

Projet Active Directory sous VMware avec pfSense – Rapport Technique Complet

1. Création de l'environnement virtualisé sous VMware

Objectif

Créer un réseau local isolé permettant de configurer un environnement Active Directory avec un serveur Windows Server 2022, une station cliente Windows 10 et un routeur pfSense. Toutes les machines doivent communiquer entre elles via le réseau personnalisé **VMnet9**.

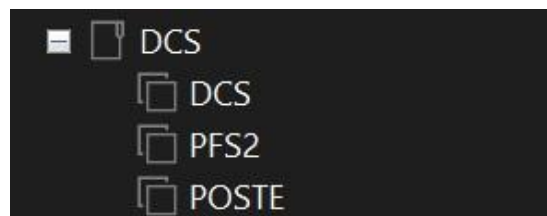
Étape 1 – Lancement du logiciel

- Ouvrir **VMware Virtual Network Editor** (exécuter en tant qu'administrateur)..

Étape 2 – Création des VMs

- Créer une machine virtuelle **Windows Server 2022**, nommée **DCS**.
- Créer une machine virtuelle **Windows 10**, nommée **POSTE**.
- Créer une machine virtuelle **pfSense**.

Chaque VM est configurée avec une seule carte réseau connectée à **VMnet9** (Bridged to: Custom, VMnet9).



DCS

▶ Power on this virtual machine

🔧 Edit virtual machine settings

▼ Devices

Memory	2 GB
Processors	2
Hard Disk (NVMe)	60 GB
CD/DVD (SATA)	Using file D:\SIO\...
Network Adapter	Custom (VMnet9)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

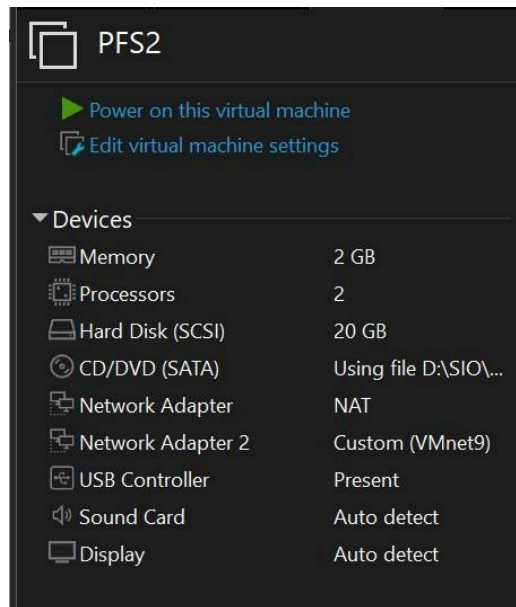
POSTE

▶ Power on this virtual machine

🔧 Edit virtual machine settings

▼ Devices

Memory	1 GB
Processors	2
Hard Disk (NVMe)	60 GB
CD/DVD (SATA)	Using file D:\VM\...
Network Adapter	Custom (VMnet9)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

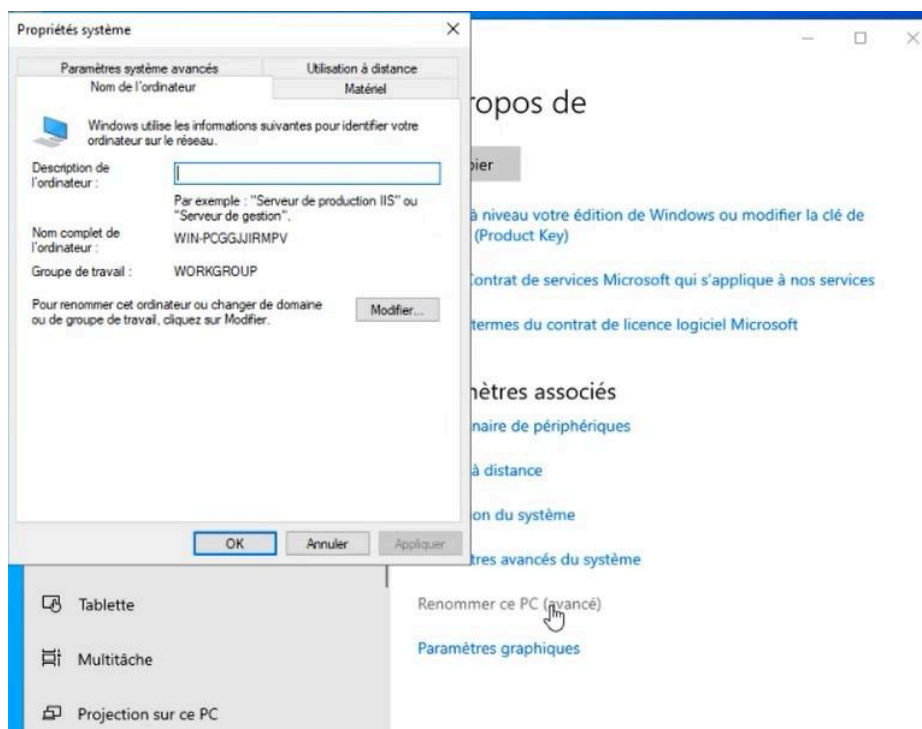


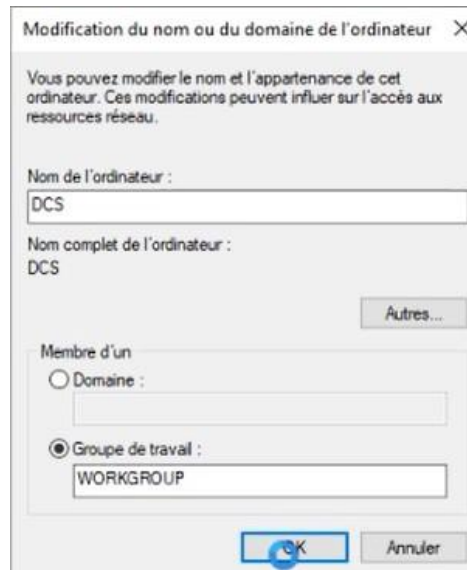
SECTION : 2. Configuration de DCS (Contrôleur de Domaine)

Étape 1 – Renommage et configuration IP

Pour des raisons de lisibilité et d'organisation, on commence par renommer la machine Windows Server 2022 en **DCS** (Domain Controller Server). Cela permet de l'identifier facilement dans l'infrastructure.

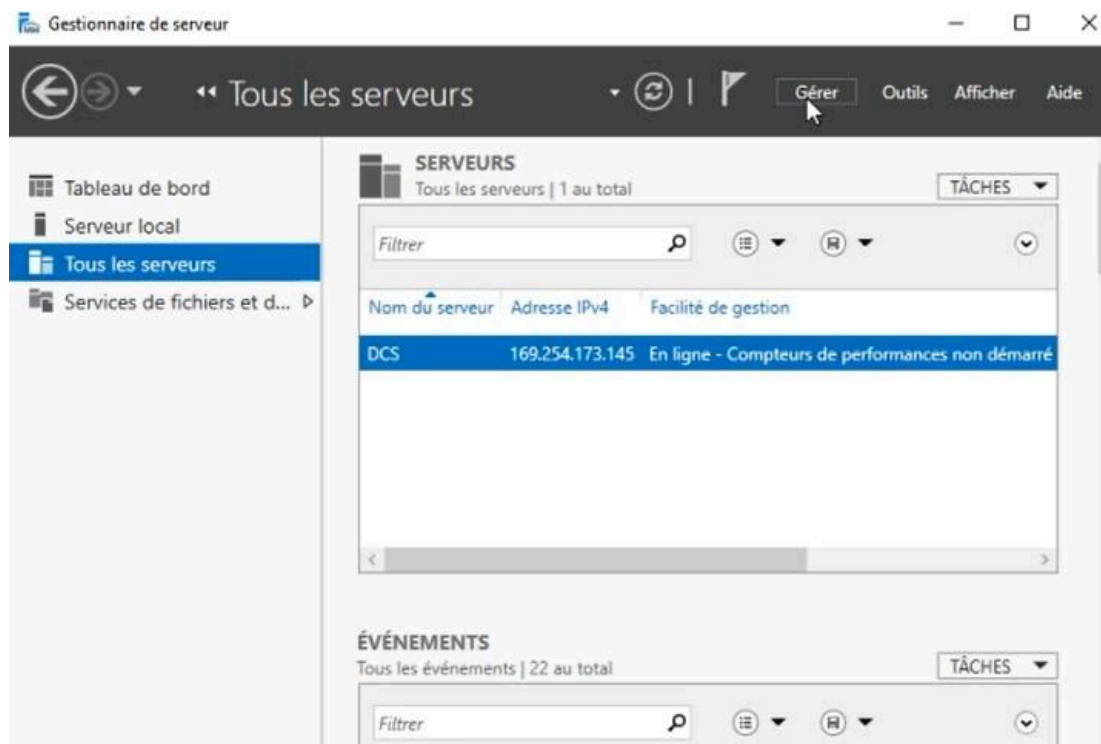
- Renommer l'ordinateur en **DCS**.





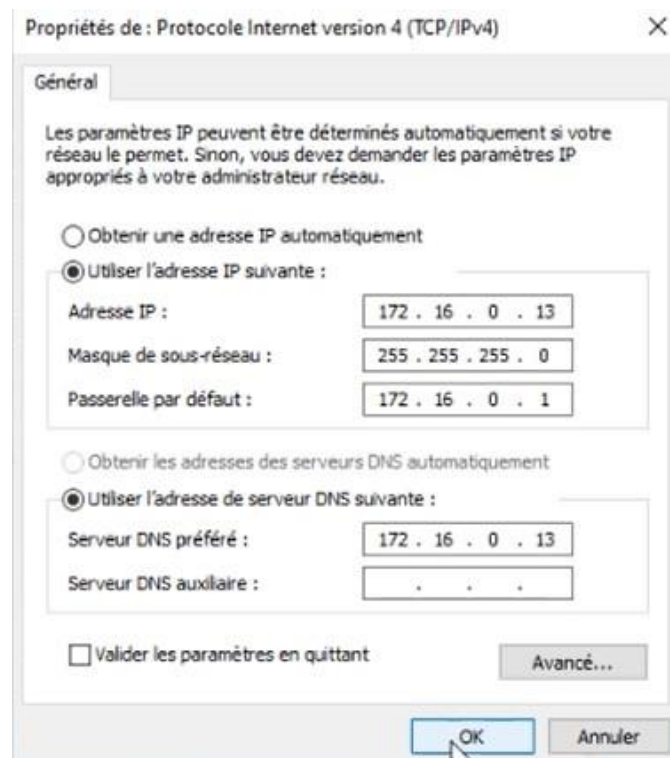
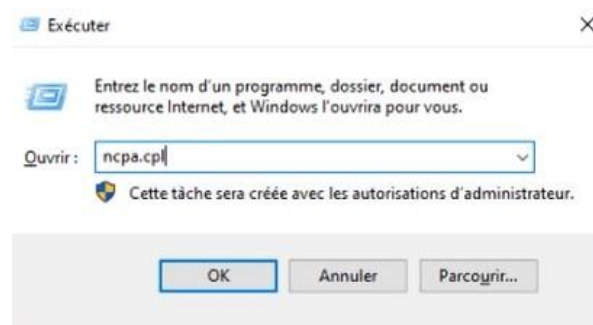
- Redémarrer le système après le renommage

Résultat:



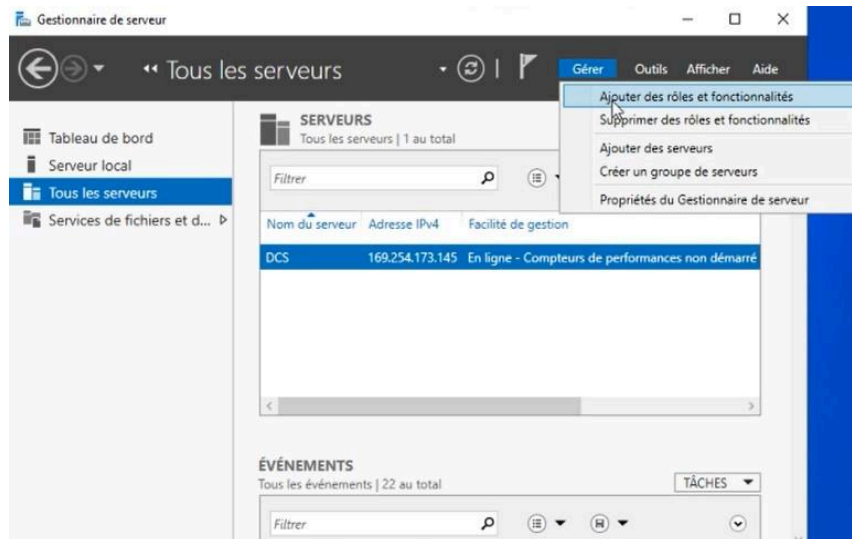
Il est nécessaire d'attribuer une IP fixe au serveur pour garantir sa stabilité réseau, essentielle pour un contrôleur de domaine

- Depuis la console `ncpa.cpl`, configurer une IP statique pour DCS :
 - IP : `172.16.0.10`
 - Masque : `255.255.255.0`
 - Passerelle : `172.16.0.1`
 - DNS : `172.16.0.10` (lui-même car futur contrôleur de domaine)

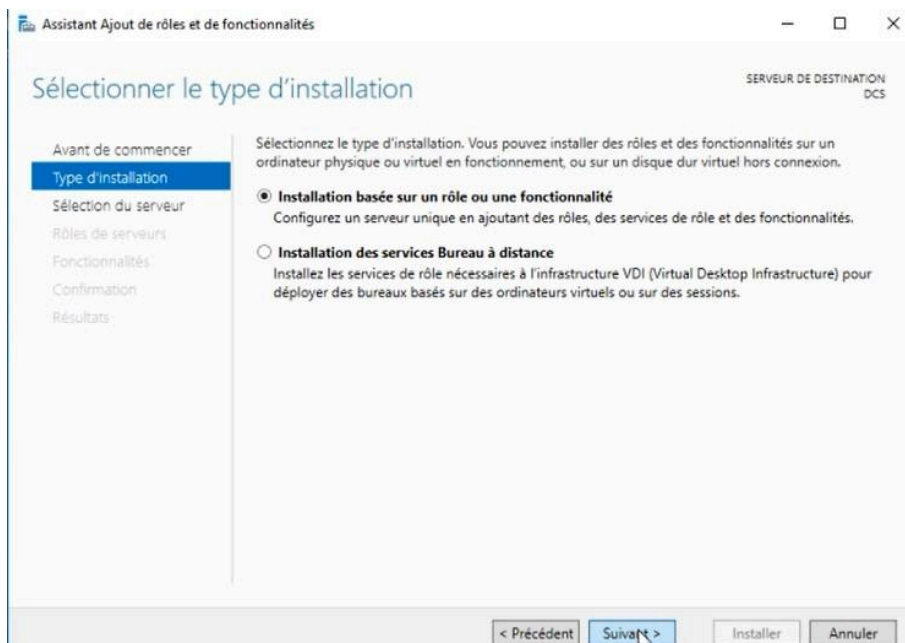


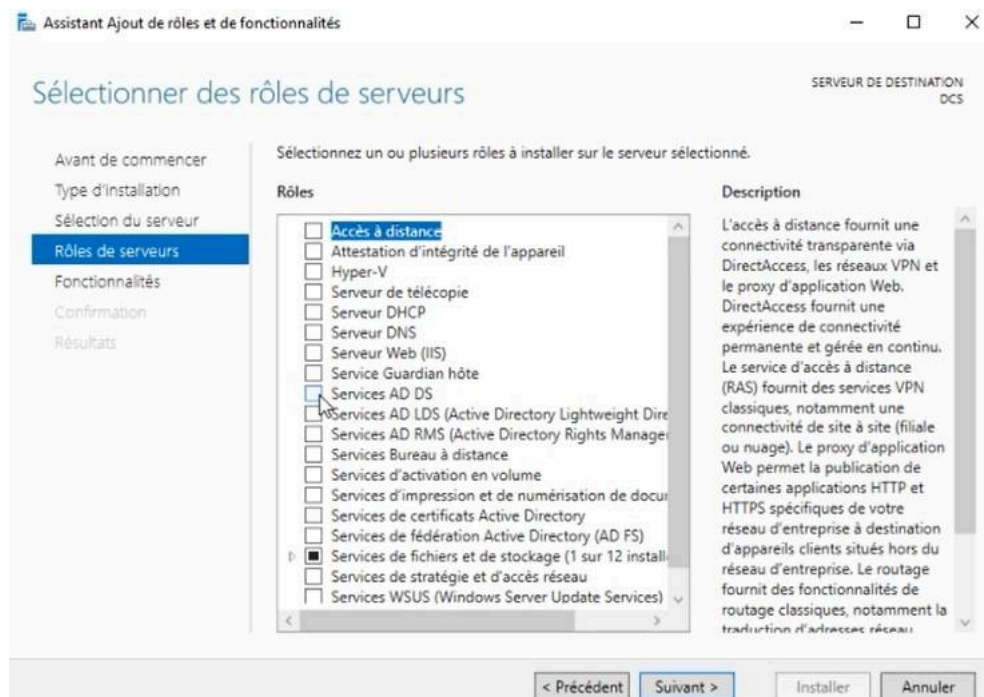
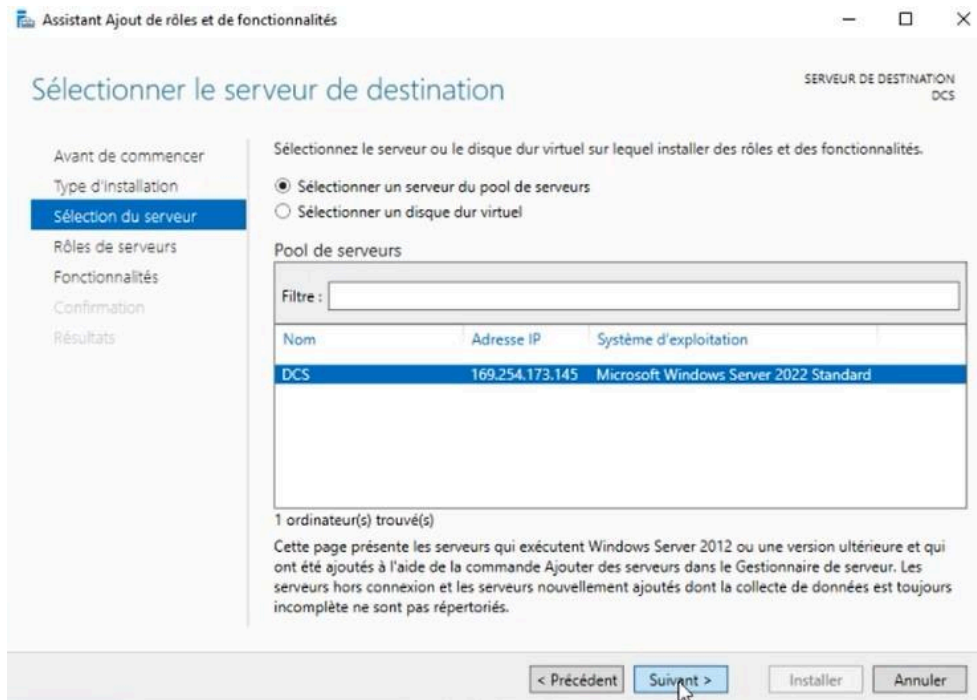
Étape 2 – Installation d'ADDS

- Ouvrir le **Gestionnaire de serveur** > **Gérer** > **Ajouter des rôles et fonctionnalités**.

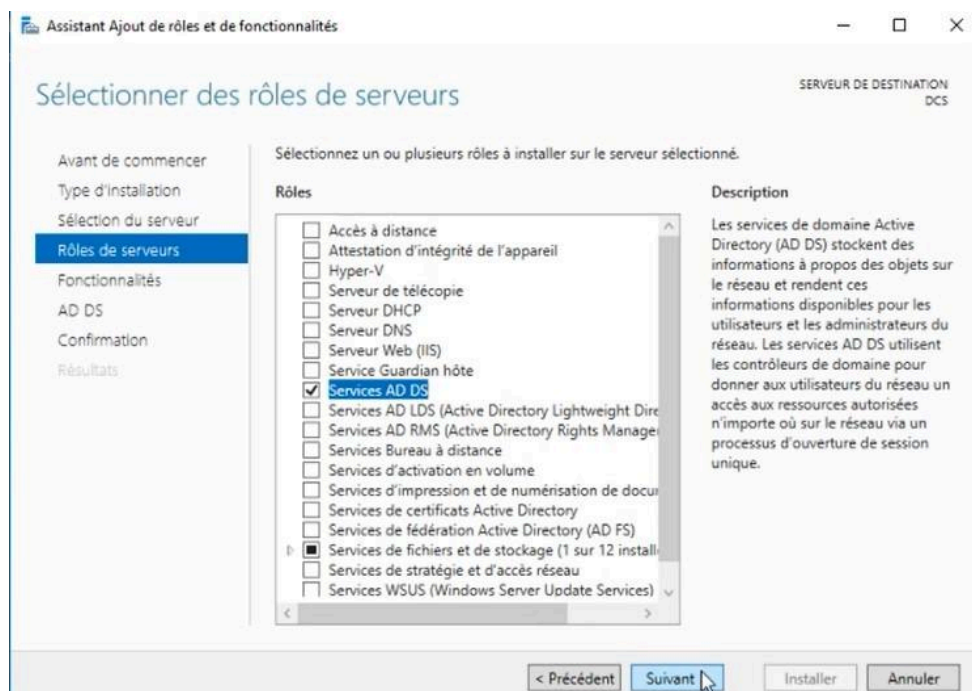


- Sélectionner le rôle **Services de domaine Active Directory (AD DS)**.

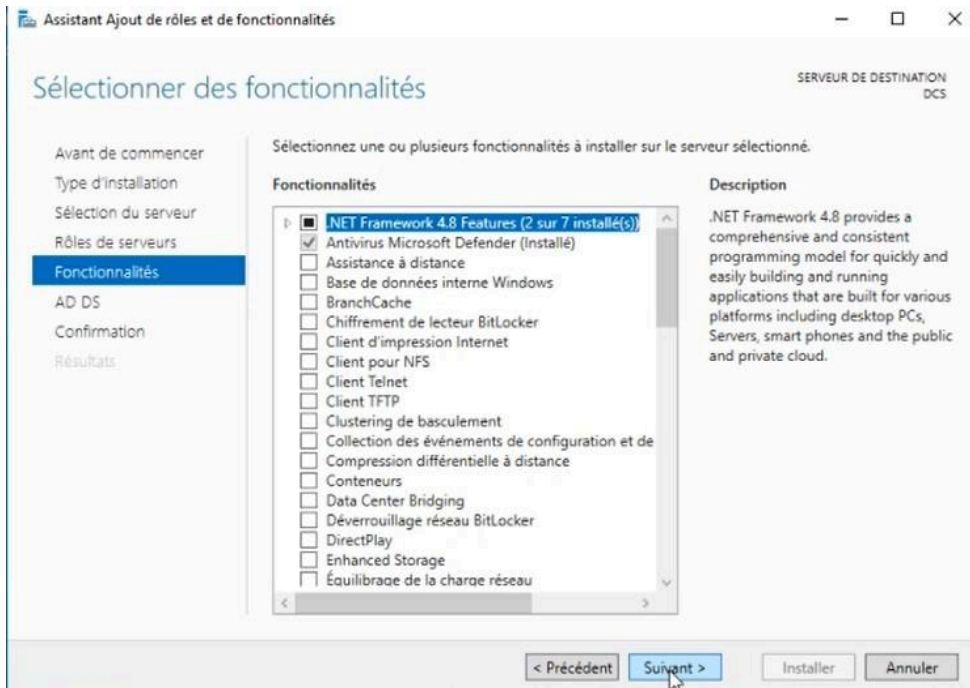


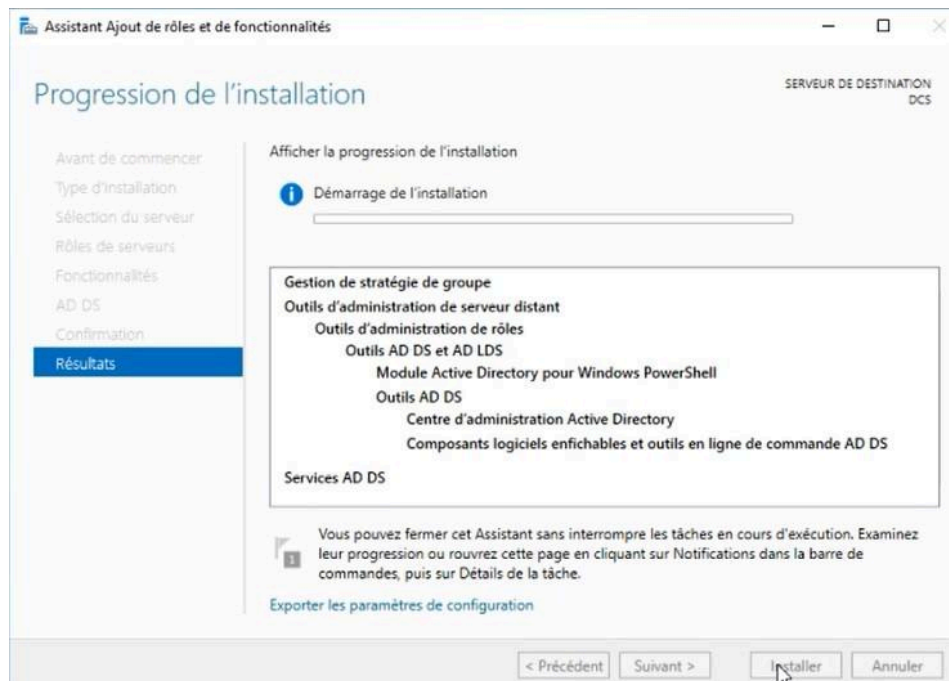


👉 Cette étape prépare le serveur à devenir un contrôleur de domaine

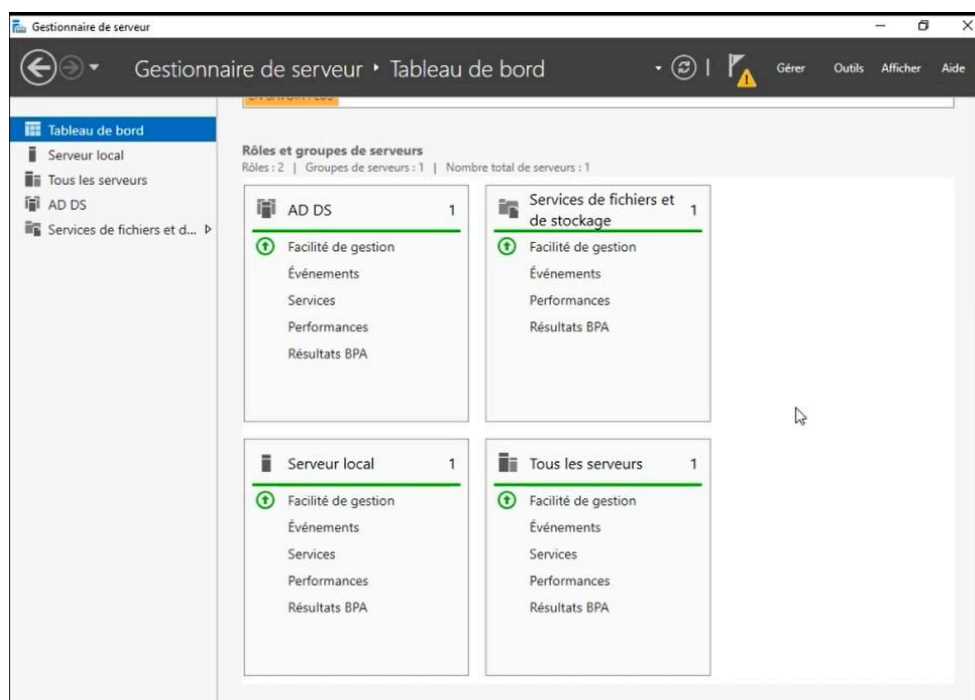


Laisser les options par défaut et cliquer sur **Suivant** jusqu'à l'installation



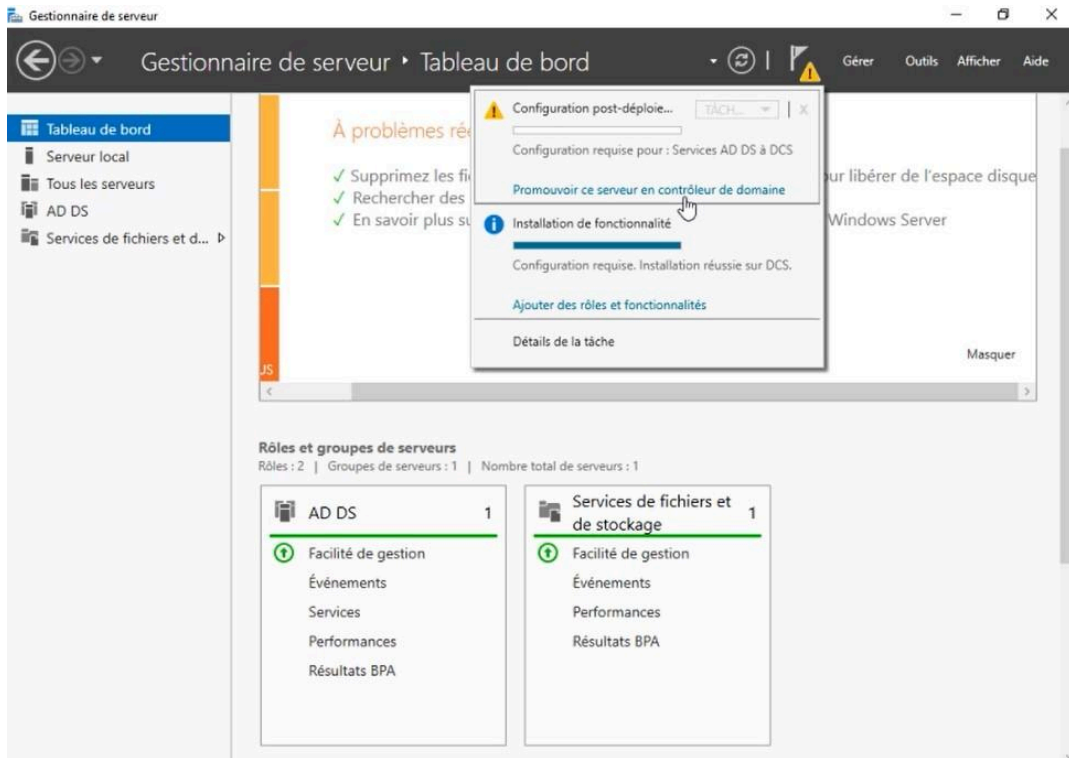


Résultat:



Après l'installation, on lance la **post-installation** :

- Cliquer sur **"Promouvoir ce serveur en contrôleur de domaine"**



👉 Cela crée une hiérarchie logique dans l'environnement Windows, gérée par Active Directory.

- Créer une **nouvelle forêt** : nom du domaine **test.fr**.

Assistant Configuration des services de domaine Active Directory

SERVEUR CIBLE DCS

Configuration de déploiement

Configuration de déploiement...

Sélectionner l'opération de déploiement

- ☐ Ajouter un contrôleur de domaine à un domaine existant
- ☐ Ajouter un nouveau domaine à une forêt existante
- ☒ Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine : test.fr

En savoir plus sur les configurations de déploiement

< Précédent Suivant > Installer Annuler

Assistant Configuration des services de domaine Active Directory

SERVEUR CIBLE DCS

Options du contrôleur de domaine

Options du contrôleur de...

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

Niveau fonctionnel de la forêt : Windows Server 2016

Niveau fonctionnel du domaine : Windows Server 2016

Spécifier les fonctionnalités de contrôleur de domaine

- ☒ Serveur DNS (Domain Name System)
- ☒ Catalogue global (GC)
- ☐ Contrôleur de domaine en lecture seule (RODC)

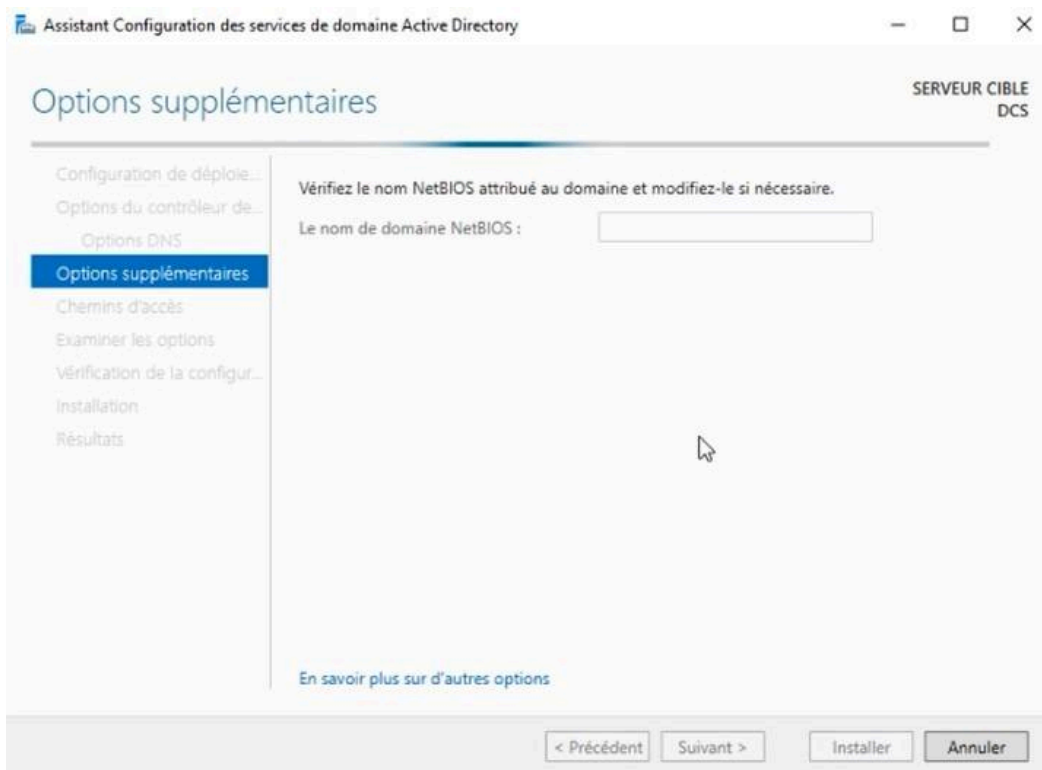
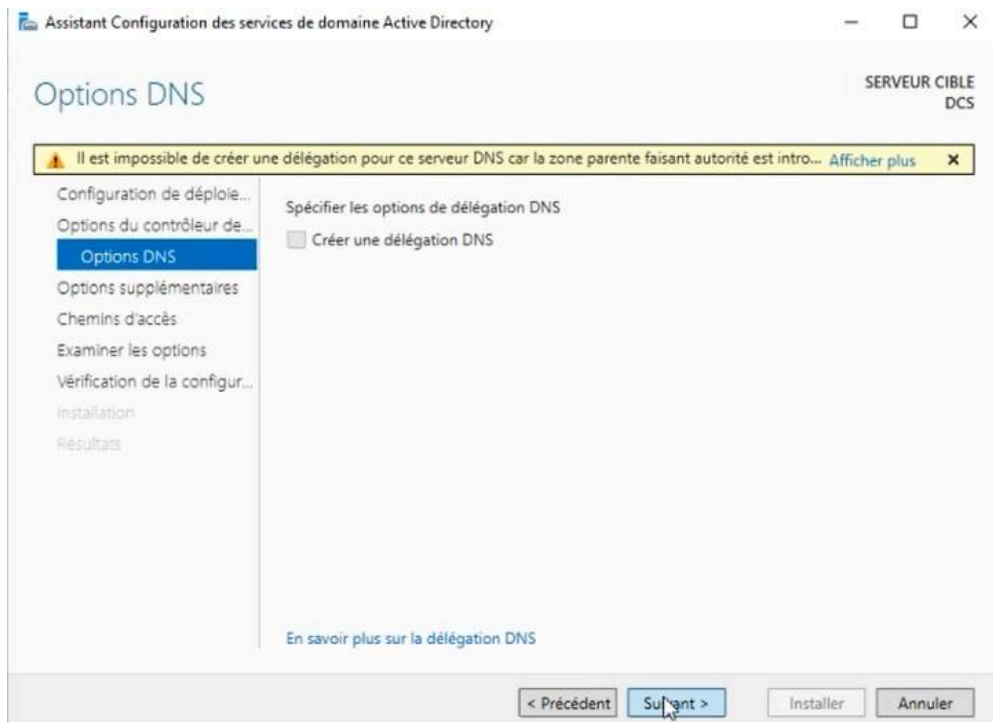
Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

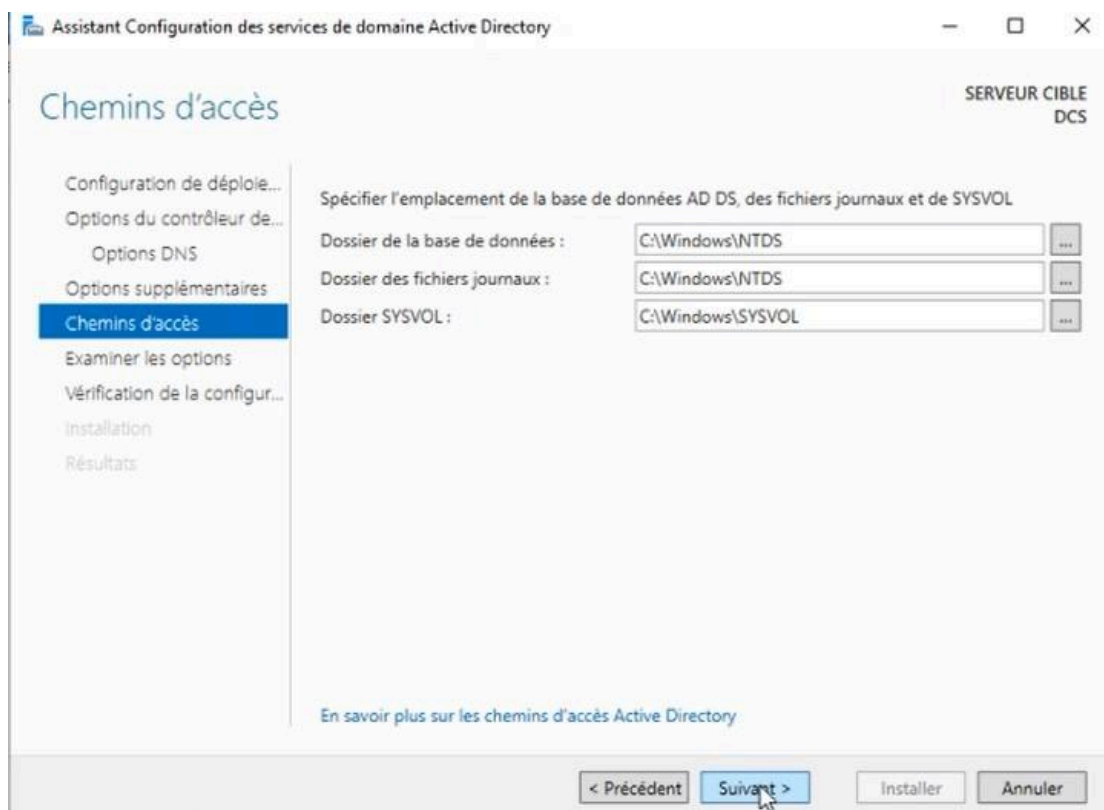
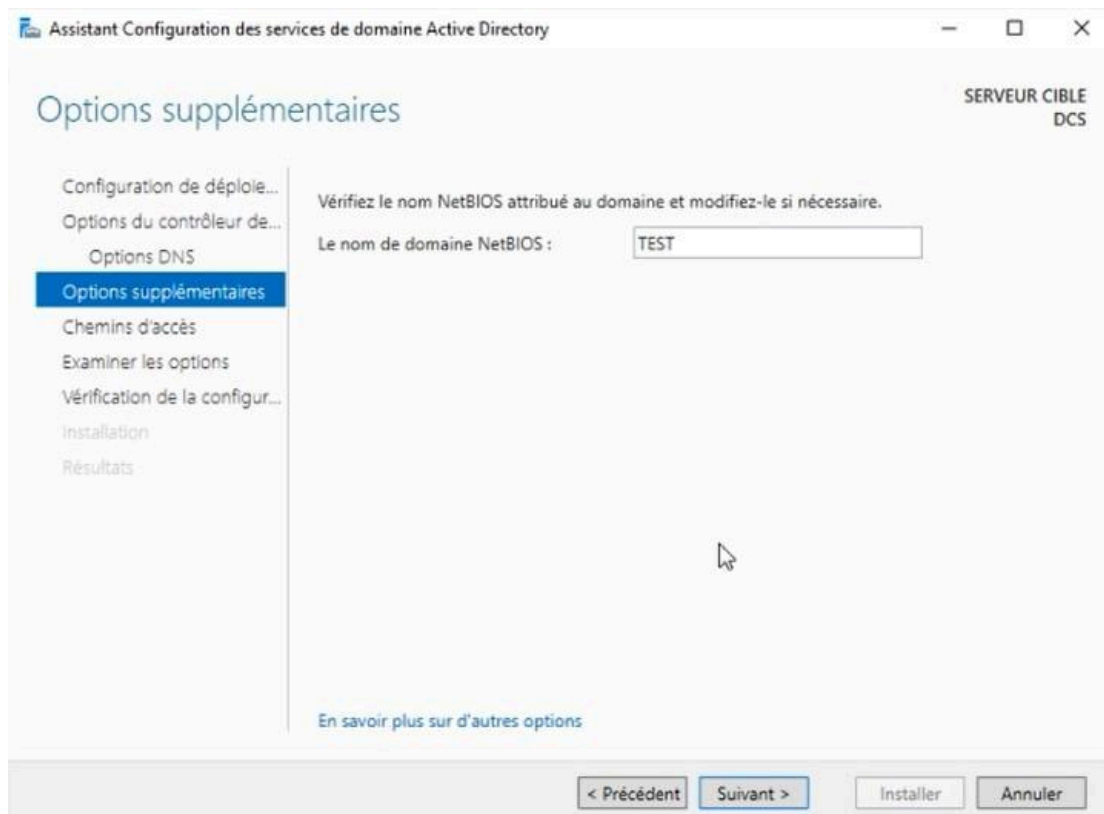
Mot de passe :

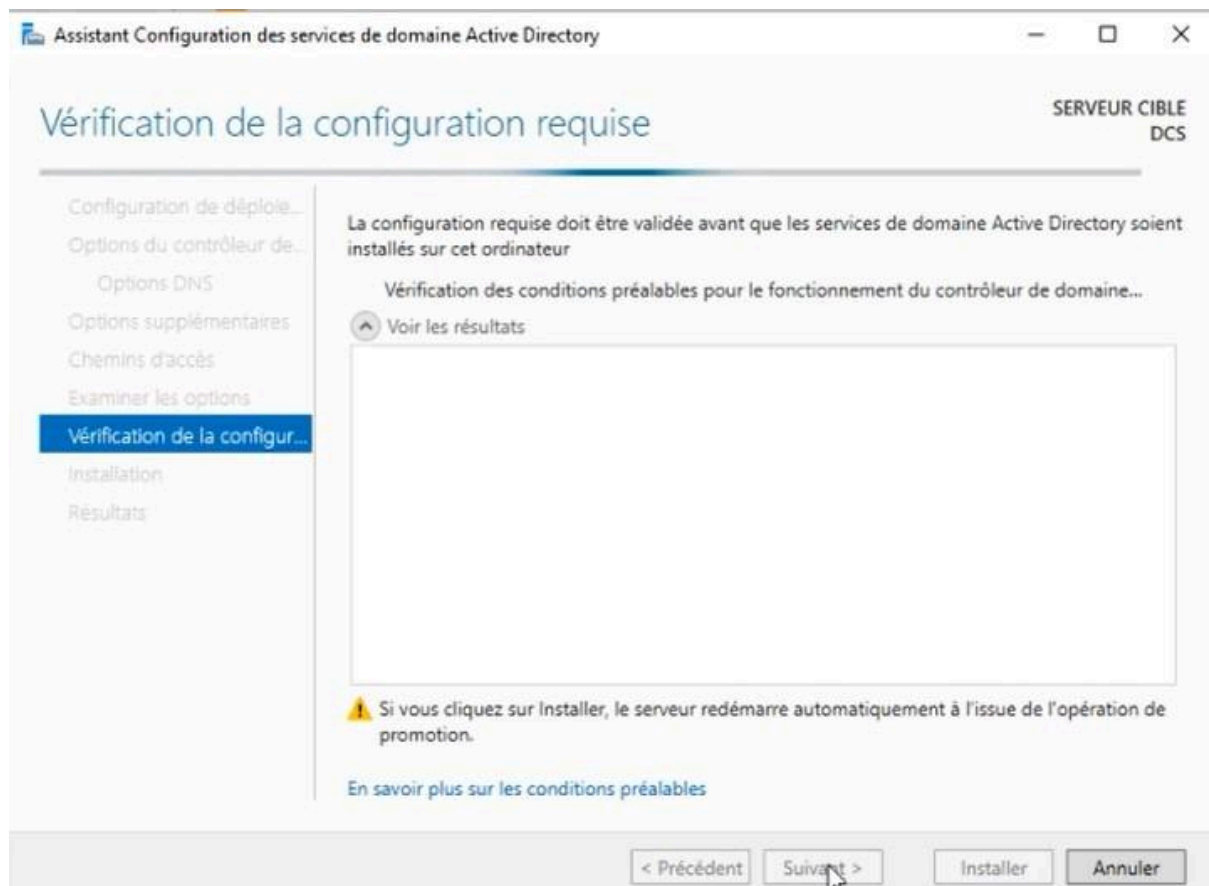
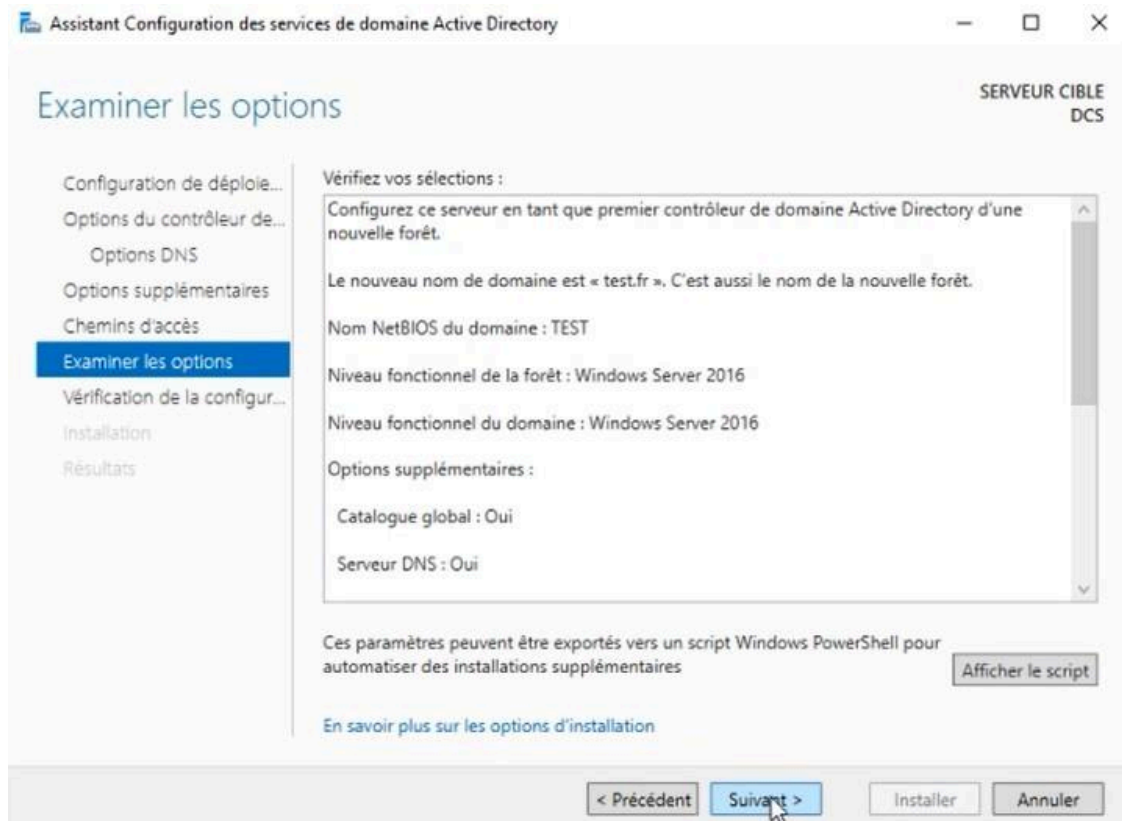
Confirmer le mot de passe :

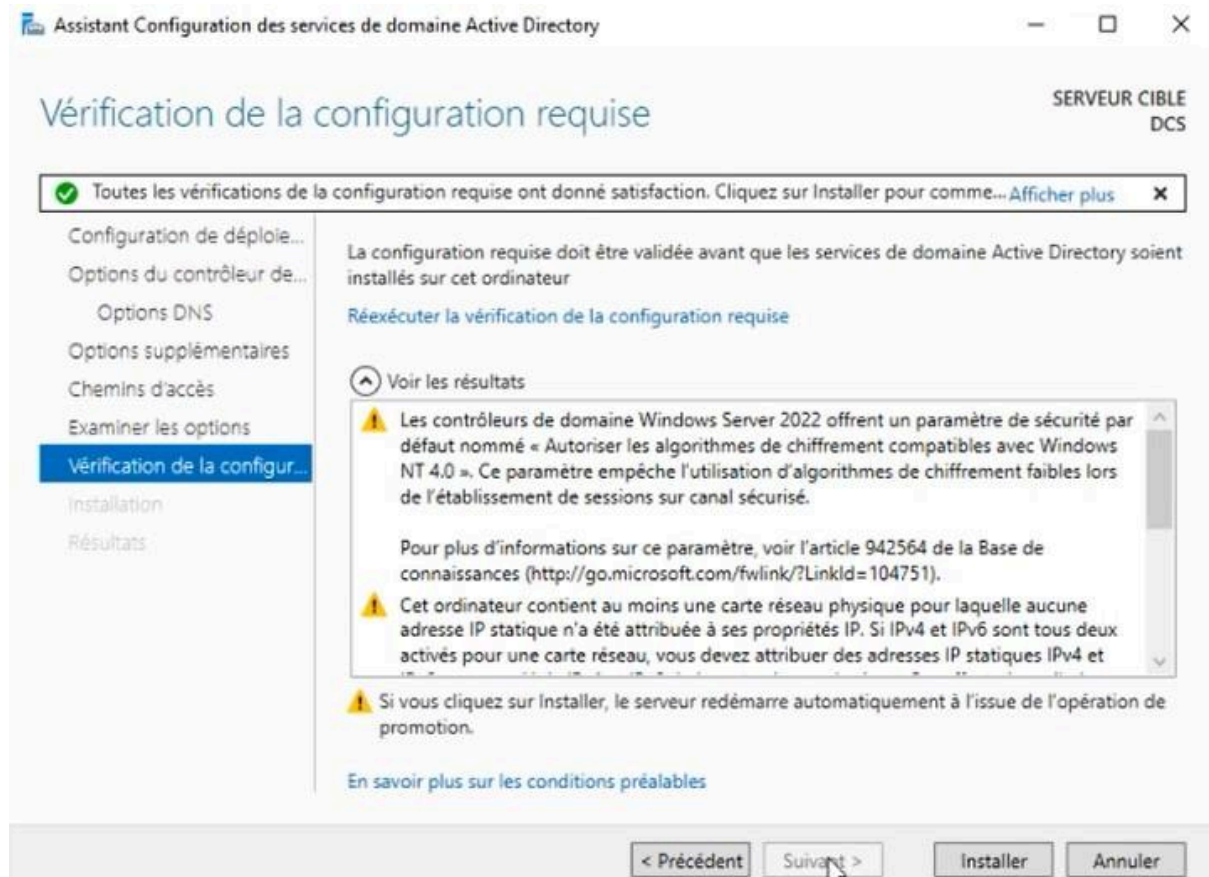
En savoir plus sur les options pour le contrôleur de domaine

< Précédent Suivant > Installer Annuler









Installation

SERVEUR CIBLE
DCS

Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats

État d'avancement

Démarrage



Afficher les résultats détaillés de l'opération



Les contrôleurs de domaine Windows Server 2022 offrent un paramètre de sécurité par défaut nommé « Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ». Ce paramètre empêche l'utilisation d'algorithmes de chiffrement faibles lors de l'établissement de sessions sur canal sécurisé.

Pour plus d'informations sur ce paramètre, voir l'article 942564 de la Base de connaissances (<http://go.microsoft.com/fwlink/?LinkId=104751>).

En savoir plus sur les options d'installation

< Précédent

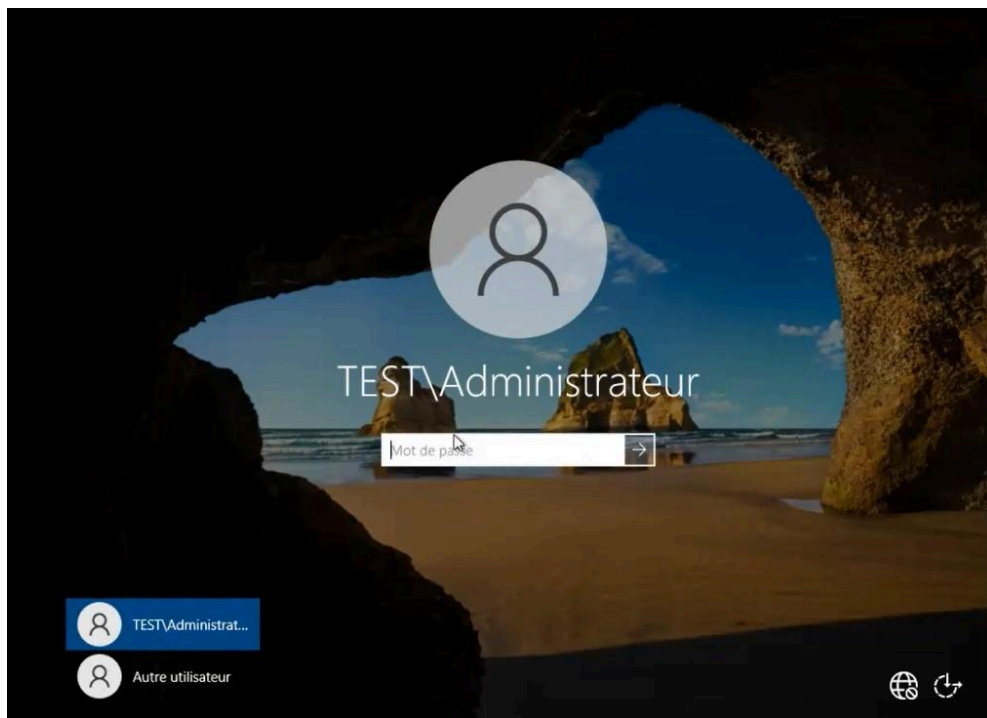
Suivant >

Installer

Annuler

- Redémarrer le serveur à la fin.

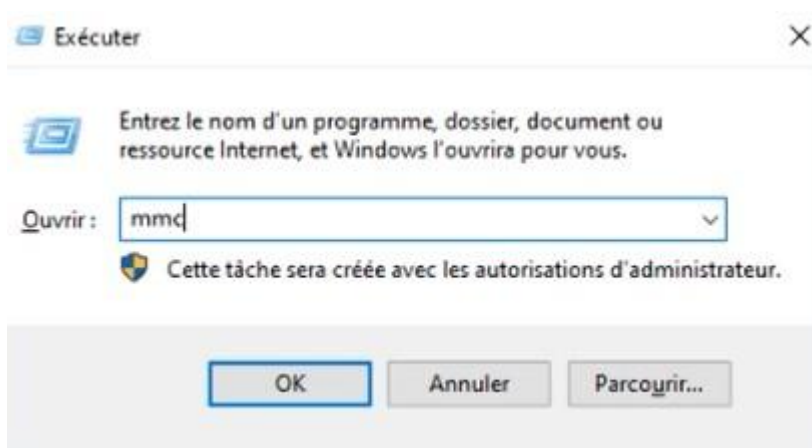
Résultat après le redémarrage:



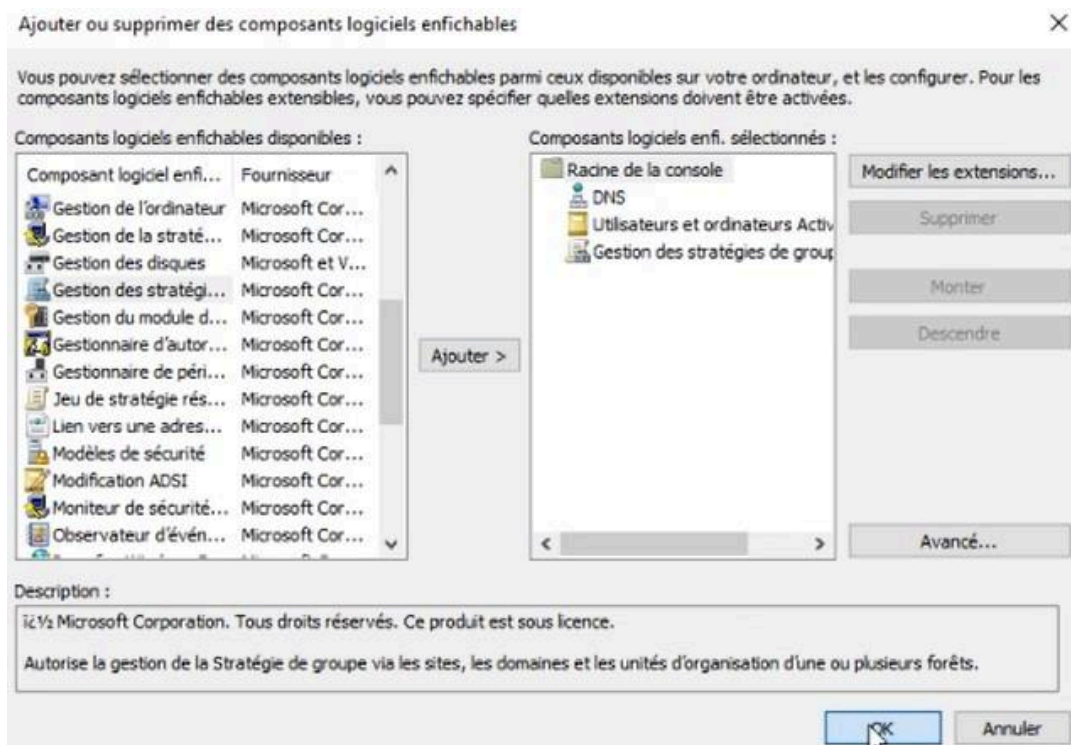
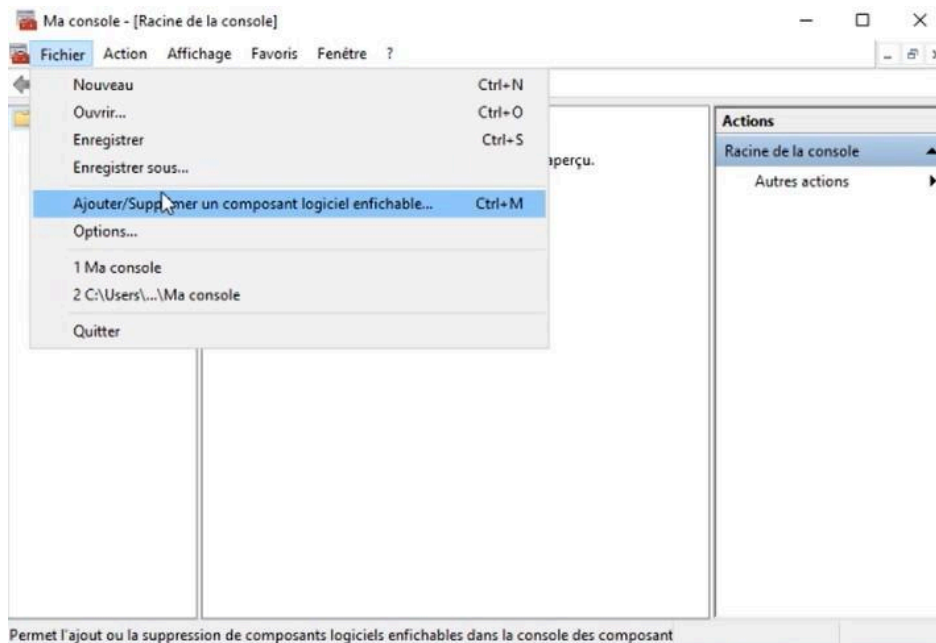
Étape 3 – Configuration de la console MMC personnalisée

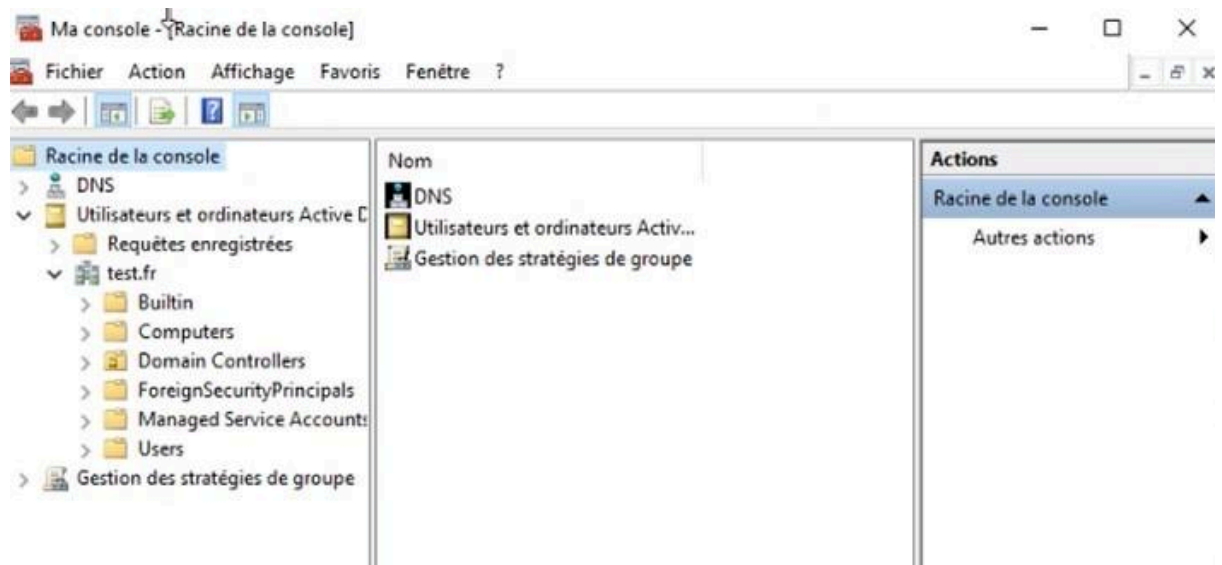
Pour faciliter la gestion centralisée des différents services, on crée une **console personnalisée MMC**.

- Lancer `mmc.exe`.

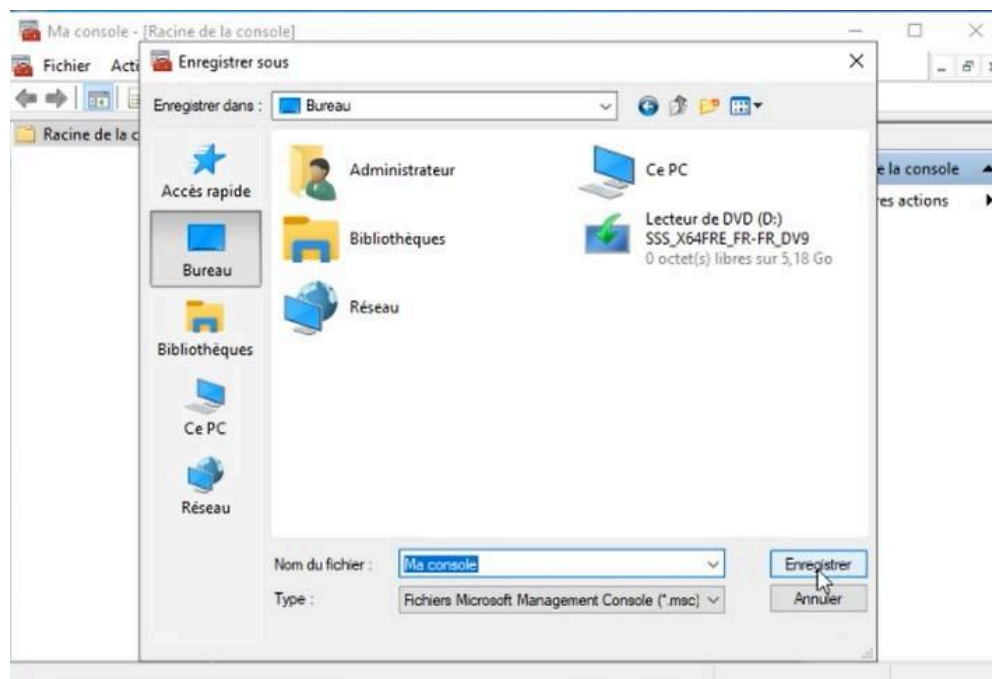


- Ajouter les **modules suivants**: Utilisateurs et ordinateurs AD, DNS, Gestionnaire des stratégies de groupe(GPO)





- Sauvegarder la console personnalisée pour la gestion centralisée.





SECTION : 3. Configuration de pfSense

Le routeur **pfSense** permet ici de gérer le réseau local, attribuer des adresses IP via DHCP, et simuler une passerelle pour l'environnement virtualisé

Étape 1 – Affectation des interfaces

Une fois pfSense installé et lancé, il faut attribuer les bonnes adresses IP aux interfaces réseau :

- Interface WAN : par défaut (inutile ici).
- Interface LAN : attribuer IP **172.16.0.1/24**. Cette adresse servira de **passerelle par défaut** pour les autres machines virtuelles connectées à VMnet9.

```
> ^CUMware Virtual Machine - Netgate Device ID: ffcfd66ca314f87cfe4a
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on PFS2 ***

WAN (wan)      -> le0      -> v4/DHCP4: 192.168.203.140/24
LAN (lan)      -> le1      -> v4: 10.75.20.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (le0 - dhcp, dhcp6)
2 - LAN (le1 - static)

Enter the number of the interface you wish to configure: █
```

```
6) Halt system          15) Restore recent configuration
7) Ping host            16) Restart PHP-FPM
8) Shell
```

Enter an option: 2

Available interfaces:

```
1 - WAN (le0 - dhcp, dhcp6)
2 - LAN (le1 - static)
```

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.16.0.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
255.255.0.0 = 16
255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24█

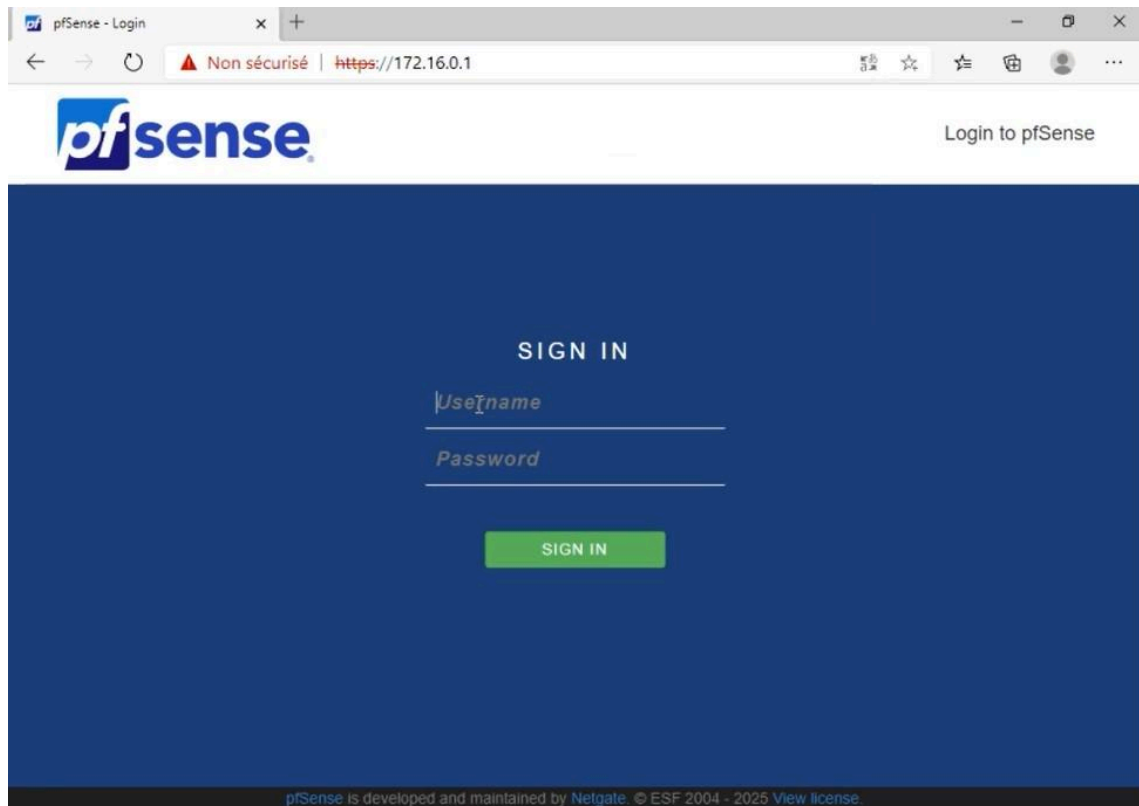
The IPv4 LAN address has been set to 172.16.0.1/24
You can now access the webConfigurator by opening the following URL in your web browser:

<https://172.16.0.1/>

Press <ENTER> to continue.█

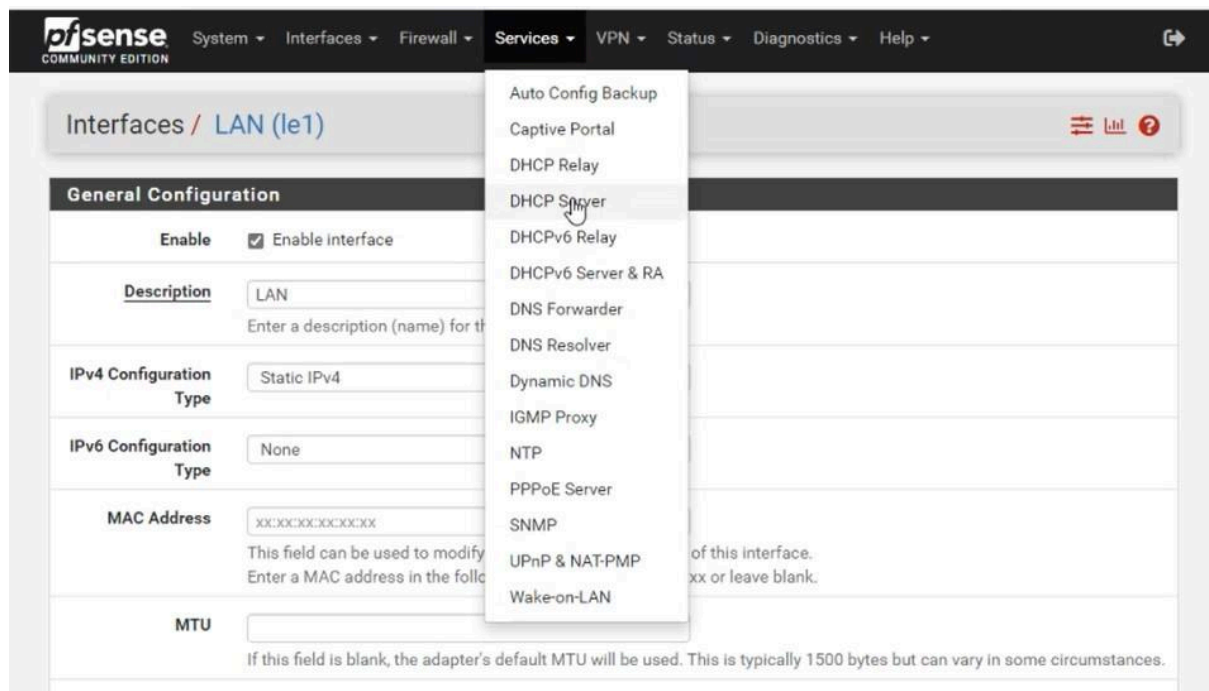
SECTION : Étape 2 – Activer le service DHCP

Il faut par la suite ouvrir un navigateur web sur le serveur et sur la barre de recherche y mettre l'adresse ip du routeur ici : **172.16.0.1** ;



Une fois connecté:

- Menu **Services > DHCP Server** sur l'interface LAN.



- Activer le DHCP pour la plage 172.16.0.10 à 172.16.0.100.

Deny unknown clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed in a static mapping on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.

Ignore denied clients ☐ Ignore denied clients rather than reject
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers ☐ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet 172.16.0.0

Subnet mask 255.255.255.0

Available range 172.16.0.1 - 172.16.0.254

Range
From To

- DNS primaire : 172.16.0.10 (le contrôleur de domaine).

Servers	
WINS servers	WINS Server 1
	WINS Server 2
DNS servers	172.16.0.13
	8.8.8.8
	DNS Server 3
	DNS Server 4

Après on enregistre les configurations:

Services / DHCP Server / LAN

The changes have been applied successfully.

SECTION : 4. Configuration de la station cliente Windows 10 (POSTE)

Cette machine représente un utilisateur standard du réseau. Elle doit être correctement configurée pour rejoindre le domaine `test.fr` et accéder aux services AD/DNS.

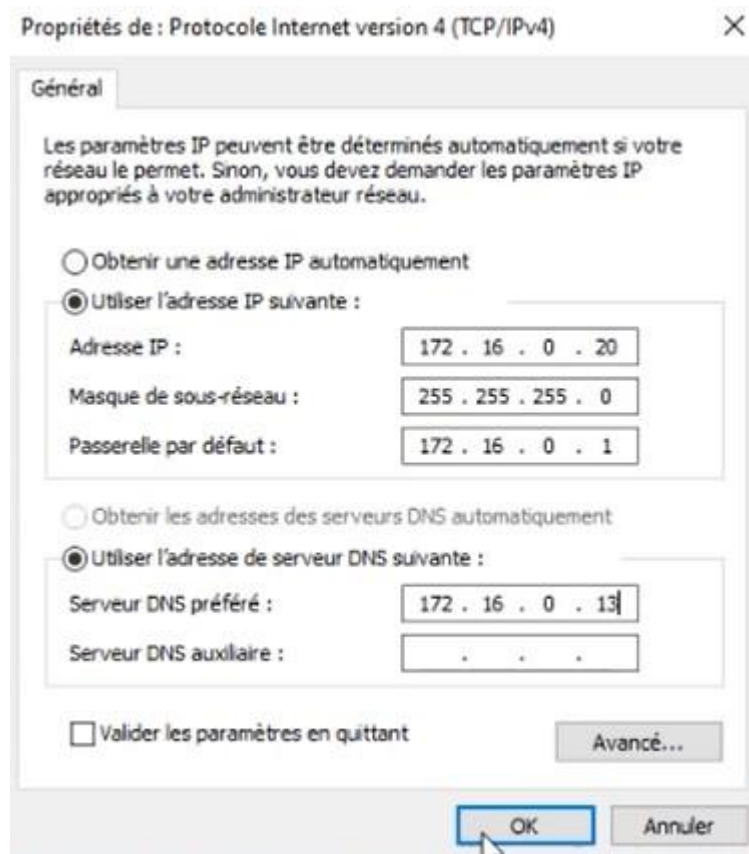
Étape 1 – Affectation IP statique temporaire

Avant de pouvoir intégrer le domaine, il est nécessaire de configurer manuellement une adresse IP pour permettre la communication avec le serveur DCS

→ Ouvrir `ncpa.cpl` pour accéder aux propriétés réseau.
Configurer les paramètres suivants :

- Configurer l'IP statique depuis `ncpa.cpl` :

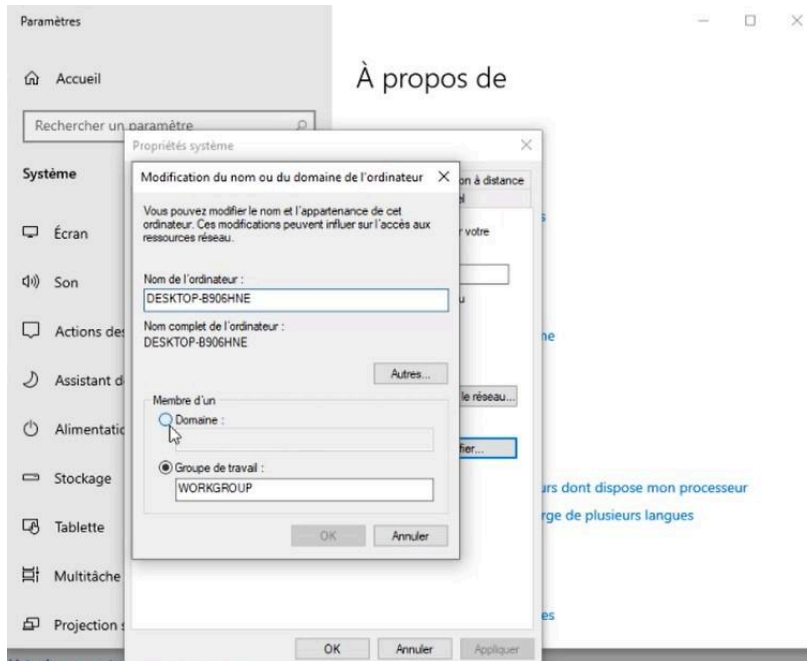
- IP : `172.16.0.20`
- Passerelle : `172.16.0.1`
- DNS : `172.16.0.10`



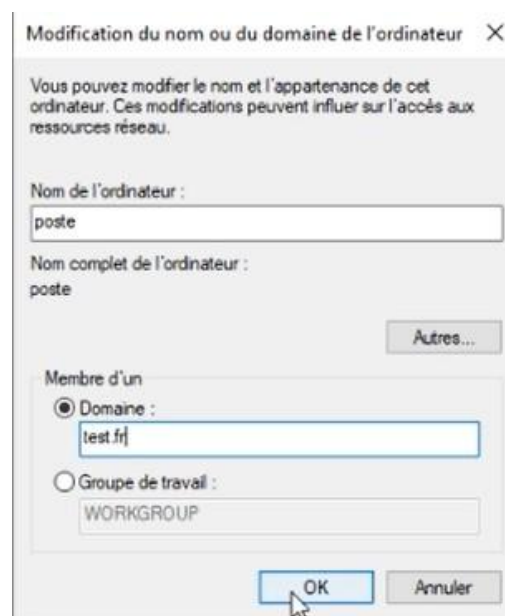
👉 Cela garantit que POSTE peut contacter le serveur DCS pour rejoindre le domaine

Étape 2 – Intégration au domaine

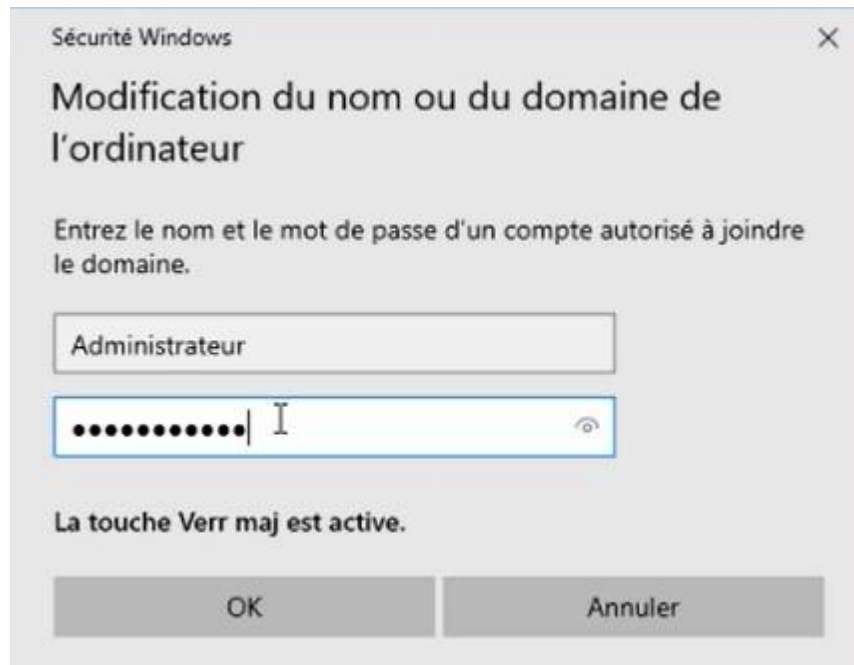
- Clic droit sur **Ce PC > Propriétés > Paramètres système avancés** ou **sysdm.cpl**.
- Cliquer sur **Modifier le nom de l'ordinateur > Cocher "Domaine"**.



- Saisir : **test.fr**

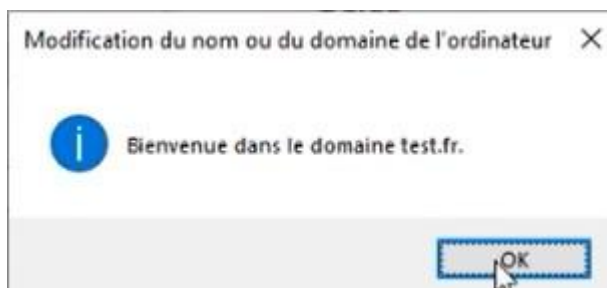


- Lorsqu'on demande des identifiants, entrer un **compte administrateur du domaine**



👉 Si les paramètres réseau sont corrects, l'intégration se fait sans erreur.

Résultat:



✅ Un message de bienvenue s'affiche : *"Bienvenue dans le domaine test.fr"*.

- 🔄 **Redémarrer la machine** après l'intégration.

Étape 4 – Repasser l'IP en automatique (DHCP)


Une fois intégré, il est recommandé de laisser pfSense gérer l'adressage IP via DHCP

➡ Retourner dans `ncpa.cp1`, puis :

- Mettre **"Obtenir une adresse IP automatiquement"**
- Mettre **"Obtenir l'adresse du serveur DNS automatiquement"**



👉 Au redémarrage, POSTE doit recevoir une IP de la plage `172.16.0.10` à `172.16.0.100`

-  **Vérification** : Ouvrir une invite de commande (cmd) et taper **ipconfig** pour confirmer l'attribution dynamique de l'IP

```
Carte Ethernet Ethernet0 :  
  
Suffixe DNS propre à la connexion. . . : home.arpa  
Description. . . . . : Intel(R) 82574L Gigabit Network Connection  
Adresse physique . . . . . : 00-0C-29-9D-49-35  
DHCP activé. . . . . : Oui  
Configuration automatique activée. . . : Oui  
Adresse IPv6 de liaison locale. . . . : fe80::507d:5eff:1bd0:418d%3(préféré)  
Adresse IPv4. . . . . : 172.16.0.10(préféré)  
Masque de sous-réseau. . . . . : 255.255.255.0  
Bail obtenu. . . . . : dimanche 13 avril 2025 12:37:21  
Bail expirant. . . . . : dimanche 13 avril 2025 14:37:22  
Passerelle par défaut. . . . . : 172.16.0.1  
Serveur DHCP . . . . . : 172.16.0.1  
IAID DHCPv6 . . . . . : 100666409  
DUID de client DHCPv6. . . . . : 00-01-00-01-2F-86-DE-A9-00-0C-29-9D-49-35  
Serveurs DNS. . . . . : 172.16.0.13  
                        8.8.8.8  
NetBIOS sur Tcpi. . . . . : Activé
```

PF52.home.arpa - Status: DHCP | x +

Non sécurisé | https://172.16.0.1/status_dhcp_leases.php

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Status / DHCP Leases

Search

Search term All

Enter a search string or *nix regular expression to filter entries.

Leases

IP address	MAC address	Client Id	Hostname	Description	Start	End	Online	Lease Type	Actions
✓ 172.16.0.10	00:0c:29:9d:49:35		poste		2025/04/08 14:10:26	2025/04/08 16:10:26	↑ active	active	<input type="button" value="+"/> <input type="button" value="+"/>

Leases in Use

Interface	Pool Start	Pool End	# of leases in use
LAN	172.16.0.10	172.16.0.100	1

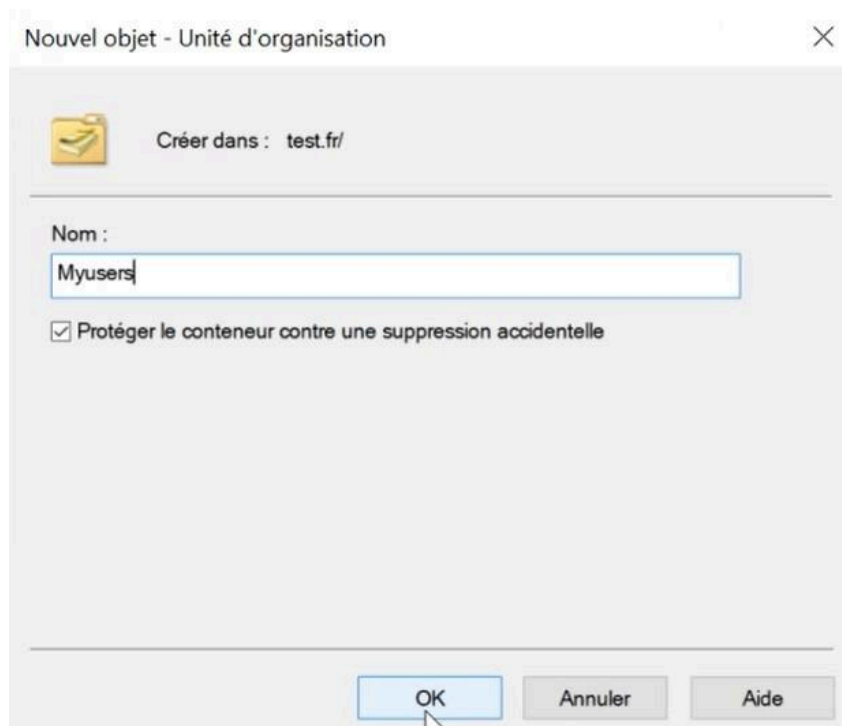
SECTION : 5. Création des utilisateurs et partages

L'objectif ici est de créer une unité d'organisation (UO) dans Active Directory, d'ajouter un utilisateur et de lui accorder l'accès à un dossier partagé sur le serveur.

Étape 1 – Utilisateurs et groupes

➡ Depuis la console "**Utilisateurs et Ordinateurs Active Directory**" (dsa.msc) :

- Créer une Unité d'Organisation (UO) nommée: **Myusers**.



- Dans cette UO, créer un **utilisateur** nommé : **Mwindjou Mhoumadi**.

Nouvel objet - Utilisateur

Créer dans : test.fr/Myusers

Prénom : Mwindjou Initiales :

Nom : Mhoumadi

Nom complet : Mwindjou Mhoumadi

Nom d'ouverture de session de l'utilisateur :
mwindjou.mhoumad@test.fr

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
TEST\ mwindjou.mhoumadi

< Précédent Suivant > Annuler

Nouvel objet - Utilisateur

Créer dans : test.fr/Myusers

Mot de passe :

Confirmer le mot de passe :

☐ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

☐ L'utilisateur ne peut pas changer de mot de passe

☒ Le mot de passe n'expire jamais

☐ Le compte est désactivé

< Précédent Suivant > Annuler

Nouvel objet - Utilisateur

Créer dans : test.fr/Myusers

Quand vous cliquerez sur Terminer, l'objet suivant sera créé :

Nom complet : Mwindjou Mhoumadi

Nom de connexion de l'utilisateur : mwindjou.mhoumadi@test.fr

Le mot de passe n'expire jamais.

< Précédent Terminer Annuler

- Créer un groupe de sécurité nommé: **Commun**.

Nouvel objet - Groupe

Créer dans : test.fr/Myusers

Nom du groupe :
Commun

Nom de groupe (antérieur à Windows 2000) :
Commun

Étendue du groupe

☐ Domaine local

☒ Globale

☐ Universelle

Type de groupe

☒ Sécurité

☐ Distribution

OK Annuler

- Insérer l'utilisateur crée dans le groupe de sécurité **Commun**.

Propriétés de : Commun

Général Membres Membre de Géré par

Commun

Nom de groupe (antérieur à Windows 2000) : Commun

Description :

Adresse de messagerie :

Étendue du groupe

☐ Domaine local

☒ Globale

☐ Universelle

Type de groupe

☒ Sécurité

☐ Distribution

Remarques :

OK Annuler Appliquer

Propriétés de : Commun

Général Membres Membre de Géré par

Membres :

Nom	Dossier Services de domaine Active Directory
-----	--

Ajouter... Supprimer

OK Annuler Appliquer

Sélectionnez des utilisateurs, des contacts, des ordinateurs, des comptes de service ou des... ✕

Sélectionnez le type de cet objet :

des utilisateurs, des comptes de service, des groupes ou Autres objets Types d'objets...

À partir de cet emplacement :

test.fr Emplacements...

Entrez les noms des objets à sélectionner (exemples) :


Mwindjou Mhoumadi (mwindjou.mhoumadi@test.fr) Vérifier les noms

Avancé... OK Annuler

Propriétés de : Commun ? ✕

Général Membre de Géré par

Membres :

Nom	Dossier Services de domaine Active Directory
 Mwindjou Mh...	test.fr/Myusers

Ajouter... Supprimer

OK Annuler Appliquer

👉 Cette organisation facilite la gestion des droits d'accès et des stratégies à appliquer

Étape 2 – Dossier partagé

- Créer un dossier nommé **Commun** à la racine du disque **C :** sur DCS

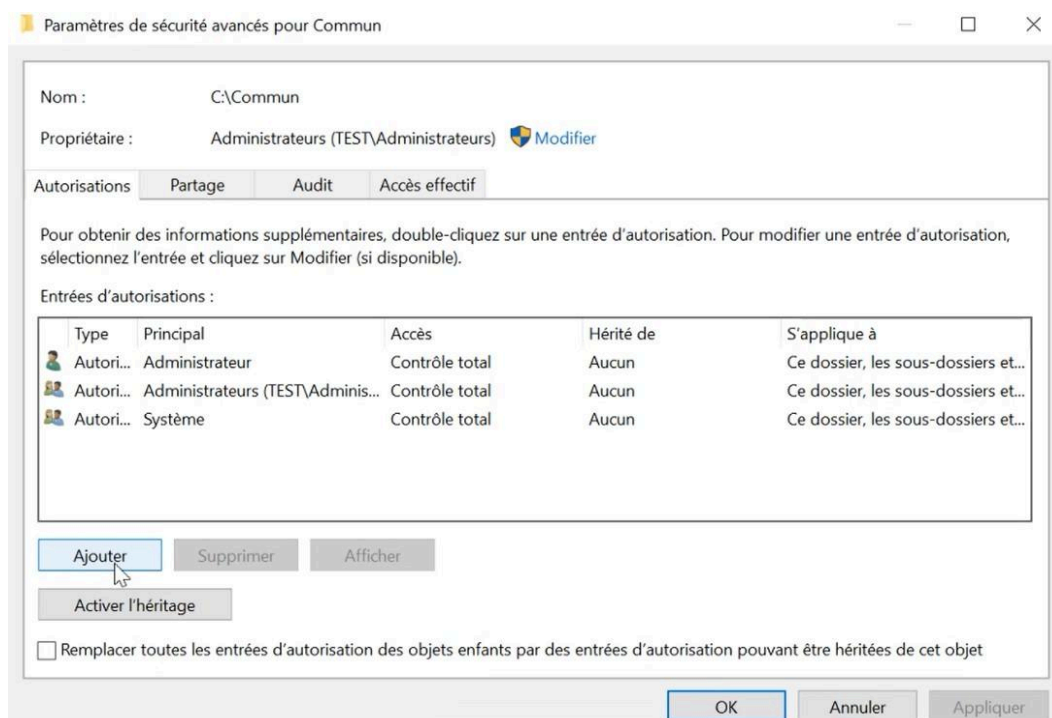
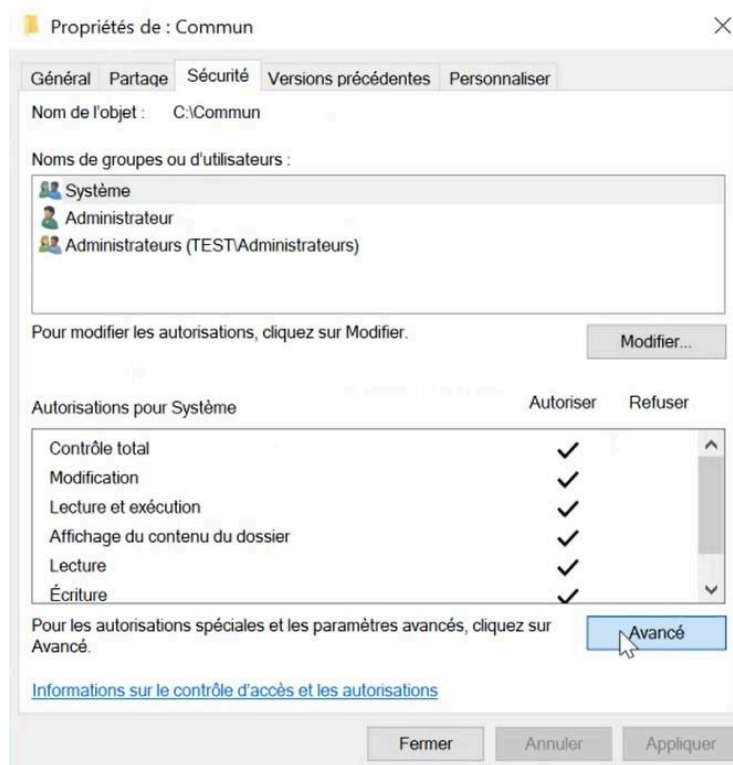
Faire un clic droit > **Propriétés** > **Partage** > **Partage avancé**

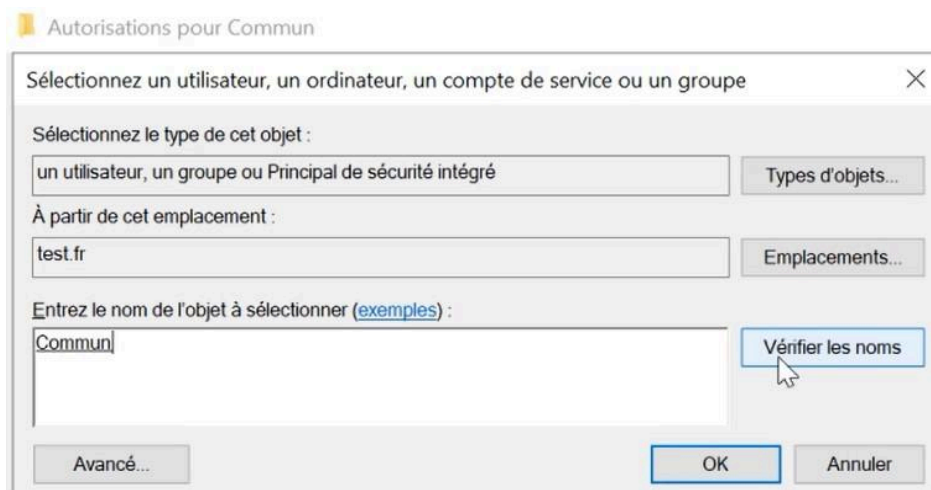
- Cocher **Partager ce dossier**
- Donner les autorisations au groupe **Commun**



Dans l'onglet **Sécurité** (NTFS) :

- Ajouter le groupe **Commun**
- Donner les **droits de lecture/écriture**



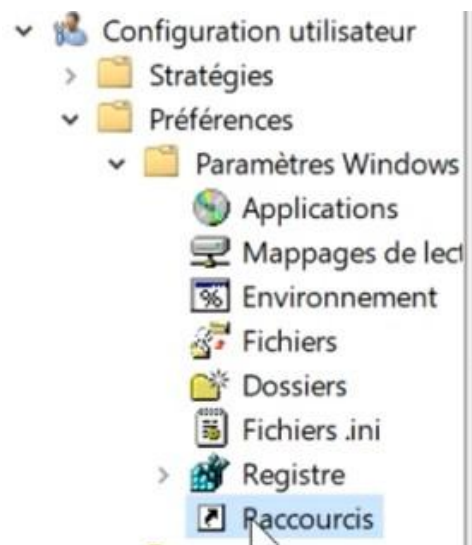
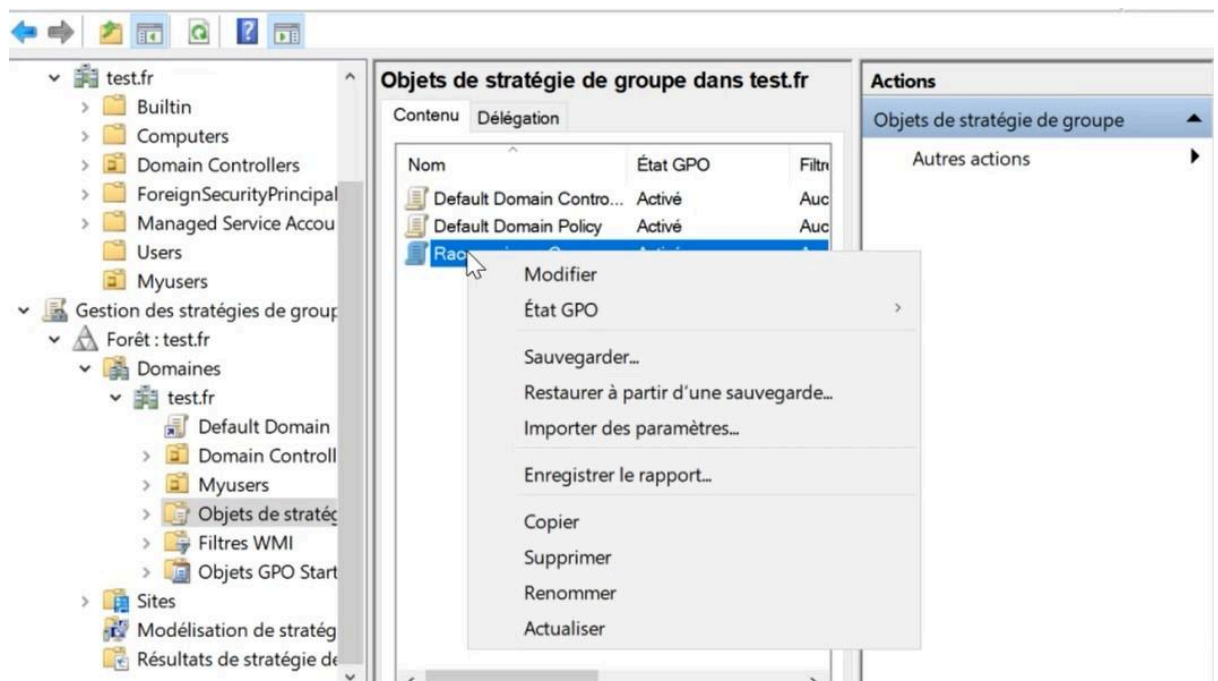
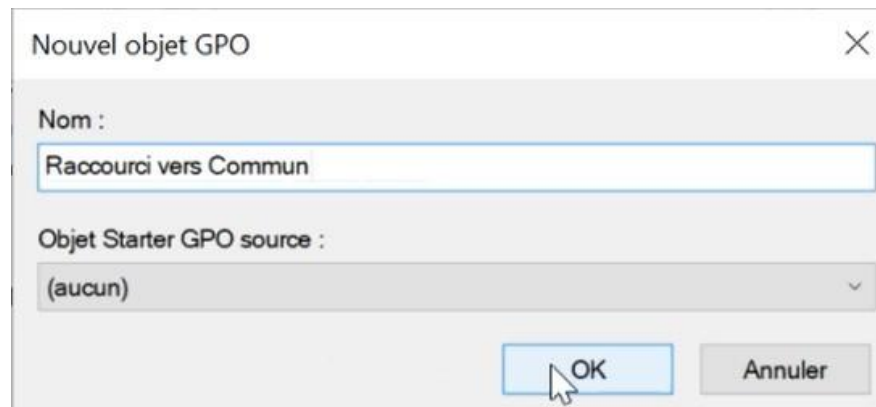


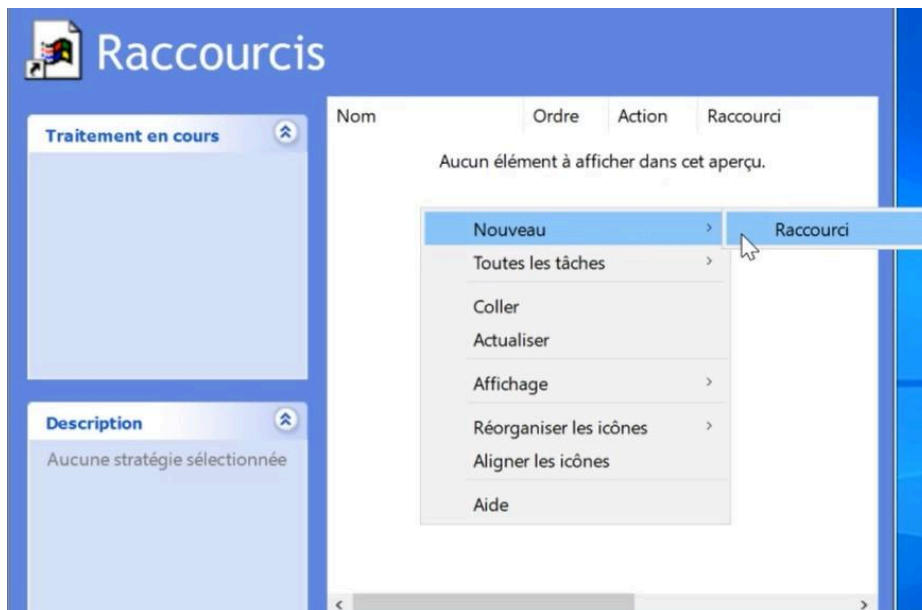
SECTION : 6. Raccourcis et scripts

Étape 1 – Raccourci vers le dossier partagé Commun:

Pour simplifier l'accès des utilisateurs au partage réseau :

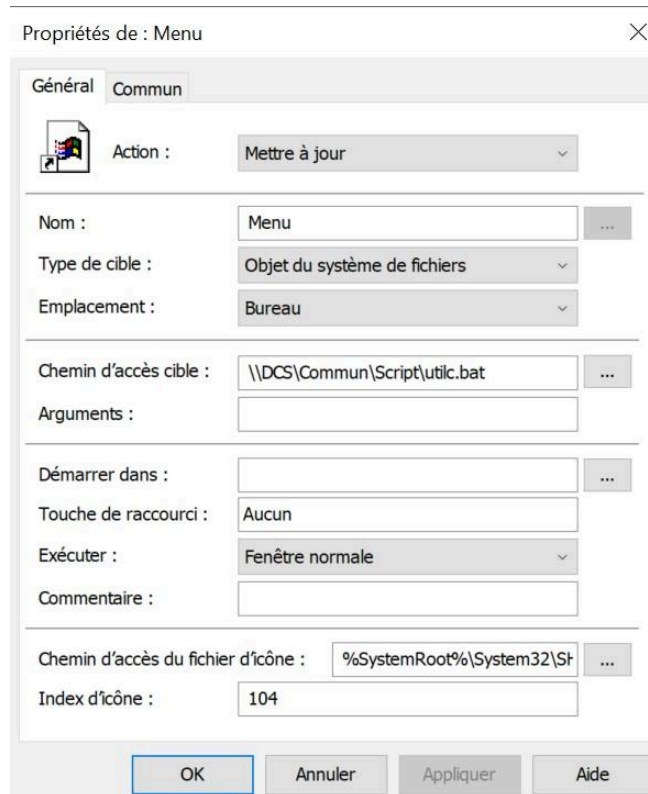
1. Depuis POSTE, se connecter avec le compte `test\Mwindjou`.
2. Créer un **raccourci sur le bureau** vers le dossier réseau :
 - Chemin UNC : `\\dcs\Commun`





Étape 2 – Script menu.bat

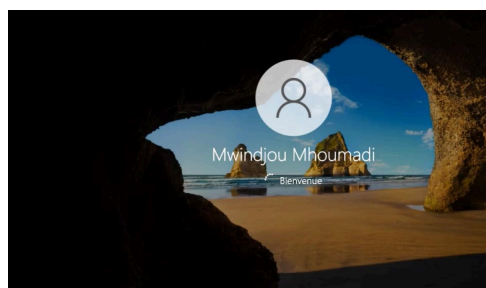
- Créer un raccourci sur le bureau vers ce script.

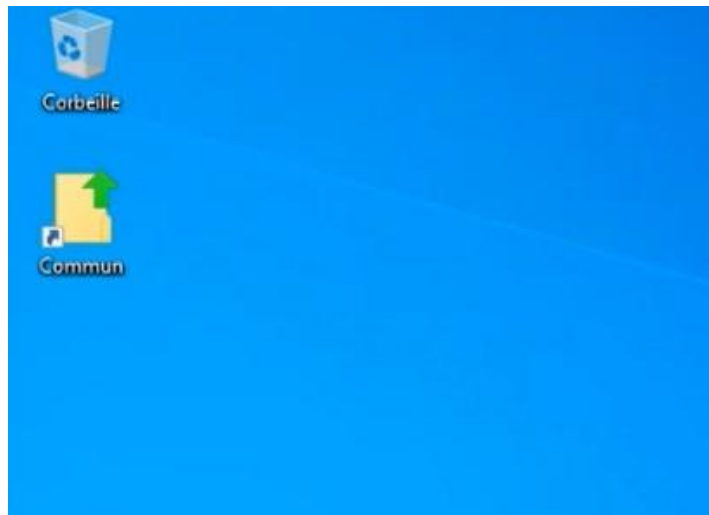


✓ SECTION : 7. Test et vérifications

Une fois toutes les configurations faites, il est important de **tester le bon fonctionnement de l'ensemble**.

➡ Sur **POSTE**, se connecter avec l'utilisateur **test\Mwindjou**.





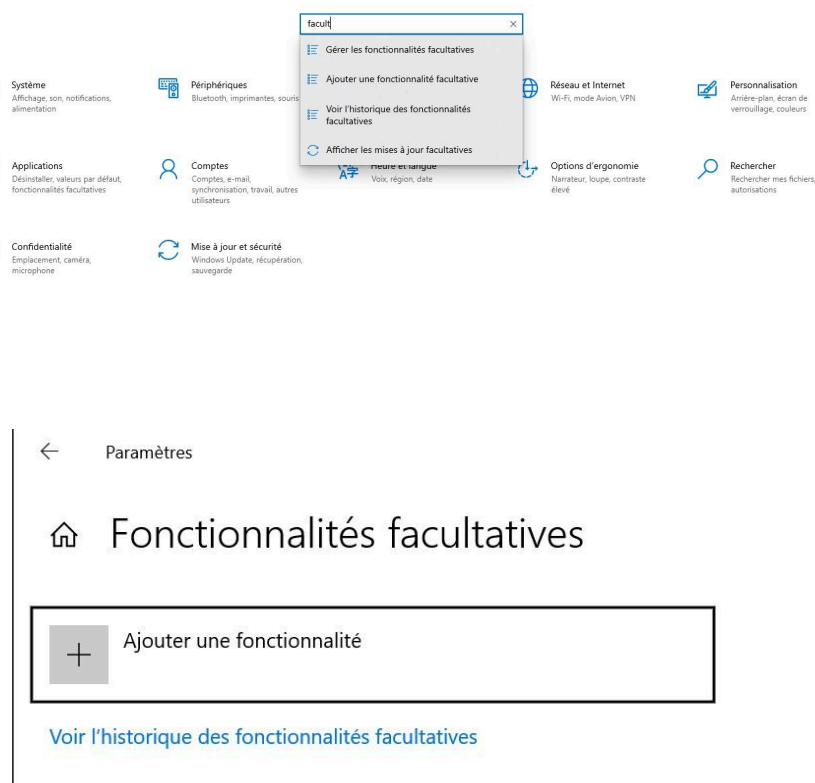
👉 Cela valide que les autorisations de groupe fonctionnent correctement.

SECTION: 8. RSAT (Remote Server Administration Tools)

RSAT permet d'administrer à distance les rôles du serveur Active Directory depuis un autre poste client (POSTE ici)

Installation :

1. Ouvrir **Paramètres > Applications > Fonctionnalités facultatives**
2. Cliquer sur **Ajouter une fonctionnalité**
3. Rechercher et installer :
 - **RSAT: Outils d'administration AD DS**
 - **RSAT: Outils DNS**
 - **RSAT: Outils de gestion des stratégies de groupe**



Ajouter une fonctionnalité facultative

Rechercher une fonctionnalité facultative disponible



Trier par : Nom ▼

<input type="checkbox"/>			
<input type="checkbox"/>		RSAT : client Gestion des adresses IP (IPAM)	226 Ko
<input type="checkbox"/>		RSAT : module Informations système pour Windows PowerShell	55,0 Ko
<input checked="" type="checkbox"/>		RSAT : outils Active Directory Domain Services Directory et services LDS (Lightweight Directory Services)	4,98 Mo

Ajouter une fonctionnalité facultative

Rechercher une fonctionnalité facultative disponible



Trier par : Nom ▼

<input type="checkbox"/>		RSAT : outils de gestion de l'accès à distance	6,70 Mo
<input checked="" type="checkbox"/>		RSAT : outils de gestion de stratégie de groupe	4,07 Mo
<input type="checkbox"/>		RSAT : outils de gestion du contrôleur de réseau	164 Ko
<input type="checkbox"/>		RSAT : outils de services de fichiers	5,07 Mo
<input type="checkbox"/>		RSAT : outils des services Bureau à distance	953 Ko
<input type="checkbox"/>		RSAT : outils des services de certificats Active Directory	1,49 Mo
<input type="checkbox"/>		RSAT : outils du serveur DHCP	1,57 Mo
<input checked="" type="checkbox"/>		RSAT : outils du serveur DNS	1,27 Mo

Installer (3)




Annuler

← Paramètres

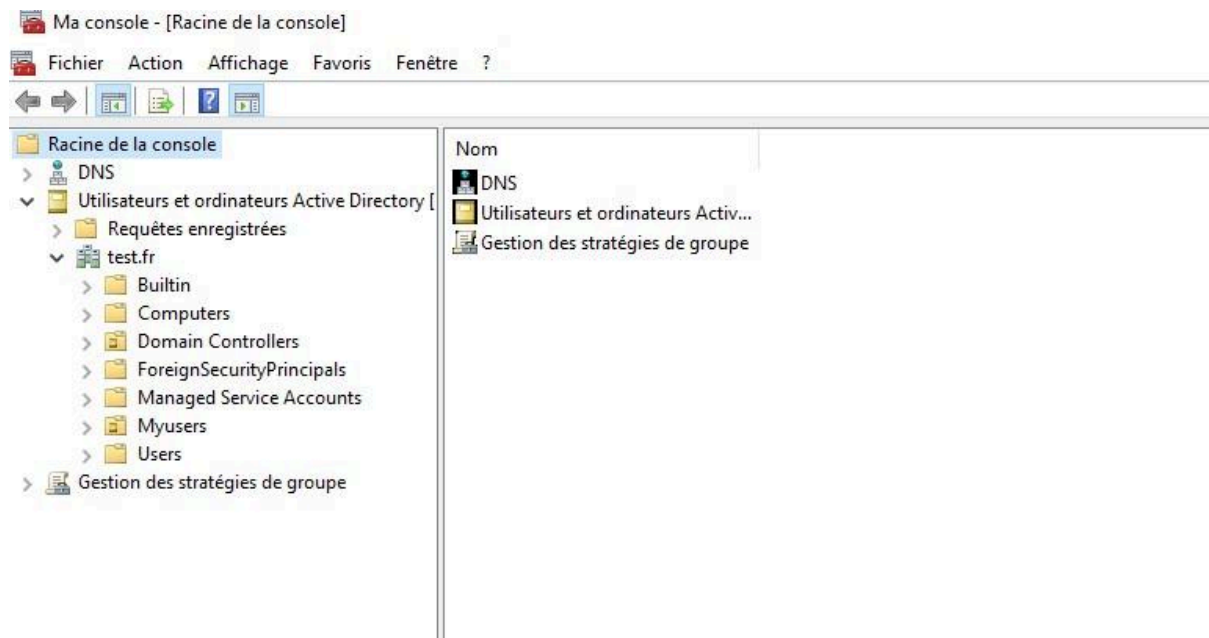
🏠 Fonctionnalités facultatives

+ Ajouter une fonctionnalité

Dernières actions

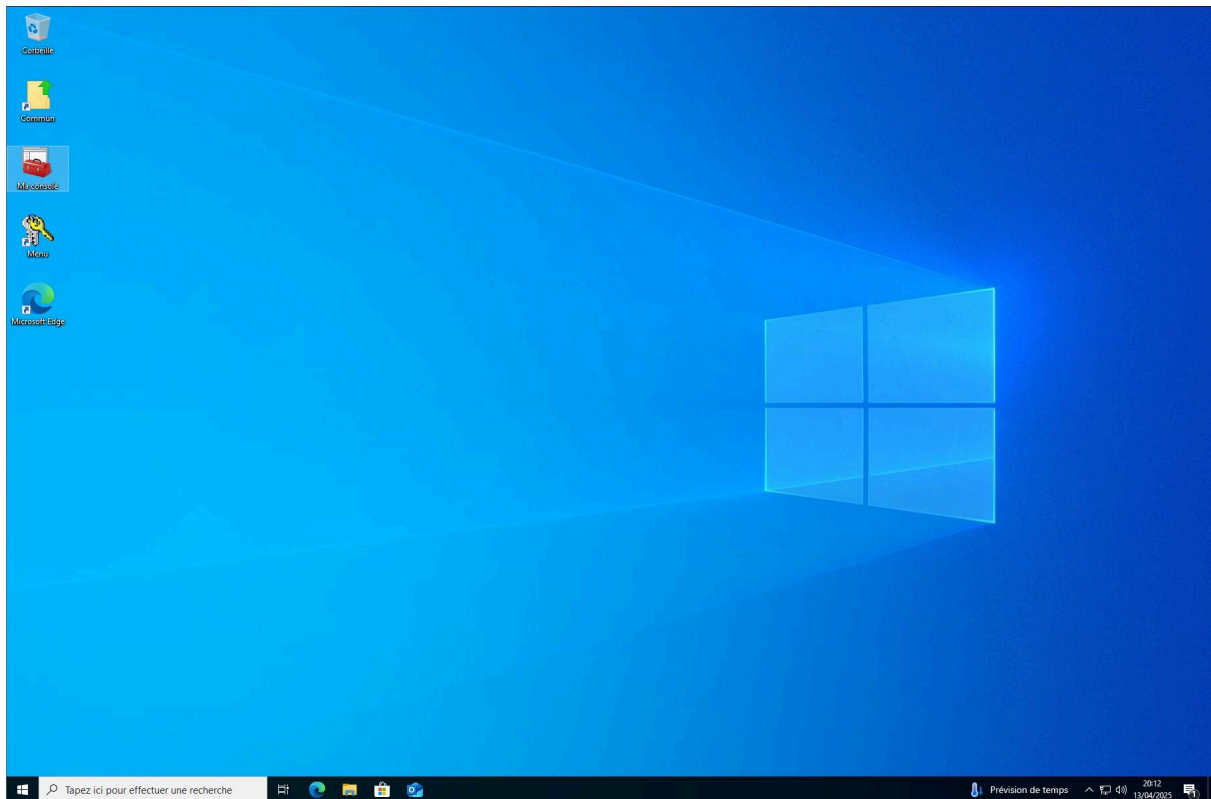
	RSAT : outils Active Directory Domain Services Directory et services LDS (Lightweight Directory Services)	Installé
	RSAT : outils de gestion de stratégie de groupe	Installé
	RSAT : outils du serveur DNS	Installé

Résultat:



👉 Cela permet de gérer les utilisateurs, les groupes, les stratégies et la configuration DNS sans se connecter directement sur DCS

Résultat final:



Conclusion

Ce projet permet de mettre en place un environnement Windows Server réaliste avec Active Directory, DNS, DHCP et gestion centralisée via RSAT. L'utilisation de pfSense pour la gestion réseau permet une meilleure maîtrise de l'infrastructure, notamment au niveau de l'adressage, du routage et du contrôle d'accès. L'ensemble du projet a été conçu pour être reproductible et facilement maintenable dans un contexte pédagogique ou professionnel.