

BTS SIO - EPREUVE E5

PROJET N°1

Yanis Mingam

KEYCE ACADEMY OGEC D'ALZON

Table des matières

I.	Mise en contexte	2
II.	Configuration du Routeur / Pare-Feu (PfSense).....	4
III.	Configuration du serveur principal (AD-DS).....	6
IV.	Création d'Unités d'Organisation (UO) et création d'utilisateurs	9
V.	Configuration des machines clientes (Windows 11).....	12
VI.	Mise en place de dossiers partagés selon l'UO (secrétariat, RH, comptabilité, etc).....	14
VII.	Mise en place de GPO spécifiques	17
VIII.	Configuration du serveur de redondance	18
IX.	Configuration avancée du Routeur / Pare-Feu PfSense (DHCP, règles de filtrage, vlan).....	22

I. Mise en contexte

L'établissement scolaire Poudlard va ouvrir ses portes. Devant accueillir un nombre assez élevé de personnel, administratif et pédagogique, mais aussi d'élèves / étudiants, il est nécessaire de mettre en place un parc informatique capable de gérer cette forte demande.

C'est dans ce contexte que cet établissement fait appel à notre société « Mingam Corp. ». Avant toute chose, il faut considérer les moyens dont Poudlard dispose afin de le rapporter aux besoins évoqués et ainsi trouver des solutions adaptées.

Ne générant pas de revenus, l'école vit et se développe grâce aux subventions et à l'investissement de l'Education Nationale. En partant de ce principe, on tentera au maximum de privilégier des solutions gratuites.

Voici le plan de l'infrastructure :

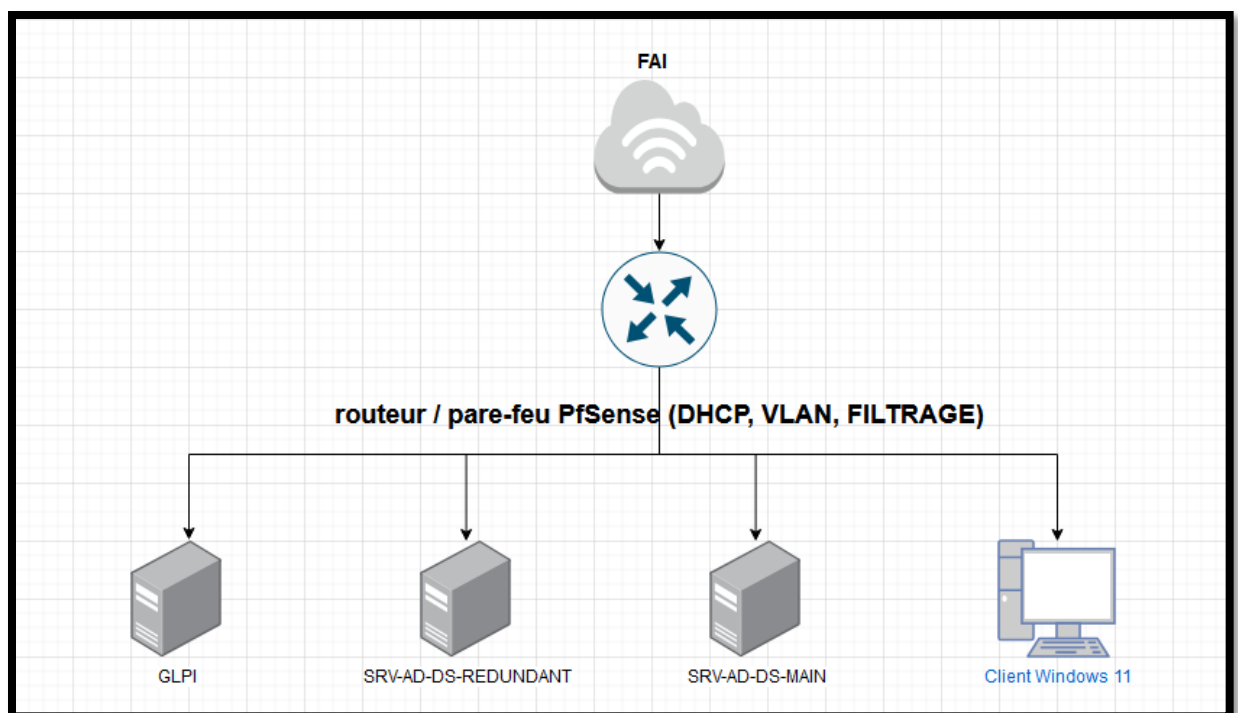


Figure 1 - Schéma de l'infrastructure

Le Schéma ci-dessus présente les composantes de l'infrastructure qui va être mise en place au sein de l'établissement. On y retrouve les éléments suivants :

- Un routeur / Pare-Feu PfSense qui permet de fournir un accès à internet aux machines du réseau tout en filtrant le trafic, en distribuant par exemple des adresses IP.
- Un serveur Active Directory (AD) sous Windows Server 2022 permettant entre-autre de gérer efficacement un grand nombre d'utilisateurs ainsi que leurs spécificités.
- Un serveur redondant qui réplique en temps réel le serveur AD afin de pouvoir assurer une continuité des services en cas de panne du serveur dit « principal ».
- Un serveur GLPI, permettant de mettre en place un système de tickets, ainsi qu'un inventaire automatique du matériel (PC, écrans, vidéoprojecteurs, etc...).
- Une machine client Windows 11, faisant partie du domaine de l'AD.

On a aussi le tableau d'adresses IP :

Nom	Adresse
Routeur / Pare-Feu (PfSense)	192.168.100.1
SRV-AD-DS-MAIN	192.168.100.2
SRV-AD-DS-REDUNDANT	192.168.100.3
GLPI	192.168.100.5
Poste Client	DHCP

Figure 2 - Tableau d'adresses IP

Le routeur / pare-feu se situe entre le FAI et le réseau local de Poudlard. Les adresses des serveurs sont toujours fixes, car il faut pouvoir interagir en permanence avec eux. Quant au poste client, il obtiendra une adresse via le DHCP.

II. Configuration du Routeur / Pare-Feu (PfSense)

La configuration WAN est la première étape lorsque l'on configure un routeur / pare-feu PfSense. On lui permet de récupérer une adresse via le DHCP sur le réseau du FAI, afin que le routeur puisse être un intermédiaire entre le FAI et le réseau local.

Voici la configuration de l'interface WAN du routeur / pare-feu :

```
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 (em0 - dhcp)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) y
Configure IPv6 address WAN interface via DHCP? (y/n) n
Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

Figure 3 - Configuration de l'interface WAN

En passant par le DHCP, l'interface WAN récupère automatiquement une adresse IP, comme vu sur la figure 3

La deuxième étape lors de la configuration PfSense consiste en l'attribution d'une adresse IP pour l'interface LAN. L'adresse IP de cette interface va déterminer l'adresse du réseau local de Poudlard. Dans notre cas, on décide que le réseau local de l'école sera **192.168.100.0** et que l'adresse de l'interface LAN de PfSense sera **192.168.100.1/24**.

Voici la configuration de l'interface LAN du routeur / pare-feu :

```
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:
> 192.168.100.1
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
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on LAN? (y/n) n
```

Figure 4 - Configuration de l'interface LAN

A présent, l'interface web de PfSense doit être disponible depuis n'importe quelle machine du réseau local de Poudlard à l'adresse de l'interface LAN, soit **192.168.100.1**.

III. Configuration du serveur principal (AD-DS)

Lors du premier démarrage, il y a un certain nombre de choses à configurer pour que le serveur ADDS soit fonctionnel. En premier lieu, on ajoute les services Active Directory et DNS:

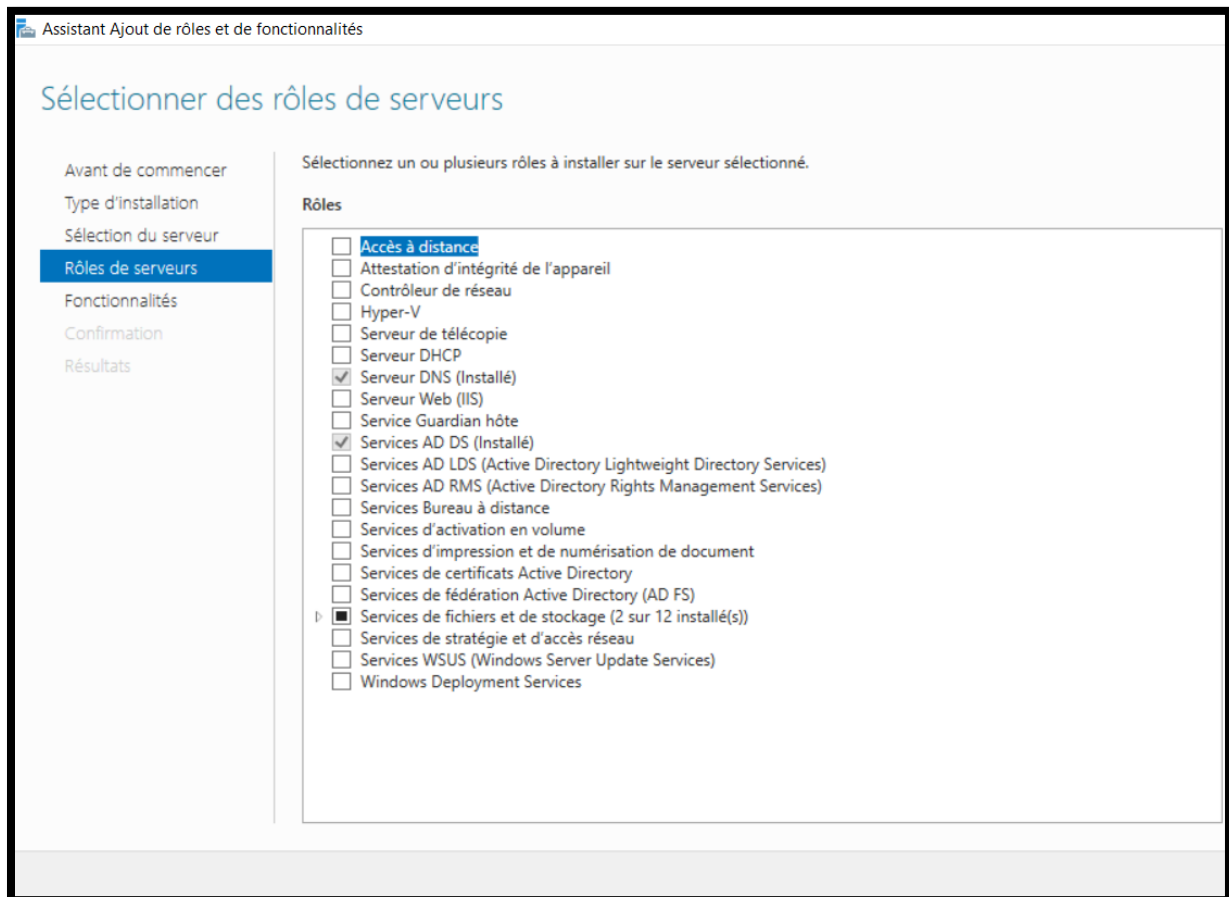


Figure 5 - Installation services AD DS et DNS

Une fois ces services installés, il faut promouvoir le serveur en contrôleur de domaine comme indiqué ci-dessous :

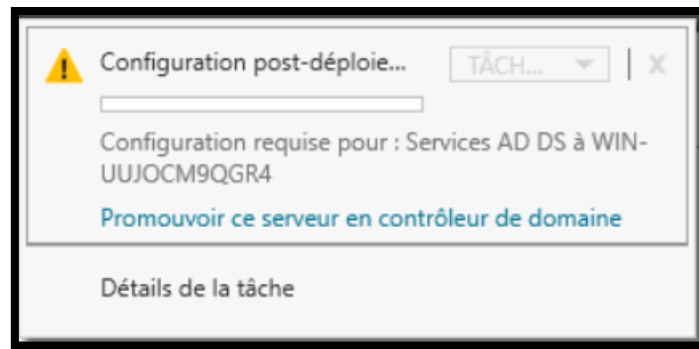


Figure 6 - Promotion du serveur en contrôleur de domaine (1)

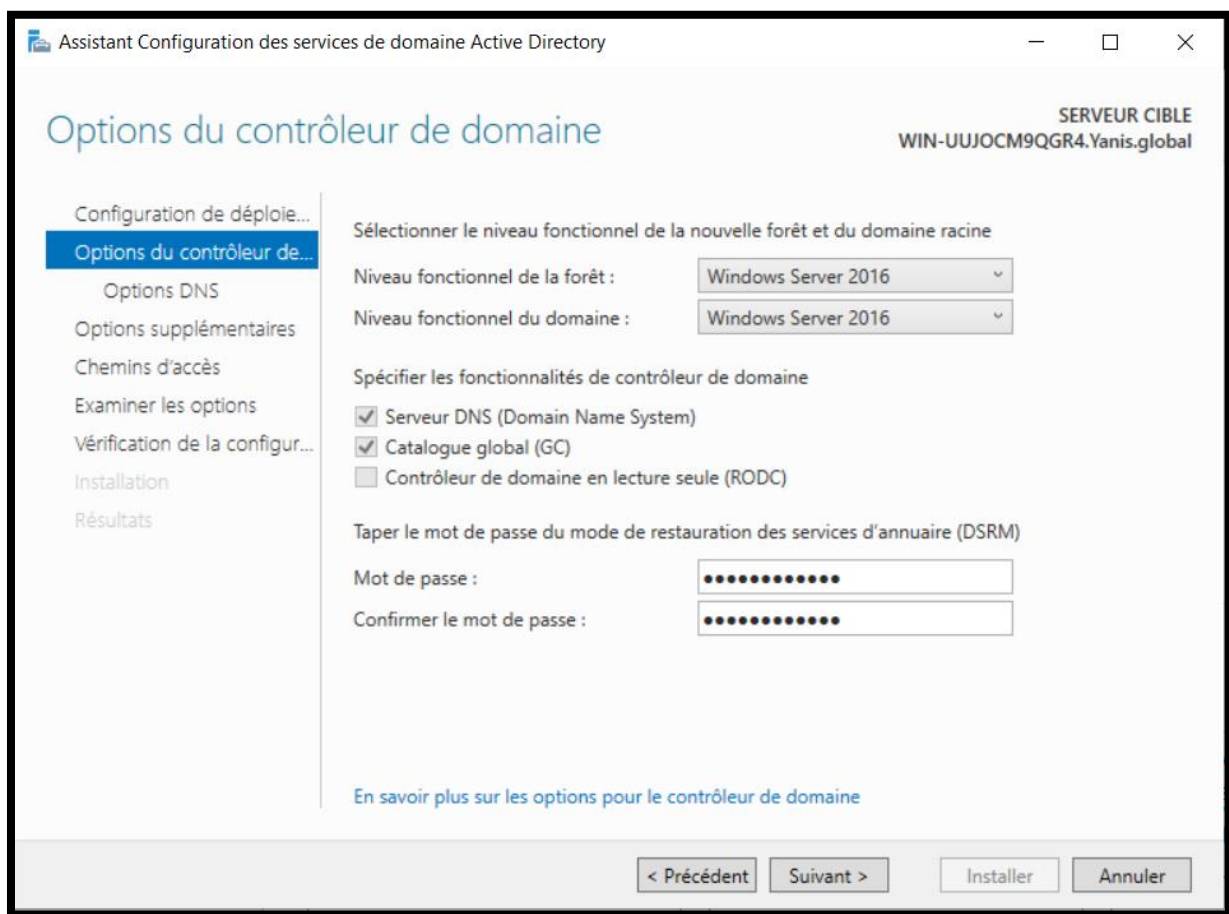


Figure 7 – Promotion du serveur en contrôleur de domaine (2)

Le serveur ADDS a maintenant le rôle de contrôleur de domaine. Il lui suffit de redémarrer afin d'être fonctionnel :

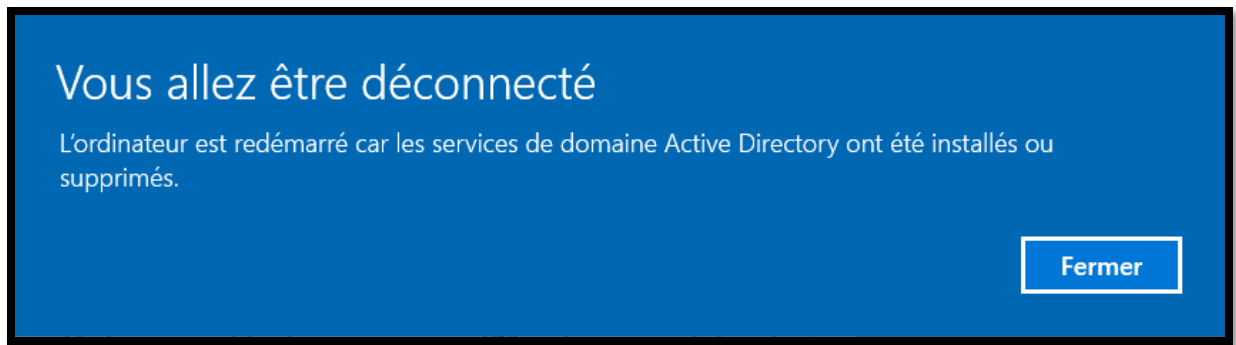


Figure 8 - Le serveur redémarre

IV. Création d'Unités d'Organisation (UO) et création d'utilisateurs

Maintenant, que le contrôleur de domaine est fonctionnel, on peut créer des Unités d'Organisations ainsi que des utilisateurs. L'avantage des UO, c'est qu'elles permettent de regrouper des utilisateurs et / ou des postes afin de pouvoir leur attribuer des règles spécifiques.

Dans « Utilisateurs et ordinateurs Active Directory », on vient créer les comptes utilisateurs et les UO :

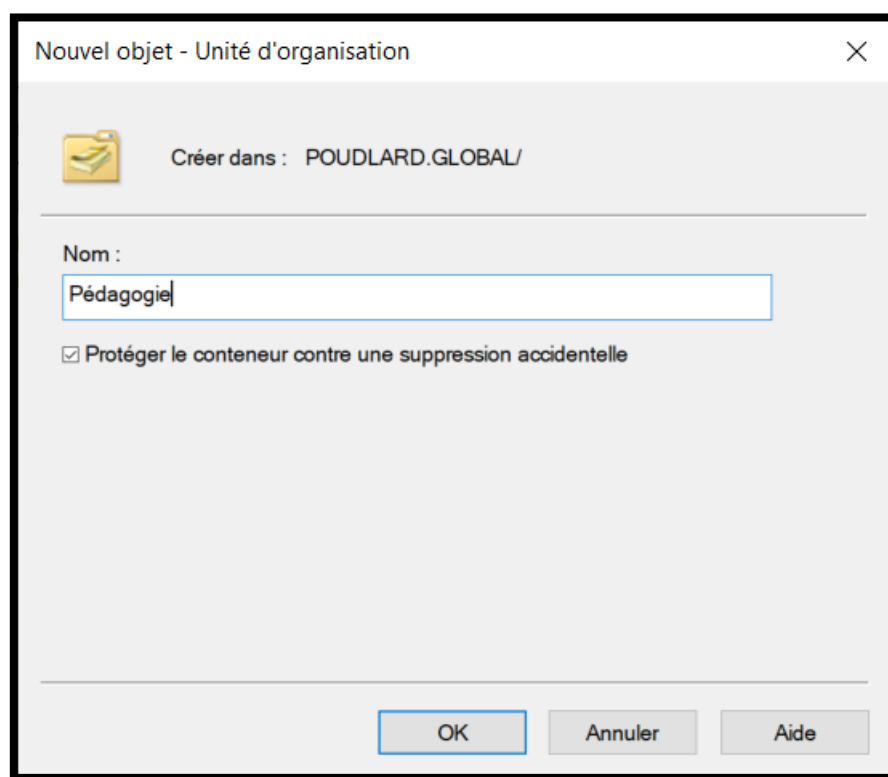


Figure 9 - Création d'une UO Pédagogie

Pour les identifiants utilisateurs, on utilise la première lettre du prénom suivie du nom de famille (voir Figure 10)

Nouvel objet - Utilisateur

Créer dans : POUDLARD.GLOBAL/Pédagogie

Prénom : Sylvie Initiales :

Nom : Tapie

Nom complet : Sylvie Tapie

Nom d'ouverture de session de l'utilisateur :
stapie @POUDLARD.GLOBAL

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
POUDLARD\stapie

< Précédent Suivant > Annuler

Figure 10 - Création d'un utilisateur dans l'UO Pédagogie

Afin de faciliter la gestion des utilisateurs, on va créer deux UO principales. Une première UO pour la partie pédagogique, une seconde pour le personnel administratif.

Au sein de cette UO, on y crée des UO secondaires : Secrétariat et RH

L'arborescence ressemble donc à cela :

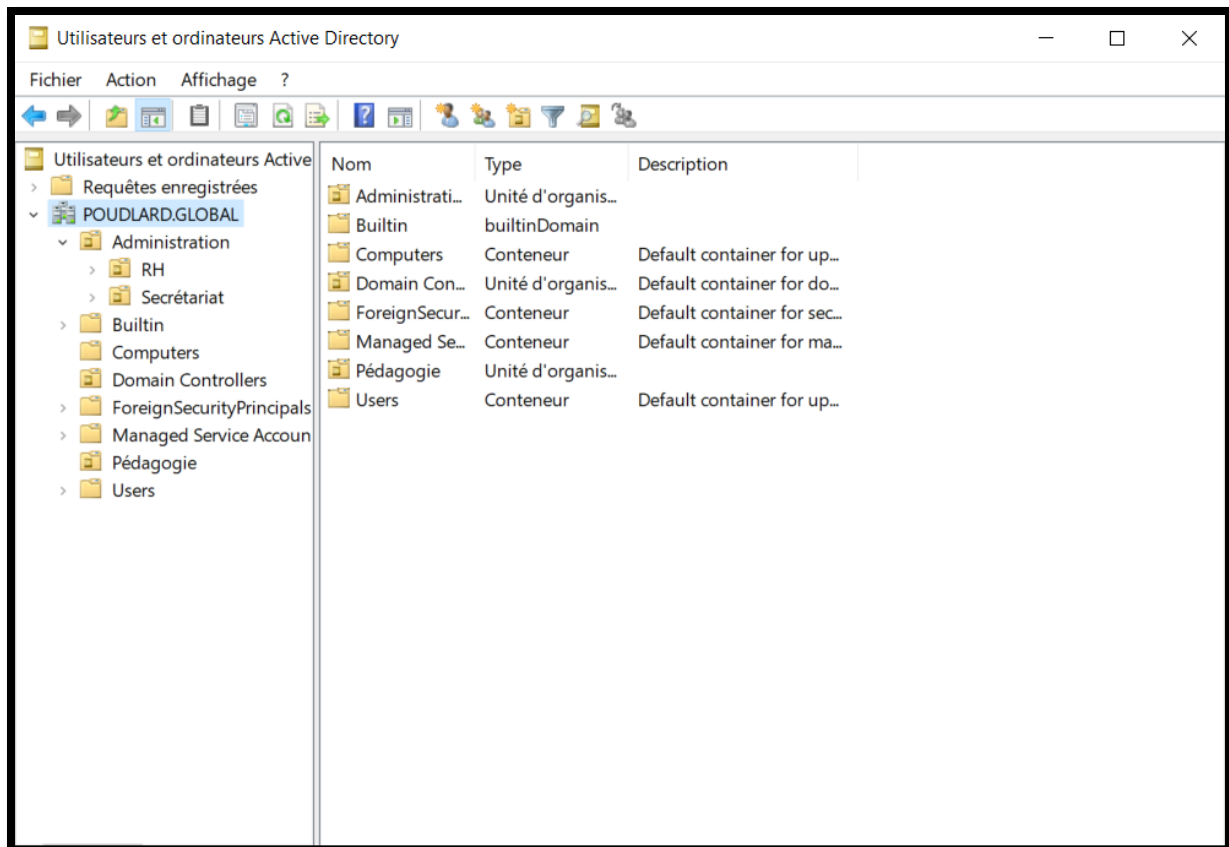


Figure 11 - Arborescence des UO et utilisateurs

Lorsque l'on ajoutera une machine dans le domaine, elle sera placée par défaut dans l'UO « **Computers** » en attendant d'être déplacée dans la bonne UO

V. Configuration des machines clientes (Windows 11)

Lors du démarrage de la machine client, il faut l'ajouter dans le domaine. Le domaine étant « **Poudlard** ».

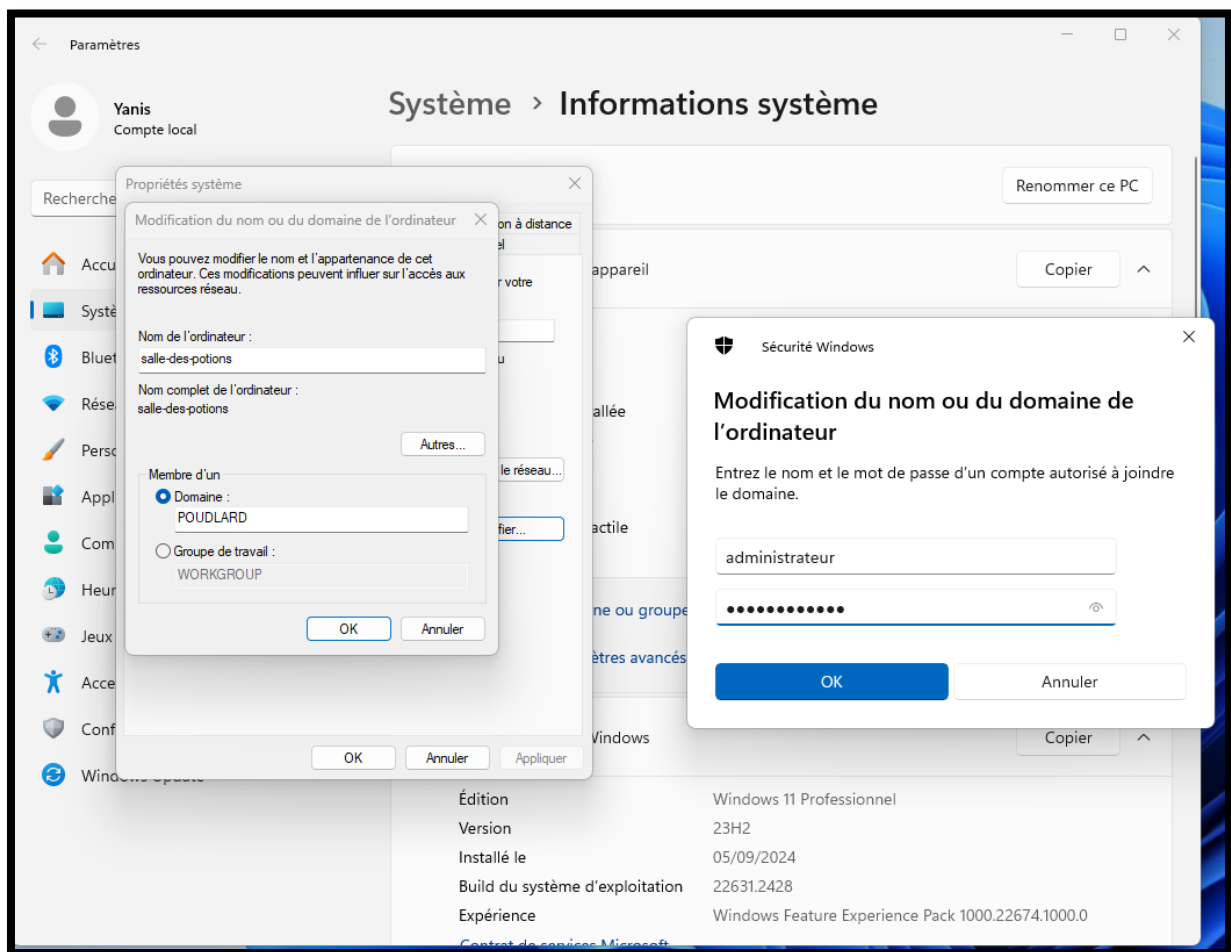


Figure 12 - Ajout de la machine au domaine

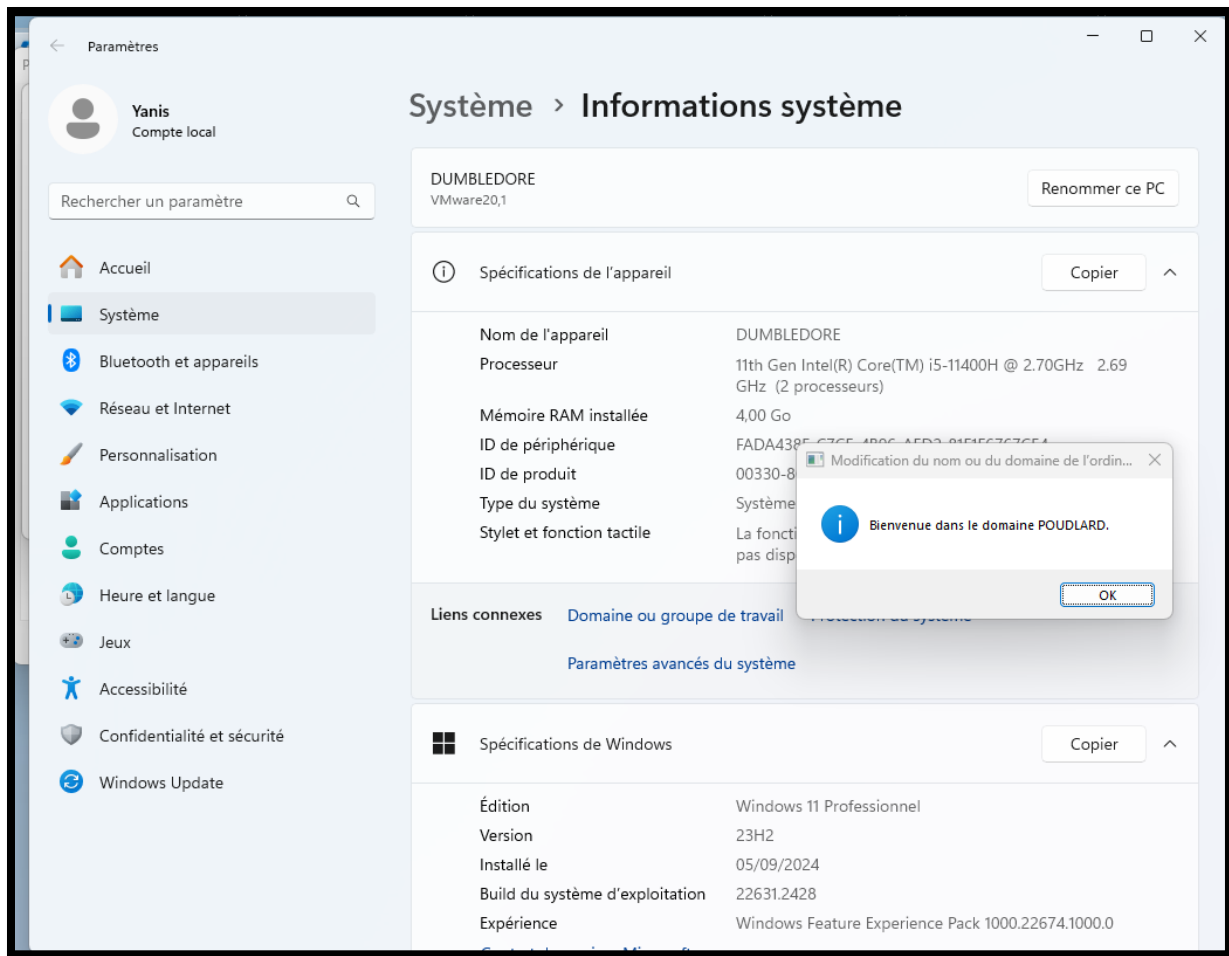


Figure 13 - Ajout dans le domaine effectif

La machine est maintenant ajoutée au domaine. Il est possible pour n'importe quel utilisateur du domaine de se connecter à la machine. Elle va redémarrer pour prendre en compte les changements

VI. Mise en place de dossiers partagés selon l'UO (secrétariat, RH, comptabilité, etc...)

On crée un dossier qui va contenir les fichiers du service RH de l'établissement que l'on va partager sur le réseau :

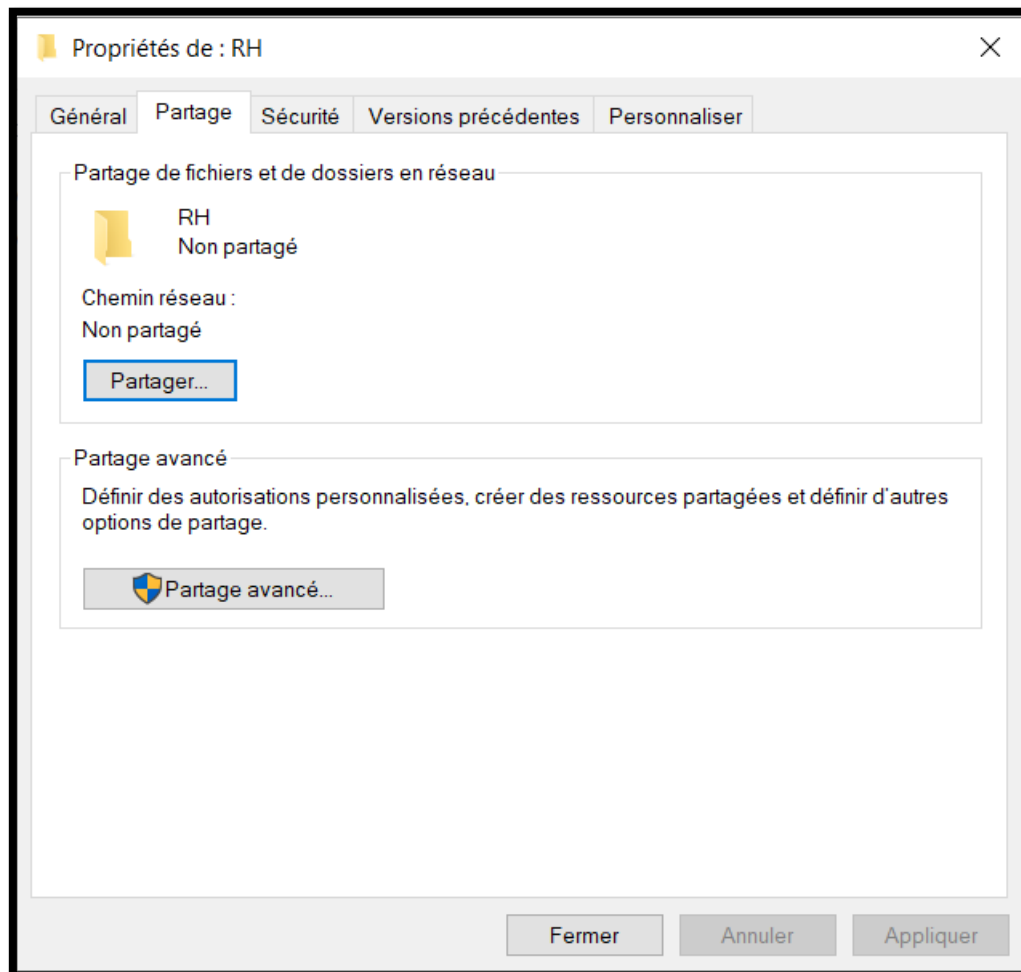


Figure 14 - Partage réseau du dossier RH

On ajoute le groupe RH dans le groupe pouvant avoir accès au dossier :

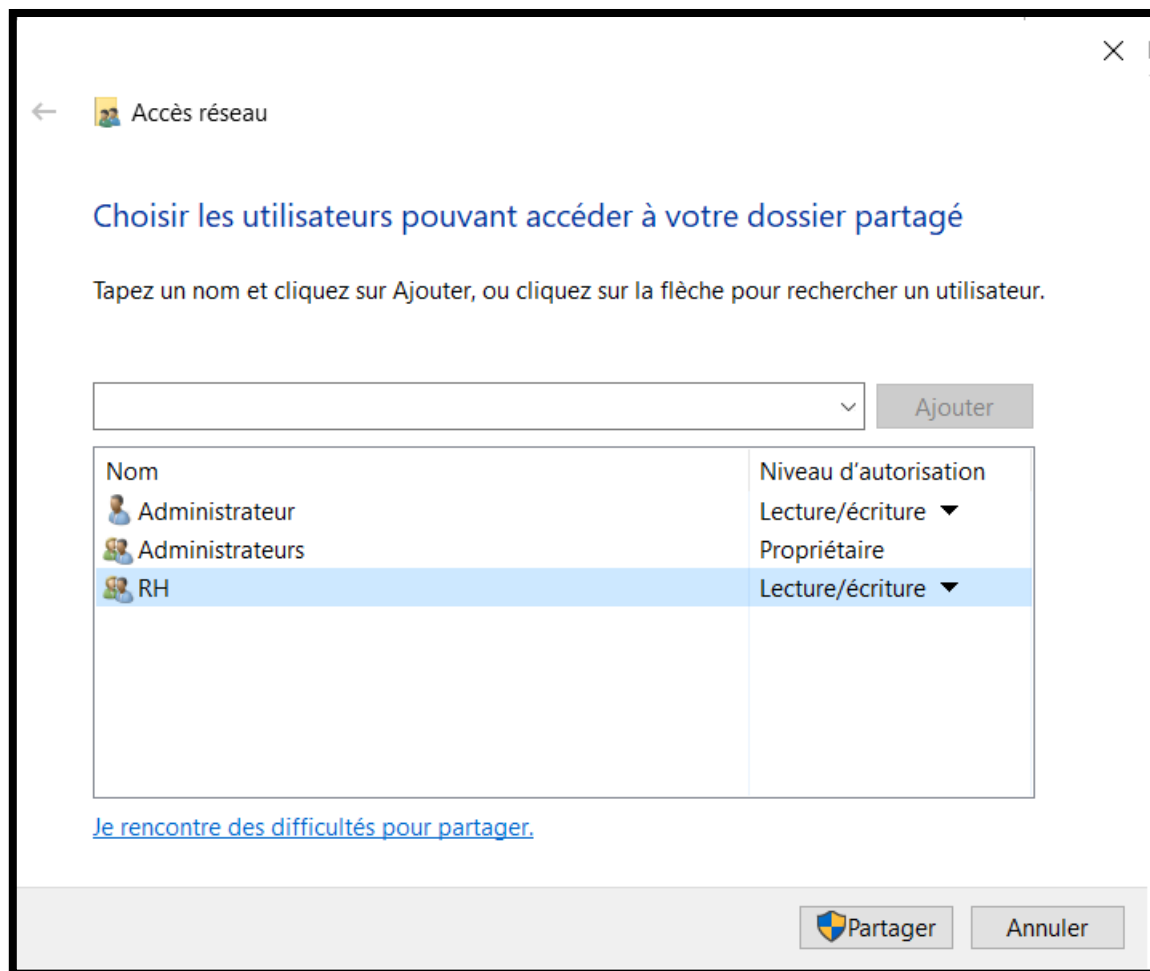


Figure 15 - Ajout des groupes de sécurité

Enfin, grâce aux groupes NTFS, on spécifie les droits sur les fichiers contenus dans le dossier partagés pour chaque utilisateur / groupe

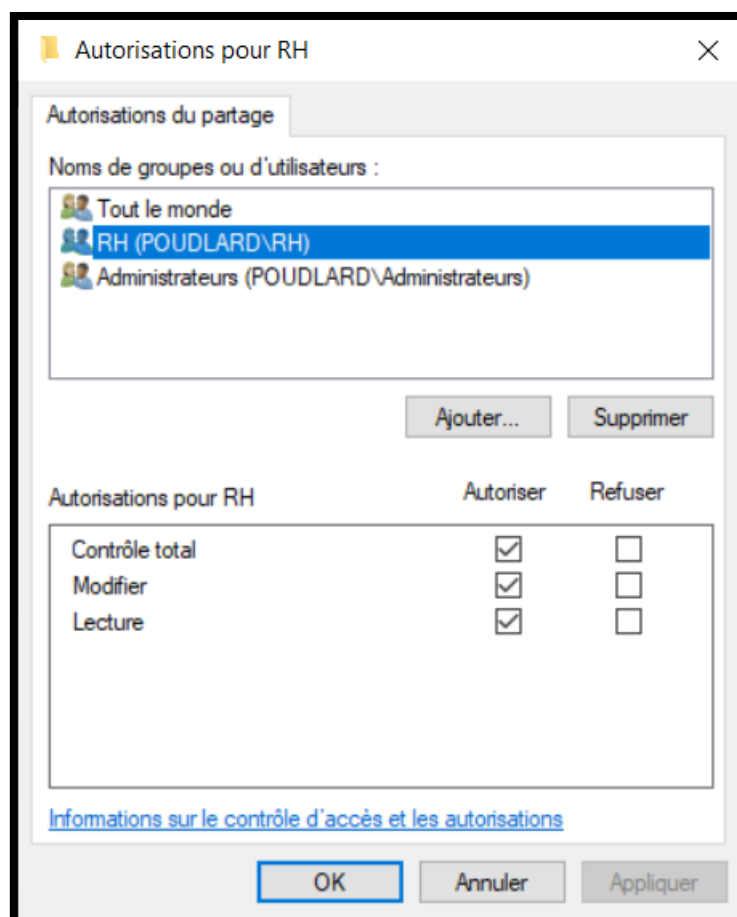


Figure 16 - Droits NTFS

Le groupe RH peut désormais accéder au dossier RH sur le réseau local, à l'adresse « \\Win-uujocm9qgr4\rh ».

On répète le même procédé pour le groupe Secrétariat et le groupe Pédagogie.

VII. Mise en place de GPO / stratégies spécifiques

On détermine une stratégie de mot de passe spécifique aux utilisateurs de l'administration. Selon les recommandations de la CNIL, il n'est pas nécessaire de changer demander aux utilisateurs de changer régulièrement de mots de passes, sauf pour les utilisateurs pouvant être emmené à avoir des données sensibles ou des accès spécifiques. Dans notre cas, pour l'administration, on adopte une stratégie d'un changement de mot de passe par an.

Ensuite, on détermine que l'utilisateur peut se tromper 3 fois de mot de passe. Passé 3 tentatives, la session est bloquée jusqu'à ce qu'un administrateur débloque le compte.

Concernant la longueur du mot de passe, il doit respecter une longueur d'au moins 12 caractères, dont 1 chiffre, 1 majuscule et 1 caractère spécial.

The screenshot shows the 'PSO_ADMINISTRATION' window for configuring password policies. The 'Paramètres de mot de passe' section is active, showing various settings for password complexity, length, and history. The 'Options d'âge du mot de passe' section is also visible, with checkboxes for applying minimum and maximum age rules. The 'S'applique directement à' section shows a list of users, with 'RH' and 'Secrétariat' listed. The 'Ajouter...' and 'Supprimer' buttons are visible next to the list.

Paramètres de mot de passe	Options d'âge du mot de passe
Nom : * PSO_ADMINISTRATION	<input checked="" type="checkbox"/> Appliquer l'âge minimal de mot de passe
Priorité : * 1	L'utilisateur ne peut pas changer le mot de passe d'ici à (jours) : * 180
<input checked="" type="checkbox"/> Appliquer la longueur minimale du mot de passe	<input checked="" type="checkbox"/> Appliquer l'âge maximal de mot de passe
Longueur minimale du mot de passe (caractères) : * 12	L'utilisateur doit changer le mot de passe après (jours) : * 365
<input checked="" type="checkbox"/> Appliquer l'historique des mots de passe	<input checked="" type="checkbox"/> Appliquer la stratégie de verrouillage des comptes :
Nombre de mots de passe mémorisés : * 24	Nombre de tentatives de connexion échouées autorisé : 3
<input checked="" type="checkbox"/> Le mot de passe doit respecter des exigences de complexité	Réinitialiser le nombre de tentatives de connexion échouées après (mins) : * 30
<input type="checkbox"/> Stocker le mot de passe en utilisant un chiffrement réversible	Le compte va être verrouillé
<input checked="" type="checkbox"/> Protéger contre la suppression accidentelle	<input type="radio"/> Pendant une durée de (mins) : *
Description :	<input checked="" type="radio"/> Jusqu'à ce qu'un administrateur déverrouille manuellement le compte

S'applique directement à
Nom
Courrier
RH
Secrétariat

Figure 17 - Règles mot de passe Administration

Pour la pédagogie (professeurs et élèves), les mots de passes n'expirent jamais. La longueur du mot de passe doit être la même que pour l'administration.

Figure 18 - Règles mot de passe Pédagogie

VIII. Configuration du serveur de redondance

On ajoute un serveur avec les services ADDS et DNS qui est redondant par rapport au premier.

Après avoir installé les services, on ajoute la machine au domaine déjà existant (Poudlard)

Les modifications faites dans l'AD sur le serveur principal seront maintenant appliquées sur le serveur redondant.

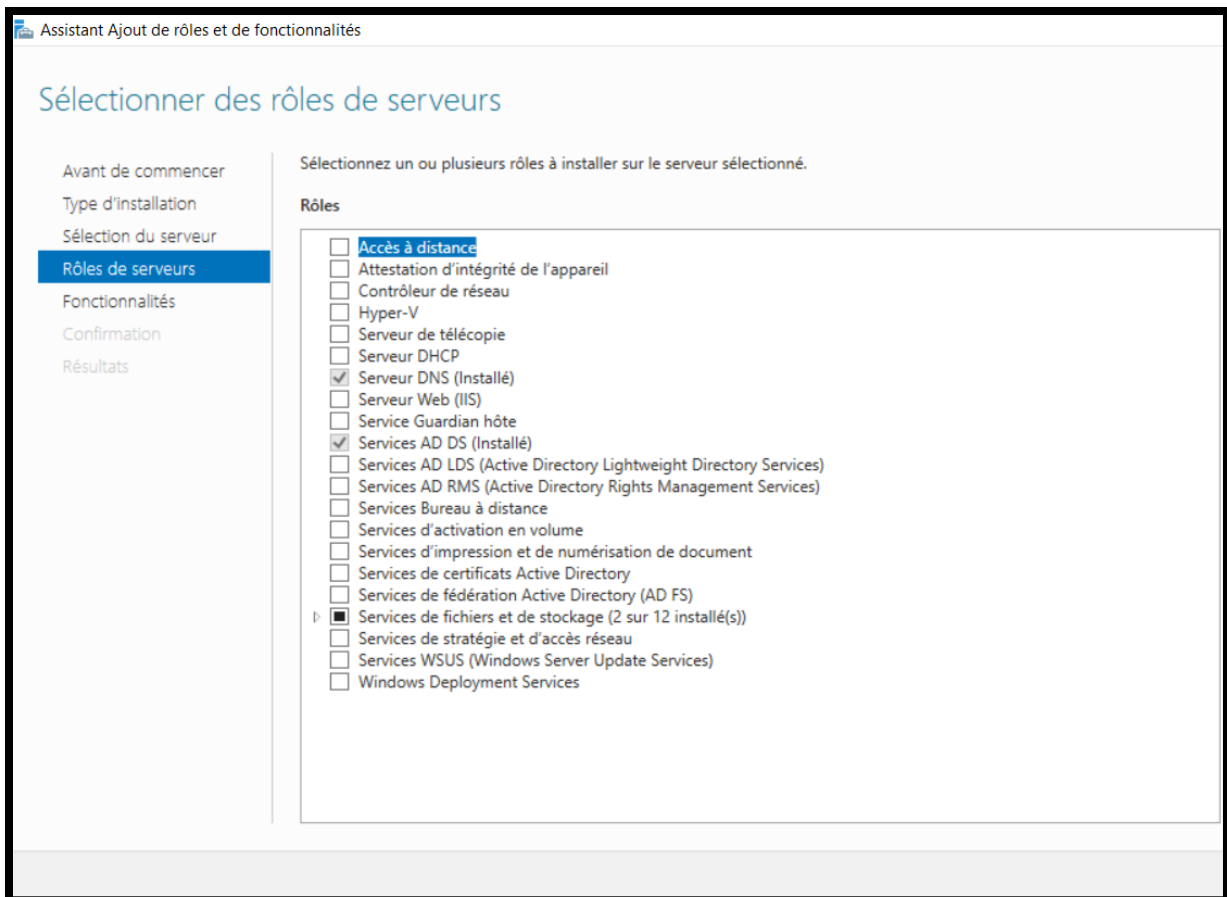


Figure 19 - Installation des rôles ADDS ET DNS

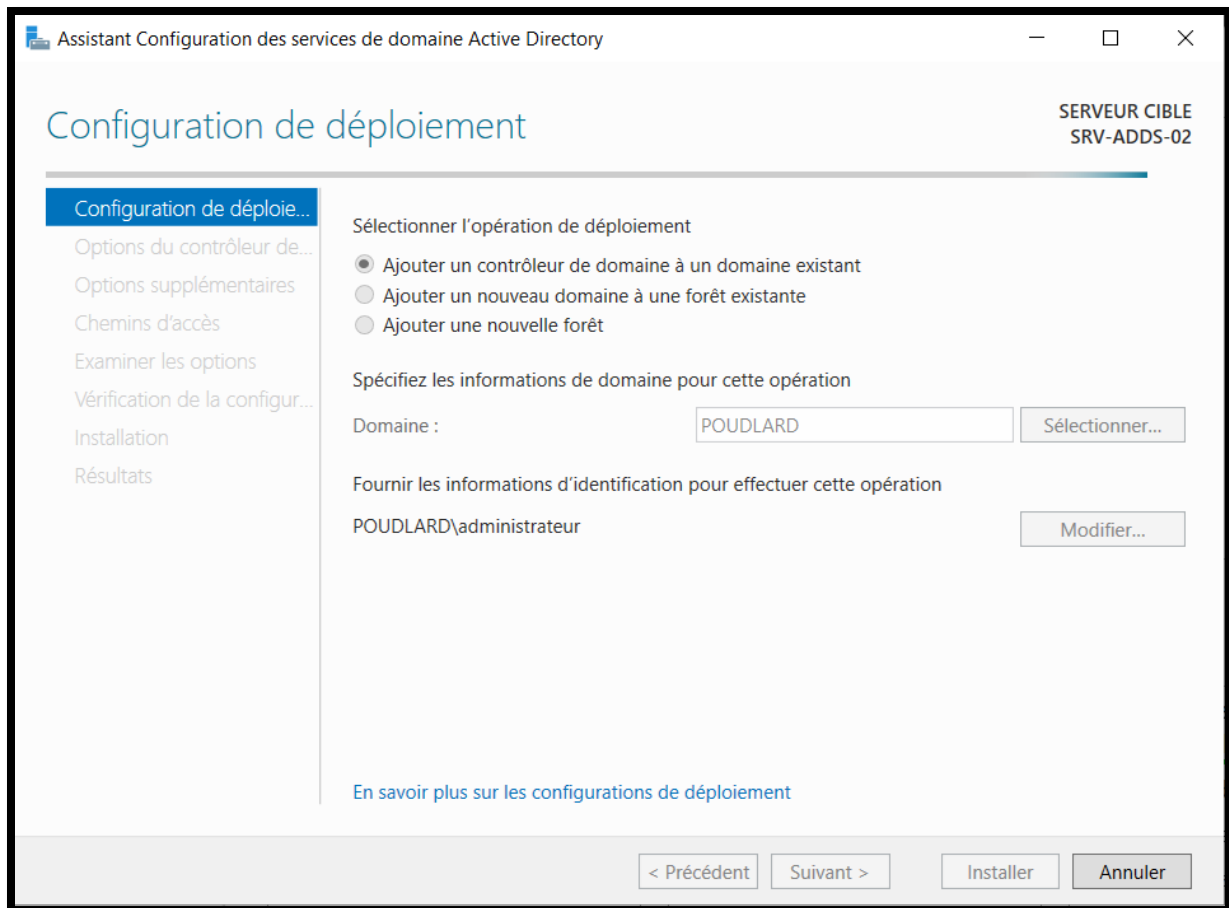


Figure 20 - Ajout du serveur redondant dans le domaine déjà existant (POUDLARD)

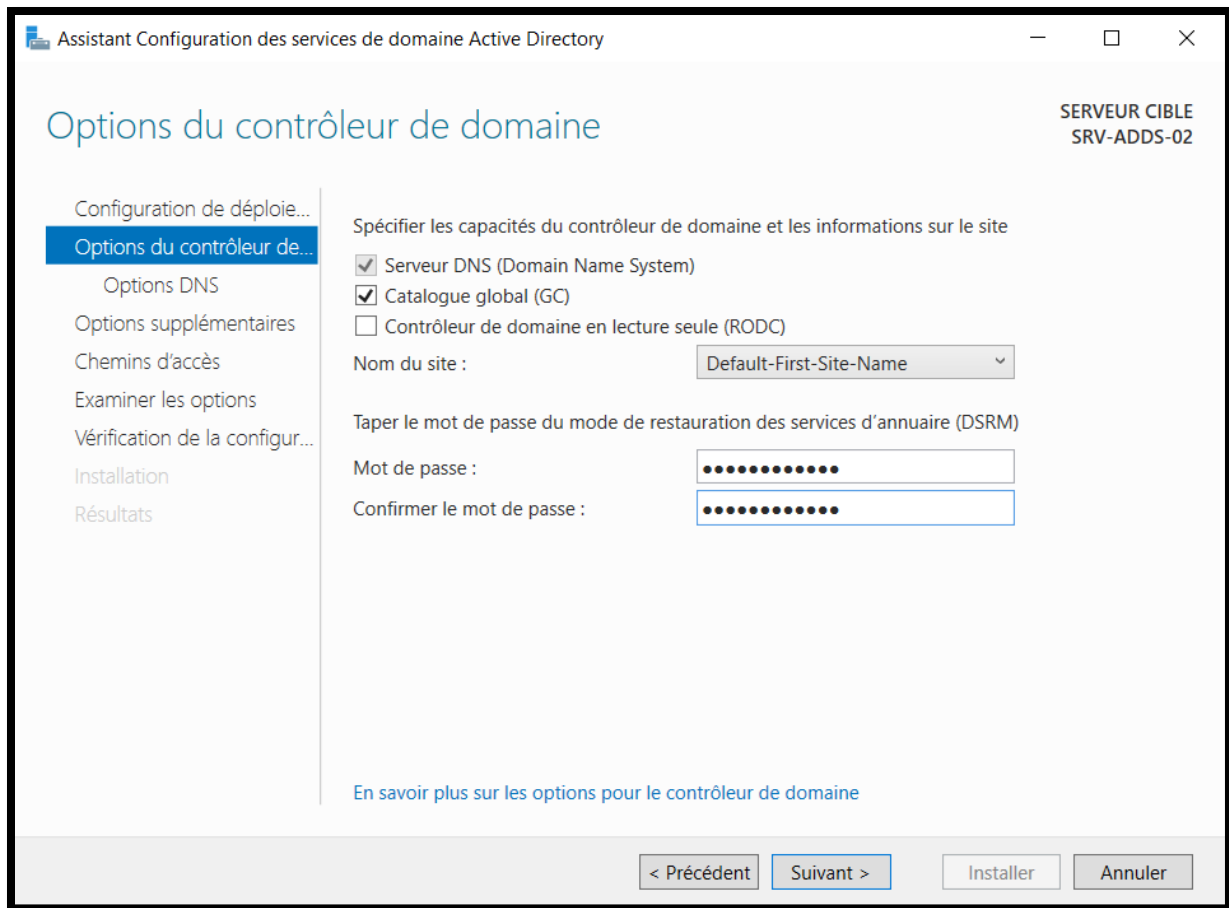


Figure 21 - Configuration du serveur redondant avant d'intégrer le domaine existant

IX. Configuration avancée du Routeur / Pare-Feu PfSense (DHCP, règles de filtrage, vlan)

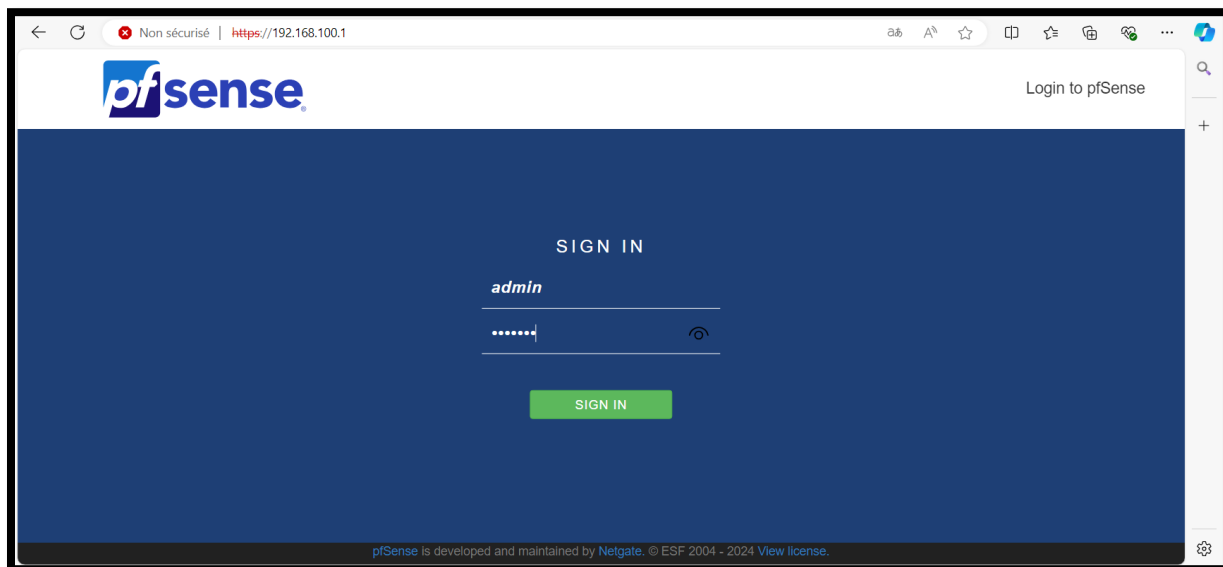


Figure 22 - Page web de connexion PfSense

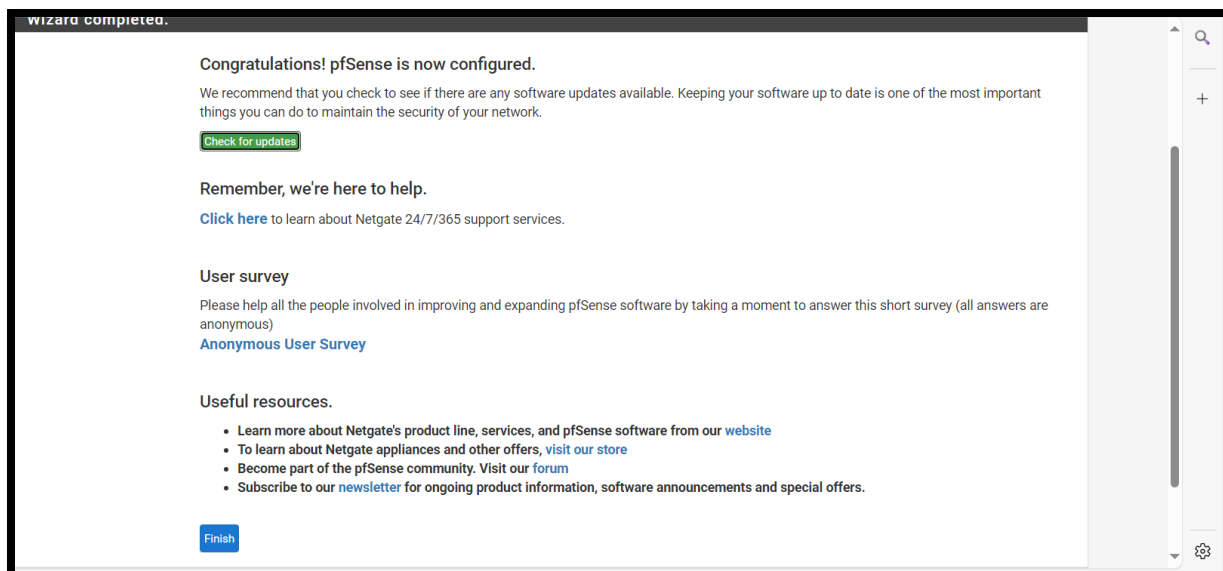


Figure 23 - Préconfiguration PfSense

On configure 3 VLAN différents. Le premier VLAN (10) correspond à la pédagogie. Le deuxième VLAN (20) correspond au secrétariat. Le troisième VLAN (30) correspond au service RH.

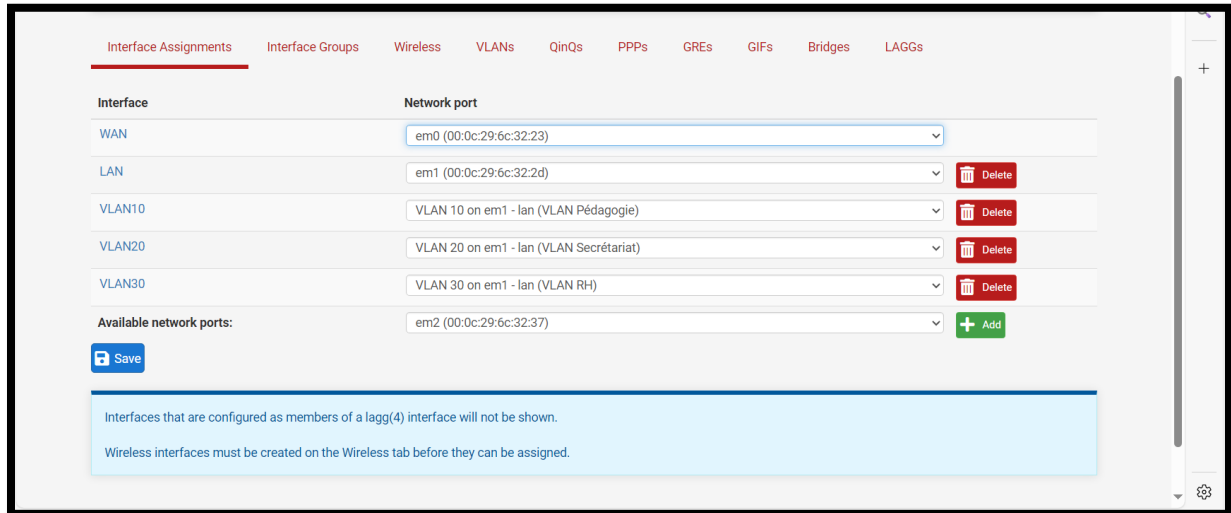


Figure 24 - Configuration des VLAN (1)

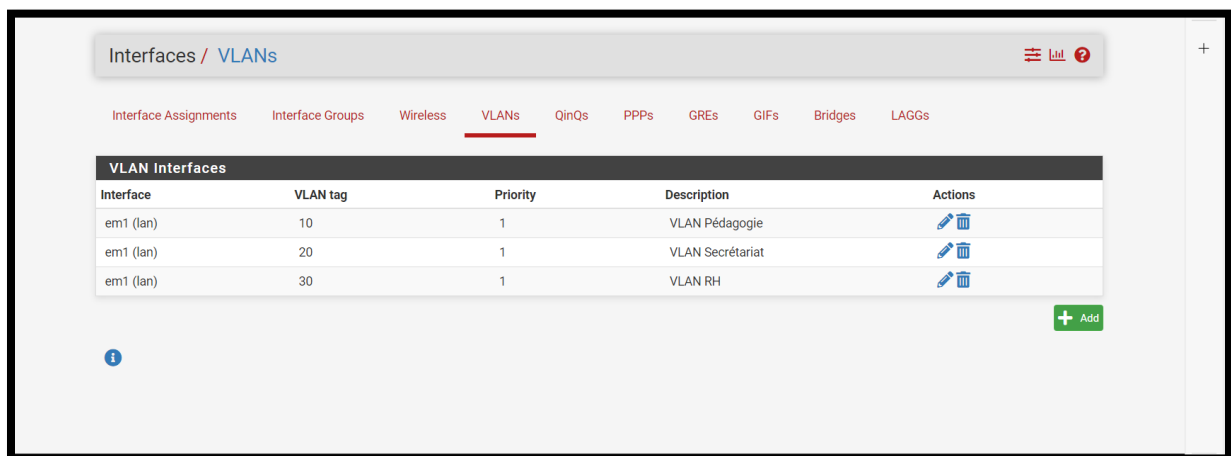


Figure 25 - Configuration des VLAN (2)

On applique maintenant des règles de filtrages sur les différents VLAN. Pour chacun d'entre eux, on bloque le trafic provenant de n'importe quel port, conformément à la RGPD. On laisse ensuite passer le trafic http et https.

Floating	WAN	LAN	VLAN10	VLAN20	VLAN30
----------	-----	-----	--------	--------	--------
















Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	443 (HTTPS)	*	443 (HTTPS)	*	none		    
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	80 (HTTP)	*	80 (HTTP)	*	none		    
<input type="checkbox"/>	✗	0/0 B	IPv4 *	*	*	*	*	*	none		    

Figure 26 - Règles de filtrage VLAN 10 (Pédagogie)

Floating	WAN	LAN	VLAN10	VLAN20	VLAN30
----------	-----	-----	--------	--------	--------
















Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	443 (HTTPS)	*	443 (HTTPS)	*	none		    
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	80 (HTTP)	*	80 (HTTP)	*	none		    
<input type="checkbox"/>	✗	0/0 B	IPv4 *	*	*	*	*	*	none		    

Figure 27 - Règles de filtrage VLAN 20 (Secrétariat)

Floating	WAN	LAN	VLAN10	VLAN20	VLAN30
----------	-----	-----	--------	--------	--------
















Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	443 (HTTPS)	*	443 (HTTPS)	*	none		    
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	80 (HTTP)	*	80 (HTTP)	*	none		    
<input type="checkbox"/>	✗	0/0 B	IPv4 TCP	*	*	*	*	*	none		    

Figure 28- Règles de filtrage VLAN 30 (RH)

