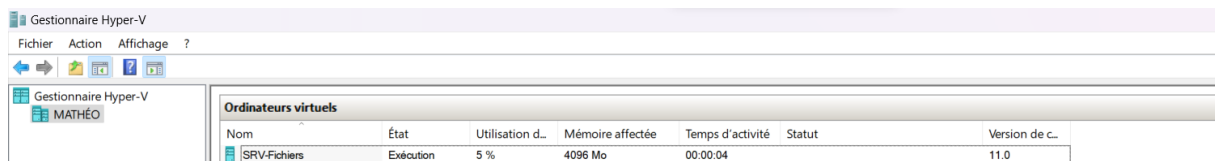


## TP Active directory/DNS

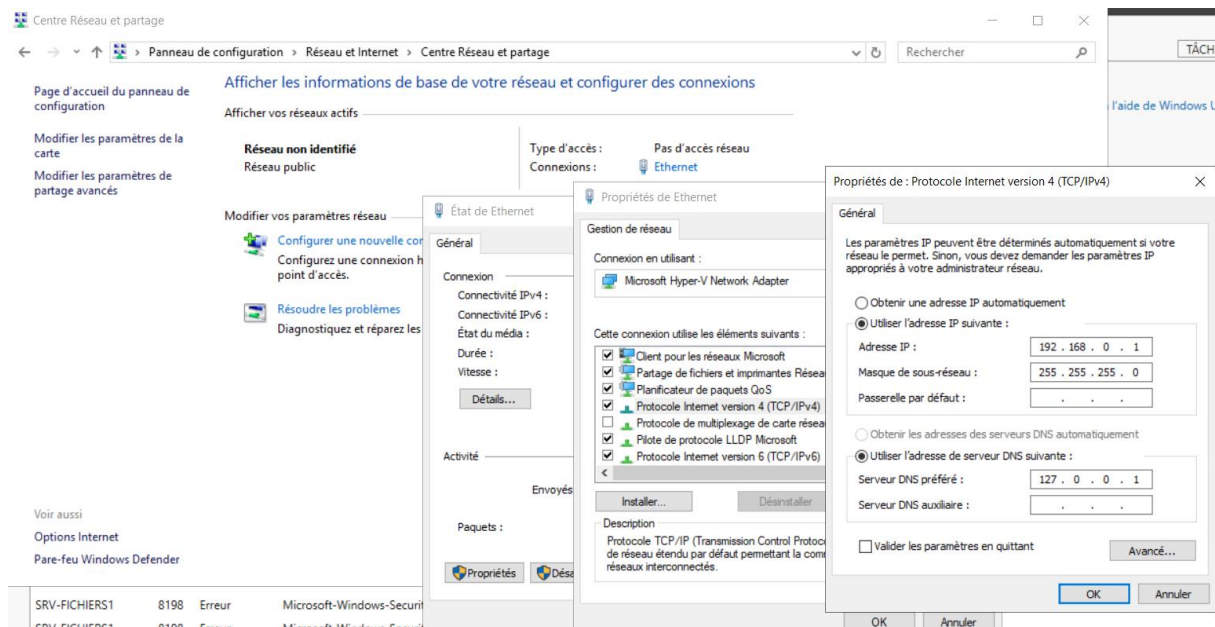
Intro :

Dans ce tp nous allons faire l'installation d'active directory et de la partie DNS pour pouvoir gérer les utilisateurs et les dossiers auxquels les utilisateurs souhaitent accéder.

Pour cela rendons nous sur hyperV où l'on lancera notre VM Windows server installé dans les précédent TP



Puis une fois connecté on va y spécifier une adresse IP et DNS ici 127.0.0.1 car ce serveur de fichier fera lui-même serveur DNS.



On va maintenant pouvoir passer à la partie de l'ajout de active directory et dns

Pour ce faire on va utiliser l'option d'ajout de fonctionnalité du gestionnaire de serveur.

Gestionnaire de serveur

Gestionnaire de serveur > Serveur local

Tableau de bord  
Serveur local  
Tous les serveurs

PROPRIÉTÉS  
Pour SRV-FICHIERS1

Nom de l'ordinateur: SRV-FICHIERS1  
Groupe de travail: WORKGROUP

Dernières mises à jour installées: Windows Update  
Jamais  
Télécharger les mises à jour

Ajouter des rôles et fonctionnalités  
Supprimer des rôles et fonctionnalités  
Ajouter des serveurs  
Créer un groupe de serveurs  
Priorités du Gestionnaire de serveur

Assistant Ajout de rôles et de fonctionnalités

### Sélectionner le type d'installation

SERVEUR DE DESTINATION  
SRV-FICHIERS1

Avant de commencer  
**Type d'installation**  
Sélection du serveur  
Rôles de serveurs  
Fonctionnalités  
Confirmation  
Résultats

Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.

- Installation basée sur un rôle ou une fonctionnalité**  
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.
- Installation des services Bureau à distance**  
Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.

< Précédent   Suivant >   Installer   Annuler

On sélectionne notre serveur on en a qu'un seul.

### Sélectionner le serveur de destination

SERVEUR DE DESTINATION  
SRV-FICHIERS1

Avant de commencer  
Type d'installation  
**Sélection du serveur**  
Rôles de serveurs  
Fonctionnalités  
Confirmation  
Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

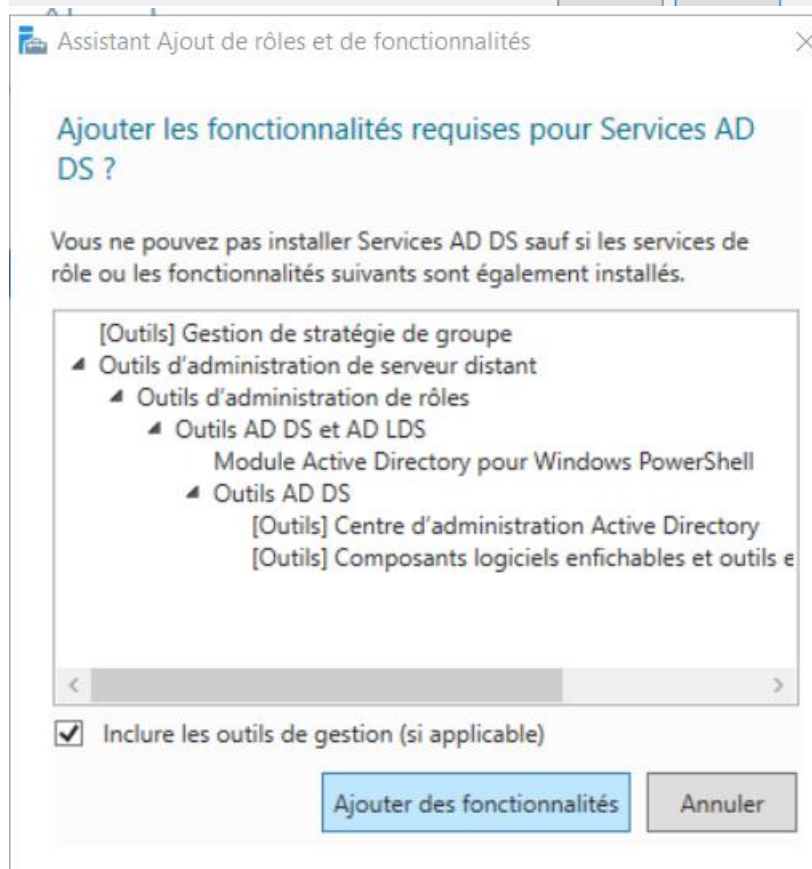
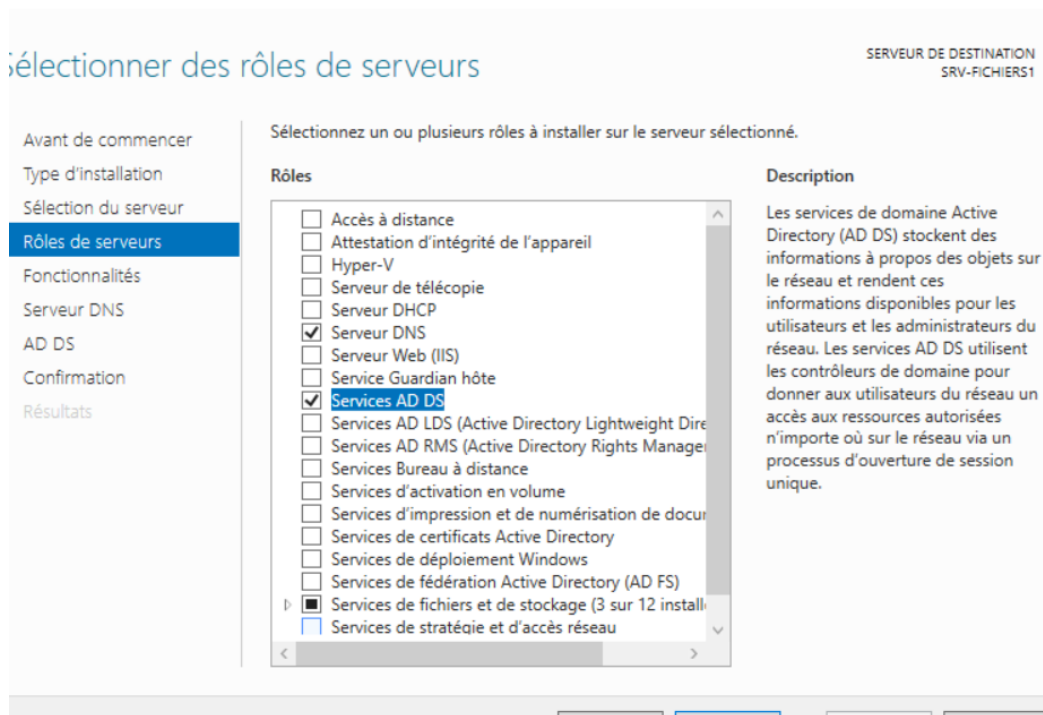
- Sélectionner un serveur du pool de serveurs
- Sélectionner un disque dur virtuel

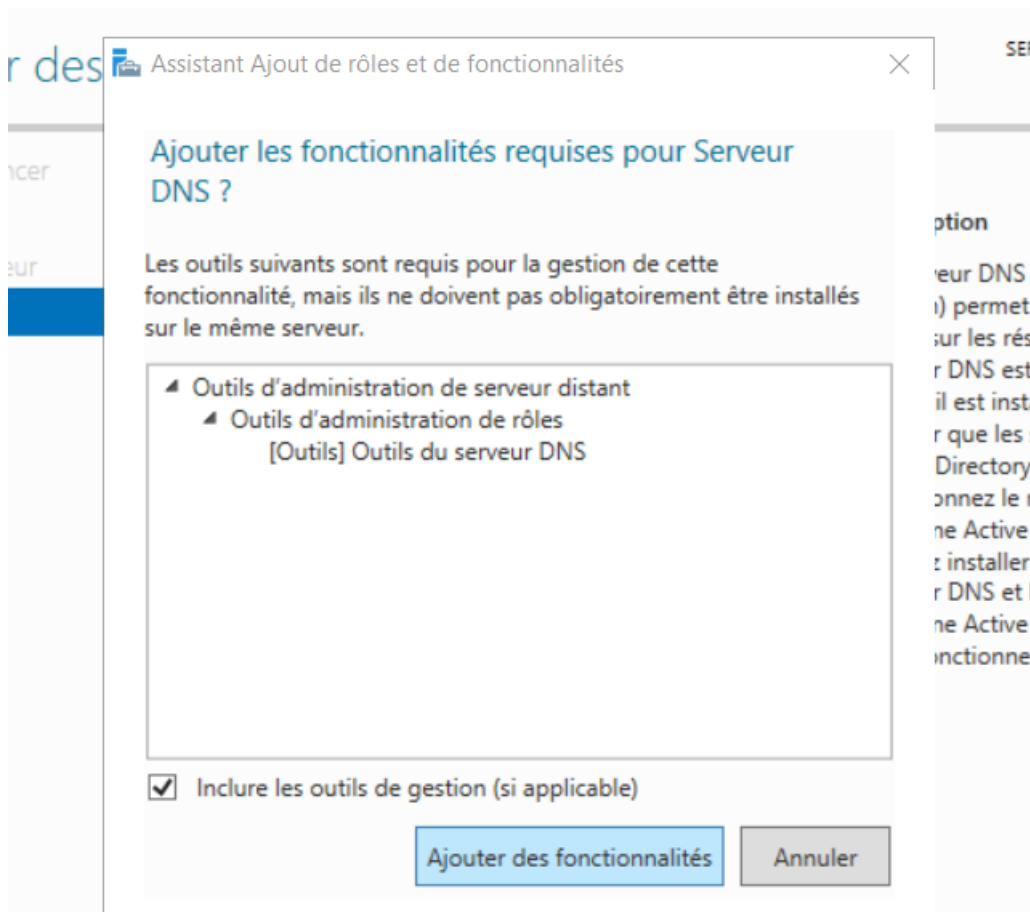
Pool de serveurs

Filtre :

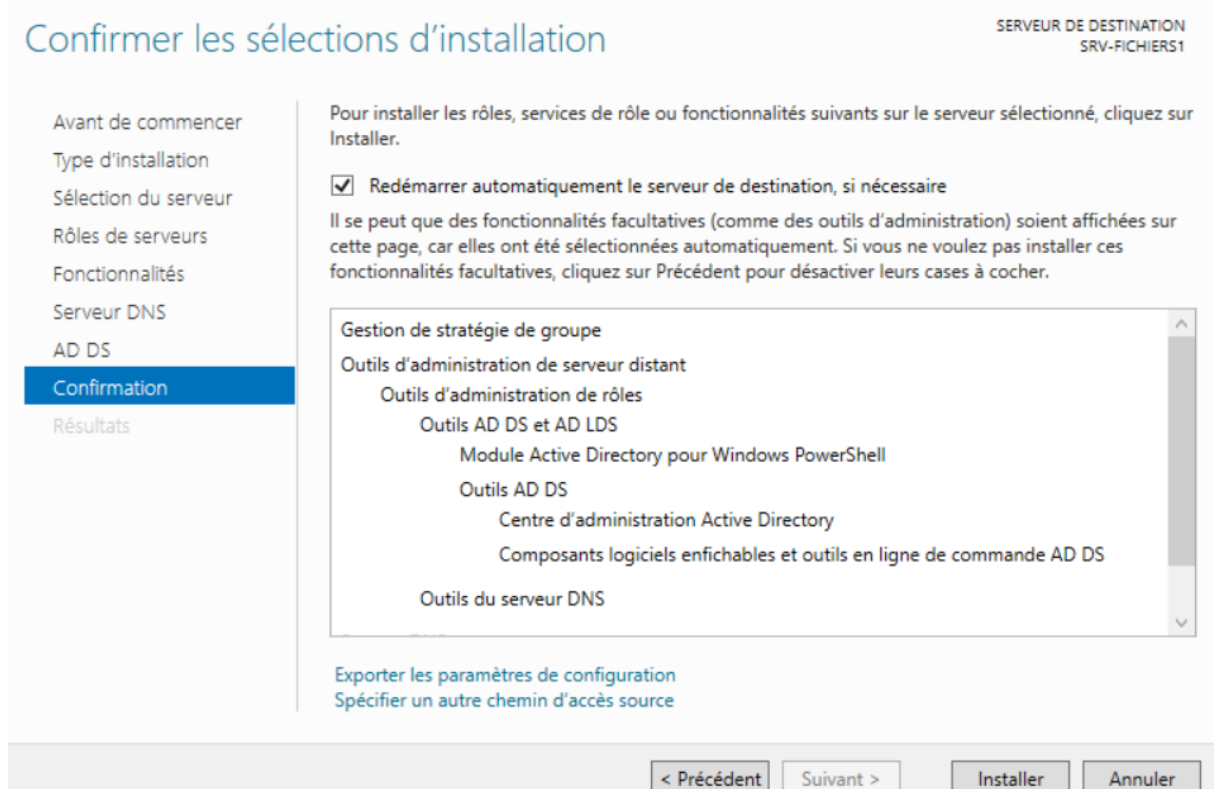
Nom	Adresse IP	Système d'exploitation
SRV-FICHIERS1	192.168.0.1	Microsoft Windows Server 2019 Standard

Puis on va sélectionner les options qui nous intéressent : Dans notre cas Service DNS et Service AD DS



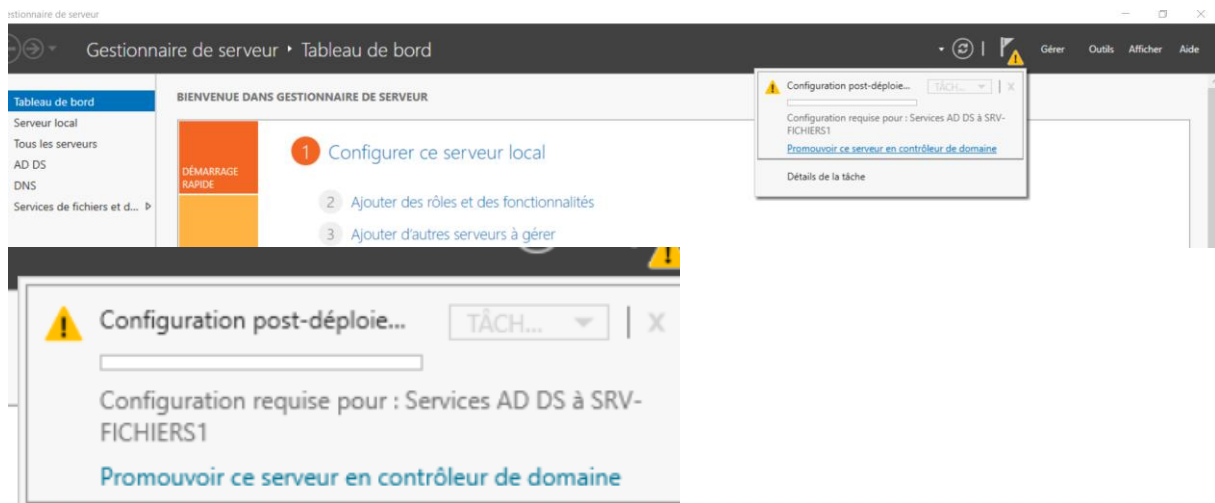


On laissera coché toute les options et fonctionnalités et on fait suivant jusqu'à que on nous demande de faire l'installation et on cochera la case de redémarrage une fois l'instalation terminé

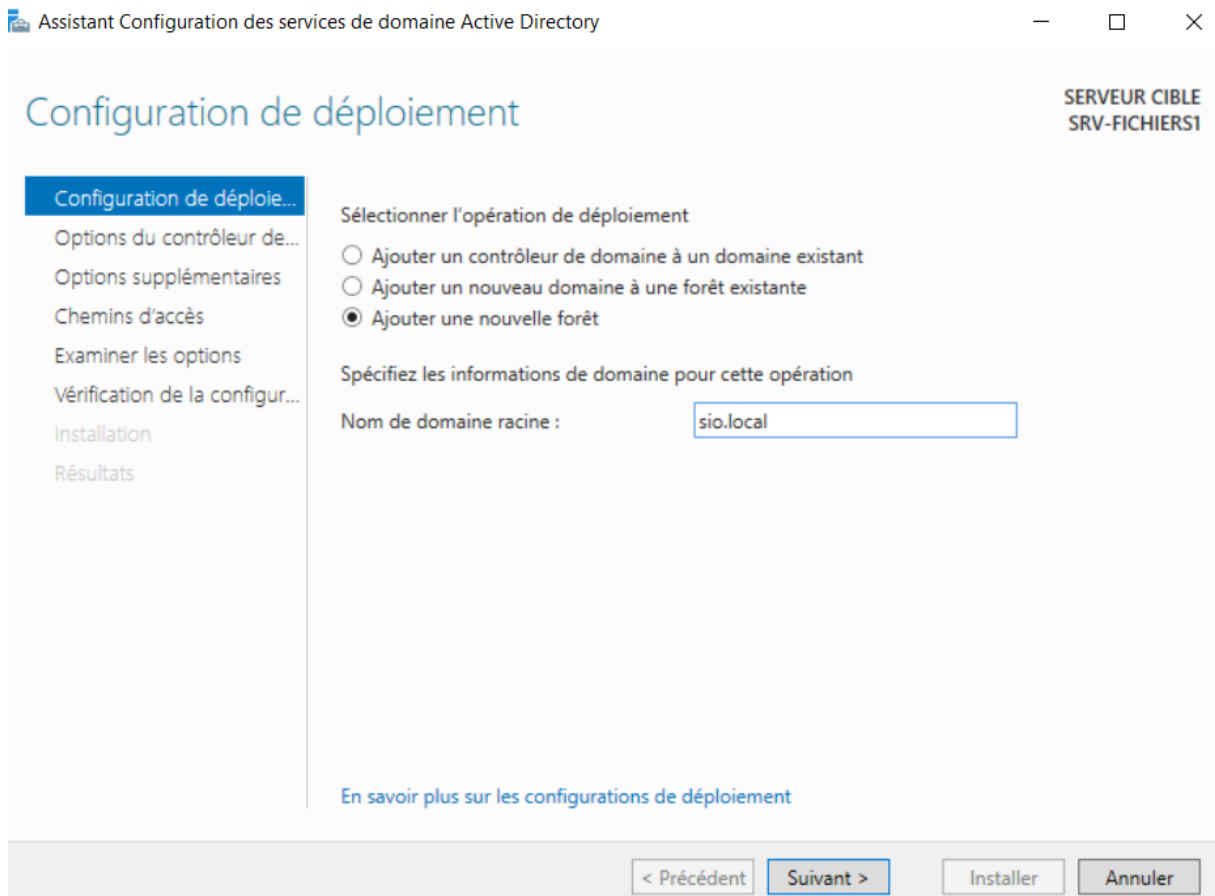


Puis si la VM ne redémarre pas automatiquement il faut le faire manuellement.

On va maintenant cliquer en haut à droite sur le triangle et faire promouvoir ce serveur en contrôleur de domaine



Comme nous n'avons encore rien nous allons créer une nouvelle forêt et choisir un nom et avec la terminaison .local pour que le serveur ne confonde pas avec internet.



Ensuite on ne changera pas les paramètres mais simplement on ajoutera un mot de passe de secours au cas où une panne surviendrait : restosio57\*

Assistant Configuration des services de domaine Active Directory

## Options du contrôleur de domaine

SERVEUR CIBLE  
SRV-FICHIERS1

- Configuration de déploiement...
- Options du contrôleur de...**
- Options DNS
- Options supplémentaires
- Chemins d'accès
- Examiner les options
- Vérification de la configuration...
- Installation
- Résultats

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

Niveau fonctionnel de la forêt :

Niveau fonctionnel du domaine :

Spécifier les fonctionnalités de contrôleur de domaine

Serveur DNS (Domain Name System)

Catalogue global (GC)

Contrôleur de domaine en lecture seule (RODC)

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

Mot de passe :

Confirmer le mot de passe :

[En savoir plus sur les options pour le contrôleur de domaine](#)

< Précédent   Suivant >   Installer   Annuler

Puis suivant sans toucher car c'est le serveur original

## Options DNS

SERVEUR CIBLE  
SRV-FICHIERS1

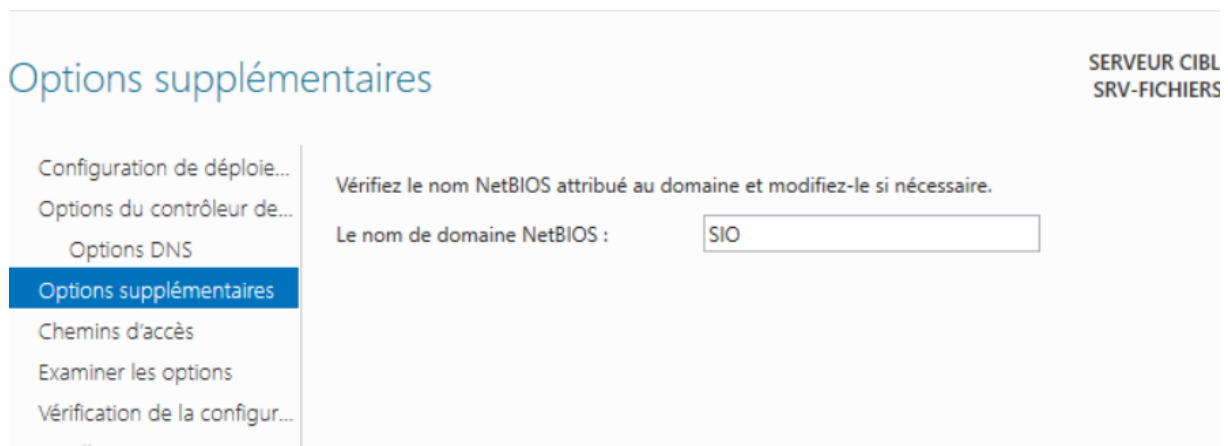
**⚠ Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est intro... [Afficher plus](#)**

- Configuration de déploiement...
- Options du contrôleur de...
- Options DNS**
- Options supplémentaires
- Chemins d'accès
- Examiner les options
- Vérification de la configuration...
- Installation
- Résultats

Spécifier les options de délégation DNS

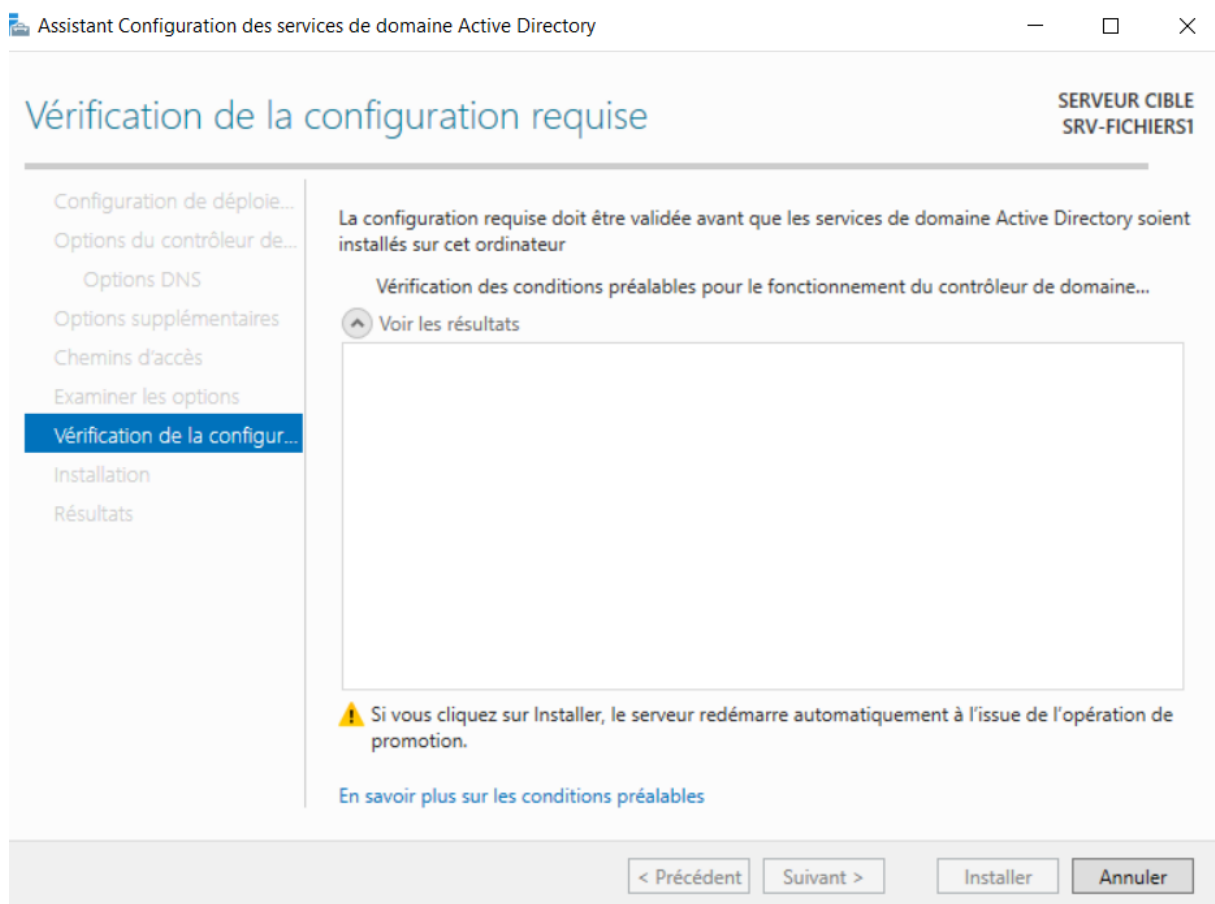
Créer une délégation DNS

Ensuite on vérifie que le nom donné par le netbios nous convient



Ensuite pour chemin d'accès et examiner les options on ne touchera a rien car les chemins sont ceux par défaut et examiner fait simplement un récapitulatif.

Puis le serveur va faire une vérification de nos prérequis.



Puis on a deux avertissements mais le processus est valide alors on peut faire installer puis redémarrer la VM à la fin de cette étape.

Vérification de la configuration requise

SERVEUR CIBLE  
SRV-FICHIERS1

✓ Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour comme... [Afficher plus](#) ✕

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

La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur

[Réexécuter la vérification de la configuration requise](#)

⬆ Voir les résultats

⚠ Les contrôleurs de domaine Windows Server 2019 offrent un paramètre de sécurité par défaut nommé « Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ». Ce paramètre empêche l'utilisation d'algorithmes de chiffrement faibles lors de l'établissement de sessions sur canal sécurisé.

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

⚠ Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez

⚠ Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération de promotion.

[En savoir plus sur les conditions préalables](#)

< Précédent   Suivant >   Installer   Annuler

On va aller vérifier une fois le démarrage fait si active directory est bien présent pour cela on va lancer outils d'administration.

Filtres ▾

Meilleur résultat

Outil Capture d'écran  
Application de bureau

Paramètres

Outils d'administration

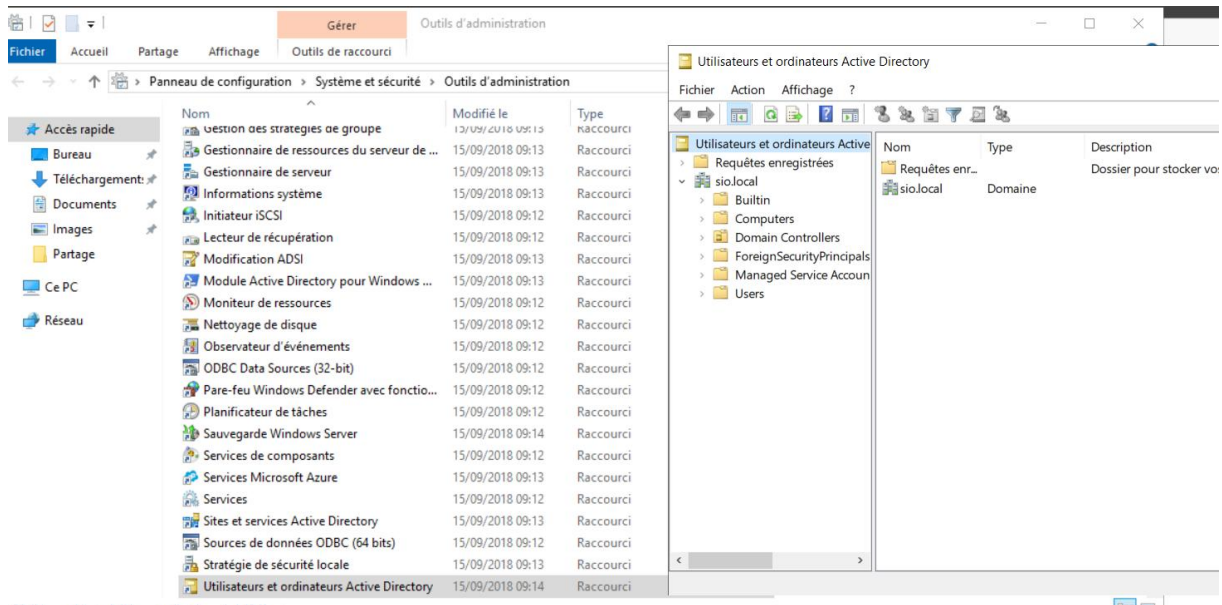
Applications

Outils d'administration Windows

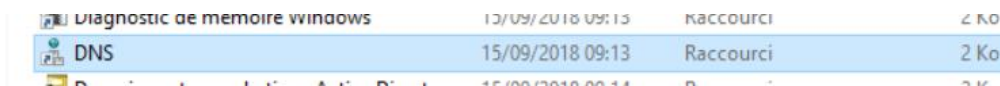
Outils d'administration|



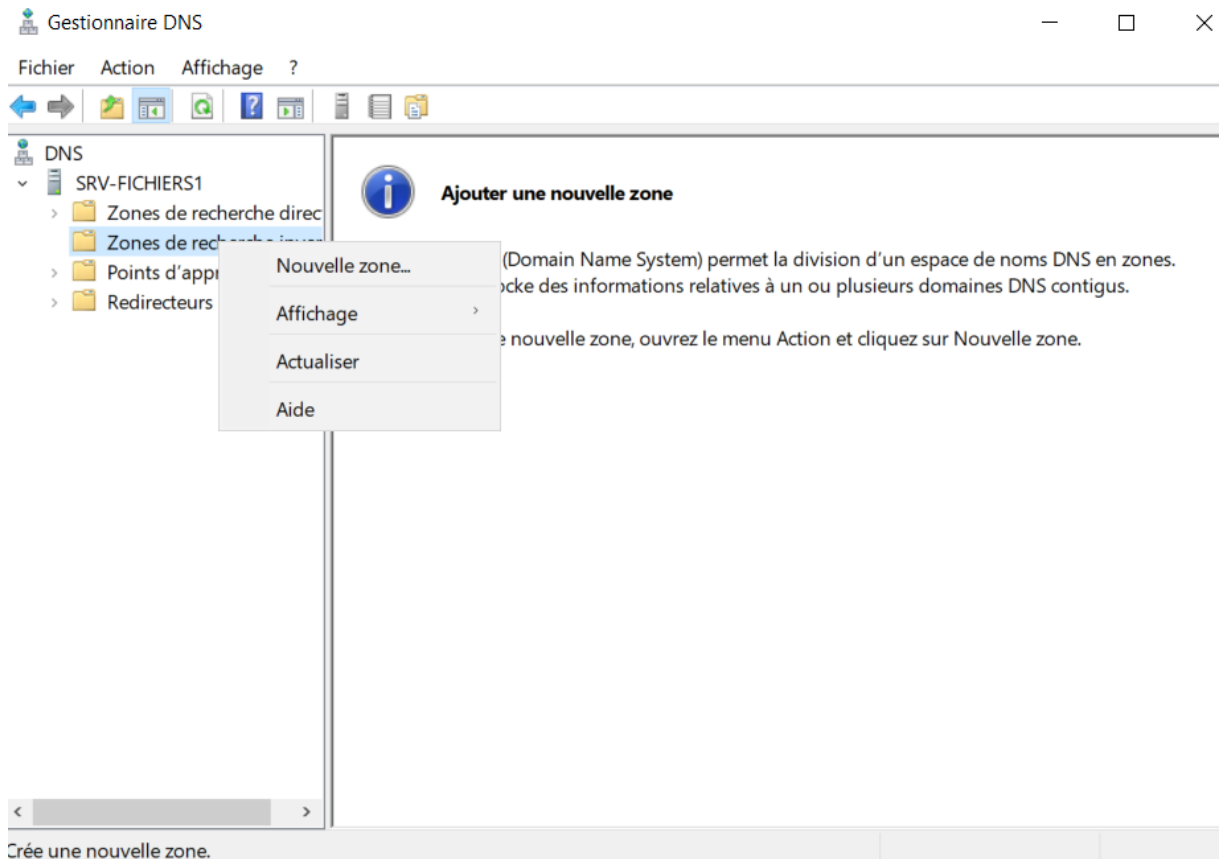
On le trouve tout en bas et il est bien fonctionnel



On va ensuite configurer le dns qui se trouve au même endroit.



Donc nous allons ajouter une zone de recherche inversé pour lier une ip à un nom.



**Type de zone**

Le serveur DNS prend en charge différents types de zones et de stockages.



Sélectionnez le type de zone que vous voulez créer :

 Zone principale

Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.

 Zone secondaire

Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.

 Zone de stub

Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone.

Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine accessible en écriture)

&lt; Précédent

Suivant &gt;

Annuler

Ce sera une zone principale qui enregistré dans l'active directory sera mise à jour en continu.

On laissera ensuite l'option par défaut pour communiquer avec tout les serveurs.

**Étendue de la zone de répllication de Active Directory**

Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.



Choisissez la façon dont les données de la zone doivent être répliquées :

Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt :  
sio.local

Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine :  
sio.local

Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : sio.local

Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition  
d'annuaire :

&lt; Précédent

Suivant &gt;

Annuler

Et bien sûr on travaille en ipv4

### Nom de la zone de recherche inversée

Une zone de recherche inversée traduit les adresses IP en

Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6.

Zone de recherche inversée IPv4

Puis il faudra rentrer les 3/4 de notre ip réseau pour mes deux VM 192.168.0

### Nom de la zone de recherche inversée

Une zone de recherche inversée traduit les adresses IP en noms DNS.



Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

ID réseau :

192 .168 .0

L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

Ensuite on laissera les mises a jour dynamiques pour plus de sécurité et on fera terminer

### Mise à niveau dynamique

Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.




Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.

Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)

Cette option n'est disponible que pour les zones intégrées à Active Directory.

Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées  
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.

 Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

Ne pas autoriser les mises à jour dynamiques  
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

< Précédent

Suivant >

Annuler

### Assistant Nouvelle zone



### Fin de l'Assistant Nouvelle zone

L'Assistant Nouvelle zone s'est terminé correctement. Vous avez spécifié les paramètres suivants :

Nom : 0.168.192.in-addr.arpa  
Type : Serveur principal intégré à Active Directory  
Type de recherche : Inversée

Remarque : ajoutez des enregistrements à la zone, ou vérifiez que les enregistrements sont mis à jour de façon dynamique. Vous pourrez ensuite vérifier la résolution des noms avec nslookup.

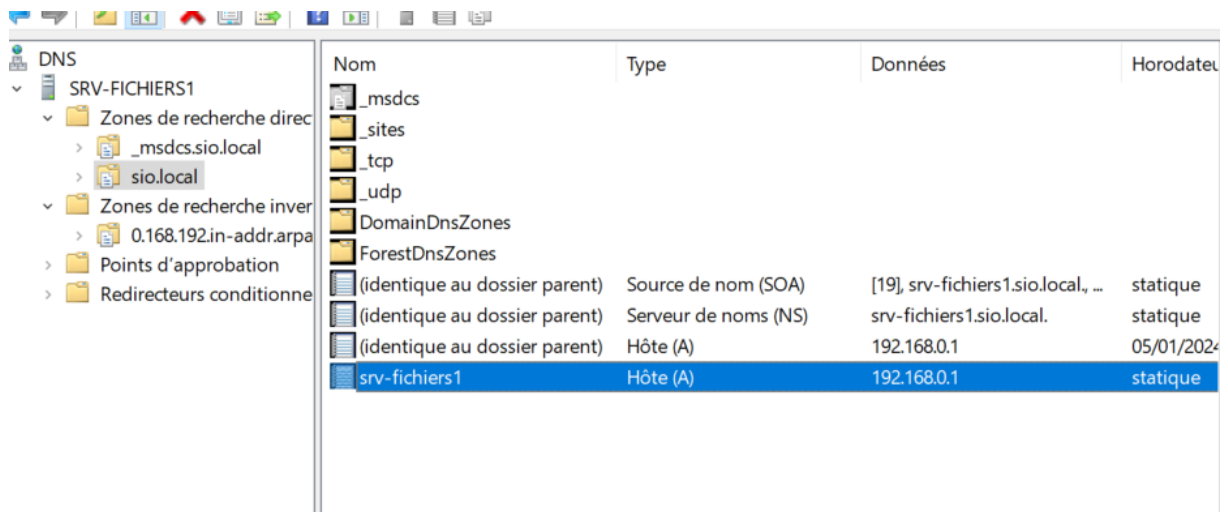
Pour fermer cet Assistant et créer une nouvelle zone, cliquez sur Terminer.

< Précédent

Terminer

Annuler

Puis il faudra aller chercher le fichier texte de notre serveur et double cliquer dessus et cocher la case pour le mettre à jour et faire appliquer.



The screenshot shows the Windows DNS console for the SRV-FICHIERS1 server. The left pane shows the tree structure: SRV-FICHIERS1 > Zones de recherche directe > sio.local. The right pane displays a list of DNS records with the following columns: Nom, Type, Données, and Horodateur.

Nom	Type	Données	Horodateur
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(identique au dossier parent)	Source de nom (SOA)	[19], srv-fichiers1.sio.local, ...	statique
(identique au dossier parent)	Serveur de noms (NS)	srv-fichiers1.sio.local.	statique
(identique au dossier parent)	Hôte (A)	192.168.0.1	05/01/2024
srv-fichiers1	Hôte (A)	192.168.0.1	statique

Propriétés de : srv-fichiers1

Hôte local (A) Sécurité

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

Nom de domaine pleinement qualifié (FQDN) :

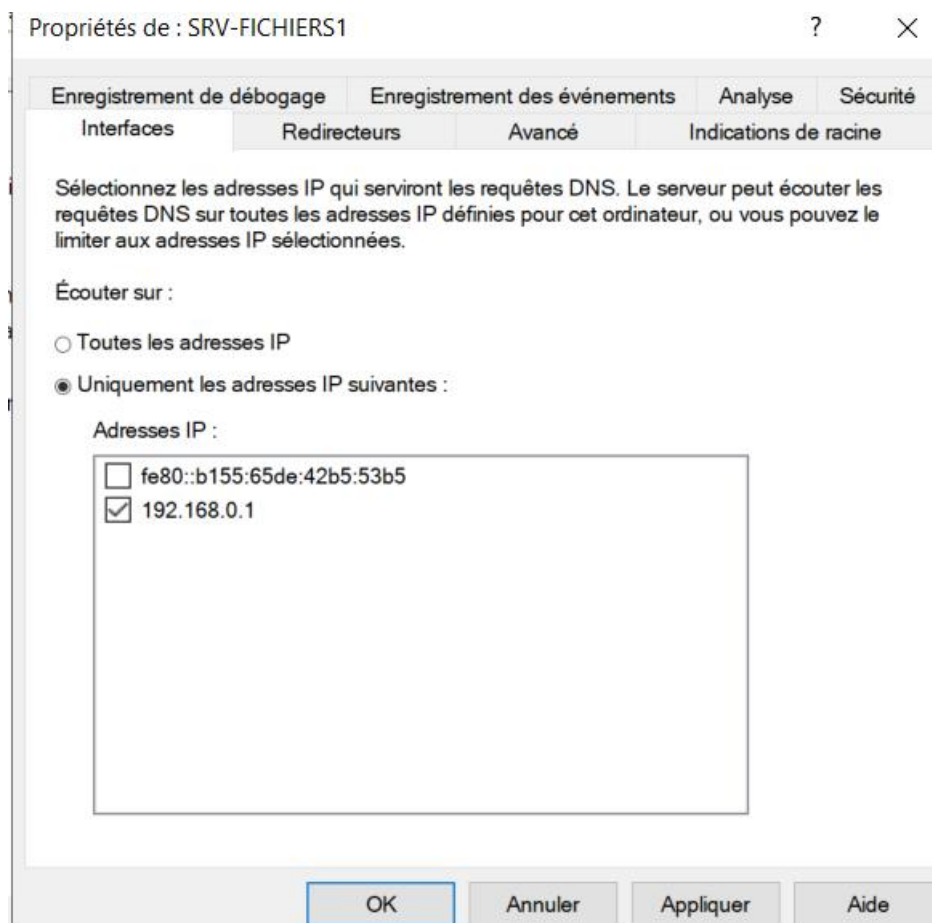
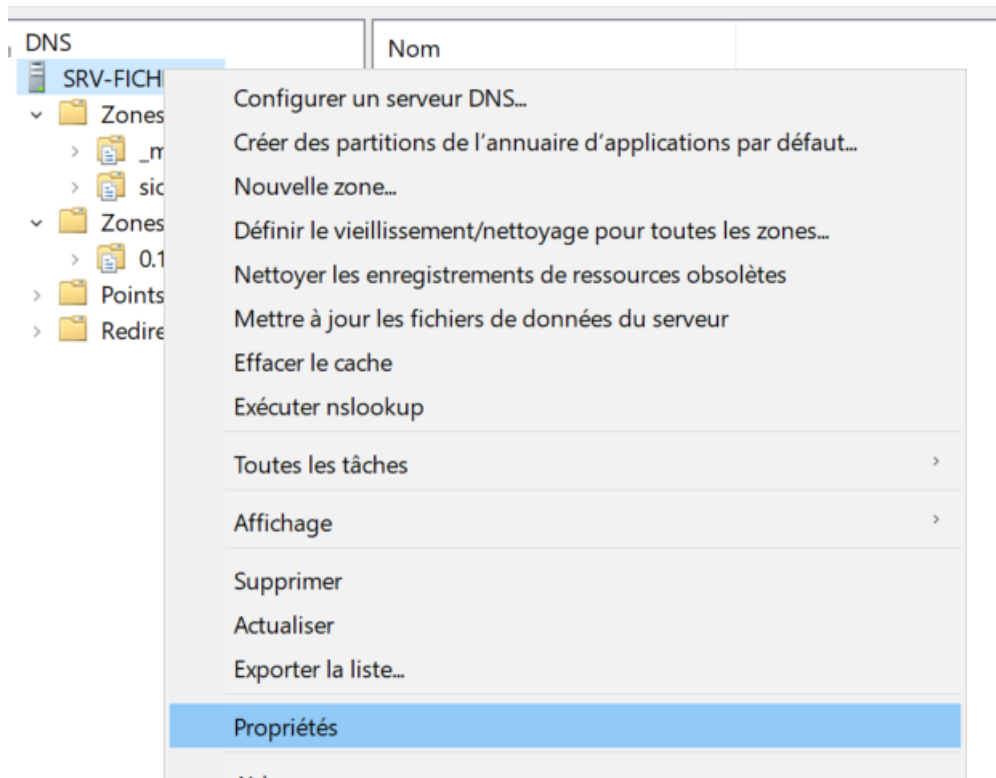
  

Adresse IP :

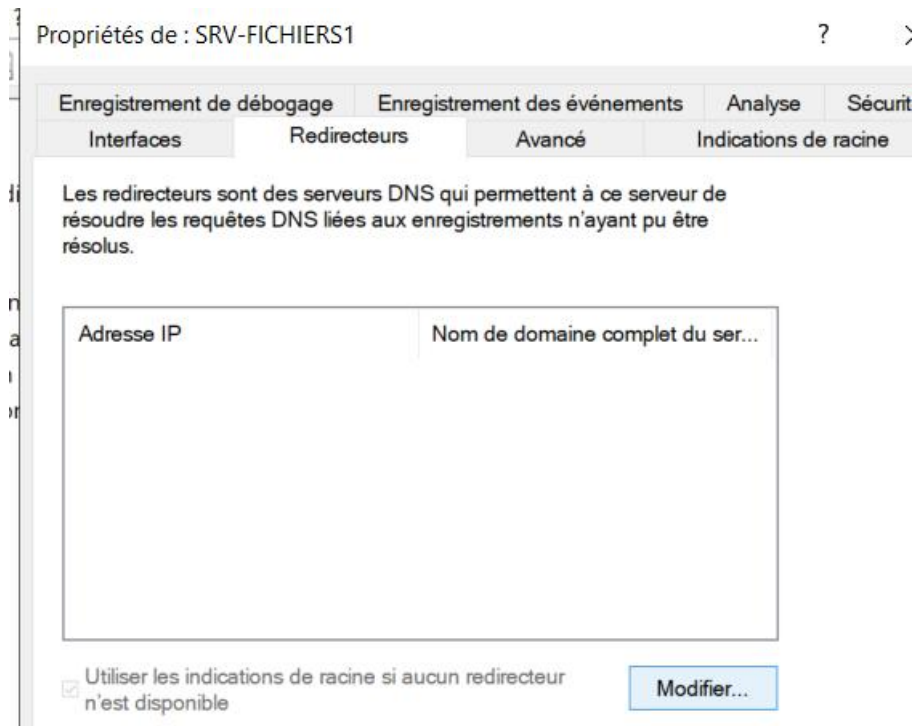
  
 Mettre à jour l'enregistrement de pointeur (PTR) associé

OK Annuler Appliquer

Pour plus de simplicité et de stabilité nous allons également désactiver l'écoute de l'ipv6 sur les propriétés du serveur.

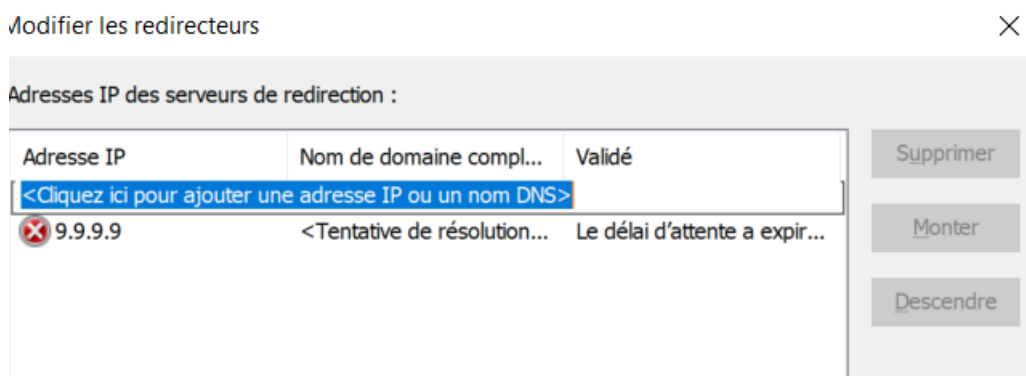


Il faut alors cliquer sur : les adresses IP suivantes et décocher la première qui n'est pas celle que vous avez renseigné, appliquez puis il faut se rendre dans le deuxième onglet Redirecteurs.



En cliquant sur modifier on pourra alors ajouter un serveur DNS au cas où le notre aurait du mal à trouver une réponse celui là pourra prendre en charge la requête.

On choisira ici 9.9.9.9 appliquer puis fermer.



Enregistrement de débogage	Enregistrement des événements	Analyse	Sécurité
Interfaces	Redirecteurs	Avancé	Indications de racine

Les redirecteurs sont des serveurs DNS qui permettent à ce serveur de résoudre les requêtes DNS liées aux enregistrements n'ayant pu être résolus.

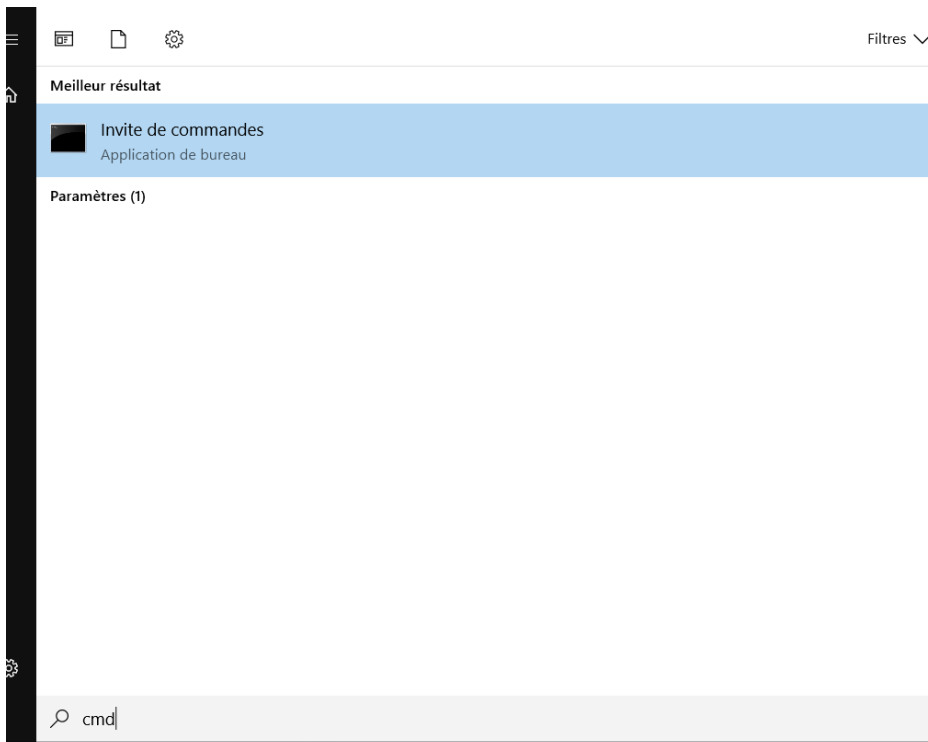
Adresse IP	Nom de domaine complet du ser...
9.9.9.9	<Résolution impossible>

Utiliser les indications de racine si aucun redirecteur n'est disponible [Modifier...](#)

Remarque : si des redirecteurs conditionnels sont définis pour un domaine donné, ils sont utilisés à la place des redirecteurs du serveur. Pour créer ou afficher des redirecteurs conditionnels, accédez au nœud Redirecteurs conditionnels dans l'arborescence de l'étendue.

OK Annuler Appliquer Aide

Enfin on va tester avec un ping vers sio.local dans le cmd pour voir s'il répond.



```
Administrateur : Invite de commandes
Microsoft Windows [version 10.0.17763.2114]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ping sio.local

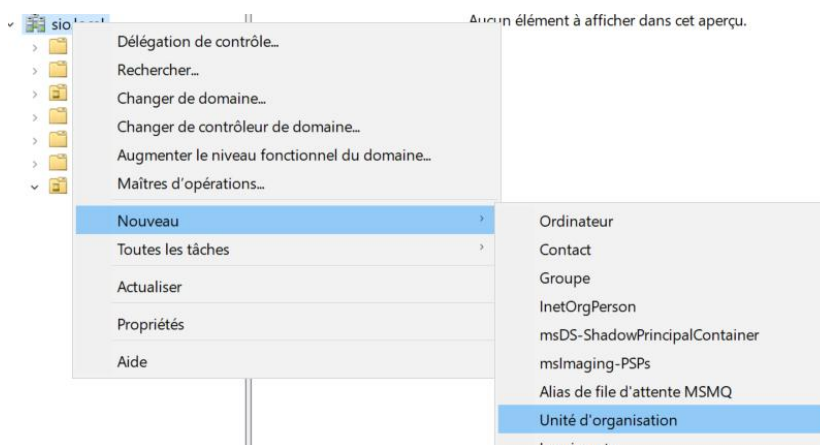
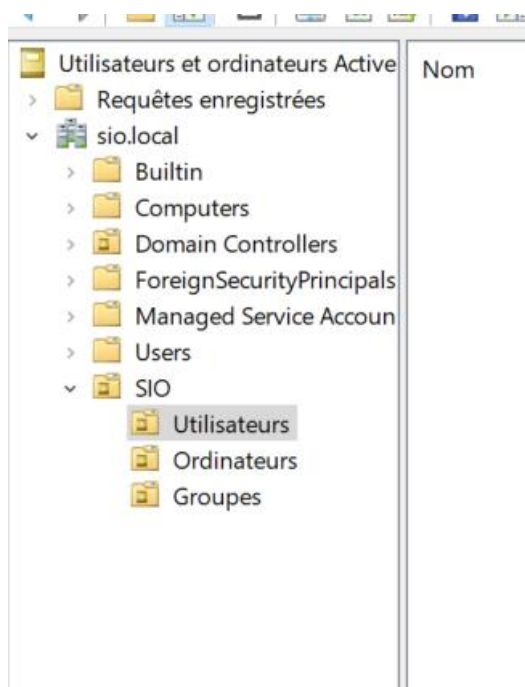
Envoi d'une requête 'ping' sur sio.local [192.168.0.1] avec 32 octets de données :
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

On a bien un retour et du nom et de l'adresse ip y correspondant ce qui veut dire que tout fonctionne correctement.

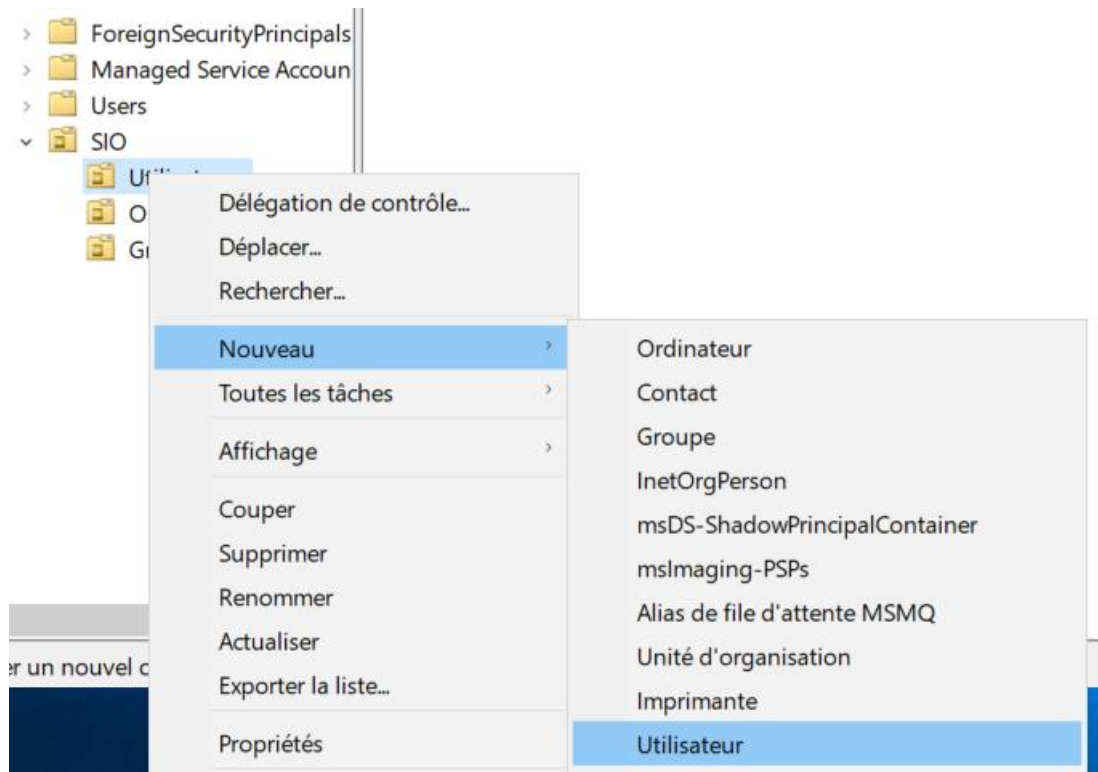
On va maintenant pouvoir lier ceci avec un utilisateur d'un pc lambda.

Pour cela on va d'abord dans l'active directory créer un nouveau répertoire avec des sous dossiers pour mieux s'y repérer





On va créer un utilisateurs




Et on va lui attribuer un nom et un nom d'ouverture de session.

A screenshot of the 'Nouvel objet - Utilisateur' dialog box. The title bar reads 'Nouvel objet - Utilisateur' and 'Créer dans : sio.local/SIO/Utilisateurs'. The dialog contains several input fields: 'Prénom' (First name) with 'user1', 'Initiales' (Initials) (empty), 'Nom' (Last name) (empty), 'Nom complet' (Full name) with 'user1', 'Nom d'ouverture de session de l'utilisateur' (User logon name) with 'user1' and '@sio.local' selected in a dropdown, and 'Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000)' (User logon name (pre-Windows 2000)) with 'SIO\' and 'user1'. At the bottom, there are three buttons: '< Précédent', 'Suivant >', and 'Annuler'.

Puis un mot de passe :

Azerty123\*

Nouvel objet - Utilisateur



Créer dans : sio.local/SIO/Utilisateurs

---

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

Et on valide puis on va créer un groupe pour nos utilisateurs qui nous simplifiera la tâche.

Nouvel objet - Groupe



Créer dans : sio.local/SIO/Groupes

---

Nom du groupe :

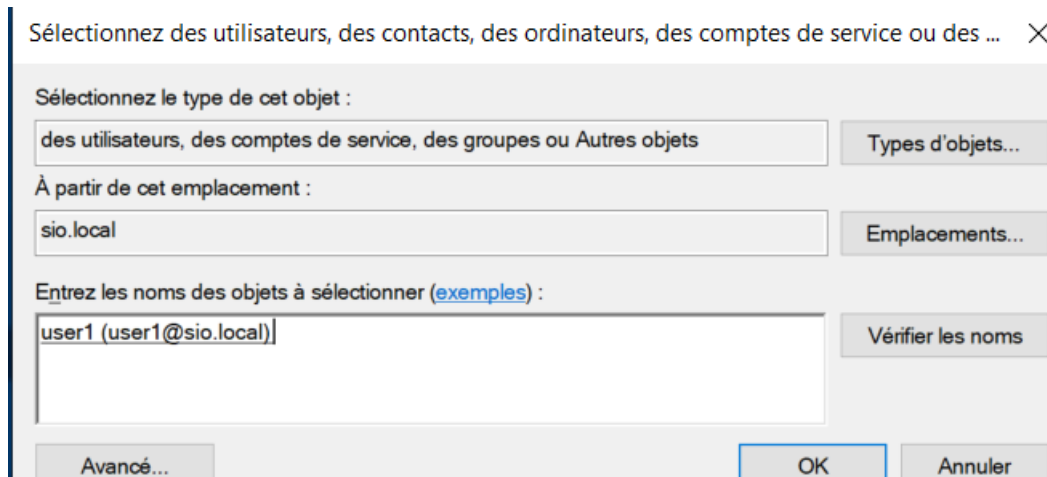
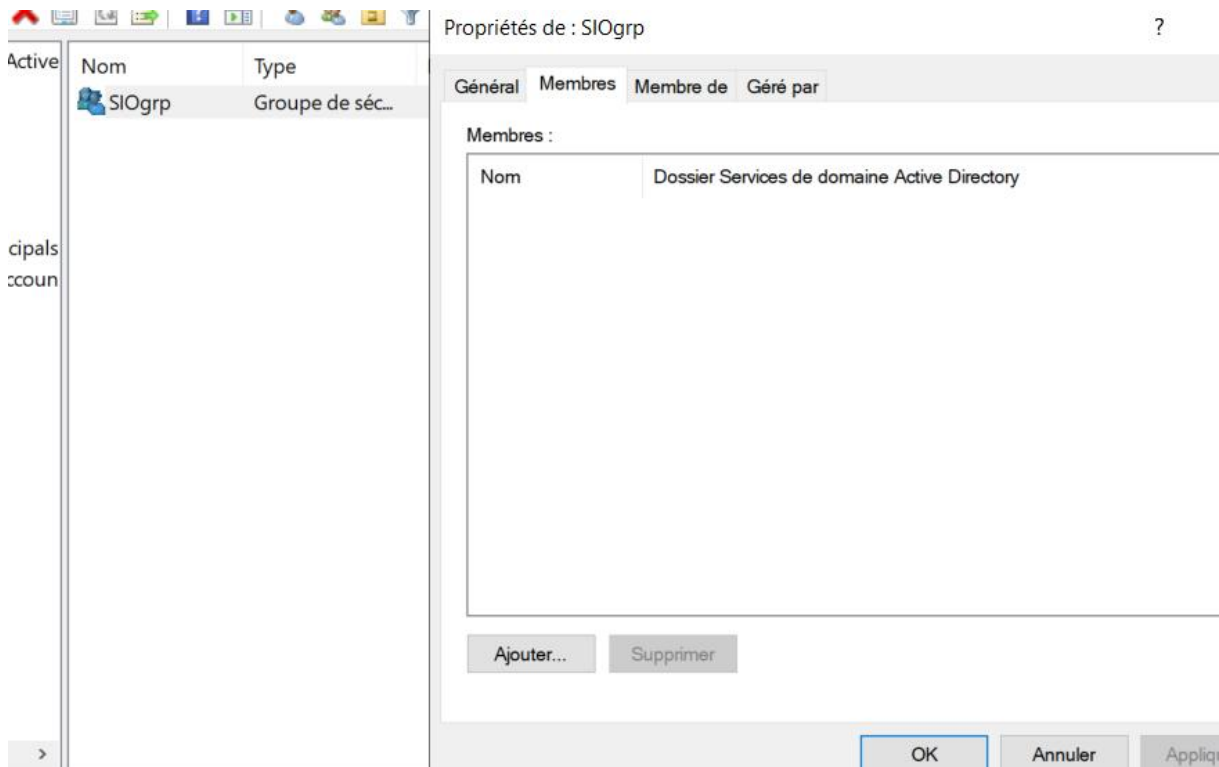
Nom de groupe (antérieur à Windows 2000) :

<p>Étendue du groupe</p> <p><input type="radio"/> Domaine local</p> <p><input checked="" type="radio"/> Globale</p> <p><input type="radio"/> Universelle</p>	<p>Type de groupe</p> <p><input checked="" type="radio"/> Sécurité</p> <p><input type="radio"/> Distribution</p>
--	--

---

OK   Annuler

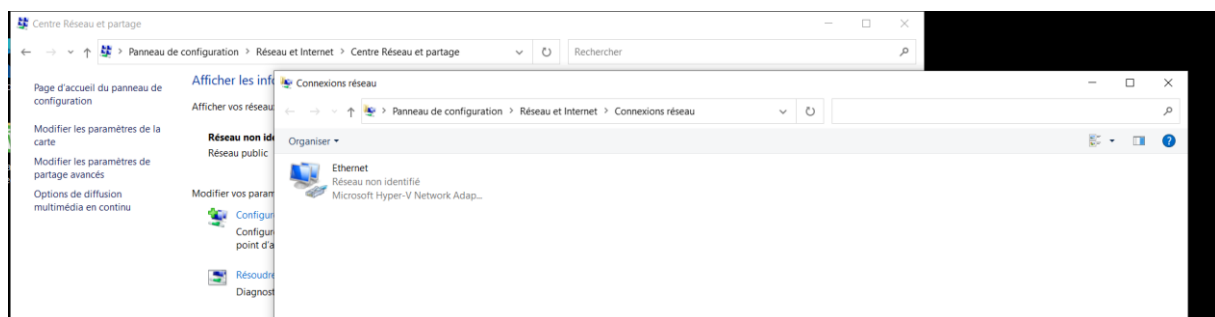
Ensuite en double cliquant sur le groupe on va dans membre y ajouter notre utilisateur



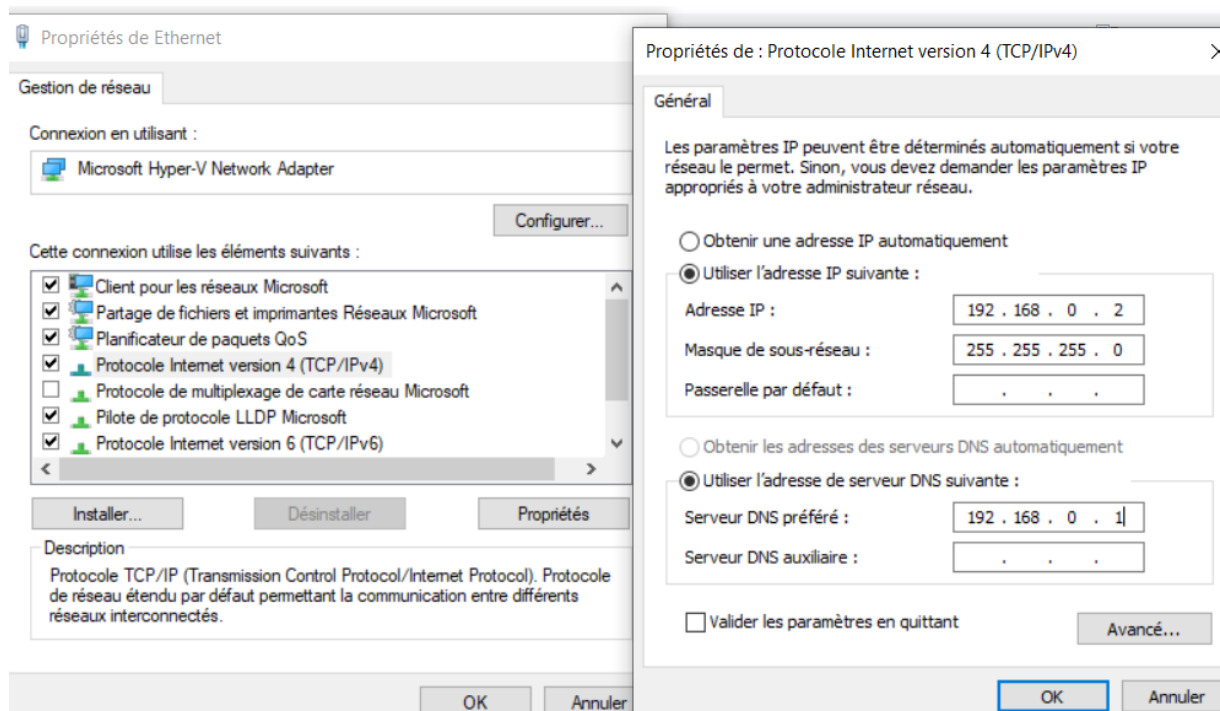
On fait ok on appliquer et notre membre sera ajouté.

Puis rendons nous sur la vm Windows 10 pro (nécessaire dans l'ajout dans un domaine) également installé lors d'un précédent TP.

Il faut alors aller dans le centre réseau et partage puis sur modifier les paramètre de la carte.



Et dans les propriétés puis IPV4 on va renseigner l'adresse ip de notre ad ici dans mon cas 192.168.0.1



Pour reprendre les vérifications :

Avec nos ipconfig on va vérifier que tout est bien paramétré.

```
C:\Users\Mathéo>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::5ca4:aeb:53a8:1a1a%10
    Adresse IPv4. . . . . : 192.168.0.2
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :
```

```
C:\Users\Mathéo>ipconfig /all

Configuration IP de Windows

Nom de l'hôte . . . . . : DESKTOP-NSFULSG
Suffixe DNS principal . . . . . :
Type de noeud . . . . . : Mixte
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non

Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : Microsoft Hyper-V Network Adapter
Adresse physique . . . . . : 00-15-5D-90-09-02
DHCP activé. . . . . : Non
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::5ca4:aeb:53a8:1a1a%10(préfééré)
Adresse IPv4. . . . . : 192.168.0.2(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . :
IAID DHCPv6 . . . . . : 167777629
DUID de client DHCPv6. . . . . : 00-01-00-01-2D-0D-E3-C6-00-15-5D-90-09-02
Serveurs DNS. . . . . : 192.168.0.1
NetBIOS sur Tcpiip. . . . . : Activé
```

Et maintenant un ping pour voir si les deux machines discutent entre elle donc de la vm pro on va ping le serveur de fichier qui est 192.168.0.1

```
C:\Users\Mathéo>ping 192.168.0.1

Envoi d'une requête 'Ping' 192.168.0.1 avec 32 octets de données :
Réponse de 192.168.0.1 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.0.1 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.0.1 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.0.1 : octets=32 temps=1 ms TTL=128

Statistiques Ping pour 192.168.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

On a une réponse donc tout fonctionne correctement.

De même pour le nom de domaine

```
C:\Users\Mathéo>ping sio.local

Envoi d'une requête 'ping' sur sio.local [192.168.0.1] avec 32 octets de données :
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.1 : octets=32 temps=3 ms TTL=128
Réponse de 192.168.0.1 : octets=32 temps=2 ms TTL=128

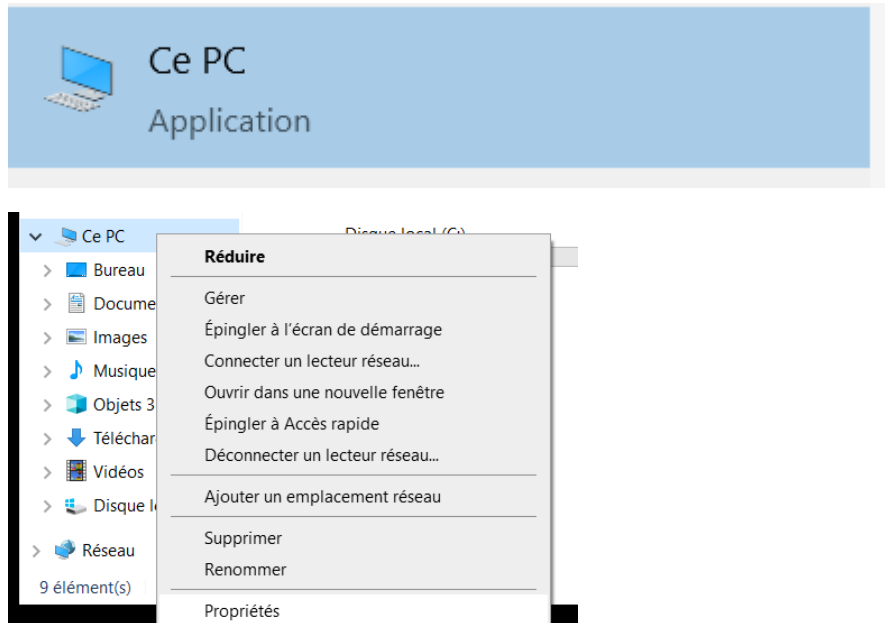
Statistiques Ping pour 192.168.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 3ms, Moyenne = 1ms
```

Et avec nslookup pour vérifier que le serveur dns répond bien correctement.

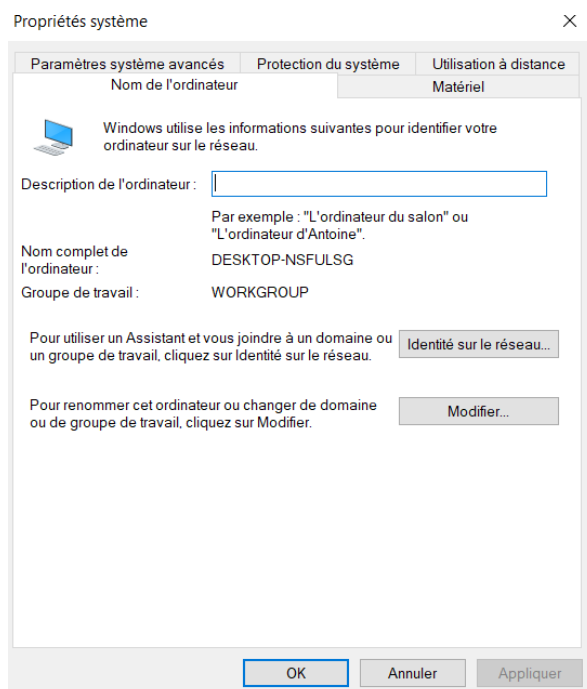
```
C:\Users\Mathéo>nslookup
Serveur par défaut : SRV-FICHIERS1.sio.local
Address: 192.168.0.1
```

On va maintenant pouvoir intégrer le pc au domaine.

Dans ce pc puis propriétés.



Puis sur paramètres avancés du système et dans nom de l'ordinateur.



Paramètres associés

[Paramètres de Bitlocker](#)

[Gestionnaire de périphériques](#)

[Bureau à distance](#)

[Protection du système](#)

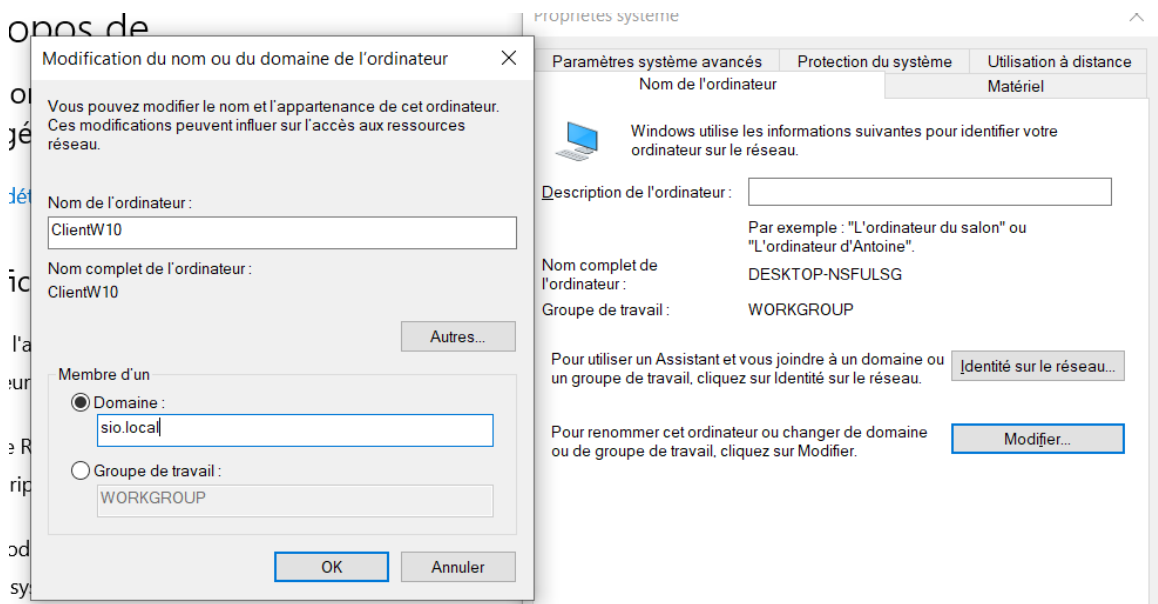
[Paramètres avancés du système](#)

[Renommer ce PC \(avancé\)](#)

 [Obtenir de l'aide](#)

 [Donner des commentaires](#)

Puis dans modifier on va changer le nom du pc pour un nom plus simple donc ClientW10 et on va cocher domaine et rentrer notre nom de domaine.



Puis en validant il nous sera alors demandé de nous authentifier.

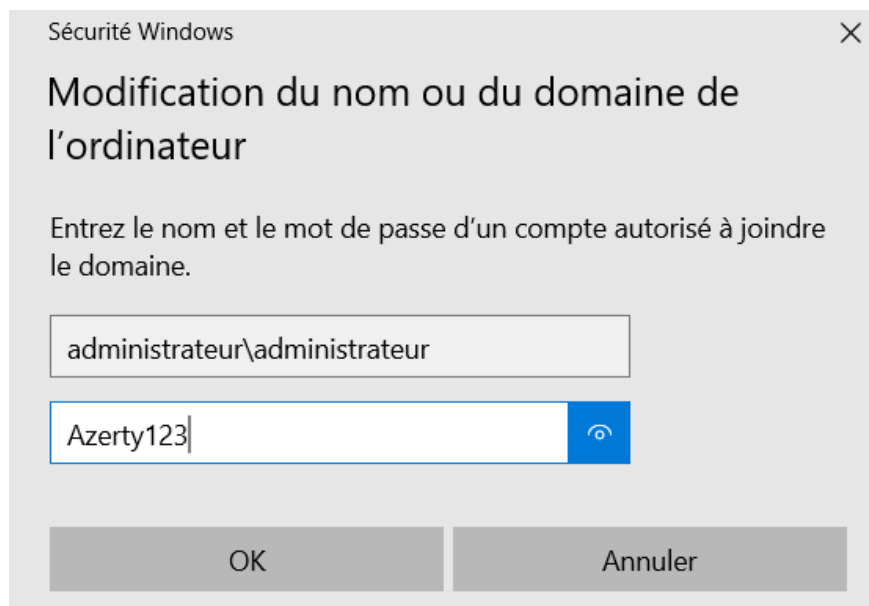
On va donc utiliser le compte admin du serveur de fichier

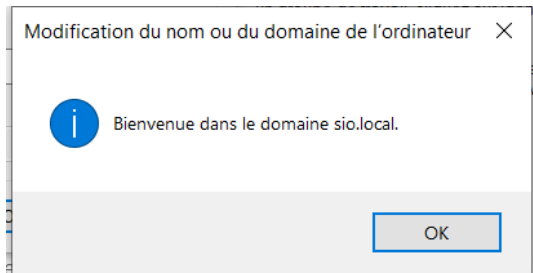
Identifiants :

administrateur

Azerty123

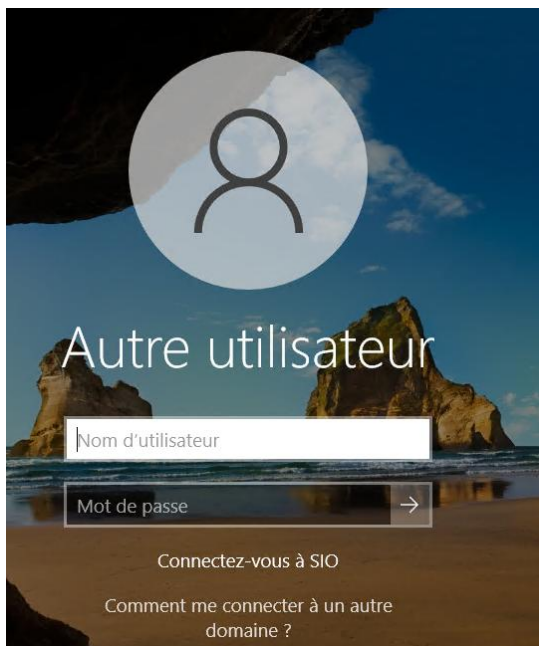
Et au dos d'administrateur on fera \administrateur qui signifie qu'on sera l'administrateur du compte administrateur(ou pc Windows 10 si je l'avais renommé de cette façon).





Une fois cette fenêtre obtenue nous sommes bien dans le domaine il suffira comme le demande le pc de redémarrer et le tour sera joué.

Puis en redémarrant on voit qu'on peut sélectionner un autre utilisateur ne bas à gauche car le pc fait partie du domaine.



On va alors s'y connecter avec notre user1 créer plus tôt

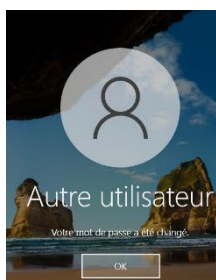
Id :

User1

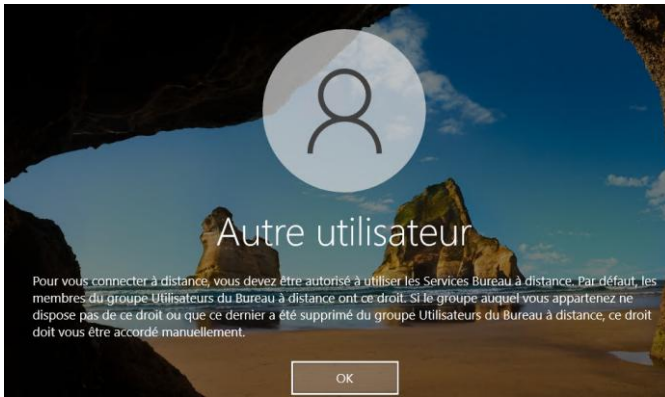
Azerty123\*

Comme la politique de changer le mot de passe avait été faite on peut éventuellement le faire on changera simplement pour Azerty123\$

Et le mot de passe sera changé.



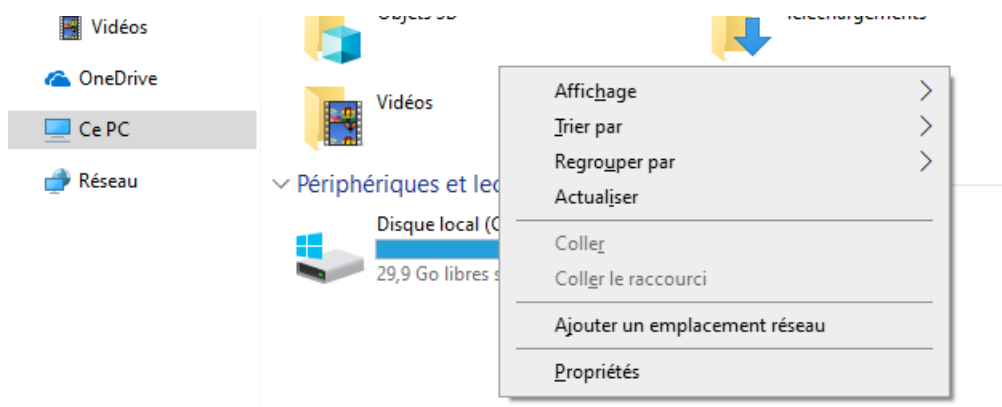




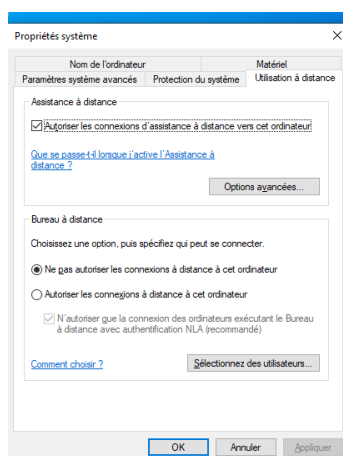
Ensuite un erreur apparaît car sur une vm il faut autoriser le bureau a distance pour s'y connecter car les simples utilisateurs n'y ont normalement pas le droit, problème inexistant avec une vrai machine physique.

Pour régler ce problème il faut aller dans le menu en haut du menu de la vm et faire session étendue puis ça se lance.

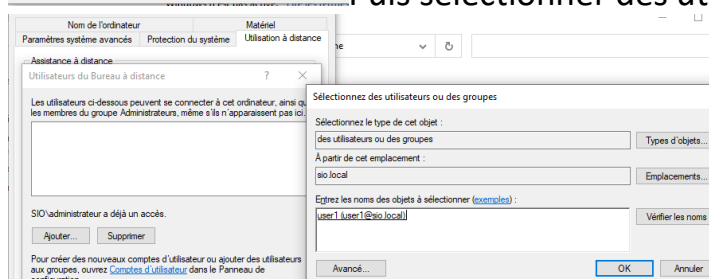
Puis en lançant la session :



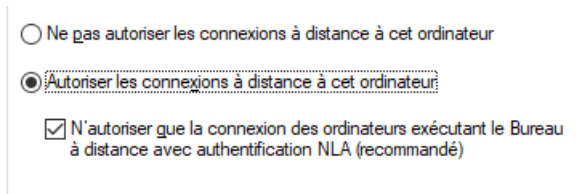
Puis dans paramètres de d'utilisation à distance si on nous demand une authentification on rentrera les infos du compte admin.



Puis sélectionner des utilisateurs et on va ajouter user1



Puis on cochera autoriser les connexion à distance de cet ordinateur.



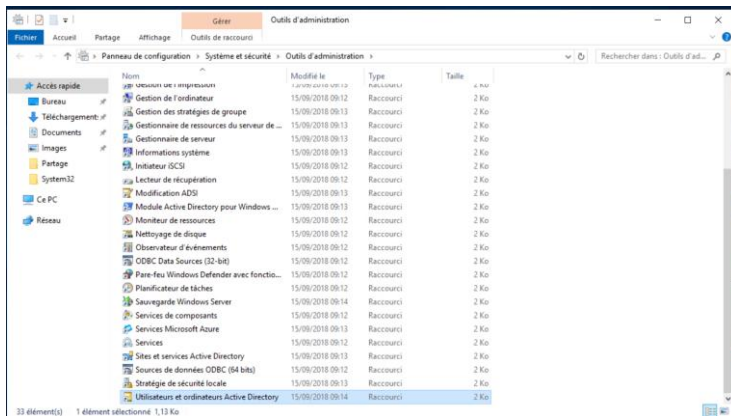
Ensuite on se deconnecte et on essaye de se reconnecter pour bien voir que on peut se connecter à la session du domaine active directory.

On va maintenant passer à la suite avec la partie des droits NTFS et du groupe AD

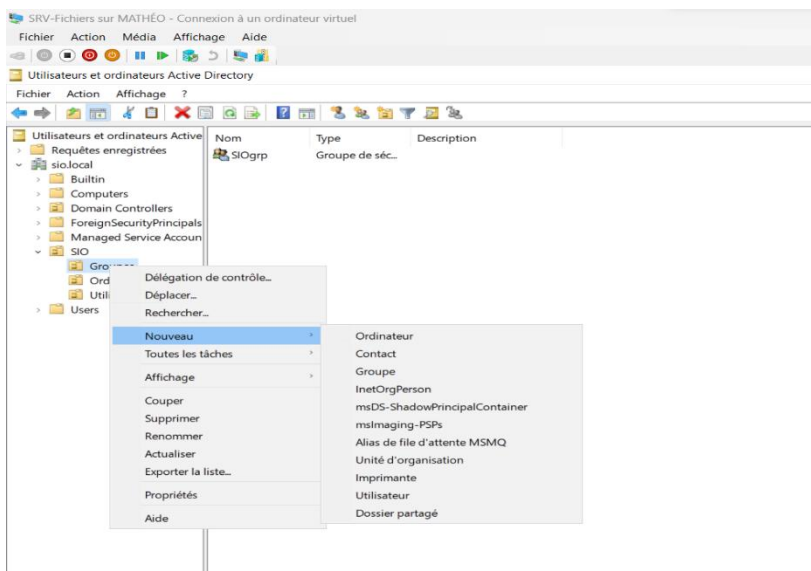
Alors rendons nous sur le serveur AD ou nous ferons le serveur de fichier également même si dans un cas réel il est fortement conseillé de les séparer.

Pour la préparation certaines manipulations ont déjà été réalisés dans un tp antérieur on va donc passer aux nouveautés.

On va alors se rendre dans l'active directory dans la liste des outils d'administration de notre serveur de fichier/AD



Et on va dans les groupes en créer trois nouveaux



Nom	Type	Description
g_compta	Groupe de séc...	
g_direction	Groupe de séc...	
g_informatiq...	Groupe de séc...	
SIOadm	Groupe de séc...	

Et dans le groupe utilisateur on va créer un nouvel utilisateur

Nom	Type	Description
user direction	Utilisateur	

Et on l'ajoute à un groupe

Nom	Type	Description
user direct		
user1		

Noms correspondants :

Nom	Description	Dossier
g_compta		sio.local/SIO/Groupes
g_direction		sio.local/SIO/Groupes

Au groupe direction donc on fera pareil avec un grp informatique et compta on ajoutera chaque utilisateur à son groupe.

Entrez les noms des objets à sélectionner (exemples) :

Propriétés de : user informatique

Environnement Sessions Contrôle à distance F

Général Adresse Compte Profil Téléphones

Membre de :

Nom	Dossier Services de domaine
g_informatique	sio.local/SIO/Groupes

On va maintenant pouvoir créer nos droit sur le fichier partage créer dans un précédant tp.

Disque local (C:) > Ce PC > Disque local (C:) > Partage

Nom	Modifié le	Type	Taille
Partage	15/12/2023 11:46	Dossier de fichiers	

On va entrer dans partage et aller dans les propriétés de compta en premier lien puis dans sécurité puis avancé en bas à droite.

Propriétés de : Compta

Nom de l'objet : C:\Partage\Compta

Noms de groupes ou d'utilisateurs :

- CREATEUR PROPRIETAIRE
- Utilisateurs authentifiés
- Système
- Administrateurs (SIO\Administrateurs)

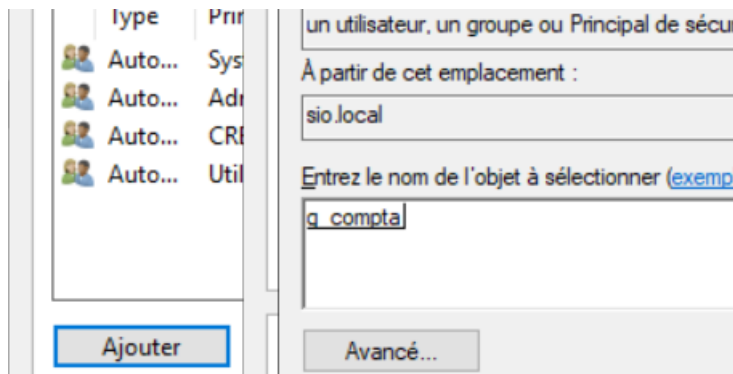
Pour modifier les autorisations, cliquez sur Modifier.

Autorisations pour CREATEUR PROPRIETAIRE

	Autoriser	Refuser
Contrôle total	<input type="checkbox"/>	<input type="checkbox"/>
Modification	<input type="checkbox"/>	<input type="checkbox"/>
Lecture et exécution	<input type="checkbox"/>	<input type="checkbox"/>
Affichage du contenu du dossier	<input type="checkbox"/>	<input type="checkbox"/>
Lecture	<input type="checkbox"/>	<input type="checkbox"/>
Ecriture	<input type="checkbox"/>	<input type="checkbox"/>
Autorisations spéciales	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Pour les autorisations spéciales et les paramètres avancés, cliquez sur Avancé.

Et sur ajouter on va rajouter le groupe compta



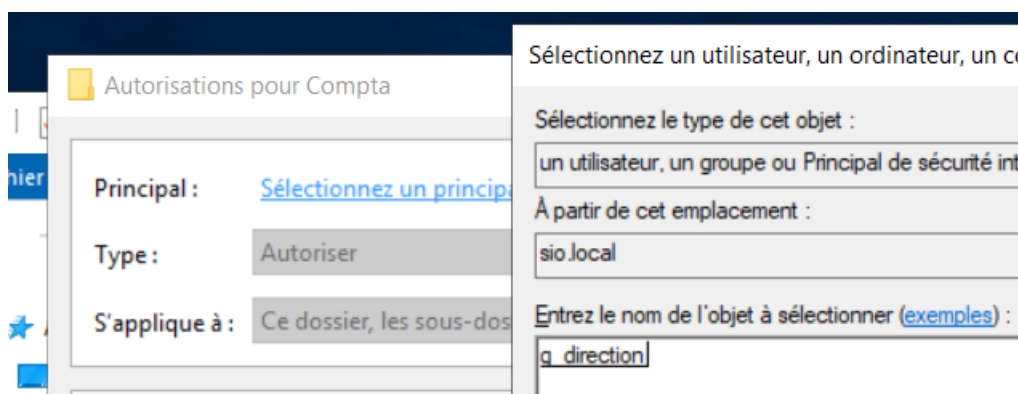
Pour les droits on laissera tout par défaut et on cochera juste la case de modifications pour qu'ils puissent modifier le contenu puis appliquer et fermer.

Autorisations avancées :

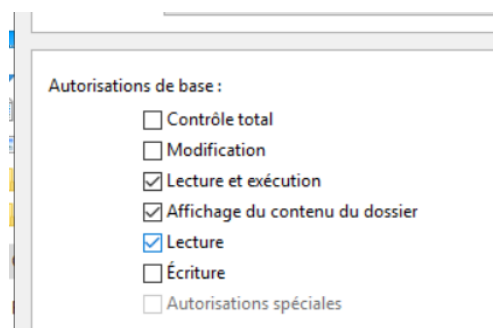
- |   |  |
|---|--|
| <input type="checkbox"/> Contrôle total                                     | <input checked="" type="checkbox"/> Attributs d'écriture         |
| <input checked="" type="checkbox"/> Parcours du dossier/exécuter le fichier | <input checked="" type="checkbox"/> Écriture d'attributs étendus |
| <input checked="" type="checkbox"/> Liste du dossier/lecture de données     | <input type="checkbox"/> Suppression de sous-dossier et fichier  |
| <input checked="" type="checkbox"/> Attributs de lecture                    | <input checked="" type="checkbox"/> Suppression                  |
| <input checked="" type="checkbox"/> Lecture des attributs étendus           | <input checked="" type="checkbox"/> Autorisations de lecture     |
| <input checked="" type="checkbox"/> Création de fichier/écriture de données | <input type="checkbox"/> Modifier les autorisations              |
| <input checked="" type="checkbox"/> Création de dossier/ajout de données    | <input type="checkbox"/> Appropriation                           |

Ensuite pareil pour direction et informatique de la même manière

Maintenant autre exemple on va faire en sorte que direction puisse uniquement lire le dossier compta. Pour cela on va aller dans sécurité avancé de compta à nouveau.

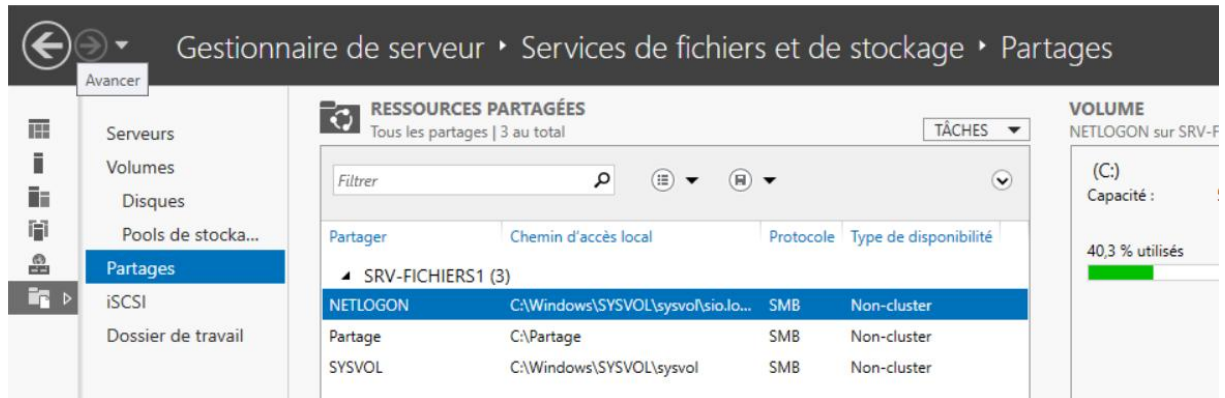


On va simplement y ajouter direction et laisser les droits par défaut c'est-à-dire les droits de lecture seul



Maintenant si on souhaite que chacun ne voit que son fichier et pas celui des autres groupes on va dans le gestionnaire de serveur.

Dans service de fichier et stockage.

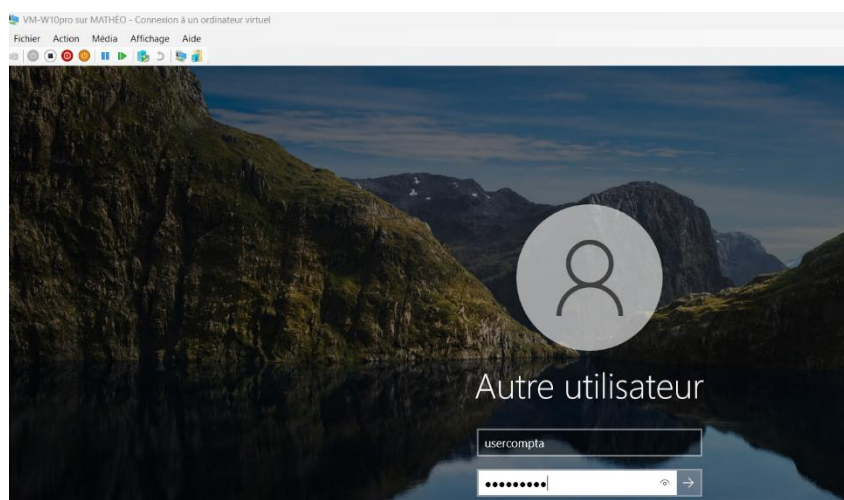


Et dans partage à gauche puis sur le dossier partage on va faire propriété puis paramètre.

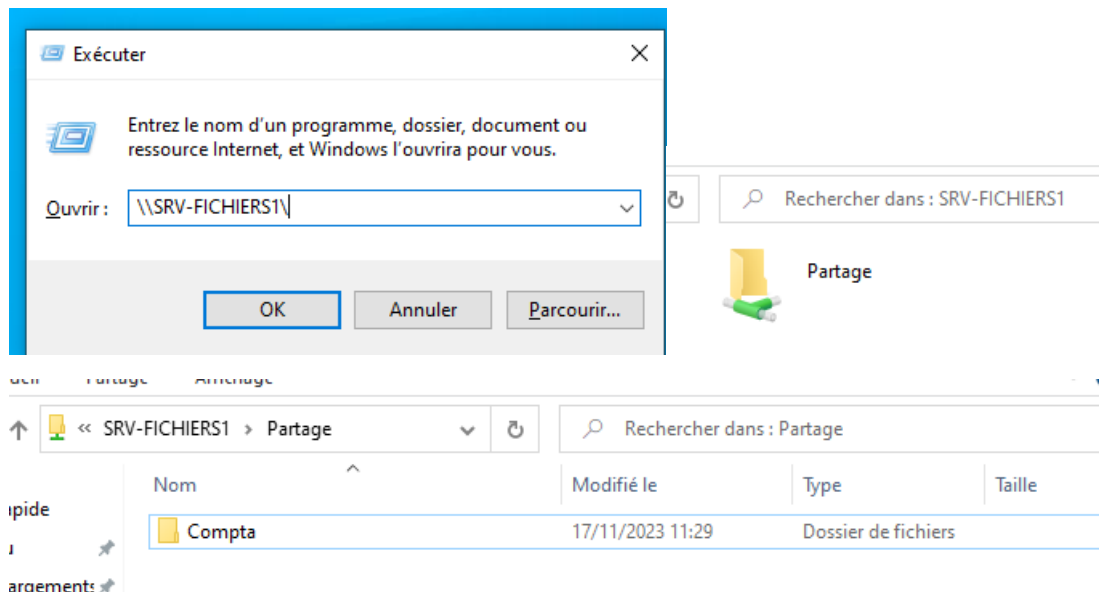


Et on active la première option qui est l'énumération basée sur l'accès. Et donc maintenant chacun ne verra que les dossier accessibles à leur groupes.

On va donc pour tester retourner sur la vm W10pro qui est client pour se connecter avec compta et vérifier les droits d'accès.



Et avec par exemple Windows r on va rechercher le nom du serveur ici : SRV-FICHIERS1 et faire entrer pour avoir accès au repertoire.



Et dans partage on a bien nos deux dossiers visible car informatique ne l'est pas par compta et les droits associés sont bien respecté car on ne peut pas créer de fichier dans compta avec un membre de direction par exemple

**Point d'attention il faut que dans tous les sous dossiers de partage utilisateur du domaines et utilisateurs authentifiés ne soient pas présent.**

Conclusion :

Voilà qui conclu ce tp ou nous avons configuré l'AD avec des groupes et utilisateurs et ses différentes fonctionnalités ainsi que le serveur DNS pour lier les ip à des noms et configurer ces ip pour que les machines discutent entre elles correctement nous avons aussi réalisé des groupes de partage pour les dossiers et les droits NTFS pour que chacun ait les accès à son dossier uniquement ou en partie réduite et pour réaliser tout ça nous avons ajouté les machines dans le domaine.