add Roles and Feature****.*
6. For the first few pages, take the defaults and click ***Next***.
7. Under ***Server******Roles***, select ***Active Directory Domain Services***.
8. Click ***Add******Features*** to accept the dependencies. Click ***Next*** until the AD DS page.
9. On the AD DS page, what is the information shown regarding the role of AD DS?

AD DS stores information about users, computers, and other devices on the network. It helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

1. Confirm installation selections and click ***Install***. DO NOT close the installation window.
2. When the installation is completed, a hyperlink showing ***Promote this server to a domain controller*** will appear in the window. (Note that if you have closed the installation window, just wait for the installation to complete. You can then get the link by clicking the ***Notifications***flag icon on the top right of the ***Server*** ***Manager*** window.)
3. Create a New Forest
4. Click the ***Promote this server to a domain controller*** hyperlink.
5. An AD DS Configuration Wizard window will open.
6. Select ***Add a new forest***, use ***csis.com*** as the Root domain name, and click ***Next***.
7. Use ***Csis2260*** as Directory Services Restore Mode (**DSRM**) password and click ***Next***.
8. Click ***Next*** to skip the warning regarding the DNS (as DNS has not been installed).
9. Take the defaults for the rest.
10. Ignore any warnings and click ***Install*** after passing through the Prerequisites Check.
11. System will restart after complete installation. Try to log in as *student1*. Can you log into the system? No
12. Log in as administrator.

Note that after AD DS has been set up, only the administrator can log into the server. To allow other users to log on to the server, security setting under group policy needs to be changed.

1. **Creating Active Directory Users [\_\_\_\_\_/3]**
2. Two Approaches to Create New Active Directory Users
3. From ***Server******Manager***, select ***Tools*** > ***Active Directory Administrative Center****.* From the pop-up window, expand the local domain ***csis (local)*** on the left and select ***Users***. From the ***Tasks*** panel on the right, select ***New*** > ***User***. Create a user with the following information and leave the other fields blank:

Full Name: **student no 3**

User SamAccountName Logon: csis\**student3**

Password: **Stud3333**

Click ***OK*** to create the user. Close the ***Active Directory Administrative Center*** window.

1. From ***Server******Manager***, select ***Tools*** > ***Active******Directory******Users******and******Computers***. From the pop-up window, expand the local domain ***csis.com*** on the left and select ***Users***. Click ***Action*** at the top and select ***New*** > ***User***. Create a user with the following information and leave the other fields blank:

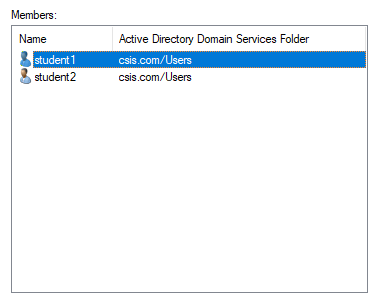
Full Name: **student no 4**

User logon name: **student4**@csis.com

Password: **Stud4444**

Click ***Next*** and ***Finish*** to create the user. Keep the ***Active******Directory******Users******and******Computers*** window open.

1. Managing Multiple Users
2. In the ***Active Directory Users and Computers*** window, expand the local domain ***csis.com*** on the left and select ***Users***.
3. Select users ***student1***and ***student2*** by holding down the Ctrl key. Right stclick and select ***Properties***. From the *Organization* tab, set *Company* as **Douglas**.
4. Click ***Apply*** and ***OK***. Close the ***Active Directory Users and Computers*** window.
5. **Creating Active Directory Groups and Organizational Units (OUs) [\_\_\_\_\_/3]**
6. Creating an Organizational Unit
7. From ***Server Manager***, select ***Tools*** > ***Active Directory Administrative Center***.
8. Right click the domain ***csis*** and select ***New*** > ***Organizational Unit***.
9. Name the new OU as ***lab*** and Click ***OK***.
10. Close the ***Active Directory Administrative Center*** window.
11. Using OU to Delegate AD Management Tasks
12. From ***Server Manager***, select ***Tools*** > ***Active Directory Users and Computers***.
13. Right click the object ***lab*** and select ***Delegate Control***.
14. Click ***Next*** and click ***Add***to add a user. From the pop-up window, type ***student1*** in the Enter box and click ***Check Names*** on the right.
15. Click ***OK*** to add the user *student1* to delegate control of the object *lab*. Click ***Next***.
16. Select ***Create a custom task to delegate*** and click ***Next***.
17. Select ***This folder, existing objects in this folder, and creation of new objects in this folder*** and click ***Next.***
18. Select ***General*** and then select ***Full******Control***from the Permissions box*.*
19. Click ***Next*** and ***Finish*** to complete the delegation.
20. Close the ***Active Directory Users and Computers*** window.
21. Creating and Managing Groups
22. From ***Server******Manager***, select ***Tools*** > ***Active Directory Administrative Center***.
23. Right click the domain ***csis (local)*** and select ***New*** > ***Group***.
24. Name the group ***labgroup***and click ***OK****.* Close***Active Directory Administrative Center***.
25. From ***Server******Manager***, click ***Tools*** > ***Active Directory Users and Computers***.
26. Select ***csis.com***, right click the object ***labgroup*** on the right, and click ***Properties***.
27. Click the ***Members*** tab and then click ***Add***. Type ***student1*** in the Enter box and click ***Check Names*** and ***OK*** to add *student1* as a member of the group.
28. Repeat the previous step to add *student2* as member.
29. Look at the *Members* tab of *labgroup* Properties to check if both *student1* and *student2* have been added as members. Take a screenshot and insert the screenshot below.



1. Click ***Apply*** and ***OK*** to close the pop-up window.
2. Close the ***Active Directory Users and Computers*** window.
3. **Managing Group Policy Objects**

***Group Policy*** is a mechanism for controlling and deploying operating system settings to computers all over your network. ***Group Policy objects (GPOs)*** can be used to manage settings such as user desktop settings and environment variables, software installation policies to ensure that users always have the latest versions of applications, folder redirection to enable users to store files on a network drive, scripts for logon, logoff, startup and shutdown commands, and security settings, etc. One can configure one or more GPOs and associate them with specific AD DS objects through ***linking***. Once a GPO is linked to a container object, all the objects in that container receive the settings configured in the GPO.

1. Create and Link a ***GPO*** to an ***OU*** **[\_\_\_\_\_/3]**
2. From ***Server******Manager***, select ***Tools*** > ***Group Policy Management***.
3. On the left panel, expand ***Forest*** > ***Domains*** > ***csis.com*** and select ***Group******Policy******Objects***.
4. Right click ***Group Policy Objects*** and select ***New*** and name the new GPO as ***csis******policy***. Click ***OK***.
5. On the left panel, right click ***lab***, the OU just created, and select ***Link an Existing GPO***.
6. Select ***csis******policy*** and click ***OK***.
7. Keep the ***Group*** ***Policy*** ***Management*** window open.
8. Managing ***Starter GPOs*** **[\_\_\_\_\_/3]**

***Starter GPOs*** are templates that create multiple GPOs with the same set of baseline Administrative Templates settings. When a GPO is created from a Starter GPO, all the policies in the starter are automatically copied to the new GPO as its default settings.

1. In the ***Group*** ***Policy*** ***Management*** window, from ***Forest*** > ***Domains*** > ***csis.com***, right click ***Starter******GPOs*** and select ***New*** to create a Starter GPO called ***GPO1***. Click ***OK***.
2. Expand ***Starter******GPOs***, right click ***GPO1***, and select ***Edit***. In the pop-up window, select ***Computer Configuration*** > ***Administrative Templates*** > ***Control Panel*** > ***Personalization***. Read through the list shown and give the first setting that is on the list in the following.

Force a specific default lock screen and logon image

1. Select ***Computer******Configuration*** > ***Administrative******Templates*** >***Server***. Read through the list shown and give the first setting that is on the list in the following.

Allow only system backup

1. Close the ***Group Policy Starter GPO Editor*** window and keep the ***Group Policy Management*** window open.

1. **Assigning User Rights** **[\_\_\_\_\_/4]**
2. In the ***Group*** ***Policy*** ***Management*** window, from ***Forest*** > ***Domains*** > ***csis.com***, expand ***Group******Policy******Objects***, right click ***Default Domain Controllers Policy*** and select ***Edit***.
3. Select ***Computer Configuration*** > ***Policies*** > ***Windows Settings*** > ***Security Settings*** > ***Local Policies*** > ***User Rights Assignment***.
4. Right click ***Allow log on locally*** and select ***Properties***.
5. Click ***Add User or Group*** and click ***Browse*** to add the user ***Administrator*** and user group ***labgroup***. (Type the user/group name in the Enter box and click ***Check*** ***Names*** on the right).
6. Check if you can see *CSIS\Administrator* and *CSIS\labgroup* in the ***Allow log on locally*** ***Properties*** window. Click ***Apply*** and ***OK***. Close the ***Group Policy Starter GPO Editor*** window and the ***Group Policy Management*** window.
7. To make sure the change is applied immediately, run a ***Command*** ***Prompt*** as administrator; type the command **gpupdate /force**, press Enter, and wait until the updates finish.
8. Switch to user *student1* (password: *Stud1234*).Can you log in successfully? Yes
9. **Shutdown the Virtual Machine**
10. Log off from all users and shut down the system.
11. Close Oracle VM VirtualBox Manager.

**Submission**

1. Save your lab file as YourFirstname\_yourID\_Lab9.docx.
2. Submit the WORD file through Blackboard before the due (do not send labs by email please. Any lab submitted by email will be ignored). Late submissions will not be marked, and the student will lose the mark of that lab.
3. You may submit your work multiple times, but only the LAST submission before the due will be graded.