2MCSA

Gabriel Verschatse, Dannequin Thomas

October 2025

Abstract

First of all, let us recap the goal of this document. The purpose of this project is to implement a solution for an enterprise of pasta (*Pasta Scaduta*) to manage and track their activity with the deployment of **Active Directory** in the different site managed by the enterprise. Hence, it has a lot of different steps to administrate rights and networks.

In order to do so, we will first define a *network infrastructure* for the enterprise and then show the different key steps to achieve this, as well as the installation process. For more precision, please consider the table of contents below.

Figure 1: Windows Server, specialized Windows OS

Contents

1 Network Infrastructure

Before going further in the installation process, we need to take a look to the overall infrastructure of a network.

1.1 Enterprise network

Our enterprise is composed of 3 sites. The first one being in France, another on in Poland and finally a site in China. Each of them have particulars features, here is how we decide the organization :

- France is considered as *the main site* along with Poland. It contain an Active Directory with other resources such as shared files (DFS) and the webpage of the company using a Windows IIS.
- Poland being in the same Forest as France, it will also contain an Active Directory that replicate the one established in France. It also have to process a IIS webserver.
- Finally, China is the last site hosting a **R**ead **O**nly **D**omain **C**ontroller, that basically act as a backup.

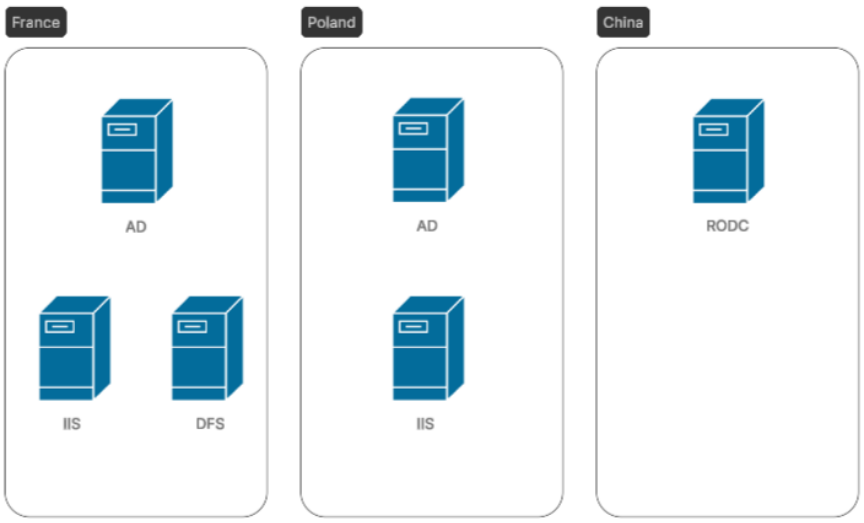

Figure 2: Illustration of the 3 sites with some services installed

Additionally, another forest need to be join to the domain. Because another society decided to join the us, we need to add a trust relationship between our 2 forests.

1.2 Virtual network

In order to organize our IT configuration, we will first take a look at our network schematic that contain every information we need, especially **IP address**

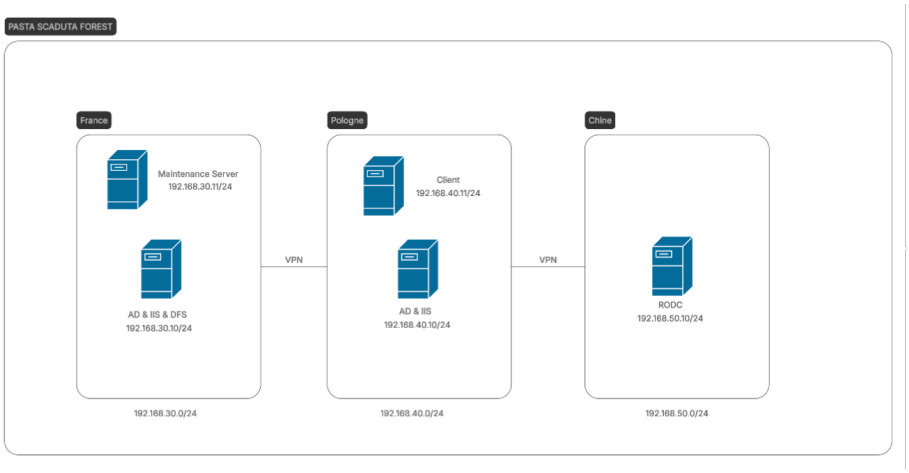

Figure 3: Our network configuration, including IP address and services

It's important to note that services are not split across multiple server in our case. Due to resource limitation, we are going to regroup services.

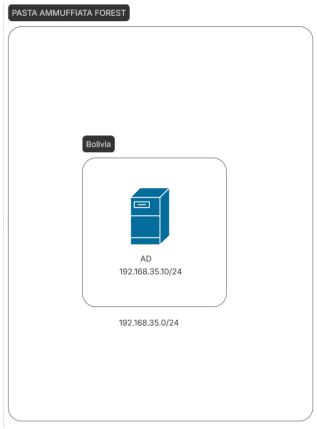

Figure 4: Network configuration of the other forest

2 Devices setup

Before going further, we need to install a virtual environment and the associated machines. For our example, we are going to use VMware as a way to create virtual devices.

As mentioned above, we are using a lot of different machine, mainly under *Windows Server 2022* to reproduce server behavior.

Before processing the virtual machine creation, make sure to acquires the *.iso* files on the Microsoft Official webpage

2.1 VM installation

Open VMware and press *Ctrl+N*, this allow you to create a new virtual machine. For the most part you can just press next, so we will only focus on important steps of this installation.

Once you have started the VM creation you will encounter a screen that allow you to choose the specific .iso file you want to use *(Check below, figure 5)*.

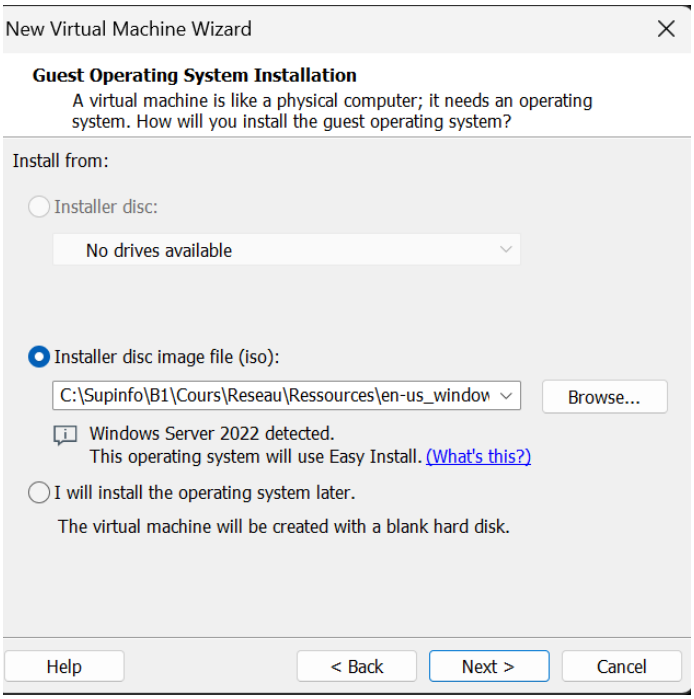

Figure 5: *.iso* file selection

Select the file you need but keep in mind that we will need **1 Windows 10/11 and 5 Windows Server 2022**. After doing so, the installation is

pretty straight forward and keep pressing next until the sum up windows appear (Check *figure 8*). From here, you can either finish or adjust the memory allocated to the VM based on your resources (If you can, allow 4GB to server that contain alot of different services).

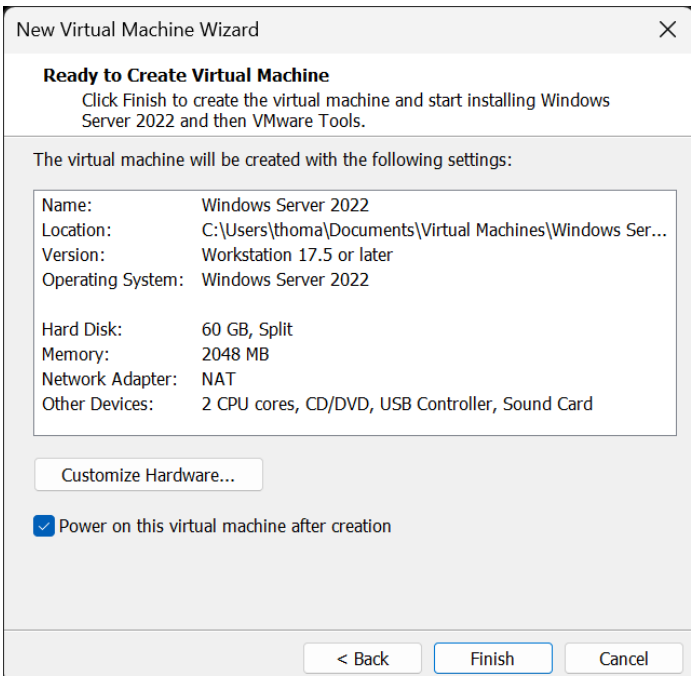

Figure 6: VM recap

From here, it's possible to **customize network** using VMware's network. It's a key point for all our networks because we need different host-only network for each site. If you go in *Customize Hardware*, you can access this panel.

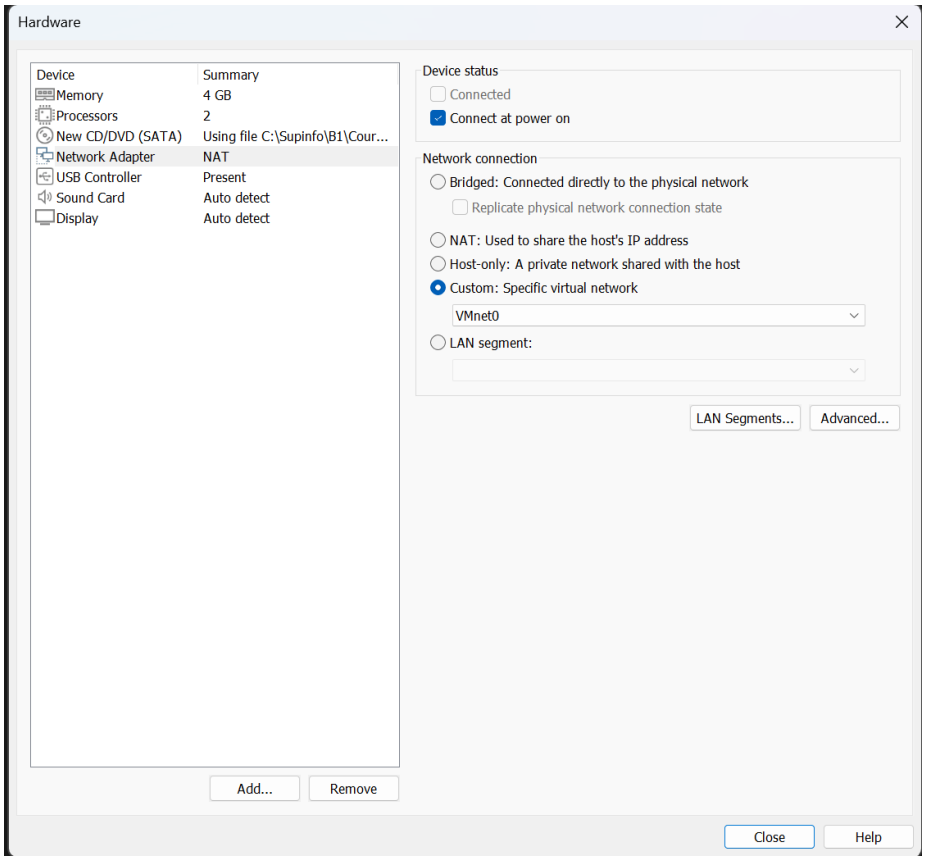

Figure 7: Hardware customization

From here, you can add another **network interface** (aka NIC) but also change the *Network Connection*. It's now important to configure each machine with a proper Network Adapter. Every computer in the **same site** need to have the **same network**. Note that another NIC will be needed for AD servers as they will act as gateway to other networks. This special network is going to represent "*Internet*".

It's required to create custom network for our configuration. You can validate the VM creation and going back later to change the Network Adapter. To create the custom network, you need to go in *Edit* < *Virtual Network Editor* < *Change Settings*

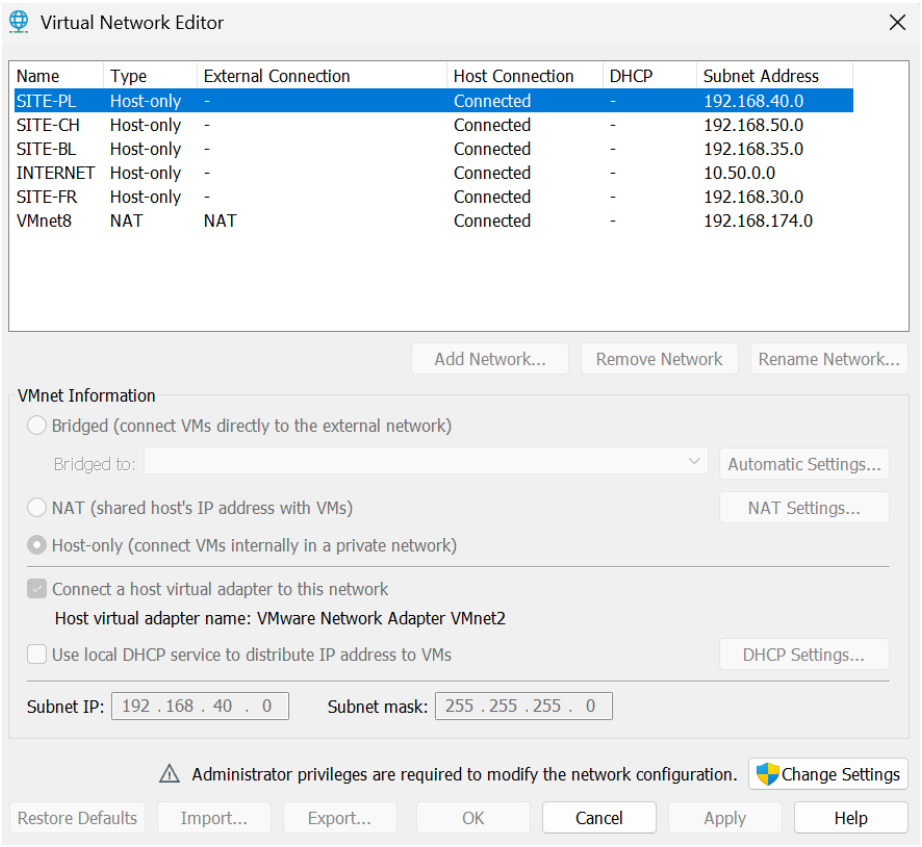

Figure 8: Virtual Network Editor

Using this interface, you can then "*Add Network*" and customize IP addresses for the subnet using the one given in the schematic of the previous part. It's important to then edit Network Adapter and configure with the proper VMware subnet. It's one of the requirement to allow server on the same site to communicate (and cross-site). We also recommend to rename network to identify easily each of them.

3 Network configuration

3.1 Static IPV4 assignement

In the section above, we have defined our network infrastructure. Let's start by adjusting the **IP addresses of each device**. But how to change the IP configuration of my machine ?

In order to change our IP adress, we need to go to *Control Panel <Network and Internet <Network and Sharing Center*. At this point you should see your Network Interfaces, we are looking for Ethernet0 (There can also stand Ethernet1, in fact it correspond to a previously configured Network Adapter).

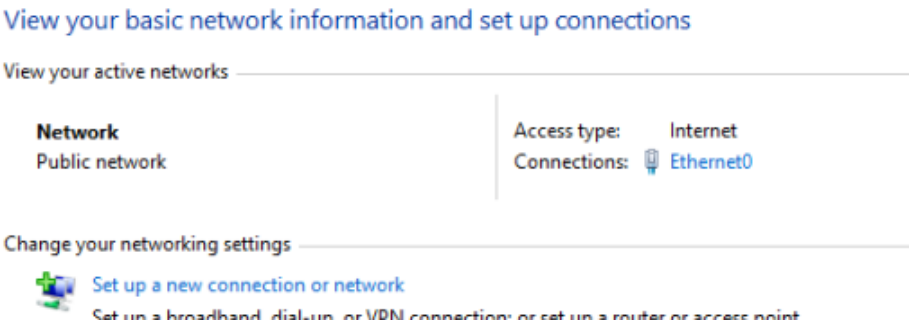

Figure 9: Ethernet0 default Interface

Select the Ethernet0 and *Properties <Internet Protocol Version 4 (TCP/IPv4)*. Now you can Edit the IP as mentioned on the Diagram earlier. As for the **Default Gateway**, you need to check the concerned network's default gateway. Just go in *Edit <Virtual Network Editor <Change Settings* and check for the network configurations.

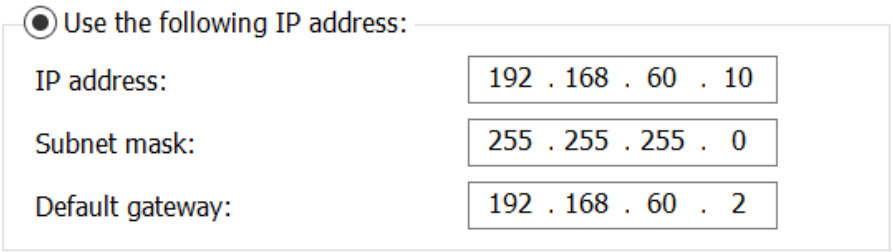

Figure 10: IP configuration of a machine

3.2 DNS configuration

In the same interface is mentioned the DNS configuration. You will just need to give the IP address of a server that act as DNS (The first time you are going to try joining a domain, be sure to give the proper DNS's IP !). You may also notice that there is no internet access which is a normal repercussion since we are using host-only network (established in VMWare).

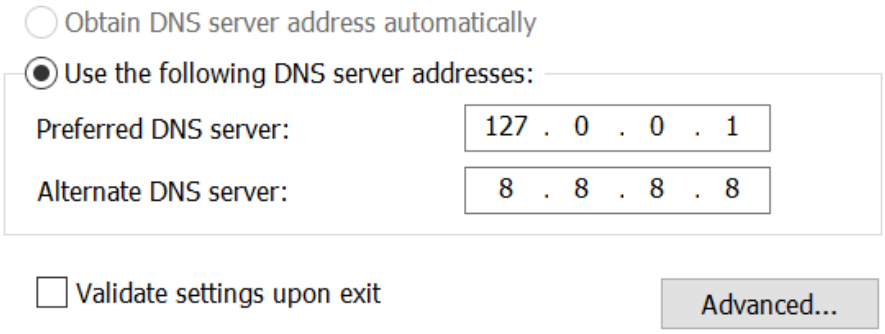

Figure 11: DNS configuration of the DNS server

On your DNS server, you can also configure the Forward Lookup Zones (which make the **translation of an URL to the requested IP address**). Go in the DNS menu, and on the left panel appear your domain. You can then create new association using right click Host A and register the IP and URL. (You need a server with the DNS role to achieve this, in our case AD server). We will comeback on this later on when dealing with IIS.

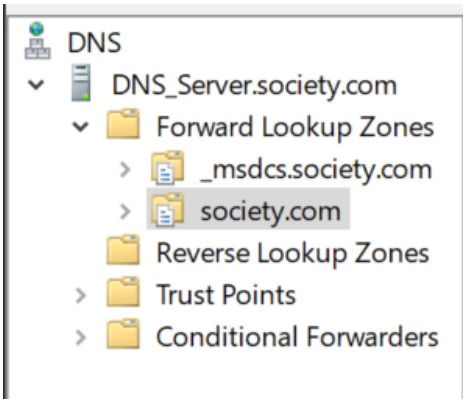

Figure 12: DNS Forward Lookup Zones

4 Active Directory Domain Services (ADDS)

Now that all required network configurations are setup, let's go through the creation of an **Active Directory**. Firstly, go on the device you consider as French server (We highly recommend doing **crystal clear configuration** beforehand by renaming each machine), in our case **AD-FR**.

Open Server Manager and click *Manage* at the top-right corner. Select *Add Roles and Features* and proceed the installation. You can go ahead for the most part but make sure to select the ADDS role when possible (Check *figure 13*). Note that restarting the VM might be needed. (You can already repeat this process on the AD-PL / AD-CH servers, for respectively Poland & China AD)

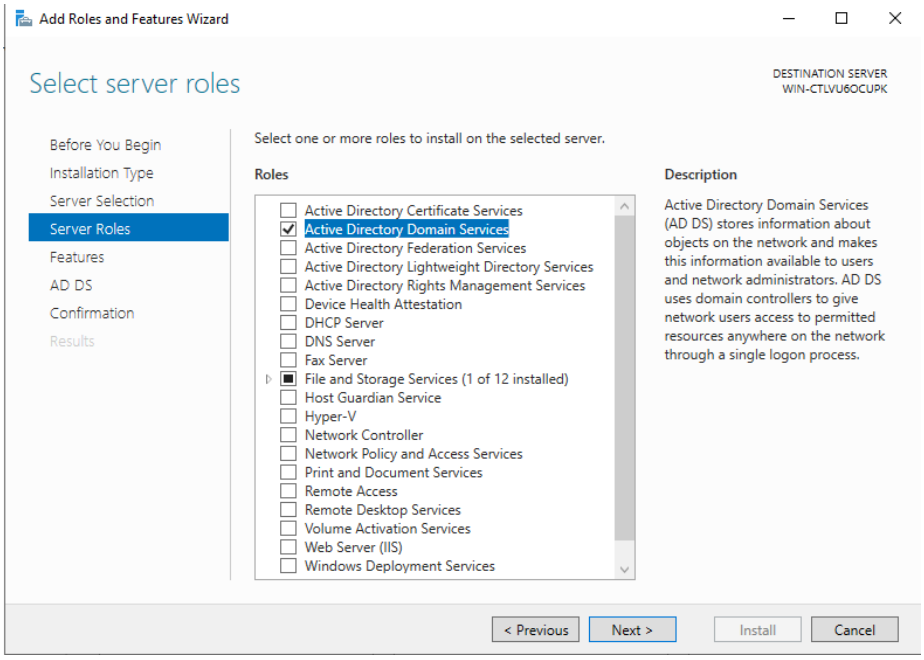

Figure 13: ADDS Role selection

4.1 Domain creation

Once the Role installed, we need to promote the current server as a Domain Controller. A yellow flag should already be displayed to indicate this.

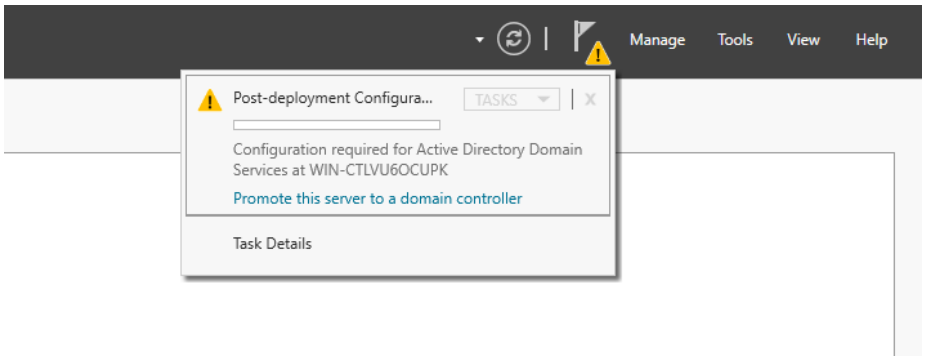

Figure 14: Promoting to Domain Controller

Click *Promote this server to a domain controller* <*Add a new forest*, then choose a domain name. For our example, we will use *scaduta.com*.

The first interface also contain options that are needed for 2^{nd} and 3^{rd} Active Directory. Once France will be setup the same process can be repeated from other AD but instead of creating another forest, we want to join an existing one (For RODC, there is an radio option right after this)

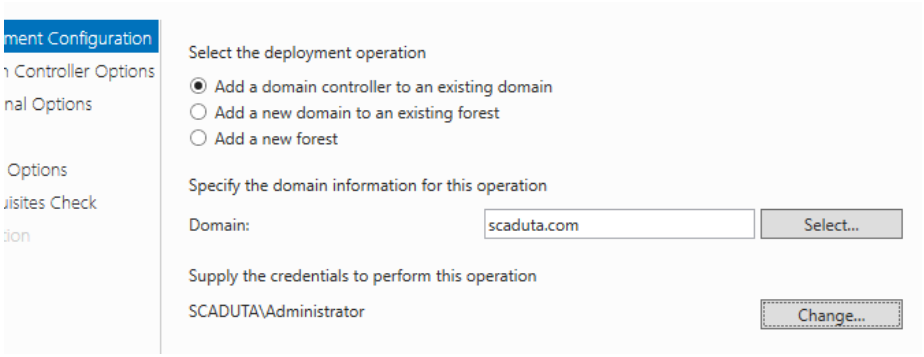

Figure 15: Joining an existing forest

You can press next a few times since default configuration is what we are looking for (It allow you to change things such as the storage path which can be interresting to store elsewhere, but virtualization sometimes cause issues). At the end press install, you might need to set a local administrator password to your device before doing so as it will become the ADDS administrator.

4.2 Join an existing domain

We have now configured our Domain Controller, it's time to add some computers to it ! Go on the computer dedicated to employee and go to *Settings* <*System* <*About*, now you should see *Advanced system settings* on the right panel, click on it and a window should appear (*Figure 16*).

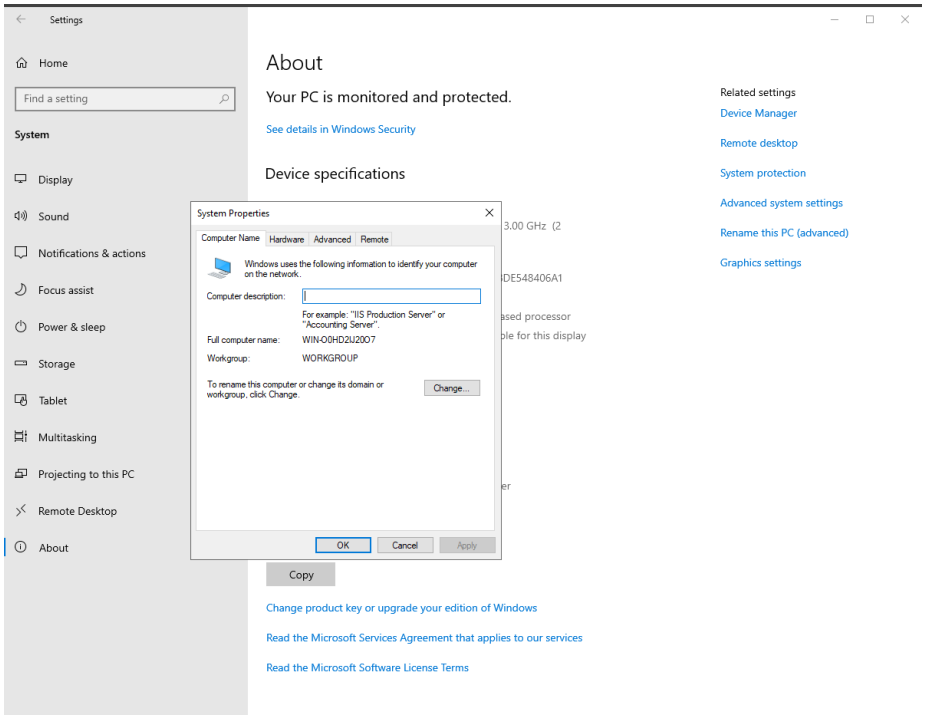

Figure 16: Promoting to Domain Controller

We now want to go to *Computer Name* and click Change, we can now select to join a domain. You will then need to precise a few parameters like the domain name and an Administrator confirmation. (Be aware that since the client is in Poland, you need to set his DNS toward the Poland's AD that has previously join the forest)

This process can be repeated if we need to join a device to our forest (beside Domain Controller)

4.3 Manage Users

Now that all of this is setup, we may want to add some users and/or groups for our freshly created domain. We can do so by going in the *Active Directory Users and Computers*. From here, we can see multiples directories and a lot of default User & Groups. We can now create User and Groups as we intend by doing a right click.

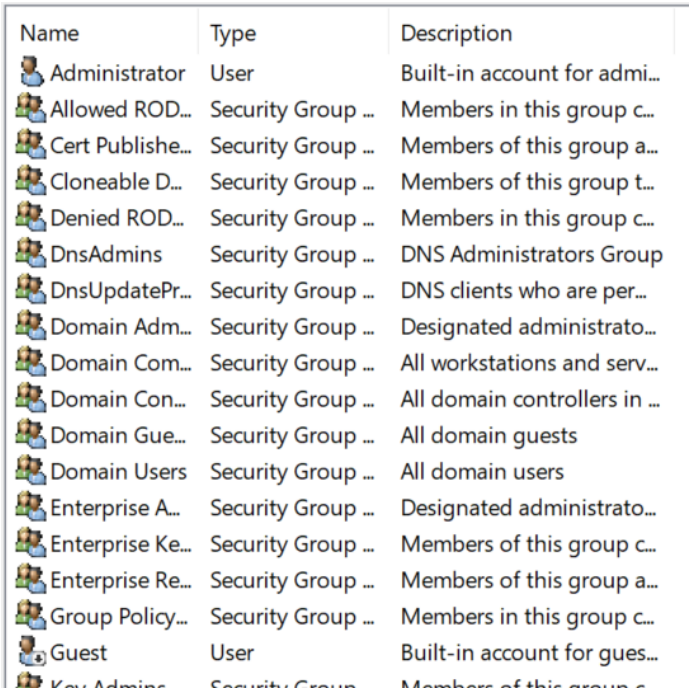

Figure 17: Default Users and Groups

Let's create some users and group to organize a realistic environment, we are going to create **O**rganizational **U**nit (act as a folder) for each group and create associated users.

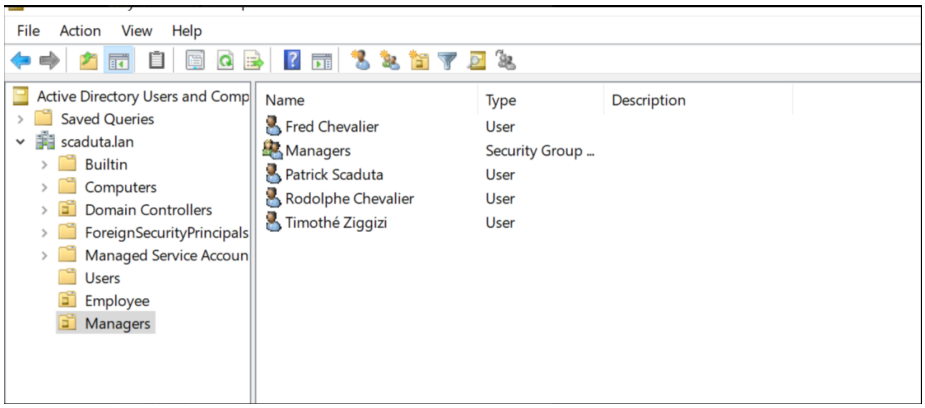

Figure 18: Example of Users and Groups organization

For instance, in our case we have created 2 separated **OU**, one for *Employee* and another one for *Managers*, each of those contain different Users and the corresponding Group (Note that you need to check the "*Member of*" property of each User and assign it to his corresponding group).

5 Active Directory Site and Replication

Now that we have configured our **3 main server** (AD-FR, AD-PL, RODC-CH), we need to organized them and clarify that each of them are on different site. Despite having different network configuration, Active Directory **does not recognize it by itself**. Let's see below how to organize sites !

5.1 Create different Sites

Firstly, go in the *Active Directory Sites and Services* menu. From this point you should see a *"Site"* Folder that contain another folder and more importantly **DefaultFirstSite** that is a default Site containing every device. You can now process the creation using *right-click* on the Site folder. We can now do a Site for France, Poland and China. After that, you can drag and drop each server to there associated site.

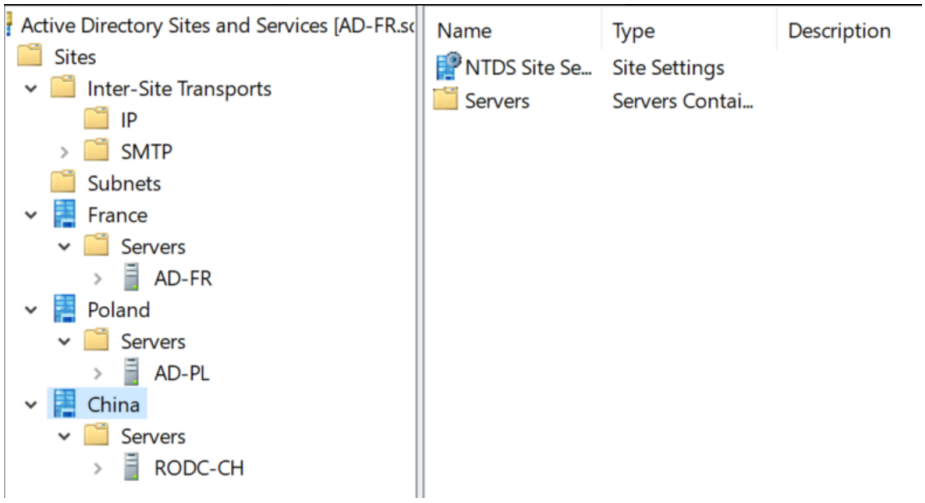

Figure 19: Site and associated server

5.2 Site configuration

Now that each Site are created, we need to add some configuration. Go in the *Subnets* folder and initiate the creation of a new subnet. From here, we can create 3 different subnets, each of them being associated to a site. You will just have to fill in with the network IP address using CIDR notation and select corresponding site.

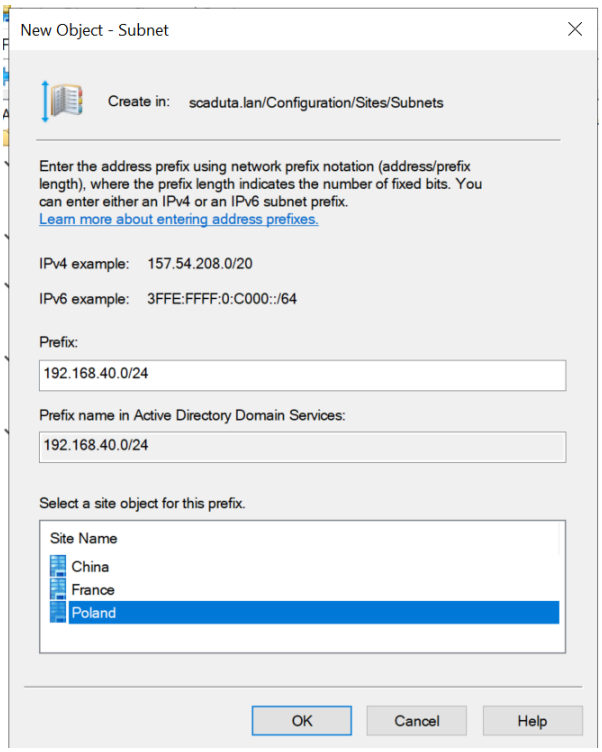

Figure 20: Site - Subnet association

Once all the subnet are configured, you should have something like this showing every site and their corresponding IP network.

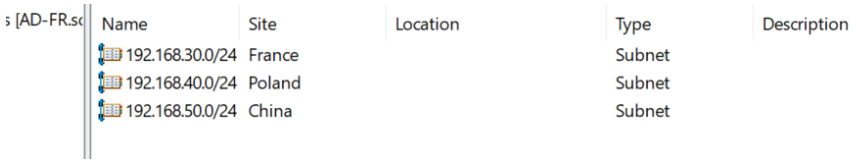

Figure 21: Site - Subnet association

Finally, we need to edit the cost of France-Poland relationship and customize replication schedule. In order to do so, go in the *Inter-Site Transports <IP* folder. You should see a default relation you've already given during setup. You can now rename it and configured as shown below.

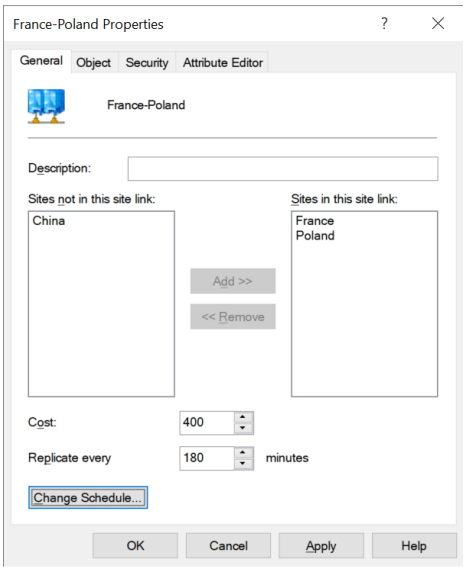

Figure 22: Site relationship settings

Finally, we can *Change Schedule* and set it to allow replication in low traffic hours.

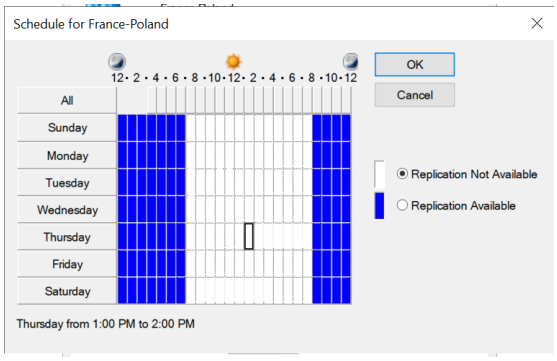

Figure 23: Replication schedule

6 DFS & Shares

Since we've already configure our main devices and their relationship, it's time to add some features that will facilitate files sharing across the company. In this part we will go throw installation of DFS services and the way it works.

6.1 Installation

As usual when installing new service, go in the *Manage <Add Roles and Features*, go throw and select **DFS namespace** and **DFS replication**. Those are going to respectively allow the creation of a namespace on our domain where we are going to be all of shared folder and the replication of those shared files across multiple server (Since we are going to have a inter-site replication between France and Poland). Install those on the two concerned server.

6.2 Manage Storage

Before going further, we need to think a bit. Storing data is a great idea but what if something happen on our storage disk ? Let's prevent that by adding dedicated storage that contain redundancy. First, let's add 2 more disk to our VM, going in the settings of both France and Poland. Add disk as shown below.

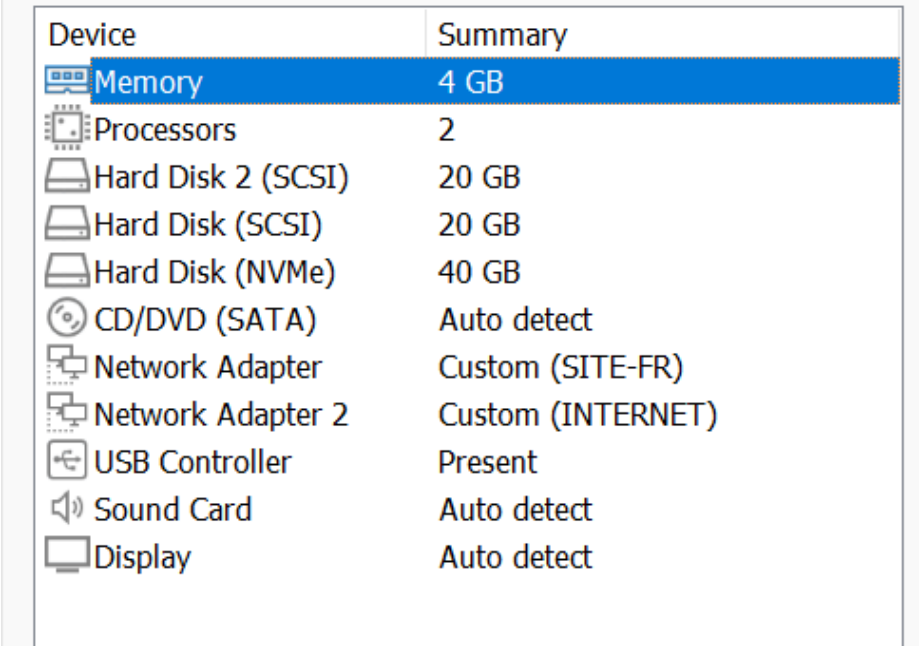

Figure 24: Add 2 disk to a Server

You may need to restart you machine after adding disk. Anyway, it's now

time to configure a **RAID**. Go in *the disk management* menu and set online both disk using right-click. You can then create a new mirrored volume using those 2 freshly installed disk. Go through installation wizard and select a distinct **Drive letter**, it will be the place where we store our shared files (This process can be done on both server). Note that mirrored RAID simply use 1 of the 2 disk to replicate data and improve safety of the installation (You can see that *S:* is capable of storing 20GB despite having 2 disk of 20GB each).

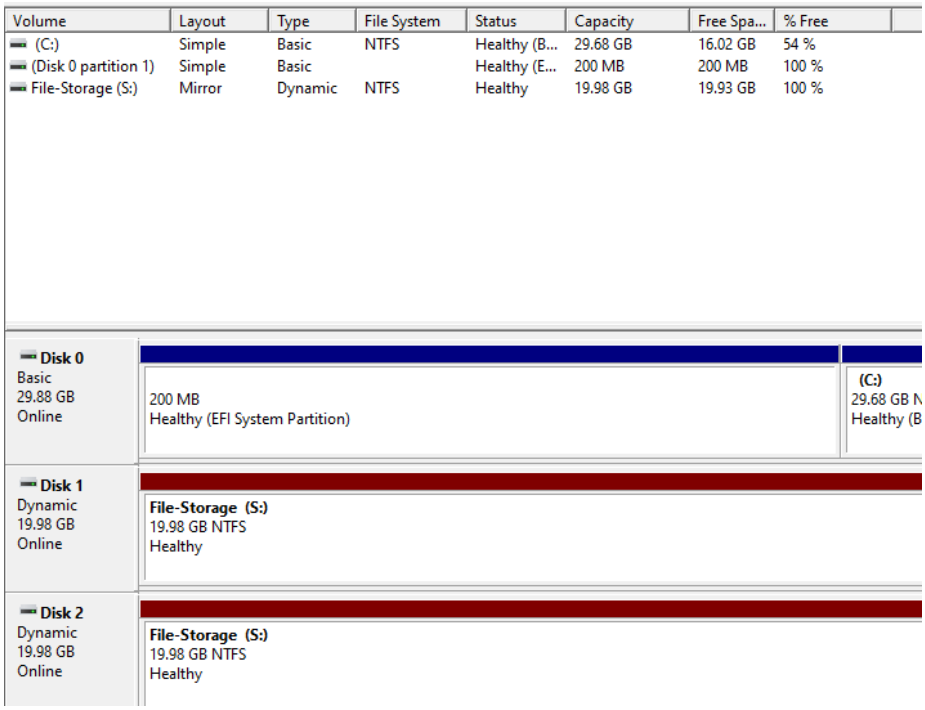

Figure 25: *"Fuse 2 disk"* to create a RAID

6.3 Namespace and replication

Now that we know where to store data, it is time to create and share folder. Go in the new disk and add some folders, for our case we are going to create 2 seperated folder, 1 for IT users and 1 for employee (those who need an access but without specific rights). Once those are created, we are going to share both of them going in their *Property* section. We can now click on *Share* and specify the "read-write-execute" rules. This allow use to specify specific uses for different category, for instance block access to IT folder for employee. A new path now appear in the property, it should look something like this :

```
\\scaduta.lan\IT or even  \\scaduta.lan\Employee
```

Since this process has been reproduce on the 2 servers, we want to do something special to allow replication. After all, they should just replicate each other. That's where namespaces perform ! Go in the *DFS Management* menu, from their you should see *Namespaces* and *Replication*. *Right-click* on Namespaces, create a new one and go through the wizard (specify the root on the new volume).

Once done, It's time to add folder ! Add a folder named IT and select the pre-created IT folder that are shared on both AD-FR and AD-PL.

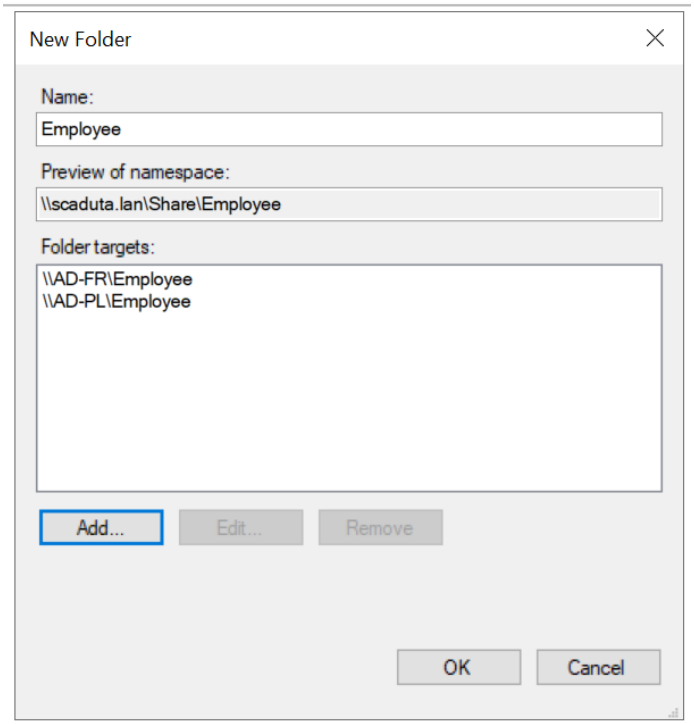

Figure 26: *Folder target*

In fact, we are using target-folder, and once we've selected multiple of them, it ask for a replication setup. That's exactly what we want, go throw the wizard, it will ask you which type of replication type you want, pick Full-mesh. It will also ask for a primary target, pick any of those but note that it will replicate based on it. At some point you will be allow to customize replication schedule, adjust like the AD schedule.

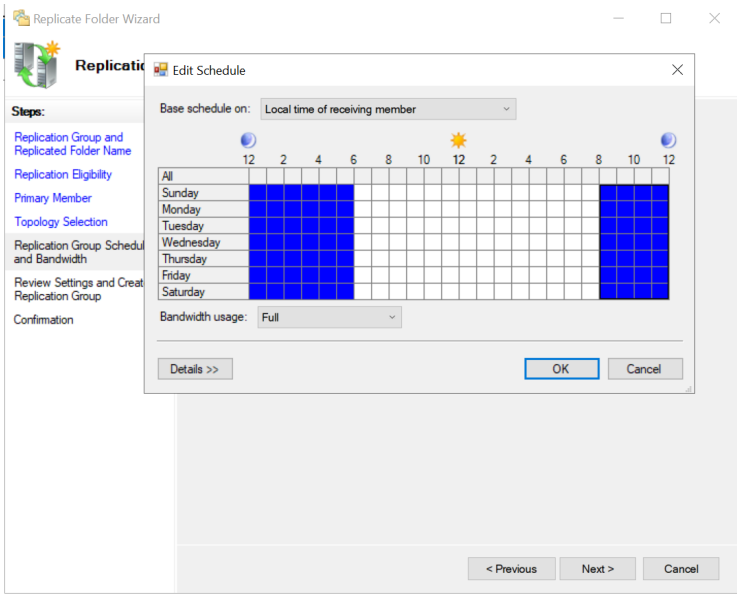

Figure 27: *Replication Files Schedule*

Once you've done this, we are good to go ! The shared folder is working as intended, just be sure to edit shared folder permission to restrict/allow groups as wanted. The DFS namespaces should now look like this (the green arrow means replication is setup).

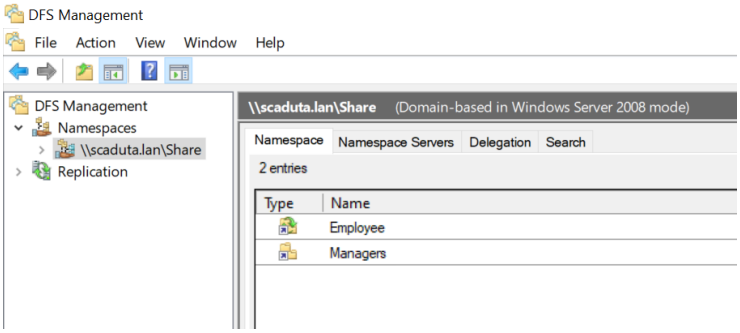

Figure 28: Namespaces after Employee replication

7 IIS or hosting webpage

Let's now take a look at webpage hosting. We are going to use an IIS service on a server, it will allow us to host a webpage.

7.1 Installation

As usual, we are first going to install the corresponding service. Go in the *Server Manager* <*Manage* <*Add Roles And Features* and process through the wizard, select IIS services. We could manage a lot of different information but nothing to special is required for what we want to do. Now that the service is installed, a *"inetpub"* folder appeared in local Drive. Inside it, a "www" root folder contain the files that concern the webpage. Copy paste all needed files here and we are done. You can now test using your browser, localhost redirect to the desired webpage.

7.2 DNS and Redirection

We have seen that the webpage is working. However, we want to be able to access it on any device, moreover being redirected on a webpage that make sense for us. Since each AD-FR and AD-PL host respectively a french and polish version of our webpage, I want to be redirected to the french version if I'm located in France and Vice-Versa. That is where DNS comes in ! Indeed, DNS allow us to add an registration that match our needs. For instance, a client in the polish Site has polish DNS as default DNS. This allow us to add a specific record in each DNS.

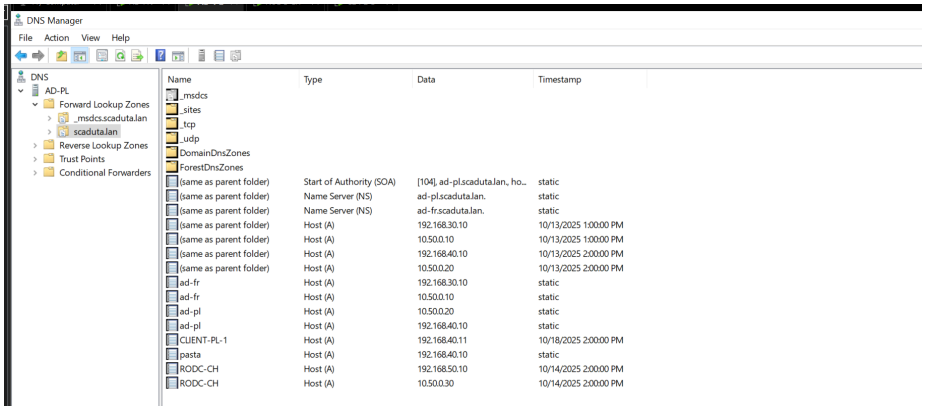

Figure 29: DNS Manager, Forward Lookup Zone

Go in the DNS manager and inside the *Forward Lookup Zone*, add a new Host(A). Specify the Fully Qualified Domain Name (this act as URL), and give the IP redirection based on the DNS. Here is the config used for polish site.

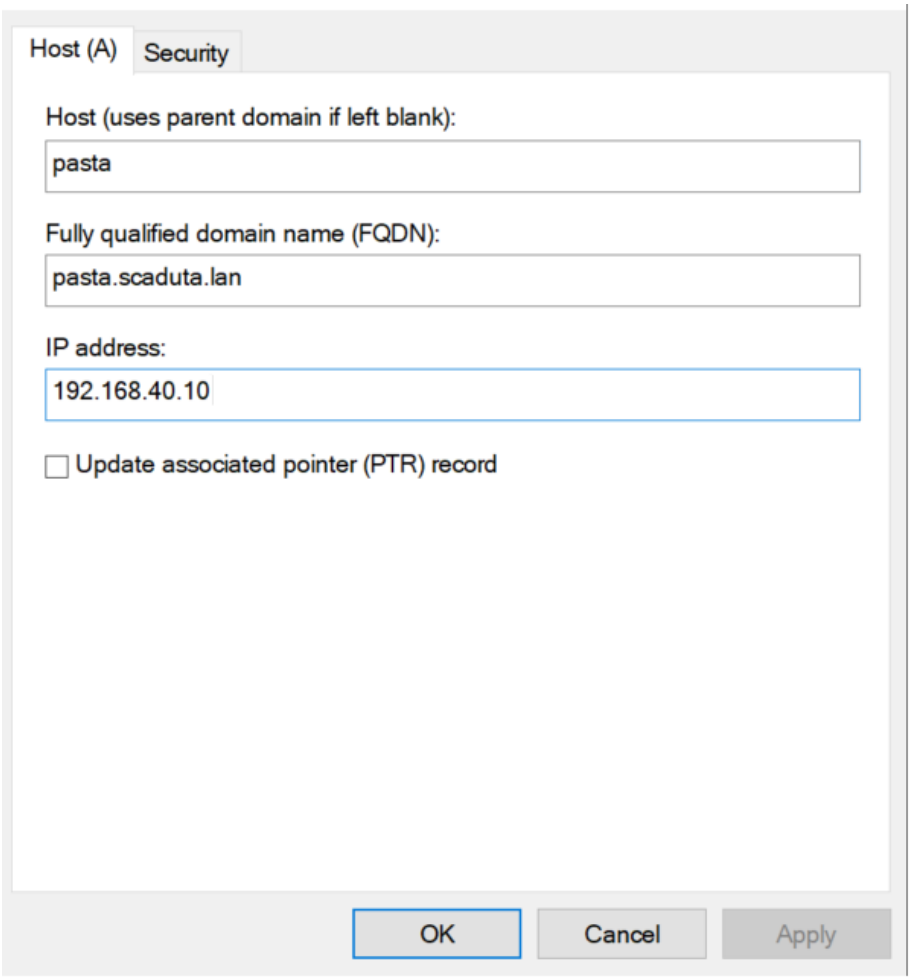

Figure 30: AD-PL DNS redirection

Once done on both DNS server, it should redirect on the correct webpage (NOTE : This is heavily based on default DNS, be sure to have the correct configuration)

8 Applying Group Policy (GPO)

8.1 Password restriction

Let's add some security restriction to our domain ! First, we are going to add specific rules for password assignment. Registered Users should have a complex password with at least 8 characters and last for 30 days. It shouldn't be one of the 5 last password. Go in Group Policy Management menu and develop until you see the domain. *Right-click* and create a new GPO, call it *"User-Password"*. Again *right-click* and edit the GPO, now go in *Computer Configuration <Policies <Windows Settings <Security Settings <Account Policies <Password Policy*. From now, it's elf explanatory, just configured with the restriction listed above. Here is how it should look.

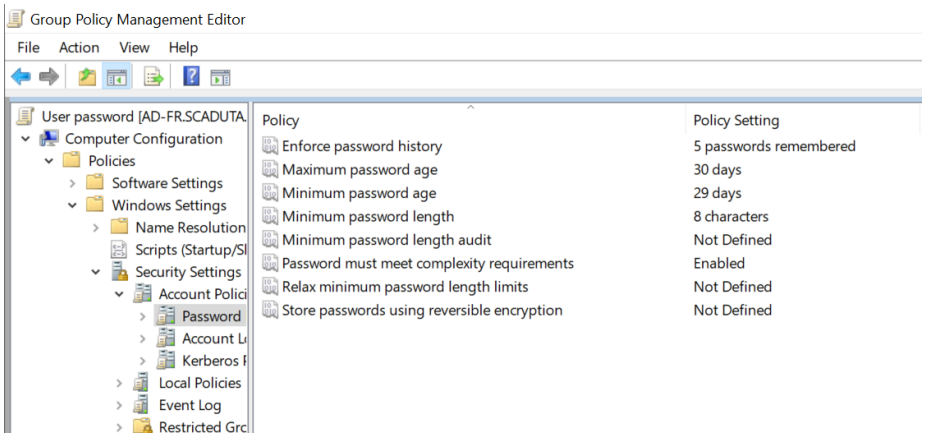

Figure 31: User password restriction

You can now do the same process for another GPO that will concern only the IT group (a specific group that we created before in an dedicated OU) but this time the minimum length is 10, max lifetime is 15 days and password historic is 10 password long. **Note that in order to be applied, targeted users need to have read right in the delegation section.**

8.2 Software Installation

Let's now hope on 7ZIP installation on every device. The installation process of a software require a specific *.msi* file. In our case, check out this website. Once installed, you can place it in a dedicated folder in your domaine namespace (preferably a *"package"* folder). Once done, create a new GPO and go in *Computer configuration <Policies <Software settings* and right-click on it, add a new software and give the **U**niversal **N**aming **C**onvention (UNC) of the .msi file.

We can also recommend installing notepad++. Let's download the *.msi* file from this website. Place it the shared package folder and create a new GPO. Create also a Powershell script (.ps1 file) that will contain the following code (Update UNC as needed !)

```
$CheminInstallation = "$env:ProgramFiles\Notepad++\notepad++.exe"

if (-not (Test-Path $CheminInstallation)) {

    Add-Type -AssemblyName System.Windows.Forms
    $Reponse = [System.Windows.Forms.MessageBox]::Show("Notepad++ n'est pas installé sur cet ordinateur.`n`nVoulez-vous l'installer mainte

    if ($Reponse -eq "Yes") {
        $CheminMSI = "\\pasta-scaduta.com\Public\Package\Notepadpp v8.6.4.msi"

        Start-Process msiexec.exe -ArgumentList "/i `"$CheminMSI`" /quiet /norestart" -Wait
    }
}
```

Figure 32: Powershell script

This script will show a pop-up and ask the User for installation (if not already installed). We just need to trigger the script at login. Create a GPO and go in *User Configuration <Policies <Windows Settings <Scripts(Logon/Logoff)*. Then, add the UNC that point to the script. Once configured, we are done for software installation !

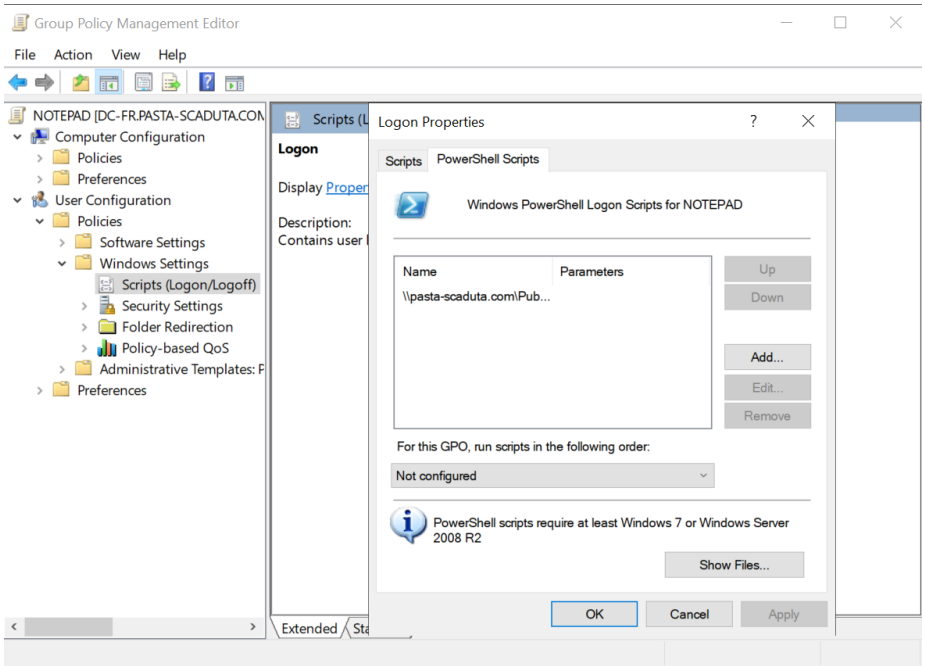

Figure 33: Script trigger on Login

8.3 Commune Wallpaper

In a similar way we did for software, get the image you want as wallpaper and place it in the package folder. Create a new GPO and go in *User configuration* <*Policies* <*Administrative template* <*Desktop* <*Desktop* <*Desktop wallpaper*. Same way, refer the UNC and be sure to apply the GPO to every domain user.

8.4 IIS homepage

Let's make our IIS the default webpage of our web browser. To achieve this, we need to acquire the policies given for our browser (In our case Microsoft Edge). Check this webpage to acquire the policies. Extract it and look for the .adm file. Then go in *Computer configuration* <*Administrative Templates*, right-click and add a new policy. Select the file and edge policies should appear. Go in the *Startup, home page and new tab* and configure as shown below (use the http://pasta-scaduta.lan address).

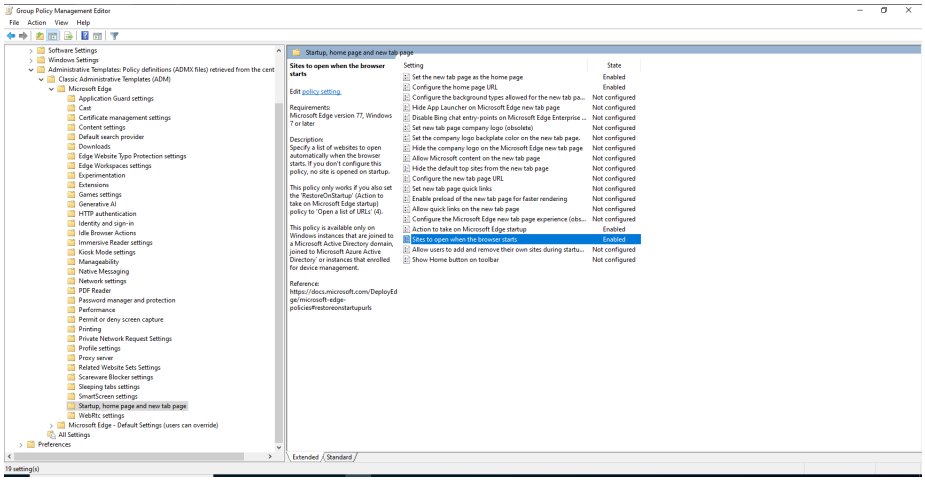

Figure 34: IIS homepage redirection

8.5 Disable Control Panel & Command Prompt

Create a new GPO, edit it. Go in *User configuration* <*Administrative Template* <*Control Panel* <*Prohibit access to Control Panel and PC settings* and disable. For command prompt, go in *User Configuration* <*Administrative Templates* <*System* and disable command prompt.

8.6 Mapped drive

Create a new GPO, edit it. Go in *User Configuration* <*Preferences* <*Windows Settings* <*Drive Maps* and right-click then add. You are now free to select the UNC you want. We are referencing the Public namespace and assigning the drive's letter. Once fully done, you should have something like this.

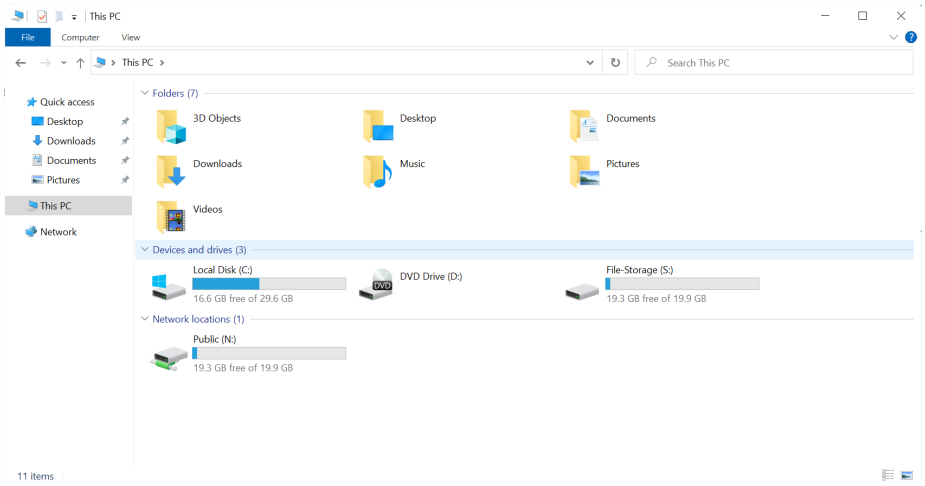

Figure 35: Commune mapped drive

9 Domaine Trust

Let's now establish a trust with the forest of another company. This allow to share Active Directory data such as users. For instance, we could connect using an account that originate from another forest.

9.1 Domaine recognition

First, we need that each device recognize the other forest. Configure a new **SRV-BL** machine with given configuration and create another forest. Open DNS menu and add a new conditional zone on both device, this will refer to the other forest. This is the configuration made on bolivian server (error isn't important here).

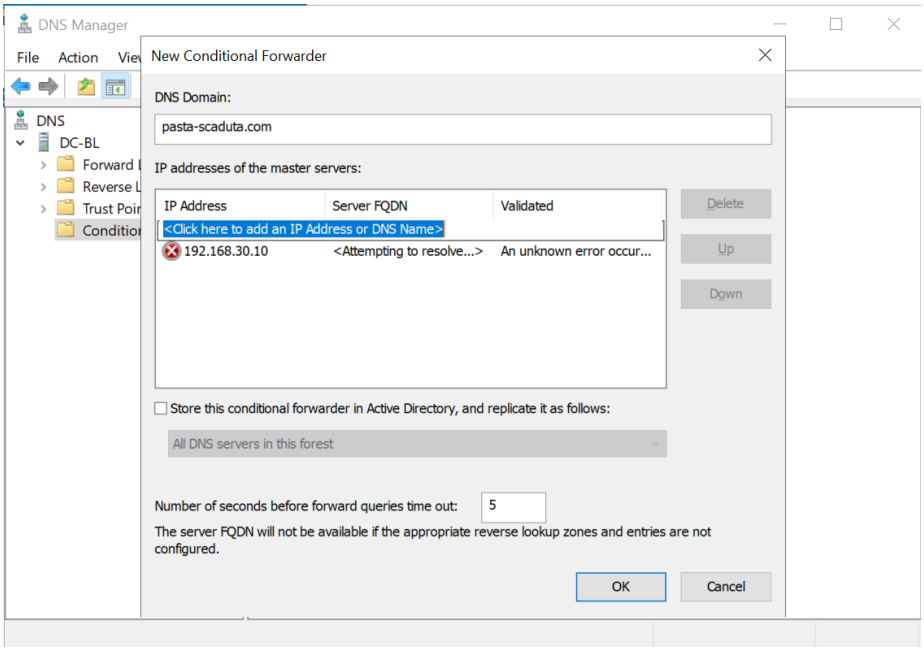

Figure 36: Conditional Forwarder

9.2 Establish the trust relationship

Then, you can head up to the *Active Directory Domains and Trusts* menu. Go in *Property* $<$ *Trust* and add a new Trust. First, give the domaine name of the forest you want to trust, then pick *Realm* $<$ *Transitive* $<$ *Two-way* and create a password. Now that it is configure, repeat the process on the other server.

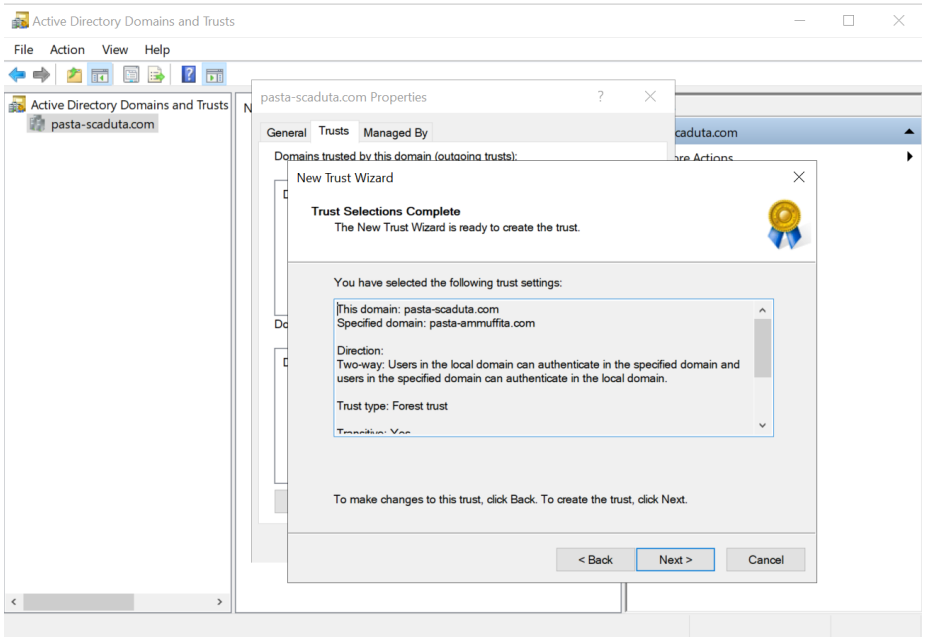

Figure 37: Creating a Trust relationship

After that, come back in the Trust subsection of the domain's properties and validate each trust using appropriate credentials. You can now view other users and roles that are used in the trust domain.

10 RDP and Management Server

For the last part, create a new server in France. This one is dedicated to Management Operations and will connect remotely using RDP.

10.1 Allowing RDP

To initiate a Remote Desktop (RDP) connection, the first essential step is to enable incoming connections on the target server. This setting, which is often disabled by default for security reasons, allows the domain controller to accept remote control requests. As illustrated below, activation is done by navigating to the server's system settings and toggling the 'Enable Remote Desktop' switch to 'On'. Note that this operation requires administrator privileges on the target machine.

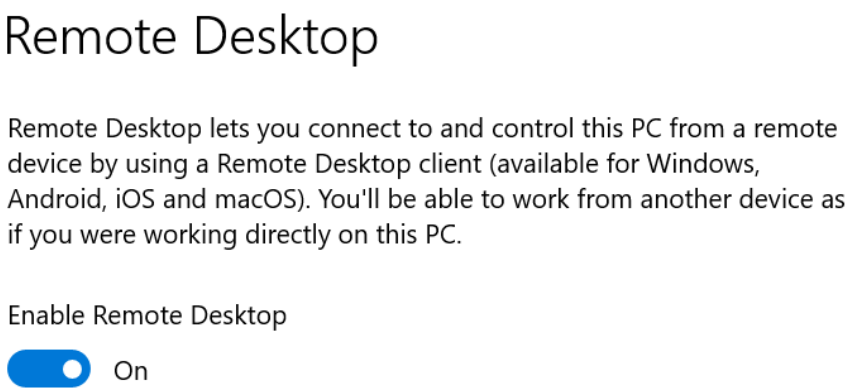

Figure 38: Allowing RDP

10.2 Add a server to manage

With remote access enabled on the target DC, the next step is to add it to the Server Manager console on your primary administration server. This allows for centralized management from a single dashboard. From the main Server Manager Dashboard, begin by clicking on "Add other servers to manage."

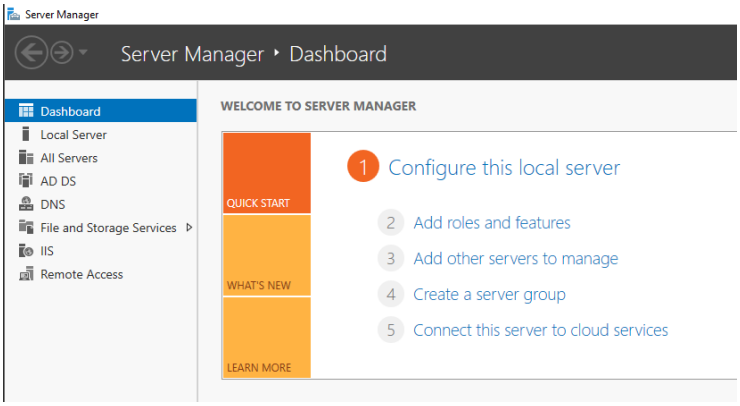

Figure 39: Add a new server to manage

In the window that appears, use the Active Directory tab to search for the target computer (in this case, DC-FR). As illustrated in the screenshot, once you find the server, add it to the "Selected" column on the right. After clicking OK, the remote server will be registered, allowing you to manage its roles and services directly from your console.

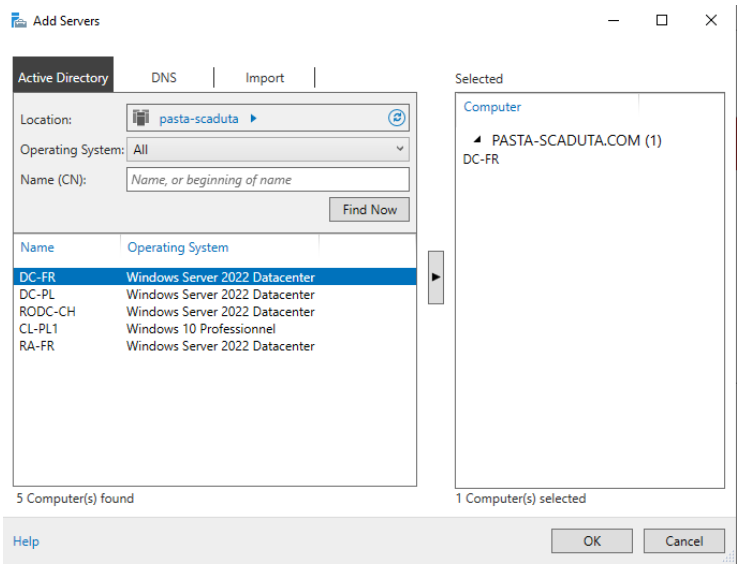

Figure 40: Add the target DC to manage

10.3 Remote connecting to a DC

With the target server now successfully added to your management pool, you can initiate a remote connection directly from the Server Manager interface. Navigate to the "All Servers" tab in the left-hand navigation pane. From the list, locate your domain controller (DC-FR), right-click on it to bring up the context menu, and select "Remote Desktop Connection."

This action will launch the Windows RDP client and begin the session, giving you full graphical access to the remote server's desktop. You can now proceed with any administrative tasks as if you were physically present at the machine.

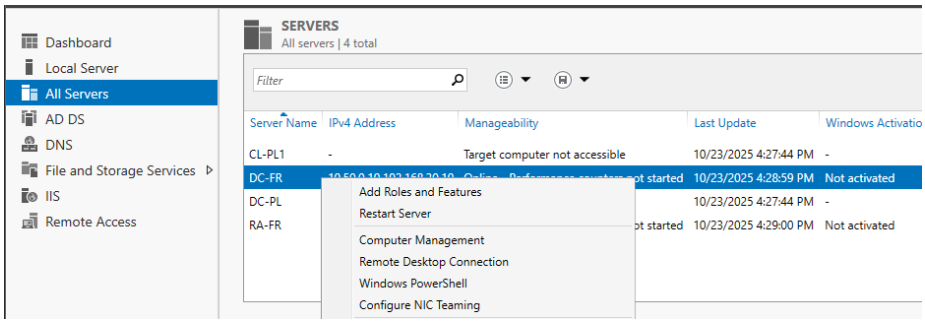

Figure 41: Remote connecting

11 Annexes

11.1 IP listing

Device Name	Interface	IP address	subnet mask	default gateway
AD-FR	Eth0	192.168.30.10	255.255.255.0	192.168.30.2
AD-FR	Eth1	10.50.0.10	255.255.0.0	
AD-PL	Eth0	192.168.40.10	255.255.255.0	192.168.40.2
AD-PL	Eth1	10.50.0.20	255.255.0.0	
AD-CH	Eth0	192.168.50.10	255.255.255.0	192.168.50.2
AD-CH	Eth1	10.50.0.30	255.255.0.0	
AD-BL	Eth0	192.168.35.10	255.255.255.0	192.168.35.2
AD-BL	Eth1	10.50.0.40	255.255.0.0	
CL-PL-1	Eth0	192.168.40.11	255.255.255.0	192.168.40.2
RA-FR	Eth0	192.168.30.11	255.255.255.0	192.168.30.2

11.2 Routing Commune Issues

You may have encounter some issues concerning the relationship between 2 Sites. For instance, you struggle discuss with Polish site from France despite having the correct configuration. First, you need to install the **Remote Access** service on both machine and configure everything related to routing. That means that during service installation, pick "routing" and after that go in **Routing and Remote Access** menu. Enable the current machine (you should see a red dot because it's not configured yet), select *Custom configuration <LAN Routing <Finish*.

You also need to configure persistent route. Those are here to tell the machine : *"Hey, want to go in this specific network ? Right, contact this guys, he surely know"*. Here is useful command

`Show routing table : route print / Add a route : route add`

This helps to tell France to contact Poland's network by contacting 10.50.0.30 rather than directly searching for 192.168.40.0/24 subnet.

11.3 Useful Commands

Command	**Action**
repadmin /syncall /APed	Forces the synchronization of AD replications.
gpupdate /force	Forces a re-application of all GPO.
gpresult /r	Lists all applied GPO.