



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Network Operating Systems and Services (NOSS)

(ACCA5023)

Worksheet 2

DEPLOYING A NETWORK DIRECTORY SERVICE AND
CREATING AND UNDERSTANDING ACTIVE DIRECTORY
NETWORK OBJECTS

Objectives

- In this part of the assessment, you are tasked with Deploying the Microsoft Active Directory Network Directory Service and demonstrating an understanding essential network directory objects.
- There are a few prerequisite steps that must be undertaken, namely, to rename the System, ensure that the firewall is off, identify a strong administrative password to enforce minimum complexity requirements and identifying a suitable Domain name (DNS zone) for your organisation,
- When the Active Directory is installed, network account creation is required.
 - An additional '*failsafe*' account (Admin, high privilege account) will be created for security purposes.
 - The different built in groups and account types must be understood along with;
 - Account parameters and object/class attributes.
- Following these steps a standalone system (e.g. Client) will be adjoined to the network and standard (non-admin) administrative accounts created and tested.
- Finally you are required, using the Schools accepted referencing system, to complete the Observational Tasks at the end of the worksheet.

NB: YOU ARE REQUIRED TO SCREEN CAPTURE THE COMPLETION OF THESE TASKS IN EVERY WORKSHEET AS YOUR EVIDENCE OF UNDERTAKING THE TASKS REQUIRED. PRACTICE USING THE SNIPPET TOOL AND CAPTURE EVIDENCE AND BUILD YOUR WORKSHEETS USING A WORD PROCESSING PACKAGE SUCH AS MICROSOFT WORD.

YOU SHOULD PROVIDE SUITABLE NARRATIVE ALONGSIDE THE SCREEN CAPTURES TO IMPROVE THE QUALITY OF YOUR PRACTICAL TASKS.

YOU SHOULD READ EVERY ELEMENT IN THE WORKSHEETS, 'VERY CAREFULLY' AS THERE ARE PRE-REQUISITE SNIPPETS OF INFORMATION YOU WILL NEED TO UNDERSTAND, BEFORE UNDERTAKING EACH TASK.

Task 1: Pre-requisite tasks:

[On the Server 1 VM]:

Check that the Server IP is Statically Defined and screenshot the evidence of this, verify that No DNS is setup and that the Firewall is turned off. (**Screenshot your evidence**).

Renaming the Computer that is going to be setup as the Domain Controller is important since it is the most important Server/Service deployed in an enterprise network for managing network resources. It is important to be able to identify which resources/hosts provide each service in our network.

- o Click the Search button and type This PC and then right Click on 'This PC' desktop app, choose Properties.
 - o Choose Advanced System Settings.
 - o Choose the Computer Name tab, click Change.
 - o In the computer name field, type in **DC1-NWT**
 - o **Choose Ok.**
 - o **When prompted to Restart your PC click on Ok again.**
 - o **Click Close on the System properties window.**
 - o **Choose Restart Now.**
 - o Now the Server will close down, log back on, go back to This PC as in the steps above and verify (via a **screenshot**) that the computer name has been changed.
-

Task 2: Deploying Active Directory as a role or feature based installation.

Active Directory is Microsoft's proprietary technology for deploying a network directory service in enterprise networks. Think of a network directory service as a 'register' of all the resources that reside in your network (workstations, servers, people, printers, policies etc.). Recall that a network directory service is method of simplifying the task of better managing, organising, locating and verifying the existence of specific items or resources that you may need catalogued, on your network.

[On the Server 1 VM]:

- o Click the Search button and type in Server Manager, click on the Server Manager desktop app.
- o Whilst in the Server Manager window, choose Dashboard
- o Now click on Add roles and features
- o At the *before you begin screen* ensure that you take account of the pre-requisite tasks that we have verified in task 1. Note that we will be using a strong password for our Administrator account. This domain admin level account is the most critical one in our network. Without it, we cannot manage the network through Active Directory.
- o Choose Next
- o At the Select Installation Type screen, choose **Role or feature-based installation**.
- o Select our DC1-NWT and the Server Selection window, choose Next.
- o In the Select server roles window, check on the radio button next to Active Directory Domain services.
- o Now an additional window will be presented asking for additional required features, click on Add Features.
- o After adding active directory features, click Next
- o At the Select features just click Next (to accept the default options).
- o The Active Directory Domain Services window gives a summary of what AD DS (Active Directory Domain Service) does, read this and choose Next.
- o At the Confirm installation selections window, click on Install to install ADDS.
- o Once the installation process is complete click on Close.

- o Within the Server Manager, note the notifications icon at the top right corner of the window, and then click on; 'Promote this server to a domain controller'.
- o In the Deployment Configuration window choose '**Add a new forest**', specify the Root domain name: **nwtraders.msft**. Click Next
- o In the Domain Controller Options window, where it states Forest functional level, ensure that Windows Server 2016 is selected. Similarly choose the same option for Domain functional level. **(DO NOT CLICK NEXT YET)**
- o Specify domain controller capabilities:
 - o Domain Name Systems (DNS) server should be checked on and
 - o the Global Catalog option should also be checked on.
- o Type the Directory Services Restore Mode (DSRM) password, set the following case sensitive password and Confirm password: **N3tW0rk1**
- o Choose **Next**
- o Ignore the warnings presented at the DNS Options window, choose Next.
- o At the Additional Options window – choose Next.
- o In the Paths window, take note of the locations of the Database Folder (this is where the Database that AD uses like a 'telephone directory' (X.500 protocol) is installed on the system). Also note the SYSVOL and Logfiles folders. SYSLOG is where the global catalog (GC) for the entire domain is installed and the Logfiles keep a record of every action performed within the Active Directory. Accept these default options, **Choose Next**.
- o At the Review Options summary page, choose Next.
- o The pre-requisites check will then be performed, and barring any errors, you are able to click Install.
- o Once the installation is complete, Windows will prompt stating that the machine has successfully been configured as a domain controller. The system should then reboot automatically.
- o At the login screen, since you have now installed a network domain in our case the nwtraders domain, you will need to login to this domain using the account we created above.
 - o **Username:** administrator
 - o **Password:** N3tw0rk1

Task 3: Creating user account objects using Active Directory Users and Computers snap-in console.

[On the Server 1 VM]:

- Active directory has several subcomponents, depending on the operations you require, but generally most AD management is done within the Active Directory Users and Computers snap in program.
 - o Click Start – Administrative Tools, From the resulting dialog window, double click on **Active Directory Users and Computers**.
 - o Note the left hand of the window is the overall directory structure and the right hand side of the window details the containers contents.
 - o Click on the arrow slightly to the left of the **nwtraders.msft** icon in the top left area of the window. This will expand your domain and its default containers and objects.
 - o Everything in Active Directory is referred to as an object (in a similar fashion to how Linux kernels see everything as a 'file').
 - o Again note on the left that there are multiple rows of what look like folders, these are referred to as *Containers or Organisational units*. They are used to manage the various objects and levels of access that coincide with these objects in the AD.
 - o Click on the Domain Controllers window (**screenshot the evidence**), verify that our Server DC1-NWT is listed as the nwtraders.msft domain controller.
 - o Now click on the Users container.
 - o Within this container there are various groups of objects, in the right hand side of the window, click on the Type Column to sort these groups by Type.
 - o Note the group, Domain Admins. This is where all the domain admin user accounts reside for AD management. The Domain Admins group is the highest level privilege group in the Active Directory forest and is unrestricted in what operations it can perform. **Double click on this group.**
 - o Click on the Members tab. Note that the Administrator account we are currently using is listed, however, it is always beneficial to create an

additional failsafe account in case of the primary administrator account being hacked or the password lost/changed intentionally or unintentionally.

- o We need to first create a User account before we can add it as an additional member of this Domain Admins group. For now, choose Ok to close this window.
- o Right Click on the Users container on the left of the window.
- o Select New and User
- o Specify your first name, Last name the Full name field should automatically populate
- o In the user logon name field: enter NWT-[Yourinitials], e.g. **NWT-LC**. Choose Next
- o In the password window, choose your own password. It will need to comply with **Microsoft's Minimum complexity requirements** (you'll possibly need to google that to determine a suitable password). We'll come across this concept again in a later worksheet.
- o In the options below it **Check off: User must change password at next logon**
- o **Check on: Password never expires.**
- o Click Next and at the last summary window click Finish.
- o The user account has now been created.
- o We now need to add this account to the Domain Admins group, so double click on the Domain Admins group.
- o Click on the **Members tab** and Click the **Add button**
- o Where it states 'Enter the object name to select', enter the name of the account you created above then click the Check Names button. You should notice the account is found and has been underlined to confirm this. Note the name of the person that holds the account is found and in brackets the UPN (User Principal Name) or as we know it, the user logon name within our domain structure is shown.
- o Choose Ok and Ok again to close the window.
- o The account has now been added as a Domain Admin account in nwtraders.msft

Task 4: Object attributes of interest.

There are a number of attributes that we can use to optimise the management of objects we use in an Active Directory. It is possible to enforce network policy options and better control our objects in this way. Here, we will investigate some of these options and setup some useful controls. For this scenario we will assume that every domain has both restricted and unrestricted groups of users. Restricted groups of users will have a number of limitations imposed upon their user activities on the network. These limitations are usually enforced via Group Policies, but it is important that the attributes of a user object are utilised to optimise such policies.

[On the Server 1 VM]:

- Within Active Directory Users and Computers, within the Users folder create a new user account (try to be sensible with the logon names etc ;-))
- By default this account will reside in a global group called Domain Users, double click this group and verify (with a **screenshot**), that the account you have just created is listed in the Members tab.
- Here we will utilise the attributes of a user object to work alongside Group Policy (**WS3**) to restrict users' logon hours. The first part of this is done in this worksheet and the second part of the task is done via GP in Worksheet 3.
- Right click on the user you have just created, choose Properties.
- Click on the Account tab, choose Logon Hours.
- Here we will set the User to be permitted logon between Monday 8am and Thursday 5pm.
- The squares in the chart represent 1 hour timeslots, deny the user account logon rights between 1 and 2pm Monday to Friday (select the square and choose the Logon Denied radio button), you should see these 1hr blocks on each day turn white. Choose Ok.
- We will also restrict the user from changing their password, as this is typically a security measure enforced at Network Admin level.
- On the Account tab, beneath *Account options*: check on, **User cannot change password.**
- Choose Ok to confirm.

Task 5: Adjoining the domain and testing user logins.

In this task, the computer account object will be created in Active Directory, we will then logon to the client, adjoin the domain and finally test the user accounts we have created to ensure that the client is properly joined to the *nwtraders.msft* domain.

[On the Server 1 VM]:

- Choose Active Directory Users and Computers, click on the Computers container. Verify that there is no computer account created for either of the client (Client 1 or Client 2) workstations.
- On the right hand side of the console window, right click in the whitespace and choose New – Computer.
- Computer Name – enter WS1-NWT, choose Ok.
- The account is now created.
- We will now need to join this Workstation to the domain.

[On the Client1 VM]:

- Login to the client PC using username: Administrator password: P@ssw0rd
- Click the Search button and type This PC and then right Click on 'This PC' desktop app, choose Properties.
- Choose Advanced System Settings.
- Choose the Computer Name tab, click Change.
- In the computer name field, type in WS1-NWT
- **You will need to restart the computer.**
- **Upon restarting Sign in again using the administrator account.**
- At this stage, we are going to need to make an IP address configuration change as we require our client to connect to the DNS server running on the Server 1 VM,
- Recall, we added the DNS service as part of our AD install.
- In the search field, type in Control Panel click on the icon
- Click on the Network and Internet option
- Under the Network and Sharing Centre option, there is an option listed entitled **View network status and tasks**, click on this option.
- On the left hand side of the window, click Change adapter settings

- Right click on the PrivNet1 Ethernet connection, click Properties.
- Double click on Internet Protocol Version 4 (TCP/IPv4)
- Ensure that use the following DNS server address is selected, enter the following value for Preferred DNS Server:
- 192.168.1.100
- Chose Ok to close down the resulting Windows.
- Now, as before click on the Search button and type in this PC then right click and choose Properties.
- Click on the Computer Name tab
- Click on the Change button
- Under the Member of click on the Domain radio button and enter **nwtraders.msft**
- You will prompted for a domain admin level account, since you are trying to adjoin the domain.
- Username: Administrator
- Password: P@ssw0rd
- You should be given a dialog welcoming you to the nwtraders.msft domain.
- You will now need to restart the client
- Upon the restart note that the workstation is on the domain. We are now able to logon locally (e.g. onto the PC as it was before we joined the domain) or onto the nwtraders.msft domain
- Recall that a second, a non-administrative account was created, you should remember and have taken a note of this account, when attempting to logon to the workstation via the domain, so enter the username and password of that account now.
- Verify that you are logged into the network by looking at the identity icon (click on Start and the icon is an icon of a person, just to the left, if you leave the mouse cursor over this icon, it should verify your name).

[On the Server 1 VM]:

- The last thing to try is to try attempting to logon onto the Server1 VM with this same non-administrative User Account.
- Note that you will be greeted with an unsuccessful error message, this is because only Domain Admin level accounts are permitted to logon to Systems with the Domain Controller role.

Task 6: Observational Tasks

NB: You should use a proper referencing style here when submitting your answers

6 a) DNS - explain what it is, how it works (illustrations) and its significance within Active Directory Domain Services.

6 b) AD is one critical 'Role or Feature based installation' as part of an enterprise network, identify and provide a brief overview of 2 other critical roles?

6 c) Explain why it is important to have different levels of access/roles within the '*Built in*' Network User Account groups (e.g. Domain Admins, DHCP Admins, etc).

6 d) Share your ideas in-detail on Microsoft's recommendations on AGDLP and AGUDLP for assigning permissions. How do you view them in the perspective of a System Administrator in strategizing and implementing within your network?