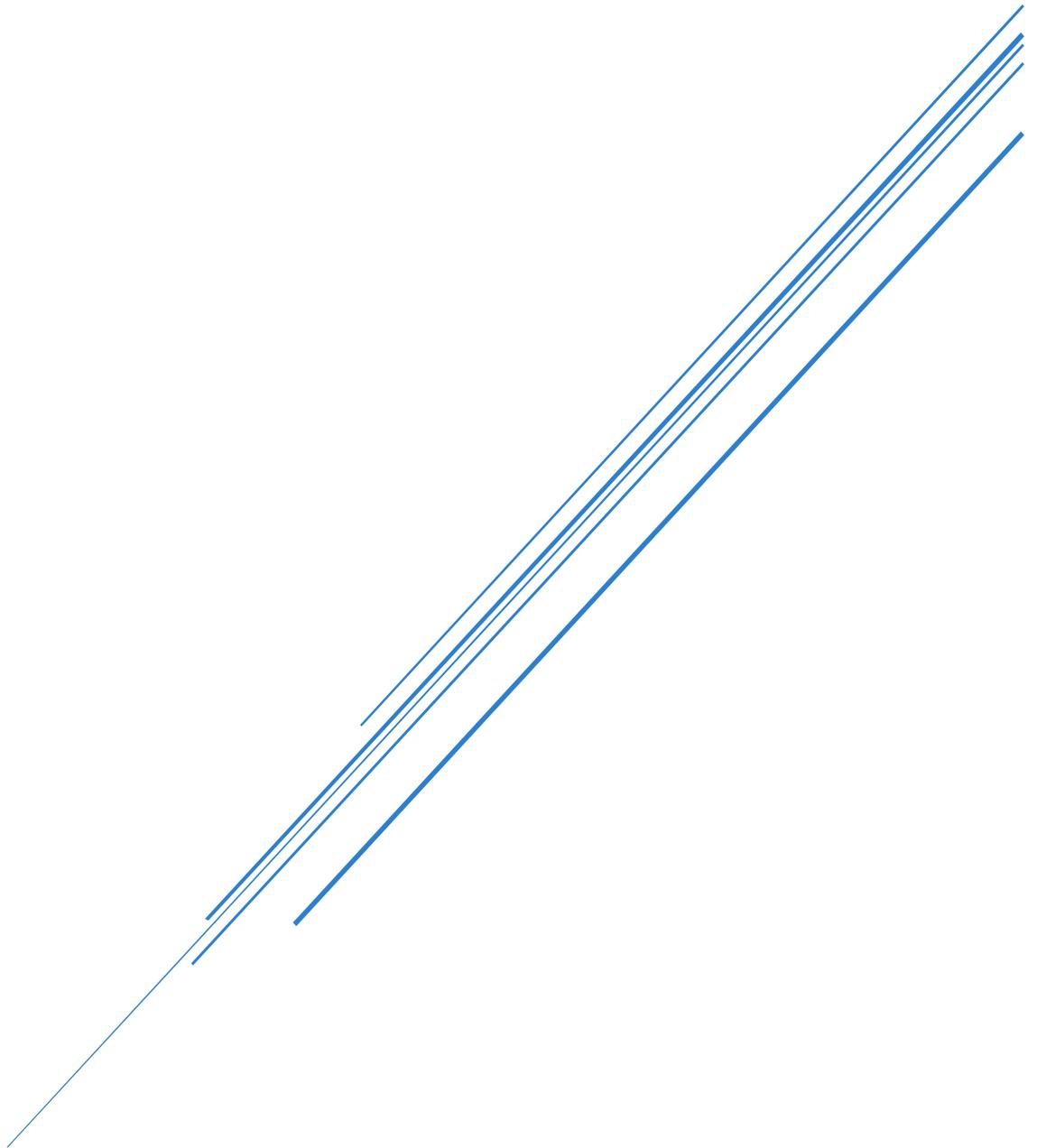


# Windows Server et Active Directory



Par Paris Steevy, Paul lallau, Toure Mohamed  
08/01/2025-09/01-2025

## TP 7 - Windows 10 sur AD:

### Prérequis :

- VirtualBox (installé sur votre machine)
- Téléchargez l'image ISO de **Windows Server 2019 Essentials** à l'adresse suivante :  
[http://rclone.edgand.fr/SIO/fr\\_windows\\_server\\_2019\\_essentials\\_updated\\_sept\\_2019\\_x64\\_dvd\\_123939ab.iso](http://rclone.edgand.fr/SIO/fr_windows_server_2019_essentials_updated_sept_2019_x64_dvd_123939ab.iso)

### Introduction

Dans le cadre de ce TP, nous allons apprendre à installer et configurer un **contrôleur de domaine Windows Server 2019** à l'aide de **VirtualBox**. Cette démarche s'inscrit dans l'apprentissage des services d'infrastructure réseau, et plus particulièrement de l'annuaire **Active Directory (AD)**, un outil essentiel dans la gestion centralisée des utilisateurs, des ressources et des politiques de sécurité au sein d'un réseau d'entreprise.

# 1 – Installation du client Windows

Après avoir téléchargée les quatre fichier OVA

 winX.ova_1	16/01/2025 08:10	Fichier OVA_1	2 522 496 Ko
 winX.ova_2	16/01/2025 08:14	Fichier OVA_2	2 522 496 Ko
 winX.ova_3	16/01/2025 08:14	Fichier OVA_3	2 522 496 Ko
 winX.ova_4	16/01/2025 08:15	Fichier OVA_4	2 522 496 Ko

Vérifie les hash des fichiers avec la commande

```
Get-FileHash -Algorithm MD5 -Path "winX.ova_1"
```

Sortie :

Algorithm	Hash	Path
MD5	AE42E0B8DC326057BB2F12FC5982211E	C:\PARTAGE\winX.ova_1

```
Get-FileHash -Algorithm MD5 -Path "winX.ova_2"
```

Sortie :

Algorithm	Hash	Path
MD5	B10416EC8C64BEB600E2FD22AA382CE1	C:\PARTAGE\winX.ova_2

```
Get-FileHash -Algorithm MD5 -Path "winX.ova_3"
```

Sortie :

Algorithm	Hash	Path
MD5	C293FF10654C45166FC5726EDCD0B1A6	C:\PARTAGE\winX.ova_3

```
Get-FileHash -Algorithm MD5 -Path "winX.ova_4"
```

Sortie :

Algorithm	Hash	Path
MD5	7E801934EA37A207563B15DFA9BCC679	C:\PARTAGE\winX.ova_4

Ensuite on met les 4 fichiers ova dans le dossier partagé avec la machine kali qui permet de faire des transferts entre Windows et kali

Puis on fait la commande suivant pour avoir le fichier ova complet

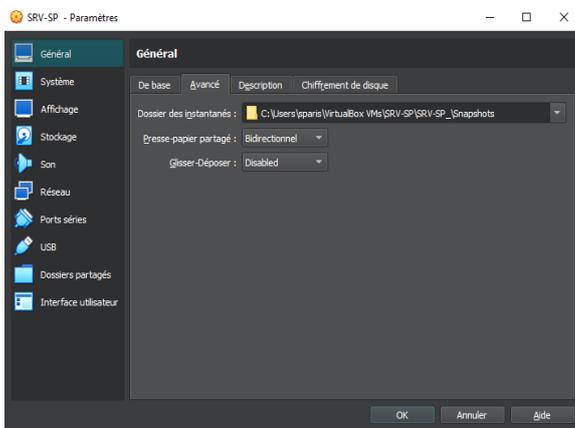
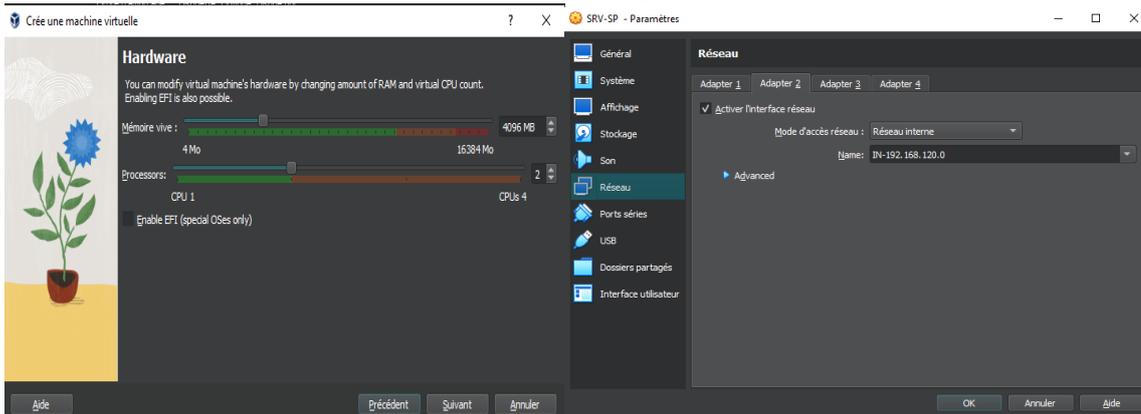
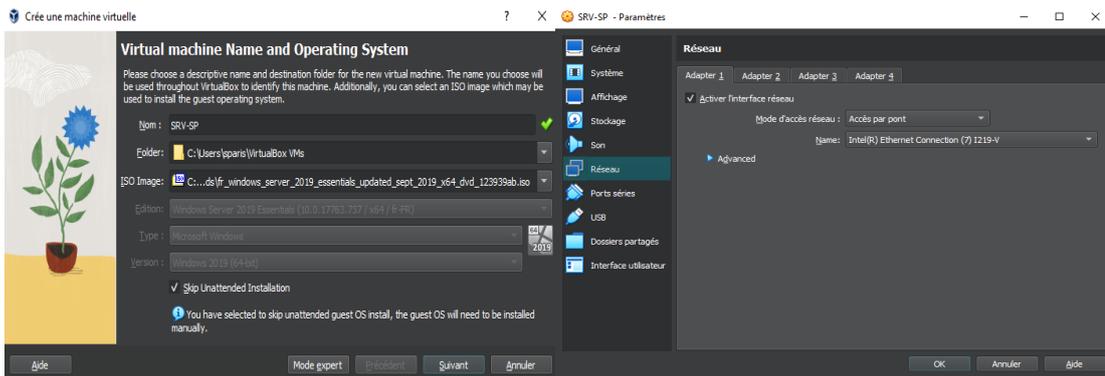
```
Cat winX.ova_1 winX.ova_2 winX.ova_3 winX.ova_4 > winX.ova
```

ensuite sur Windows on récupère le fichier comme ceci

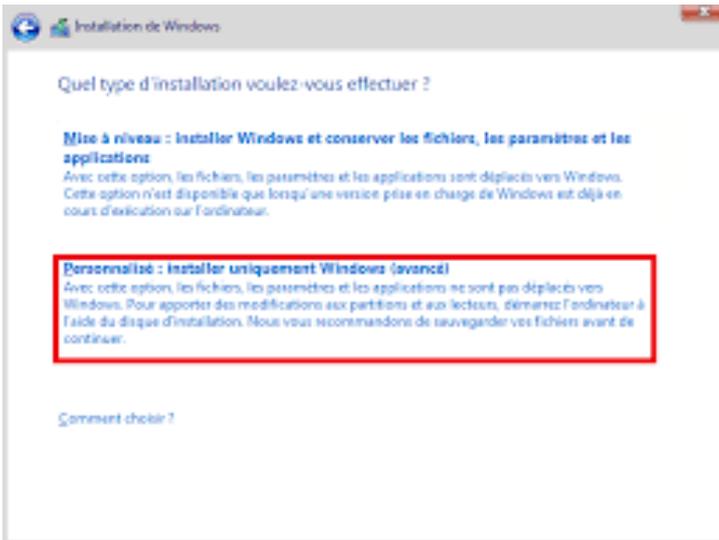
 winX.ova	16/01/2025 09:30	Fichier OVA	10 089 982 Ko
--	------------------	-------------	---------------

Quand on l'ouvre il se passe ceci

## Création d'une VM Windows Server avec VirtualBox

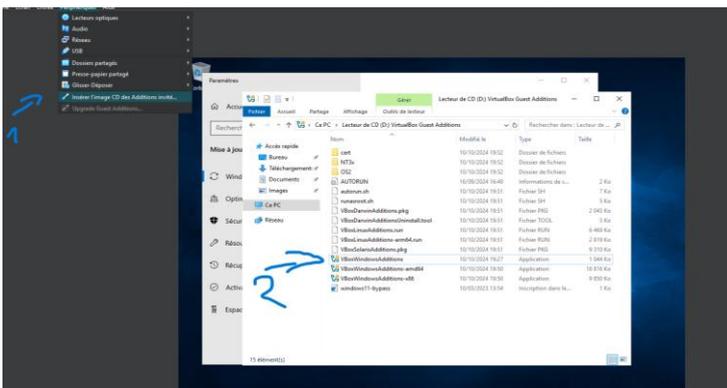


Ensuite, démarre la machine virtuelle et suis les étapes jusqu'à l'installation de Windows.



## Configurer le package Guest Additions

1. Sélectionnez l'onglet "**Périphériques**" dans VirtualBox.
2. Cliquez sur "**Insérer l'image CD des Additions Invité**".
3. Ouvrez le CD inséré dans la machine virtuelle et lancez le fichier "**VBoxWindowsAdditions.exe**" pour démarrer l'installation.



Il ne reste plus qu'à suivre les étapes d'installation.

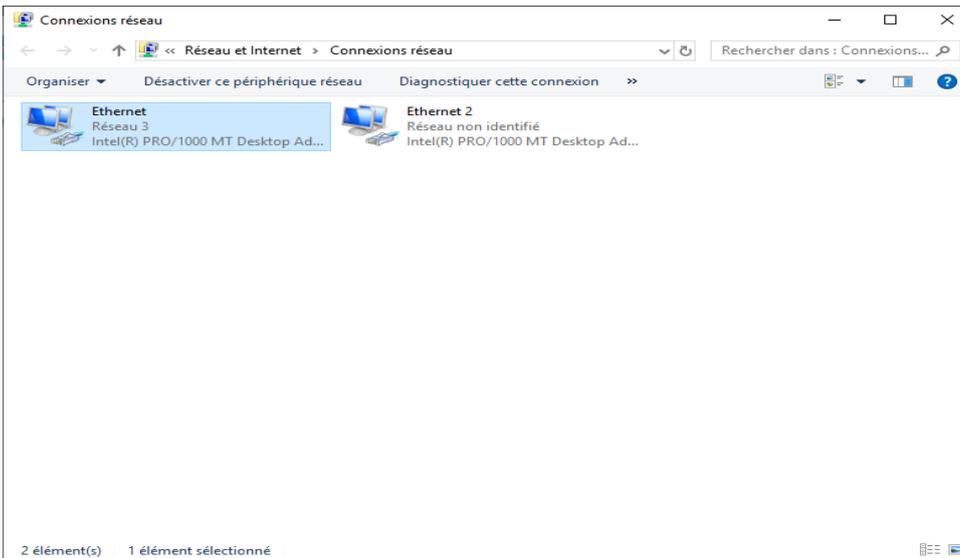
## Mise à jour de Windows Server

1. Cliquez sur le logo Windows, puis tapez "**Rechercher les mises à jour**" dans la barre de recherche.
2. Ouvrez le menu correspondant et lancez la recherche des mises à jour.

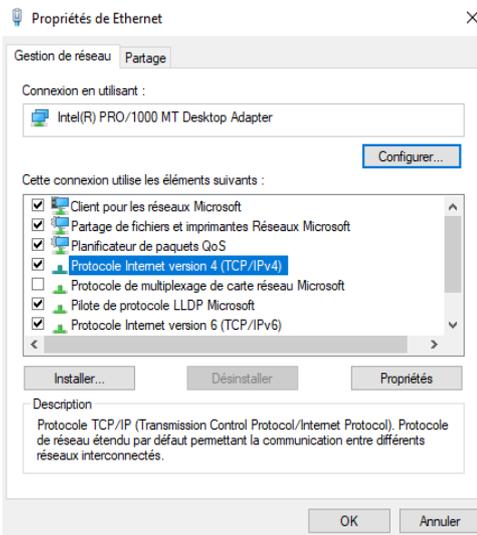
⚠ Cette étape peut être fastidieuse, surtout sur des ordinateurs peu performants.

## Configuration réseau

1. Ouvrez le panneau de configuration réseau.
2. Sélectionnez l'interface **Ethernet** que vous souhaitez configurer.
3. Cliquez avec le bouton droit et choisissez "**Propriétés**" pour accéder aux paramètres réseau.



- Sélectionnez l'interface **Ethernet**, puis cliquez sur **Propriétés**.
- Dans la liste des éléments, double-cliquez sur le **quatrième élément** (généralement, **Protocole Internet version 4 (TCP/IPv4)**).



Voici la fenêtre de configuration du réseau ethernet

### Configuration de Steevy :

Propriétés de : Protocole Internet version 4 (TCP/IPv4) X

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

Obtenir une adresse IP automatiquement

Utiliser l'adresse IP suivante :

Adresse IP : 192 . 168 . 120 . 1

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : . . .

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : . . .

Serveur DNS auxiliaire : . . .

Valider les paramètres en quittant

Avancé...

OK Annuler

### Configuration de Mohamed :

Propriétés de : Protocole Internet version 4 (TCP/IPv4) X

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

Obtenir une adresse IP automatiquement

Utiliser l'adresse IP suivante :

Adresse IP : 192 . 168 . 112 . 1

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : . . .

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 127 . 0 . 0 . 1

Serveur DNS auxiliaire : . . .

Valider les paramètres en quittant

Avancé...

OK Annuler

### Configuration de Paul :

Propriétés de : Protocole Internet version 4 (TCP/IPv4) X

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

Obtenir une adresse IP automatiquement

Utiliser l'adresse IP suivante :

Adresse IP : 192 . 168 . 117 . 1

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : . . .

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 127 . 0 . 0 . 1

Serveur DNS auxiliaire : . . .

Valider les paramètres en quittant

Avancé...

OK Annuler

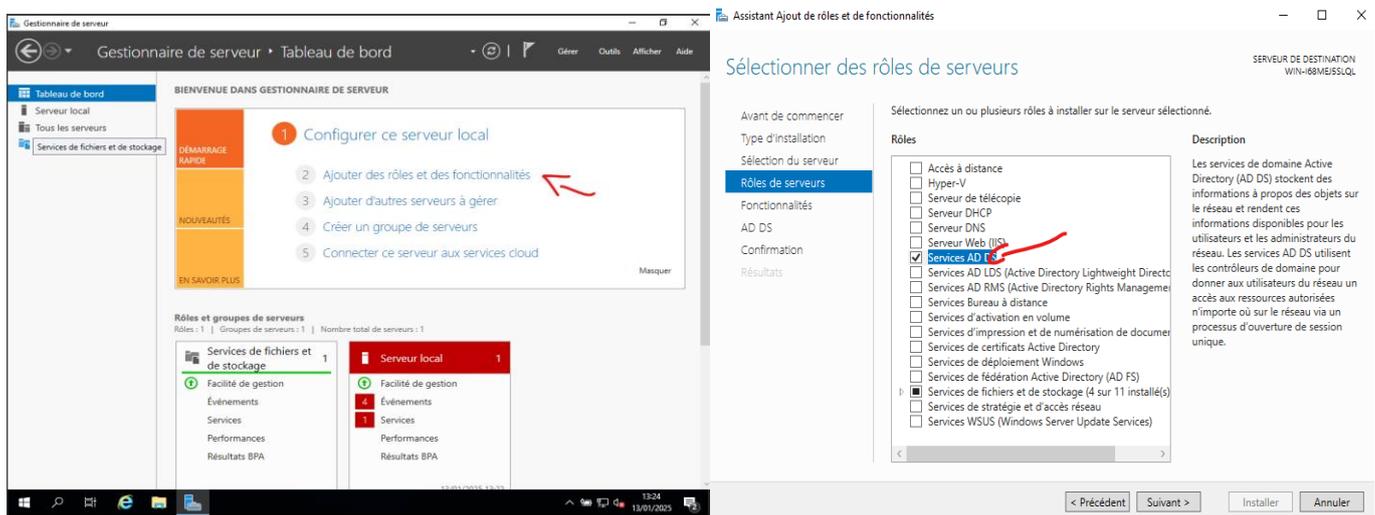
## Configuration réseau

3. Cochez l'option "**Valider les paramètres en quittant**", puis cliquez sur **OK** pour appliquer les modifications.

## 5 - Installation d'Active Directory

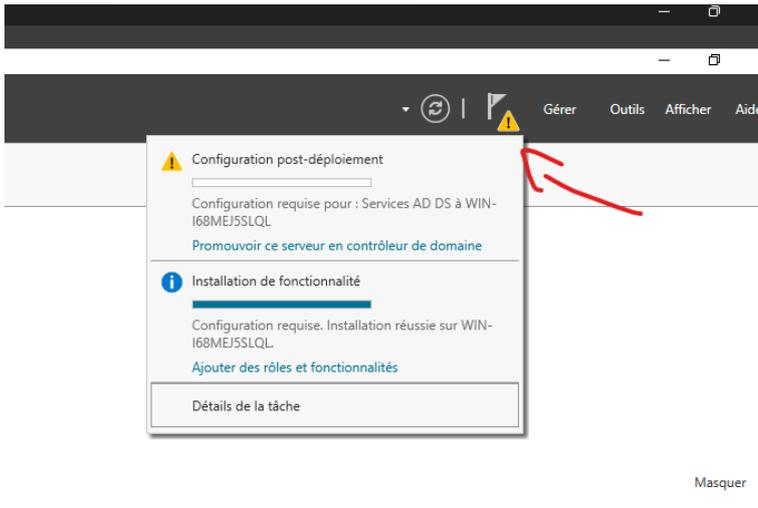
### 5.1 - Gestionnaire de serveur

1. Ouvrez le Gestionnaire de serveur en appuyant sur **Windows + R**, puis en tapant **servermanager** et appuyez sur **Entrée**.
2. Une fois le Gestionnaire de serveur ouvert, procédez à l'installation du rôle **Active Directory**.



Sélectionner Service AD DS, Enfin cliquer sur installer en bas à droite.

## 5.2 - Promotion en contrôleur de domaine



Résultat de la commande ipconfig :

**Steevy :**

```
Carte Ethernet Ethernet :  
  
Suffixe DNS propre à la connexion. . . :  
Adresse IPv6. . . . . : fd00::5137:cb55:596:e118  
Adresse IPv6 de liaison locale. . . . : fe80::26ca:b8d2:6951:f3b5%6  
Adresse IPv4. . . . . : 192.168.120.1  
Masque de sous-réseau. . . . . : 255.255.255.0  
Passerelle par défaut. . . . . : fe80::2%6  
  
Carte Ethernet Ethernet 2 :  
  
Suffixe DNS propre à la connexion. . . :  
Adresse IPv6 de liaison locale. . . . : fe80::9356:b16d:91d0:2e82%11  
Adresse d'autoconfiguration IPv4 . . . : 169.254.113.71  
Masque de sous-réseau. . . . . : 255.255.0.0  
Passerelle par défaut. . . . . :  
  
C:\Users\Administrateur>
```

**Paul :**

```
Carte Ethernet Ethernet :  
  
Suffixe DNS propre à la connexion. . . :  
Adresse IPv6 de liaison locale. . . . : fe80::18d1:2f45:5cf7:95a5%7  
Adresse IPv4. . . . . : 192.168.117.1  
Masque de sous-réseau. . . . . : 255.255.255.0  
Passerelle par défaut. . . . . :  
  
Carte Ethernet Ethernet 2 :  
  
Suffixe DNS propre à la connexion. . . : edgand.fr  
Adresse IPv6 de liaison locale. . . . : fe80::8b90:851:ebc5:4653%5  
Adresse IPv4. . . . . : 172.25.192.21  
Masque de sous-réseau. . . . . : 255.255.0.0  
Passerelle par défaut. . . . . : 172.25.254.254  
  
C:\Users\Administrateur>
```

## Mohamed :

```
Carte Ethernet Ethernet :  
  
  Suffixe DNS propre à la connexion. . . : edgand.fr  
  Adresse IPv6 de liaison locale. . . . : fe80::184c:698:b276:b74b%15  
  Adresse IPv4. . . . . : 172.25.193.71  
  Masque de sous-réseau. . . . . : 255.255.0.0  
  Passerelle par défaut. . . . . : 172.25.254.254  
  
Carte Ethernet Ethernet 2 :  
  
  Suffixe DNS propre à la connexion. . . :  
  Adresse IPv6 de liaison locale. . . . : fe80::3e60:e74e:8639:b60a%9  
  Adresse IPv4. . . . . : 192.168.122.1  
  Masque de sous-réseau. . . . . : 255.255.255.0  
  Passerelle par défaut. . . . . :
```

## 4 - Vérifications DNS

Résultat :> nslookup ad-sp

```
C:\Users\AdminLocal>nslookup ad-sp  
Serveur : UnKnown  
Address: fec0:0:0:ffff::1  
  
*** UnKnown ne parvient pas à trouver ad-sp : No response from server  
C:\Users\AdminLocal>_
```

> nslookup 192.168.120.1

```
C:\Users\AdminLocal>nslookup 192.168.120.1  
Serveur : UnKnown  
Address: fec0:0:0:ffff::1  
  
*** UnKnown ne parvient pas à trouver 192.168.120.1 : No response from server
```

> nslookup alpine

```
C:\Users\AdminLocal> nslookup alpine  
Serveur : UnKnown  
Address: fec0:0:0:ffff::1  
  
*** UnKnown ne parvient pas à trouver alpine : No response from server  
C:\Users\AdminLocal>_
```

> nslookup win1

```
C:\Users\AdminLocal>nslookup win1  
Serveur : UnKnown  
Address: fec0:0:0:ffff::1  
  
*** UnKnown ne parvient pas à trouver win1 : No response from server  
C:\Users\AdminLocal>_
```

> nslookup win2

```
C:\Users\AdminLocal>nslookup win2  
Serveur : UnKnown  
Address: fec0:0:0:ffff::1  
  
*** UnKnown ne parvient pas à trouver win2 : No response from server  
C:\Users\AdminLocal>_
```

> nslookup edgand.fr

```
C:\Users\AdminLocal>nslookup edgand.fr
Serveur : UnKnown
Address: fec0:0:0:ffff::1

*** UnKnown ne parvient pas à trouver edgand.fr : No response from server
```

> nslookup

```
C:\Users\AdminLocal>nslookup 8.8.8.8
Serveur : UnKnown
Address: fec0:0:0:ffff::1

*** UnKnown ne parvient pas à trouver 8.8.8.8 : No response from server
```

4) Le problème est qu'il n'y a pas de DHCP le client ne peut donc pas récupérer des informations provenant de l'active directory dans ce cas-là, il faut l'ajouter à l'active directory un DHCP dans la configuration pour que le client puisse récupérer des informations.

#### 4.1

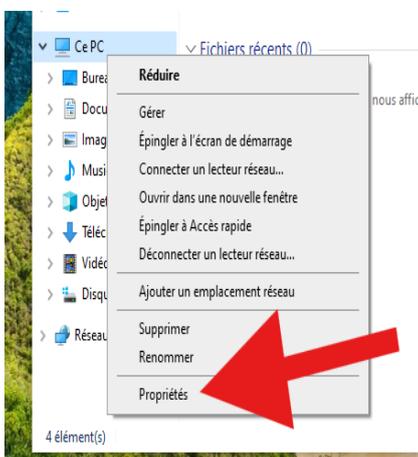
```
C:\Users\utilisateur1>ping lallau.sio

Envoi d'une requête 'ping' sur lallau.sio [192.168.117.1] avec 32 octets de données :
Réponse de 192.168.117.1 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.117.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\utilisateur1>
```

- 5 Intégration d'une machine windows sur le domaine
- Dans l'explorateur de fichier de Windows on fait clic droit sur "ce pc" puis propriété



- En bas des paramètres

## Paramètres associés

[Paramètres de Bitlocker](#)

[Gestionnaire de périphériques](#)

[Bureau à distance](#)

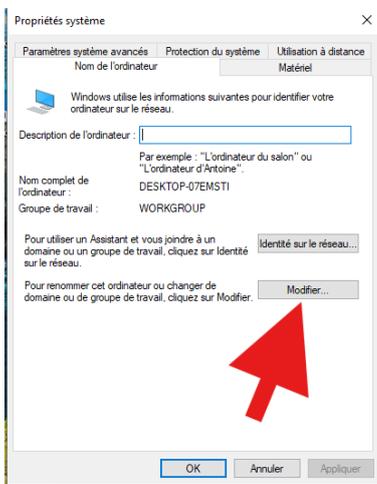
[Protection du système](#)

[Paramètres avancés du système](#)

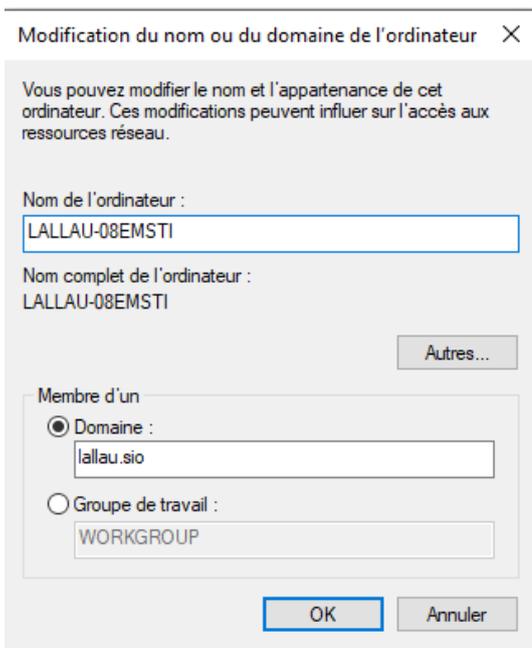
[Renommer ce PC \(avancé\)](#)



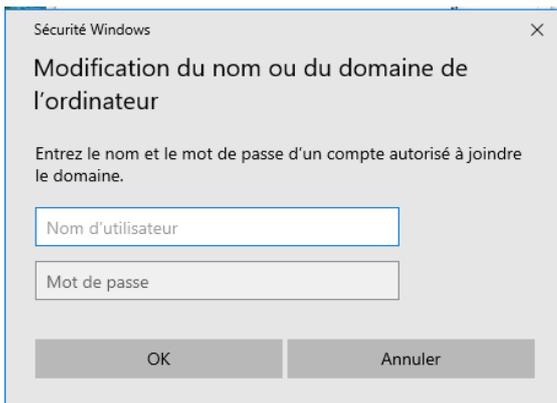
- Dans la page qui s'est ouvert aller dans "nom de l'ordinateur" modifier



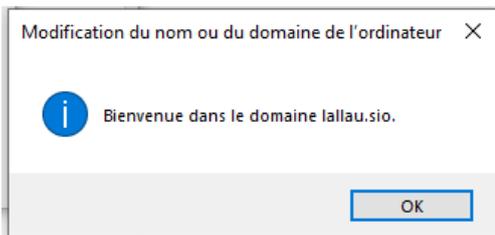
- Mettre le domaine 'domaine.sio' et changer le nom de l'ordinateur par la même occasion, puis cliquer sur OK.



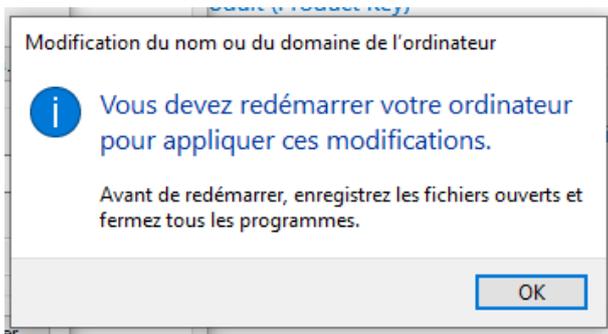
- Une page de sécurité Windows s'ouvre pour entrer les identifiants d'un compte administrateur du domaine. Une fois les identifiants entrés, cliquez sur OK.



- Après avoir attendu l'intégration du PC au domaine, ce message apparaît si tout s'est bien passé.



- Après avoir cliqué sur OK, ce message apparaît : 'Appuyer sur OK pour appliquer les paramètres. La machine redémarrera pour appliquer les paramètres du domaine.'



- Une fois la machine redémarrée, un autre utilisateur peut voir que la machine est correctement reliée au domaine.

## Résultats

Paul :



Steevy :



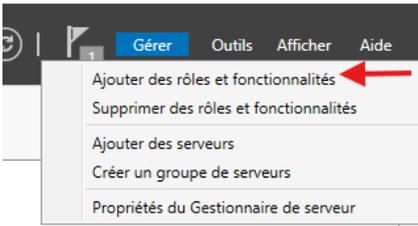
Mohamed :



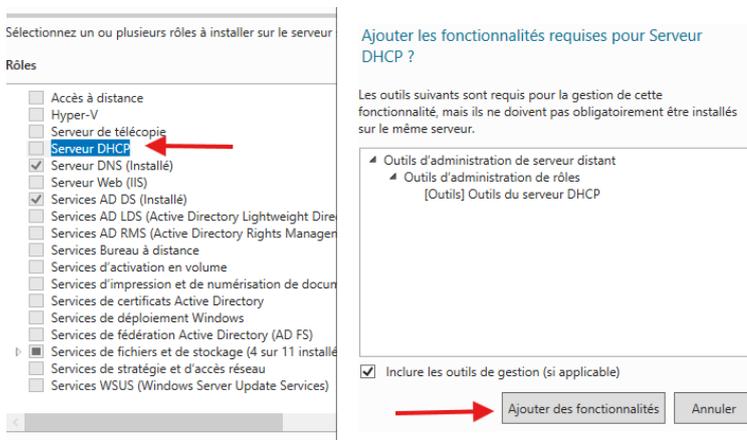
## TP 8B - Configuration AD :

### 1 – Configuration du DHCP :

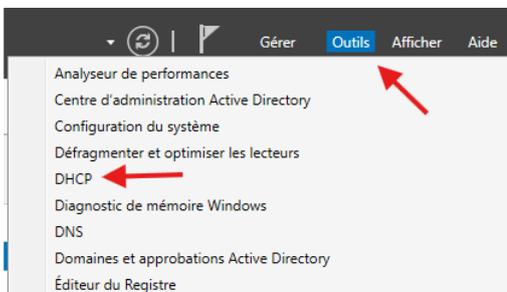
- **Gérer -> ajouter des rôles et fonctionnalités**



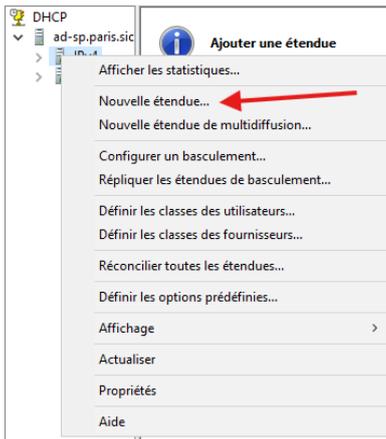
- **Rôle serveurs -> Serveur DHCP -> ajoute des fonctionnalités ensuite faire suivant jusqu'à installer**



- **Après installations du DHCP aller dans le menu Outils puis DHCP**



- **Dans le Domain ad-XX.Nom.sio aller dans ipv4 puis crée une nouvelle étendue**



## 2 - Configuration pc individuel :

### Steevy configuration :

Assistant Nouvelle étendue

#### Nom de l'étendue

Vous devez fournir un nom pour identifier l'étendue. Vous avez aussi la possibilité de fournir une description.



Tapez un nom et une description pour cette étendue. Ces informations vous permettront d'identifier rapidement la manière dont cette étendue est utilisée dans le réseau.

Nom :

Description :

< Précédent **Suivant >** Annuler

Assistant Nouvelle étendue

#### Plage d'adresses IP

Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.



#### Paramètres de configuration pour serveur DHCP

Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début :

Adresse IP de fin :

#### Paramètres de configuration qui se propagent au client DHCP

Longueur :

Masque de sous-réseau :

< Précédent **Suivant >** Annuler

- Faire suivant jusqu'à routeur (passerelle par défaut)

Assistant Nouvelle étendue

### Routeur (passerelle par défaut)

Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.



Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP :

192 . 168 . 120 . 1	Ajouter
	Supprimer
	Monter
	Descendre

< Précédent   Suivant >   Annuler

Assistant Nouvelle étendue

### Nom de domaine et serveurs DNS

DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.



Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.

Domaine parent : paris.sio

Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.

Nom du serveur :	Adresse IP :	
	192 . 168 . 120 . 1	Ajouter
		Supprimer
		Monter
		Descendre

Résoudre

< Précédent   Suivant >   Annuler

- Puis faire suivant jusqu'à la fin

## Paul configuration :

Assistant Nouvelle étendue

### Nom de l'étendue

Vous devez fournir un nom pour identifier l'étendue. Vous avez aussi la possibilité de fournir une description.



Tapez un nom et une description pour cette étendue. Ces informations vous permettront d'identifier rapidement la manière dont cette étendue est utilisée dans le réseau.

Nom : LALLAU[SIO]

Description :

< Précédent   Suivant >   Annuler

Assistant Nouvelle étendue

### Plage d'adresses IP

Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.



Paramètres de configuration pour serveur DHCP

Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début :

Adresse IP de fin :

Paramètres de configuration qui se propagent au client DHCP.

Longueur :

Masque de sous-réseau :

< Précédent **Suivant >** Annuler

- Faire suivant jusqu'à routeur (passerelle par défaut)

Assistant Nouvelle étendue

### Routeur (passerelle par défaut)

Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.



Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP :

< Précédent **Suivant >** Annuler

Assistant Nouvelle étendue

### Nom de domaine et serveurs DNS

DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.



Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.

Domaine parent :

Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.

Nom du serveur :

Adresse IP :

< Précédent **Suivant >** Annuler

## Mohamed configuration :

Assistant Nouvelle étendue

### Nom de l'étendue

Vous devez fournir un nom pour identifier l'étendue. Vous avez aussi la possibilité de fournir une description.



Tapez un nom et une description pour cette étendue. Ces informations vous permettront d'identifier rapidement la manière dont cette étendue est utilisée dans le réseau.

Nom :   
Description :

< Précédent **Suivant >** Annuler

Assistant Nouvelle étendue

### Plage d'adresses IP

Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.



Paramètres de configuration pour serveur DHCP

Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début :   
Adresse IP de fin :

Paramètres de configuration qui se propagent au client DHCP.

Longueur :   
Masque de sous-réseau :

< Précédent **Suivant >** Annuler

- Faire suivant jusqu'à routeur (passerelle par défaut)

Assistant Nouvelle étendue

### Routeur (passerelle par défaut)

Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.



Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP :

< Précédent **Suivant >** Annuler

### Nom de domaine et serveurs DNS

DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.



Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.

Domaine parent : TOURE.sio

Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.

Nom du serveur : Adresse IP : 192 . 168 . 122 .

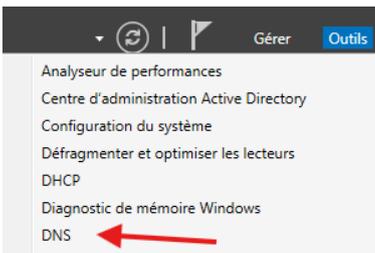
Résoudre Ajouter Supprimer Monter Descendre

< Précédent Suivant > Annuler

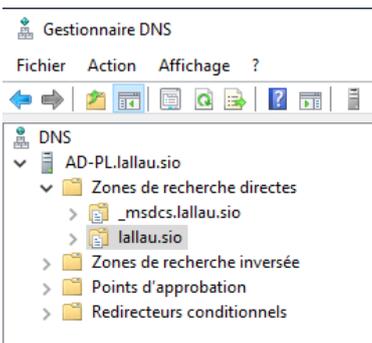
- Puis faire "suivant" jusqu'à la fin

## 3 – Configuration du DNS

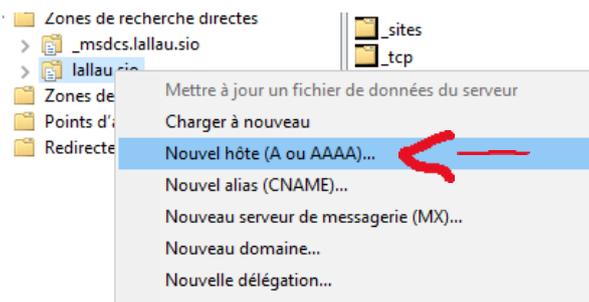
La configuration DNS permet de contacter une machine avec un nom plutôt que son IP qui est souvent dynamique sur un réseau d'entreprise et cela permet de récupérer une machine facilement sans a cherchée après l'IP sur le DHCP



- Dans zone de recherche directe -> nom.sio



- Clic droit sur nom.sio -> Nouvelle hôte (A ou AAAA)



- Crée le nom DNS pour l'AD (ad-pl.nom.sio) avec l'adresse IP 192.168.XXX.XXX
- Activer l'option (Créer un pointeur d'enregistrement PTR associé)

Paul :

The dialog box 'Nouvel hôte' contains the following fields and options:

- Nom (utilise le domaine parent si ce champ est vide) : ad-pl
- Nom de domaine pleinement qualifié (FQDN) : ad-pl.lallau.sio.
- Adresse IP : 192.168.117.1
- Créer un pointeur d'enregistrement PTR associé
- Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

Buttons: Ajouter un hôte, Annuler

Steevy :

The dialog box 'Nouvel hôte' contains the following fields and options:

- Nom (utilise le domaine parent si ce champ est vide) : ad-sp
- Nom de domaine pleinement qualifié (FQDN) : ad-sp.paris.sio.
- Adresse IP : 192.168.120.1
- Créer un pointeur d'enregistrement PTR associé
- Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

Buttons: Ajouter un hôte, Annuler

Mohamed :

The dialog box 'Nouvel hôte' contains the following fields and options:

- Nom (utilise le domaine parent si ce champ est vide) : ad.pl
- Nom de domaine pleinement qualifié (FQDN) : ad.pl.toure.sio.
- Adresse IP : 192.168.122.1
- Créer un pointeur d'enregistrement PTR associé
- Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

Buttons: Ajouter un hôte, Annuler

- Crée la même chose pour alpine (alpine.nom.sio) avec l'adresse IP 192.168.1XX.1

Nouvel hôte

Nom (utilise le domaine parent si ce champ est vide) :  
alpine

Nom de domaine pleinement qualifié (FQDN) :  
alpine.lallau.sio.

Adresse IP :  
192.168.117.10

Créer un pointeur d'enregistrement PTR associé  
 Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

Ajouter un hôte Annuler

Steevy :

Nouvel hôte

Nom (utilise le domaine parent si ce champ est vide) :  
alpine

Nom de domaine pleinement qualifié (FQDN) :  
alpine.paris.sio.

Adresse IP :  
192.168.120.10|

Créer un pointeur d'enregistrement PTR associé  
 Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

Ajouter un hôte Annuler

Mohamed :

Nouvel hôte

Nom (utilise le domaine parent si ce champ est vide) :  
alpine

Nom de domaine pleinement qualifié (FQDN) :  
alpine.toure.sio.

Adresse IP :  
192.168.122.1|

Créer un pointeur d'enregistrement PTR associé  
 Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

Ajouter un hôte Annuler

- Crée la même chose pour win1 (win1.nom.sio) avec l'adresse IP 192.168.1XX.21

Nouvel hôte ✕

Nom (utilise le domaine parent si ce champ est vide) :

Nom de domaine pleinement qualifié (FQDN) :

Adresse IP :

Créer un pointeur d'enregistrement PTR associé  
 Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

Steevy :

Nouvel hôte ✕

Nom (utilise le domaine parent si ce champ est vide) :

Nom de domaine pleinement qualifié (FQDN) :

Adresse IP :

Créer un pointeur d'enregistrement PTR associé  
 Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

Mohamed :

Nouvel hôte ✕

Nom (utilise le domaine parent si ce champ est vide) :

Nom de domaine pleinement qualifié (FQDN) :

Adresse IP :

Créer un pointeur d'enregistrement PTR associé  
 Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

- Créé la même chose pour win2 (win2.lallau.sio) avec l'adresse IP 192.168.117.22

Paul :

The dialog box 'Nouvel hôte' contains the following fields and options:

- Nom (utilise le domaine parent si ce champ est vide) : win2
- Nom de domaine pleinement qualifié (FQDN) : win2.lallau.sio.
- Adresse IP : 192.168.117.22
- Créer un pointeur d'enregistrement PTR associé
- Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

Buttons: Ajouter un hôte, Annuler

Steevy :

The dialog box 'Nouvel hôte' contains the following fields and options:

- Nom (utilise le domaine parent si ce champ est vide) : win2
- Nom de domaine pleinement qualifié (FQDN) : win2.paris.sio.
- Adresse IP : 192.168.120.22
- Créer un pointeur d'enregistrement PTR associé
- Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

Buttons: Ajouter un hôte, Annuler

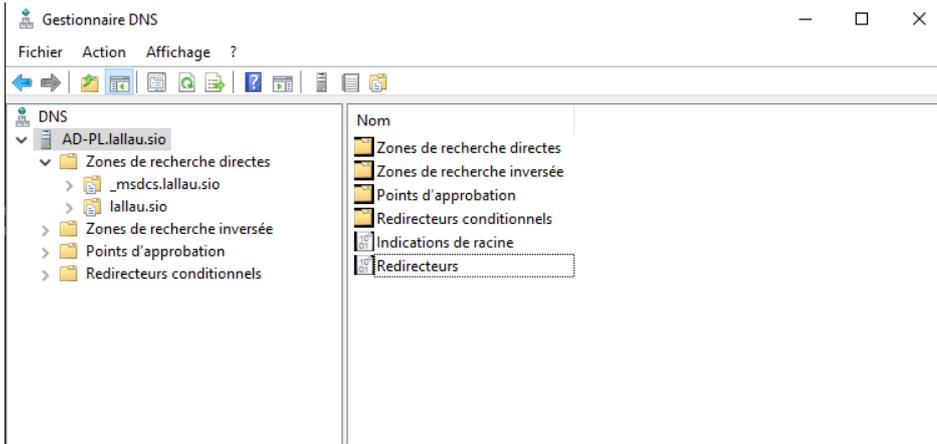
Mohamed :

The dialog box 'Nouvel hôte' contains the following fields and options:

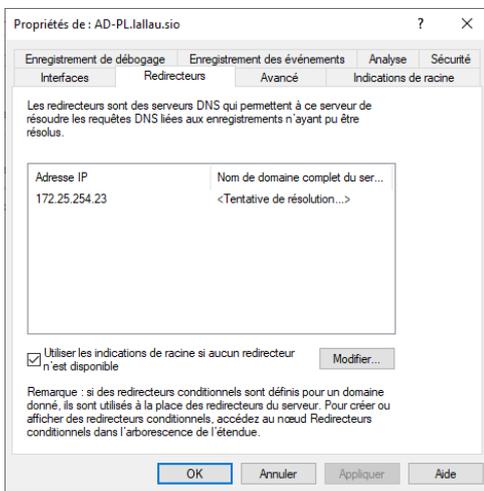
- Nom (utilise le domaine parent si ce champ est vide) : win2
- Nom de domaine pleinement qualifié (FQDN) : win2.toure.sio.
- Adresse IP : 192.168.122.1
- Créer un pointeur d'enregistrement PTR associé
- Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

Buttons: Ajouter un hôte, Annuler

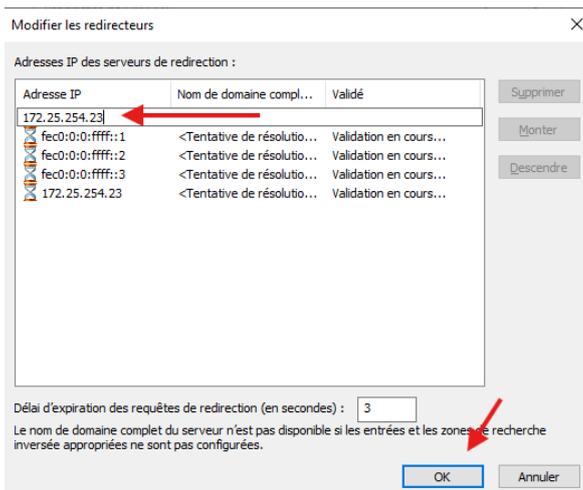
- Activer le forwarder



- Dans redirecteur on vérifie que dans le redirecteur il y est l'IP 172.25.254.23
- Si des adresses mac apparaisse supprimer les



- Si l'IP du redirecteur n'apparait pas cliqué sur le bouton modifier est ajouter la manuellement



- Effectuez les différents tests nslookup du TP précédent



Mohamed :

```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.19045.5247]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\AdminLocal>nslookup AD.mt
Serveur : UnKnown
Address: 192.168.122.1

Nom : AD.mt.toure.sio
Address: 192.168.122.1
```

```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.19045.5247]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\AdminLocal>nslookup alpine
Serveur : UnKnown
Address: 192.168.122.1

Nom : alpine.toure.sio
Address: 192.168.122.1
```

```
C:\Users\AdminLocal>nslookup win1
Serveur : UnKnown
Address: 192.168.122.1

Nom : win1.toure.sio
Address: 192.168.122.1
```

```
C:\Users\AdminLocal>nslookup win2
Serveur : UnKnown
Address: 192.168.122.1

Nom : win2.toure.sio
Address: 192.168.122.1
```

```
C:\Users\AdminLocal>nslookup 8.8.8.8
Serveur : UnKnown
Address: 192.168.122.1

Nom : dns.google
Address: 8.8.8.8
```

Steevy:

```
C:\Users\AdminLocal>nslookup AD-sp
Serveur : UnKnown
Address: 192.168.120.1

Nom : AD-sp.PARIS.sio
Addresses: 192.168.120.1
          172.25.192.64

C:\Users\AdminLocal>
```

```
C:\Users\AdminLocal>nslookup alpine
Serveur : UnKnown
Address: 192.168.120.1

Nom : alpine.PARIS.sio
Address: 192.168.120.10
```

```
C:\Users\AdminLocal>nslookup win1
Serveur : UnKnown
Address: 192.168.120.1

Nom : win1.PARIS.sio
Address: 192.168.120.21
```

```
C:\Users\AdminLocal>nslookup win2
Serveur : UnKnown
Address: 192.168.120.1

Nom : win2.PARIS.sio
Address: 192.168.120.22
```

```
C:\Users\AdminLocal>nslookup 8.8.8.8
Serveur : UnKnown
Address: 192.168.120.1

Nom : dns.google
Address: 8.8.8.8
```

La configuration du DNS et du forwarder fonctionne lorsque les demandes DNS ne sont pas destinées au réseau local. Dans ce cas, la demande de nslookup est envoyée au DNS redirecteur configuré, en l'occurrence le DNS edgand.fr pour les domaines externes tels que Google, avec 8.8.8.8 qui renvoie à dns.google.com.

### 3 – Gestion des utilisateurs

La gestion des utilisateurs permet de donner des accès restreints à un réseau d'entreprise. Par exemple, un employé normal aura moins de droits que l'équipe informatique, qui aura les permissions administrateur pour pouvoir connecter un appareil au domaine ou encore installer des applications qui nécessitent des permissions administrateur.

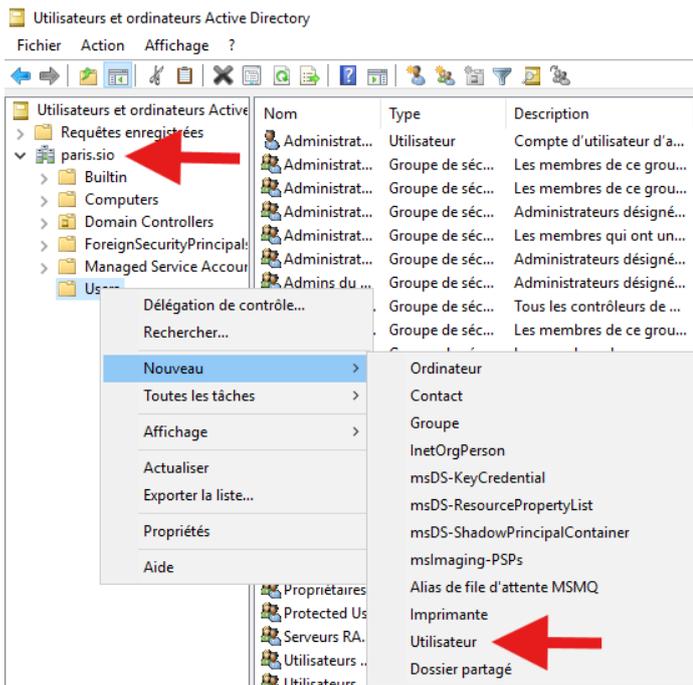
#### 1. Créer des utilisateurs :

- accéder à l'application

- Ouvrir Outils -> Utilisateurs et ordinateurs Active Directory.



- Puis dans Utilisateur qui et dans le nom.sio
- Clic droit sur le dossier 'Users', et dans la catégorie 'Nouveau', on clique sur 'Utilisateur'.



## 2. Ajouter trois utilisateurs avec privilèges différents :

Compte invité :

Paul :

Nouvel objet - Utilisateur

Créer dans : lallau.sio/Users

Prénom : invite1    Initiales :

Nom :

Nom complet : invite1

Nom d'ouverture de session de l'utilisateur :  
 @lallau.sio

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

< Précédent    Suivant >    Annuler

Steevy :

Nouvel objet - Utilisateur

Créer dans : paris.sio/Users

Prénom : invite1    Initiales :

Nom :

Nom complet : invite1

Nom d'ouverture de session de l'utilisateur :  
 @paris.sio

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

< Précédent    Suivant >    Annuler

## Mohamed :

Nouvel objet - Utilisateur

Créer dans : toure.sio/Users

Prénom : invite1 Initiales :

Nom :

Nom complet : invite1

Nom d'ouverture de session de l'utilisateur :  
invite1 @toure.sio

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :  
TOURE\ invite1

< Précédent Suivant > Annuler

- Ensuite on ajoute un mot de passe (invit1\_ABCD)
- Décocher “ l'utilisateur doit changer de mot de passe à la prochaine ouverture de session”

## Paul :

Nouvel objet - Utilisateur

Créer dans : lallau.sio/Users

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

## Steevy :

Nouvel objet - Utilisateur

Créer dans : paris.sio/Users

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

Mohamed :

Nouvel objet - Utilisateur

Créer dans : toure.sio/Users

Mot de passe : [dots]

Confirmer le mot de passe : [dots]

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

- Après avoir fini la création du compte, dans user, clic droit sur le compte invite1 puis propriété

Propriétés de : invite1

Environnement Sessions Contrôle à distance Profil des services Bureau à distance COM+

Général Adresse Compte Profil Téléphones Organisation Membre de Appel entrant

invite1

Prénom : invite1

Nom : [empty]

Nom complet : invite1

Description : [empty]

Bureau : [empty]

Numéro de téléphone : [empty] Autre...

Adresse de messagerie : [empty]

Page Web : [empty] Autre...

OK Annuler Appliquer Aide

Propriétés de : invite1

Environnement Sessions Contrôle à distance Profil des services Bureau à distance COM+

Général Adresse Compte Profil Téléphones Organisation Membre de Appel entrant

Membre de :

Nom	Dossier Services de domaine Active Directory
	Utilisateurs du do... parts.sio/Users

Ajouter... Supprimer

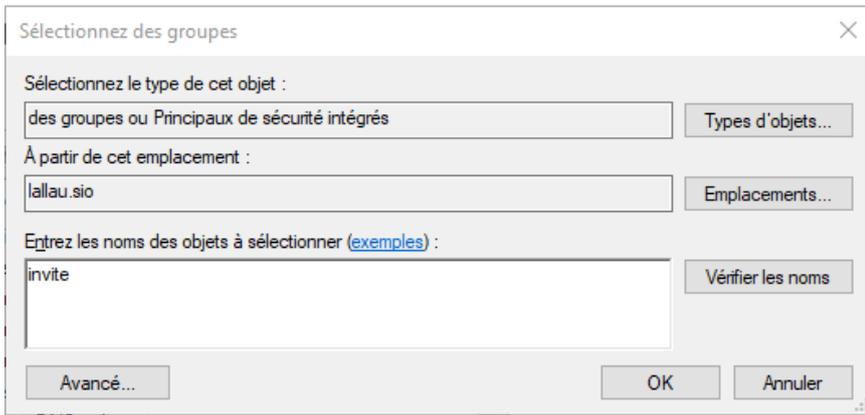
Groupe principal : Utilisateurs du domaine

Définir le groupe principal

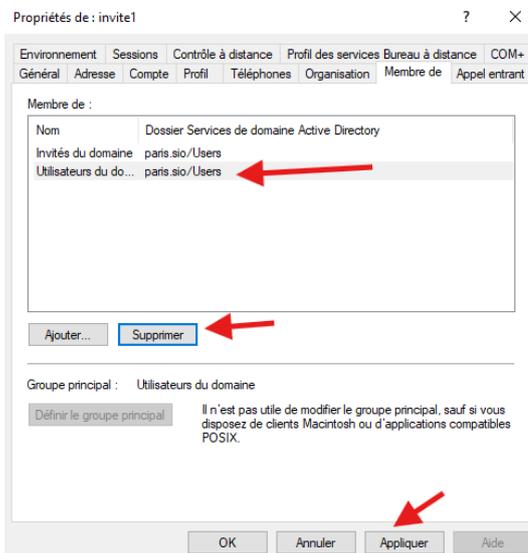
Il n'est pas utile de modifier le groupe principal, sauf si vous disposez de clients Macintosh ou d'applications compatibles POSIX.

OK Annuler Appliquer Aide

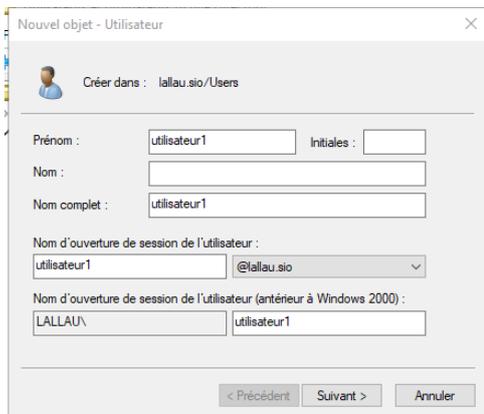
- Dans le champ de recherche écrire "invite" puis cliquer sur ok



- Définir "Invités du domaine" comme groupe principal puis supprimer 'Utilisateurs du domaine'.
- Appliquer après avoir supprimé 'Utilisateurs du domaine'.



- Crée utilisateur1, click droit dans user -> nouveau -> utilisateur



- Insérer les mots de passe (util1\_ABCD)
- Décocher " l'utilisateur doit changer de mot de passe à la prochaine ouverture de session"

Nouvel objet - Utilisateur

Créer dans : lallau.sio/Users

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

- Le groupe par défaut "Utilisateurs du domaine" appliquée automatiquement
- Crée un compte admin, click droit dans user -> nouveau -> utilisateur

Paul :

Nouvel objet - Utilisateur

Créer dans : lallau.sio/Users

Prénom :  Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur :  
 @lallau.sio

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

< Précédent **Suivant >** Annuler

Steevy :

Nouvel objet - Utilisateur

Créer dans : paris.sio/Users

Prénom :  Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur :  
 @paris.sio

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

< Précédent **Suivant >** Annuler

Mohamed :

Nouvel objet - Utilisateur

Créer dans : toure.sio/Users

Prénom : admin1 Initiales :

Nom :

Nom complet : admin1

Nom d'ouverture de session de l'utilisateur :  
admin1 @toure.sio

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :  
TOURE\ admin1

< Précédent Suivant > Annuler

- Renseigner le mot de passe (**mdp-S!SR-2019**)
- Décocher “ l'utilisateur doit changer de mot de passe à la prochaine ouverture de session”

Nouvel objet - Utilisateur

Créer dans : lallau.sio/Users

Mot de passe :

Confirmer le mot de passe :

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

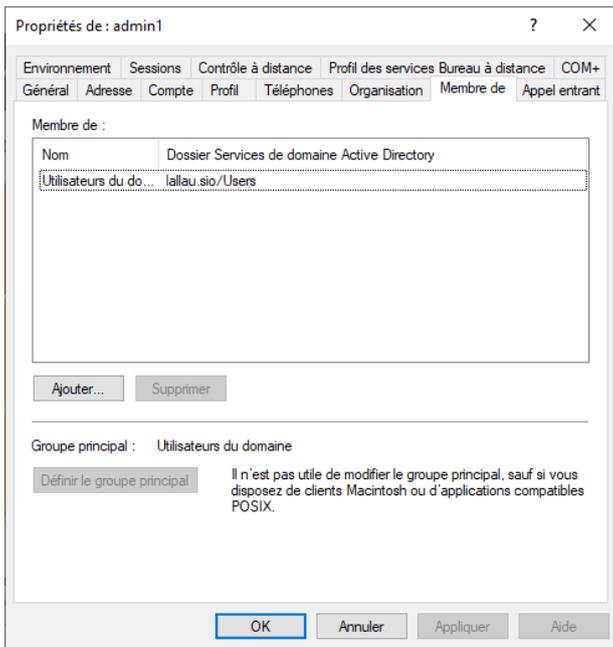
L'utilisateur ne peut pas changer de mot de passe

Le mot de passe n'expire jamais

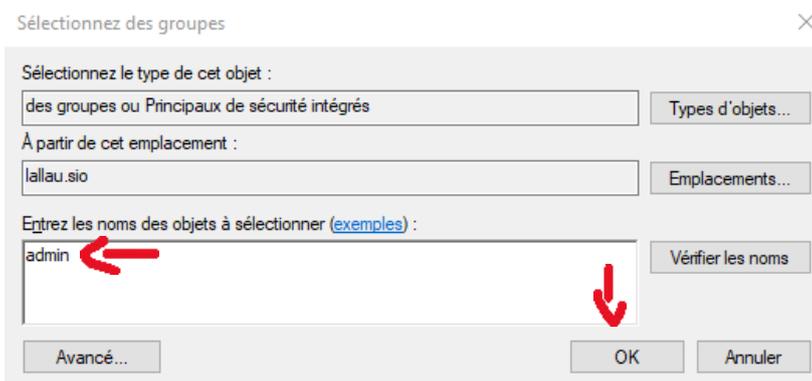
Le compte est désactivé

< Précédent Suivant > Annuler

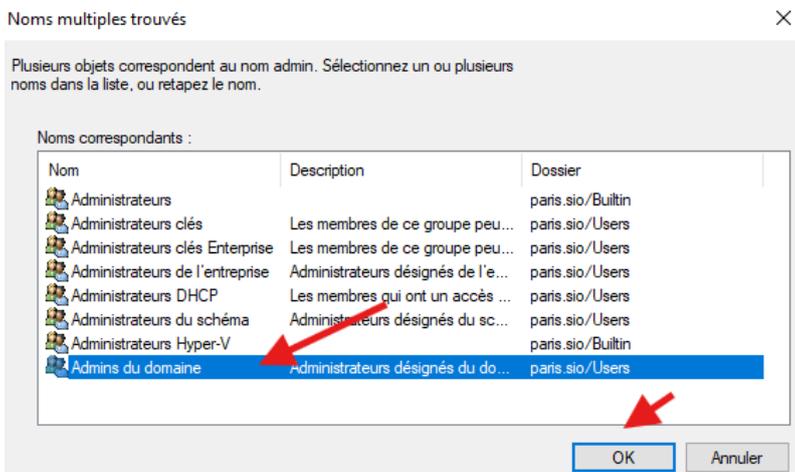
- Puis dans la configuration du compte, clic droit -> propriétés dans la catégorie -> membre de



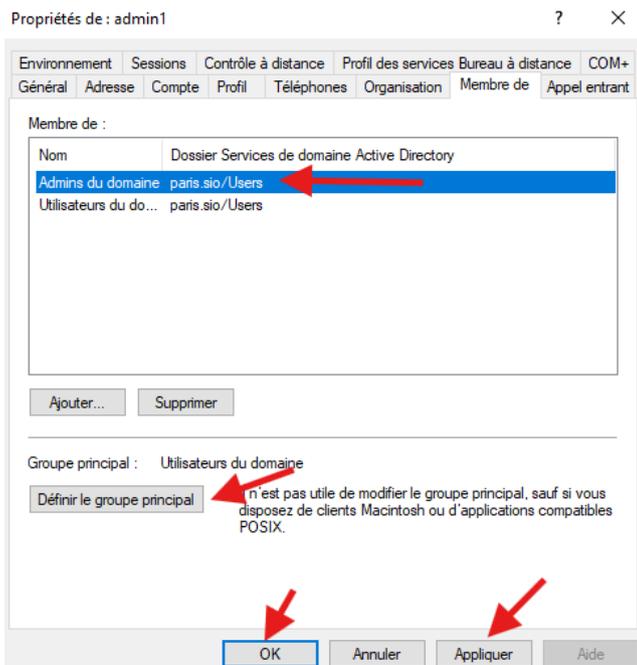
- Ajouter un rôle admin puis ok



- Dans le menu suivant prendre "admins du domaine" puis OK



- Faire du groupe "admins du domaine" le groupe principal puis appliquer puis ok



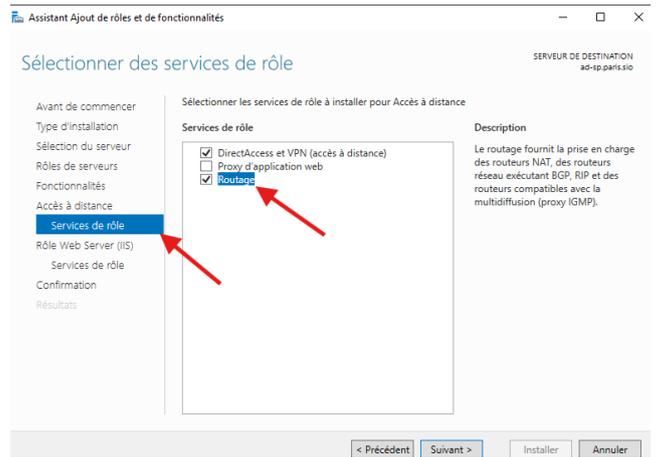
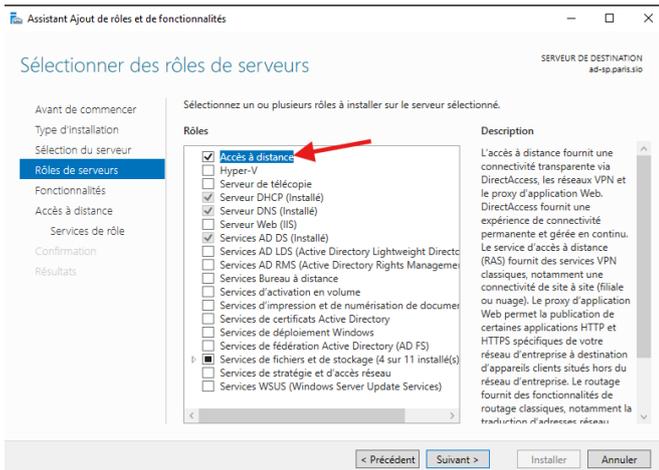
## TP 8C - Routage sur AD :

### 3 - Ajout de fonction de routage

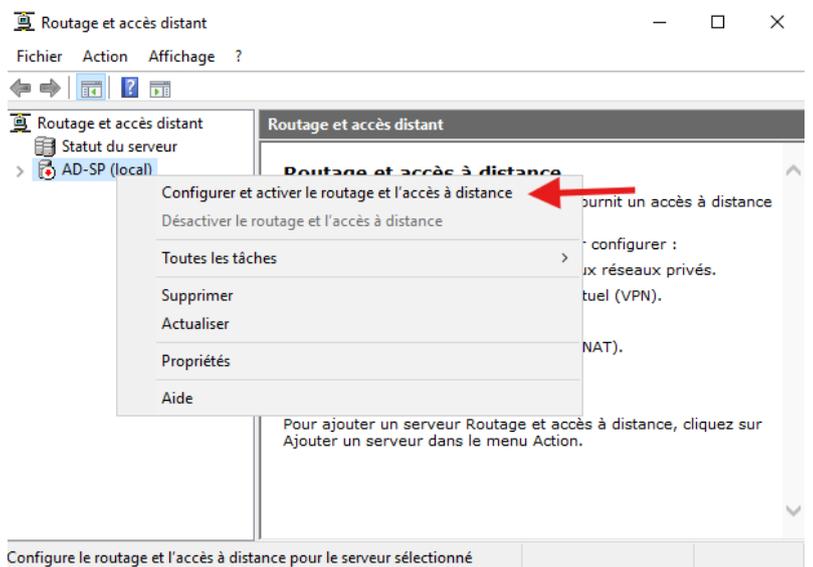
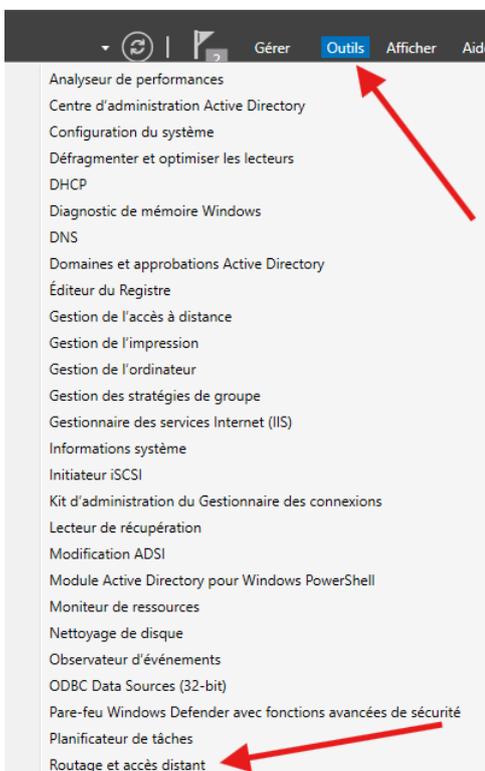
1. Installez le rôle "Accès à distance" :



- Cocher accès à distance



#### 4 - Configurez le routage et l'accès distant :



#### Assistant Installation d'un serveur Routage et accès distant

##### Configuration

Vous pouvez activer l'une des combinaisons de services suivantes ou vous pouvez personnaliser ce serveur.

- Accès à distance (connexion à distance ou VPN)  
Autoriser les clients distants à se connecter à ce serveur via une connexion d'accès à distance ou via Internet au moyen d'une connexion sécurisée à un réseau privé virtuel (VPN).
- NAT (Network address translation)  
Autoriser les clients internes à se connecter à Internet en utilisant une adresse IP publique.
- Accès VPN (Virtual Private Network) et NAT  
Autoriser les clients distants à se connecter à ce serveur par Internet et les clients locaux à se connecter à Internet en utilisant une seule adresse IP publique.
- Connexion sécurisée entre deux réseaux privés  
Connecter ce réseau à un réseau distant tel que celui d'une succursale.
- Configuration personnalisée  
Sélectionner une combinaison de fonctionnalités disponibles dans Routage et accès distant.

< Précédent   Suivant >   Annuler

#### Assistant Installation d'un serveur Routage et accès distant

##### Fin de l'Assistant Installation d'un serveur de routage et d'accès à distance

Vous avez terminé l'Assistant Installation d'un serveur de routage et d'accès distant.

##### Routage et accès distant

###### Démarrer le service

Le service Routage et accès distant est prêt.

Démarrer le service   Annuler

et accès distant après avoir fermé cet Assistant.

Pour fermer cet Assistant, cliquez sur Terminer.

< Précédent   Terminer   Annuler

#### Assistant Installation d'un serveur Routage et accès distant

##### Configuration personnalisée

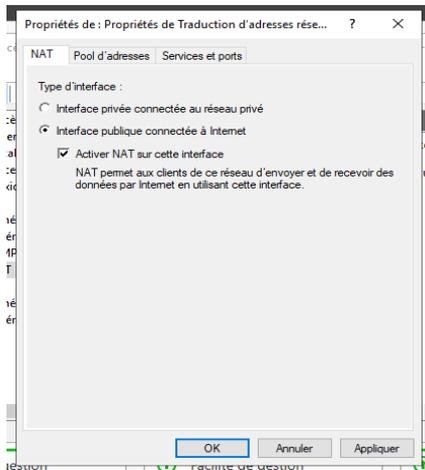
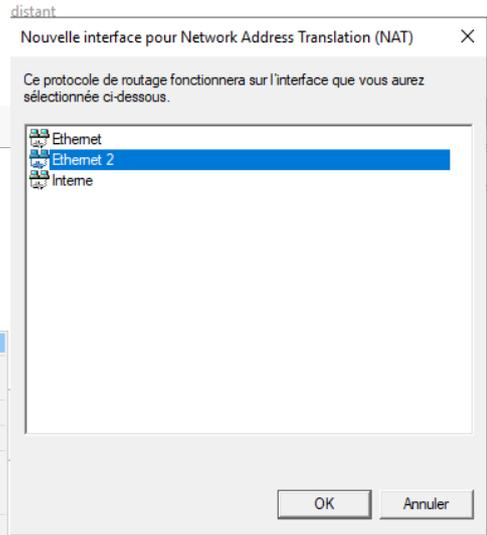
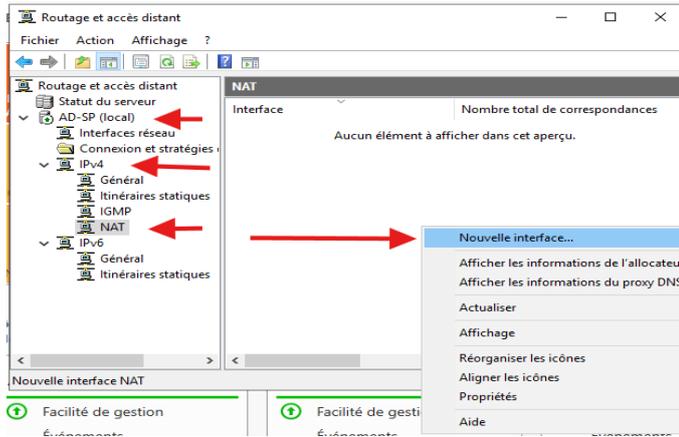
À la fermeture de l'Assistant, vous pourrez configurer les services sélectionnés dans la console Accès à distance et routage.

Sélectionnez les services que vous voulez activer sur ce serveur.

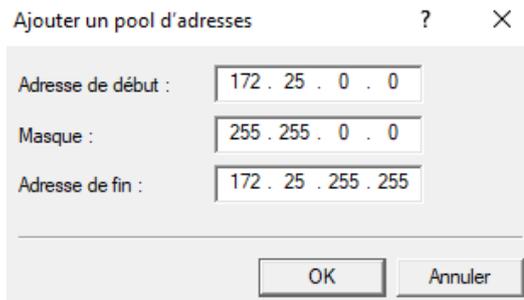
- Accès VPN
- Accès réseau à distance
- Connexions à la demande (utilisées pour le routage au niveau d'une agence)
- NAT
- Routage réseau

< Précédent   Suivant >   Annuler

## 5 - Configurez les interfaces réseau :



## Configuration Ethernet



Configuration :

Steevy :

Ajouter un pool d'adresses ? ✕

Adresse de début : 192 . 168 . 120 . 0

Masque : 255 . 255 . 255 . 0

Adresse de fin : 192 . 168 . 120 . 255

OK Annuler

Paul :

Ajouter un pool d'adresses ? ✕

Adresse de début : 192 . 168 . 117 . 0

Masque : 255 . 255 . 255 . 0

Adresse de fin : 192 . 168 . 117 . 255

OK Annuler

Mohamed :

Modifier le pool d'adresses ? ✕

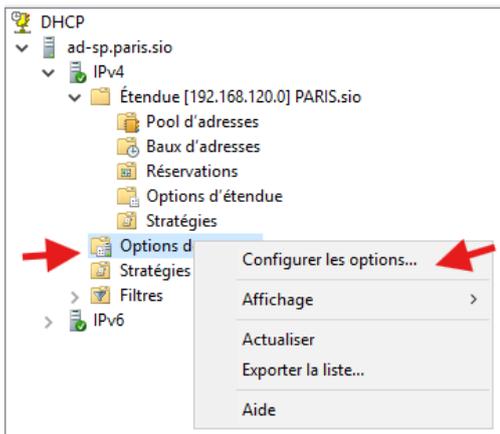
Adresse de début : 192 . 168 . 122 . 0

Masque : 255 . 255 . 0 . 0

Adresse de fin : 192 . 168 . 122 . 255

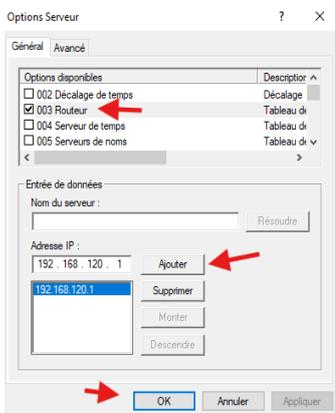
OK Annuler

- Pour récupérer une passerelle, modifier la configuration du DHCP pour cela allez dans outil -> clic droit DHCP puis clic droit sur option de server, puis sélectionner routeur est ajouter la passerelle par défauts.

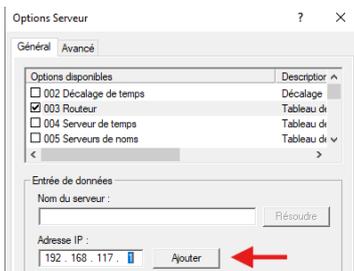


## Configuration

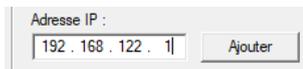
### Steevy



### Paul



### Mohamed



**Résultat IP config Windows client :**

## Steevy

```
Carte Ethernet Ethernet :  
Suffixe DNS propre à la connexion. . . : PARIS.sio  
Adresse IPv6 de liaison locale. . . . : fe80::22c9:3662:3369:9bed%4  
Adresse IPv4. . . . . : 192.168.120.7  
Masque de sous-réseau. . . . . : 255.255.255.0  
Passerelle par défaut. . . . . : 192.168.120.1
```

## Paul

```
Carte Ethernet Ethernet :  
Suffixe DNS propre à la connexion. . . : lallau.sio  
Adresse IPv6 de liaison locale. . . . : fe80::616b:2c7a:8a89:19d5%4  
Adresse IPv4. . . . . : 192.168.117.5  
Masque de sous-réseau. . . . . : 255.255.255.0  
Passerelle par défaut. . . . . : 192.168.117.1
```

## Mohamed :

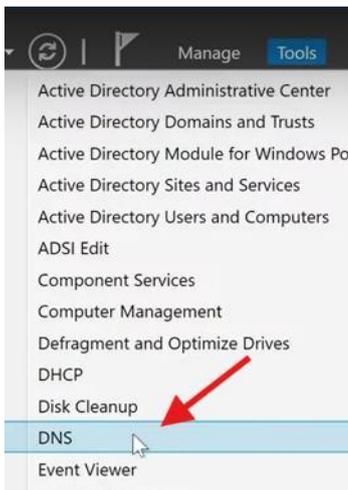
```
Carte Ethernet Ethernet :  
Suffixe DNS propre à la connexion. . . : toure.sio  
Adresse IPv6 de liaison locale. . . . : fe80::4cda:f3b1:1c5d:4c84%4  
Adresse IPv4. . . . . : 192.168.122.5  
Masque de sous-réseau. . . . . : 255.255.255.0  
Passerelle par défaut. . . . . : 192.168.122.1
```

## 6 - Vérifications

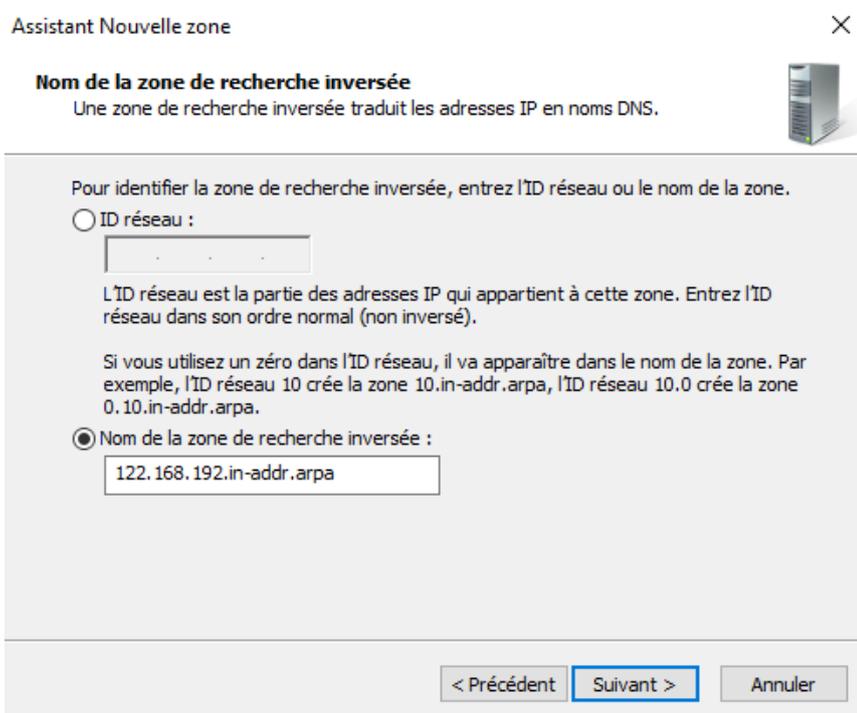
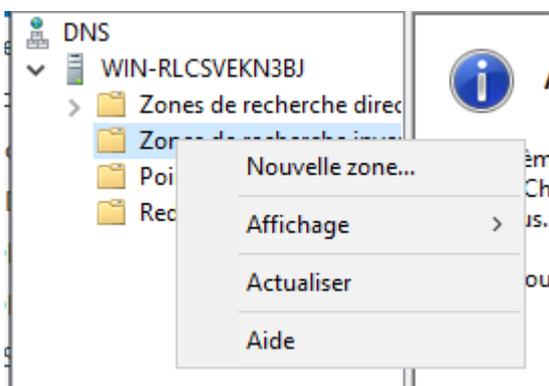
A partir du poste windows client, essayer maintenant de contacter (ou pinger) l'adresse du proxy 172.16.0.1 ou le dns de google. Pouvez-vous naviguer sur internet directement à partir du navigateur ?

Activer le revers DNS

Aller dans outils puis DNS.



Clic droit sur zone de recherche inversée



Pour l'activation du routage NAT par l'AD (ou un équipement équivalent sur le réseau interne) est indispensable pour contacter les réseaux extérieurs à votre réseau interne ?

Il faut activer le NAT sur l'AD (ou un autre routeur). Sinon, les machines internes ne pourront pas communiquer avec l'extérieur.

Essayer de joindre (un ping) un hôte windows 10 d'un domaine AD\_XX autre que le vôtre.

Qu'observez-vous et pourquoi ?

Steevy :

```
C:\Users\AdminLocal>ping AD-sp

Envoi d'une requête 'ping' sur ad-sp.local [fe80::8f51:f812:559d:70ab%3] :
Réponse de fe80::8f51:f812:559d:70ab%3 : temps=1 ms
Réponse de fe80::8f51:f812:559d:70ab%3 : temps=2 ms
Réponse de fe80::8f51:f812:559d:70ab%3 : temps=1 ms
Réponse de fe80::8f51:f812:559d:70ab%3 : temps=1 ms

Statistiques Ping pour fe80::8f51:f812:559d:70ab%3:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms

C:\Users\AdminLocal>
```

Mohamed :

```
C:\Users\AdminLocal>ping AD-MT

Envoi d'une requête 'ping' sur AD-MT.toure.sio [192.168.122.1] avec 32 octets de données :
Réponse de 192.168.122.1 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.122.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

## Bilan du TP

La mise en place d'un Active Directory permet de relier des machines à un domaine et de gérer les connexions avec un compte unique par employé. Cela permet de gérer les permissions de données en accordant plus ou moins de droits selon la personne, qu'il s'agisse d'un administrateur ou d'un employé.

Le DNS permet de donner un nom à une machine, ce qui permet de la contacter par son nom plutôt que par son adresse IP. Cela est pratique lorsqu'il y a un DHCP qui attribue des adresses IP dynamiques aux machines.

Le DHCP permet de donner automatiquement une adresse IP à toute machine qui se connecte au réseau.

## TP5-CSI

### 1 - Objectif

Nous venons de déployer une infrastructure de base d'un réseau d'une petite/moyenne organisation.

Les postes clients sont utilisables à partir d'une base d'utilisateurs centralisée dans l'AD, les postes disposent des ressources du réseau et d'une configuration automatique (adresse IP par DHCP, DNS, partage de dossier ou imprimante, authentification centralisée, fourniture d'un service web sur internet)

Les cases sont-elles toutes cochées ? Bien sûr que non ! Par défaut, windows propose très peu de fonctionnalités liées à la sécurité (pas de "secure by design" ?)

Nous allons simplement ici utiliser un outil de diagnostic de sécurité AD pour effectuer le premier audit de notre environnement.

### 2 - Présentation de PingCastle

Présentation de PingCastle Dans le cadre de la sécurisation des infrastructures informatiques, il est essentiel d'évaluer régulièrement l'état de santé d'Active Directory afin d'identifier les vulnérabilités potentielles. PingCastle est un outil (français à l'origine racheté par Netwix en 2024) d'audit automatisé qui permet d'analyser rapidement un domaine Active Directory et de générer un rapport détaillé sur les risques liés aux comptes utilisateurs, aux configurations obsolètes ou aux mauvaises pratiques de sécurité.

Il existe des alternatives à PingCastle pour la réalisation d'audit comme Purple Knight et d'autres plus axés sur l'aspect offensif/pentesting : LAPSToolkit, BloodHound ou ADRecon

### 3 - Auditer avec PingCastle

L'utilisation de l'outil est simple, depuis un poste connecté à un domaine AD ou sur un windows server contrôleur du domaine (pas conseillé et plus difficile à mettre en oeuvre), il Suffit de télécharger et d'exécuter l'outil qui va se charger de fournir un audit de l'infrastructure AD.

#### 3.1 - Mode opératoire

Téléchargez l'outils depuis la dernière release sur <https://github.com/netwrix/pingcastle>

- Partager le fichier avec votre vm winX à l'aide d'une partage fichier fait avec virtualbox
- Décompresser l'archive dans un dossier de votre winX
- Ouvrir un PowerShell
- Ensuite ls pour voir le répertoire où vous vous trouvez

Puis naviguer jusqu'à dans le répertoire PingCastle\_3.3.0.1 avec les commandes ci dessous

- cd .\Desktop\  
- cd .\PingCastle\_3.3.0.1\  
- Exécuter la commande .\PingCastle.exe --healthcheck

Après avoir fait tout ça, aller voir dans le dossier que vous avez installé et cliquer sur celui-ci sélectionné.

 Active_Directory_Security_Self_Assessme...	13/09/2024 19:50	Microsoft Edge P...	2 739 Ko
 ad_hc_toure.sio	04/02/2025 15:42	Microsoft Edge H...	1 432 Ko
 ad_hc_toure.sio	04/02/2025 15:42	Microsoft Edge H...	44 Ko
 changelog	25/09/2024 22:15	Document texte	37 Ko
 license	03/02/2024 10:58	Document au for...	13 Ko
 PingCastle v3.0.0	07/02/2023 18:37	Microsoft Edge P...	1 657 Ko
 PingCastle	25/09/2024 22:08	Application	2 678 Ko
 PingCastle.exe.config	25/09/2024 21:57	Fichier CONFIG	6 Ko
 PingCastleAutoUpdater	24/09/2024 17:21	Application	89 Ko
 PingCastleAutoUpdater.exe.config	24/09/2024 17:11	Fichier CONFIG	1 Ko

```
Free Edition of PingCastle 3.3.0 - Not for commercial use
Starting the task: Perform analysis for paris.sio
[13:10:18] Getting domain information (paris.sio)
[13:10:21] An exception occurred when doing the task: Perform analysis for paris.sio
Active Directory not Found: Aucune entrée DNS n'existe pour l'hôte paris.sio.
Task Perform analysis for paris.sio completed
PS C:\Users\utilisateur1\Desktop\PingCastle_3.3.0.1> .\PingCastle.exe --healthcheck

Free Edition of PingCastle 3.3.0 - Not for commercial use
Starting the task: Perform analysis for paris.sio
[13:17:58] Getting domain information (paris.sio)
[13:17:59] Gathering general data
[13:18:00] This domain contains approximatively 160 objects
[13:18:30] Gathering user data
[13:18:55] Gathering computer data
[13:18:55] Gathering trust data
[13:18:56] Gathering privileged group and permissions data
[13:18:56] - Initialize
[13:18:56] - Searching for critical and infrastructure objects
[13:18:57] - Collecting objects - Iteration 1
[13:18:57] - Collecting objects - Iteration 2
[13:18:58] - Collecting objects - Iteration 3
[13:18:58] - Collecting objects - Iteration 4
[13:18:58] - Collecting objects - Iteration 5
[13:18:58] - Completing object collection
[13:18:58] - Export completed
[13:18:58] Gathering delegation data
[13:18:59] Gathering gpo data
[13:19:01] Gathering pki data
[13:19:01] Gathering sccm data
[13:19:01] Gathering exchange data
[13:19:01] Gathering anomaly data
[13:19:03] Gathering dns data
[13:19:03] Gathering WSUS data
[13:19:03] Gathering MSOL data
[13:19:03] Gathering domain controller data (including null session) (including RPC tests)
[13:20:12] Gathering network data
[13:20:12] Computing risks
[13:20:13] Export completed
[13:20:13] Generating html report
[13:20:16] Generating xml file for consolidation report
[13:20:16] Export level is Normal
[13:20:16] Personal data will NOT be included in the .xml file (add --level Full to add it. Ex: PingCastle.exe --interac
ive --level Full)
[13:20:16] Done
Task Perform analysis for paris.sio completed
PS C:\Users\utilisateur1\Desktop\PingCastle_3.3.0.1>
PS C:\Users\utilisateur1\Desktop\PingCastle_3.3.0.1> $
$ : Le terme «$» n'est pas reconnu comme nom d'applet de commande, fonction, fichier de script ou programme
```

### 3.2 - Afficher l'audit

Steevy :

Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

#### Indicators

Domain Risk Level: 85 / 100  
It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

[Compare with statistics](#)  
[Privacy notice](#)

<p>Stale Object : 46 /100 It is about operations related to user or computer objects</p>	<p>12 rules matched</p>	<p>Trusts : 0 /100 It is about connections between two Active Directories</p>	<p>0 rules matched</p>
<p>Privileged Accounts : 50 /100 It is about administrators of the Active Directory</p>	<p>5 rules matched</p>	<p>Anomalies : 85 /100 It is about specific security control points</p>	<p>17 rules matched</p>

#### Risk model

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust impermeability	Golden tickets
Old authentication protocols	Delegation Check	Trust inactive	Local group vulnerability
Provisioning	Irreversible change	Trust with Azure	Network sniffing
Replication	Privilege control		Pass-the-credential
Vulnerability management	Read-Only Domain Controllers		Password retrieval
			Reconnaissance
			Temporary admins
			Weak password

Legend:  
■ score is 0 : no risk identified but some improvements detected

Paul :

lallau.sio 2025-02-03 About

#### Active Directory indicators

This section focuses on the core security indicators.  
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

#### Indicators

Domain Risk Level: 85 / 100  
It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

[Compare with statistics](#)  
[Privacy notice](#)

<p>Stale Object : 16 /100 It is about operations related to user or computer objects</p>	<p>9 rules matched</p>	<p>Trusts : 0 /100 It is about connections between two Active Directories</p>	<p>0 rules matched</p>
<p>Privileged Accounts : 30 /100 It is about administrators of the Active Directory</p>	<p>3 rules matched</p>	<p>Anomalies : 85 /100 It is about specific security control points</p>	<p>17 rules matched</p>

#### Risk model

Mohamed :

## Active Directory Indicators

This section focuses on the core security indicators.

Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

### Indicators



Domain Risk Level: 85 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

[Compare with statistics](#)

[Privacy notice](#)



### Risk model @

Stale Objects	Privileged accounts	Trusts	Anomalies
inactive user or computer	Account take over	Old trust protocol	Audit
Network topology	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust Impenetrability	Golden ticket
Old authentication protocols	Delegation Check	Trust inactive	Local group vulnerability
Provisioning	Irreversible change	Trust with Azure	Network sniffing
Replication	Privilege control		Pass-the-credential
Vulnerability management	Read-Only Domain Controllers		Password retrieval
			Reconnaissance
			Temporary admins
			Weak password

Legend:

- score is 0 - no risk identified but some improvements detected
- score between 1 and 10 - a few actions have been identified
- score between 10 and 30 - rules should be looked with attention
- score higher than 30 - major risks identified

#### 4.Principale corrections :

##### 4.1 - Corbeille pour AD

- Pour cela win + r -> dsac.exe

Entrez le nom d'un programme, dossier, document ou ressource Internet, et Windows l'ouvrira pour vous.

: dsac.exe

 Cette tâche sera créée avec les autorisations d'administrateur.

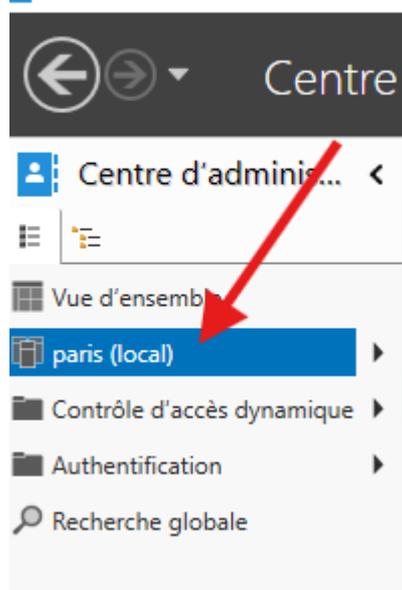
OK

Annuler

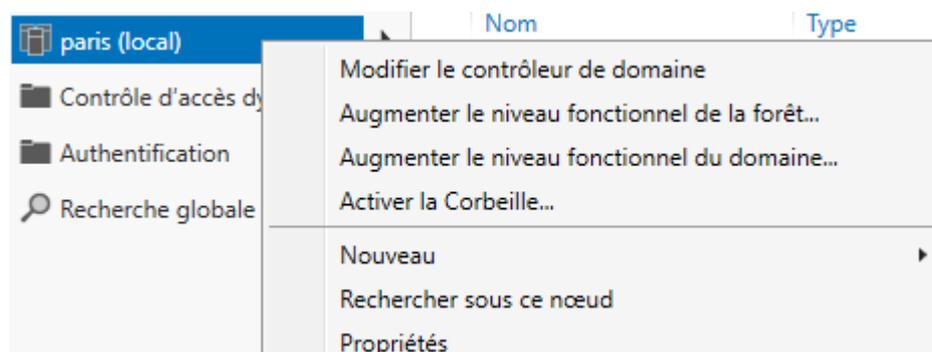
Parcourir...

- Clic droit sur domaine (local)

Centre d'administration Active Dir



- Activer la corbeille

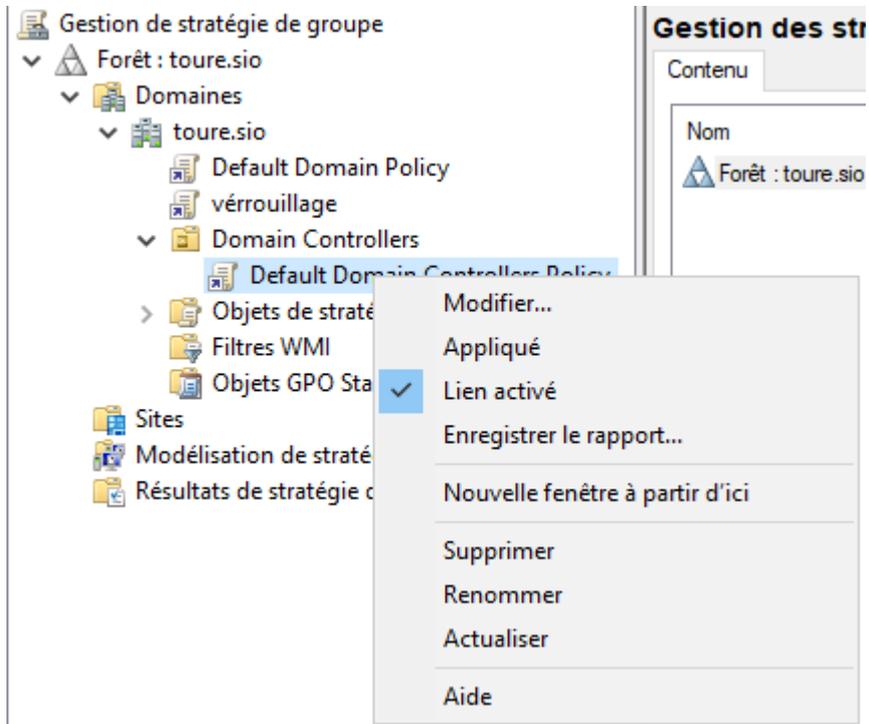


- Puis redémarrer le serveur AD

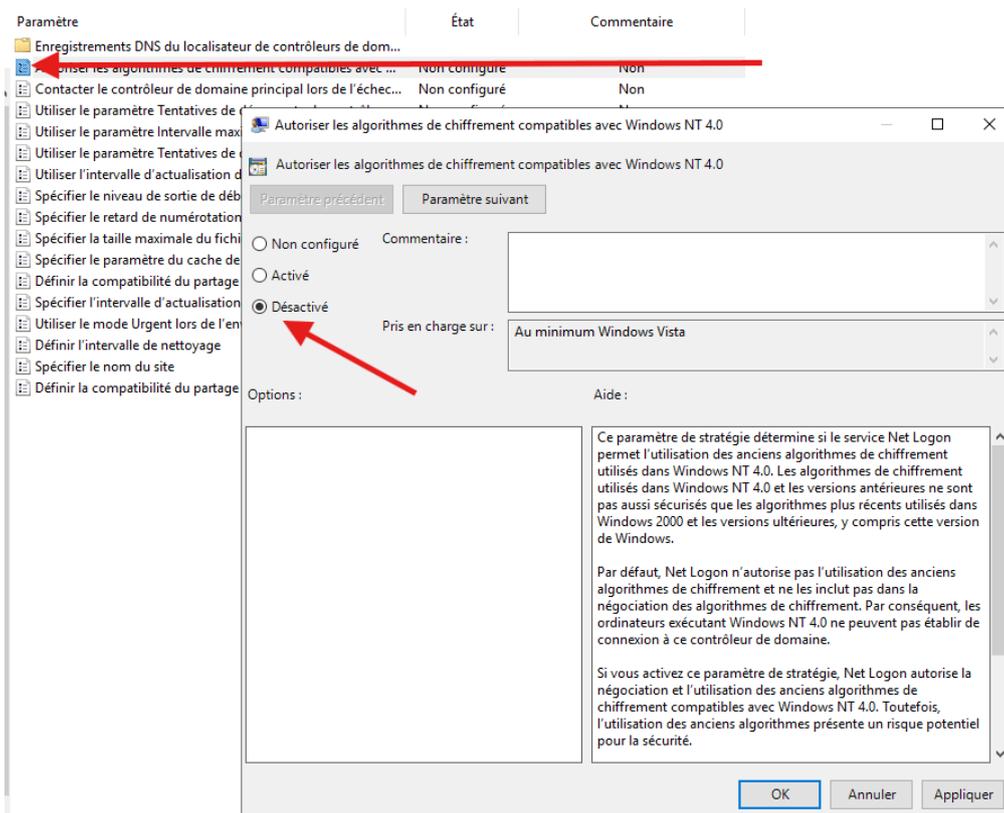
## 4.2 - Suppressions des algorithmes cryptographiques obsolètes

### Désactiver le paramètre AllowNT4Crypto

- Désactivation du paramètre AllowNT4Crypto
- Windows + r -> gpmmc.msc



- Cliquer sur modifier
- Dans configuration ordinateur -> stratégies -> modèles d'administration -> système -> puis chercher net logon et cliquer dessus
- Dans net logon double clic sur le deuxième
- Une page ouvre, désactiver le paramètre -> appliquer et quitter

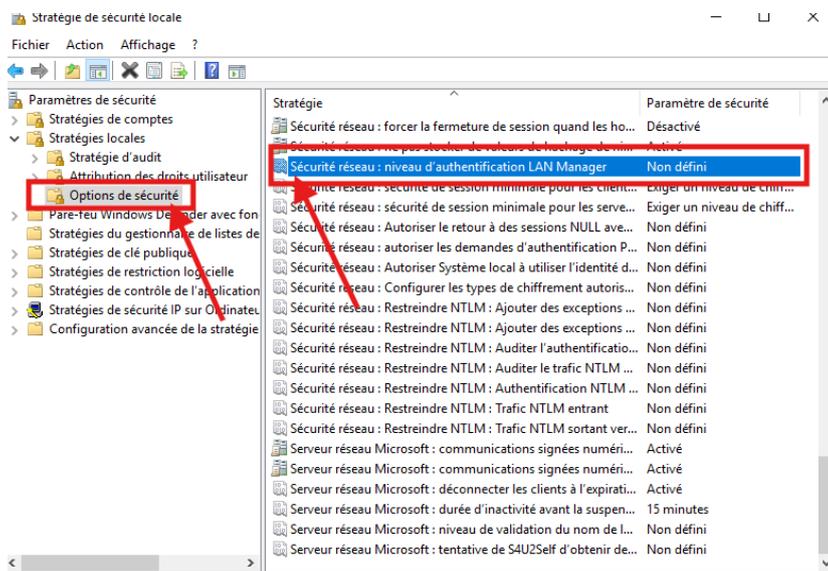


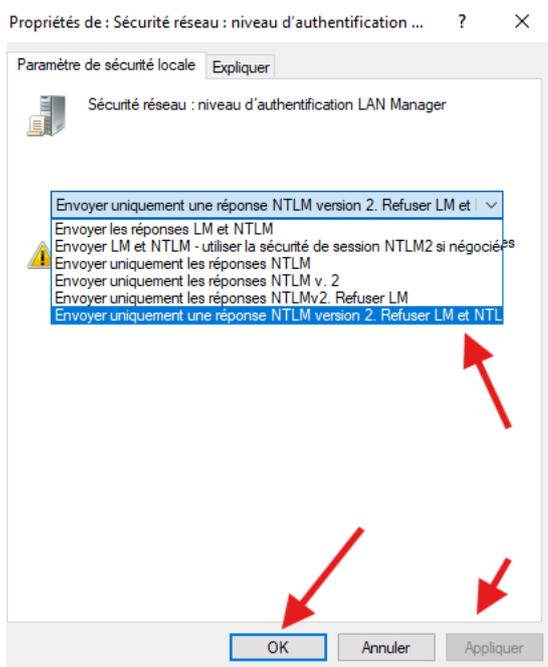
### 4.3 - Suppression des anciens protocoles NTLMv1 et LM

- Windows + r secpol.msc

- Stratégie locales → cliquer sur options de sécurité → double cliquer sur sécurité réseau niveau d'authentification LAN manager

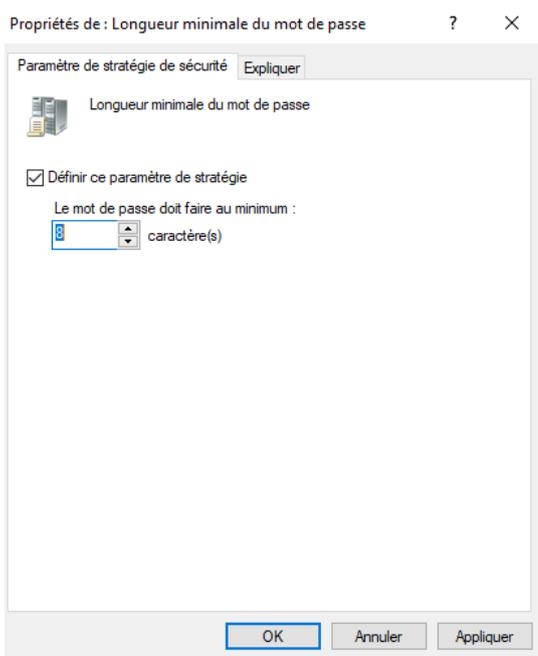
- Sélectionner le dernier appliquer et quitter





#### 4.4 - Politique de mot de passe

- Dans le volet gauche, localisez l'unité d'organisation ou le domaine où vous souhaitez appliquer la GPO.
- Faites un clic droit sur le domaine et sélectionnez "Créer un objet GPO dans ce domaine, et le lier ici".
- Faites un clic droit sur la GPO que vous venez de créer ou de modifier, puis sélectionnez "Modifier".
- Accédez à Configuration de l'ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégies de mot de passe.
- Double-cliquez sur "Longueur minimale du mot de passe"
- Cochez "Activé" et définissez la longueur minimale à 8
- Appliquer et quitter



## 5 - Autres corrections indispensables :

Établir une sauvegarde régulière de l'AD permet de revenir à une situation normale en cas d'incident grave. Elle peut être déclenchée manuellement ou programmée pour une exécution quotidienne ou hebdomadaire. Le support de sauvegarde doit se faire sur un média différent du disque dur de l'AD.

### 5.1- Procédure de sauvegarde de l'Active Directory

Crée un dossier partager dans le client pour cela

- Aller dans ce PC > disque local C > crée un dossier nomer "sauvegard AD"
- Puis clic droit > propriété > partager et encore partager >
- Dans la barre de recherche, sélectionner "rechercher des personnes"
- Écrire ad en appuyer sur entrer, sélectionner administrateur et quitter

Dans la VM administrateur :

- Dans le panneau de droite, cliquez sur "Planifier une sauvegarde"
- L'Assistant de sauvegarde s'ouvre. Cliquez sur "Suivant".
- Choisissez "Sauvegarde personnalisée" et cliquez sur "Suivant".
- Sélectionnez "Sauvegarde de l'état du système" pour inclure Active Directory et cliquez sur "Suivant".

- Choisissez un emplacement de sauvegarde. Il est recommandé de sélectionner un lecteur réseau ou un disque externe pour éviter de sauvegarder sur le même disque que le système.
- Configurez la fréquence de la sauvegarde (quotidienne ou hebdomadaire) et les heures de sauvegarde.

Finalisez la configuration et cliquez sur "Terminer".

Dans la VM administrateur :

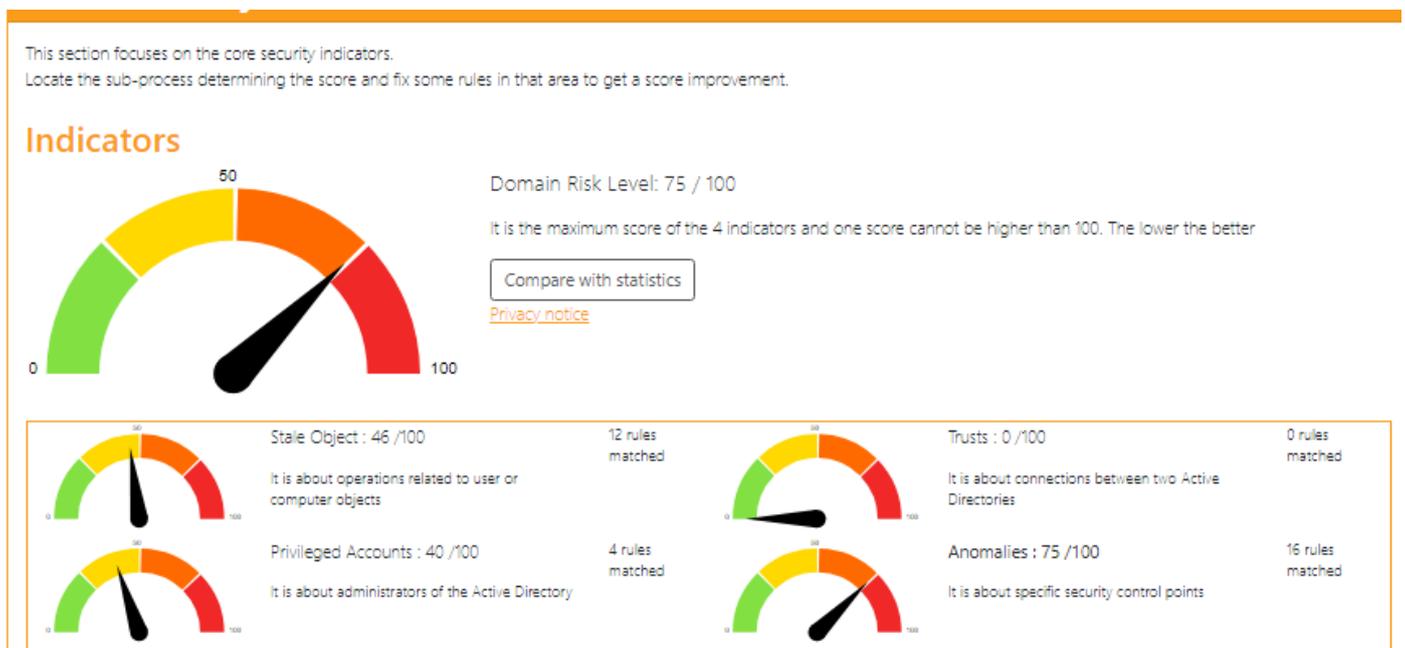
- Explorateur de fichier > réseau > dans la barre de recherche écrire IP du client
- Double clic sur le dossier, dans la barre de recherche copier adresse et renseigner le dans l'tape demander dans la sauvegarde

## 5.2 - Politique de sécurité des administrateurs locaux

La gestion LAPS (Local Administrator Password Solution) est une solution de Microsoft qui permet de gérer les mots de passe des comptes administrateurs locaux sur les ordinateurs d'un domaine. Elle génère automatiquement des mots de passe uniques et complexes pour chaque machine, qui sont ensuite stockés de manière sécurisée dans Active Directory. Cela renforce la sécurité en évitant l'utilisation de mots de passe par défaut identiques sur plusieurs ordinateurs. Seuls les utilisateurs autorisés peuvent accéder à ces mots de passe, ce qui améliore la protection des systèmes.

## 6 - Evaluer les effets de la correction

Mohamed :

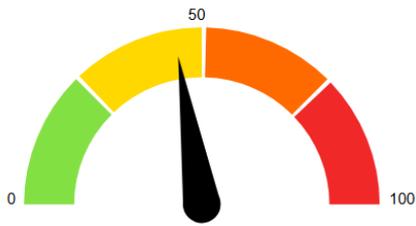


Paul :

This section focuses on the core security indicators.

Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

## Indicators

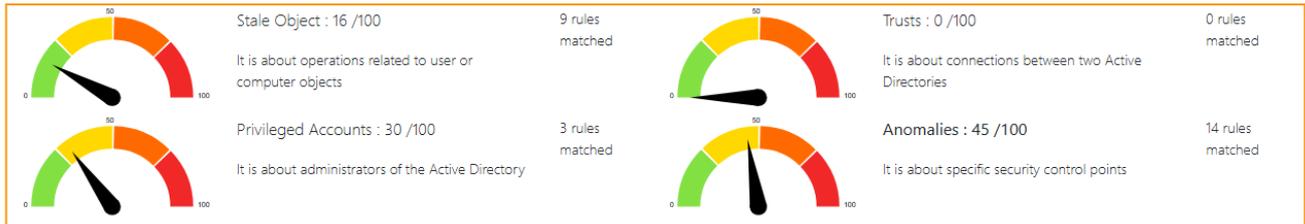


Domain Risk Level: 45 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

[Compare with statistics](#)

[Privacy notice](#)



**Risk model** ?