

SAE3.ROM.3

Rapport Technique

Réalisé par
Marietou Ndiaye SEYDI
RT2-ROM- 2024/2025

SOMMAIRE

Pages 3-4..... Informations Générales et Contexte

Page 5 Création de VMs

Page 8 Partie AD-DS et DNS

Page 19 Partie automatisation de taches avec PowerShell et mise en place de GPO

Page 23 Partie Web IIS

Page 26 Partie Réseau

Page 33 Partie WIFI

Page Partie Veille technologie

Informations générales :

Login de connexion : **Sae_Etu17** et mot de passe : **@S.3PeBr**

Nom Machine et Serveurs	Adresse IP	Passerelle	Masque	Mot de Passe
SAE3_ROM3_ETU17_SW16_1	192.168.108.161	192.168.104.1	255.255.248.0	Finzat74
SAE3_ROM3_ETU17_SW16_2	192.168.108.162	192.168.104.1	255.255.248.0	Finzat74
SAE3_ROM3_ETU17_WIN10	192.168.108.164	192.168.104.1	255.255.248.0	final409

Contexte :

Notre responsable administration réseaux nous demande de concevoir, tester un nouveau réseau permettant d'accéder aux services et aux ressources de l'entreprise.

Les services réseaux de l'entreprise fonctionnent encore sur des Windows serveur 2008 et sur des serveurs Linux debian 7. Il faut changer ça !

Il nous demande de passer à minima, sur des serveurs Windows 2016 et Debian 11.

Ils ont de nouvelles fonctionnalités intéressantes et moins de failles de sécurité.

Nous utiliserons toutes nos compétences pour faire évoluer le réseau.

Problématique : Une Pme qui souhaite développer son activité, nous demande de concevoir et tester un nouveau réseau informatique permettant d'accéder aux différents services réseaux.

Activité Pratique : Evolution du réseau d'entreprise

I. Création de VM

Sous Vmware, nous allons créer deux serveurs DNS (primaire et secondaire) sur des environnements de Windows Server 2016. Pour cela, nous allons consulter le [guide de compatibilité](#).

Storage	LSI Logic SAS	Supported	Virtual LSI Logic SAS adapter
	BusLogic	Not Supported	Virtual BusLogic Parallel SCSI adapter
	LSI Logic	Not Supported	Virtual LSI Logic Parallel SCSI adapter
	IDE	Supported	Virtual IDE adapter for ATA disks
	VMware Paravirtual	Supported(Recommended)	VMware Paravirtual SCSI (PVSCSI) adapter
	NVMe	Supported	NVM Express Adapter
	SATA	Supported	Virtual SATA adapter
Networking	VMXNET	Not Supported	VMware virtual NIC
	Vlance	Not Supported	Emulated AMD 79C970 PCnet32 Lance NIC
	e1000	Not Supported	Emulated Intel 82545EM Gigabit Ethernet NIC
	Enhanced VMXNET	Not Supported	Second generation VMware virtual NIC
	e1000e	Supported	Emulated Intel 82574L Gigabit Ethernet Controller
	VMXNET 3	Supported(Recommended)	Third generation VMware virtual NIC

Nous allons créer un modèle de la machine virtuelle pour ensuite déployer nos VM à partir du modèle créé.

Nous avons donc utilisé les paramètres recommandés pour notre serveur.

Avec la taille de disque dur recommandé par Windows :

RECHERCHER COPILOT ÉCOLE VIDÉOS IMAGES CARTES ACTUALITÉS

Environ 52 500 résultats

32 Go

L'espace disque minimal requis pour installer Windows Server 2016 est de **32 Go**

Résumé de la machine créée :

Modifier les paramètres...

Modèle_SAE_ROM3_Etu17_SW16



Matériel virtuel

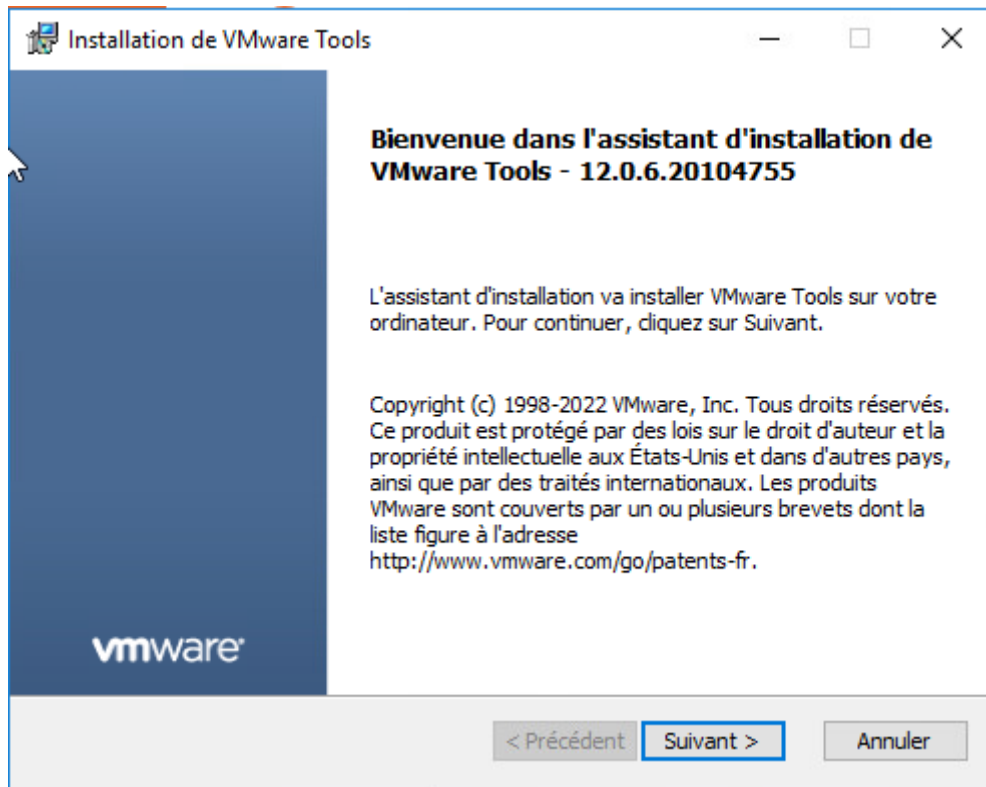
Options VM

AJOUTER UN PÉRIPHÉRIQUE

> CPU	2	▼	
> Mémoire	4	Go	▼
▼ Disque dur 1	32	Go	▼
Taille maximale 180,34 Go			
Stratégie de stockage VM ▼			
Type	Provisionnement dynamique		

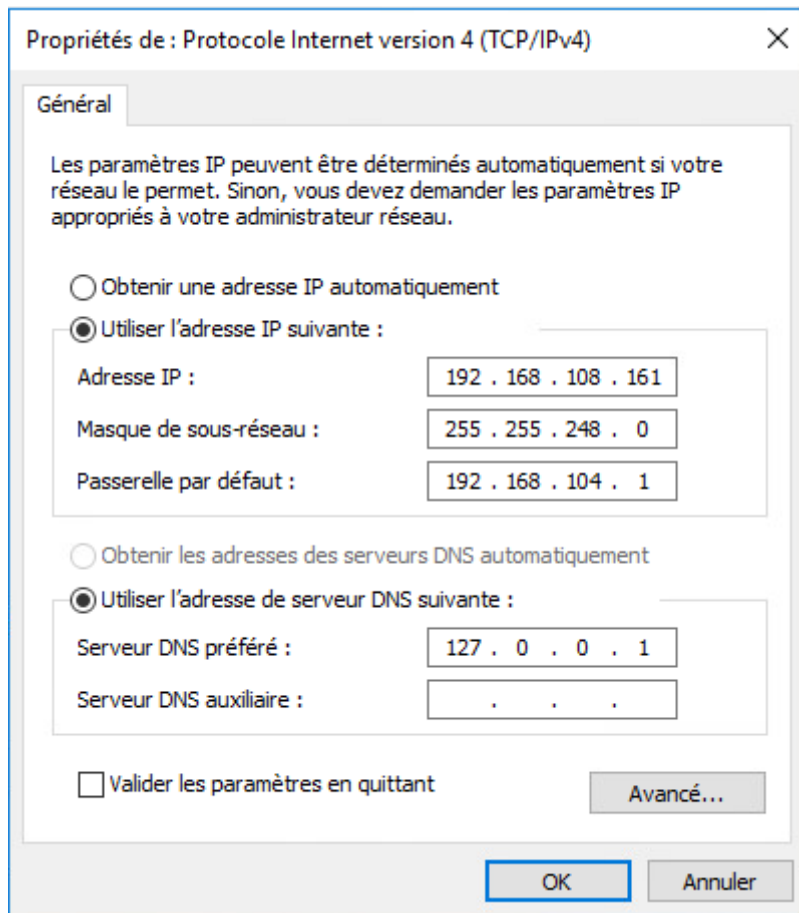
▼ Lecteur CD/DVD 1	Fichier ISO banque de données ▼	<input checked="" type="checkbox"/> Connecté
Statut <input type="checkbox"/> Connecter lors de la mise sous tension		
Support CD/DVD	[ISO] 2016_64Bit_French_	PARCOURIR...
Mode Périphérique Émuler CD-ROM ▼		
Nœud de périphérique virtuel Contrôleur SATA 0 ▼ SATA(0:0) Lecteur CD/DVD 1 ▼		
▼ Lecteur CD/DVD 2	Fichier ISO banque de données ▼	<input checked="" type="checkbox"/> Connecté
Statut <input type="checkbox"/> Connecter lors de la mise sous tension		
Support CD/DVD	[] /vmimages/tools-isoima	PARCOURIR...

Installation de VMWareTools :



II. Partie AD-DS et DNS :

Pour l'installation de l'AD-DS, nous allons changer l'adresse DNS en 127.0.0.1.



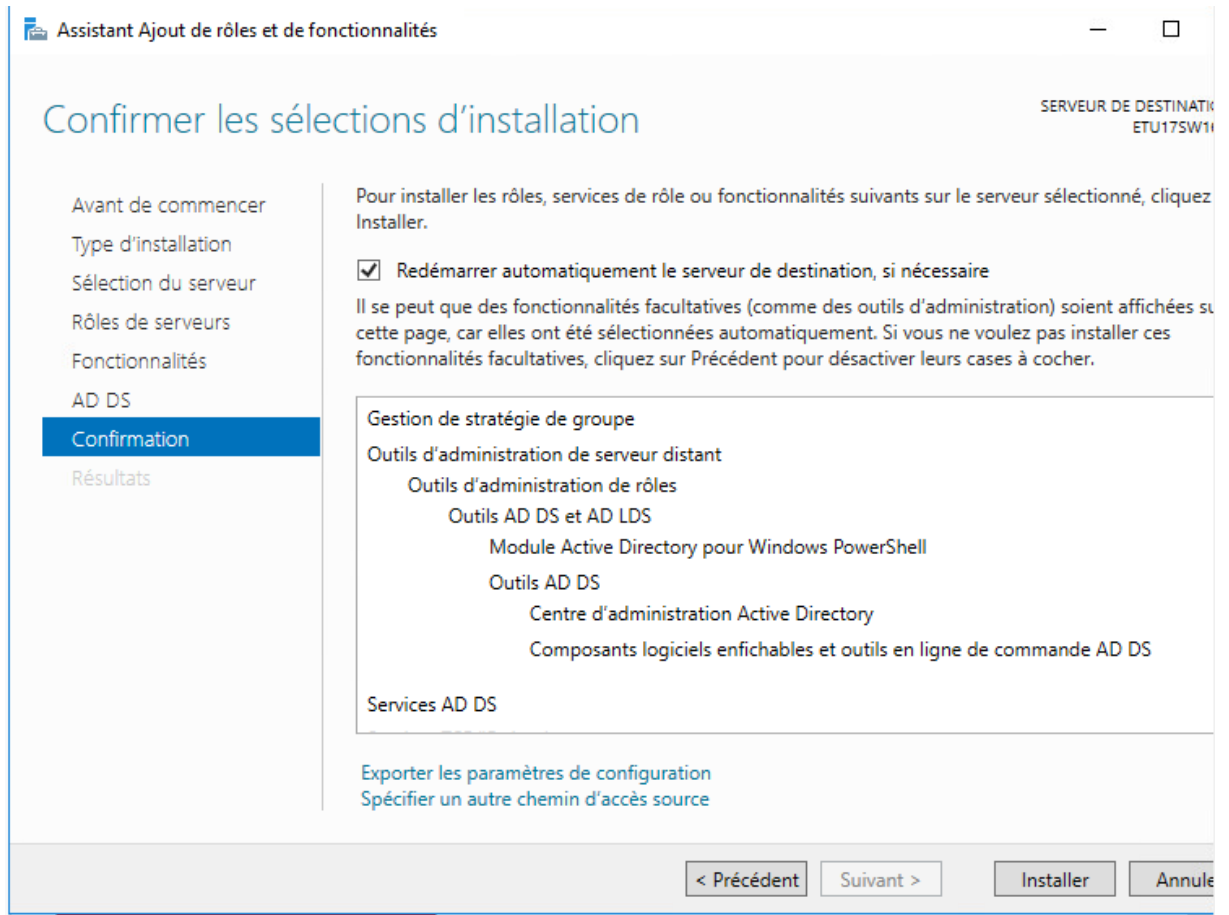
Active Directory Domain Services, est un service de gestion des identités et des accès développés par Microsoft. Il joue un rôle essentiel dans les environnements réseau basés sur Windows. Il intègre le service **DNS**.

Il permet de gérer les utilisateurs et groupes, gérer les stratégies de groupe, l'authentification et l'autorisation des utilisateurs, sécurité, etc.

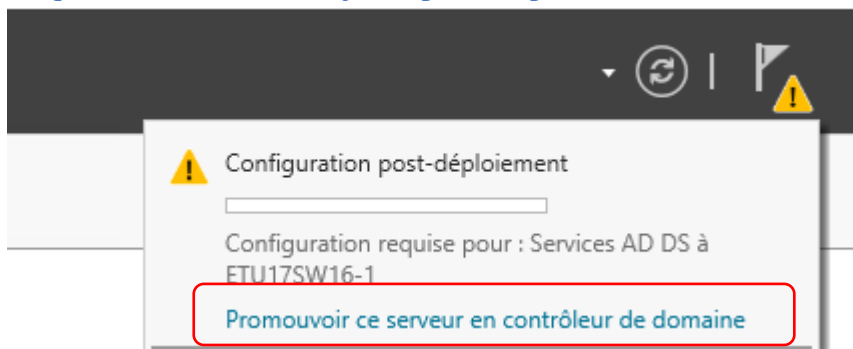
Voici le processus d'installation de l'[AD-DS](#).

Etapes à suivre :

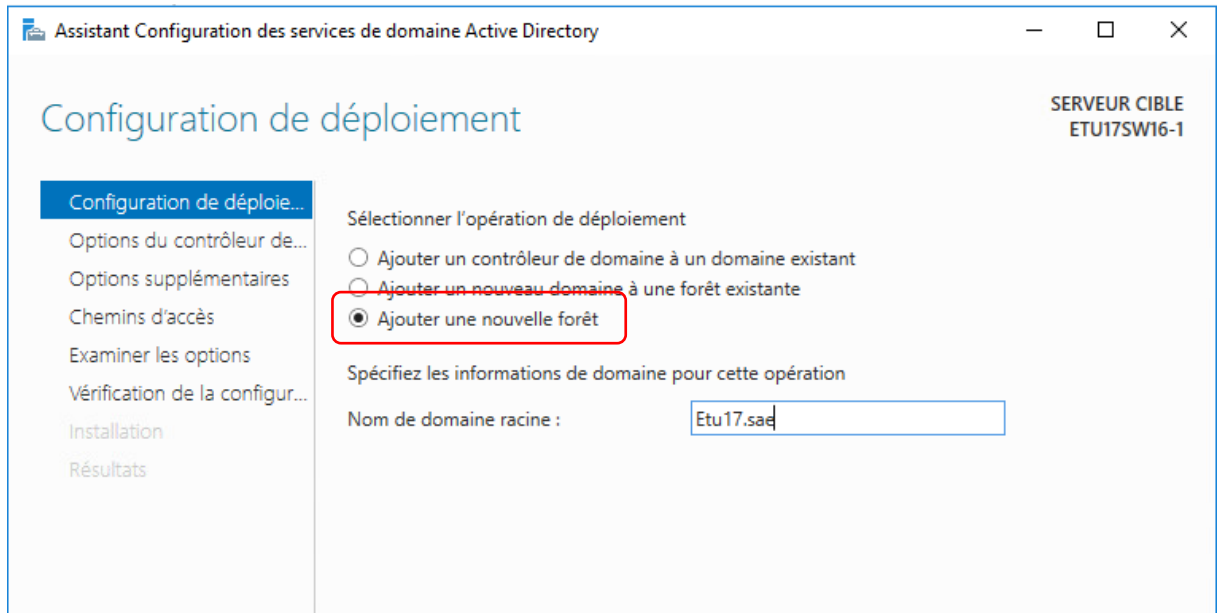
- [Aller dans gérer](#)
- [Ajouter des rôles et fonctionnalités](#)
- [Suivant x 3](#)
- [On coche le service AD DS](#)
- [Ajouter des fonctionnalités \(de base y a des fonctionnalités qui sont par défaut cocher mais on peut bien évidemment en ajouter d'autres\)](#)
- [Puis installer](#)



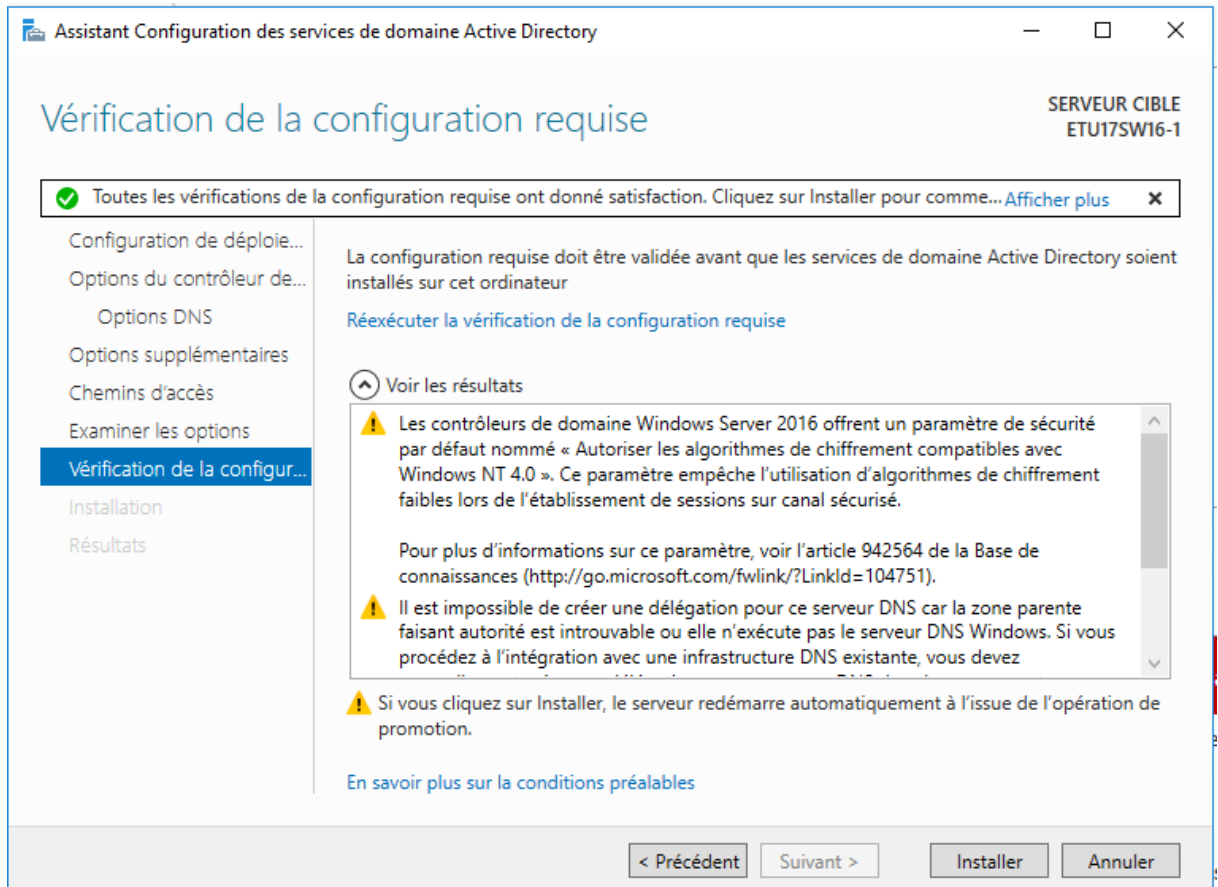
- Cliquer sur la notification jaune puis sur promouvoir



- Cocher sur Ajouter une nouvelle Forêt et renseigner le nom de domaine (etu17.sae3)



- Saisir le mot de passe (**Finzat73**)
- Suivant ... et installer



← → Gestionnaire de serveur ▸ Tableau de bord

Tableau de bord

- Serveur local
- Tous les serveurs
- AD DS
- DNS
- Services de fichiers et d... ▸

BIENVENUE DANS GESTIONNAIRE DE SERVEUR

DÉMARRAGE RAPIDE

1 Configurer ce serveur local

- Ajouter des rôles et des fonctionnali
- Ajouter d'autres serveurs à gérer
- Créer un groupe de serveurs
- Connecter ce serveur aux services cl

NOUVEAUTÉS

EN SAVOIR PLUS

Rôles et groupes de serveurs

Rôles : 3 | Groupes de serveurs : 1 | Nombre total de serveurs : 1

Rôle	Nombre
AD DS	1
DNS	1

AD DS

- Facilité de gestion
- Événements
- Services
- Performances
- Résultats BPA

DNS

- Facilité de gestion
- Événements
- Services
- Performances
- Résultats BPA

Conversion de la machine en modèle :

Modèle_SAE_ROM3_Etu17_SW16 | [icônes] ACTIONS ▾

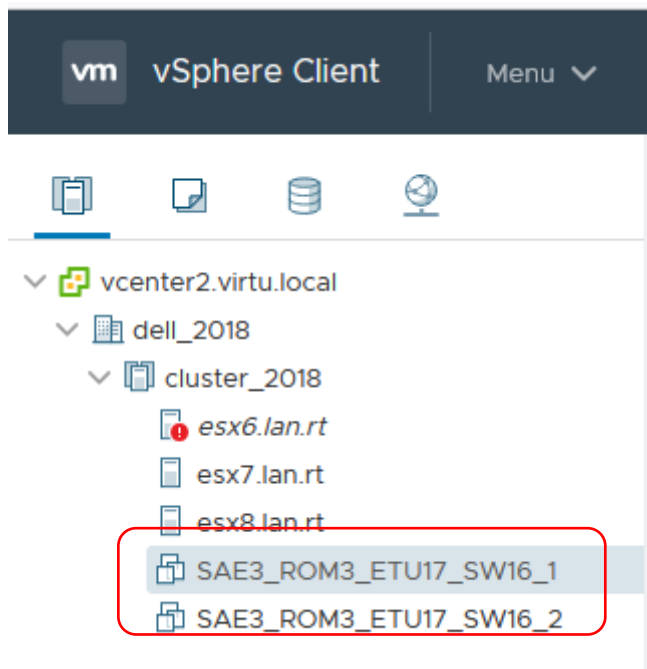
Résumé | Surveiller | Configurer | Autorisations | Banques de données | Réseaux

Hors tension

SE invité : Microsoft Windows Server 2016 or later (64-bit)
 Compatibilité : ESXi 6.7 Update 2 et versions ultérieures (VM version 15)
 VMware Tools : Inactif, version :12294 (Actuel)
[Plus d'infos](#)

Nom DNS : WIN-RHN75HL46G4
 Adresses IP :
 Hôte : esx8.lan.rt

De ce modèle, on va déployer nos deux serveurs (DNS primaires et secondaires) :

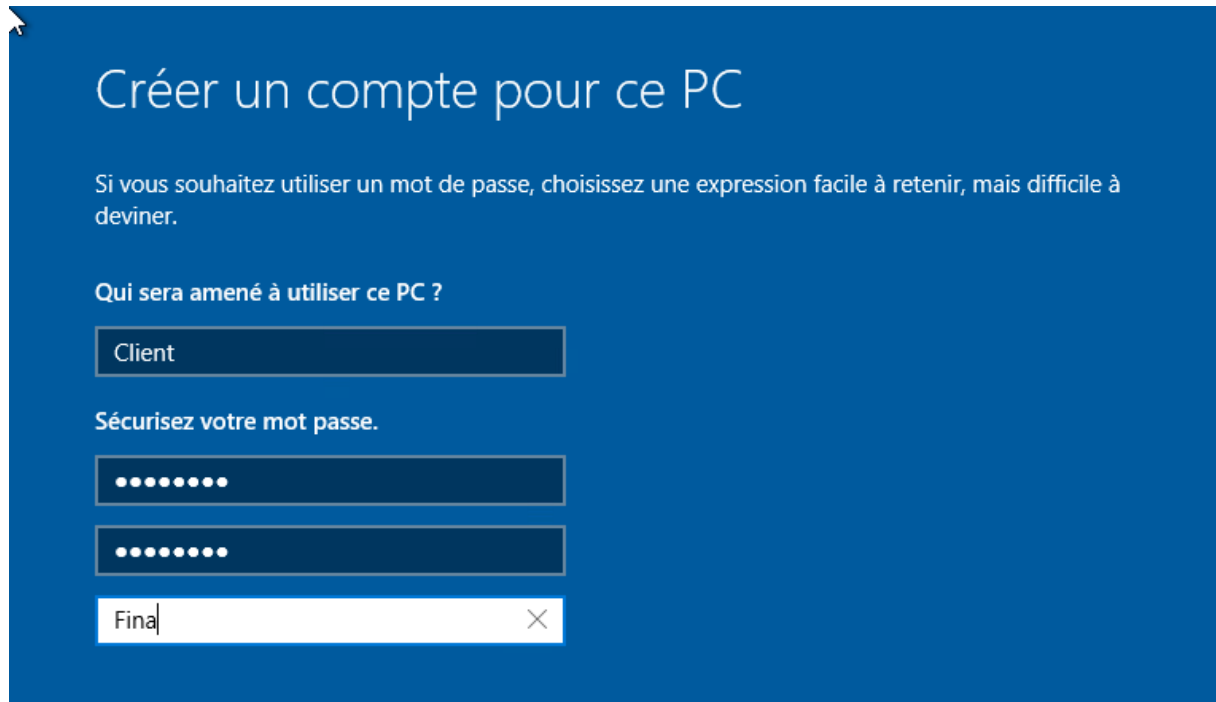


Création du VM client :

Sur VMWare compatibility :

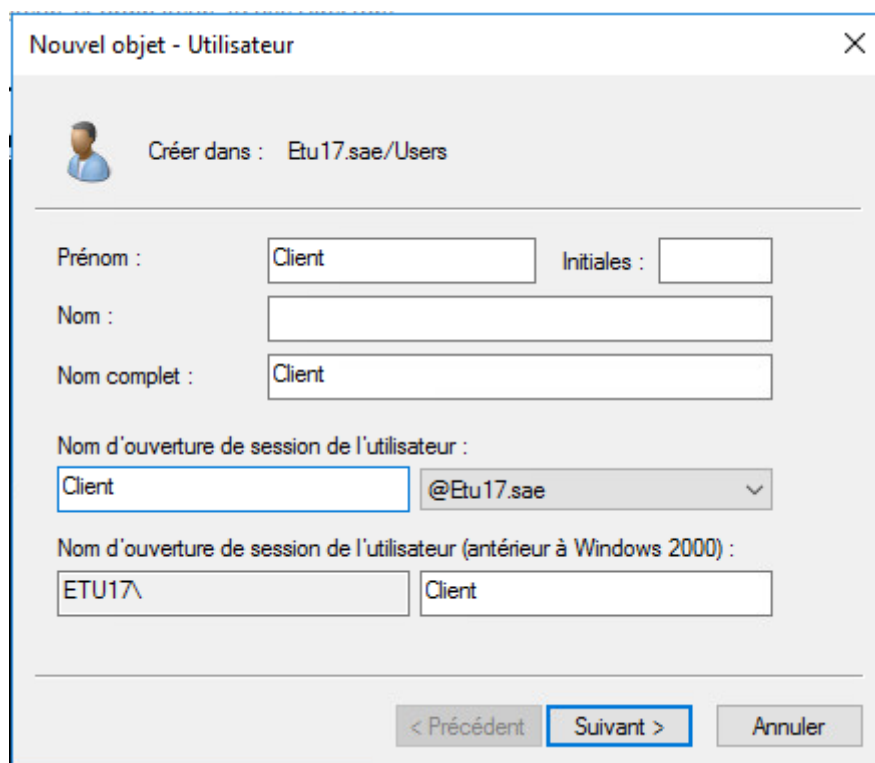
Category	Features	Features Support	Description
Storage	LSI Logic SAS	Supported	Virtual LSI Logic SAS adapter
	BusLogic	Not Supported	Virtual BusLogic Parallel SCSI adapter
	LSI Logic	Not Supported	Virtual LSI Logic Parallel SCSI adapter
	IDE	Supported	Virtual IDE adapter for ATA disks
	VMware Paravirtual	Supported(Recommended)	VMware Paravirtual SCSI (PVSCSI) adapter
	NVME	Supported	NVM Express Adapter
Virtual Hardware	SATA	Supported	Virtual SATA adapter
	Hot Add Memory	Supported	Ability to add memory to a running virtual machine with zero downtime
	Hot Add vCPU	Not Supported	Ability to add a virtual CPU to a running virtual machine with zero downtime
Networking	SMP	Supported	Virtual Symmetric Multiprocessing
	VMXNET	Not Supported	VMware virtual NIC
	Vlance	Not Supported	Emulated AMD 79C970 PCnet32 Lance NIC
	e1000	Not Supported	Emulated Intel 82545EM Gigabit Ethernet NIC
	Enhanced VMXNET	Not Supported	Second generation VMware virtual NIC
	e1000e	Supported	Emulated Intel 82574L Gigabit Ethernet Controller
	VMXNET 3	Supported(Recommended)	Third generation VMware virtual NIC

Nom d'utilisateur et mot de passe du compte client : fina1409



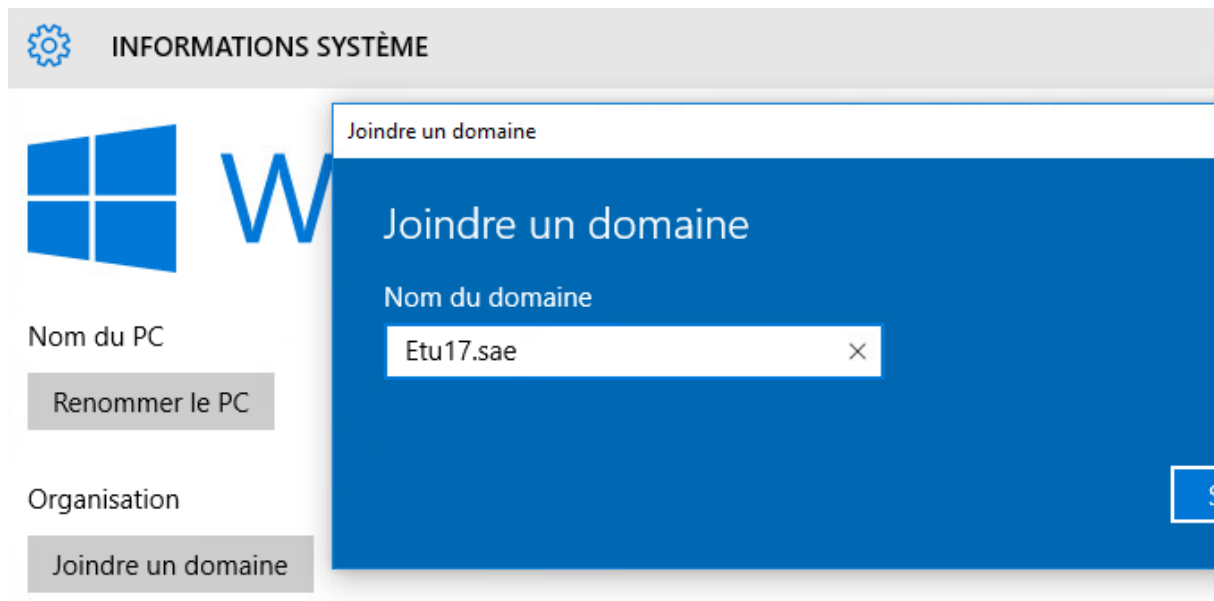
Nous allons intégrer notre machine cliente à notre domaine Etu17.sae :

Tous d'abord, au niveau du serveur, nous allons créer un utilisateur permettant de nous connecter depuis le client au domaine :

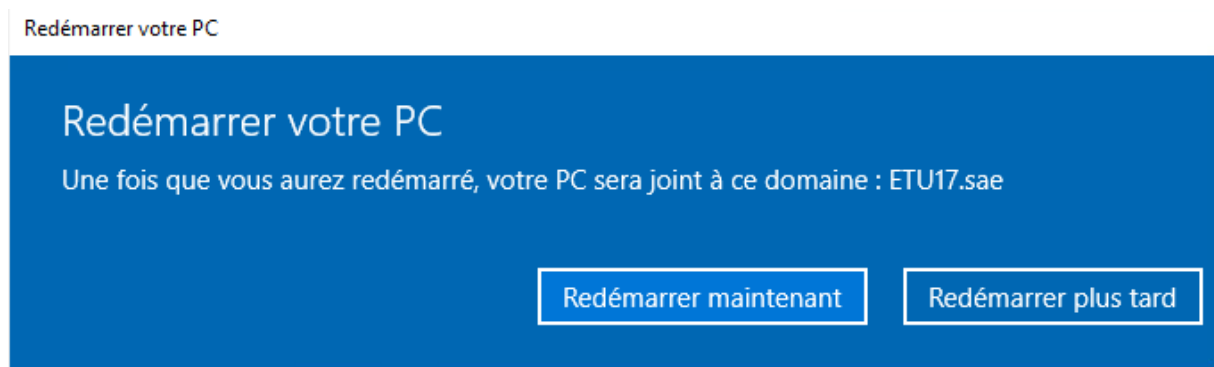


Avec comme mot de passe : Finzat73.

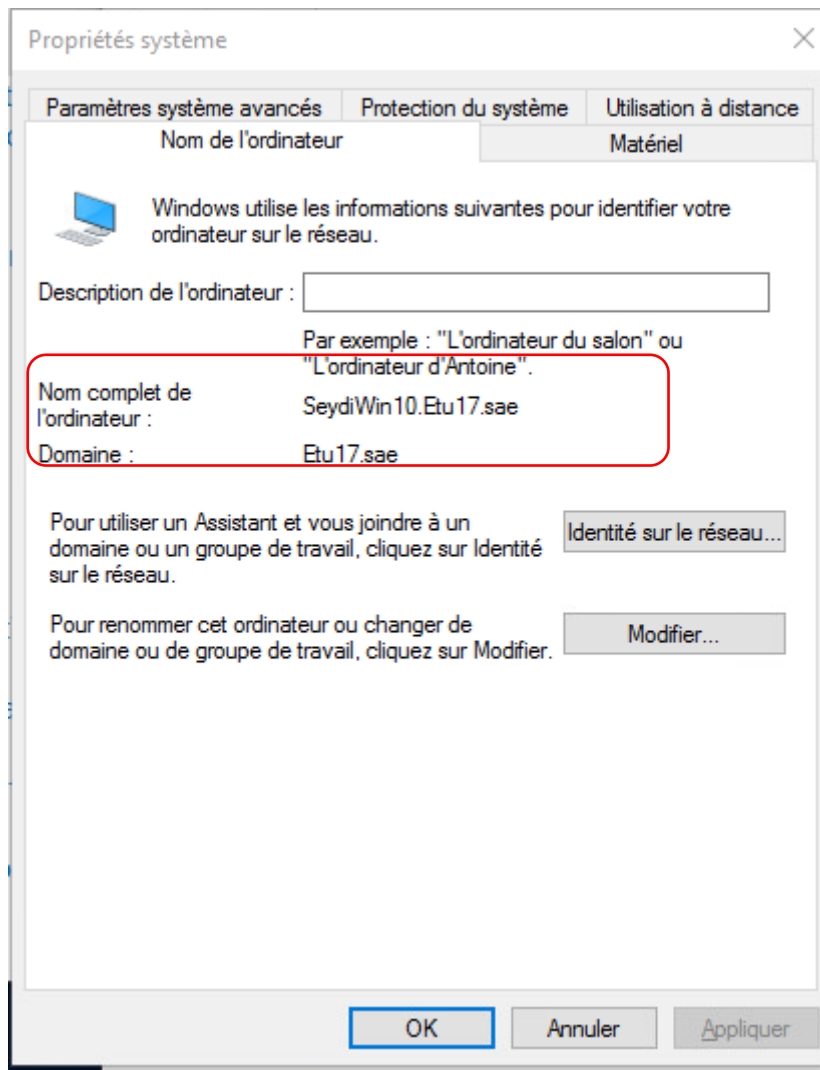
Dans les Informations du Système :



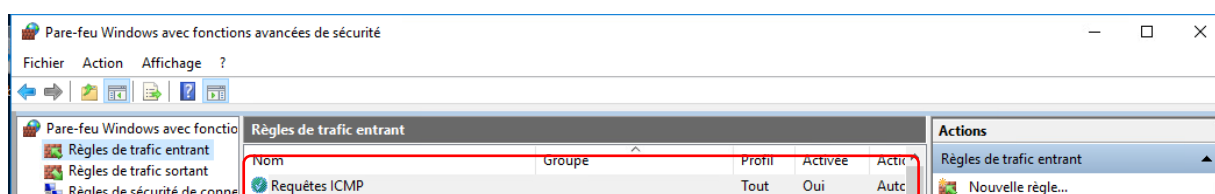
Après avoir renseigné l'utilisateur et le mot de passe, redémarrer la machine pour prendre en compte les modifications :



Dans les propriétés du système :



Au niveau du pare feu, nous allons ajouter une nouvelle règle de trafic entrant permettant les requêtes ICMP entrantes :



Gestionnaire DNS :

Dans le gestionnaire DNS, la configuration du **DNS** est pré-fait par l'**AD-DS**. Effectivement en ayant coché l'installation DNS le service s'est installé et a près configuré une zone de recherche directe pour notre domaine Etu17.sae. Il a donc suffi de demander au professeur de faire une délégation pour mon sous-domaine Etu17.sae et le service est maintenant fonctionnelle.

Test de la délégation :

Au niveau de notre serveur primaire :

```
C:\Users\Administrateur.WIN-7G96S96C3QD>nslookup
Serveur par défaut : ns1.lan.rt
Address: 10.250.250.12

> set type=NS
Type=NS
> Etu17.sae
Serveur : ns1.lan.rt
Address: 10.250.250.12

DNS request timed out.
timeout was 2 seconds.
Réponse ne faisant pas autorité :
Etu17.sae nameserver = Etu17.sae
Etu17.sae internet address = 192.168.108.161
```

On y retrouve des enregistrements de type AAA de toutes les machines qui ont rejoint le domaine **Etu17.sae**.

Au niveau de la machine 1 :

Nom	Type	Données	Horodateur
(identique au dossier parent)	Source de nom (SOA)	[38], etu17sw16-1.etu17.sae...	statique
(identique au dossier parent)	Serveur de noms (NS)	etu17sw16-1.etu17.sae.	statique
(identique au dossier parent)	Hôte (A)	192.168.108.161	28/11/2024 17:00:00
etu17sw16-1	Hôte (A)	192.168.108.161	statique
SeydiWin10	Hôte (A)	192.168.108.163	02/12/2024 22:00:00

Nous allons créer une nouvelle de recherche inversée. La configuration de la zone de recherche inverse est très importante dans la résolution de nom car permettant de lier le nom d'une machine à son adresse IP. Ainsi, on peut **ping** une machine par son **nom** au lieu de son **IP**.

Nom	Type	État	État DNSSEC
108.168.192.in-addr.arpa	Serveur principal intégré à Act...	En cours d'ex...	Non signé

Dans cette zone, nous allons créer des pointeurs vers les machines primaire et secondaire et vers la machine cliente. Les enregistrements SOA et NS ont été configurés directement :

DNS	Nom	Type	Données	Horodateur
ETU17SW16-1	(identique au dossier parent)	Source de nom (SOA)	[1], etu17sw16-1.etu17.sae...	statique
▼ Zones de recherche directes	(identique au dossier parent)	Serveur de noms (NS)	etu17sw16-1.etu17.sae.	statique
> _msdcs.Etu17.sae	192.168.108.162	Pointeur (PTR)	etu17sw16-2.Etu17.sae	
> Etu17.sae	192.168.108.161	Pointeur (PTR)	etu17sw16-1.Etu17.sae	
▼ Zones de recherche inversée	192.168.108.163	Pointeur (PTR)	SeydiWin10.Etu17.sae	
108.168.192.in-addr.arpa				

Ayant déployé les deux machines à partir d'un modèle, nous allons rajouter au niveau du serveur primaire une enregistrement de type A pour le serveur secondaire. L'ensemble de nos enregistrements :

(identique au dossier parent)	Source de nom (SOA)	[38], etu17sw16-1.etu17.sa...	statique
(identique au dossier parent)	Serveur de noms (NS)	etu17sw16-1.etu17.sae.	statique
(identique au dossier parent)	Hôte (A)	192.168.108.161	28/11/2024 17:00:00
etu17sw16-1	Hôte (A)	192.168.108.161	statique
SeydiWin10	Hôte (A)	192.168.108.163	02/12/2024 22:00:00
etu17sw16-2	Hôte (A)	192.168.108.162	

Les redirecteurs :

Modifier les redirecteurs			×
Adresses IP des serveurs de redirection :			
Adresse IP	Nom de domaine compl...	Validé	
<Cliquez ici pour ajo...			Supprimer
✓ 10.250.250.12	ns1.lan.rt	OK	Monter
✓ 10.250.250.5	dnssec.lan.rt	OK	Descendre

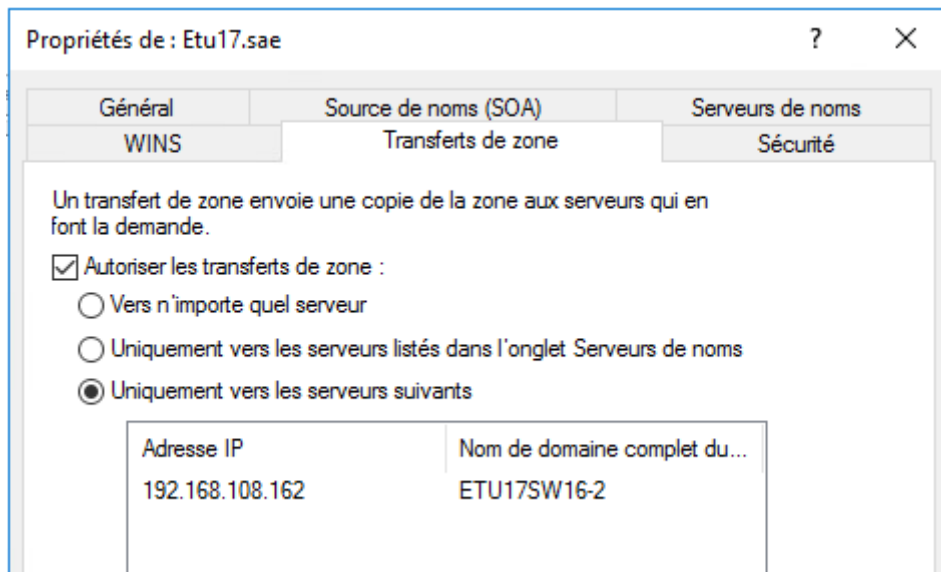
Faire un transfert de zone vers la machine 2 pour assurer la redondance :

Dans les propriétés de la zone, cliquer sur Transfert de zone :

Fichier	Action	Affichage	?
DNS			
▼ ETU17SW16-1			
▼ Zones de recherche directes			
> _msdcs.Etu17.sae			
> Etu17.sae			
▼ Zones de recherche inversée			
108.168.192.in-addr.arpa			
Points d'approbation			
Redirecteurs conditionnels			

Propriétés de : Etu17.sae	
Général	Source
WINS	
Un transfert de zone envoie une co... font la demande.	
<input checked="" type="checkbox"/> Autoriser les transferts de zone	
<input type="radio"/> Vers n'importe quel serveur <input type="radio"/> Uniquement vers les serveurs... <input checked="" type="radio"/> Uniquement vers les serveurs...	
Adresse IP	

Autoriser les transferts de zone		
Zone DNS : Etu17.sae		
Adresses IP des serveurs secondaires :		
Adresse IP	Nom de domaine compl...	Validé
<Cliquez ici pour ajouter une adresse IP ou un nom DNS>		
✓ 192.168.108.162	ETU17SW16-2	OK



Test de nos configurations :

Depuis la machine cliente WIN10, nous avons interrogé nos deux serveurs avec **nslookup**.

Ici, c'est le serveur principal qui répond directement ce qui est normal. On remarque la résolution de nom est correcte.

```
>
C:\Users\Client.ETU17>nslookup
Serveur par défaut : etu17sw16-1.Etu17.sae
Address: 192.168.108.161

> set type=NS
> Etu17.sae
Serveur : etu17sw16-1.Etu17.sae
Address: 192.168.108.161

Etu17.sae      nameserver = etu17sw16-1.Etu17.sae
etu17sw16-1.Etu17.sae  internet address = 192.168.108.161

> set type=SOA
> Etu17.sae
Serveur : etu17sw16-1.Etu17.sae
Address: 192.168.108.161

Etu17.sae
primary name server = etu17sw16-1.Etu17.sae
responsible mail addr = marietou.Etu17.sae
serial = 47
refresh = 900 (15 mins)
retry = 600 (10 mins)
expire = 86400 (1 day)
default TTL = 3600 (1 hour)
etu17sw16-1.Etu17.sae  internet address = 192.168.108.161
```

Essayons d'interroger notre serveur secondaire pour vérifier la redondance de notre serveur :

```
>
C:\Users\Client.ETU17>nslookup
Serveur par défaut :   etu17sw16-1.Etu17.sae
Address:  192.168.108.161

> server etu17sw16-2
Serveur par défaut :   etu17sw16-2.Etu17.sae
Address:  192.168.108.162

> set type=NS
> Etu17.sae
Serveur :   etu17sw16-2.Etu17.sae
Address:  192.168.108.162

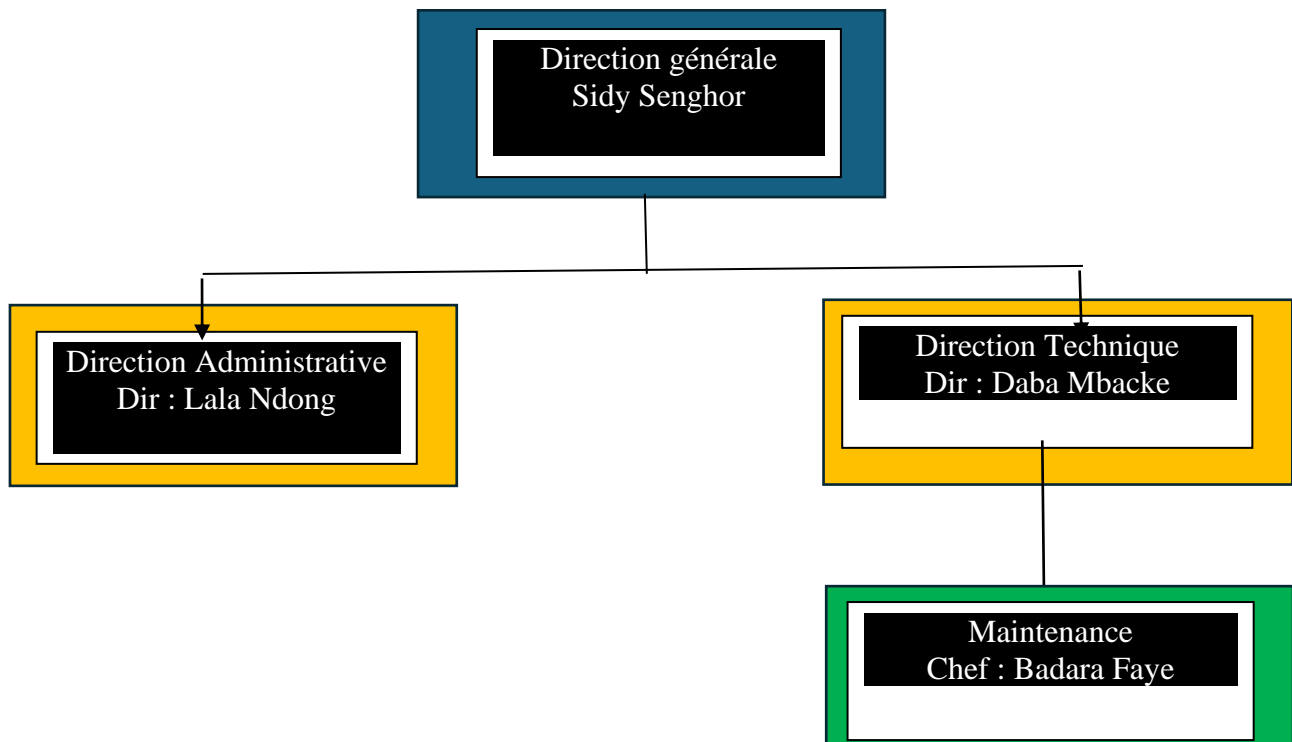
Etu17.sae      nameserver = etu17sw16-2.Etu17.sae
etu17sw16-2.Etu17.sae  internet address = 192.168.108.162
> set type=soa
> Etu17.sae
Serveur :   etu17sw16-2.Etu17.sae
Address:  192.168.108.162

Etu17.sae
    primary name server = etu17sw16-2.Etu17.sae
    responsible mail addr = marietou.Etu17.sae
    serial    = 79
    refresh  = 900 (15 mins)
    retry    = 600 (10 mins)
    expire   = 86400 (1 day)
    default TTL = 3600 (1 hour)
etu17sw16-2.Etu17.sae  internet address = 192.168.108.162
```

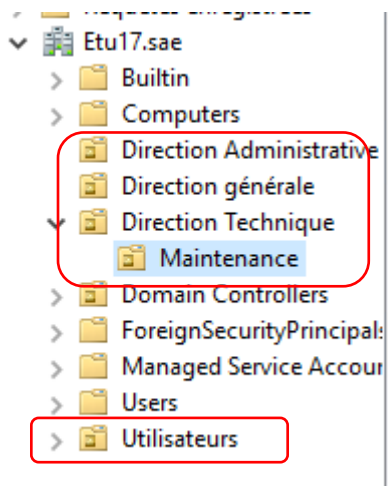
En interrogeant le serveur secondaire, nous constatons que le serveur secondaire assure la redondance et que la résolution de nom est correcte.

III. Partie automatiséation de taches avec PowerShell et mise en place de GPO :

Organigramme de l'entreprise :



Nous allons d'abord créer les différents OU de notre organigramme :



L'OU Utilisateurs créée permet de récupérer l'ensemble de nos utilisateurs qu'on va créer avec le script powershell.

Avec Powershell, nous allons créer l'ensemble de nos utilisateurs à partir d'un fichier csv.

Avec le tutoriel sur [IT-Connect](#), nous avons un script powershell permettant de créer des utilisateurs à partir de ce fichier [Utilisateurs.csv](#).

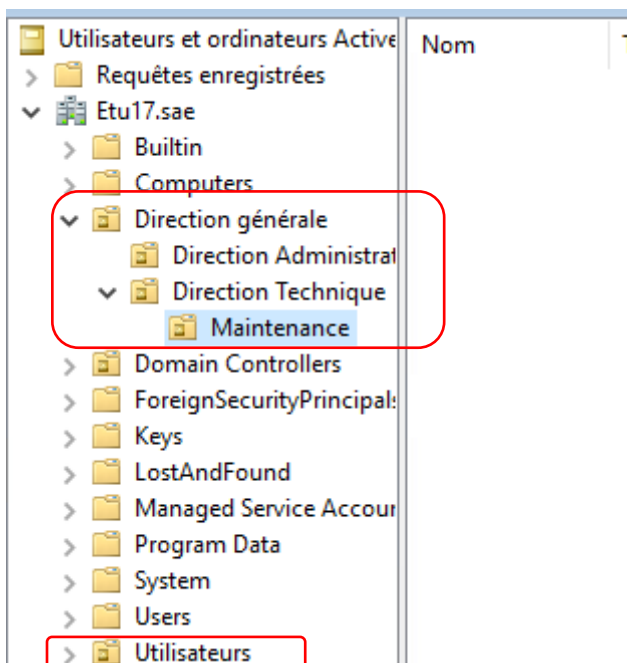
Lancer Powershell ISE, dans Fichier, ouvrir un fichier puis sélection le script créé ensuite apppyer sur run (l'icone vert en haut de la barre d'outils) :

The screenshot shows the Windows PowerShell ISE interface. The script 'Users.ps1' is open in the editor. The script defines variables for user creation and includes a check to see if the user already exists in the AD. If not, it creates the user with specific attributes. The console window at the bottom shows the execution of the script, creating three users: nIdya (Ndong Lala), mdaba (Mbacke Daba), and fbadara (Faye Badara).

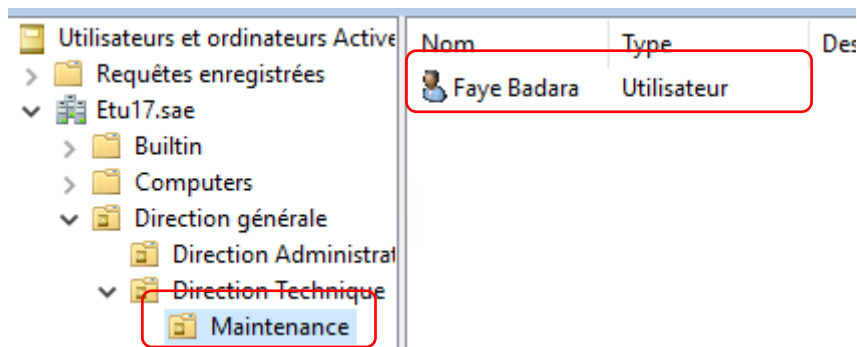
```

7 $UtilisateurNom = $Utilisateur.lenom
8 $UtilisateurLogin = $Utilisateur.Login
9 $UtilisateurEmail = "$UtilisateurLogin@Etu17.sae"
10 $UtilisateurMotDePasse = "Finzat73"
11 $UtilisateurFonction = $Utilisateur.ladescription
12
13 # Vérifier la présence de l'utilisateur dans l'AD
14 if (Get-ADUser -Filter {SamAccountName -eq $UtilisateurLogin})
15 {
16     Write-Warning "L'identifiant $UtilisateurLogin existe déjà dans l'AD"
17 }
18 else
19 {
20     New-ADUser -Name "$UtilisateurNom $UtilisateurPrenom" `
21         -DisplayName "$UtilisateurNom $UtilisateurPrenom" `
22         -GivenName $UtilisateurPrenom `
23         -Surname $UtilisateurNom `
24         -SamAccountName $UtilisateurLogin `
25         -UserPrincipalName "$UtilisateurLogin@Etu17.sae" `
26         -EmailAddress $UtilisateurEmail `
27         -Title $UtilisateurFonction `
28         -Path "OU=Utilisateurs,DC=Etu17,DC=sae" `
29         -AccountPassword(ConvertTo-SecureString $UtilisateurMotDePasse -AsPlainText -Force) `
30         -ChangePasswordAtLogon $false `
31         -Enabled $true
32
33     Write-Output "Création de l'utilisateur : $UtilisateurLogin ($UtilisateurNom $UtilisateurPrenom)"
34 }
35
PS C:\Users\Administrateur.WIN-7G96S96C3QD> C:\Users\Administrateur.WIN-7G96S96C3QD\Downloads\Users.ps1
Création de l'utilisateur : msidy (Senghor Sidy)
Création de l'utilisateur : nIdya (Ndong Lala)
Création de l'utilisateur : mdaba (Mbacke Daba)
Création de l'utilisateur : fbadara (Faye Badara)
  
```

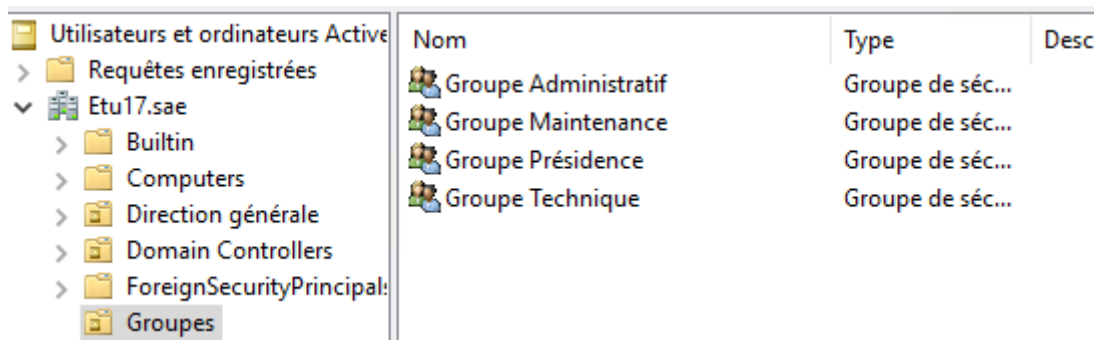
Nous constatons que nos utilisateurs sont créés.



Ensuite, il reste juste qu'à déplacer manuellement les utilisateurs sous leur OU respective. Par exemple, l'utilisateur Badara Faye dans l'OU maintenance :



Création des groupes d'utilisateurs et mettre chaque utilisateur dans leur groupe respectif :



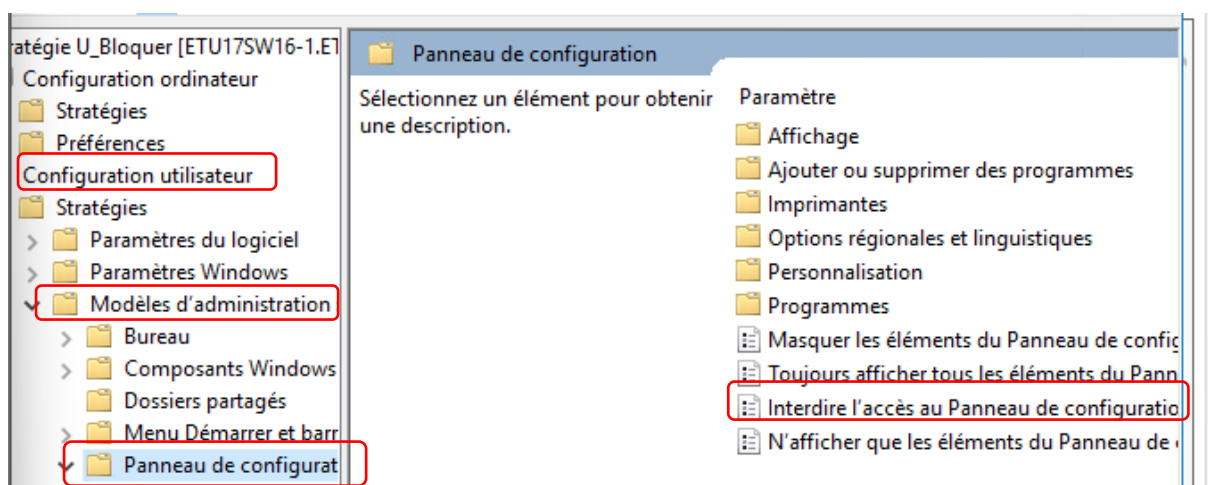
Ces groupes vont nous permettent de mettre des stratégies de groupe ou de faire des délégations, de donner des droits ou restrictions à un groupe.

Mise en place de GPO :

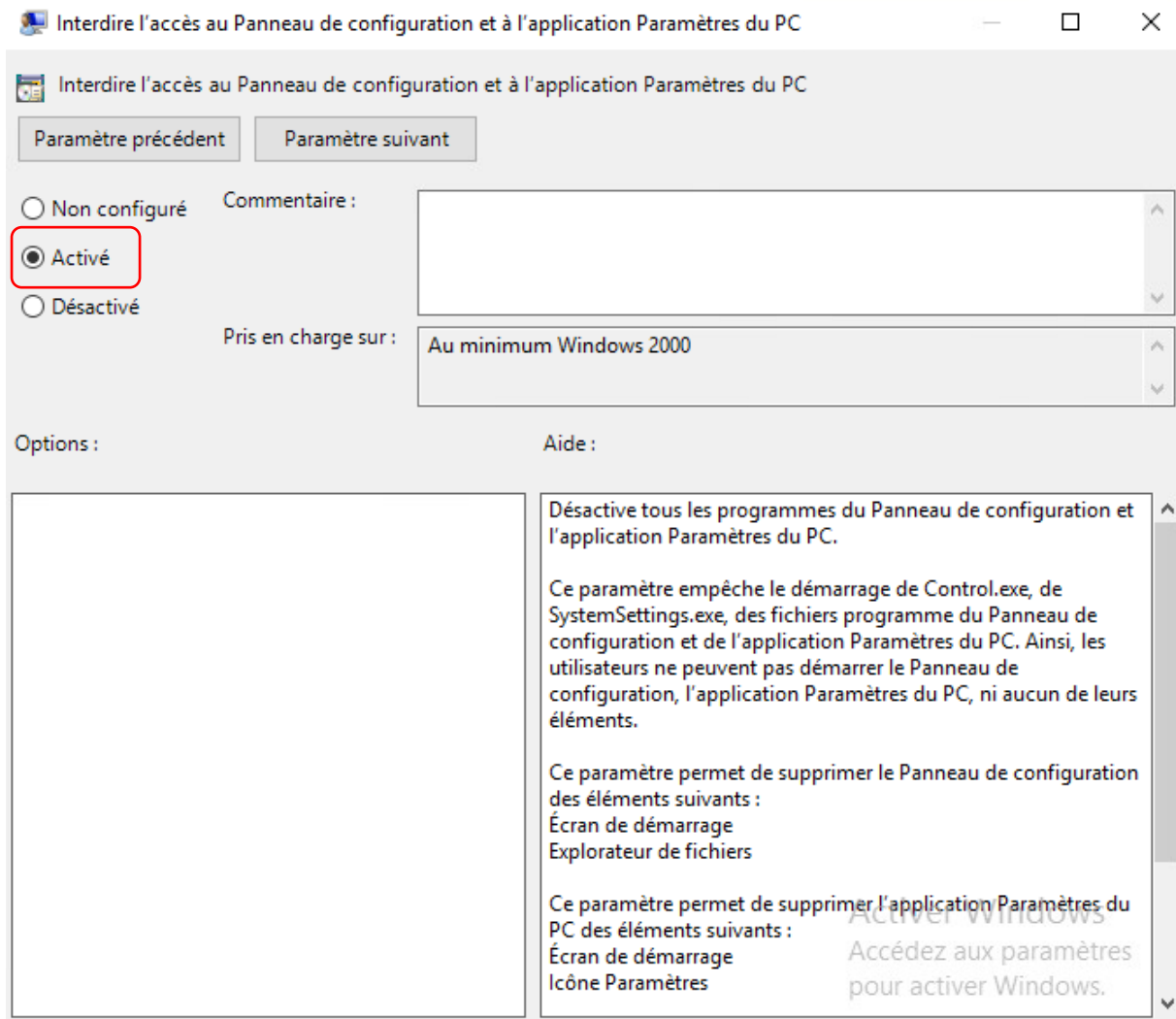
[Comment créer sa première GPO dans l'Active Directory ?](#)

Nous allons créer une stratégie de groupe permettant de bloquer le panneau de configuration :

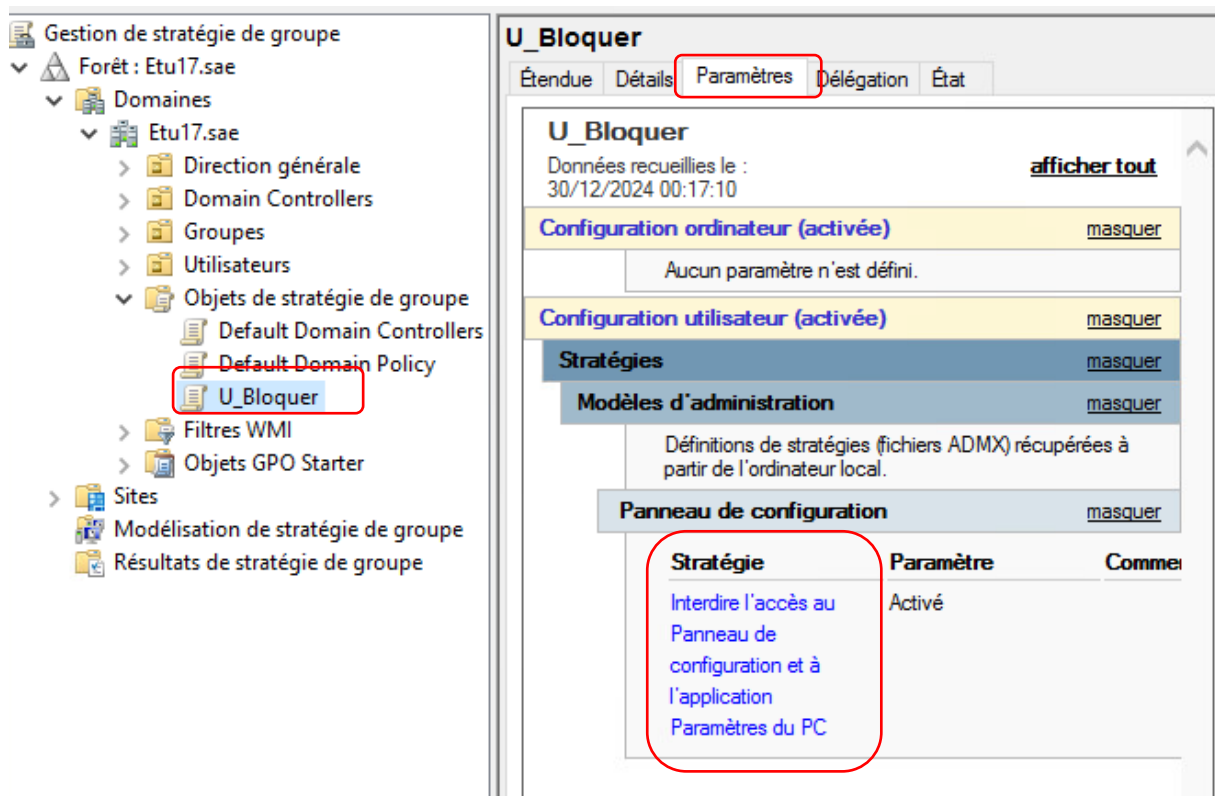
Pour cela, nous allons d'abord créer un nouvel objet de stratégie de groupe dans le gestionnaire de stratégie de groupe, puis faire un clic droit pour modifier cet objet.



Concernant, notre configuration, activez ce paramètre et validez.

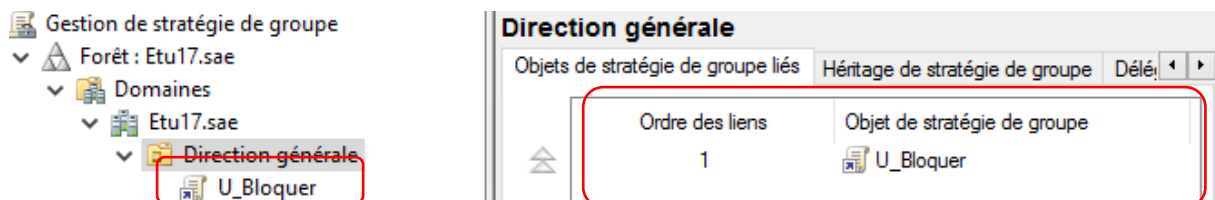


Dans la console GPMC :



Liaison de cette stratégie de groupe à l'active directory :

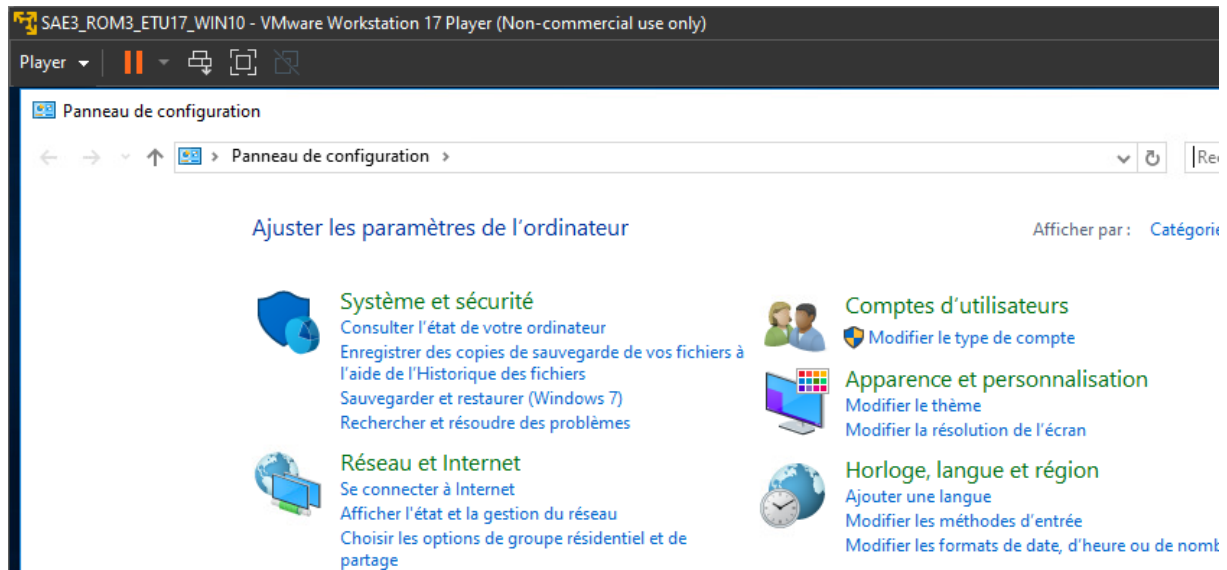
Au niveau de notre OU Direction Générale, faire un clic droit puis Lier un objet de stratégie de groupe existant :



Test de notre GPO depuis une machine cliente :

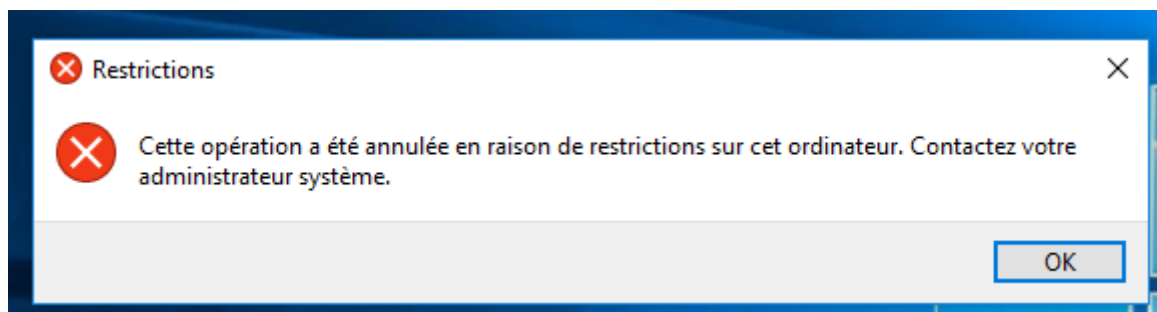
Au premier test, nous constatons que notre stratégie ne fonctionne pas.

On a toujours accès au panneau de configuration :



Dans le cas où la session existera déjà, il se peut que la GPO ne s'applique pas immédiatement. Il existe un temps de rafraîchissement pour les stratégies de groupe, ce qui est d'autant plus vrai pour les stratégies ordinatrices qui s'appliquent généralement au démarrage de la machine. **Pour forcer l'actualisation des stratégies de groupe sur un poste, que ce soit pour les paramètres ordinateurs ou utilisateurs, il y a une commande magique et qu'il est indispensable de connaître : gpupdate /force. Cette commande est associée à l'utilitaire Group Policy Update.**

Après cette commande, si nous essayons d'ouvrir le panneau de configuration, nous avons :

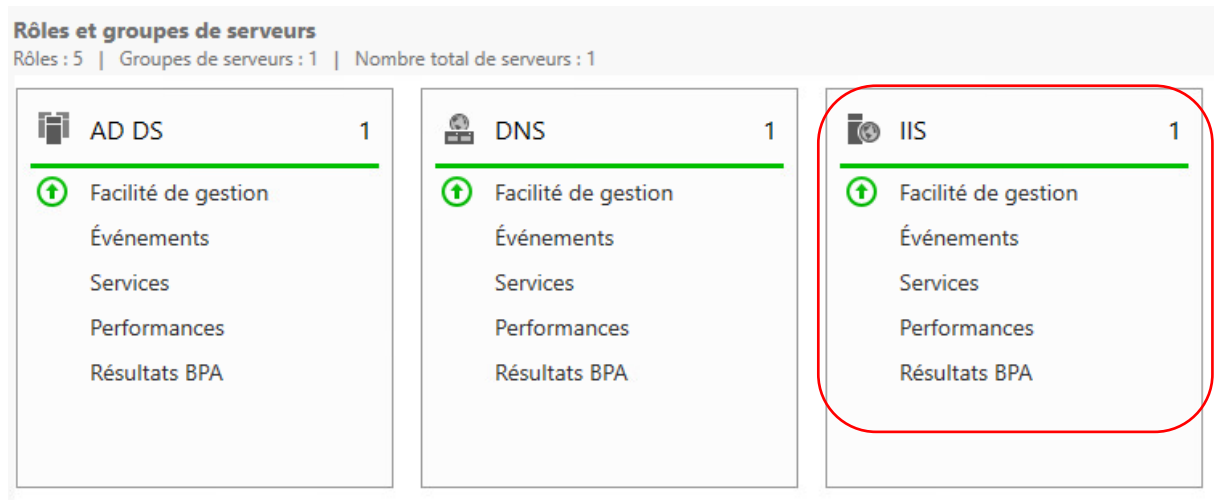


Nous constatons que notre GPO a marché !!!

IV. Serveur Web IIS

IIS est une suite logicielle développée par Microsoft qui permet de gérer un serveur web pour héberger des sites et applications de manière simple et sécurisée.

[Guide d'installation](#)



Une fois le service installé, on va dans gestionnaire de service puis créer notre site **saesite**.

Ajouter un site Web

Nom du site : saesite Pool d'applications : saesite Sélectionner...

Répertoire de contenu

Chemin d'accès physique : C:\ ...

Authentification directe

Se connecter en tant que... Tester les paramètres...

Liaison

Type : https Adresse IP : Toutes non attribuées Port : 443

Nom de l'hôte : saesite

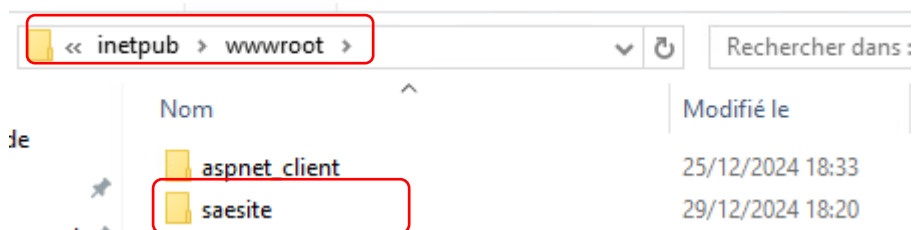
☐ Exiger l'indication de nom du serveur

Certificat SSL : ETU17SW16-1.Etu17.sae Sélectionner... Afficher...

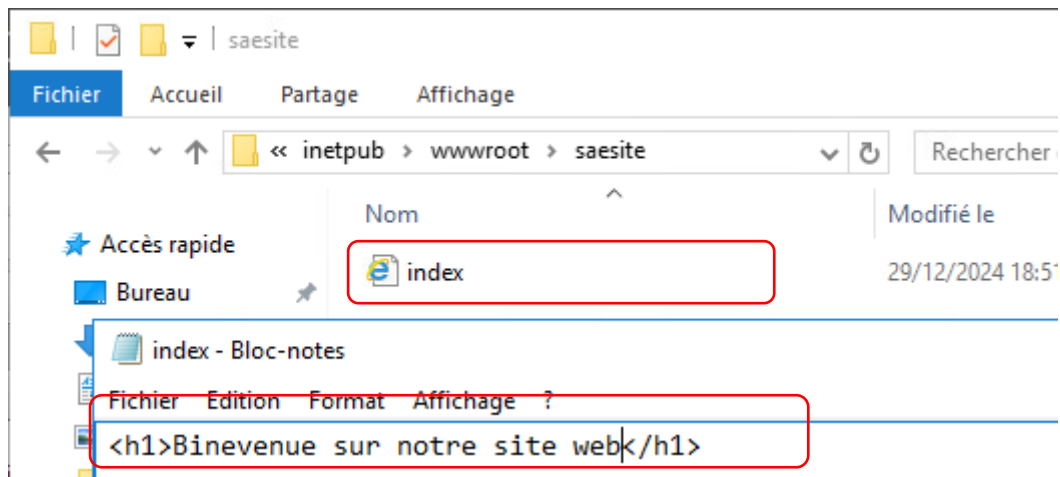
☒ Démarrer le site Web immédiatement

OK Annuler

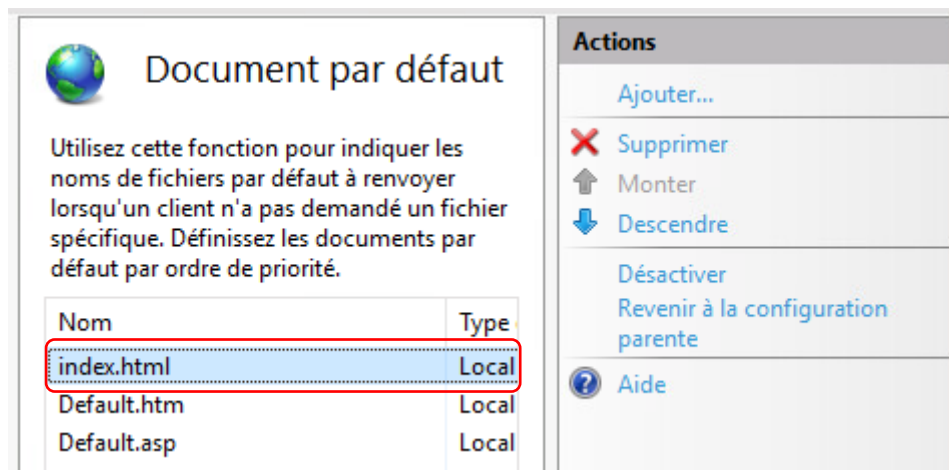
Ensuite dans le dossier **wwwroot**, nous allons créer un dossier **saesite**.



Dans ce dossier nous allons créer un fichier **index.html** :



Ensuite, dans document par défaut, nous allons monter notre fichier **index.html** en première ligne et on redémarre le service.

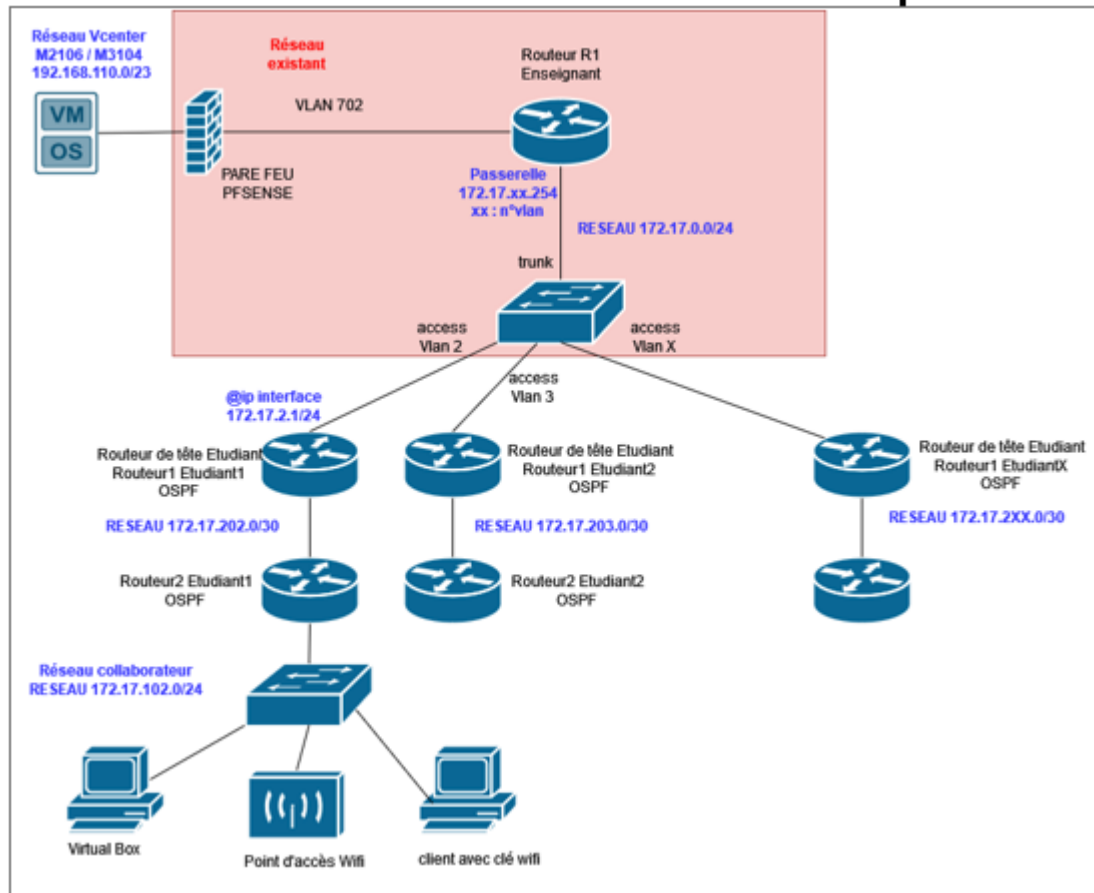


Nous allons accéder à notre site web depuis notre machine cliente avec le nom de notre serveur ou de l'adresse IP :

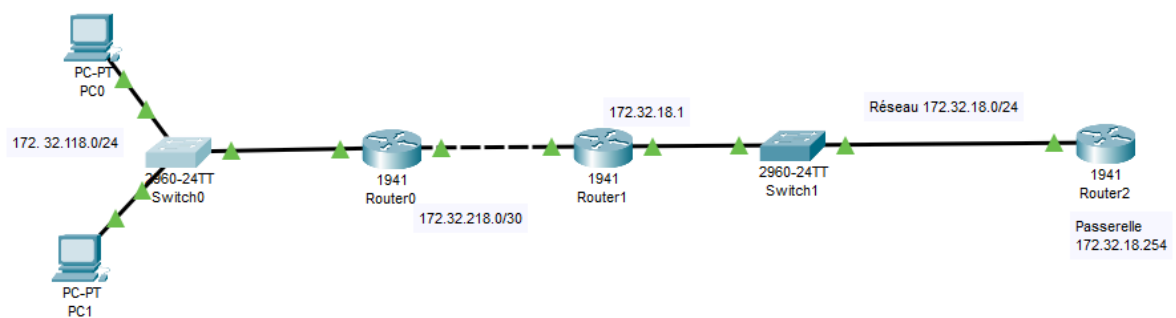


V. Partie Réseau :

La topologie de base est la suivante:



Dans cette, nous allons d'abord faire une simulation sur packet tracer pour ensuite la faire de façon réelle:



Dans la simulation réelle:**Sur le switch du réseau collaborateur :**

Nous avons configuré l'interface en access pour le connecter à un PC, et l'autre interface en mode trunk qui est connecté au routeur 2 étudiant.

```
!  
interface GigabitEthernet1/0/1  
  switchport trunk native vlan 18  
  switchport mode trunk  
!  
interface GigabitEthernet1/0/2  
  switchport access vlan 18  
  switchport mode access  
!
```

Sur le routeur 2 étudiant:

Dans cette configuration, nous avons l'adresse 172.32.118.1 qui la passerelle du réseau collaborateur encapsulé dans le port g0/0/0.18.

Nous avons aussi l'adresse 172.32.218.1/30 qui est l'adresse du réseau reliant le routeur 2 et routeur 1 étudiant.

```
!  
interface GigabitEthernet0/0/0.18  
  encapsulation dot1Q 18  
  ip address 172.32.118.1 255.255.255.0  
!  
interface GigabitEthernet0/0/1  
  ip address 172.32.218.1 255.255.255.252  
  negotiation auto  
!
```

Sur cette partie, nous avons le réseau reliant les deux routeurs et le réseau collaborateur avec le protocole OSPF.

```
!  
router ospf 10  
  network 172.32.118.0 0.0.0.255 area 0  
  network 172.32.218.0 0.0.0.3 area 0  
!
```

Sur le routeur 1 étudiant:

Nous avons l'adresse 172.32.218.2/30 qui est l'adresse du réseau reliant le routeur 2 et routeur 1 étudiant

Nous avons aussi 172.32.18.1/24 avec l'interface reliant au routeur tête du prof.

```
!
interface GigabitEthernet0/0/0
 ip address 172.32.218.2 255.255.255.252
 negotiation auto
!
interface GigabitEthernet0/0/1
 ip address 172.32.18.1 255.255.255.0
 negotiation auto
!
```

Nous avons les réseaux des routeurs étudiants, le réseau collaborateur et le réseau du prof:

```
!
router ospf 10
 network 172.32.18.0 0.0.0.255 area 0
 network 172.32.118.0 0.0.0.255 area 0
 network 172.32.218.0 0.0.0.3 area 0
!
```

Sur notre routeur 2 étudiant :

Avec cette commande, nous avons l'ensemble des réseaux connectés à notre routeur.

```
R2#sh ip ospf database

        OSPF Router with ID (172.32.118.1) (Process ID 10)

        Router Link States (Area 0)

Link ID        ADV Router    Age          Seq#          Checksum Link count
172.32.105.254 172.32.105.254 602          0x8000000A   0x00261A 2
172.32.118.1   172.32.118.1   913          0x80000006   0x004AB5 2
172.32.138.1   172.32.138.1   890          0x80000007   0x004C4D 2
172.32.205.2   172.32.205.2   182          0x80000008   0x00A95C 2
172.32.218.2   172.32.218.2   905          0x80000006   0x00308A 2
172.32.238.1   172.32.238.1   993          0x8000000F   0x00F645 2
172.32.239.1   172.32.239.1   3331         0x8000000B   0x00EFD7 2
172.32.239.2   172.32.239.2   3386         0x8000000D   0x004DE6 2
255.255.255.255 255.255.255.255 176          0x80000020   0x00BDB1 46

        Net Link States (Area 0)

Link ID        ADV Router    Age          Seq#          Checksum
172.32.5.254   255.255.255.255 181          0x80000001   0x00A824
172.32.18.254  255.255.255.255 915          0x80000001   0x00C2EF
172.32.38.254  255.255.255.255 1731         0x80000002   0x00DAAF
172.32.205.2   172.32.205.2   604          0x80000001   0x00DE53
172.32.218.1   172.32.118.1   913          0x80000001   0x0093CE
172.32.238.1   172.32.238.1   993          0x80000002   0x00832A

        Type-5 AS External Link States

Link ID        ADV Router    Age          Seq#          Checksum Tag
0.0.0.0        255.255.255.255 716          0x8000000B   0x00C9D5 10
```

Sur notre routeur 1 étudiant, connecté au routeur tête du prof :

Ici aussi, nous avons l'ensemble des réseaux connectés au routeur :

```
R1#sh ip ospf database

        OSPF Router with ID (172.32.218.2) (Process ID 10)

        Router Link States (Area 0)

Link ID        ADV Router    Age          Seq#          Checksum Link count
172.32.105.254 172.32.105.254 660          0x80000000A  0x00261A 2
172.32.118.1   172.32.118.1   973          0x800000006  0x004AB5 2
172.32.138.1   172.32.138.1   947          0x800000007  0x004C4D 2
172.32.205.2   172.32.205.2   240          0x800000008  0x00A95C 2
172.32.218.2   172.32.218.2   962          0x800000006  0x00308A 2
172.32.238.1   172.32.238.1   1051         0x80000000F  0x00F645 2
172.32.239.1   172.32.239.1   3389         0x80000000B  0x00EFD7 2
172.32.239.2   172.32.239.2   3444         0x80000000D  0x004DE6 2
255.255.255.255 255.255.255.255 234          0x800000020  0x00BDB1 46

        Net Link States (Area 0)

Link ID        ADV Router    Age          Seq#          Checksum
172.32.5.254   255.255.255.255 239          0x800000001  0x00A824
172.32.18.254  255.255.255.255 973          0x800000001  0x00C2EF
172.32.38.254  255.255.255.255 1789         0x800000002  0x00DAAF
172.32.205.2   172.32.205.2   662          0x800000001  0x00DE53
172.32.218.1   172.32.118.1   973          0x800000001  0x0093CE
172.32.238.1   172.32.238.1   1051         0x800000002  0x00832A

        Type-5 AS External Link States

Link ID        ADV Router    Age          Seq#          Checksum Tag
0.0.0.0        255.255.255.255 774          0x80000000B  0x00C9D5 10
```

Mise en place du DHCP au niveau du routeur R2 relié au switch étudiant :

En mettant le réseau opérateur ainsi que l'IP de nos serveurs primaire et secondaire :

```
ip dhcp pool seydi_sae3
 network 172.32.118.0 255.255.255.0
 default-router 172.32.118.1
 dns-server 192.168.108.161
```

La carte ethernet de notre machine au niveau du réseau collaborateur :


```

Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : Intel(R) Ethernet Connection (17) I219-LM
Adresse physique . . . . . : 64-4E-D7-69-3F-7C
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::3df4:f94a:858e:2a74%15(préfééré)
Adresse IPv4. . . . . : 172.32.118.2(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : jeudi 9 janvier 2025 15:39:47
Bail expirant. . . . . : vendredi 10 janvier 2025 15:39:48
Passerelle par défaut. . . . . : 172.32.118.1
Serveur DHCP . . . . . : 172.32.118.1
IAID DHCPv6 . . . . . : 191123159
DUID de client DHCPv6. . . . . : 00-01-00-01-2E-1F-04-BE-64-4E-D7-69-3F-7C
Serveurs DNS. . . . . : 192.168.108.161
NetBIOS sur Tcpi. . . . . : Activé

```

Test de connectivité depuis un PC du réseau collaborateur vers la passerelle du routeur enseignant qui a pour adresse 172.32.18.254 :

```

C:\Users\Admin>ping 172.32.18.254

Envoi d'une requête 'Ping' 172.32.18.254 avec 32 octets de données :
Réponse de 172.32.18.254 : octets=32 temps=1 ms TTL=253
Réponse de 172.32.18.254 : octets=32 temps=1 ms TTL=253
Réponse de 172.32.18.254 : octets=32 temps=1 ms TTL=253
Réponse de 172.32.18.254 : octets=32 temps=1 ms TTL=253

Statistiques Ping pour 172.32.18.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms

```

Depuis le réseau collaborateur, nous allons tester la connectivité avec nos machines virtuelles.

Vers le serveur primaire :

```

C:\Users\Admin>ping 192.168.108.161

Envoi d'une requête 'Ping' 192.168.108.161 avec 32 octets de données :
Réponse de 192.168.108.161 : octets=32 temps=1 ms TTL=124
Réponse de 192.168.108.161 : octets=32 temps=1 ms TTL=124

Statistiques Ping pour 192.168.108.161:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
Ctrl+C
^C

```

Vers notre machine cliente :

```
C:\Users\Admin>ping 192.168.108.163

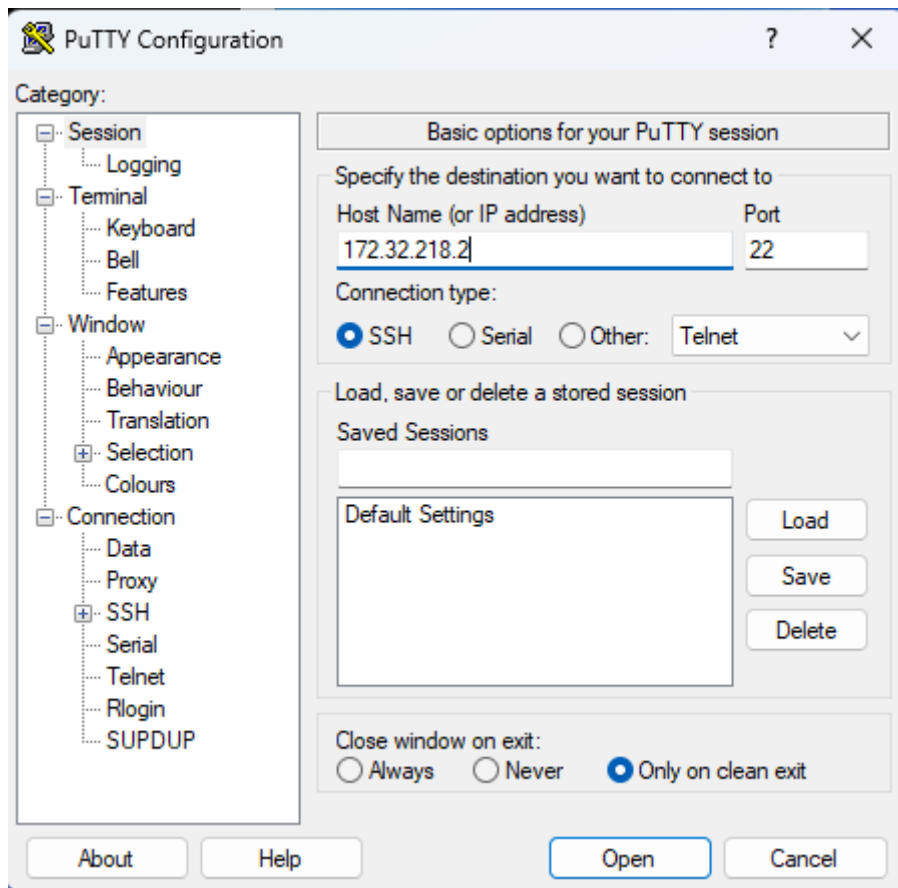
Envoi d'une requête 'Ping' 192.168.108.163 avec 32 octets de données :
Réponse de 192.168.108.163 : octets=32 temps=1 ms TTL=124
Réponse de 192.168.108.163 : octets=32 temps=8 ms TTL=125
Réponse de 192.168.108.163 : octets=32 temps=1 ms TTL=124
Réponse de 192.168.108.163 : octets=32 temps=1 ms TTL=125

Statistiques Ping pour 192.168.108.163:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 8ms, Moyenne = 2ms
```

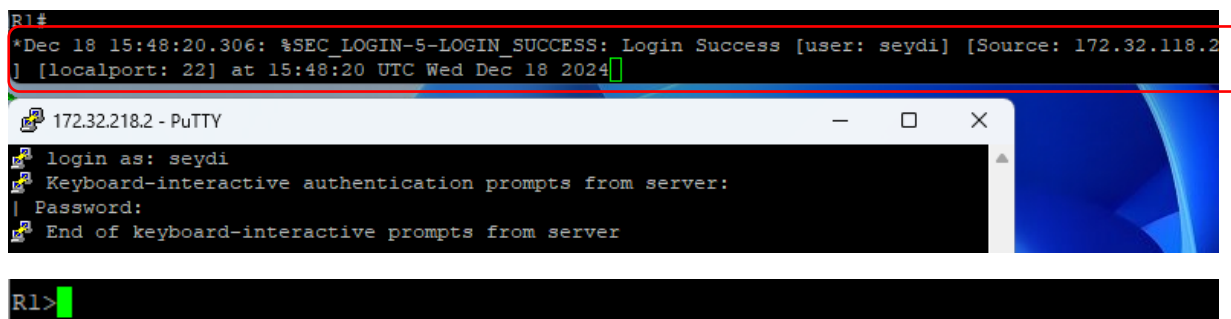
Mise en place de ssh dans tous les équipements :

```
R1#sh ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha2-256,hmac-sha2-512,hmac-shal,hmac-shal-96
KEX Algorithms:diffie-hellman-group-exchange-shal,diffie-hellman-group14-shal
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 2048 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): R1.EtU17.sae
Modulus Size : 2048 bits
ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAQDw7acySQklw/ix9Rin9w6AqGq5SAgvfd3yh7/+YJ6t
ym9fBx4jJknGhlGkpfplKDKTp5zI3W3Y0tLfT7m/0qNLSobZKEHSZMnOs9AhJ0tgazfdNt/iqDSBK8T0
w7VYRVGKiX0kiB/YFekZc+1S/YYwFH1OaFSdE0cb2sx15Xp+NMj1P3sIQBaLD8Dw4AfUykMtIXeqMR1L
0Zd9Mr1OvvqWTOOrMW9ASznW+oj3EvDO7D2JCH44ENx7tYUABdKH9a8/3hdveaFkxRlyiMP26VvzLBd9+
ALTtpIj3nSF0BasbdCsU+yoJfhchFWwgaXv/10xG0Bfrr/+5M1q5gRIssD5F
```

Test de connexion à distance :



La connexion à distance a fonctionné :

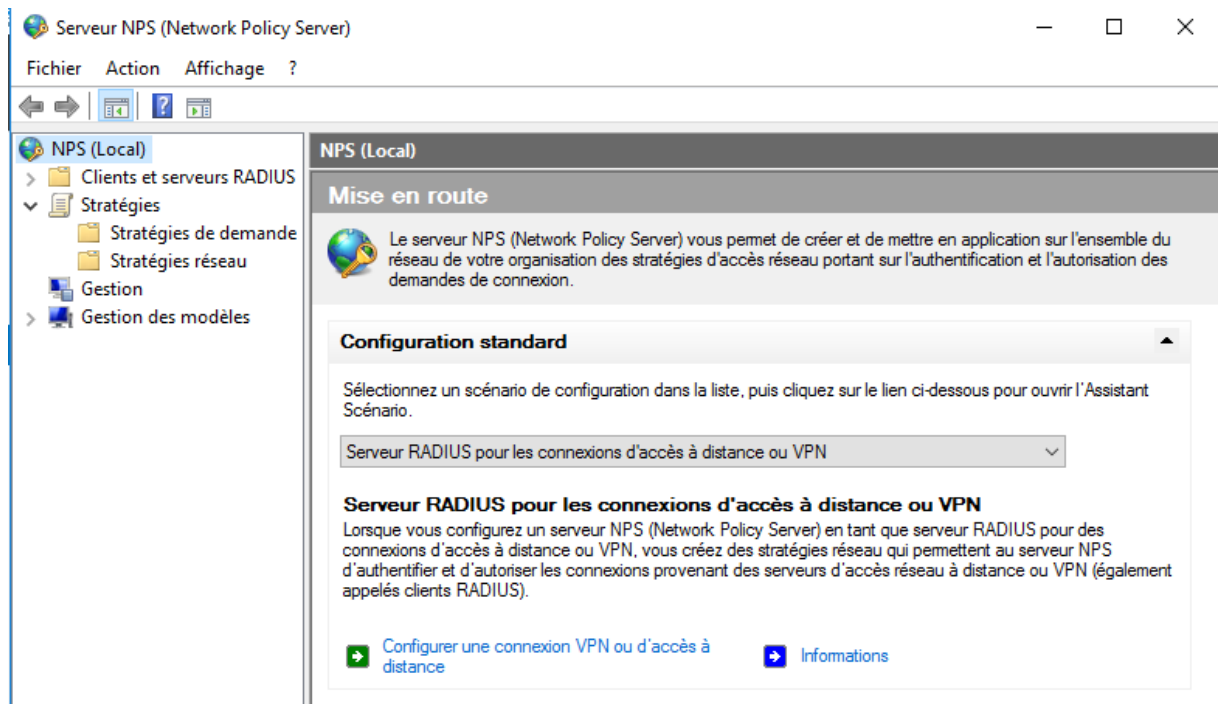


VI. Partie WIFI :

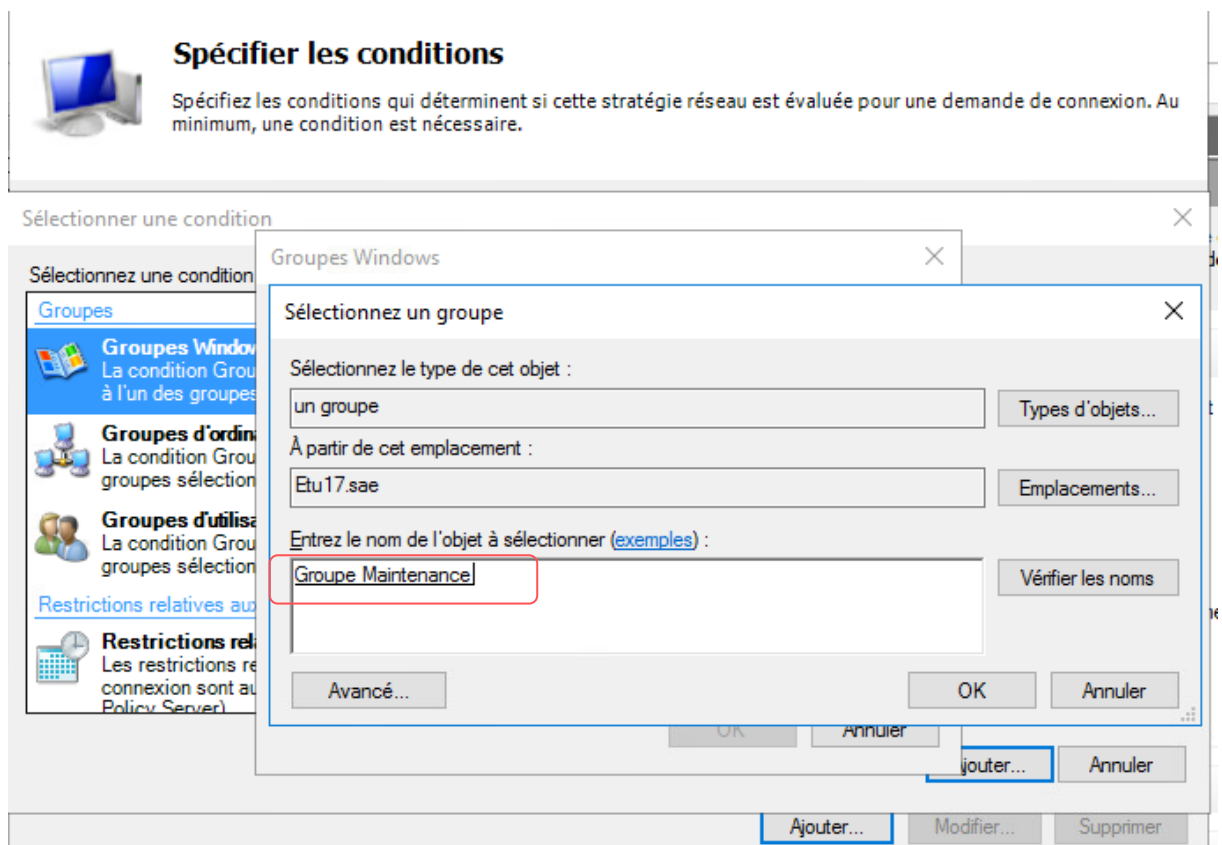
1- Installation d'un serveur radius :

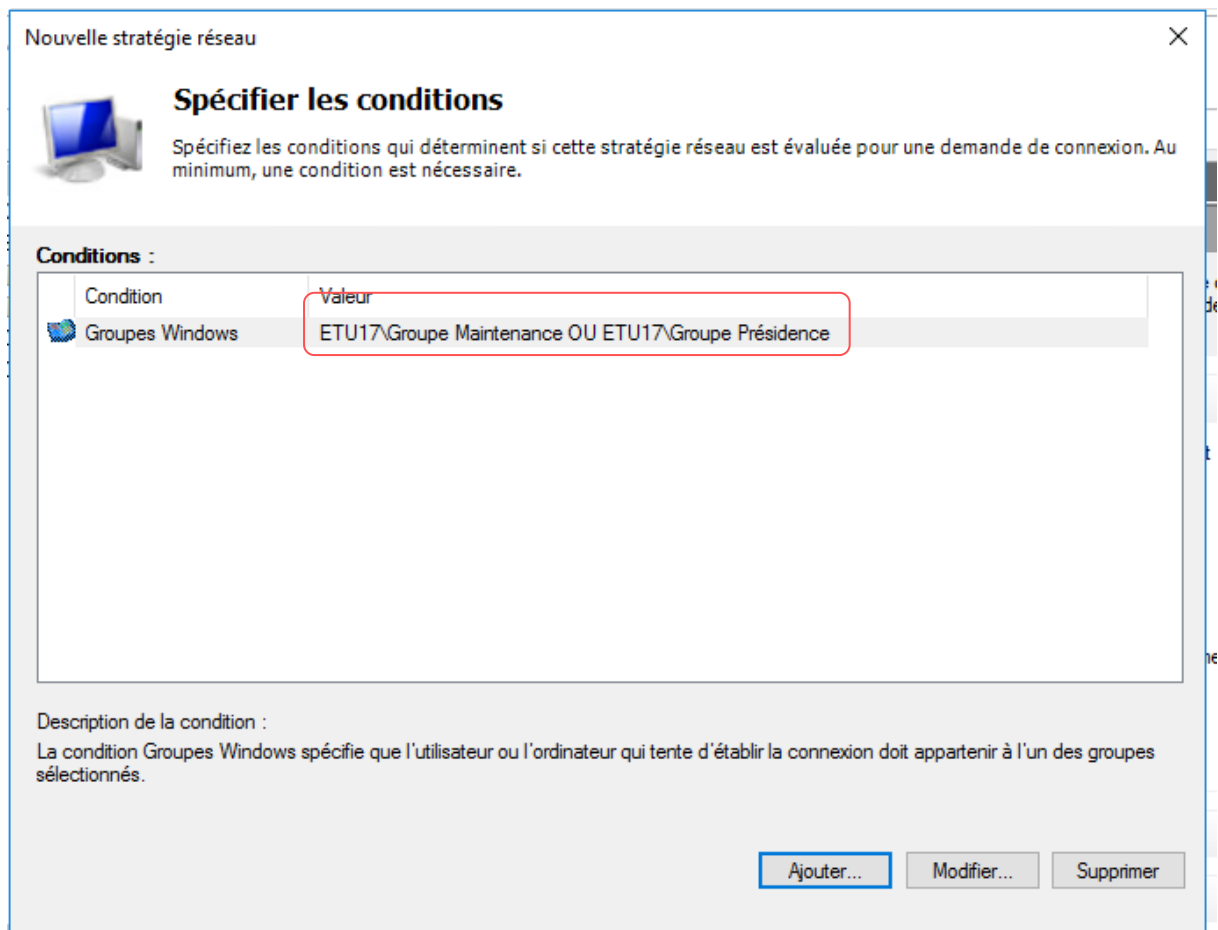
<https://all-it-network.com/radius/>

Après installation :

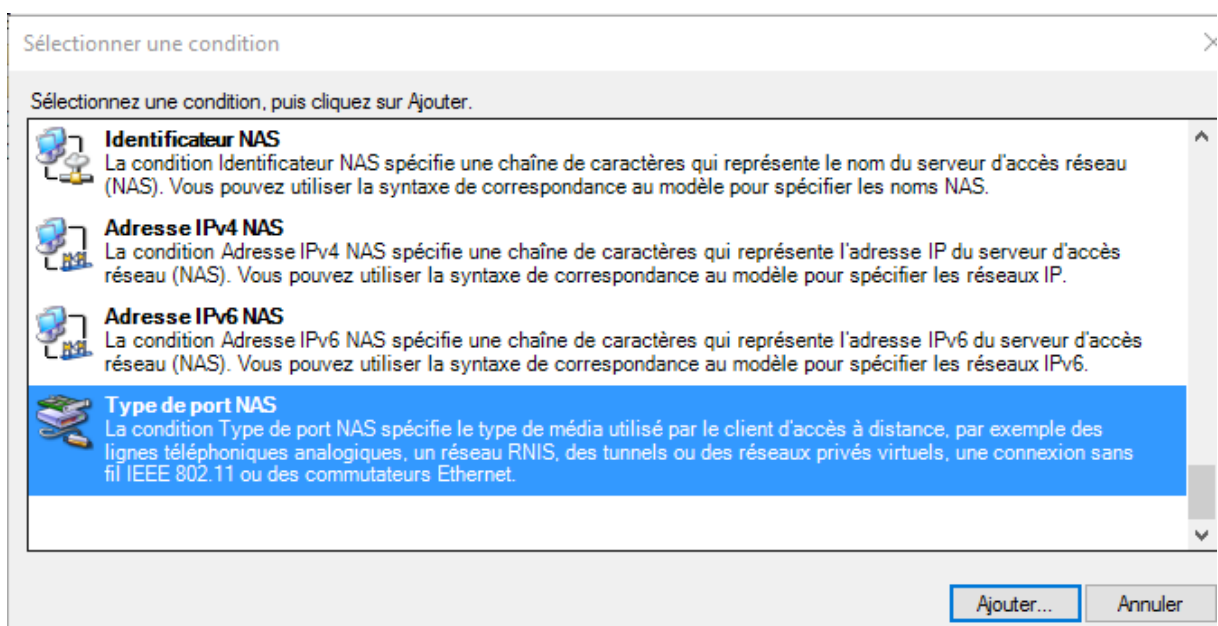


Dans la partie spécifier les conditions, nous avons ajouté le groupe maintenance et présidence créés sur l'AD comme étant les seuls à se connecter au wifi :





Cette fois ci sélectionner « Type de port NAS » et cliquer sur « Ajouter... ».



Puis sélectionner :

Type de port NAS [X]

Spécifiez les types de médias d'accès nécessaires pour correspondre à cette stratégie.

Types de tunnels pour connexions d'accès à distance et VPN standard

- ☐ Asynchrone (Modem)
- ☐ RNIS synchrone
- ☐ Synchrone (ligne T1)
- ☐ Virtuel (VPN)

Types de tunnels pour connexions 802.1X standard

- ☐ Ethernet
- ☐ FDDI
- ☒ Sans fil - IEEE 802.11
- ☐ Token Ring

Autres

- ☐ RNIS asynchrone V.120
- ☐ RNIS synchrone
- ☒ Sans fil - Autre
- ☐ SDSL - DSL symétrique

OK Annuler

Nouvelle stratégie réseau [X]

Spécifier les conditions

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

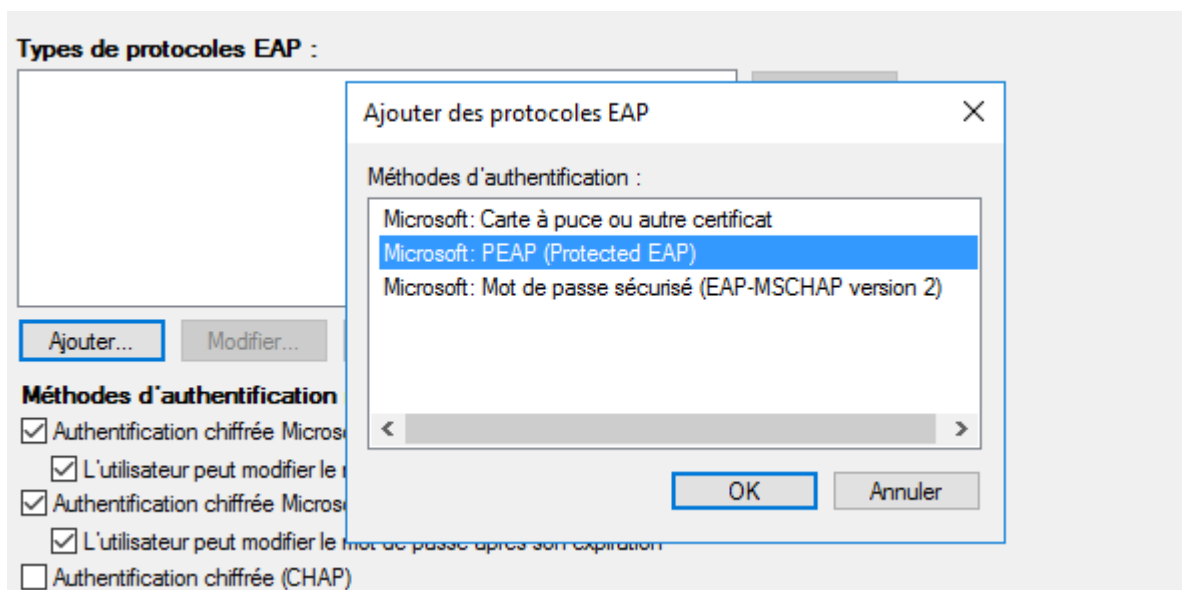
Conditions :

Condition	Valeur
Groupes Windows	ETU17\Groupe Maintenance OU ETU17\Groupe Présidence
Type de port NAS	Sans fil - IEEE 802.11 OU Sans fil - Autre

Laisser cocher « Accès accordé » et cliquer sur « Suivant ».



Sélectionner « Microsoft PEAP » cliquez sur « OK » et cliquez sur « Suivant » sur l'autre fenêtre.



Sur la fenêtre suivante « Configurer des contraintes », laissez par défaut et cliquez sur « Suivant ». Faites de même pour la fenêtre « Configurer les paramètres ». Une fenêtre récapitulant la configuration va apparaître cliquez sur « Terminer ».

- Ajout de la borne :

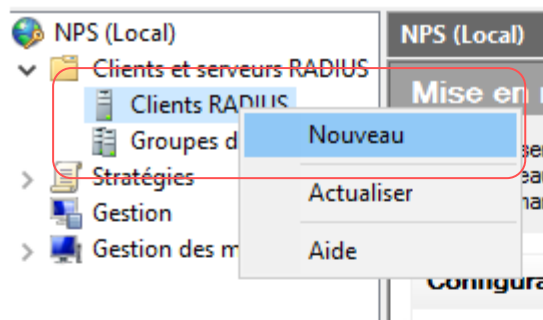
pour que l'accès fonctionne, nous allons devoir ajouter la borne WiFi sur le serveur **RADIUS**. Elle va avoir le rôle de NAS (Network Access Server) qui est un équipement intermédiaire entre le serveur **RADIUS** et l'utilisateur. Allez dans le

gestionnaire de serveur et cliquez sur « Outils » puis sur « Serveur NPS (Network Policy Server) »:

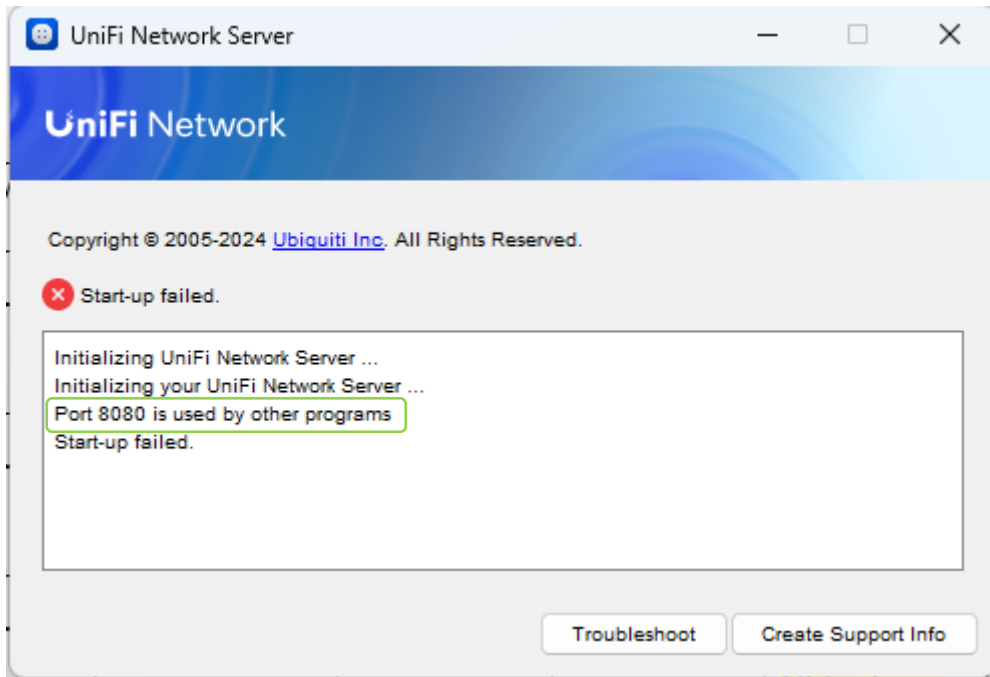
Nous allons renseigner les informations de la borne wifi sur le serveur.

- Laissez coché « Activer ce client RADIUS ».
- Nom convivial : Entrer le nom d'hôte de la borne WiFi.
- Adresse IP : Renseigner l'adresse IP de la borne WiFi donnée par le dhcp :
- Pour le secret laissez coché « Manuel » et renseigner la clé que vous saisissez aussi sur la borne WiFi.

Cliquez ensuite sur « OK ».

A screenshot of the 'Nouveau client RADIUS' (New RADIUS Client) dialog box. The 'Paramètres' (Parameters) tab is active. The 'Activer ce client RADIUS' checkbox is checked. Under 'Nom et adresse', the 'Nom convivial' (Friendly name) field contains 'seydi_wifi' and the 'Adresse (IP ou DNS)' (IP or DNS address) field contains '172.32.118.4'. In the 'Secret partagé' (Shared secret) section, the 'Manuel' (Manual) radio button is selected. The 'Secret partagé' field and its confirmation field both contain five dots, indicating masked text. The 'OK' and 'Annuler' (Cancel) buttons are at the bottom right.

2- Nous allons télécharger et installer le contrôleur UBIQUITI pour votre borne.
Après l'installation, on vérifie quelles connexions réseau utilisent le port 8080.



La première commande pour vérifier et la deuxième commande qui termine de force le processus utilisant le port 8080 dont l'identifiant PID est 9152.

```
PS C:\windows\system32> netstat -ano | findstr 8080
TCP 0.0.0.0:8080 0.0.0.0:0 LISTENING 9152
TCP 0.0.0.0:48080 0.0.0.0:0 LISTENING 7728
PS C:\windows\system32> taskkill /F /PID 9152
Opération réussie : le processus avec PID 9152 a été terminé.
```

Après cette étape, nous avons :



Cliquer sur Manage Server in Browser puis créer un compte :



Set Local Access Credentials

Use these credentials to locally access your Network Server. [Learn More](#)

Username

sm08386y

Password

•••••

Confirm Password

•••••

Email

marietou.ndiaye.seydi@etu.univ-st-etienne.fr

Après avoir fait une réinitialisation du point d'accès, cliquer sur **Unifi Devices**, nous constatons que le point d'accès connecté au switch du réseau étudiant a obtenu une adresse IP : 172.32.118.5 par le DHCP :

Type	Name	Application	Status	IP Address	Uplink
•	UAP-AC-Lite	Network	Up to date	172.32.118.5	GbE

Dans Profiles → Radius, cliquer sur Create new pour ajouter le radius créé au niveau du serveur en renseignant l'IP du serveur ainsi que le secret partagé :

Search Settings

WiFi

Networks

Internet

VPN

Security

Routing

Profiles

System

Network 9.0.108

Submit Support Ticket

< Name seydi_wifi

RADIUS Assigned VLAN Support

Wired Networks i ☐

Wireless Networks i ☐

RADIUS Settings

TLS i ☐

Authentication Servers

IP Address 1812 Shared Secret i Add

IP Address	Port	Shared Secret	Edit
192.168.108.161	1812	

Accounting ☐

Interim Update Interval ☐

Création des deux SSID :

- Un pour les membres de l'entreprise : mdp : seydiseydi

Name seydi_network

Broadcasting APs i ☒ All ☐ Specific ☐ Groups

Advanced

Auto Manual

Private Pre-Shared Keys i ☐

Hotspot 2.0 i

☒ Off ☐ Captive Portal ☐ Passpoint

Security Protocol ⓘ

WPA2 Enterprise

RADIUS Profile

seydi_wifi

NAS ID

☐ AP MAC ☐ Site Name ☐ AP Name ☒ BSSID ☐ Custom

DAS/DAC (CoA) ⓘ

☐

PMF ⓘ

☐ Required ☐ Optional ☒ Disabled

Group Rekey Interval ⓘ

☐ 0 Sec

WiFi Blackout Scheduler ⓘ

Off On

Add WiFi Network

Cancel

Name	Network	Broadcasting APs	WiFi Band	Clients	Security
seydi_network	Default	All APs	2.4 GHz 5 GHz	-	WPA2 Enterprise

Create New

Manage

Radios

Go To Radio Manager

Channelization

Optimize Now

☐ Channel Optimization ⓘ

2.4 GHz 2412-2484 MHz

5 GHz 5180-5885 MHz

20 MHz 1 2 3 4 5 6 7 8 9 10 11 12 13 -

20 MHz 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 144 148 152 156 160

40 MHz 3 4 5 6 7 8 9 10 11 12

40 MHz 38 42 46 50 54 58 62 66 102 106 110 114 118 122 126 130 134 138 142 146 150

80 MHz 42 58 106 122 138 154

80 MHz 42 58 106 122 138 154

160 MHz 50 114

160 MHz 50 114

In Use DFS Not available ⓘ

- L'autre pour invités, visiteurs de l'entreprise : mdp : seydivisite

Name	seydi_visiteurs
Broadcasting APs ⓘ	<input checked="" type="radio"/> All <input type="radio"/> Specific <input type="radio"/> Groups
Advanced	<input type="radio"/> Auto <input checked="" type="radio"/> Manual
Private Pre-Shared Keys ⓘ	<input type="checkbox"/>
Hotspot 2.0 ⓘ	<input type="radio"/> Off <input checked="" type="radio"/> Captive Portal <input type="radio"/> Passpoint

i We have applied your [Hotspot Portal](#) to this WiFi name. By default, portal guests will be isolated from other guests and network resources.

i Hotspot Portal can be found in [Insights](#).

Diminution du débit :

Network

Search Settings

WiFi

Networks

Internet

VPN

Security

Routing

Profiles

System

Name

debit

Download Bandwidth Limit ⓘ

2.4 Mbps

Upload Bandwidth Limit ⓘ

5 Mbps

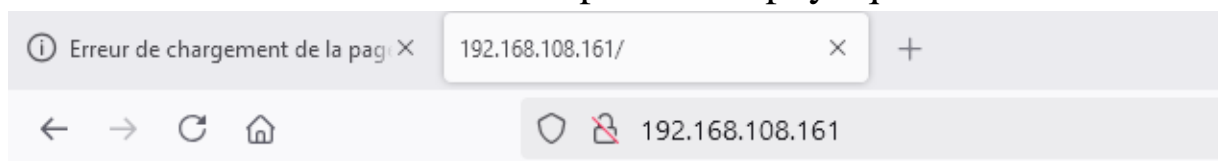
Test de la connexion sur un PC physique :

Nous allons une machine physique dans notre domaine Etu17.sae et se connecter avec un utilisateur qui a accès à notre wifi, définit avec les stratégies réseaux lors de la création du client radius.

Pour cela, au niveau de notre serveur primaire, nous allons changer la passerelle en mettant la passerelle du routeur prof : 172.32.18.254.

Au niveau de la machine, après intégration, nous allons nous connecter avec l'utilisateur, puis avec la clé wifi se connecter au wifi.

Nous constatons que nous arrivons à se connecter au wifi et on aussi accès à notre site web depuis le PC physique.



Bienvenue sur notre site web

VII. Veille Technologie

Dans cette partie, nous allons utiliser Zabbix qui est un outil open-source de supervision et de surveillance informatique. Il permet de suivre les performances des infrastructures informatiques, comme les serveurs, les réseaux, les bases de données, et les applications.

Pour cela, nous allons installer Zabbix Server et l'interface Web sur notre machine debian puis installer l'agent Zabbix sur la machine Windows.

1. Installation de Zabbix server sur debian :

Etape 1 :

Avant toute installation, il est toujours recommandé de mettre à jour le système. `# apt update & upgrade`

Etape 2 : Installation et configuration zabbix

- Installation d'une repository zabbix :

Pour obtenir la dernière version de Zabbix, vous devez ajouter le dépôt officiel de Zabbix à votre système.

Avec les commandes :

```
# wget https://repo.zabbix.com/zabbix/7.2/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.2+debian12_all.deb
```

```
# dpkg -i zabbix-release_latest_7.2+debian12_all.deb
```

#apt update (ces commandes à exécuter en tant que super utilisateur)

- Installation de zabbix server, frontend, agent :

apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent -y

Etape 3 : Installer et configurer la base de données (MYSQL)

Zabbix utilise une base de données pour stocker ses données. Dans cette étape, nous allons installer MySQL, le configurer pour la sécurité, puis créer une base de données spécifique pour Zabbix.

- Installation de MySQL- server avec la commande : **apt install mariadb-server -y**
- Connection à l'interface de ligne de commande de MySQL en utilisant la commande : **# mysql -u root -p**

```
root@seydi:~# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.5.26-MariaDB-0+deb11u2 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> █
```

- Maintenant, création d'une base de données pour Zabbix et attribution des droits nécessaires :

```
root@seydi:~# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 10.5.26-MariaDB-0+deb11u2 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0,001 sec)

MariaDB [(none)]> create user zabbix@localhost identified by 'fina';
Query OK, 0 rows affected (0,009 sec)

MariaDB [(none)]> grant all privileges on zabbix.*to zabbix@localhost;
Query OK, 0 rows affected (0,002 sec)

MariaDB [(none)]> set global log_bin_trust_function_creators=1;
Query OK, 0 rows affected (0,000 sec)
```

Mdp : **nafi** au lieu de **fina**

Pour résumer, nous n'avons créé une base de données nommée zabbix, un nom d'utilisateur zabbix avec un mot de passe nafi. Et on active l'option `log_bin_trust_function_creators`.

Une fois ces étapes terminées, notre base de données MySQL est alors prête à être utilisée par Zabbix Server.

- Importez le schéma de la base Zabbix :
`zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --defaultcharacter-set=utf8mb4 -uzabbix -p zabbix` en renseignant le mdp créé avec la base de donnée.
Après désactiver l'option `log-bin-trust-function-creators` après l'importation du schéma de base de données :
`set global log_bin_trust_function_creators = 0;`

Etape 4: CONFIGURATION DE ZABBIX AVEC MYSQL

- Maintenant que Zabbix est installé, il est essentiel de le configurer pour qu'il interagisse correctement avec MySQL. Éditez le fichier de configuration de Zabbix pour lui indiquer comment se connecter à la base de données :
`# nano /etc/zabbix/zabbix_server.conf`
Recherchons et modifions les lignes suivantes avec les bonnes valeurs :
`DBHost=localhost`
`DBName=zabbix`
`DBUser=zabbix`
`DBPassword=nafi`
- Lancer le service Zabbix et s'assurez-vous qu'il démarre automatiquement au démarrage :
`# systemctl restart zabbix-server zabbix-agent apache2`
`# systemctl enable zabbix-server zabbix-agent apache2`

Étape 5 : Configuration du frontend

Le frontend Zabbix offre une interface web conviviale pour surveiller vos ressources réseau, vos serveurs, vos périphériques réseau, et plus encore. Installer le paquet nécessaire pour le frontend Zabbix en utilisant la commande suivante : `# apt install zabbix-frontend-php`

Etape 6 : ACCÉDEZ A L'INTERFACE WEB DE ZABBIX

Après avoir correctement installé et configuré Zabbix, l'étape suivante est d'accéder à son interface web pour commencer la surveillance des infrastructures.

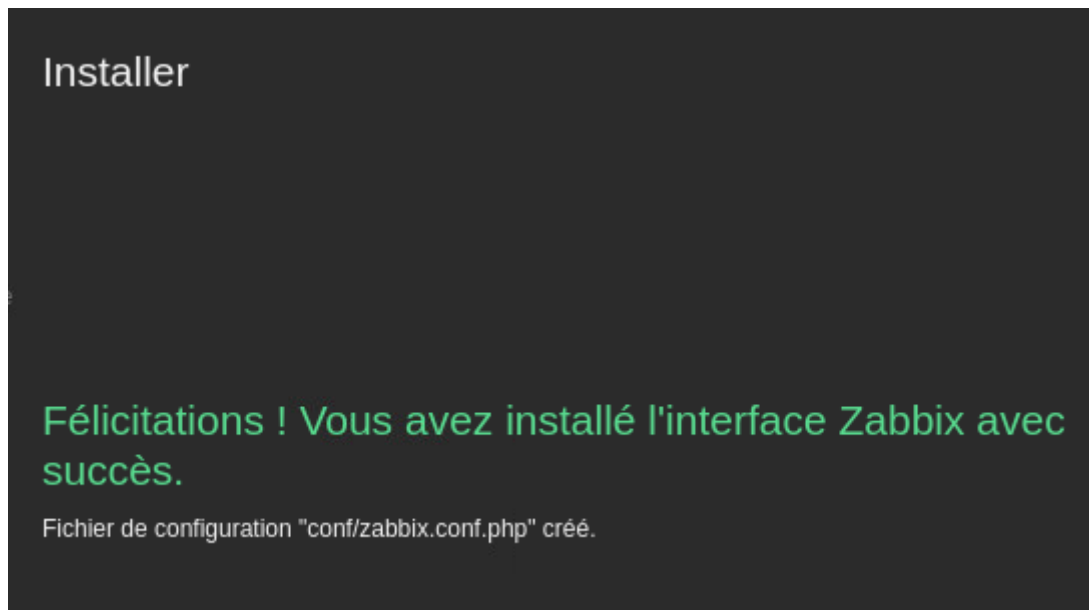
Ouvrez un navigateur et saisissez l'URL du serveur Zabbix. # <http://192.168.108.165/zabbix>



Cliquez sur next step et suivez la configuration de Zabbix.

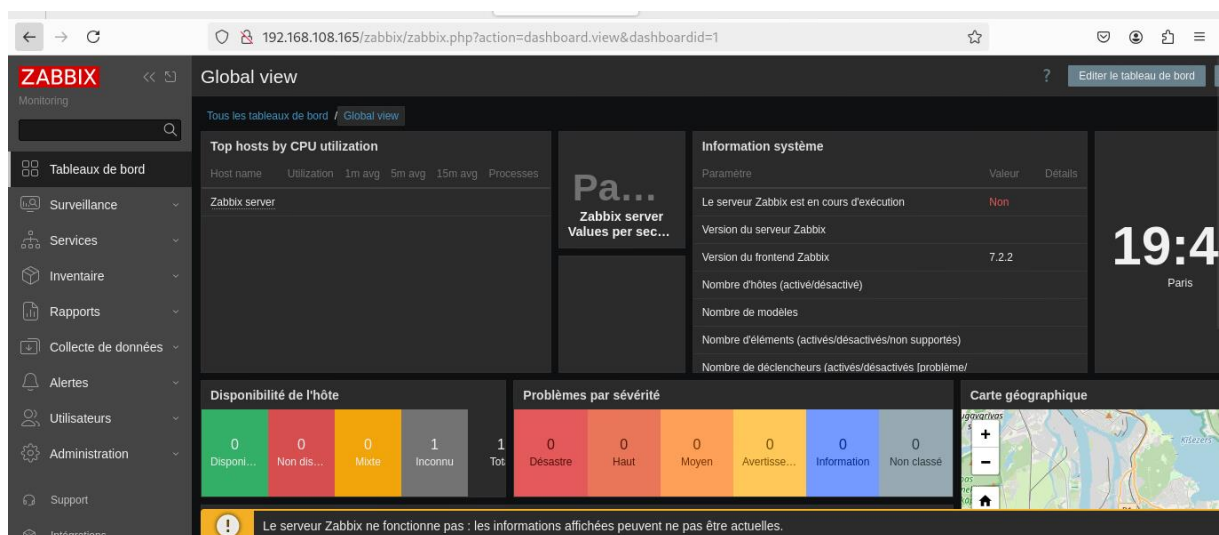
Résumé de l'installation :



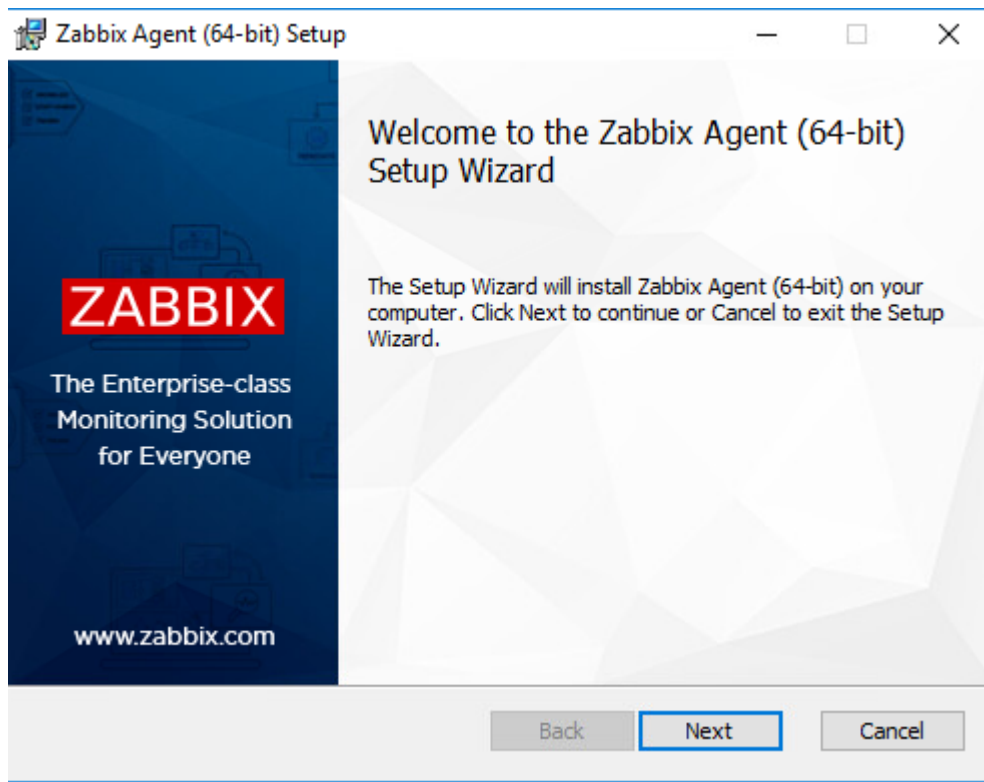


Puis s'identifier avec **Admin** mdp : **zabbix**.

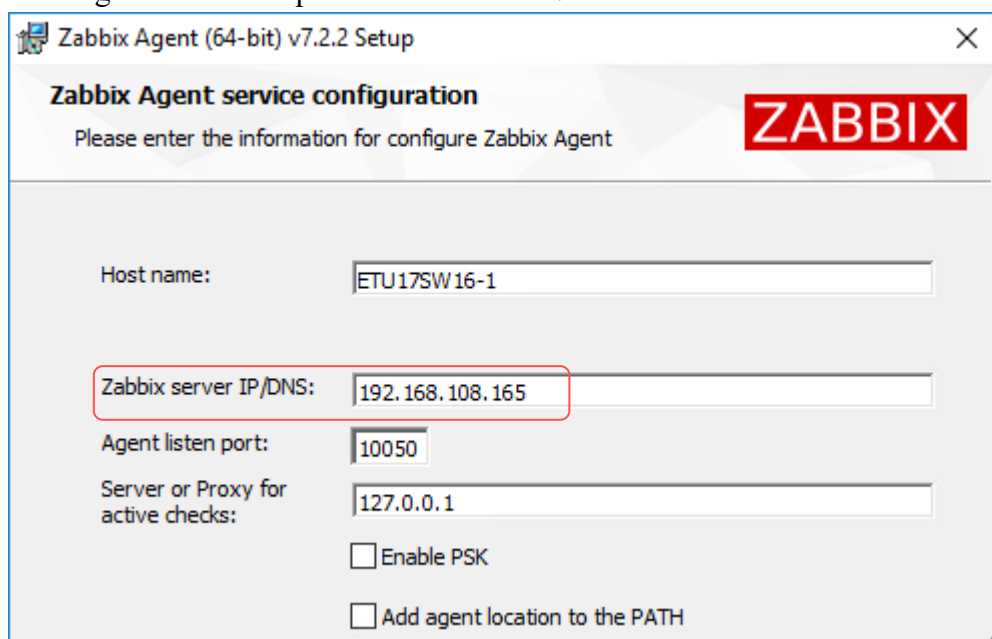
L'interface de zabbix :



2. Installation de l'agent zabbix sur Windows : [Télécharger les agents Zabbix](#)

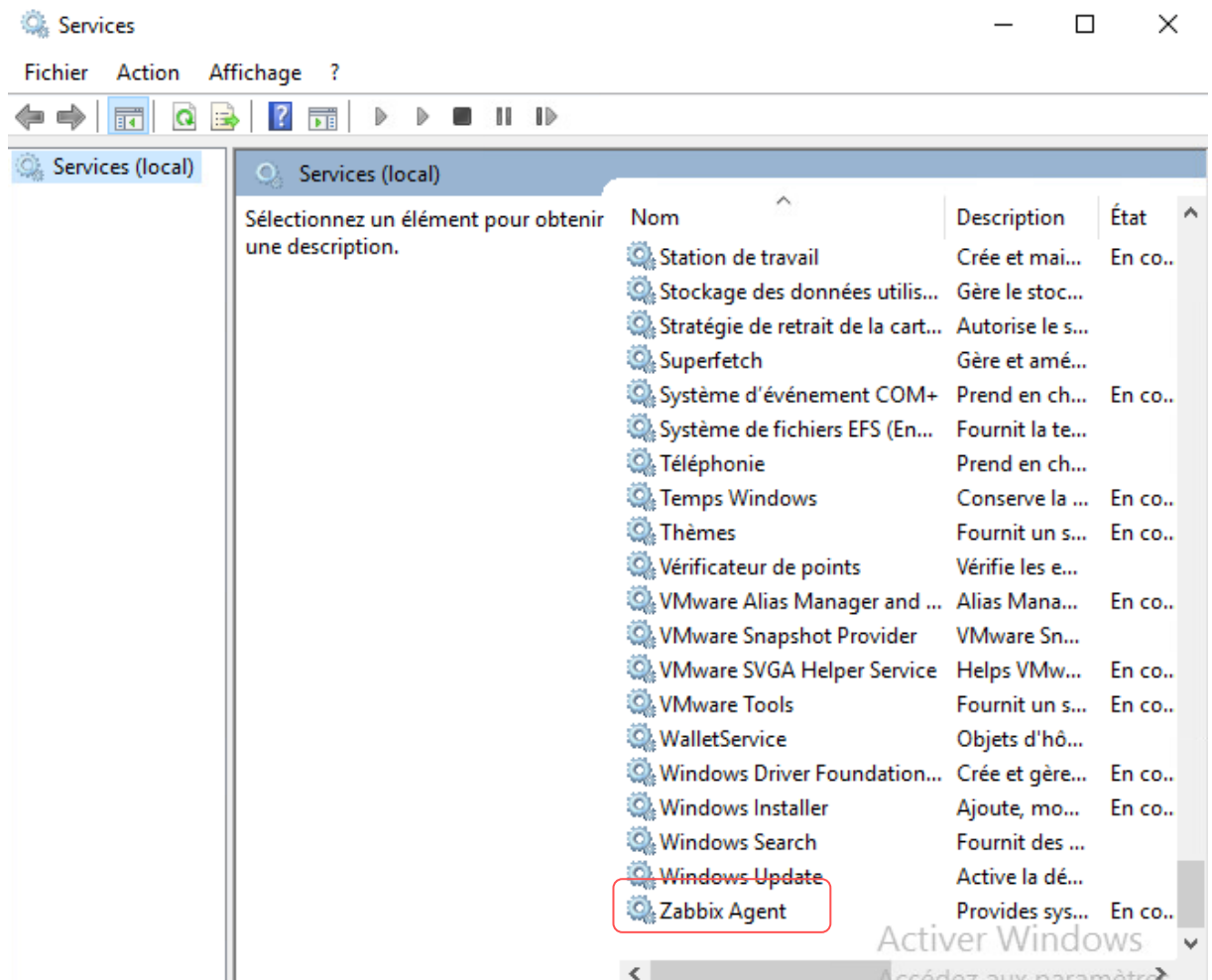


Renseignez l'adresse Ip du serveur zabbix :

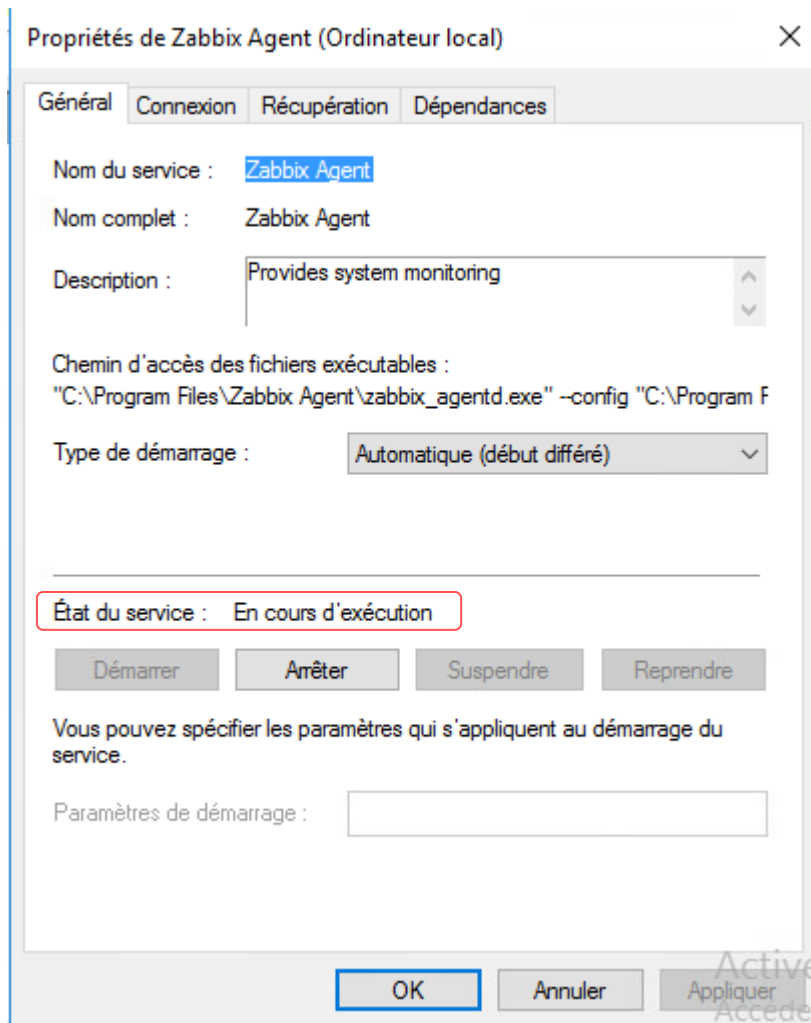


Puis terminer l'installation.

Vérifier l'état de l'agent zabbix pour voir s'il fonctionne normalement. Pour ce faire, nous allons dans la barre de recherche Windows, tapez **services**, et scrollez jusqu'en bas

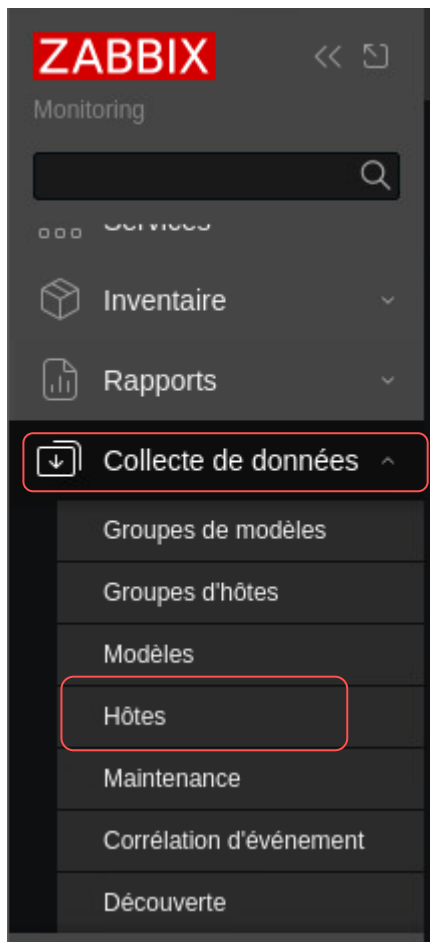


Faire un clic droit puis dans propriétés :



L'agent zabbix fonctionne.

Retourner sur notre serveur zabbix et ajouter notre machine Windows.
Data collection → Hosts → Create host



Création de l'hôte en renseignant l'IP du serveur primaire :

The screenshot shows the 'Nouvel hôte' (New Host) form in Zabbix. The form is filled out with the following information:

- Nom de l'hôte:** Windows
- Nom visible:** Windows
- Modèles:** Windows by Zabbix agent (highlighted with a red box)
- Groupes d'hôtes:** host (nouveau) (highlighted with a red box)
- Interfaces:**

Type	adresse IP	Nom DNS	Connexion à	Port
Agent	192.168.108.161	ETU17SW16-1	IP DNS	10050

La machine a bien été ajouté :

Nom	Éléments	Déclencheurs	Graphiques	Découverte	Web	Interface	Proxy	Modèles	État	Disponibilité
Windows	Éléments 34	Déclencheurs 13	Graphiques 5	Découverte 4	Web	192.168.108.161:10050		Windows by Zabbix agent	Actif	ZBX

Dans Monitoring → Hosts pour vérifier l'état de la machine avec les éventuels problèmes.

Allez dans **Monitoring > Latest Data** pour vérifier les métriques collectées par l'agent.

The screenshot shows the Zabbix Monitoring interface with the filter configuration for Hosts. A red box highlights the filter configuration area, which includes the following fields and buttons:

- Groupe d'hôtes:** A search bar with the text "host" and a "Sélectionner" button.
- Hôtes:** A search bar with the text "Windows" and a "Sélectionner" button.
- Nom:** A search bar.
- Tags:** A section with "Et/Ou" and "tag" buttons, and an "Ajouter" button.
- Voir les tags:** A button.
- Priorité d'affichage des tags:** A button.
- État:** A button.
- Afficher les détails:** A checkbox.
- Enregistrer sous:** A button.
- Appliquer:** A button, highlighted with a red box.
- Réinitialiser:** A button.

Below the filter configuration, there is a note: "Ce filtre affecte uniquement les données filtrées".

Ainsi, nous avons une connectivité entre l'agent et le zabbix server :

<input type="checkbox"/>	Windows	Cache bytes	component: memory	Graphique
<input type="checkbox"/>	Windows	Context switches per second	component: cpu	Graphique
<input type="checkbox"/>	Windows	CPU DPC time	component: cpu	Graphique
<input type="checkbox"/>	Windows	CPU interrupt time	component: cpu	Graphique
<input type="checkbox"/>	Windows	CPU privileged time	component: cpu	Graphique
<input type="checkbox"/>	Windows	CPU queue length	component: cpu	Graphique
<input type="checkbox"/>	Windows	CPU user time	component: cpu	Graphique
<input type="checkbox"/>	Windows	CPU utilization	component: cpu	Graphique