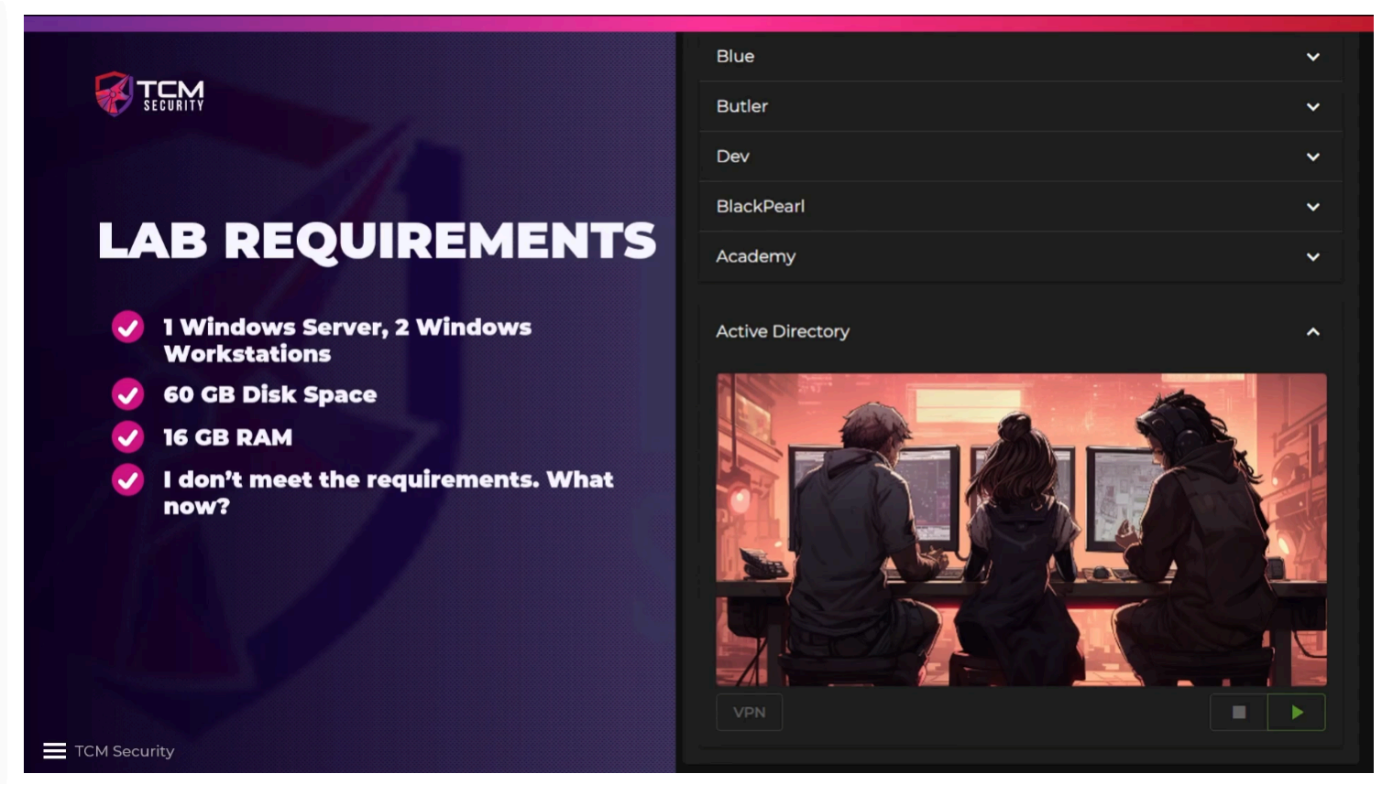
9.0 - Setting Up the Domain Controller



So, we are going to set up a windows server with 2 windows workstations.

We are going to download from "https://www.microsoft.com/en-us/evalcenter".

One "Windows 10 Enterprise", and one "Windows Server 2022".

Go to the website, and download it.

Then, we are going to start with the Windows Server 2022, which is going to be our Domain Controller.

1 - Setting Up Domain Controller

We are going to create New Virtual Machine. Pick the ".iso" file for the Windows Server to be installed. You can create a name, the storage location, and VMware also allows to create a Password to be used every time the user wants to boot it. Then, make sure to hit a key after it boots and prompts to hit a key, otherwise it will try to boot from a floppy, and it wont go any further. Then, if it is not booting, and it is asking for the activation code, or if you are getting a error message saying there is no Microsoft key set, or something about key, maybe there is a floppy driver created together with the virtual machine. Just get in the virtual machine settings and delete/remove the floppy disk and try booting again. It should work.

It is going to open the virtual machine.

Select the language desired.

We are going to install the "Windows Server 2022 Standard Evaluation (Desktop Experience)" version.

Select the custom installation. Select the one partition shown, click new, then click apply, then hit ok.

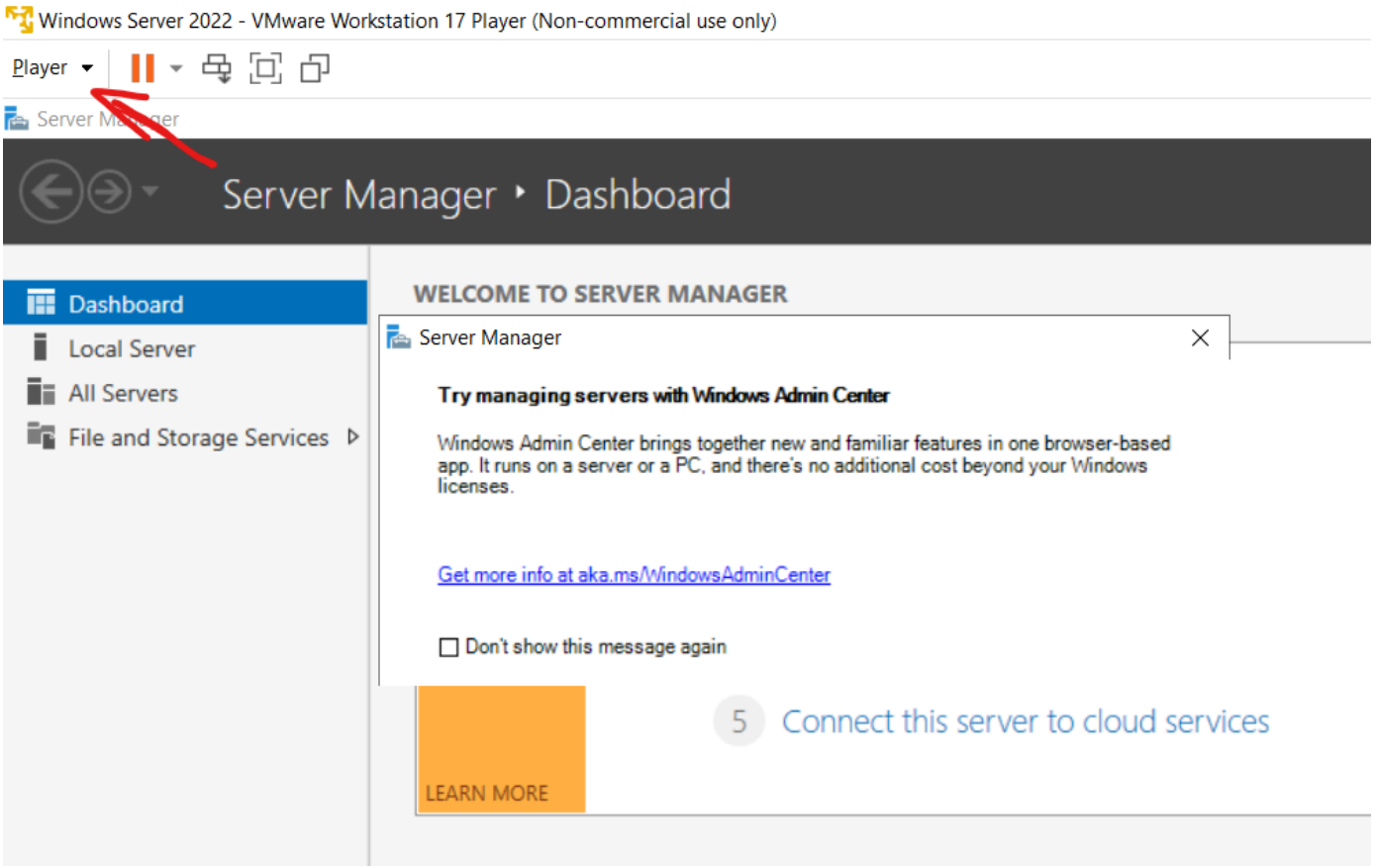
Click Next.

Let it install.

Then, we are going to create a password for the built-in Administrator account. We are going to use weak password : "P@$$w0rd!".

We can then log in to the administrator account, and install VMware tools, so we can make it bigger and see better.

To do that,



Then,

Manage > Install VMware Tools.

If you cannot select the option (if it is faded out), then it is very like there is a floppy disk installed with the machine. Power the machine down to remove it. It wont make you reinstall anything at this point if

you power off.

Then, on the virtual machine navigate to the "D:" drive, and run "setup64.exe". That will installs the tools. You can select "Complete" instead of "Typical". Restart is not always required for tools to work.

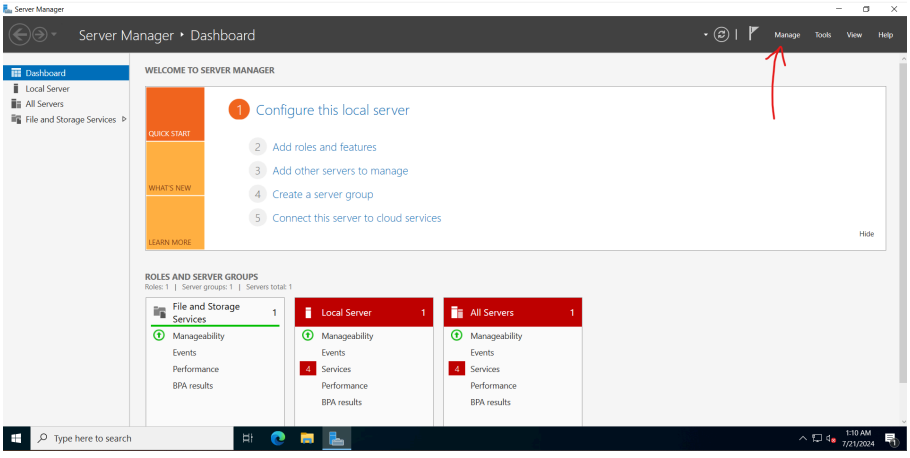
Now, we are going to be renaming this computer. The default name is something very weird. The idea here is that we need to know this is one of our machines in the network. We can create a specific name convention. Lets use MACHINE_NAME-MACHINE_ROLE. This example in particular is not a good idea because it discloses the machine role in its name, and that just make it easier for an attacker. But, it is a good idea to use a name convention that is understood and controlled by the Network Administrator. So, that is why we should change the name, and do not leave the default. Remember this is going to be the Domain Controller Personal Computer name in the network, ergo the name of the Domain Controller machine.

1- Just type "Rename" or "Name" in the Windows search bar > Rename PC.

We will need to restart, so the name sinks to the system. Then, we can proceed to the next step.

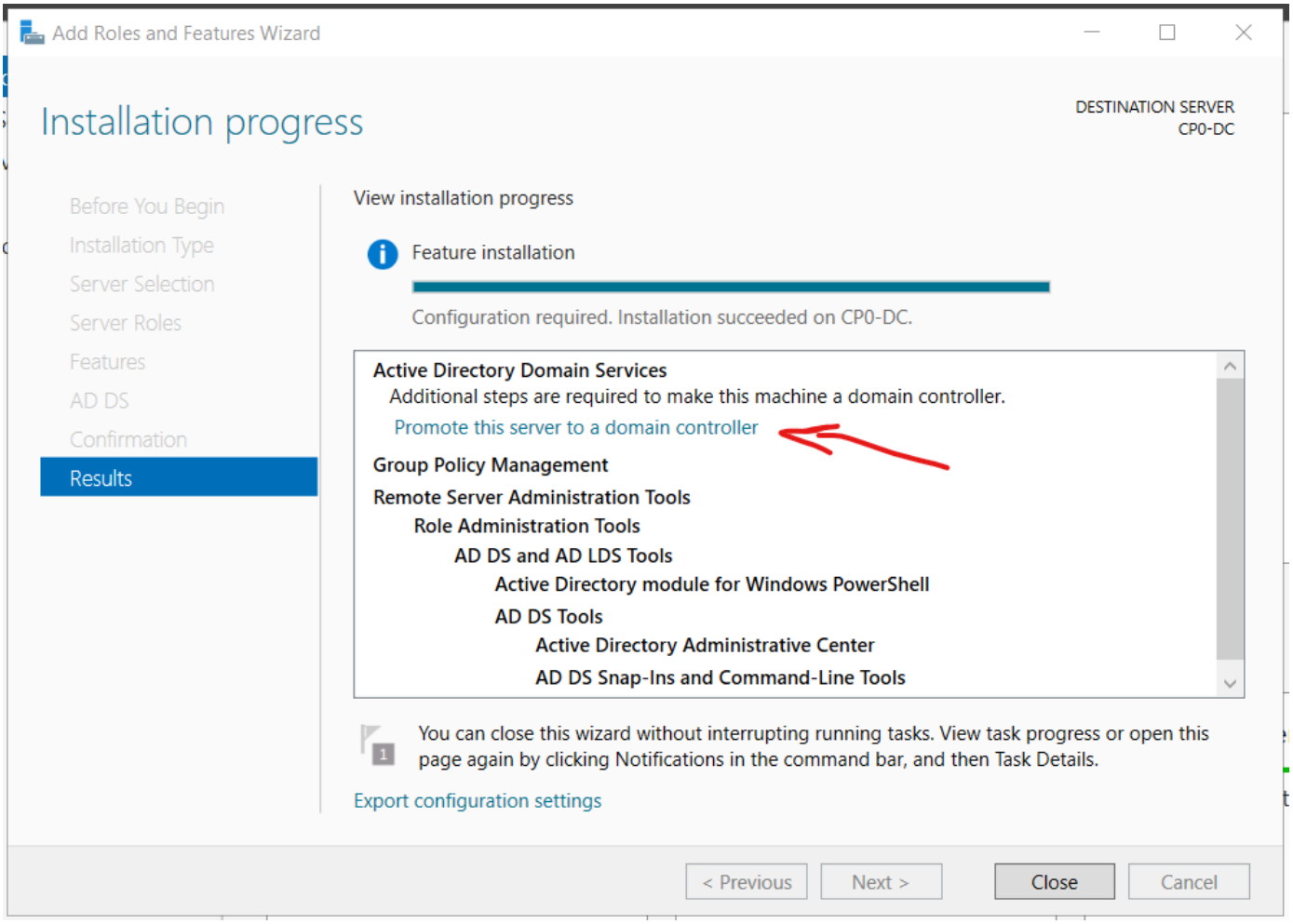
Now, we are going to make this the Domain Controller. For that, we need to add the role and features of a Domain Controller in this machine. Luck enough, the "Server Manager" application allows us to do that fairly easy.

2- Make it Domain Controller > Go to "Manage" on Server Manager > "Add Roles and Features".



The wizard will pop up. Click next > Select "Role-Base or feature-based installation" > Leave Server Selection as default > On Server Roles, we want to add "Active Directory Domain Service" > Add Features > Click Next until the Confirmation screen > On the Confirmation screen, select "Restart the destination server automatically if required." > Install.

Before doing anything else, we want to "Promote this server to a domain controller."

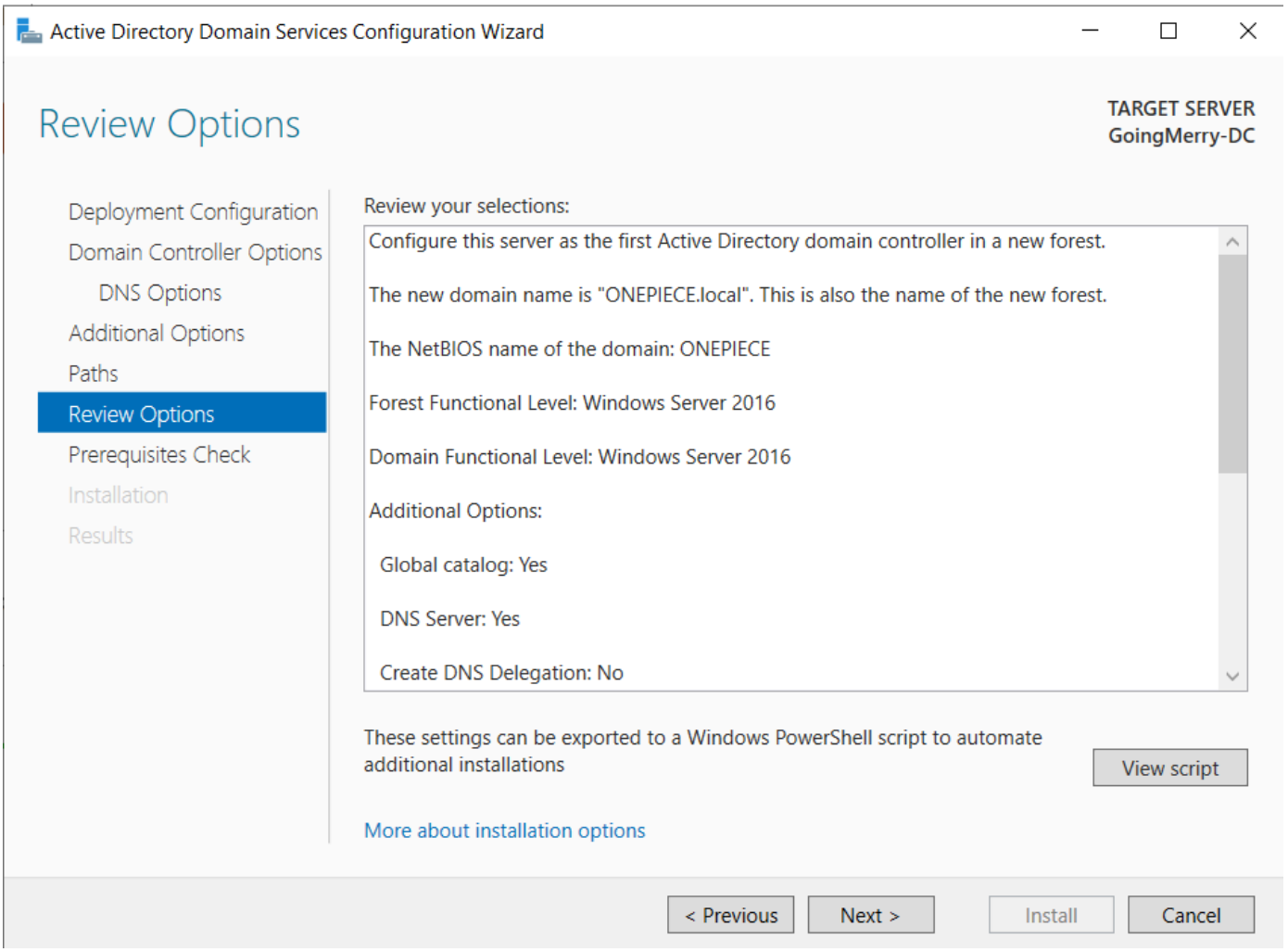


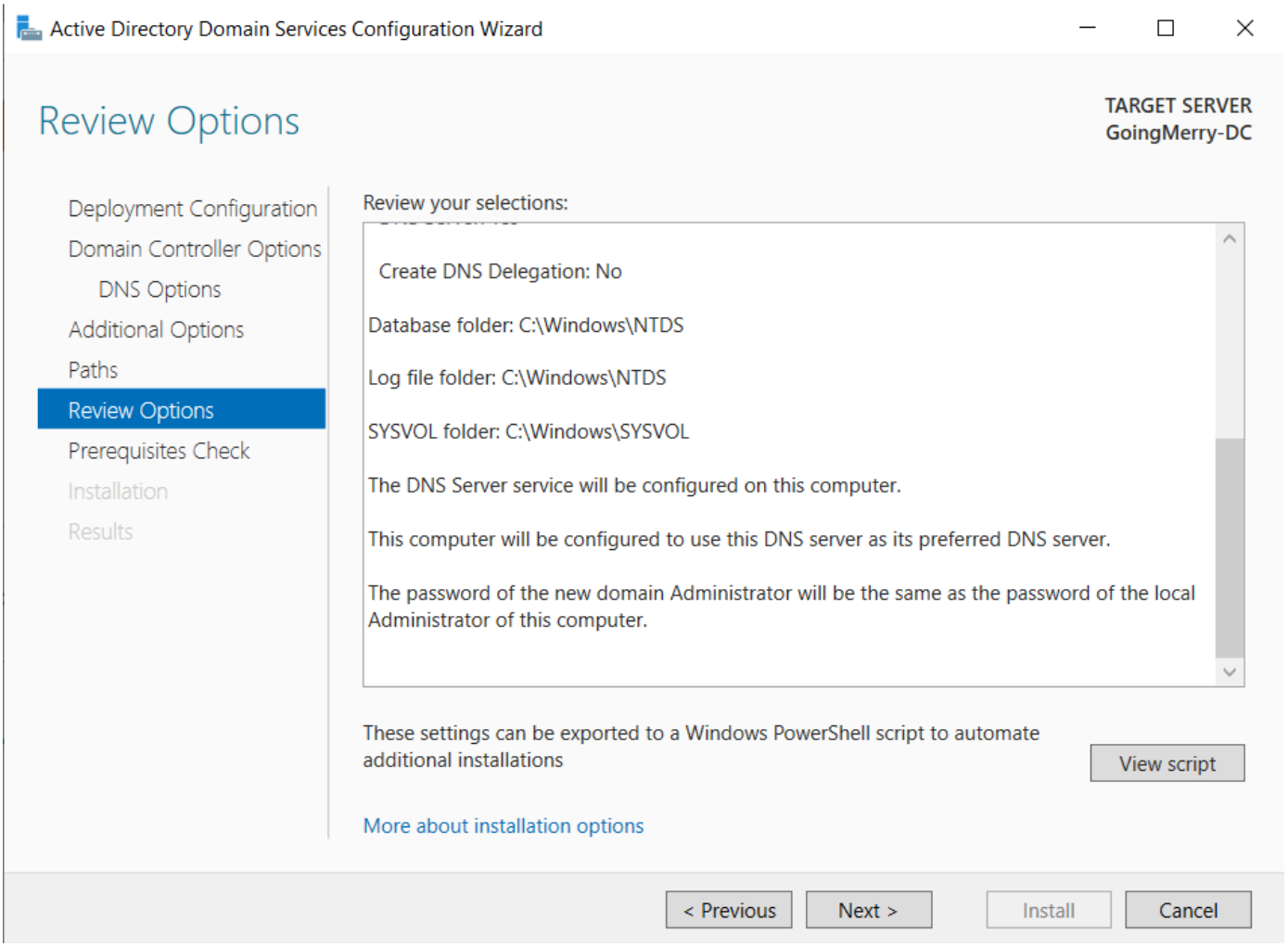
So, do not click close.

At this point there is no existing domain we can add our machine to. We cannot add a new domain to an existing forest (there is no forest). So, we are going to "Add a new forest".

We will "add new forest", then we can join our Domain to it. Name convention here is going to be "ANY_NAME.local" > Set password to be the same as Administrator password > Click Next > Next >

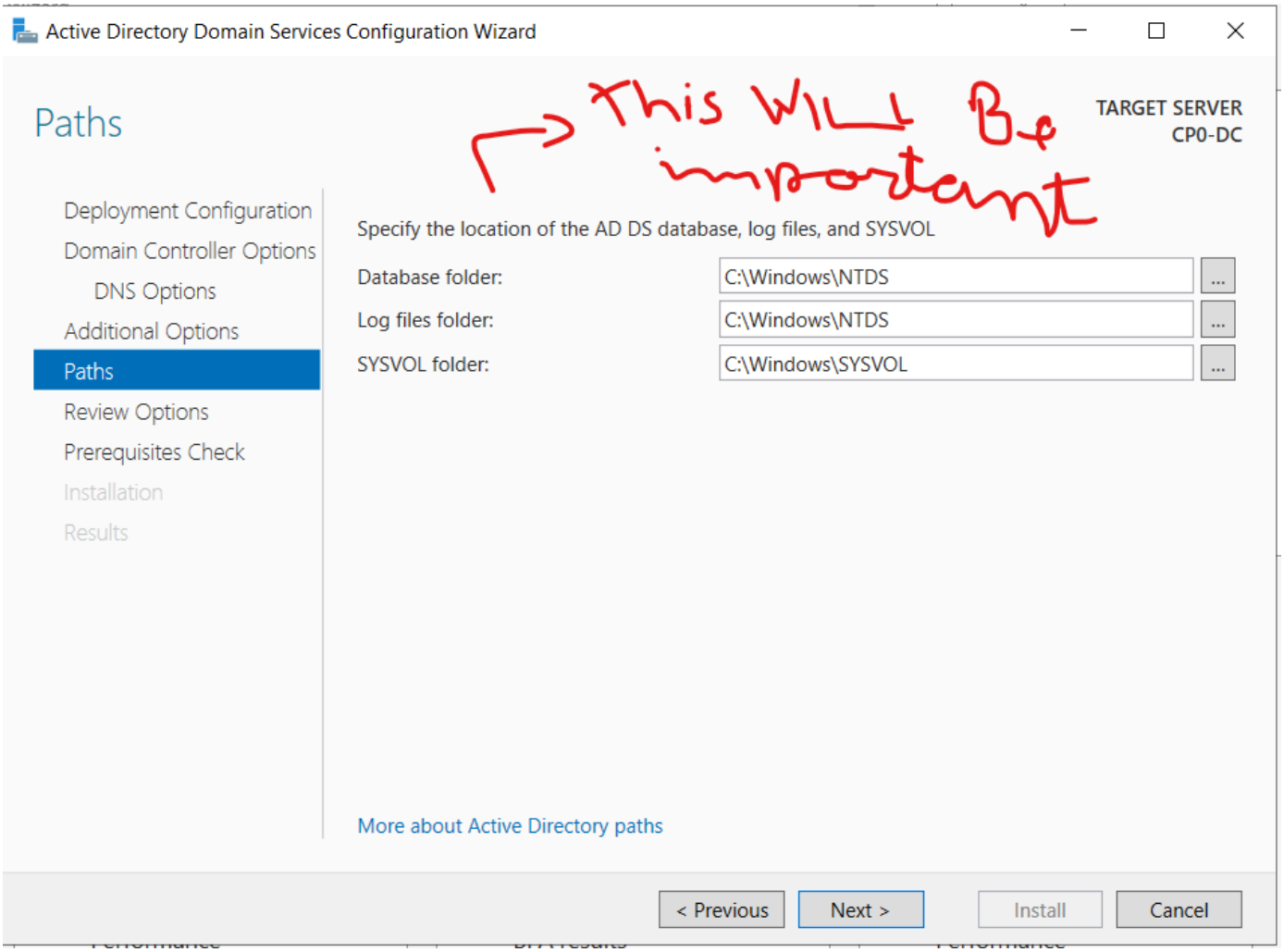
Next > On the "Review Options" screen, we can double check all the information.





We can see it is possible to export these settings to a PowerShell script. Not sure why Microsoft gives us that option.

This will come up later on in this course.



Keep clicking next.

After prerequisite check, go ahead and install.

We are going to getting a warning that we are being signed out. Go ahead and click close.

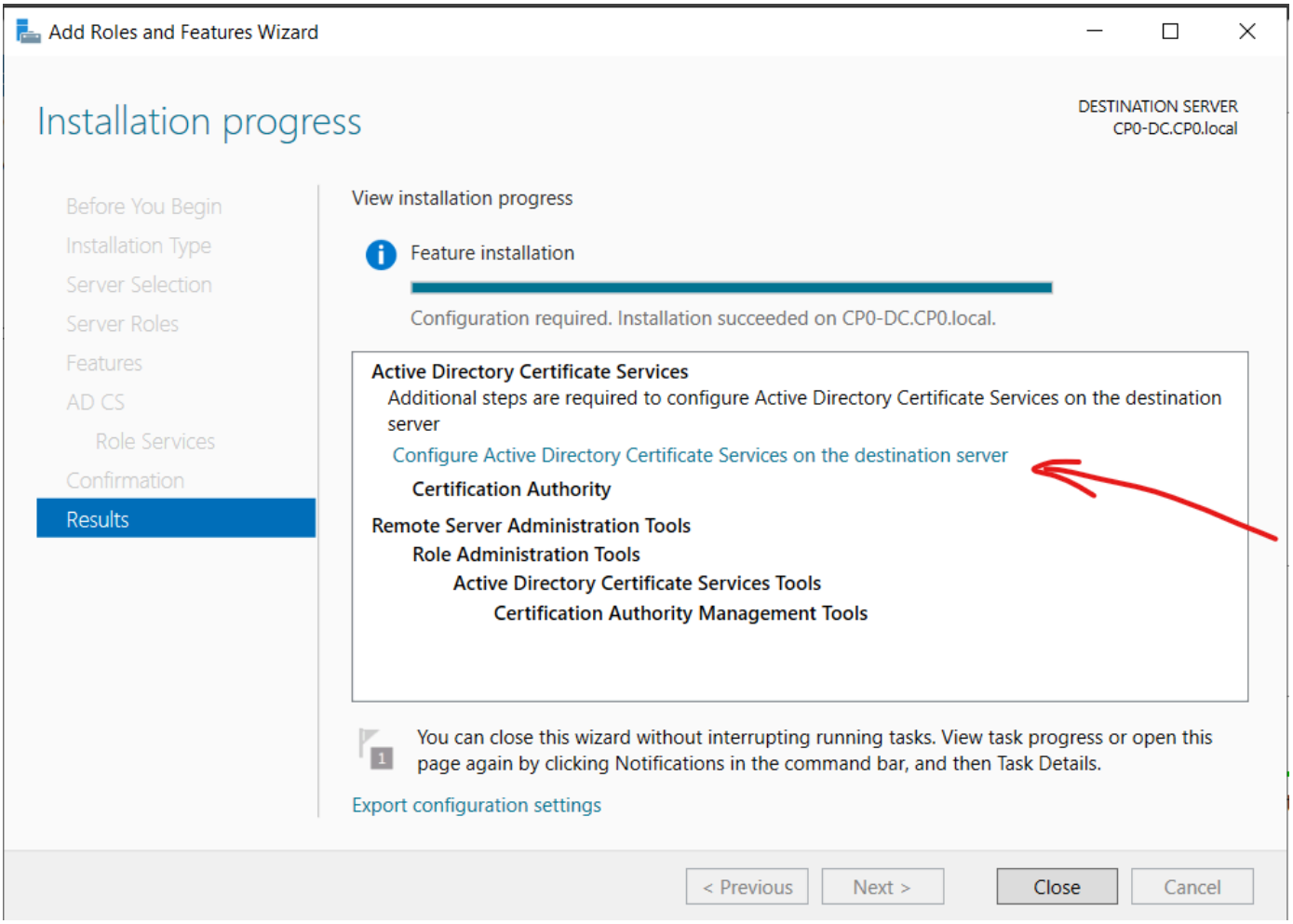
It is going to reboot.

Log in with the built-in Administrator password.

Last step is to set up "Certificates Services".

Open "Server Manager" > Go to "Manage" > "Add Roles and Features" > click next until Server Roles screen > On Server Roles, select "Active Directory Certificate Services" > Add feature > Next... > On the Confirmation screen, select "Restart the destination...." > Install.

Do not close the screen. Select "Configure Active Directory Certificate...."



On "Credentials" click Next > Make sure "Certification Authority" is selected >Enterprise CA > Root CA > Select "Create a new private key" > SHA256 > Default > Default > "Valid Period", Change it to 99 years > Configure.

Reboot it, and we are done.

9.1 - Setting Up the User Machines

2 - Setting Up the User Machines (Windows Client)

Install the ".iso" file for the Windows Client. We are going to select "Windows 10 Enterprise" for this install instead of the "Windows 10 Education". If you wanna give a particular name for the virtual machine, this is the name the machine will appear in VMware Workstation.

We are going to do a Custom Install. Select the drive, then click new. Same as for the Windows Server.

Don't forget to remove the floppy disks after installation.

We are going to get to a screen that asks us if we want to sign in a Microsoft account. Here, we want "Domain join instead". This allows us to join a local account to the domain instead of a Microsoft online account.

Client_1 is the name of the virtual machine. "frank" is the username(I believe to be the local admin as for this machine), and pwd is "Password1". The PC name is "THEROBOT".

Client_2 is the name of the virtual machine. "nami" is the username(I believe to be the local admin for this machine), and pwd is "Password1". The PC name is "THENAVIGATOR".

Then, lets install VMware tools. Do a "Complete" install.

Search "View PC Name" > Change pc name > rename it to whatever you want (I changed mine to THEROBOT and THENAVIGATOR to match).

Here, it is important to know the difference between the virtual machine name for VMware, the account name for each client, the PC name for each machine. The virtual machine name is not going to matter. We are just going to see those to boot from VMware workstation.

9.2 - Setting Up Users, Groups, and Policies

3 - Setting Up Users, Groups, and Policies.

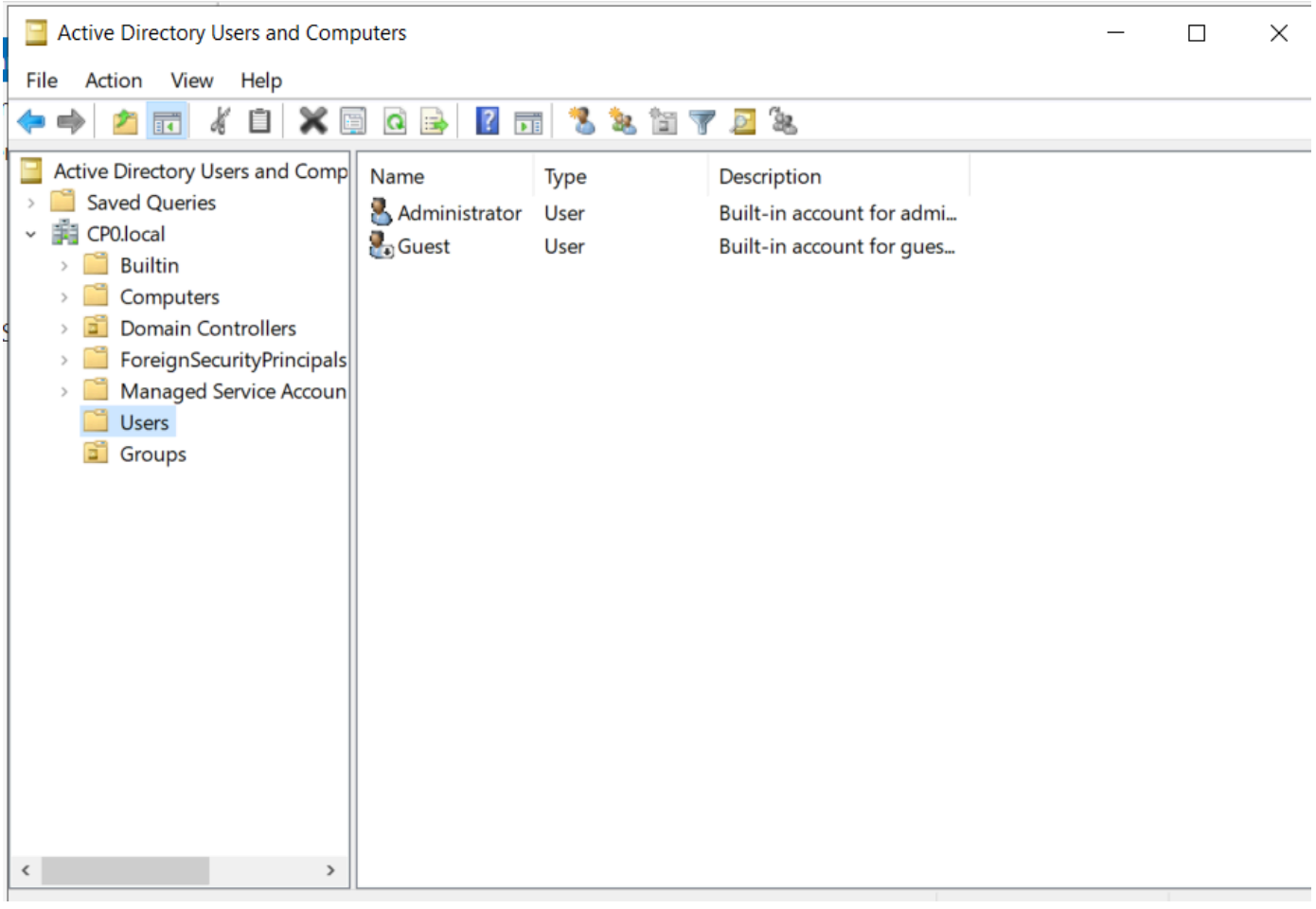
Here, we are going to use the DC. Which is the Windows Server.

Server Manager > Tools > Active Directory Users and Computers.

It stores all users and computers. OUs (Organizational Units for the Active Directory).

To make it more organized, we are going to separate the users from the groups. For that purpose, we are going to create a new organizational unit to move the groups to that "folder"(which is actually an OU). So, open the local domain, right click it > New > Organizational Unit > We are going to name it "Groups".

Now, go to the "Users" OU ("folder"), and move all the groups to the new OU. We should have left only the Administrator, and Guest account left.



We are going to create a new Administrator account.

Lets just copy the Built-in Administrator.

Right-click it > Copy.

That is a shortcut to copy all the privileges of the Administrator account.

To check Admin privileges, right-click admin built-in account > Member Of > And you should be able to see the Groups the account is associated.

This is going to be the Domain Administrator:

Name: Usopp

Last: Sogeking

User Logon Name: USogeking@ONEPIECE.local

(Pre - Windows 2000): ONEPIECE/USogeking

Password : Password12345!

Select the "Password never expires" box (which is not a good idea in a real live environment).

Now, we are going to do another big no-no, which is create a Service Account that is a Domain Administrator.

Services account are used to run a service.

Copy the built-in Admin again.

name : SQL ; last: : Service

User Logon Name : SQLService@ONEPIECE.local

Password: MYpassword123#

Select the "Password never expires" box (which is not a good idea in a real live environment).

Then, we are going to right-click the new account > properties > in the Description field we are going to put the password for the account, which is another big no-no.

Next, we are going to create 2 regular users. Regular meaning low level users.

Right-click "Users" OU > New > Users.

Here, we are going to create the user accounts in the Active Directory. So far, the accounts created were in the local computer, but now they are going to be created in the Active Directory. Meaning, all computer joined to the domain are going to be available for those users to login. Just like in a University where you can login to many different computers with one single credential.

User 1 : Luffy Monkey, LMonkey@ONEPIECE.local, Password1 .

Select the "Password never expires" box (which is not a good idea in a real live environment).

User 2 : Zoro Roronoa, ZRoronoa@ONEPIECE.local, Password2 .

Select the "Password never expires" box (which is not a good idea in a real live environment).

Next thing, we are going to create a file share.

Server Manager > File and Storage Service (on the left Menu Bar) > Shares > TASKS > New Share > Select "SMB Share - Quick" > Next > Share name: hackme > Accept Default for all the rest > Create.

Next, We are going to finish setting up Service Account.

Run CMD as Admin > Then, run "#setspn -a GoingMerry-DC/SQLService.ONEPIECE.local:60111 ONEPIECE\SQLService"

So, Domain Controller PC name (GoingMerry-DC), and then Domain name (ONEPIECE.local).

To make sure the system took the command and in fact updated object, we can run:

" #setspn -T ONEPIECE.local -Q */* "

```
C:\Users\Administrator>setspn -a GoingMerry-DC/SQLService.ONEPIECE.local ONEPIECE\SQLService
Checking domain DC=ONEPIECE,DC=local

Registering ServicePrincipalNames for CN=SQL Service,CN=Users,DC=ONEPIECE,DC=local
        GoingMerry-DC/SQLService.ONEPIECE.local
Updated object

C:\Users\Administrator>setspn -T ONEPIECE.local -Q */*
Checking domain DC=ONEPIECE,DC=local
CN=GOINGMERRY-DC,OU=Domain Controllers,DC=ONEPIECE,DC=local
        Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/GoingMerry-DC.ONEPIECE.local
        ldap/GoingMerry-DC.ONEPIECE.local/ForestDnsZones.ONEPIECE.local
        ldap/GoingMerry-DC.ONEPIECE.local/DomainDnsZones.ONEPIECE.local
        DNS/GoingMerry-DC.ONEPIECE.local
        GC/GoingMerry-DC.ONEPIECE.local/ONEPIECE.local
        RestrictedKrbHost/GoingMerry-DC.ONEPIECE.local
        RestrictedKrbHost/GOINGMERRY-DC
        RPC/4b263b8a-6a51-45f6-b6ad-ef58442d540e._msdcs.ONEPIECE.local
        HOST/GOINGMERRY-DC/ONEPIECE
        HOST/GoingMerry-DC.ONEPIECE.local/ONEPIECE
        HOST/GOINGMERRY-DC
        HOST/GoingMerry-DC.ONEPIECE.local
        HOST/GoingMerry-DC.ONEPIECE.local/ONEPIECE.local
        E3514235-4B06-11D1-AB04-00C04FC2DCD2/4b263b8a-6a51-45f6-b6ad-ef58442d540e/ONEPIECE.local
        ldap/GOINGMERRY-DC/ONEPIECE
        ldap/4b263b8a-6a51-45f6-b6ad-ef58442d540e._msdcs.ONEPIECE.local
        ldap/GoingMerry-DC.ONEPIECE.local/ONEPIECE
        ldap/GOINGMERRY-DC
        ldap/GoingMerry-DC.ONEPIECE.local
        ldap/GoingMerry-DC.ONEPIECE.local/ONEPIECE.local
CN=krbtgt,CN=Users,DC=ONEPIECE,DC=local
        kadmin/changepw
CN=SQL Service,CN=Users,DC=ONEPIECE,DC=local
        GoingMerry-DC/SQLService.ONEPIECE.local

Existing SPN found!

C:\Users\Administrator>
```

Now, we are going to set up Group Policy. For that we will need to open Group Policy Management. We can find it by searching it on the Windows search box.

Group Policy Management > Expand Forest > Expand Domains > Right-Click "ONEPIECE.local" > "Create GPO in this Domain, and ...." > We are going to name it "Disable Windows Defender" > Disable Windows Defender.

This will create a GPO (Group Policy Object?) for the whole domain. It is possible to create GPOs for specific users, groups, and/or computers. But, this wont be the case here.

The new Policy should pop up under the ONEPIECE.local > Right-Click it > Edit > Expand "Policies" under "Computer Configuration" > Expand "Administrative Templates" > "Windows Components" > Select "Microsoft Defender Antivirus" > Right-click or Double-Click "Turn Off Microsoft Defender Antivirus" > Edit > Enable > Apply > Save.

Go to Group Policy Management > Right-Click Policy just created > Select "Enforced".

What will happen is any time a user or computer joins the domain, it is going to get this policy. Or if the user or computer is already domain joined, then the policy is going to be enforced as soon as it updates and sink to the systems.

Lastly,

Go to windows search bar > Type "ncpa.cpl" > Right-Click Network > Double Click "Internet Protocol Version 4 ..." > We are going to use a static Ip address. Just set to the same one found on "#ipconfig" command in CMD (IP ADDRESS, Gateway, Subnet Mask) > Do not give an alternate DNS Server, and leave Preferred DNS Server to be 127.0.0.1 (localhost).

9.3 - Joining Our Machines to the Domain

4 - Joining Our Machines to the Domain

We want to be able to utilize a DNS Server. We want to point it directly to our DNS Server which is going to be our Domain Controller machine IP Address

The file to open Network Adapters is "ncpa.cpl".

Go to properties > Double-Click IPv4 > set "Preferred DNS server" to the Domain Controller IP Address.

Leave "Obtain an IP address automatically" selected.

Then, to join to the domain, go to the search bar > Type "domain" > Open "Access Work or School" > Click the big "Connect" plus sign > Click "Join this device to a local Active Directory Domain" > ONEPIECE.local > Username: administrator, Password: "P@$$w0rd!" (credentials for local admin in Domain Controller) > add administrator user > restart now.

We can check under the "Computers" tab in the Active Directory Users and Computers the just added computers over in the DC.

Login as ONEPIECE/Administrator again. It is going to load. > Go to the search bar > type "users" > Open " Edit Local Users and Groups" > Users > Set Password for built-in administrator account ("Password1!") > Double-click Administrator > Uncheck "Account is disable" > Ok. We are enabling the built-in Administrator account here. Best practices says otherwise. (For both Client_1 and Client_2, password should be the same).

Go to Groups > Double-click administrators > We can see the Administrators on this computer. > We want to add one more user here. Keep in mind this is the Administrator group, so the user we add here is also going to be an Administrator in this machine. We want to add one of the users created in the Active Directory by the Domain Controller. It could be either LMonkey@ONEPIECE.local or ZRoronoa@ONEPIECE.local .

For Nami, which is Client_2, THENAVIGATOR, I will join LMonkey@ONEPIECE.local to the Administrators Group.

For Frank, which is Client_1, THEROBOT, I will join ZRoronoa@ONEPIECE.local and LMonkey@ONEPIECE.local to the Administrators Group.

Turn on network discovery and file sharing. Open Windows Explorer > Click Network > If it is not on yet, then go ahead and click the yellow tab at the top > Turn on network discovery and file sharing.

You should see the DC. If you open it, you should see the "hackme" file share folder.

Log out. Then, login again as a local administrator.

For Client_2, it would be Nami. If it says "Sign in to :ONEPIECE", then you will need to use the username ".\Nami". That is because Nami is not part of the ONEPIECE.local Domain, but she is the local administrator for the account. I think it is because this was the first account to be set up by the system, so it is automatically an admin account?. Not sure. In any case, we are login in locally, and not in the domain.

Open File Explore > This PC > Computer (On the top menu) > Select Drive: Z: > Folder: \\GoingMerry-DC\hackme > Select both boxes (Reconnect at sign-in, and Connect using....) > Finish > administrator:P@$$w0rd! .

Now we have that as a shared drive in this machine.

Now, we are all set up!