



# Installation, (sur Windows Server 2019)

## De fonctionnalités de :

- Active Directory
- DNS
- DHCP
- Stratégie de groupe
- Active directory secondaire (bonus)

### Qu'est-ce que Active directory ? DNS ? DHCP ?

En informatique, **Active Directory (AD)**, est un système serveur centralisé, le cœur de Windows Server, qui repose sur les concepts de domaine (notamment un domaine Windows Server) et d'annuaire, c'est-à-dire un ensemble de services réseau, mieux connu sous le nom de "directory service", géré par un contrôleur de domaine et adopté par les systèmes d'exploitation Microsoft à partir de Windows Server 2000. Il définit la manière dont toutes les ressources réseau sont attribuées aux utilisateurs à travers les concepts de : comptes d'utilisateurs, comptes d'ordinateurs, dossiers partagés, imprimantes réseau, etc. ... selon l'attribution par l'administrateur système de la stratégie de groupe "Group Policy".

Active Directory est le cadre de référence dans le monde de la technologie informatique pour gérer un domaine. C'est le nom utilisé par Microsoft pour désigner sa mise en œuvre de la sécurité dans un réseau distribué d'ordinateurs. Dans Active Directory, LDAP est utilisé comme base de données qui stocke de manière centralisée toutes les informations d'un domaine de réseau, relatives à l'authentification et à l'accès aux services, avec l'avantage de garder toutes ces informations synchronisées entre les différents serveurs d'authentification pour l'accès au réseau.

Le serveur DNS (Domain Name System), qu'on peut traduire en « système de noms de domaine », est complémentaire de l'utilisation d'AD. En effet est le service informatique distribué utilisé pour traduire les noms de domaine Internet en adresse IP ou autres enregistrements.

Le DHCP, (*Dynamic Host Configuration Protocol*) est un protocole d'application (auxiliaire) qui permet aux appareils ou terminaux d'un certain réseau local de recevoir automatiquement, à chaque demande d'accès, à partir d'un réseau IP, la configuration IP nécessaire pour établir une connexion et fonctionner sur un protocole de réseau Internet plus large, c'est-à-dire interagir avec tous les autres sous-réseaux en échangeant des données, à condition qu'ils soient également intégrés de la même manière avec le protocole IP.

Si nous avons une connexion réseau fixe à la maison, puis un routeur, nous l'utilisons tous les jours pour nous connecter à Internet. Le serveur DHCP est en fait intégré au router, et nous permet d'utiliser une adresse IP pour se connecter à Internet.

### Pourquoi avons-nous besoin de tout cela ?

La fonctionnalité la plus importante d'AD est certainement la centralisation, l'identification et l'authentification d'un réseau de postes Windows. Cela nous permet potentiellement d'avoir un contrôle pratiquement complet sur notre flotte de PC, avec des possibilités de personnalisation infinies. En cela, nous allons configurer un serveur capable de partager des fichiers et des dossiers avec le réseau interne, avec la possibilité de créer des utilisateurs et des groupes de personnes. Il sera également indiqué, comment créer un serveur DHCP et comment créer des stratégies de groupe.



[Retour au  
Sommaire](#)

# SOMMAIRE

- 1) Conseils de pré-installation
- 2) Installation Active directory (AD DS), Server DNS, Server DHCP
- 3) Configuration du contrôleur de domaine
- 4) Configuration du DNS
- 5) Création d'un utilisateur sur le contrôleur de domaine
- 6) Configurer la machine « client » sur le domaine précédemment défini
- 7) Configuration DHCP
- 8) Mettre en place de stratégie de groupe
- 9) Active directory secondaire (bonus)
- 10) Implémenter une console MMC (partie extra)
- 11) Conclusion

Dans les pages suivantes, la procédure étape par étape pour configurer les fonctions décrites ci-dessus sera expliquée avec une explication d'accompagnement :

Dans ce tutoriel, nous utiliserons deux machines virtuelles :

- Une machine virtuelle agira comme un serveur (Win Server 2019)
- Une autre machine agira en tant que « client PC » (Win 10 vers.20H2)

Il sera possible de récupérer toutes les images en haute résolution [en cliquant ici](#) ou s'il s'agit d'une version imprimée, au lien suivant : <https://drive.google.com/drive/u/5/folders/19jDoq29RcYz5FWwdADRSE42P4Jn6dyu6>

Raccourci	Explication
IP	Internet Protocol
Subnet Mask	Masque de sous-réseau
MAC Address	Media access control address
DNS	Domain Name System
AD DS	Services de domaine Active Directory
GPO/GP	Stratégie de groupe (Group Policy Object)
PC	Personal computer (ordinateur)

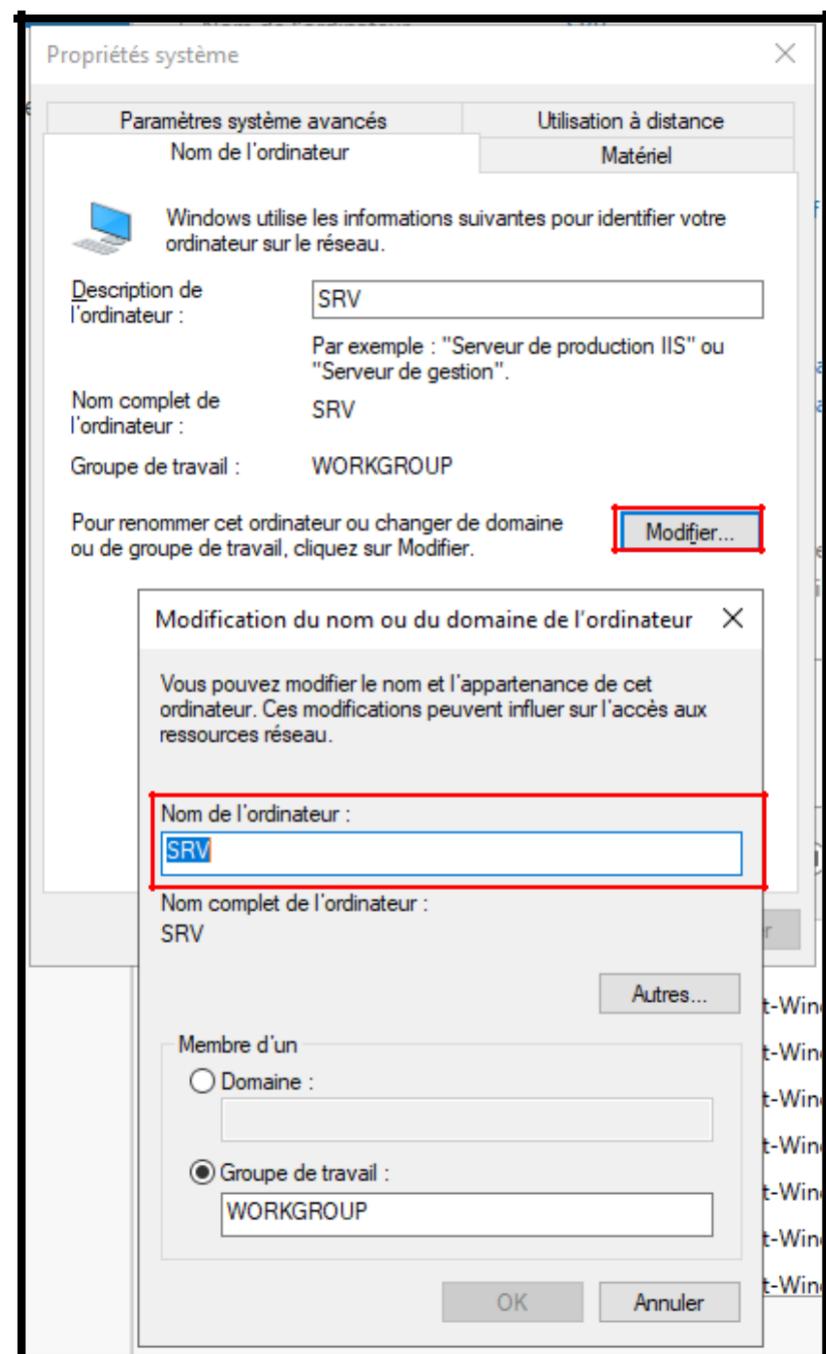
## Conseils généraux avant de commencer. Conseils de pré-installation

Tout d'abord, pour des raisons évidentes et aussi pour des raisons de commodité, nous avons défini un nom personnalisé pour le serveur, dans ce cas je l'ai appelé trivialement : **SRV**

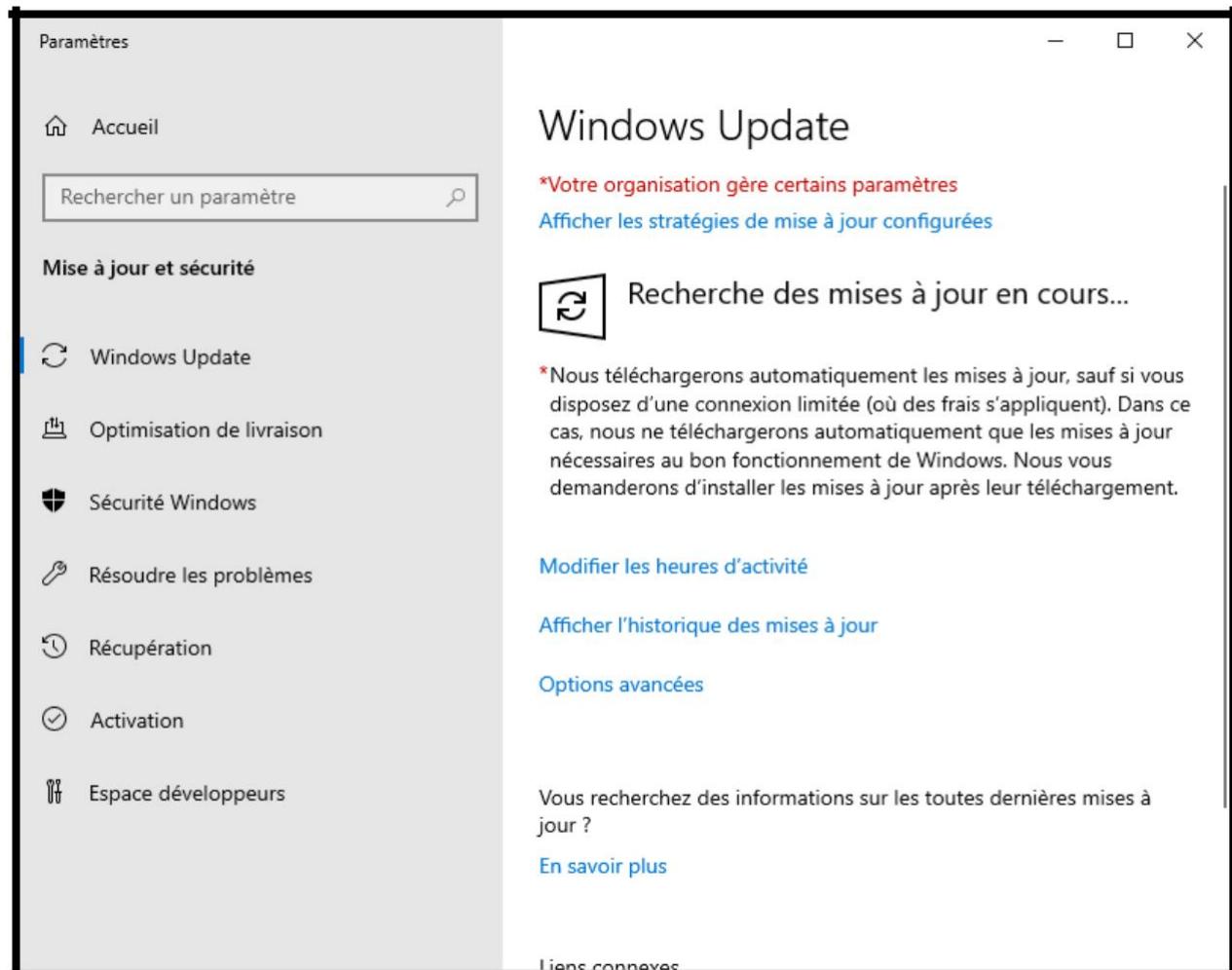
Il est fortement recommandé, pour des raisons évidentes de commodité, de toujours saisir un suffixe pour indiquer si le serveur est virtuel ou physique, ainsi que d'autres détails qui peuvent être utiles pour une identification facile du serveur.

Après avoir changé le nom de la machine, il est fortement recommandé de redémarrer le serveur, pour des raisons évidentes. (Un redémarrage est nécessaire pour que le nom soit appliqué.)

Pour aller dans cette fenêtre il suffit d'aller sur ce chemin : "**Panneau de configuration \ Système et sécurité \ Système**" puis cliquer sur : "**Modifier les paramètres**". Cliquez ensuite sur "**Modifier...**"



Il est toujours recommandé de mettre à jour tous les systèmes d'exploitation, de toujours disposer des derniers « **patch de sécurité** ». Ceci, pour éviter les problèmes et évidemment pour des raisons évidentes de sécurité.

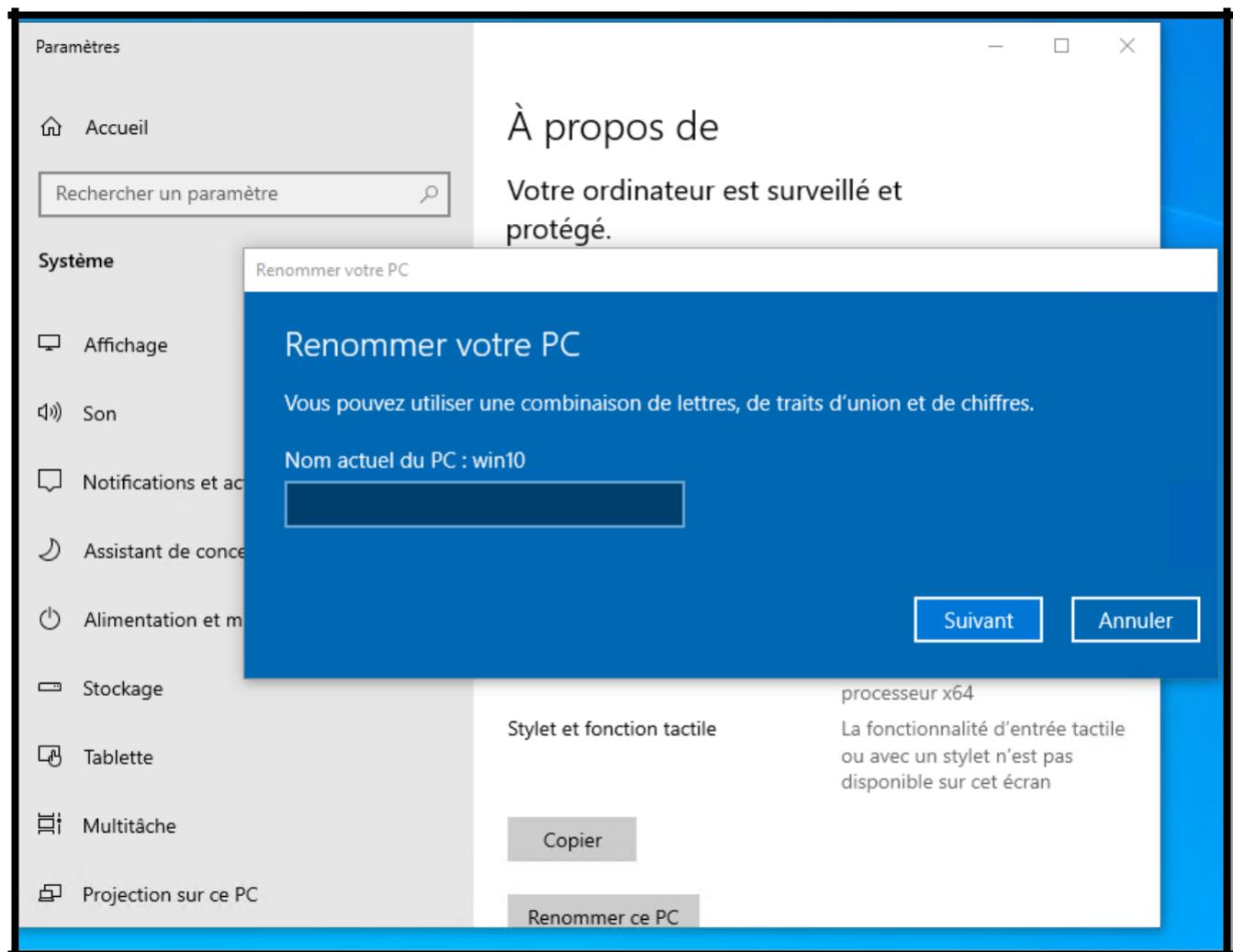


Il est également possible de mettre à jour le système d'exploitation en cliquant avec le bouton gauche de la souris, sur le menu avec l'icône Windows en bas à gauche, puis cliquez sur "**Paramètres**" (icône d'engrenage), puis "**Mise à jour et sécurité**" puis cliquez sur "**Recherche des mises à jour**"

Nous ferons la même chose pour la machine avec Windows10, (dans ce cas, il s'agit d'une machine « cliente »). Alors nous mettrons à jour le système d'exploitation et changerons le nom « par défaut » du PC.

Après avoir changé le nom de l'ordinateur, il est fortement recommandé de redémarrer le pc, pour des raisons évidentes. (Un redémarrage est nécessaire pour que le nom soit appliqué.)

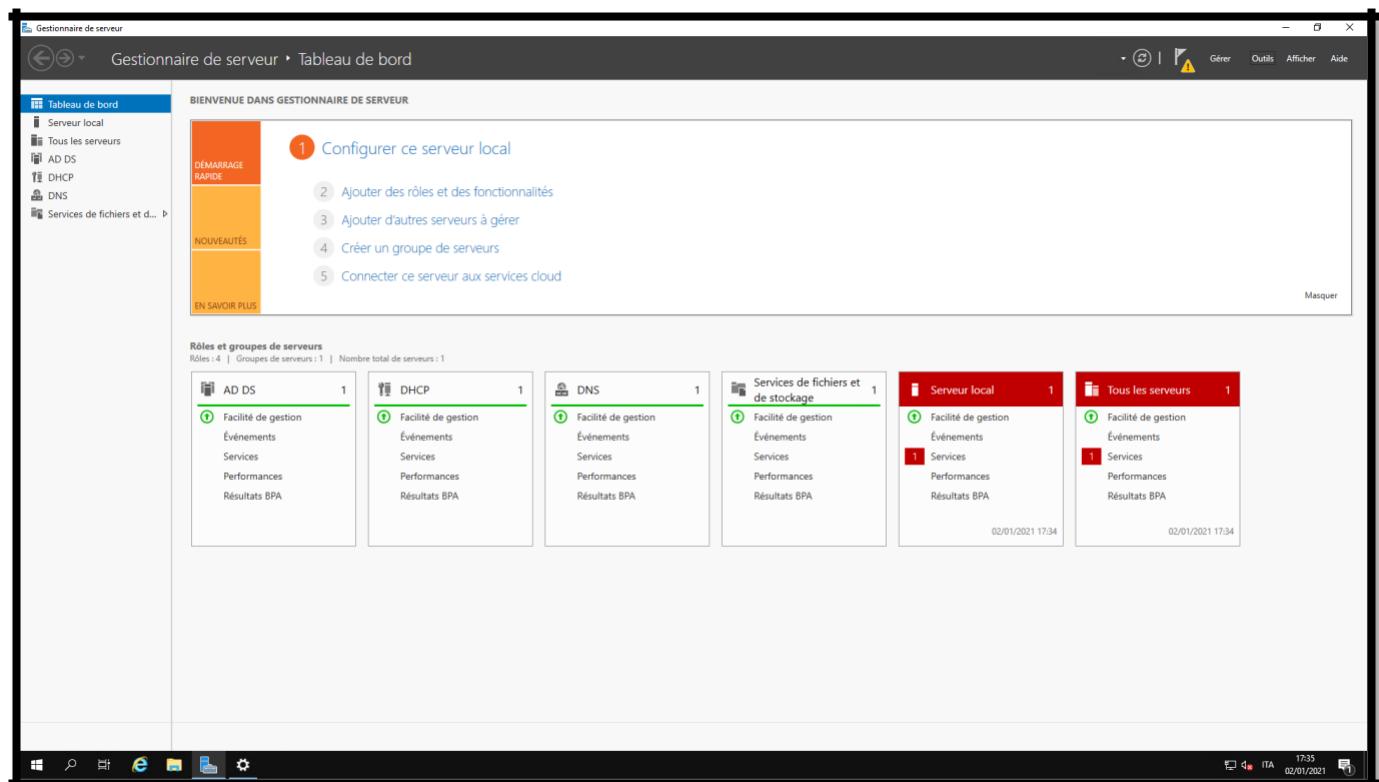
Le groupe de travail par défaut de *Microsoft* lors de l'installation d'un système d'exploitation est toujours "**WORKGROUP**"



De là, nous pouvons voir la nouvelle interface graphique (GUI Graphics User Interface) du gestionnaire de serveur.

Est une console qui sera souvent utilisée pour gérer le serveur  
(À partir de Windows Server 2008, cette console a été implémentée).

Il est utilisé pour gérer le serveur local et potentiellement tous les serveurs du réseau également

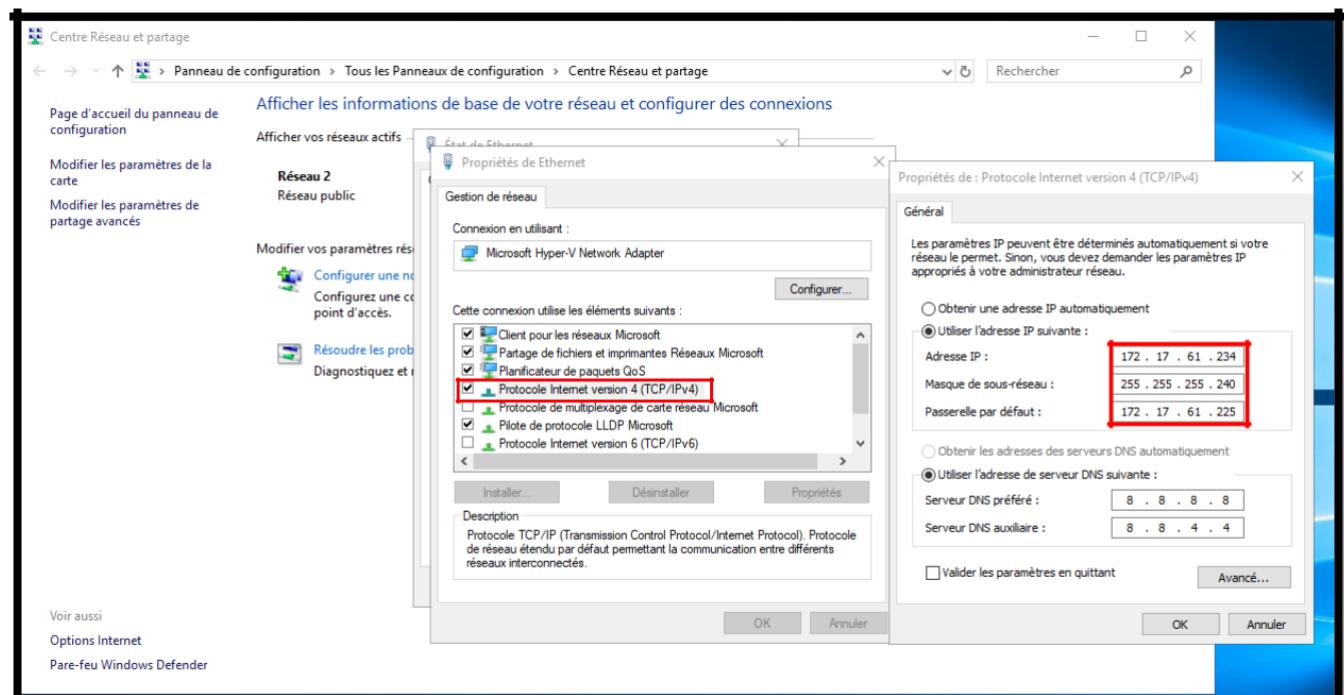


## Installation Active Directory – Server DNS – Server DHCP

À Partir de là, nous définirons une adresse IP fixe sur notre serveur (comme cela devrait être pour tous les serveurs), sinon dans le serveur DNS, il se peut qu'il ne puisse pas résoudre le nom, si l'IP change. puis ils définissent une adresse IP statique dans le sous-réseau, dans notre cas, nous définissons les paramètres affichés dans la capture d'écran.

Dans ce cas, nous allons tout configurer, via le protocole ipv4, mais la procédure est absolument réalisable même en ipv6.

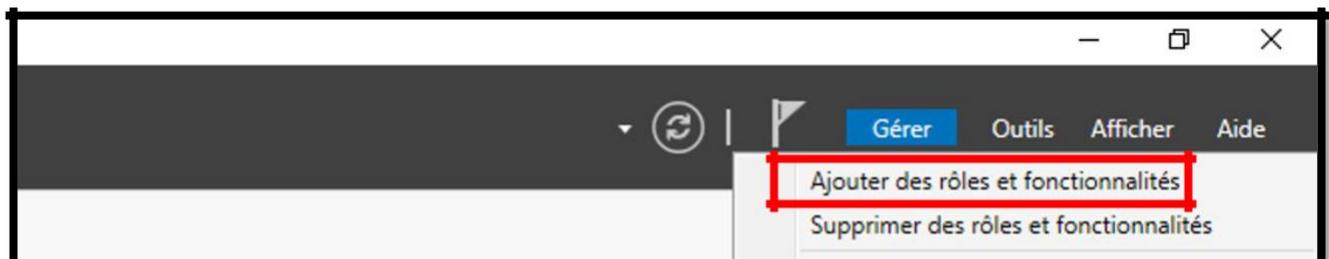
Dans ce cas par exemple, je suis allé définir une IP statique **172.17.61.234**, avec un masque de sous-réseau (MAC Address) **255.255.255.240**, une passerelle : **172.17.61.225** et le DNS classique de Google (**8.8.8.8** et **8.8.4.4**).



[Retour au Sommaire](#)

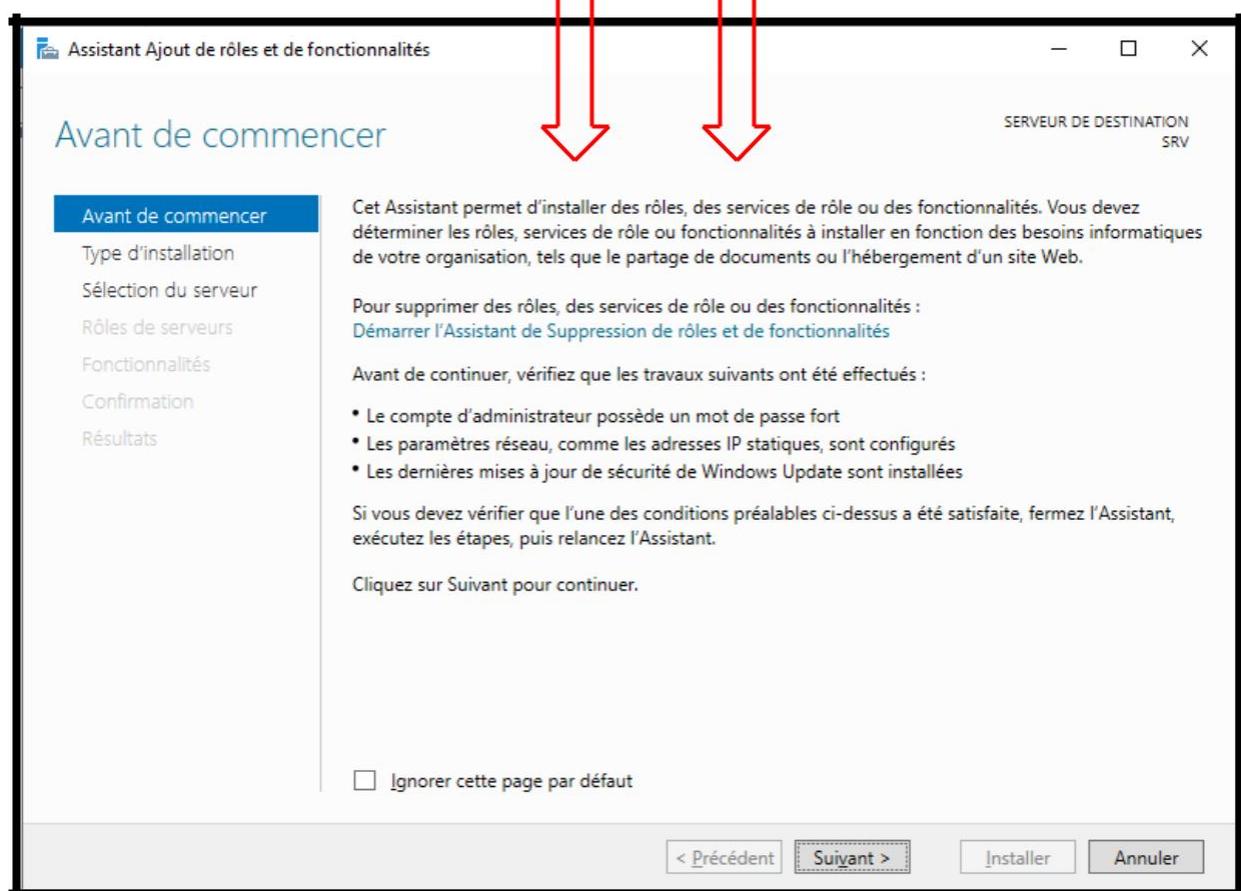
Une fois la carte réseau configurée, ajoutons les rôles et fonctionnalités, donc les services que nous souhaitons installer, dans ce cas nous installerons les fonctionnalités listées :

- Active Directory
- Serveur DNS
- DHCP



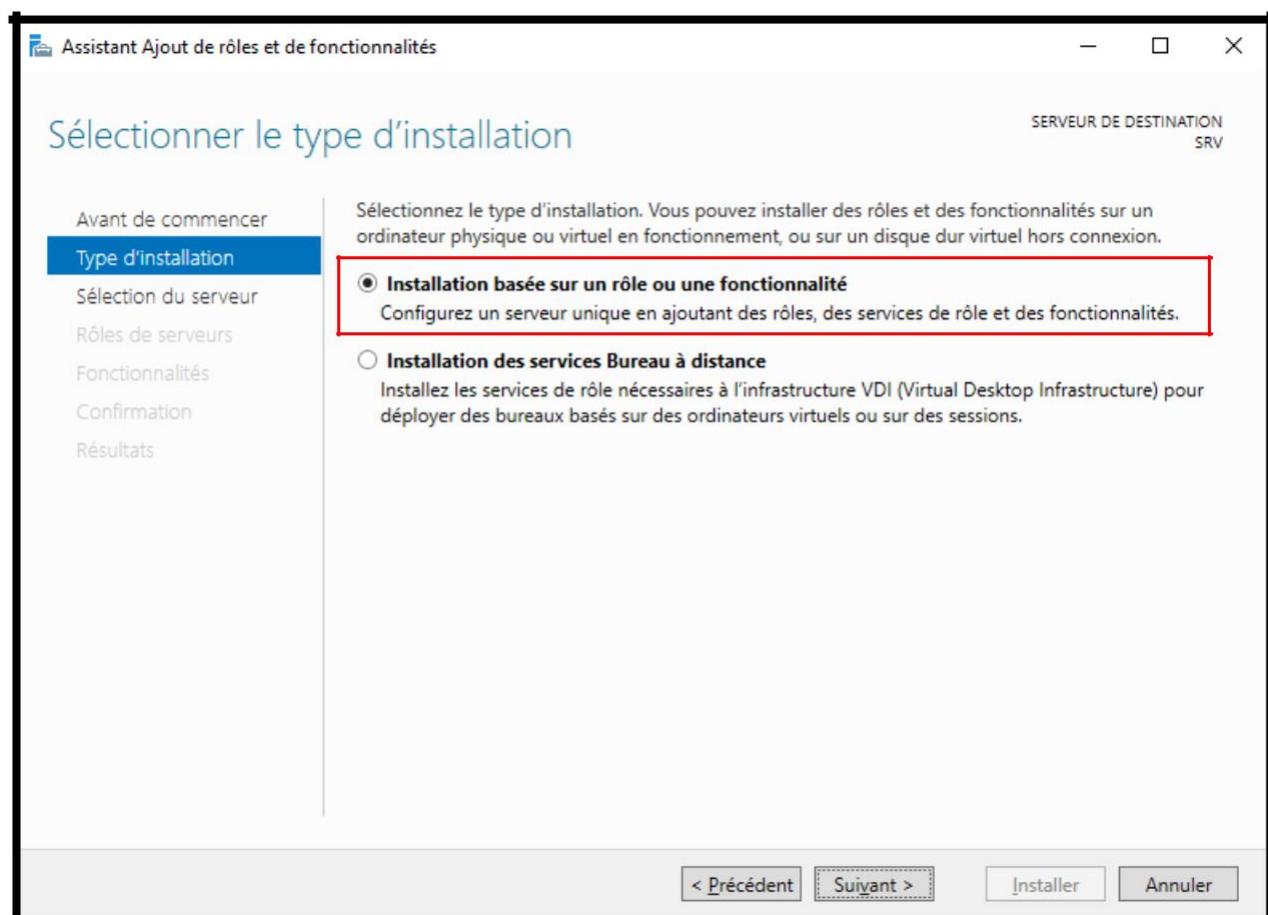
Donc à partir de là, nous suivons la procédure d'installation des services susmentionnés :  
Cliquez ensuite sur le bouton "**Suivant >**"

Il est toujours recommandé de lire les notes d'information que le système d'exploitation affiche à l'écran.

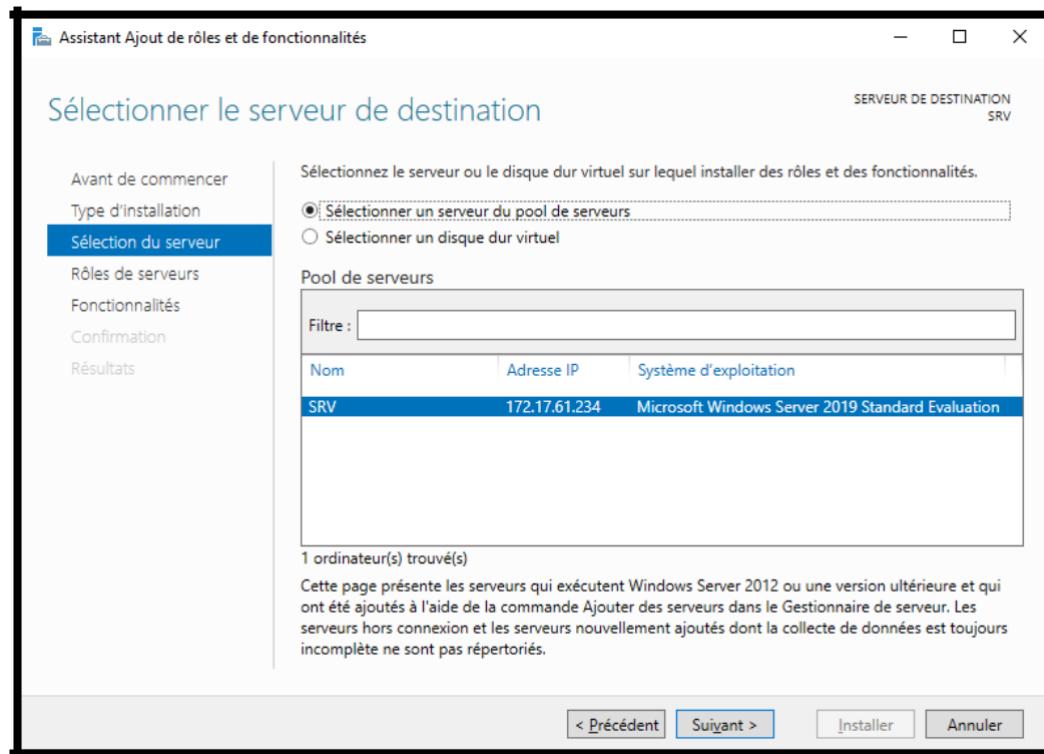


[Retour au Sommaire](#)

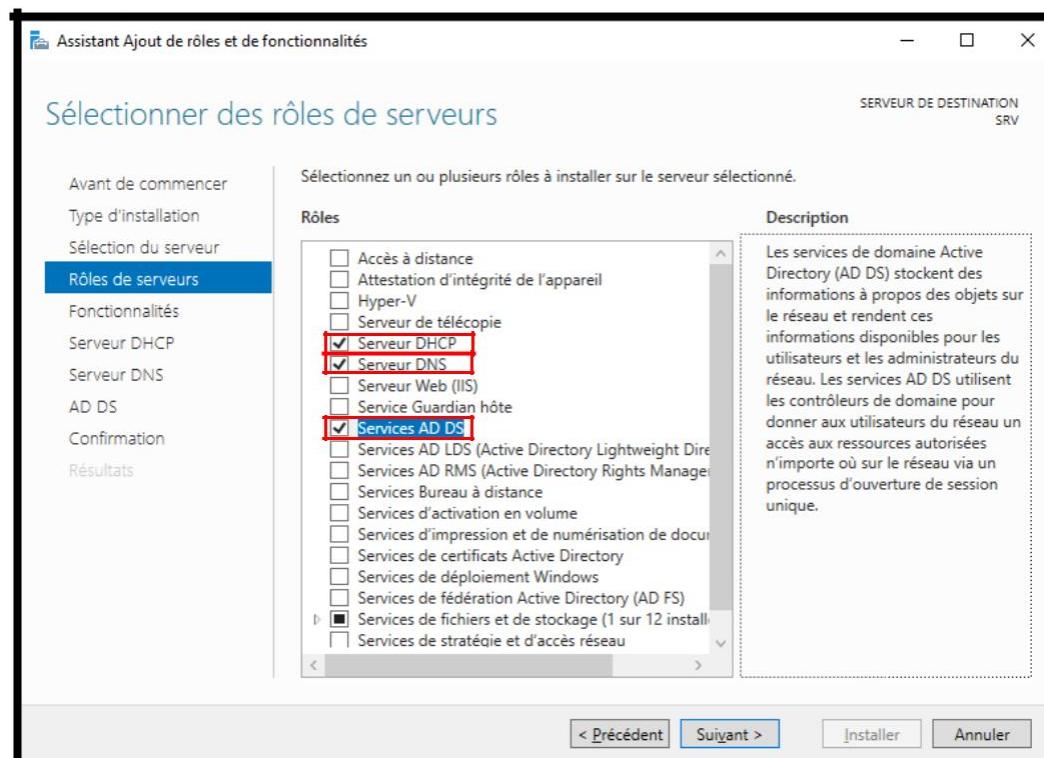
Assurez-vous que l'option est cochée : "Installation basée sur un rôle ou une fonctionnalité"



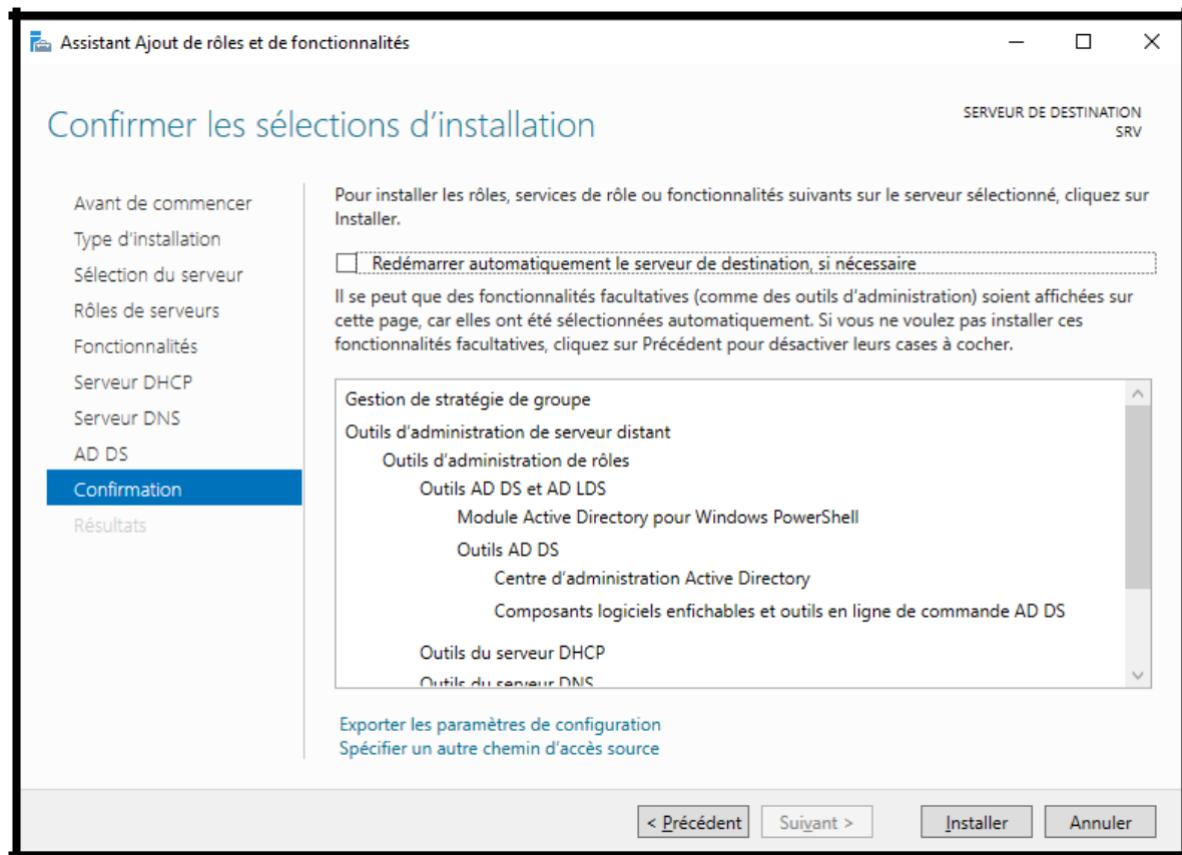
Vous pouvez choisir le serveur sur lequel installer. Dans ce cas, nous avons le serveur local « SRV ». Si tel est le cas, tous les serveurs qui seront ajoutés sur notre réseau apparaîtront ici. Il est donc également possible de réaliser des installations à distance.



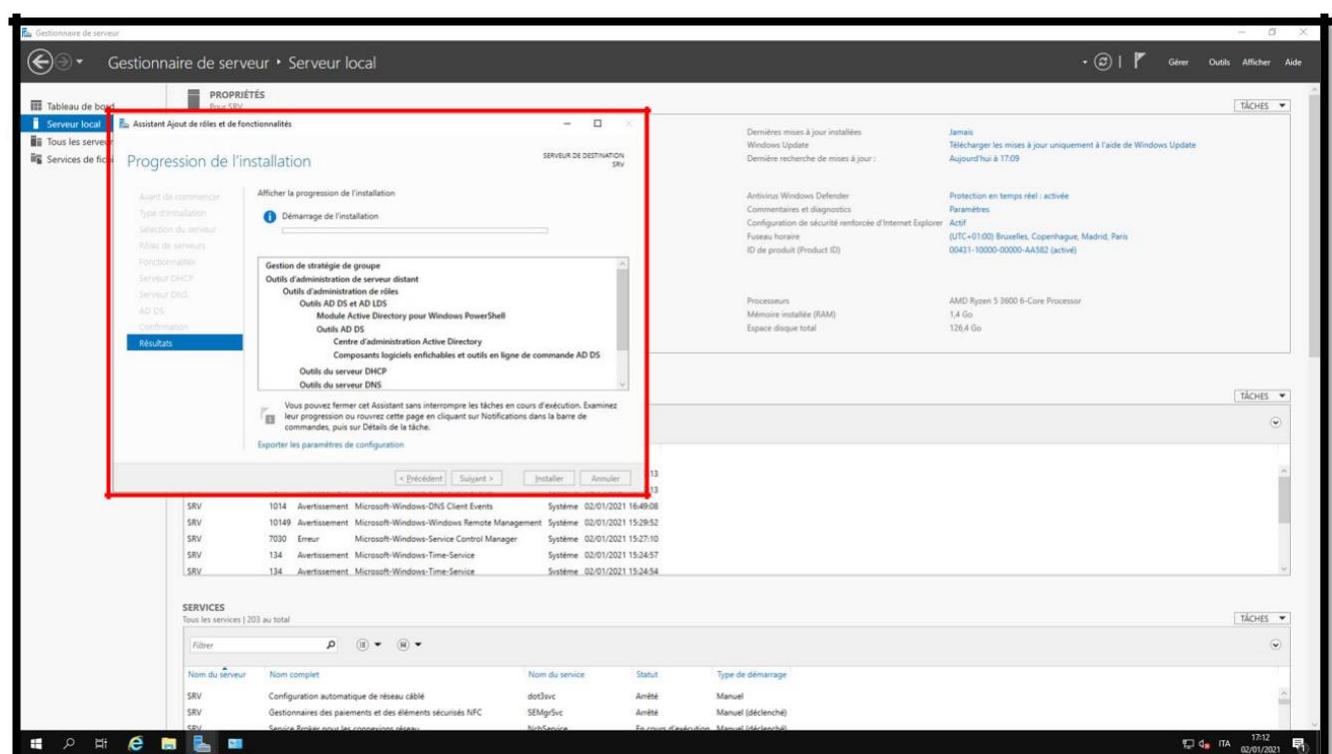
Dans cette fenêtre, nous choisirons d'installer le service AD DS (Active Directory) DNS et DHCP Evidemment nous irons choisir les fonctionnalités dont nous aurons besoin. Bien que généralement lors de l'installation de la fonctionnalité AD DS, le serveur DNS sera installé automatiquement.



Nous confirmons tous les paramètres précédemment décidés et cliquons sur "**Installer**"

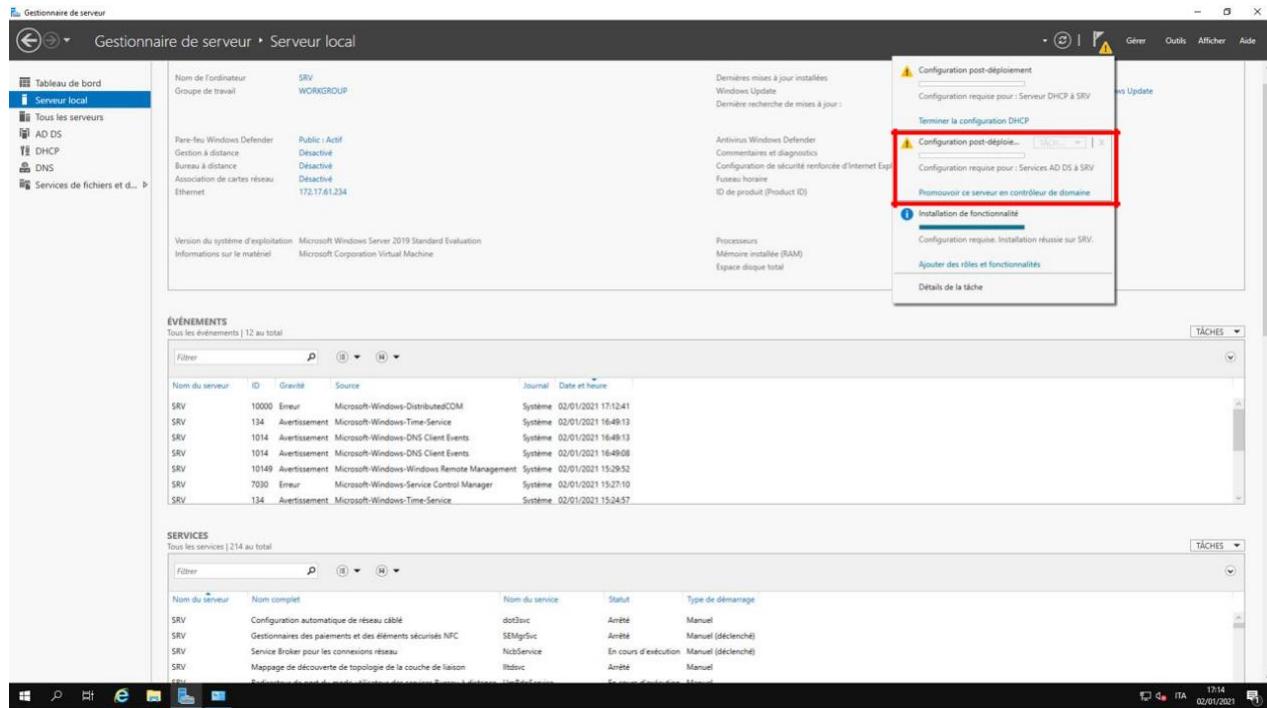


Depuis cet écran, nous pouvons voir le processus d'installation.



## Configuration du contrôleur de domaine

Nous pouvons voir sur cet écran, que maintenant, il y a une alerte (triangle orange) qui signifie qu'il y a une installation à configurer. Il faudra ensuite cliquer sur "Promouvoir ce serveur en contrôleur de domaine"



Ici, nous allons définir une option spécifique. Nous avons donc 3 options :

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

Notre cas est le troisième cas, car nous n'avons ni domaine ni forêt. La forêt n'est rien de plus qu'un ensemble de domaines. Nous n'avons même pas de contrôleur de domaine.

Il faut donc créer une nouvelle forêt. Nous donnerons dans la fenêtre que nous verrons un nom de domaine avec l'extension local (généralement des noms de domaine avec l'extension «**.Local**», «**.priv**» ou «**.int**») sont utilisés.

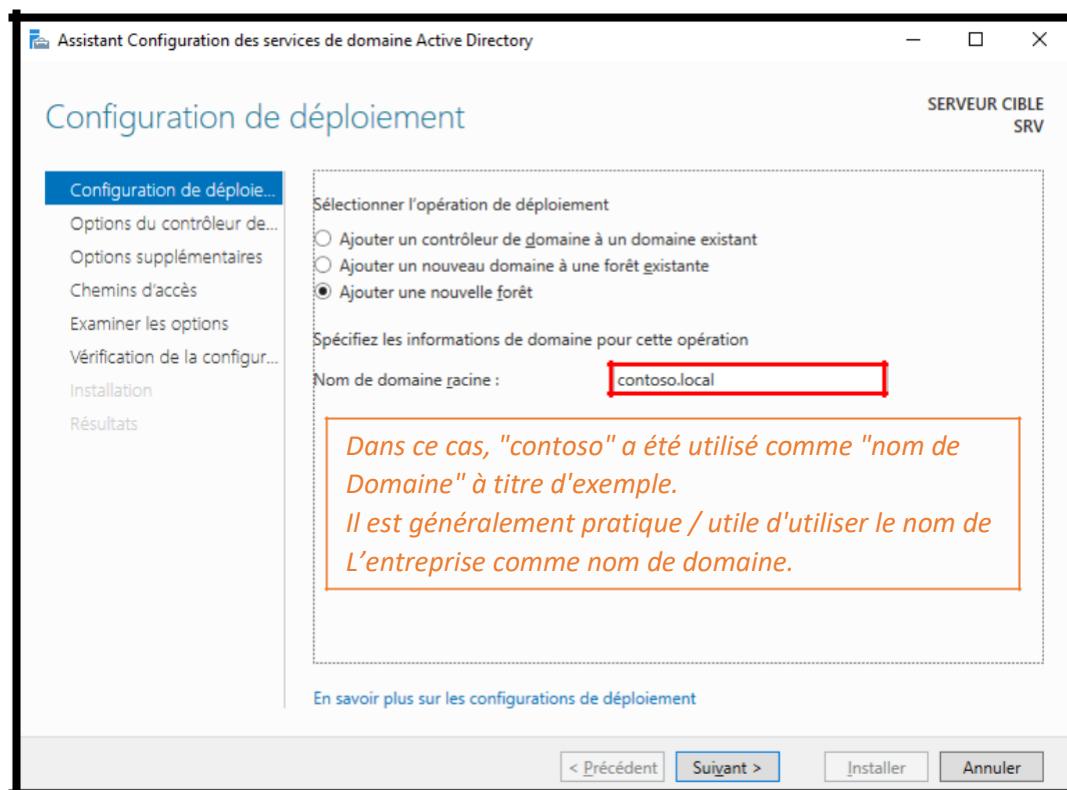
En général, il est recommandé d'utiliser le suffixe «**.Local**» (*cit. M. Kevin Roth*).

Ceci afin d'éviter qu'ils puissent entrer en conflit avec la résolution de nom des domaines publics.

Cela est vrai pour la plupart des entreprises. Certaines entreprises utilisent également des domaines publics dans le réseau local. Évidemment, dans ce dernier cas, une architecture infrastructurelle d'un certain type sera nécessaire.

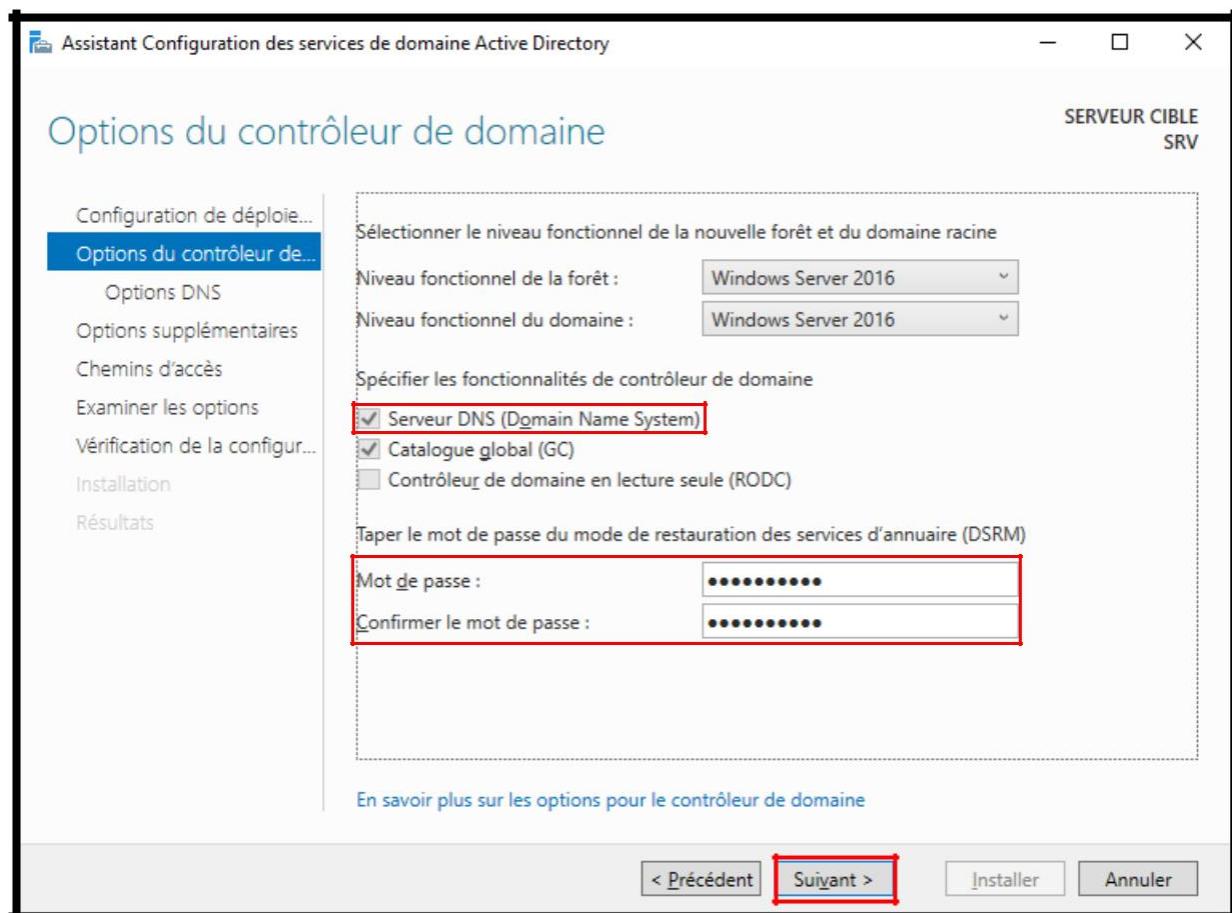
En général, le nom de domaine est le nom de l'entreprise. Dans ce cas, juste à titre d'exemple, (à ne pas utiliser dans les cas réels), nous allons utiliser l'exemple que Microsoft utilise souvent : "contoso.local".

En faisant cela, nous sommes sûrs qu'il n'existe pas dans les domaines publics, car l'extension «**.Local**» n'est pas un domaine public



Depuis cette fenêtre, il sera nécessaire d'installer le serveur DNS, car il remarque que le serveur DNS n'est pas installé. Il y a la possibilité de ne pas l'installer, mais dans notre cas c'est nécessaire, car les machines clientes ne seraient pas en mesure de résoudre le domaine.

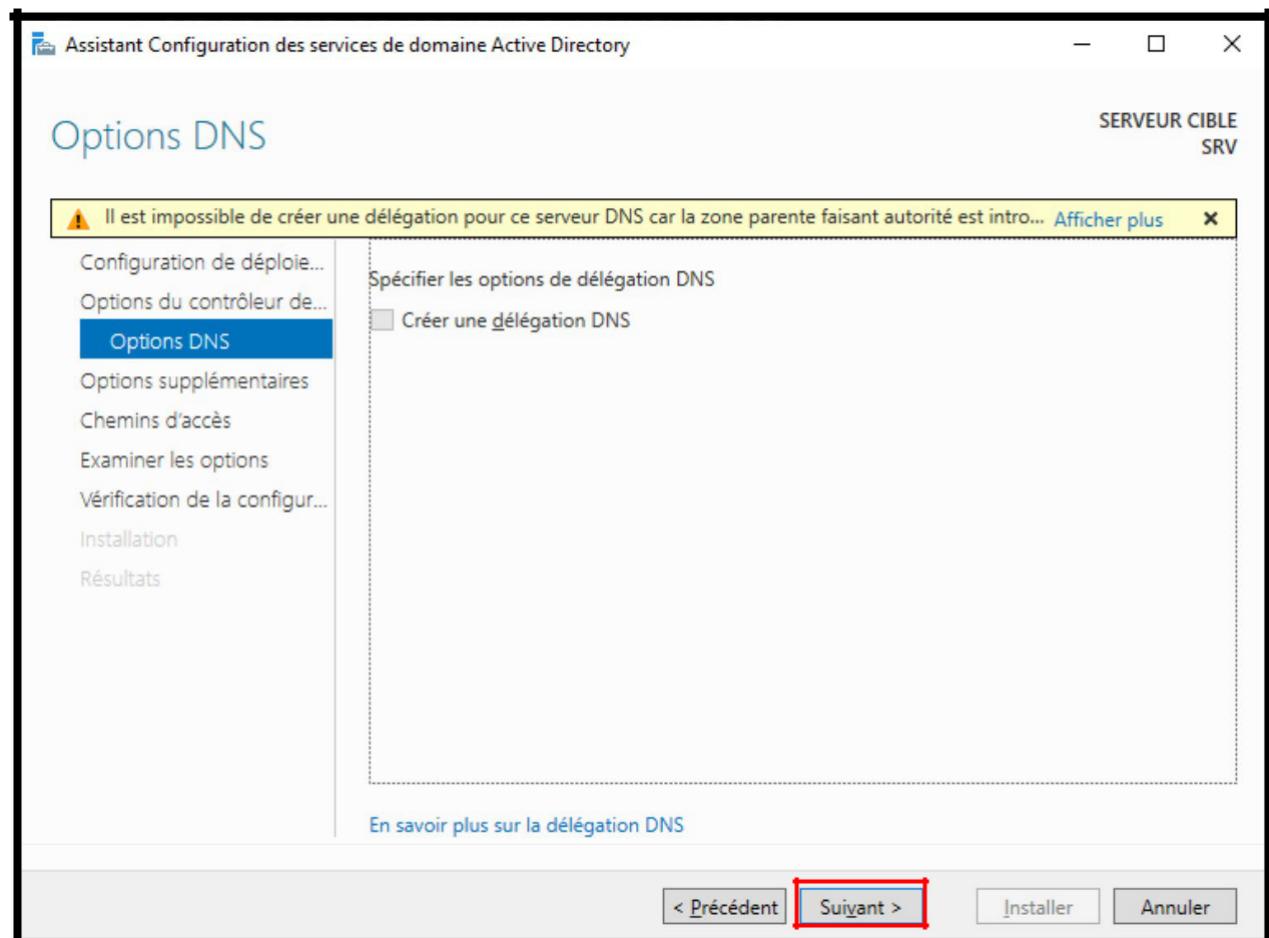
Le mot de passe demandé est le mot de passe que nous devrons utiliser si nous avons des problèmes avec le contrôleur de domaine, il démarrera en mode récupération, en demandant ce mot de passe afin d'effectuer la procédure de récupération (récupération du mot de passe du service AD DS)



Attention : le mot de passe (sur Win Server 2019) doit contenir des minuscules, des majuscules et des caractères spéciaux pour des raisons de sécurité (sinon, le système répond par une erreur).

[Retour au Sommaire](#)

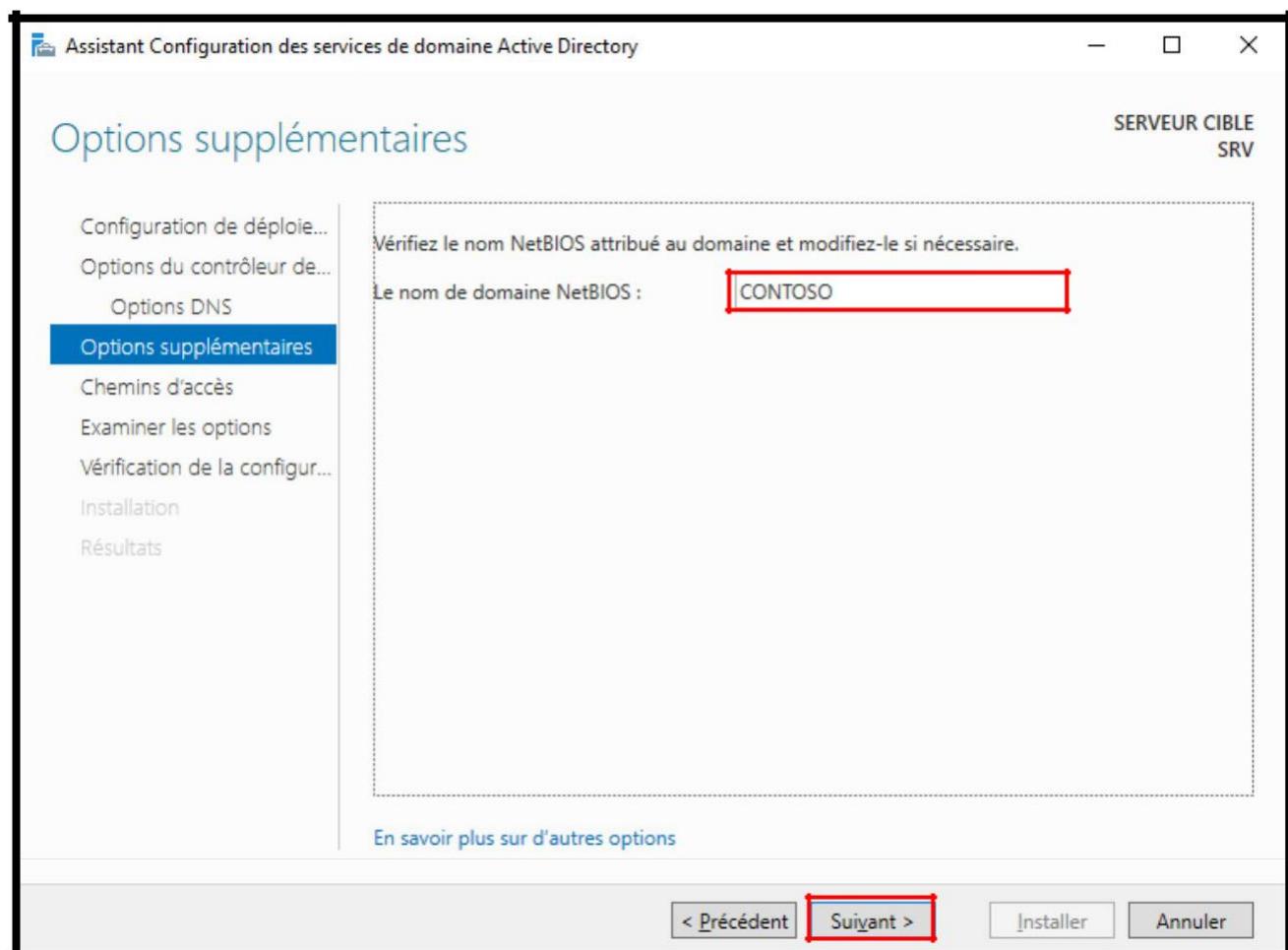
Dans cette fenêtre, une "alerte" s'affiche, ce qui est tout à fait normal, puisqu'il n'y a pas encore de serveur DNS, il n'est pas possible de créer la délégation pour la zone faisant autorité parente. Ce n'est pas un problème, car tout cela se fera automatiquement lors de l'installation.





[Retour au  
Sommaire](#)

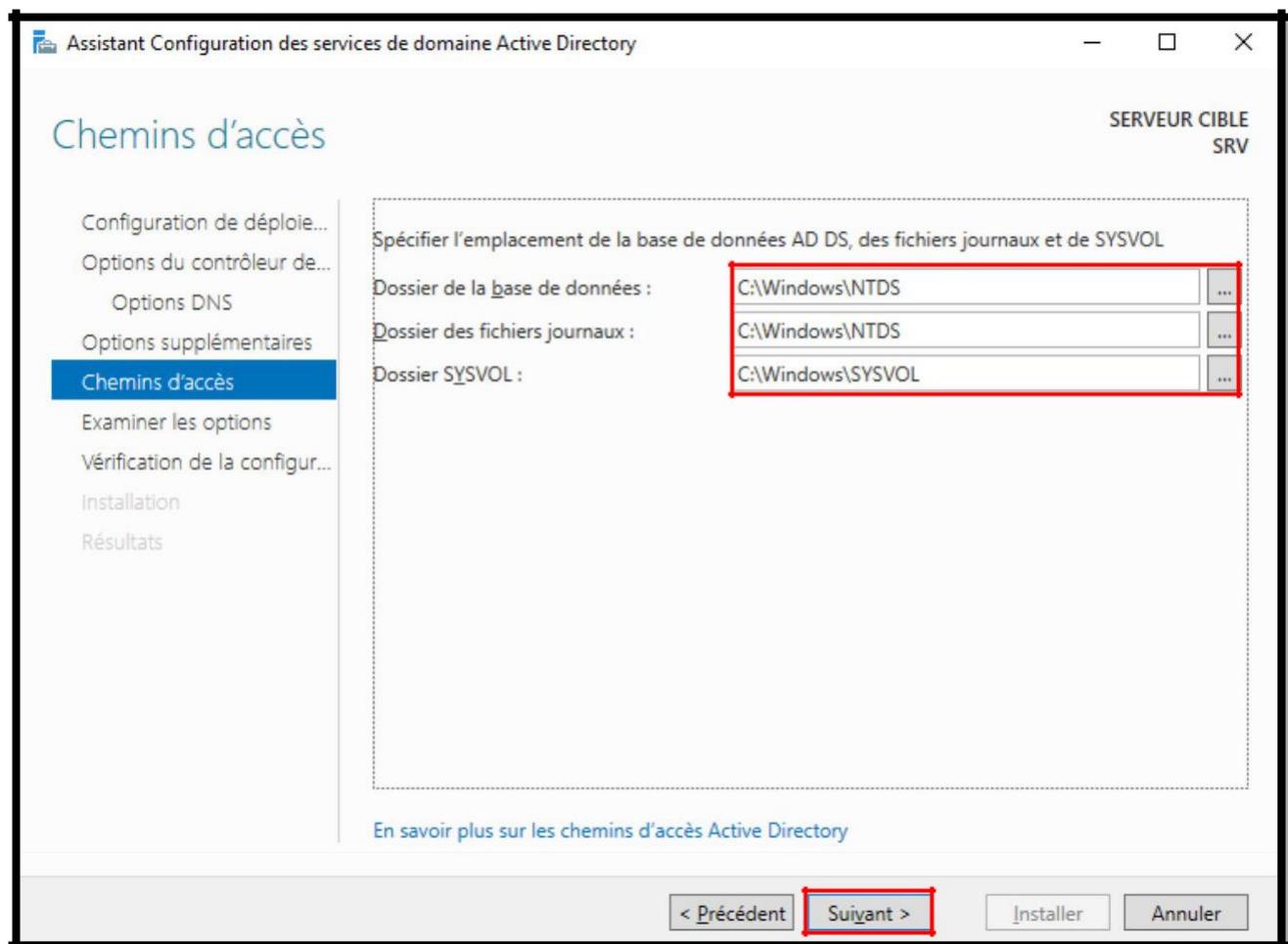
Le nom NetBIOS est défini automatiquement, ce n'est rien d'autre que le nom de domaine sans l'extension



Ici, nous pouvons choisir où (le contrôleur de domaine) enregistrer les informations AD DS, puis :

- La base de données
- Les fichiers journaux
- La SYSVOL

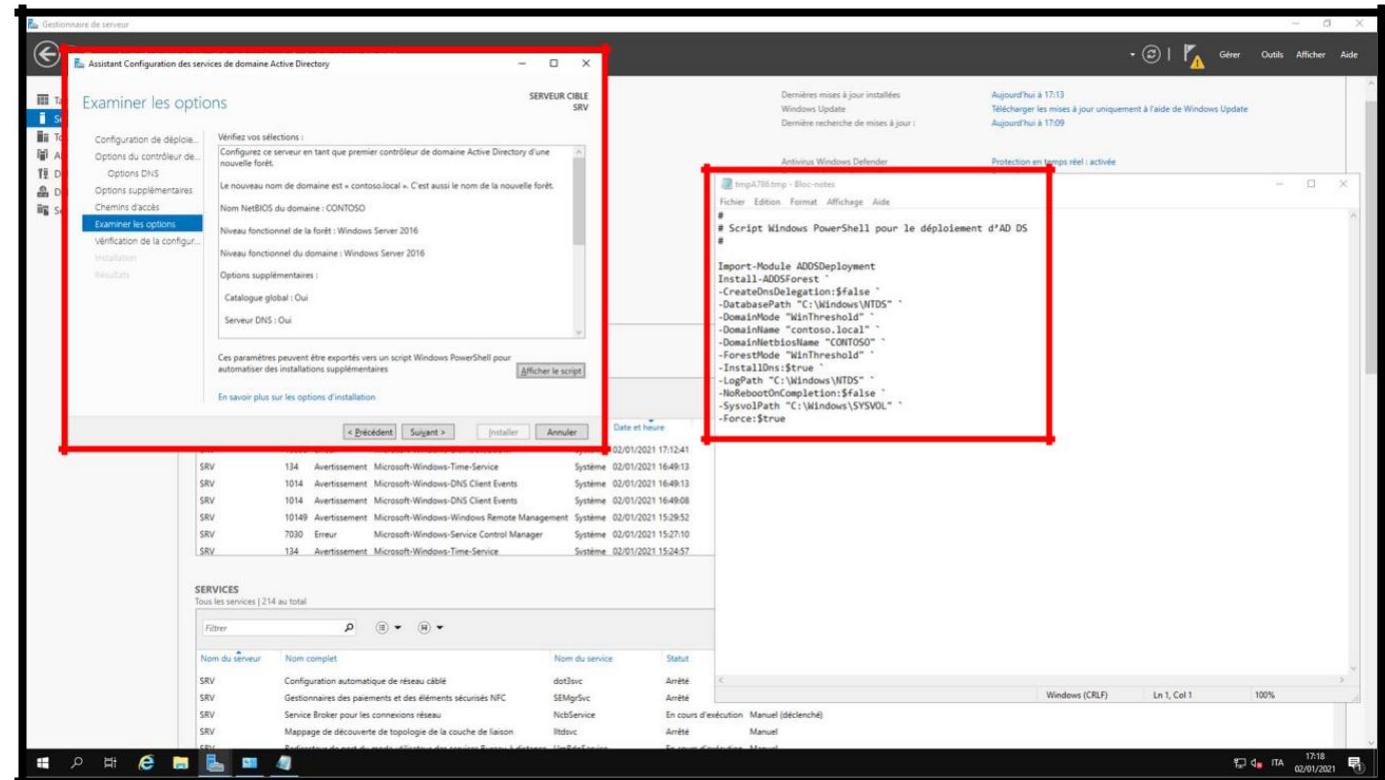
Par défaut, les dossiers affichés dans la capture d'écran sont choisis, mais il est possible de changer le chemin, pour ceux qui ont des besoins différents. Comme le stockage externe où enregistrer ces informations.



Ici, nous avons un petit résumé de tous les paramètres.  
Un bref diagnostic des prérequis sera fait.

Nous pourrions également enregistrer le script d'installation pour pouvoir le réutiliser plus tard pour d'autres installations via PowerShell

(PowerShell est un logiciel Microsoft qui intègre une interface en ligne de commande)



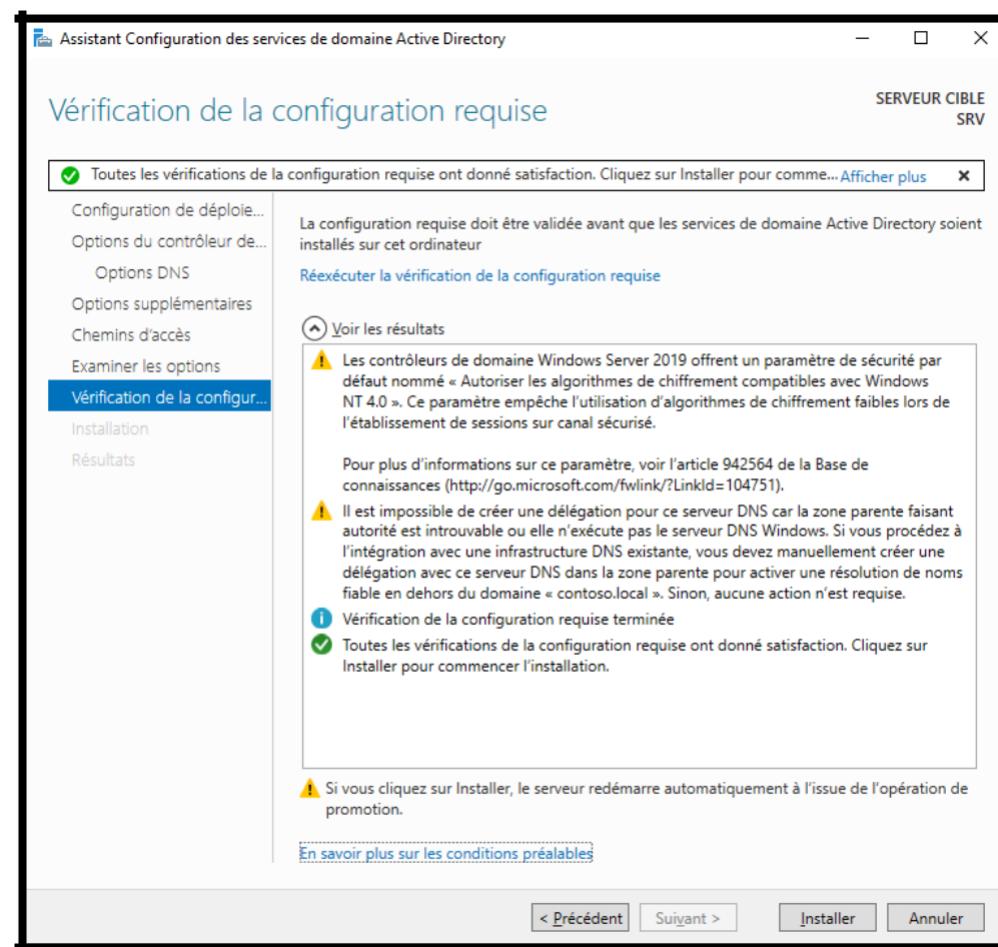
Nous aurons certainement des "*alertes*" qui nous informent que :

- La zone parent ne peut pas être créée.
- Les exigences concernant les paramètres de sécurité des algorithmes de chiffrement pour Win. NT4.0 ne sera pas satisfait.

Nous pouvons ignorer les deux alertes en toute sécurité, car les conditions préalables sont remplies et nous pouvons procéder à l'installation.

Ensuite, l'installation AD DS démarrera, ce qui prendra un certain temps en fonction de notre support de stockage.

(*En général, environ 10min pour un disque dur classique et moins de 5min pour un ssd*)

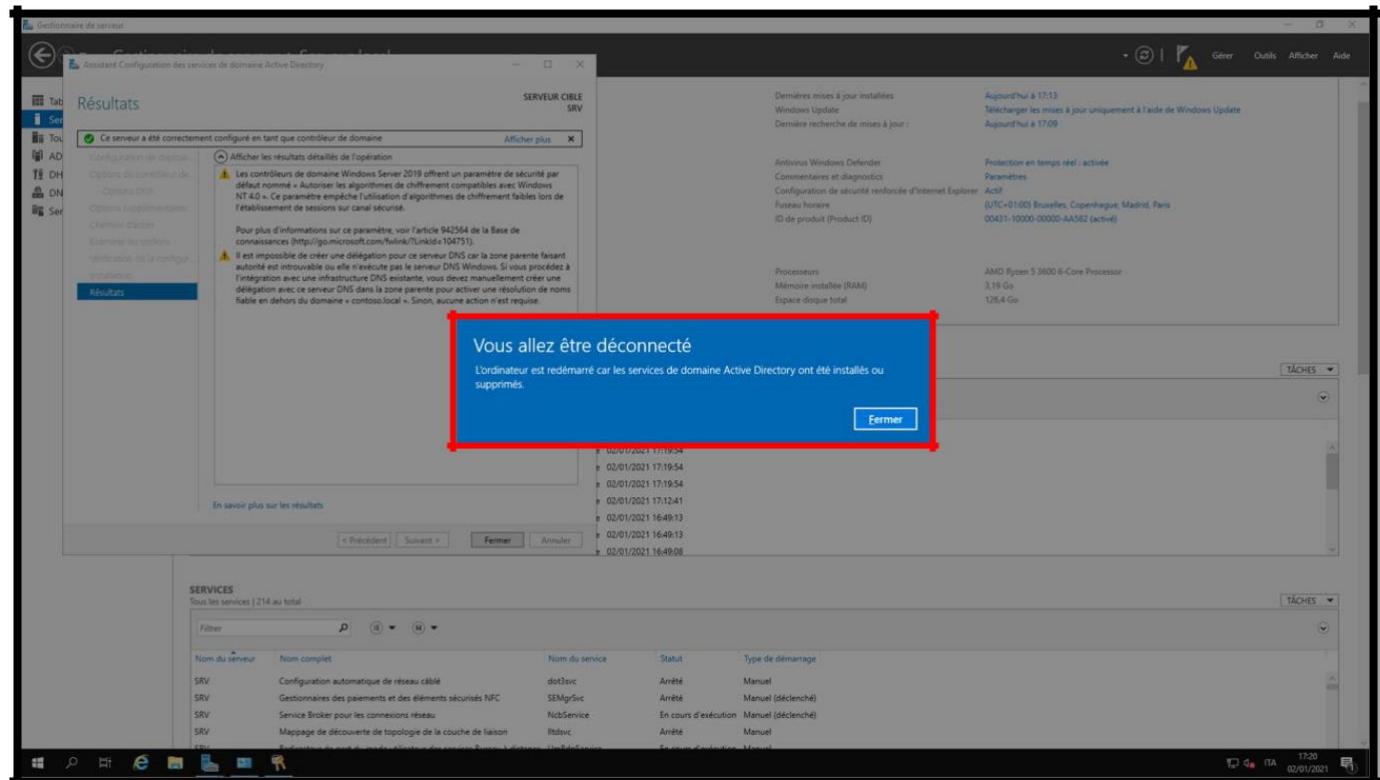


Dans ce cas, par conséquent, le rôle de contrôleur de domaine sera installé, en l'associant aux cinq rôles typiques de contrôleur de domaine. Évidemment, dans le réseau plus tard, il est possible d'ajouter plus d'un contrôleur de domaine (pour des raisons évidentes) et d'associer des rôles spécifiques à chaque contrôleur de domaine.

Je profite de cette occasion pour dire que **dans un réseau, il devrait y avoir au moins deux contrôleurs de domaine**, car dans le cas où l'un des deux ne serait pas restreint, les machines peuvent continuer à fonctionner et par conséquent les utilisateurs peuvent continuer à s'authentifier et donc travailler sans interruption.

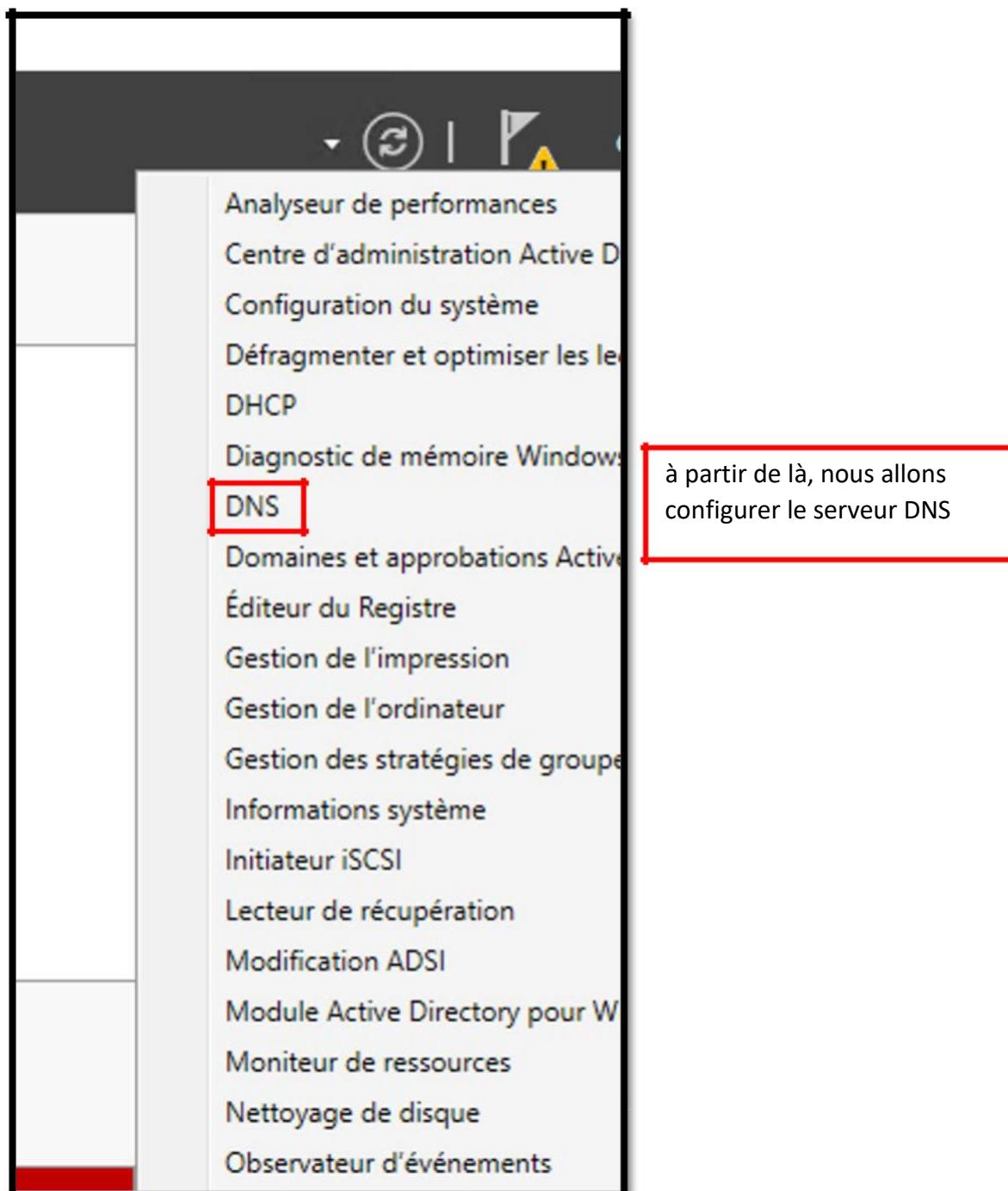
Après l'installation, le serveur redémarrera.

Le premier démarrage d'un contrôleur de domaine nouvellement créé est légèrement plus lent car il doit définir toutes les configurations.

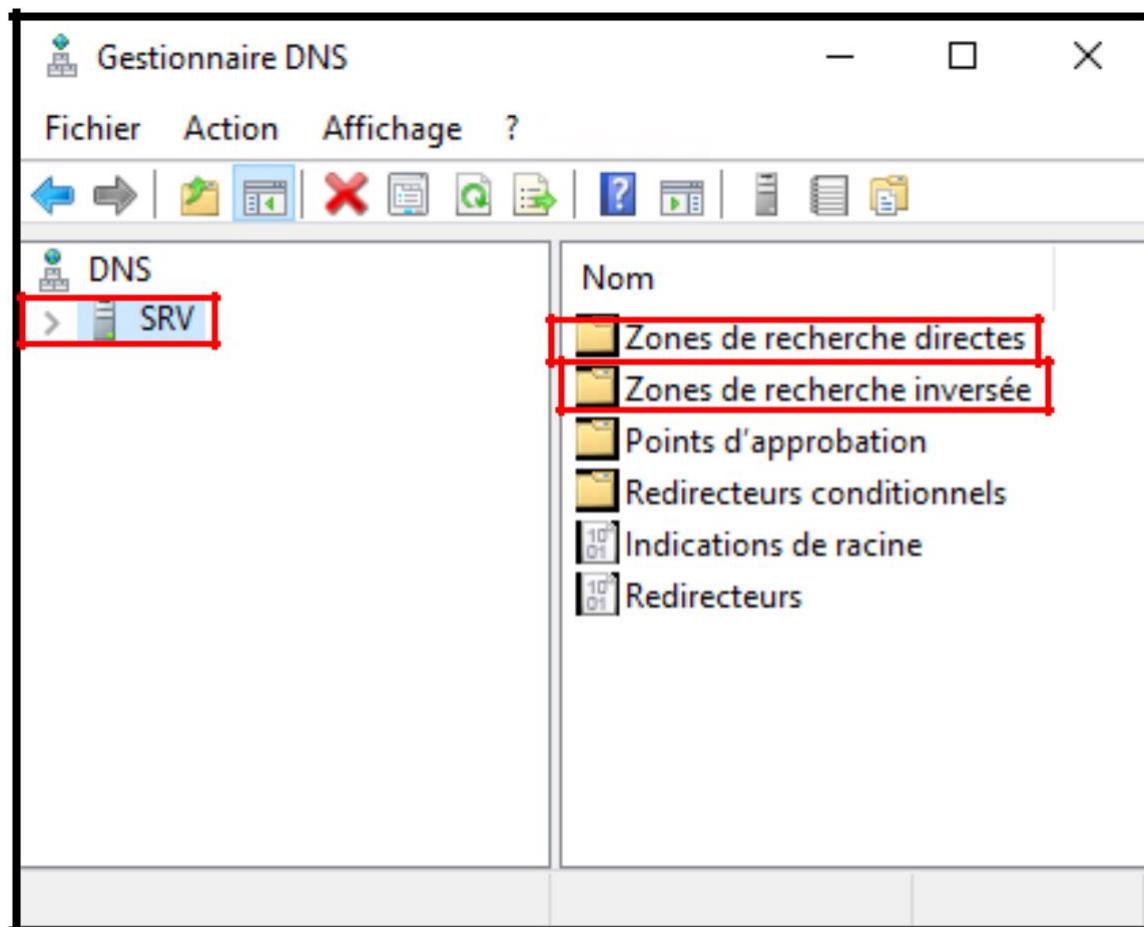


## Configuration du DNS

De là, nous allons configurer le serveur DNS

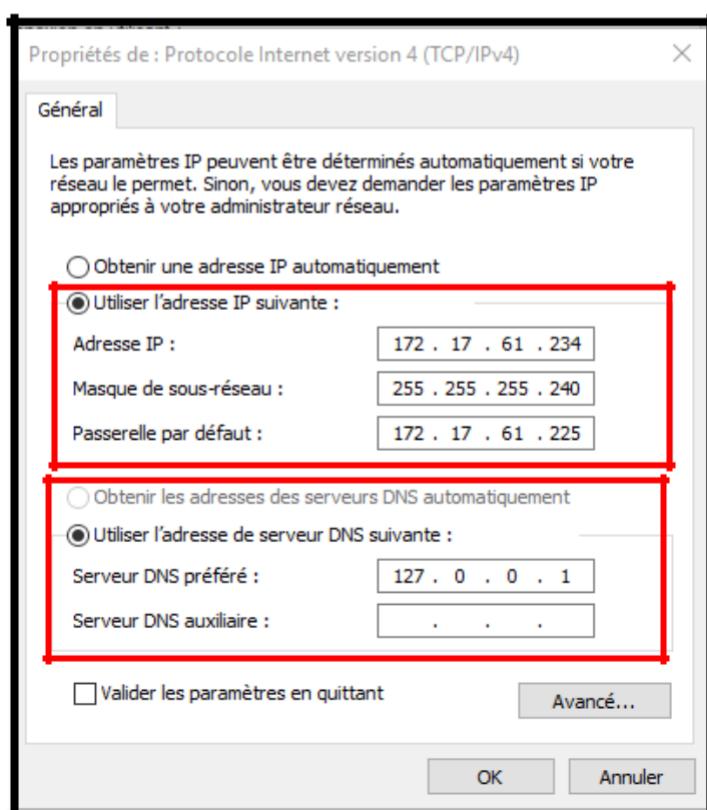
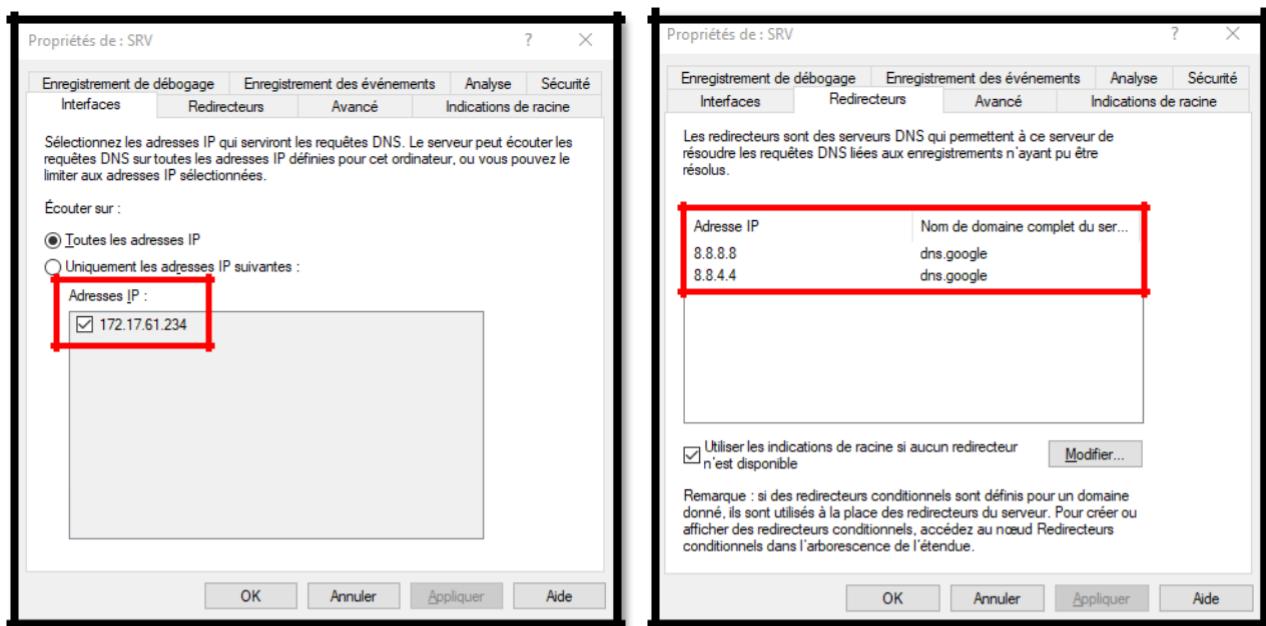


Depuis cette console dans la capture d'écran ci-dessous, vous pouvez gérer tous les serveurs DNS du réseau. En cela, nous n'avons que le serveur précédemment créé, puis SRV.



En cliquant avec le bouton droit de la souris sur "propriétés" sur notre serveur DNS (dans notre cas SRV), vous pouvez sélectionner les interfaces sur lesquelles le serveur DNS doit fonctionner. On peut également noter que dans les serveurs DNS Redirecteurs, (Wizard en anglais) a déjà paramétré le DNS précédemment défini auparavant.

Ensuite, dans la carte réseau, il a défini l'adresse IP **127.0.0.1** comme serveur DNS, c'est parce que notre serveur le fera directement à partir du serveur DNS, donc tout ce qu'il ne pourra pas résoudre, il l'enverra aux serveurs Redirecteurs (donc dans ce cas aux serveurs de transfert google précédemment mis en place 8.8.8.8 et 8.8.4.4)



Depuis cette fenêtre, nous pouvons voir que la zone contoso.local a été créée avec succès, nous avons déjà le premier "record" qui est le contrôleur de domaine.

Dans cette fenêtre, nous verrons automatiquement toutes les machines qui seront ajoutées au réseau et au domaine "contoso".

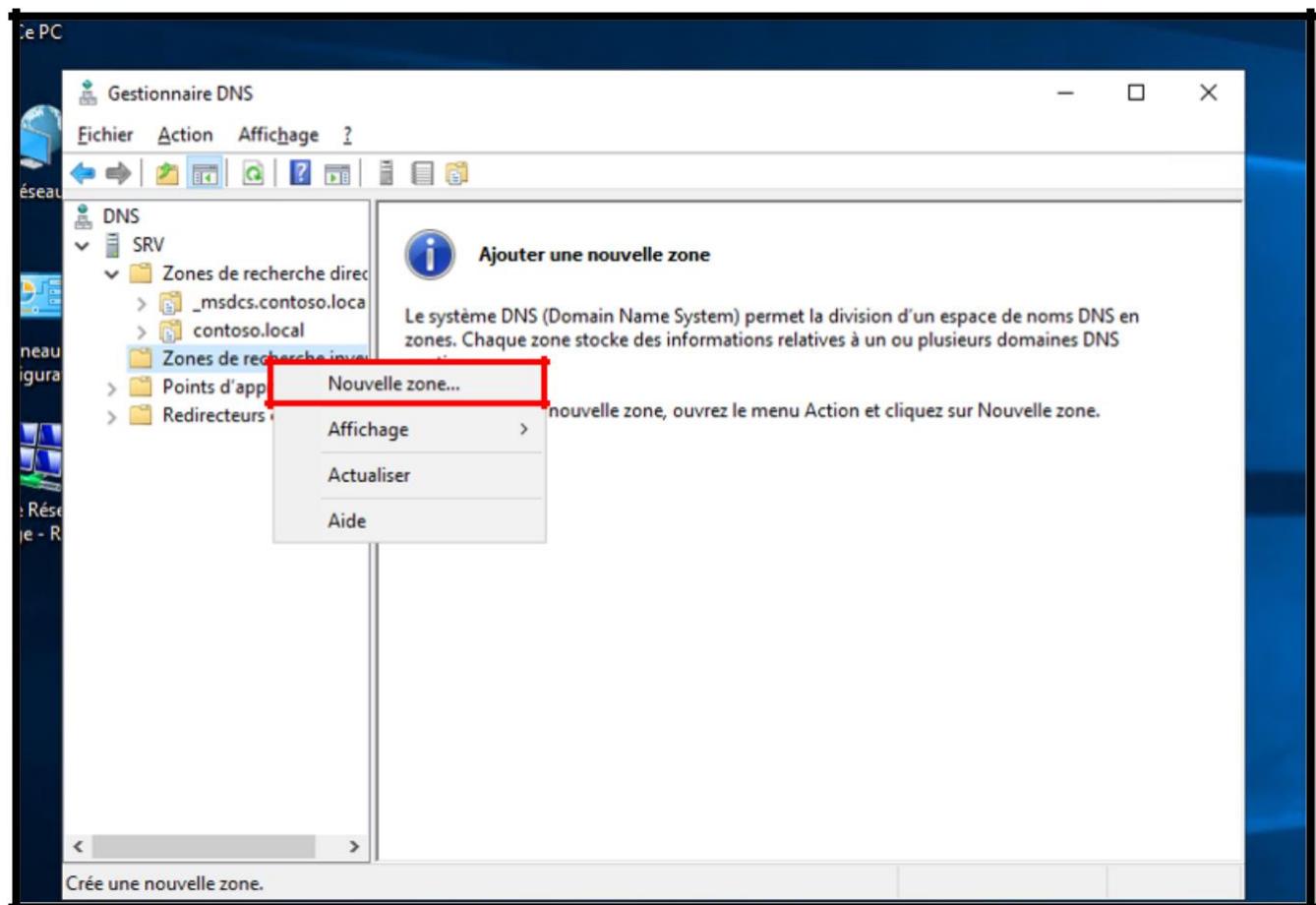
The screenshot shows the Windows DNS Manager interface. On the left, the navigation pane displays the tree structure: DNS > SRV > Zones de recherche directe > \_msdcs > contoso.local. The main pane lists DNS records for the 'contoso.local' zone. A red box highlights the first record, 'srv', which is of type 'Hôte (A)' with an IP address of '172.17.61.234'. Other records listed include '\_msdcs' (Source de nom (SOA)), '\_sites' (Serveur de noms (NS)), '\_tcp' (Hôte (A)), '\_udp' (Hôte (A)), 'DomainDnsZones' (identique au dossier parent), 'ForestDnsZones' (identique au dossier parent), and '(identique au dossier parent)' (Hôte (A)).

Nom	Type	Données	Horodaté
_msdcs	Source de nom (SOA)	[19], srv.contoso.local., ho...	statique
_sites	Serveur de noms (NS)	srv.contoso.local.	statique
_tcp	Hôte (A)	172.17.61.234	02/01/202
_udp	Hôte (A)	172.17.61.234	statique
DomainDnsZones	(identique au dossier parent)		
ForestDnsZones	(identique au dossier parent)		
(identique au dossier parent)	Hôte (A)	172.17.61.234	statique
<b>srv</b>	<b>Hôte (A)</b>	<b>172.17.61.234</b>	<b>statique</b>

La zone inversée n'a pas encore été créée ! c'est en effet une chose à faire ! Cliquez ensuite avec le bouton droit de la souris sur "nouvelle zone ..."

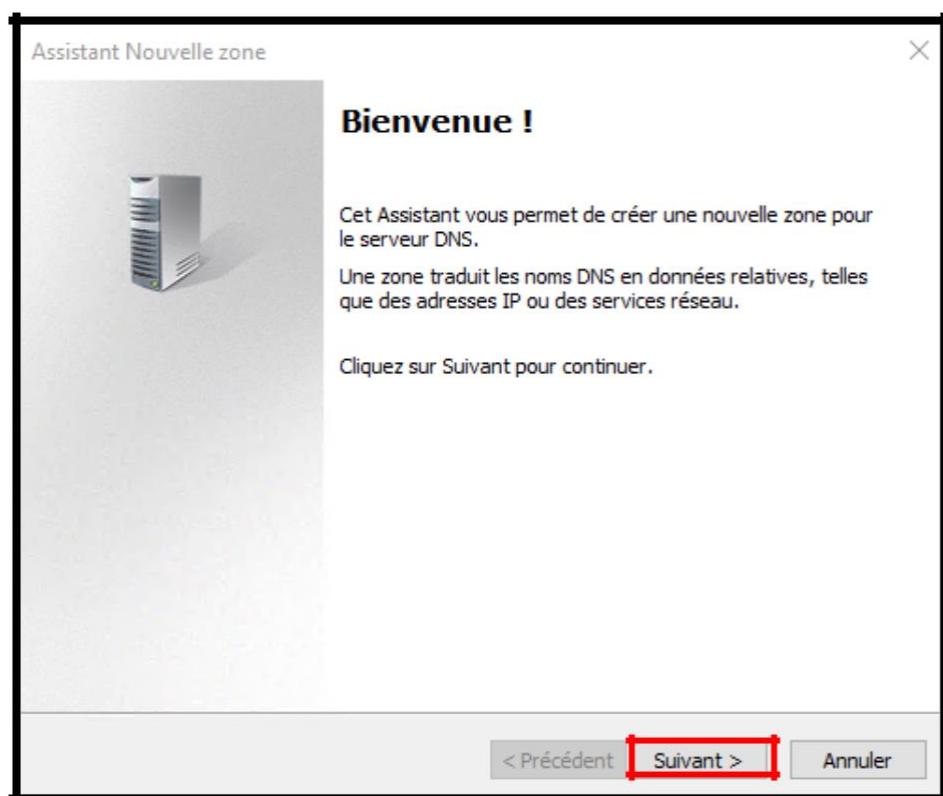
### A quoi sert la "zone inversée" ?

Tandis que la "zone directe" résout le nom et renvoie l'adresse IP, la zone inversée résout le nom à partir de l'adresse IP. C'est "Best\_Practice" pour créer également la zone inverse, sinon il pourrait y avoir des problèmes avec le fonctionnement de tout le domaine.

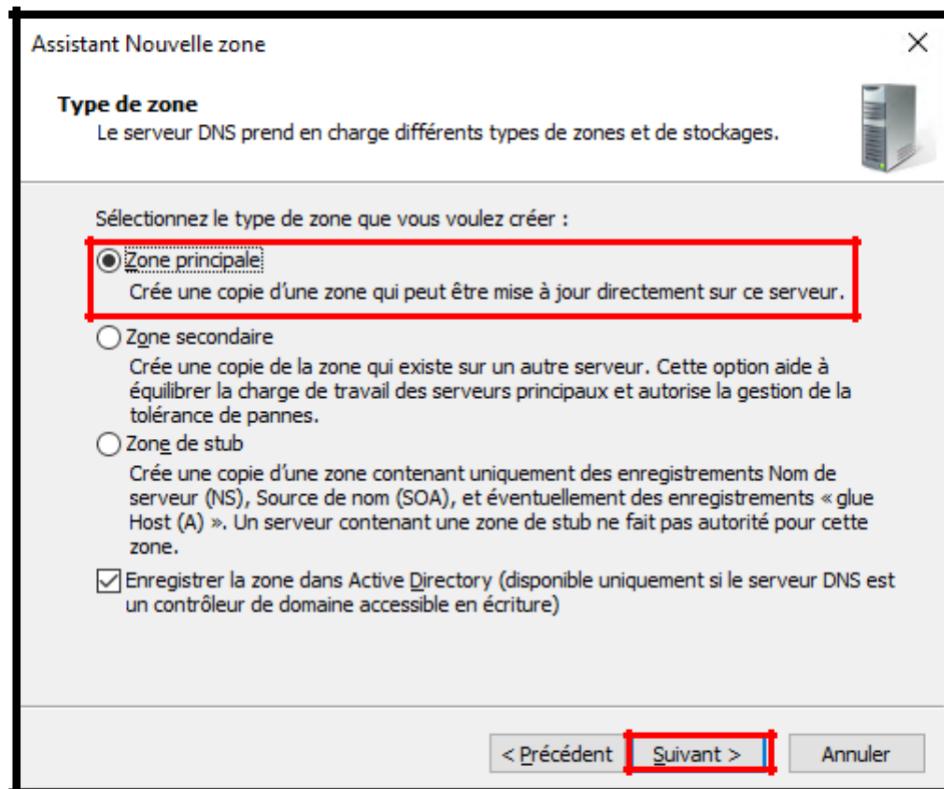


[Retour au  
Sommaire](#)

Cliquez ensuite sur « *Suivant >* »

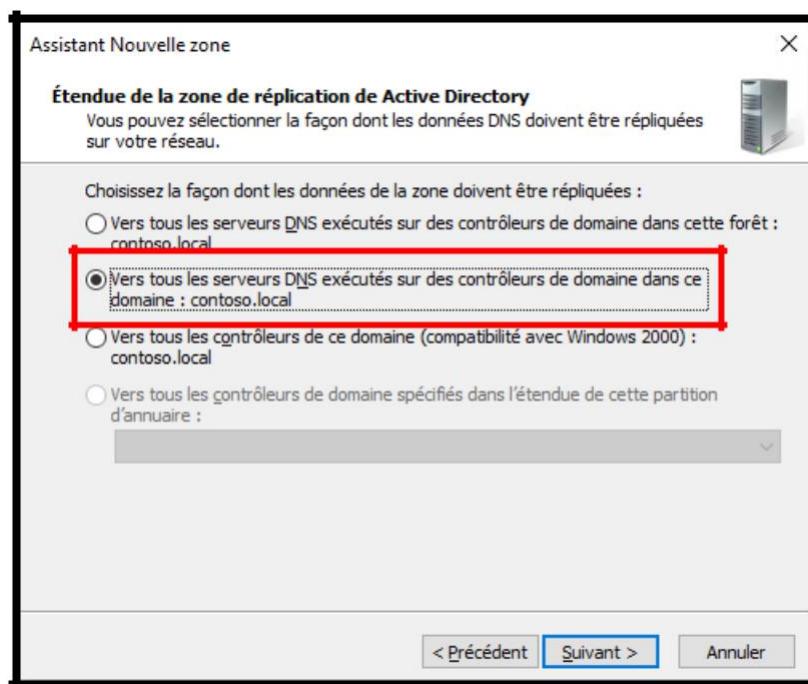


Nous allons donc créer une zone principale.

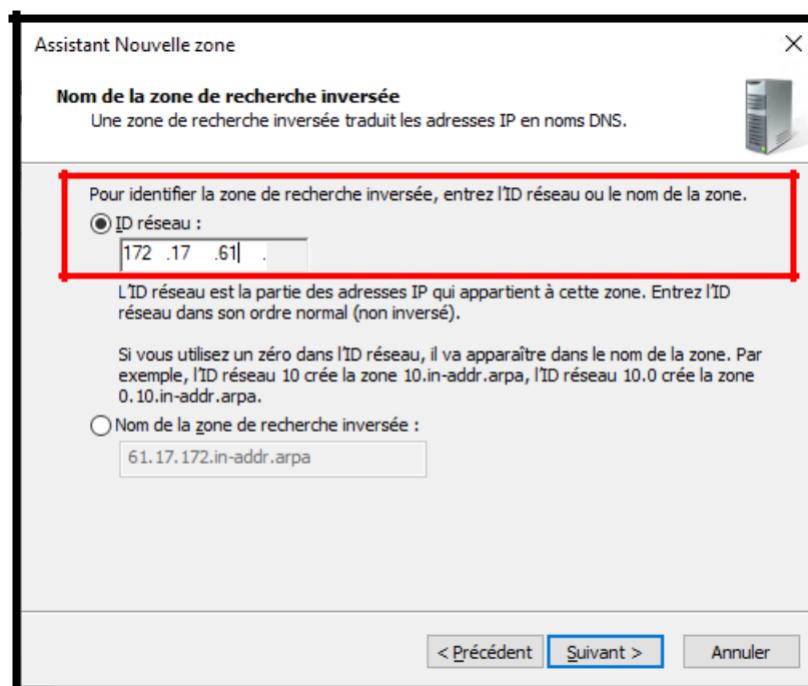


[Retour au Sommaire](#)

Nous autoriserons la réPLICATION de tous les serveurs DNS dans le domaine «contoso»

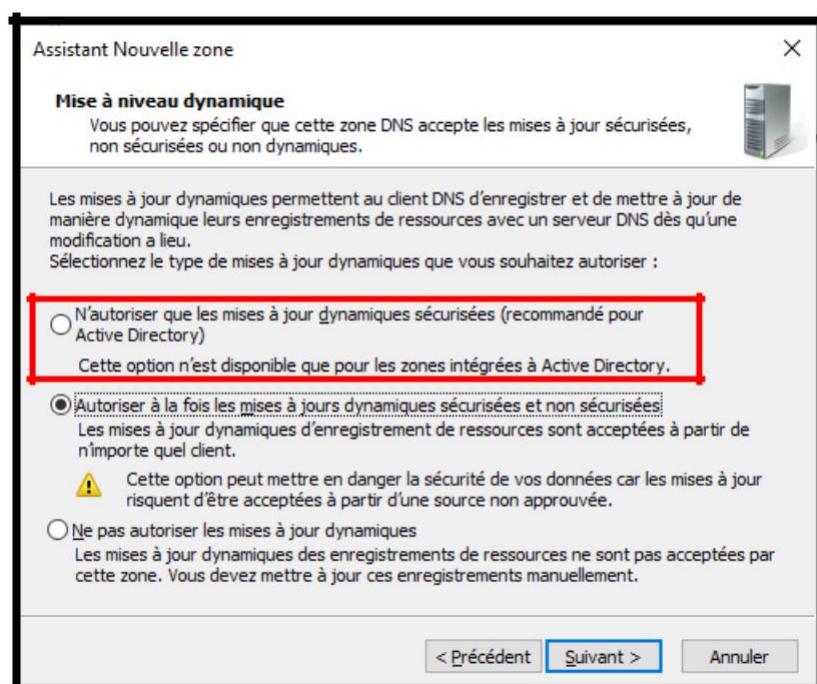


Ici, nous allons entrer l'ID du réseau. Le dernier octet est implicite, vous n'avez donc pas besoin de l'insérer. Dans ce cas, l'ID à saisir est donc les trois premiers octets de l'adresse IP précédemment définie dans la carte réseau.



[Retour au Sommaire](#)

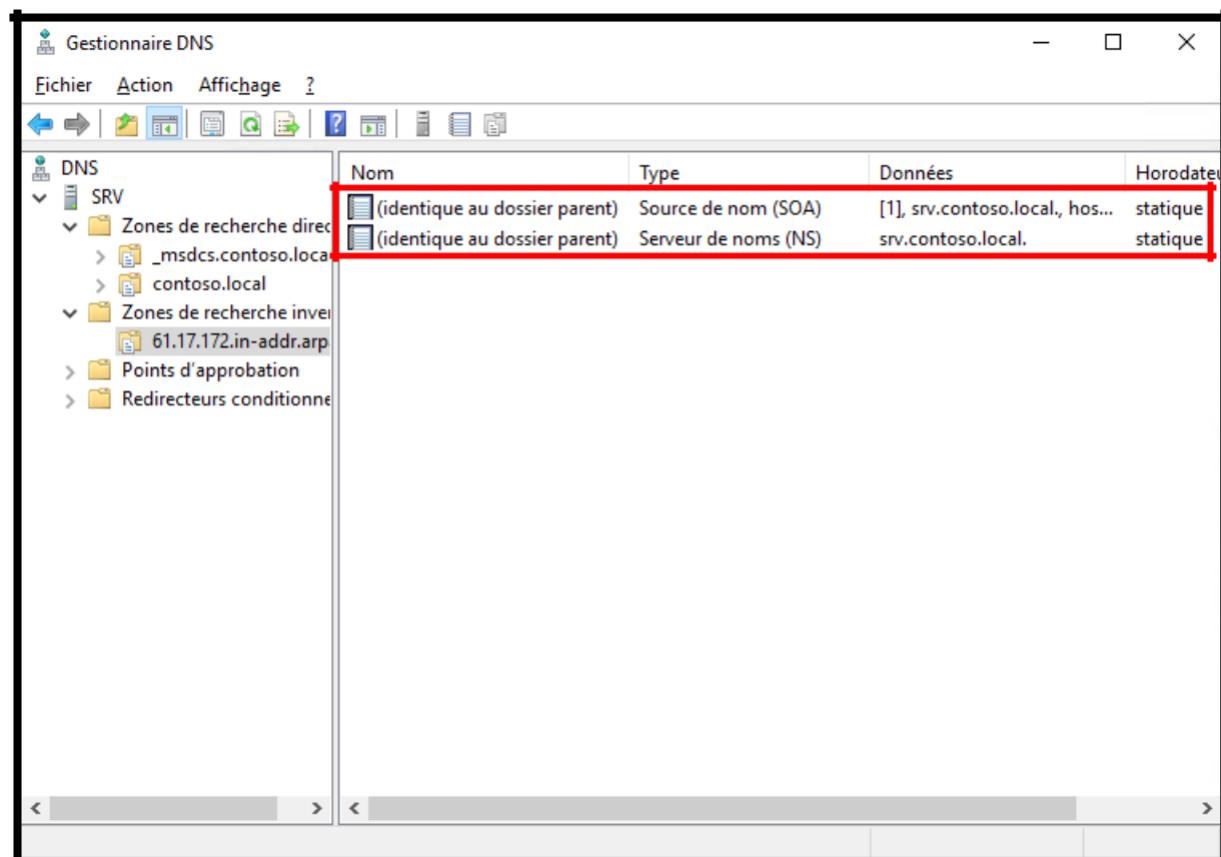
Il est toujours recommandé d'utiliser la première option pour des raisons de sécurité évidentes, mais, dans certains cas, dans le cas où nous allons utiliser un DNS local qui n'a pas à résoudre des noms publics qui ne sont pas sur un réseau public, nous pouvons également définir des mises à jour dynamiques sécurisées et non sécurisées.



En cliquant sur "Terminer" nous avons créé la "zone inverse".

...où nous avons déjà le premier "Record" qui est le contrôleur de domaine.

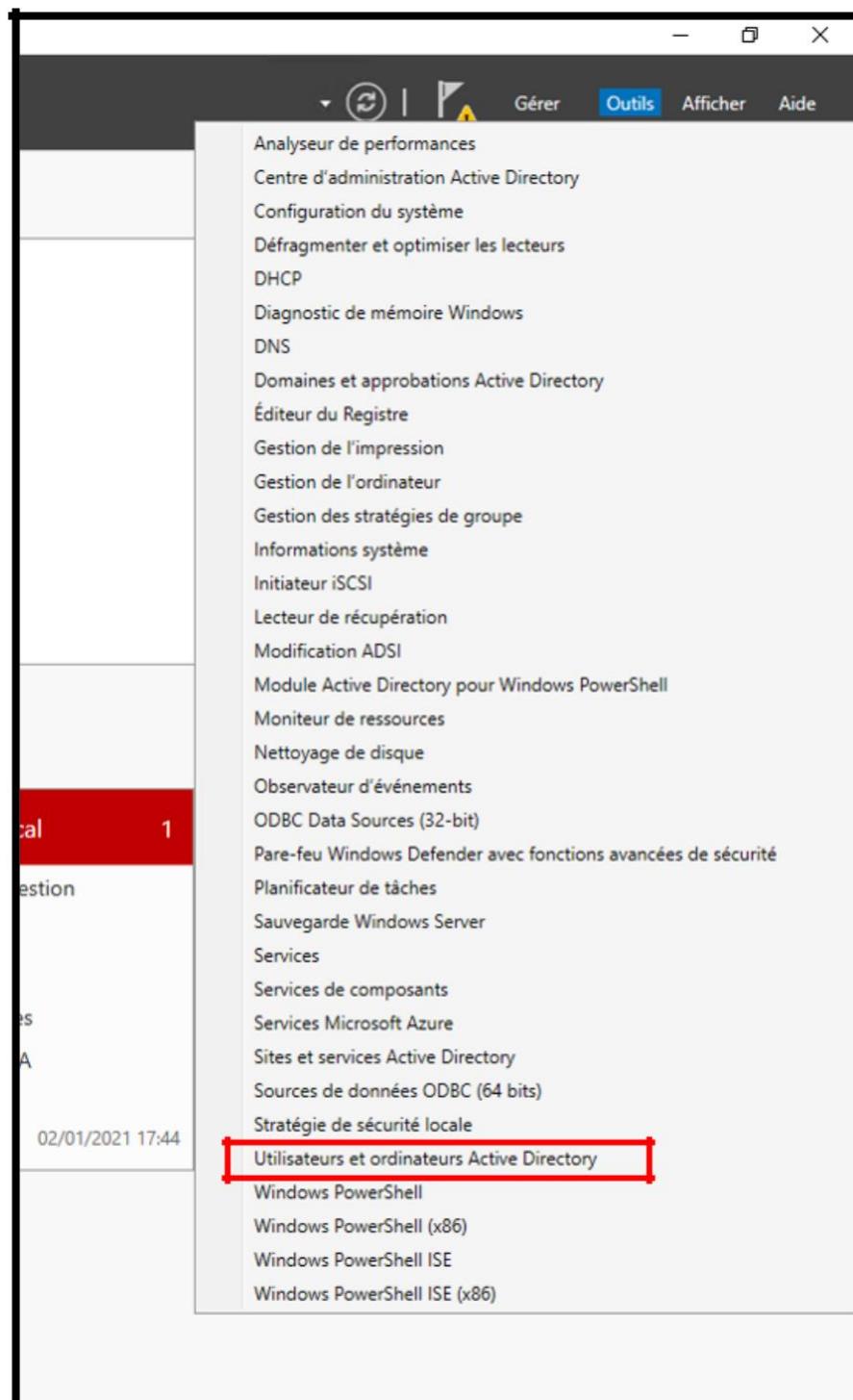
Nous avons donc terminé la configuration du serveur DNS ici.



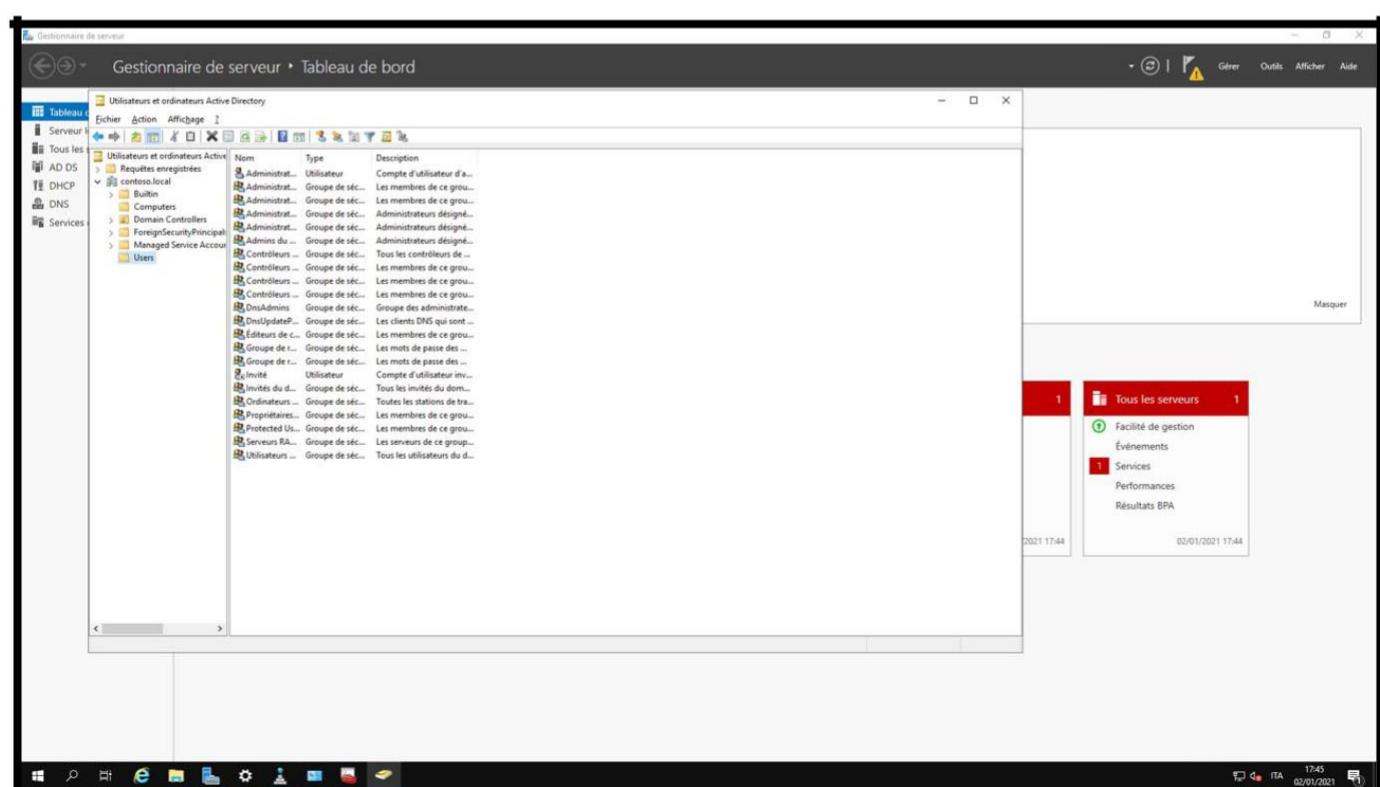
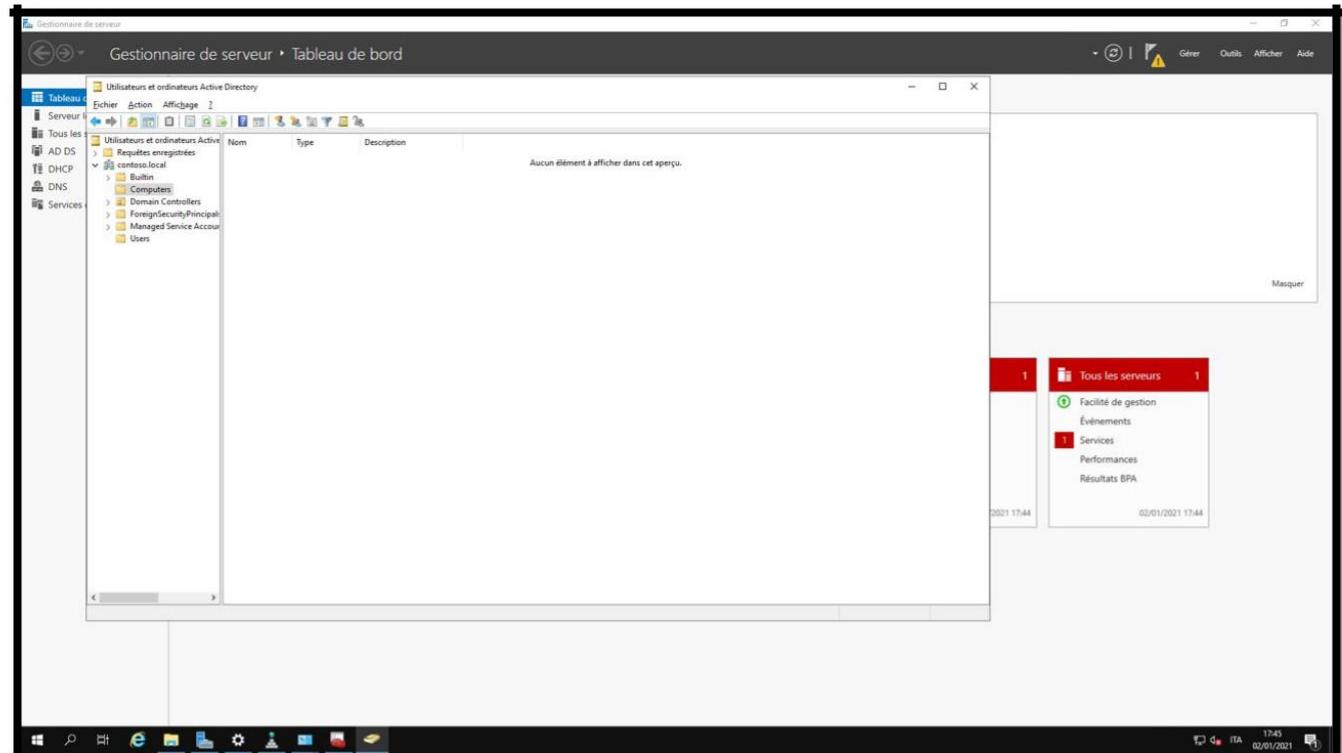


## Création d'un utilisateur sur le contrôleur de domaine

Une fois AD DS créé, nous pouvons procéder à l'ajout d'utilisateurs au domaine.  
Depuis ce menu, on cliquera sur : "**Utilisateurs et ordinateurs Active Directory**"



"Utilisateurs et ordinateurs Active Directory" est l'ensemble des objets qui font partie du domaine, au sein du domaine nous avons donc une série d'objets / conteneurs. L'un des conteneurs les plus importants est "user", qui contiendra tous les utilisateurs que nous configurerions sur notre contrôleur de domaine, qui seront alors les utilisateurs utilisés par le PC faisant partie du domaine



On peut donc en déduire que tout est centralisé, on peut configurer tous les utilisateurs du réseau dans cette "console".

Vous pouvez ajouter d'autres conteneurs, appelés « unités d'organisation » pour mieux organiser les services AD DS.

Dans ce cas à titre d'exemple, nous avons créé l'utilisateur BTS Sio.

Il suffit alors de créer un nouvel utilisateur (il est également possible de créer une "unité organisationnelle" distincte comme cela a été fait dans ce cas) en faisant un clic droit sur "nouvel" "utilisateur".

Ensuite, vous pouvez entrer votre nom, prénom et nom d'utilisateur (le nom de domaine est automatiquement entré).

Nouvel objet - Utilisateur X

Créer dans : contoso.local/customs users folder

Prénom :	bts	Initiales :	sio
Nom :			
Nom complet :	bts sio		
Nom d'ouverture de session de l'utilisateur :			
btssio		@contoso.local	
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :			
CONTOSO\		btssio	

[< Précédent](#) [Suivant >](#) [Annuler](#)

---

[Retour au  
Sommaire](#)

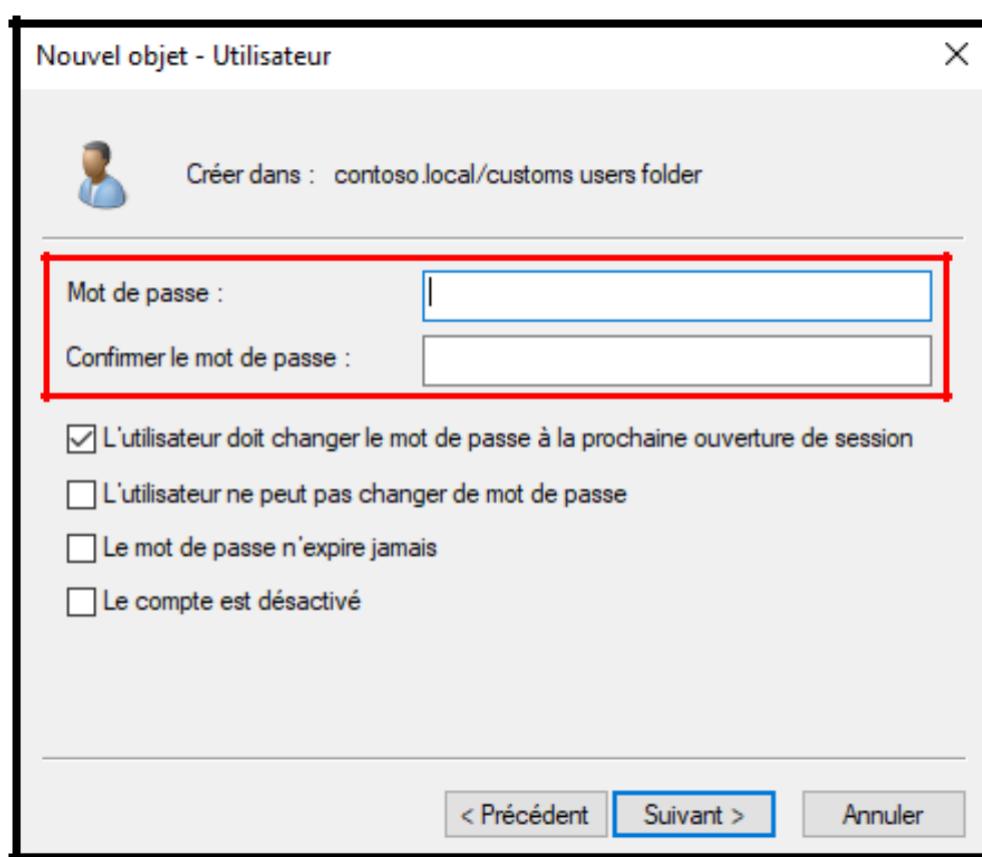


Vous devrez donc définir un mot de passe qui doit répondre aux exigences de mot de passe du contrôleur de domaine Microsoft, puis :

- ✓ Huit caractères minimums
- ✓ Une minuscule minimum
- ✓ Une majuscule minimum
- ✓ Un numéro minimum
- ✓ Il ne doit pas y avoir plus de 3 caractères égaux au nom ou au prénom.

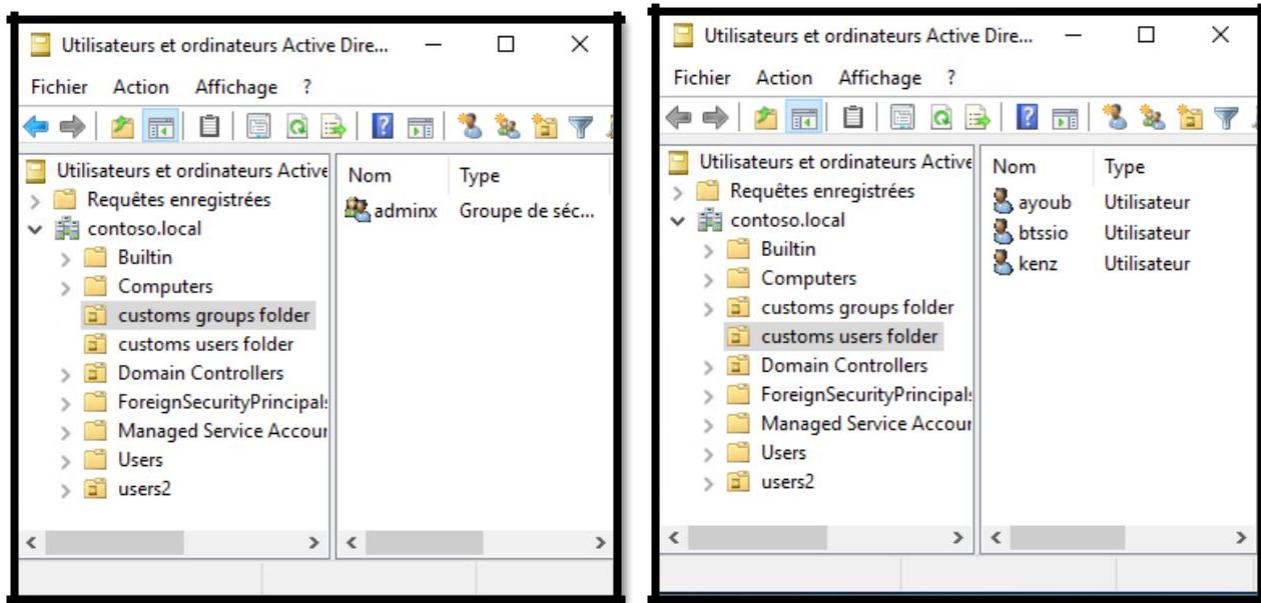
Il serait souhaitable de laisser le consentement pour changer le mot de passe lors du prochain accès, pour des raisons évidentes de sécurité.

Il suffira donc de cliquer sur « suivant » et « terminer » pour ajouter l'utilisateur.



[Retour au Sommaire](#)

L'icône d'un utilisateur est un "petit homme" tandis que l'icône du groupe est composée de "2 petits hommes".

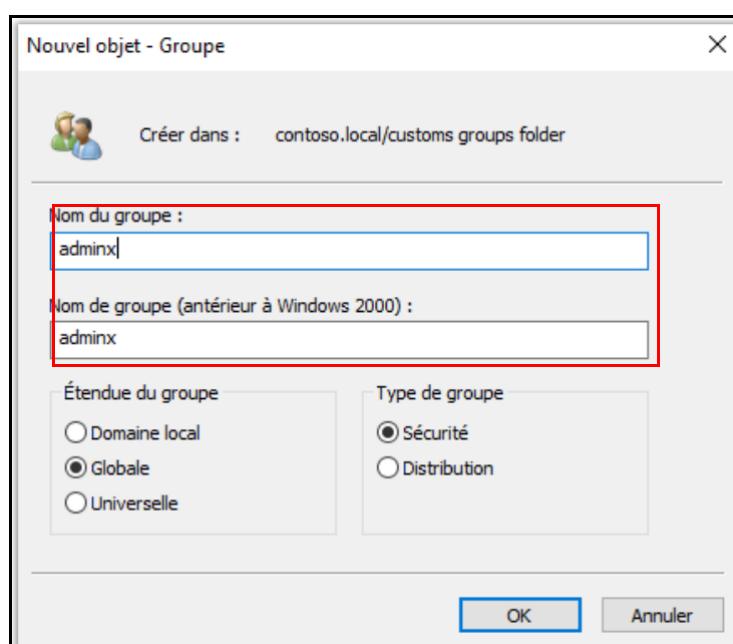


Nous pouvons également créer des groupes.

L'utilisation des groupes est bientôt bien expliquée :

En supposant une entreprise de 1000 employés, dont, à titre d'exemple, 100 utilisateurs sont des techniciens qui doivent tous fonctionner avec des règles spécifiques, il faudrait trop de temps pour personnaliser 100 utilisateurs un par un. Avec les groupes, ce "problème" est résolu. En fait, nous pouvons créer un groupe spécifique avec des paramètres spécifiques, puis associer les 100 travailleurs à un groupe spécialement créé.

Il sera évidemment possible d'associer plus de groupes à un utilisateur spécifique.



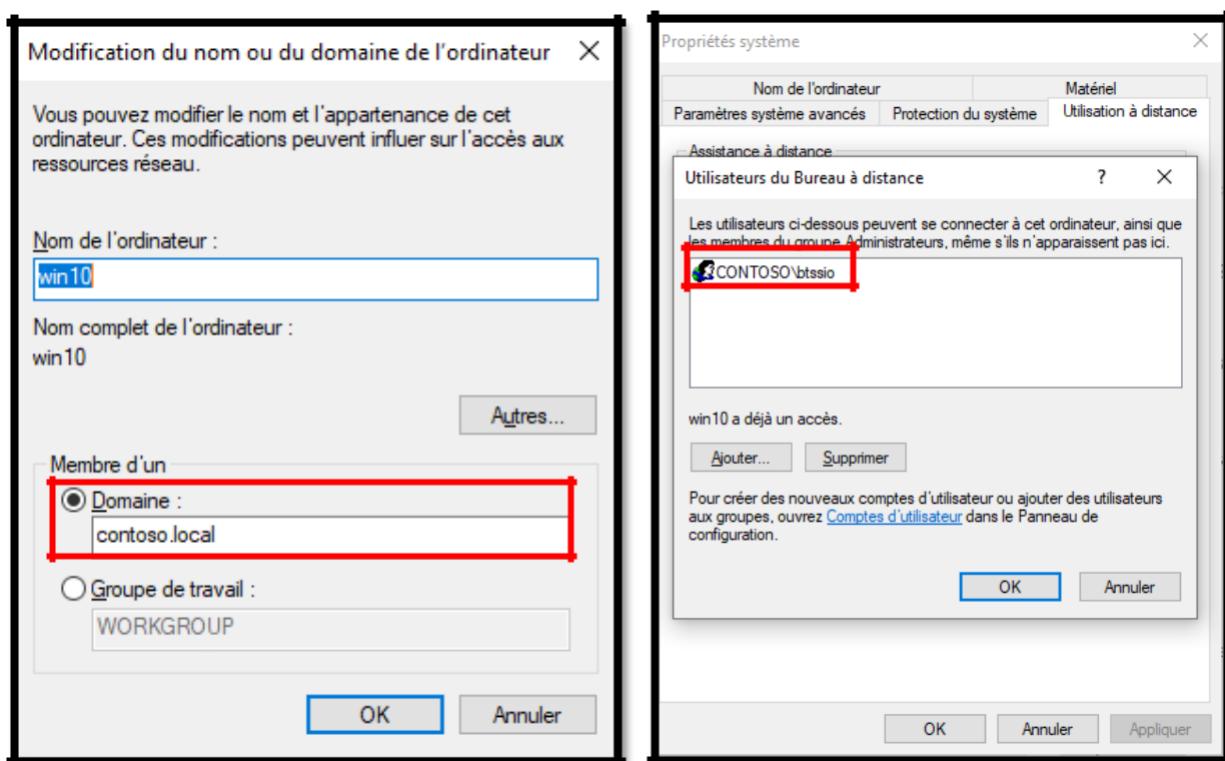
## Configurer la machine « client » sur le domaine précédemment défini.

Pour ajouter une machine au domaine vous devez : cliquez sur l'icône Windows en bas à gauche, puis allez dans "paramètres" puis "à propos de votre pc" "renommer ce pc" puis cliquez sur "modifier" et entrez dans le groupe de travail précédemment créé.

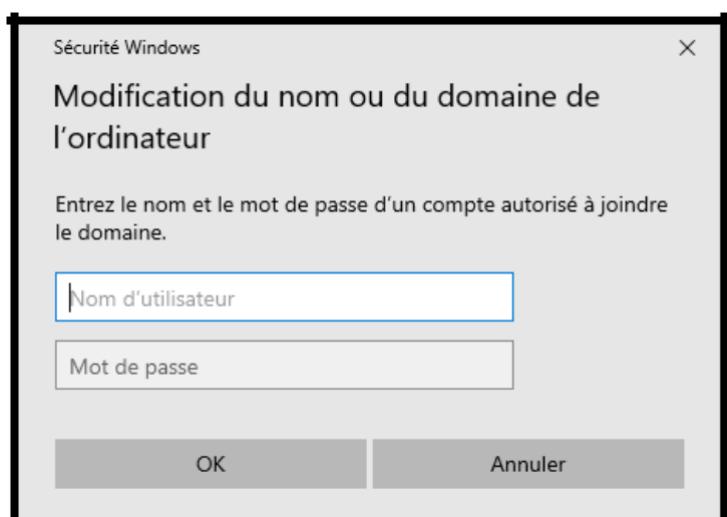
Avant d'effectuer cette opération, il est nécessaire de définir l'adresse IP du serveur précédemment définie comme DNS.

Évidemment, si l'adresse IP du contrôleur de domaine précédemment créée n'a pas été définie comme DNS, ce PC ne pourra pas résoudre le contrôleur de domaine

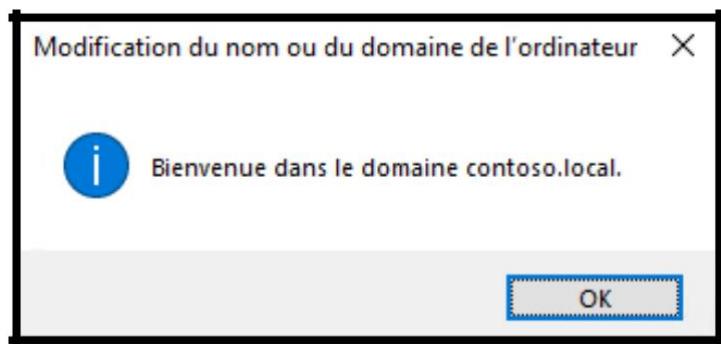
Dans cet exemple, l'utilisateur btssio précédemment créé a été utilisé.



à Ce stade, nous devons simplement entrer les informations d'identification pour ajouter ce PC au contrôleur de domaine



Une fenêtre de confirmation s'affichera ensuite.



Il est donc possible de vérifier que ce pc est associé au contrôleur de domaine simplement en vérifiant depuis la capture d'écran ci-dessous.

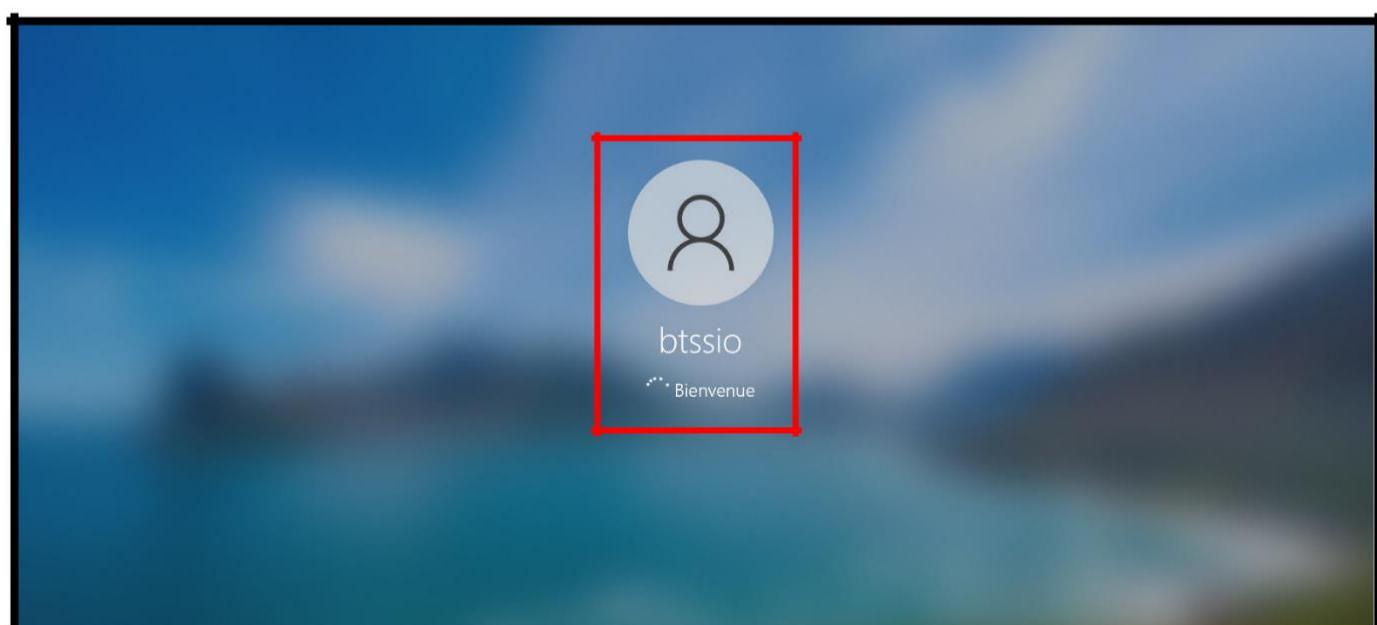
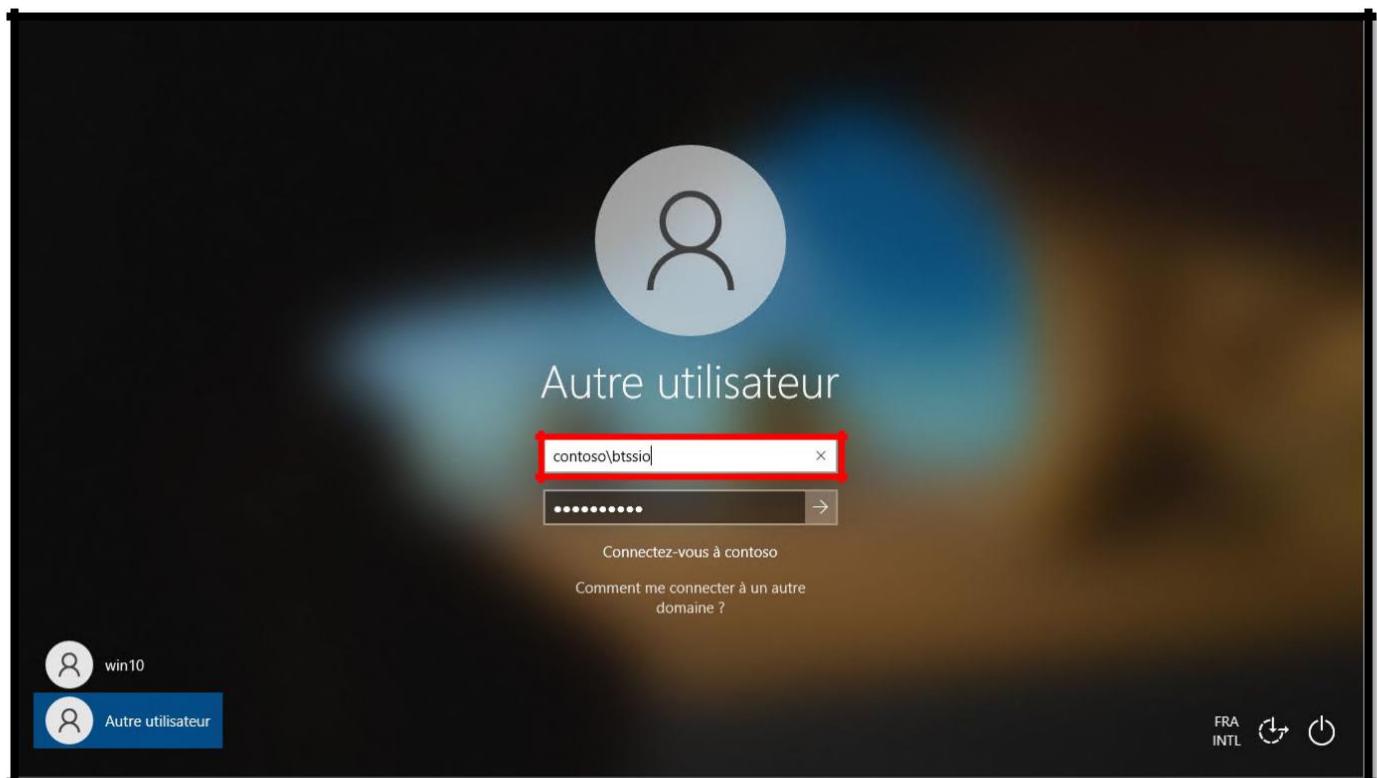
Nom de l'appareil	win10
Nom complet de l'appareil	win10.contoso.local
Processeur	AMD Ryzen 5 3600 6-Core Processor 3.60 GHz
Mémoire RAM installée	2,24 Go
ID de périphérique	8B536AF4-7994-4982-885E-0B98A2A2034C
ID de produit	00330-80000-00000-AA095
Type du système	Système d'exploitation 64 bits, processeur x64
Stylet et fonction tactile	La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran

**Spécifications de Windows**

Édition	Windows 10 Professionnel
Version	20H2
Installé le	02/01/2021

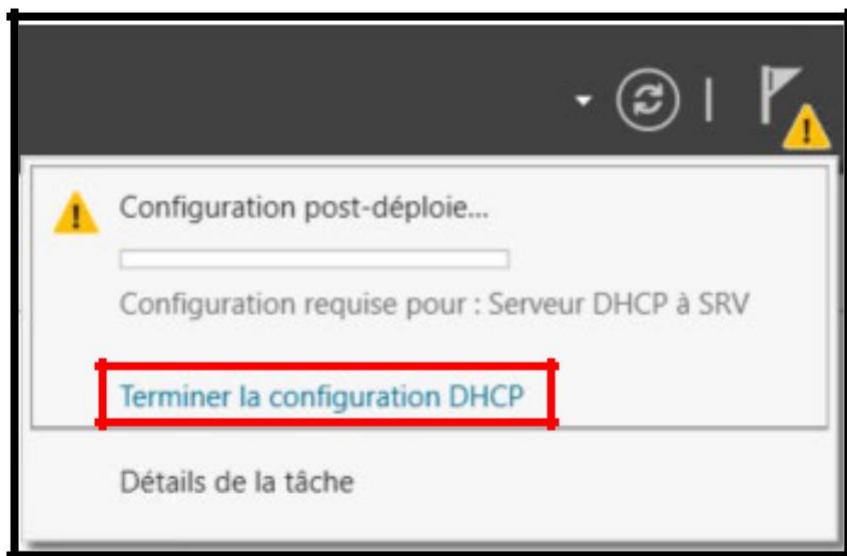
Au redémarrage, vous pouvez accéder en vous connectant directement avec l'utilisateur souhaité. Donc, dans ce cas, nous nous connecterons avec le compte contoso \ btssio dont :

- ✓ **contoso**: est le nom de domaine
- ✓ **btssio**: le nom de l'utilisateur

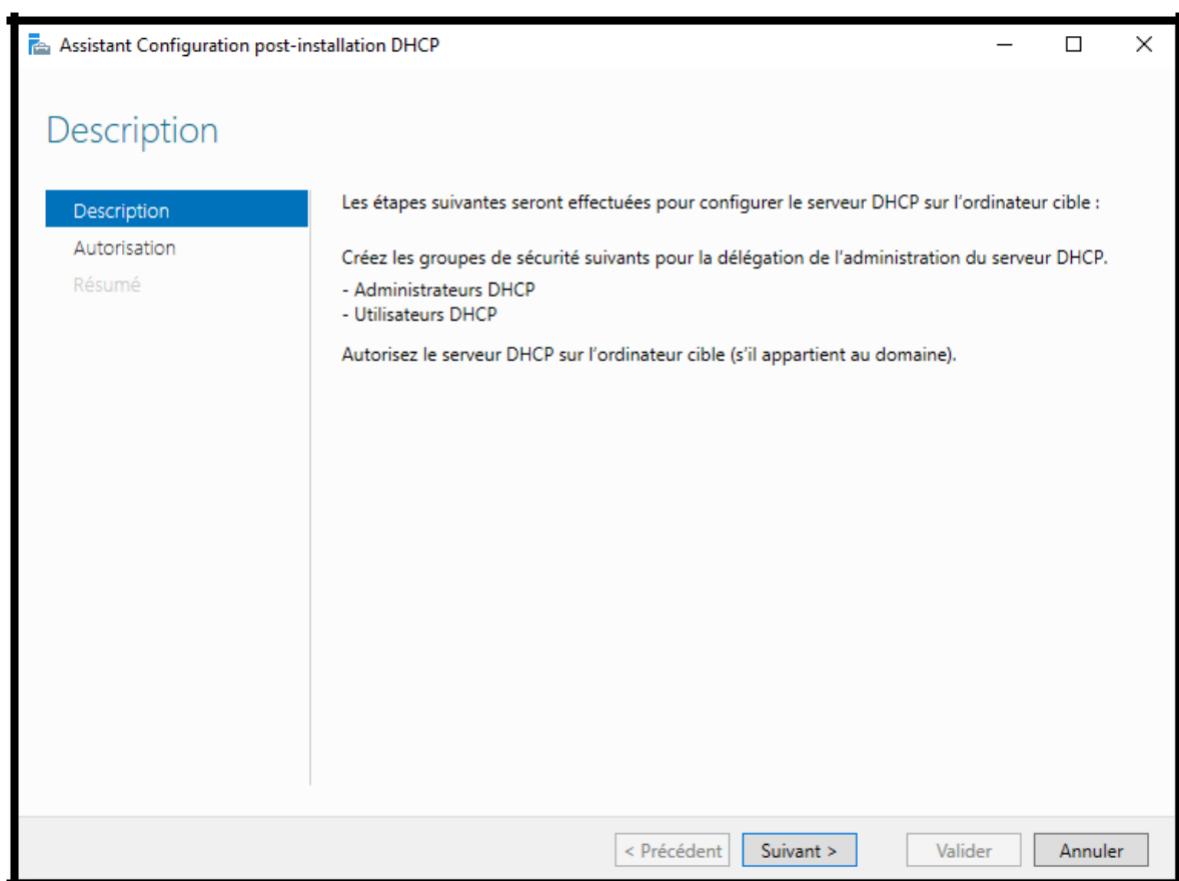


## Configuration DHCP

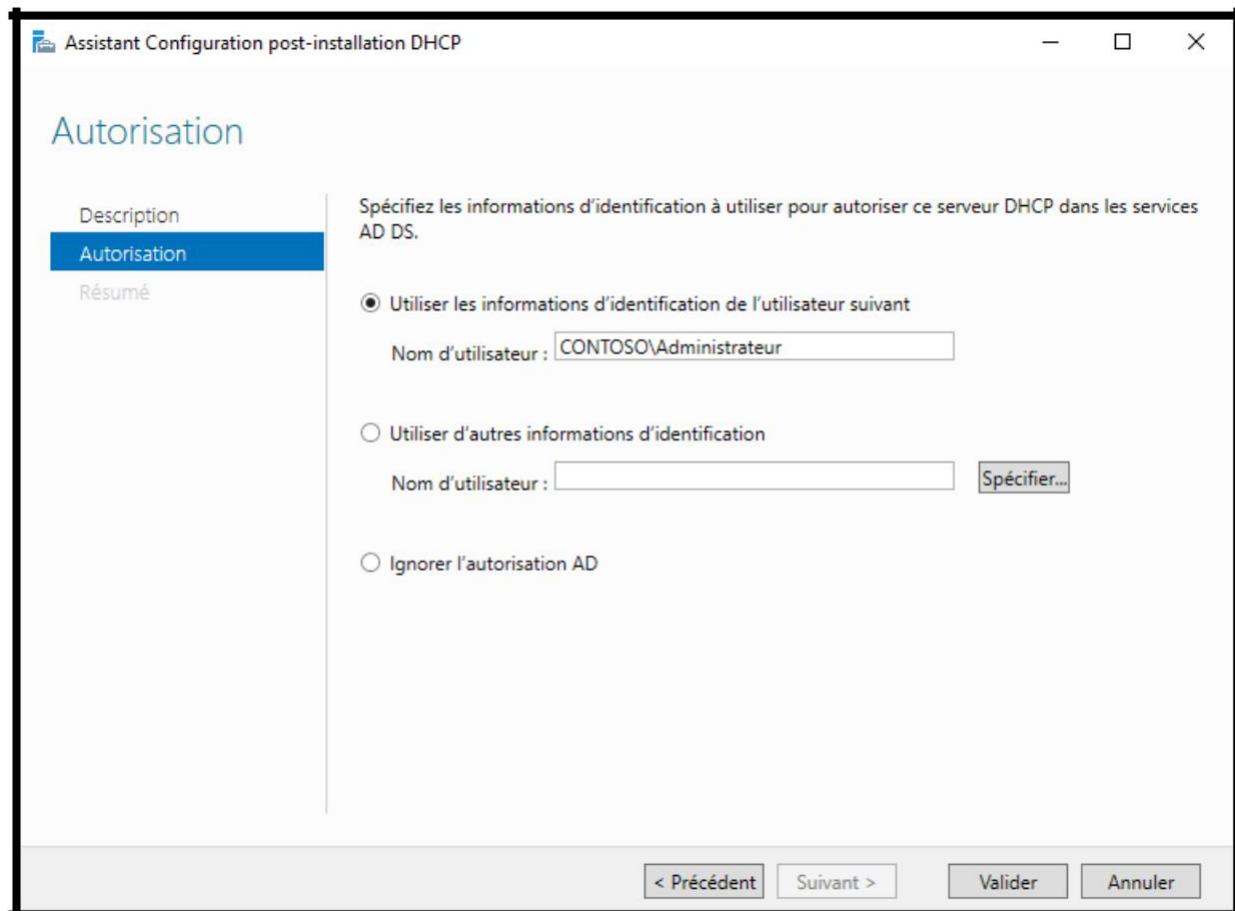
Dans ce chapitre, nous allons configurer le serveur DHCP nouvellement installé.  
Ensuite, nous irons cliquer sur "Terminer la configuration DHCP"



Nous aurions donc cette fenêtre initiale.

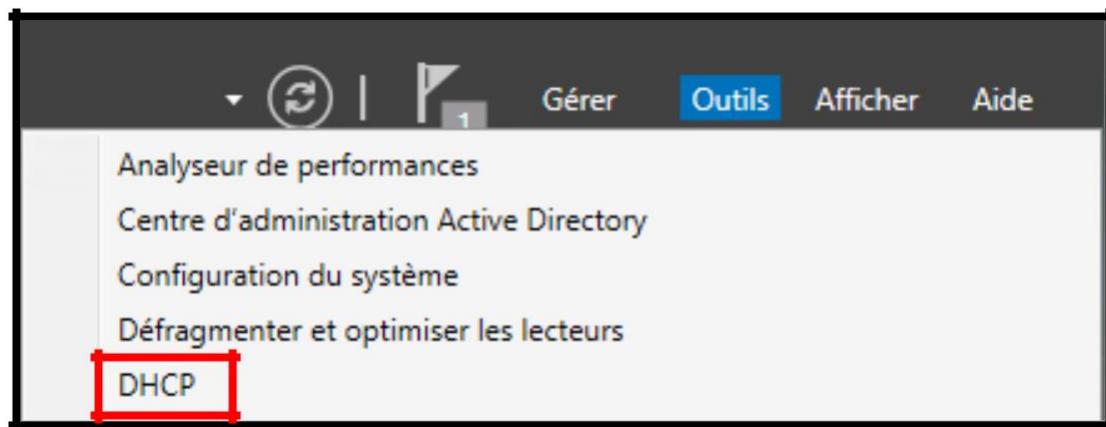


Après cela, nous pouvons choisir de créer le serveur DHCP à partir d'un domaine déjà existant ou non. L'autorisation AD peut également être ignorée. Dans tous les cas, il est généralement recommandé d'avoir un serveur DHCP avec un serveur DNS et AD DS attachés.



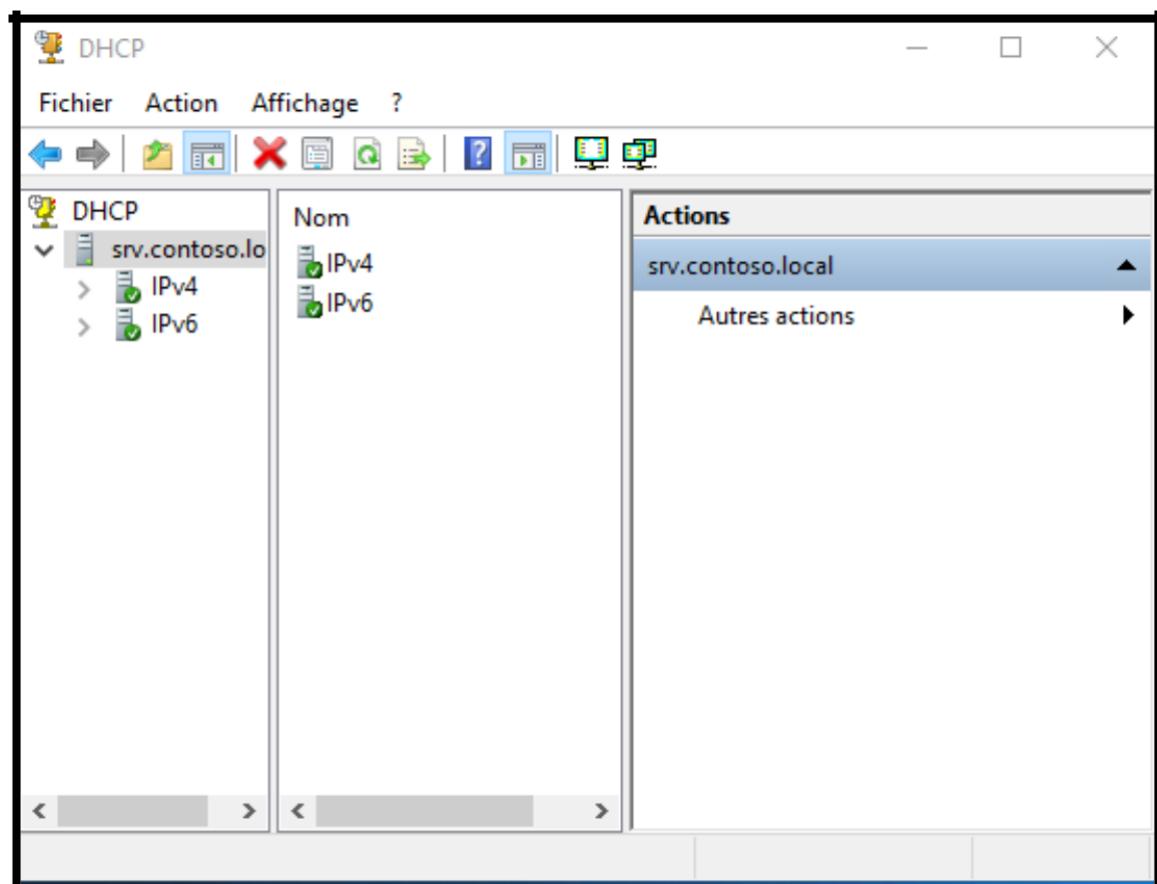
À Ce stade, le serveur DHCP est installé sur notre serveur, nous devons maintenant passer à la configuration, à l'étape suivante.

Toujours depuis le menu "outils". Cliquez sur « DHCP » pour aller configurer le serveur DHCP :

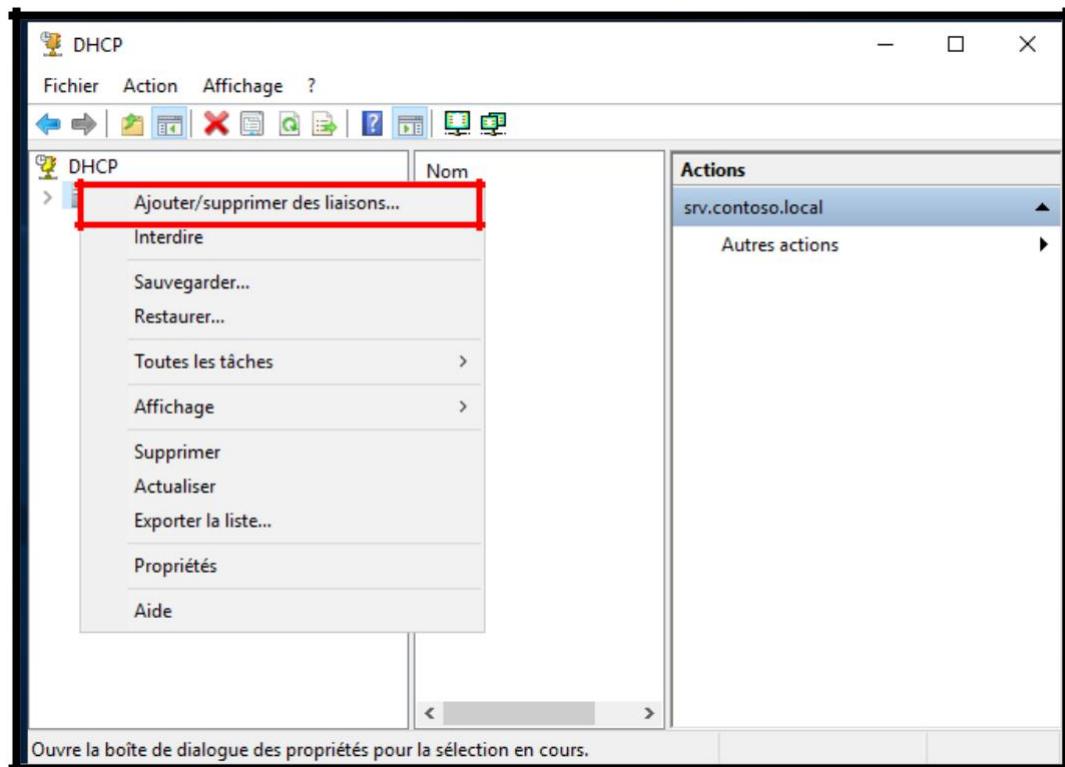


Dans la console, on peut donc voir les deux sections ipv4 et ipv6

Dans notre cas, nous traiterons de la configuration d'ipv4, mais la configuration d'ipv6 peut également être définie. IPv4 dans un réseau local est généralement plus que suffisant.

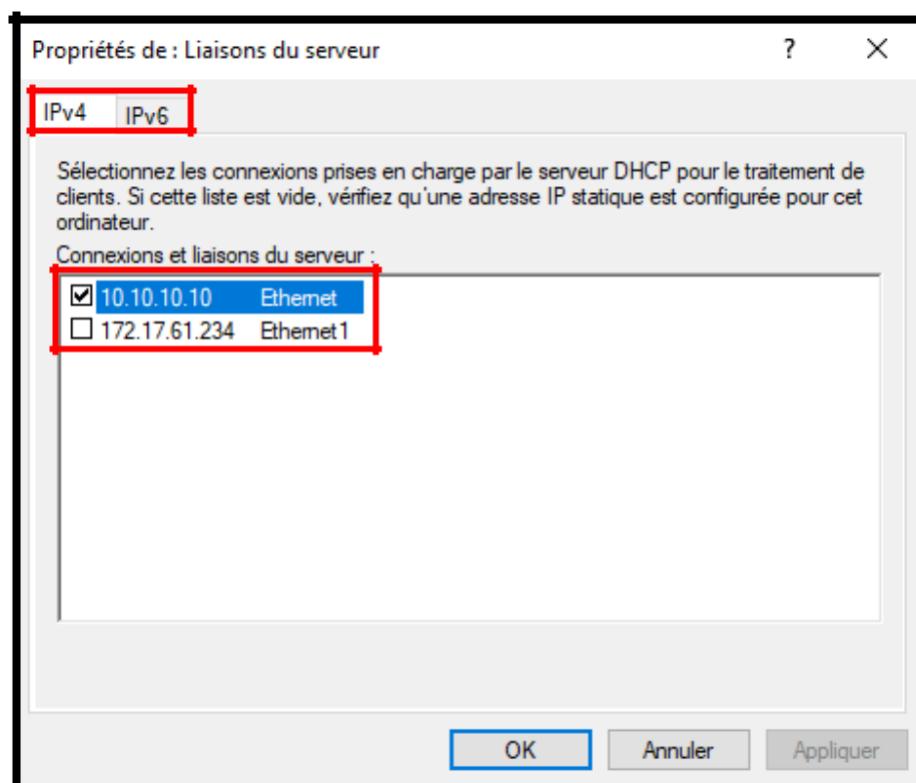


Clic droit, puis "Ajouter / supprimer des liaison"

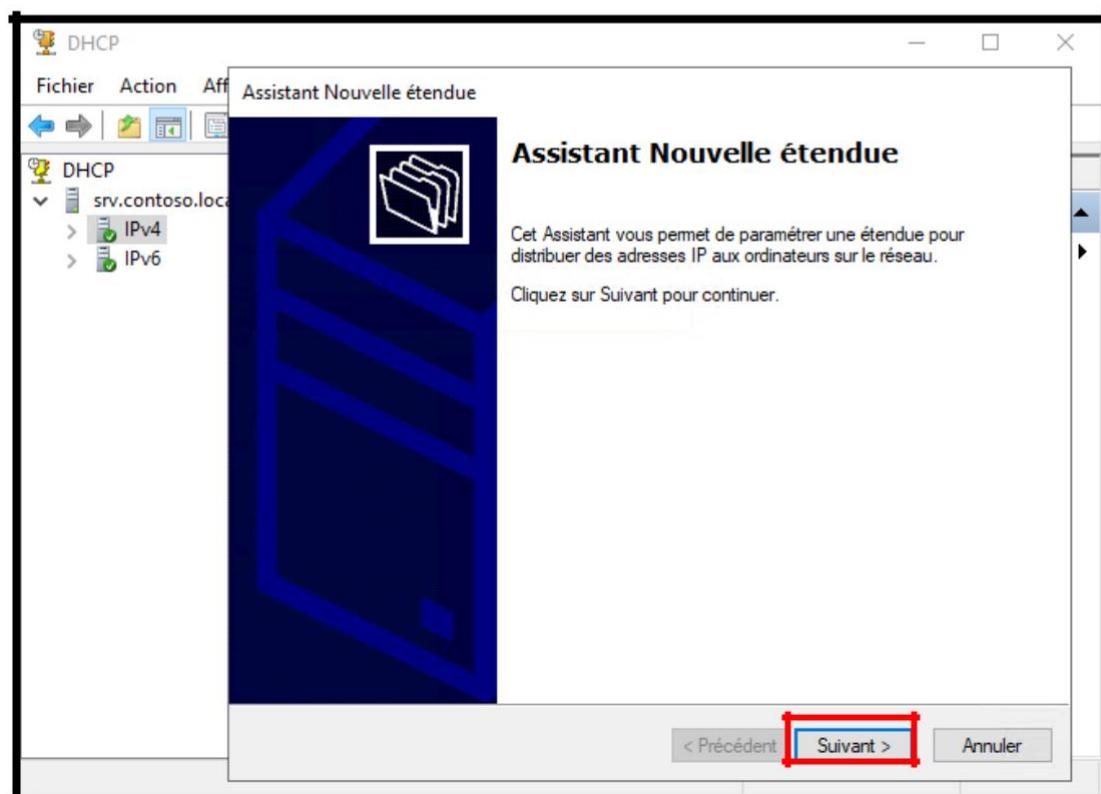
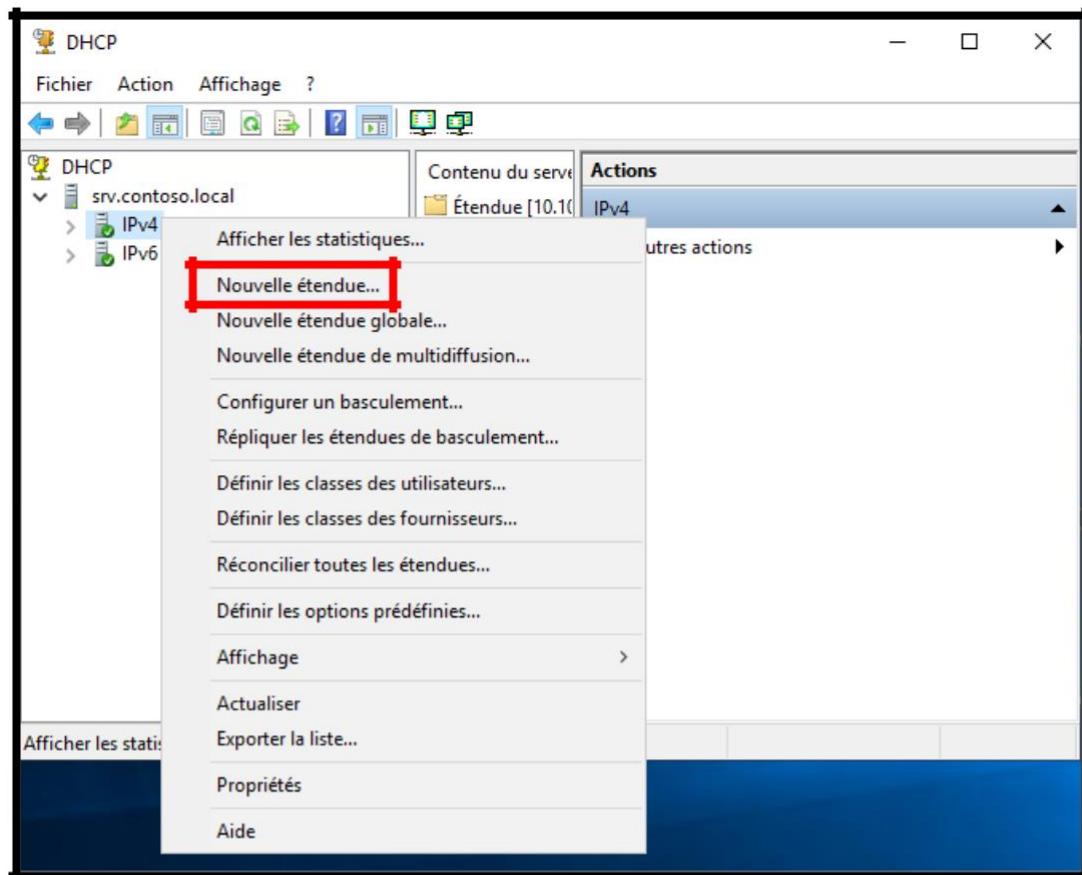


Ici, toutes les connexions réseau seront affichées, nous allons donc choisir la carte réseau que nous avons choisi.

Bien sûr, nous pouvons choisir à la fois ipv4 et ipv6

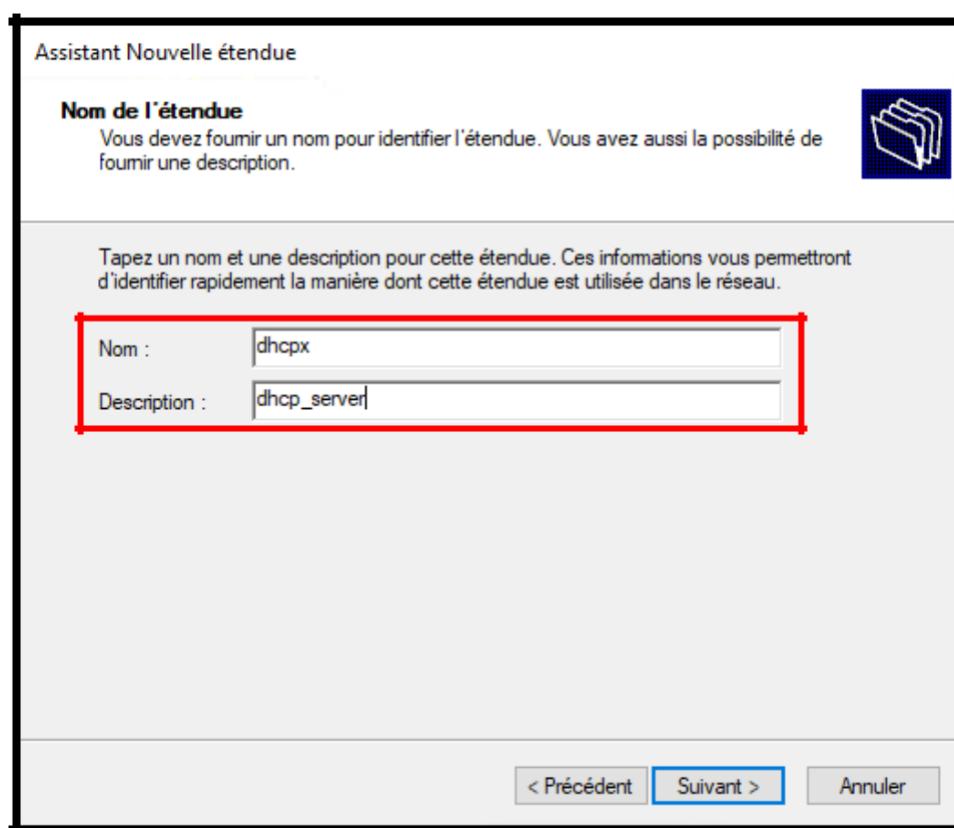


Depuis cette fenêtre, nous cliquons sur "Nouvelle étendue"



[Retour au Sommaire](#)

Nous avons la possibilité de donner un nom et une description au serveur DHCP :  
Ce sera alors le nom affiché dans la console une fois la configuration terminée

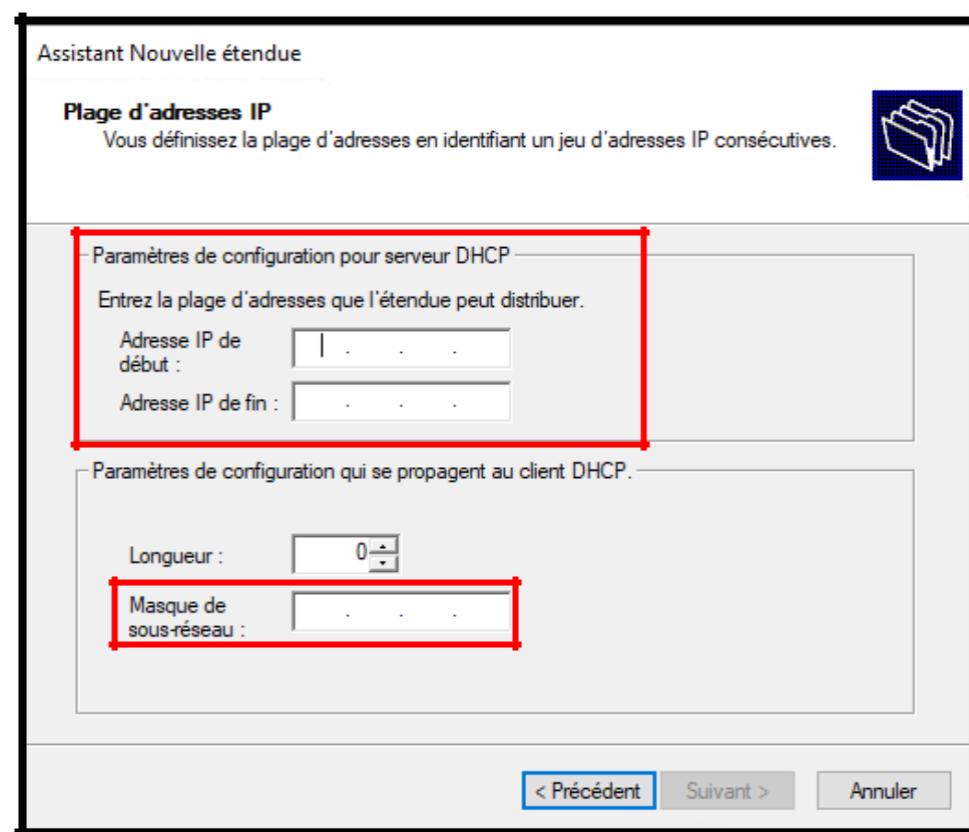


Ici, il nous demande la plage IP à attribuer aux périphériques clients. Donc si par exemple on insère la plage d'IP 10.10.10.100 (adresse IP de début) et 10.10.10.200 (adresse IP finale); cela signifie que 101 adresses IP peuvent être attribuées.

On ira donc aussi paramétriser la masque de sous-réseau (subnet\_mask en anglais).

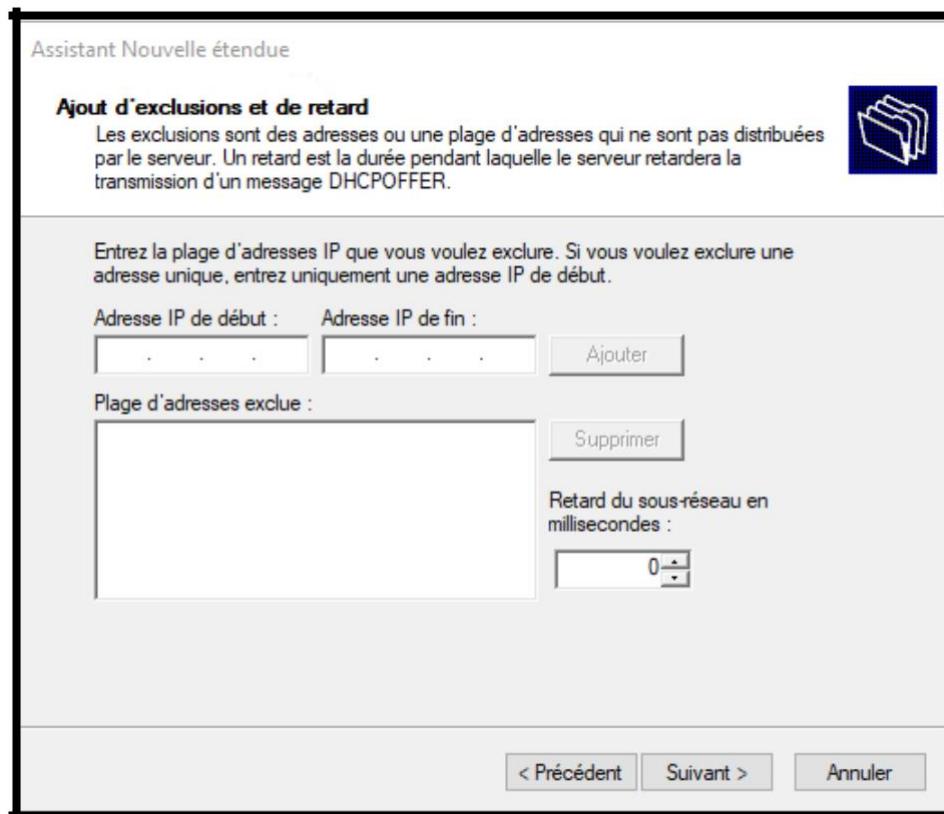
Evidemment, cette configuration doit être réglée en fonction des paramètres définis dans notre carte réseau.

La longueur du masque sera attribuée automatiquement en fonction du sous-réseau





Il est possible d'exclure une plage d'adresses IP. La raison est bientôt expliquée : par exemple dans un réseau, il est nécessaire d'avoir des adresses IP fixes pour des appareils spécifiques qui doivent avoir une adresse IP statique. C'est le cas par exemple d'une imprimante réseau, d'un scanner réseau, d'un IP-camera ou de tout appareil nécessitant une route statique.



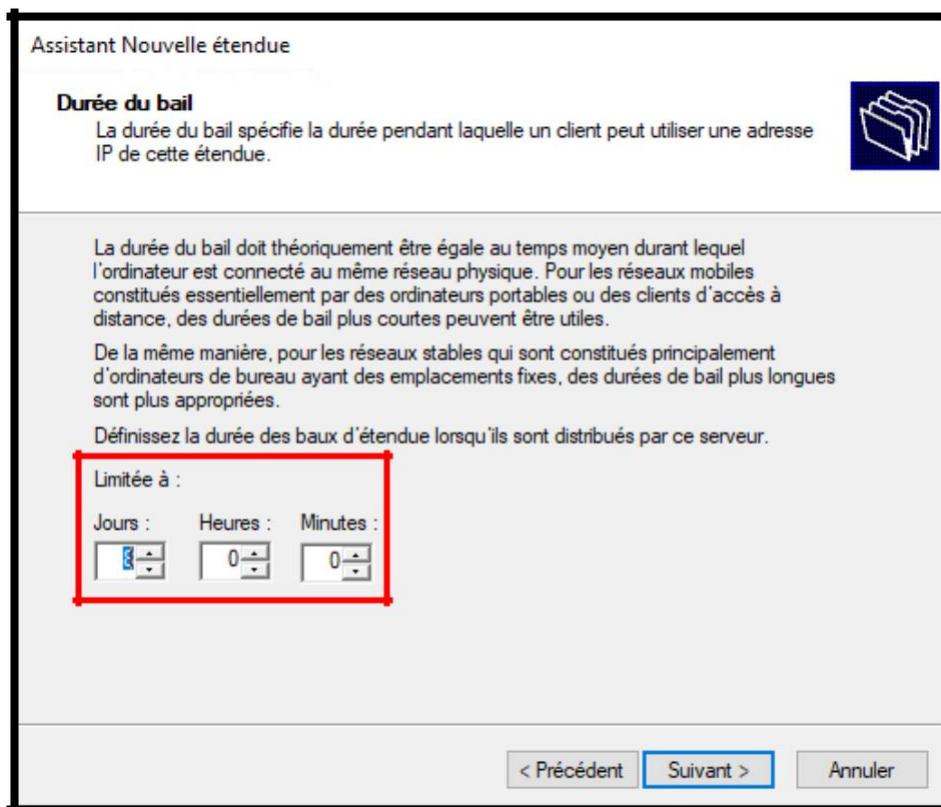
Dans cette fenêtre, nous pouvons choisir la durée du bail.

C'est donc le nombre de jours / heures / minutes que le serveur conservera la même adresse IP pour un appareil spécifique.

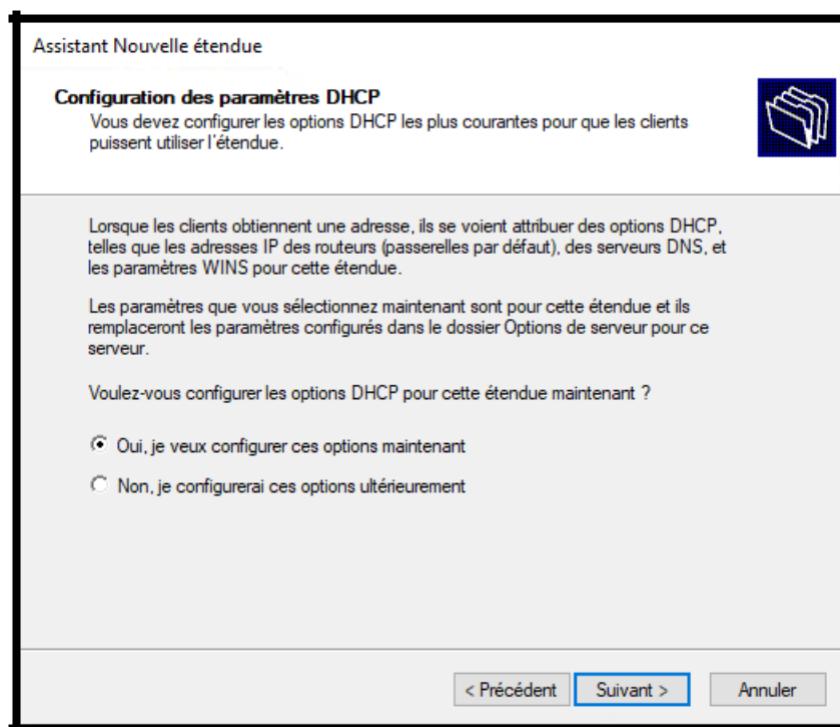
Cela signifie que si un appareil est connecté à notre serveur, ce même appareil (qui est reconnu par l'adresse MAC) conservera la même adresse IP pour les jours / heures / minutes précédemment définis.

Ainsi, après x jours / heures / minutes prédefinis, il sera susceptible de changer l'adresse IP qu'il avait précédemment, car il aura évidemment libéré l'adresse précédente.

Par exemple, s'il s'agit d'un réseau public, il est conseillé de fixer un bail court pour des raisons évidentes.

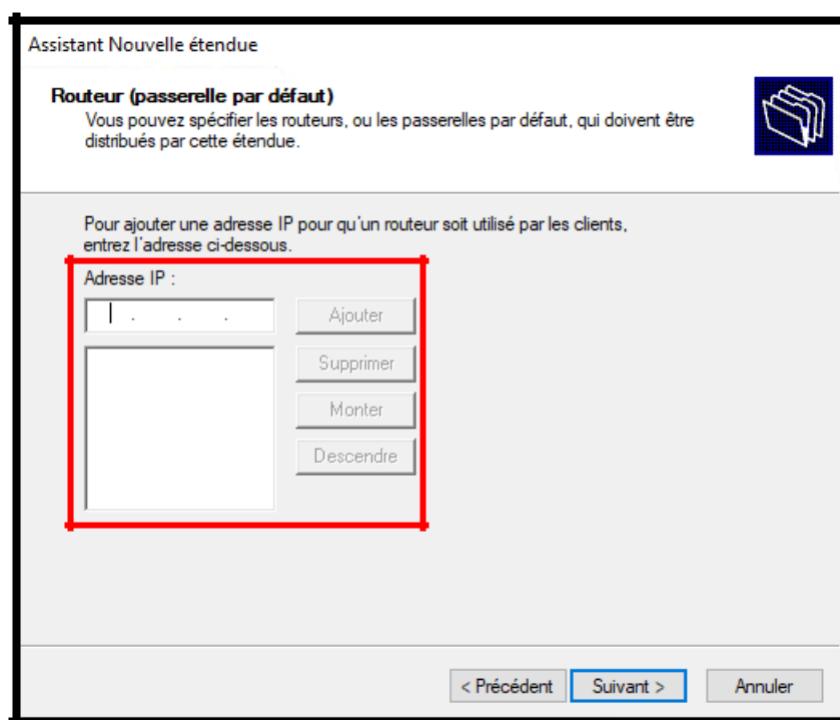


Dans cette fenêtre, il nous est demandé si vous souhaitez procéder à la configuration d'autres paramètres.

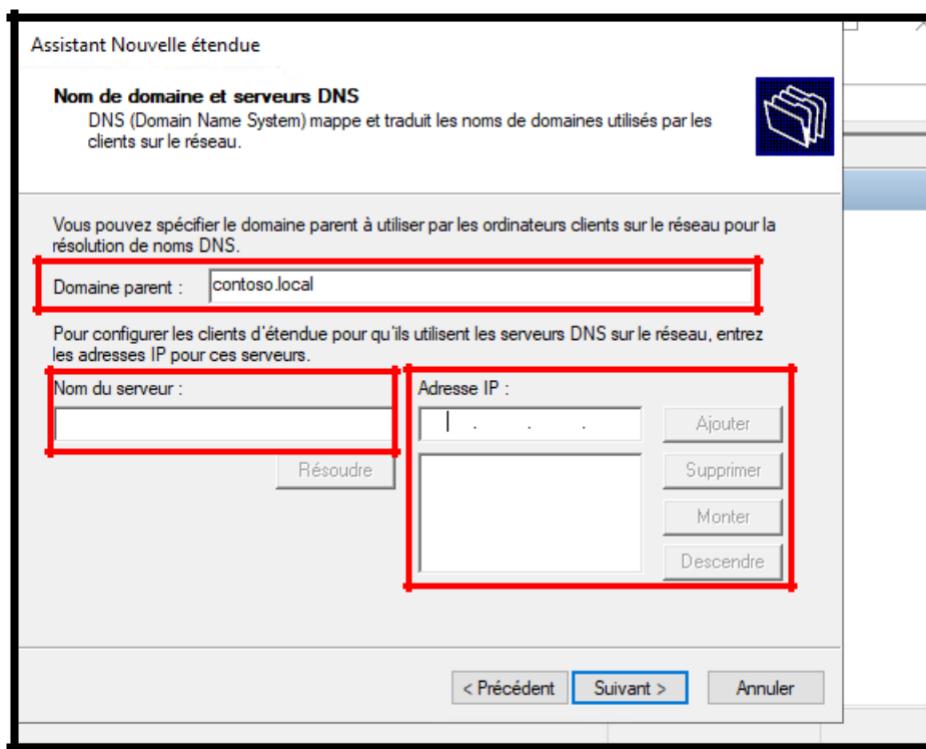


Il demande si je veux ajouter une passerelle (Gateway en anglais).

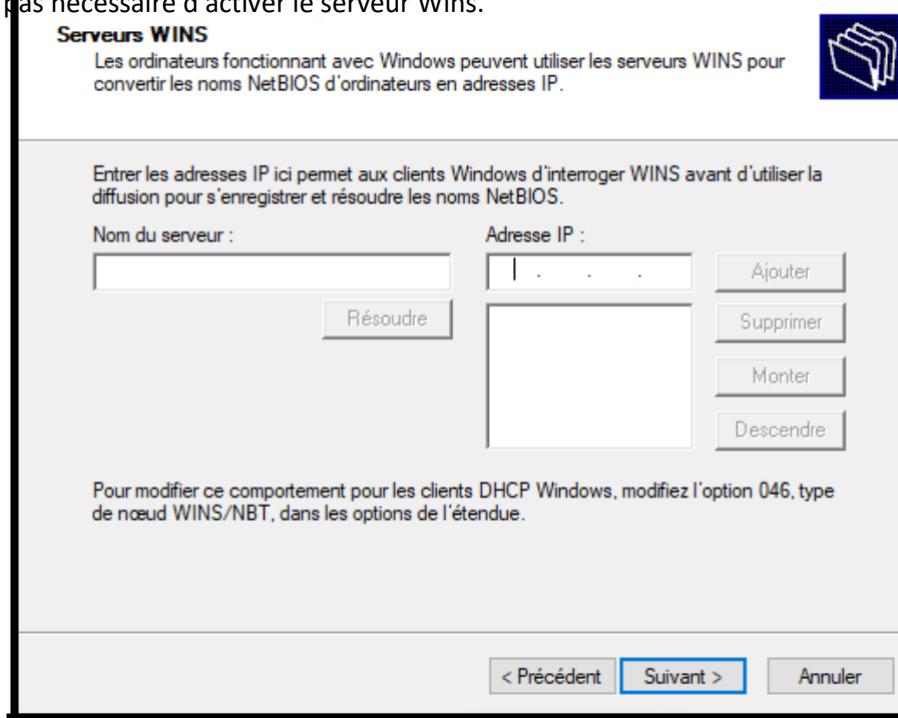
Dans le cas où il s'agit d'un réseau interne qui n'a pas besoin d'accès à Internet, la passerelle est facultative.



On peut donc décider ici d'entrer ou non le domaine parent. Donc aussi le nom du serveur.

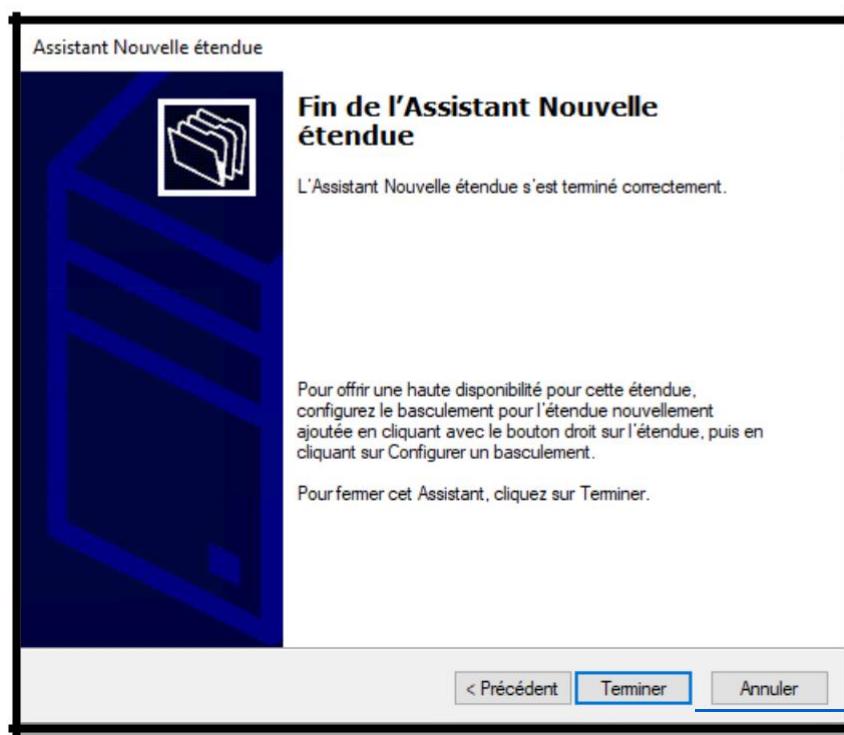
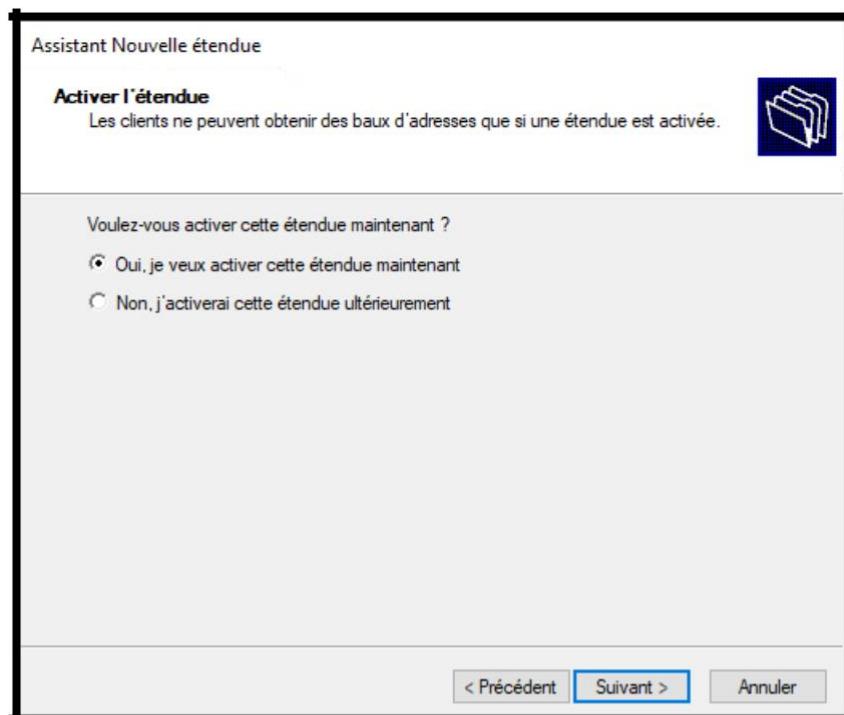


Nous pouvons choisir d'activer le serveur Wins. N'oubliez pas que Wins est une résolution de nom qui était auparavant utilisée sur les clients plus anciens. Dans les nouveaux systèmes, il n'est généralement pas nécessaire d'activer le serveur Wins.



[Retour au  
Sommaire](#)

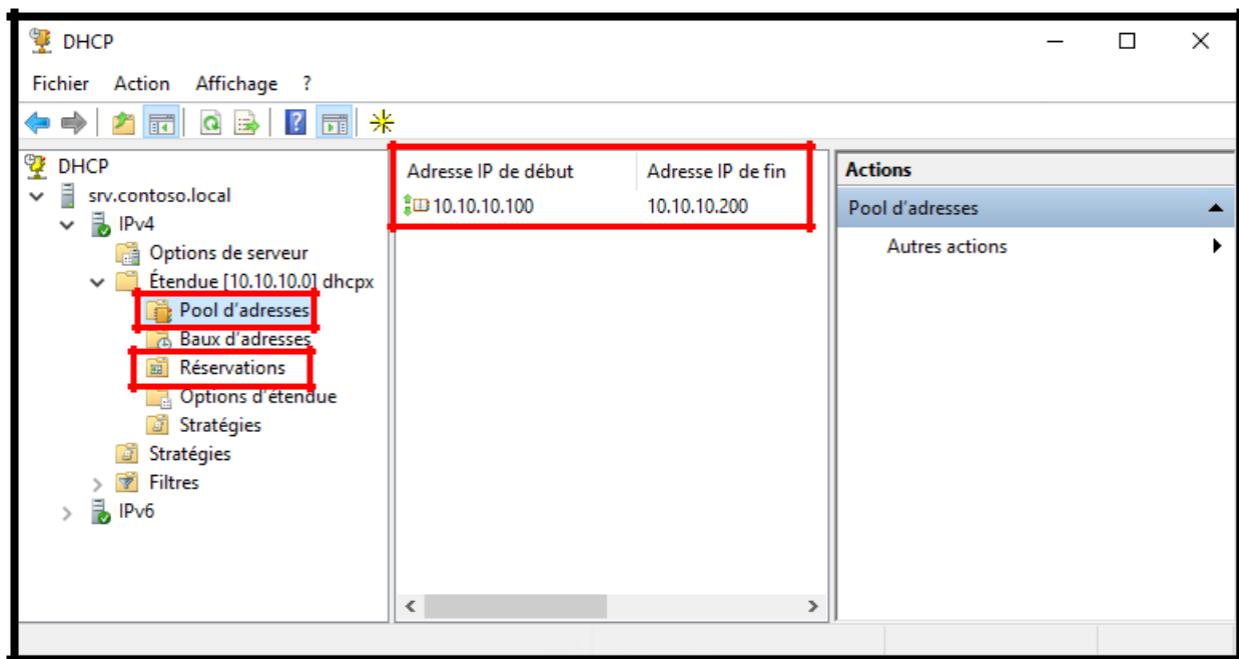
Dans cette fenêtre, il vous est demandé si vous souhaitez activer le serveur immédiatement ou non.  
À ce stade, nous pouvons ensuite terminer la configuration nouvellement créée.



[Retour au  
Sommaire](#)

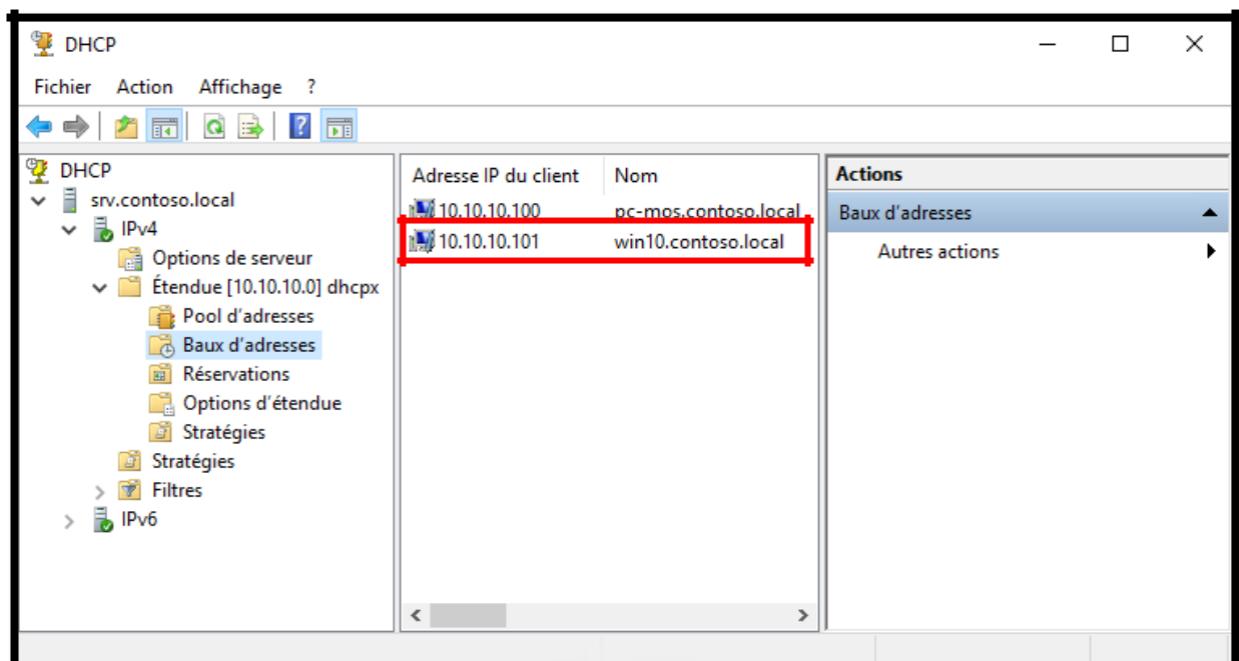
Nous avons donc dans cette fenêtre le pool d'adresses IP qui peuvent être attribuées, donc la plage d'utilisation. Dans notre cas, nous avons préalablement configuré la plage : du 10.10.10.100 au 10.10.10.200

Dans le dossier « Réservations », il est possible de paramétriser les appareils avec une adresse IP fixe, spécifiant ainsi le nom de la réservation, l'adresse IP et l'adresse MAC.



Dans ce cas, nous pouvons identifier la machine cliente qui a déjà pris l'adresse IP automatiquement (win10.cotoso.local)

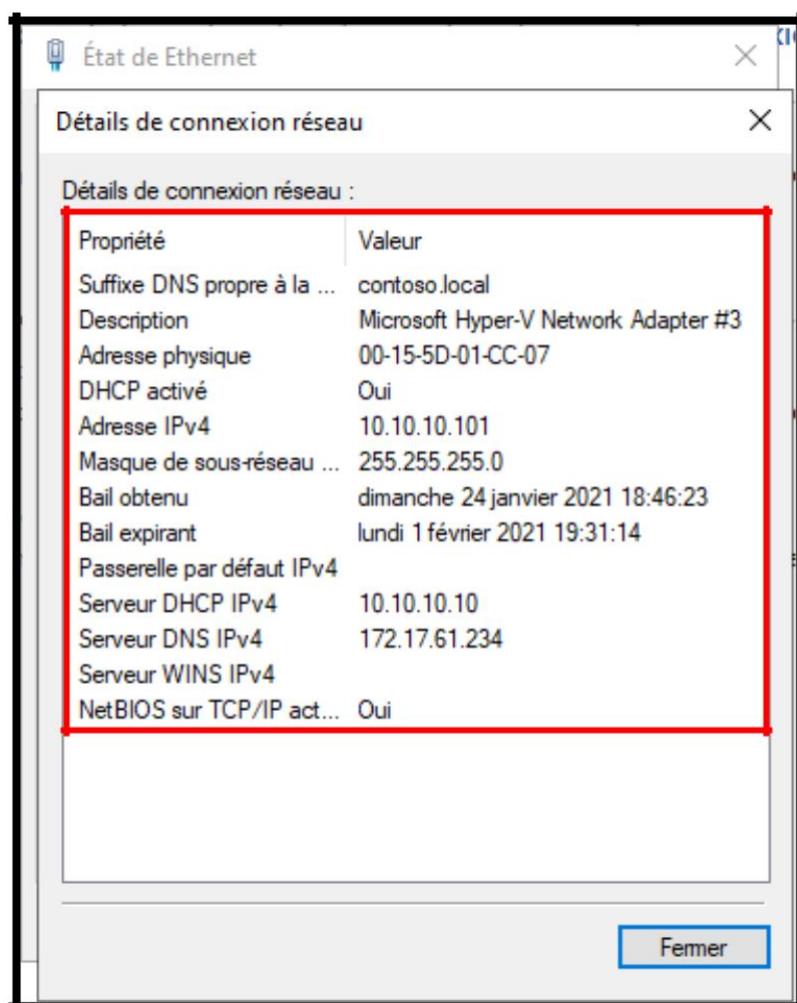
Évidemment, dans la machine cliente, il sera nécessaire de définir comme DNS, l'adresse IP de notre carte réseau sur laquelle le serveur DHCP est défini.



Il s'agit de l'écran de détail de la carte réseau du PC client qui a pris l'adresse IP 10.10.10.101 (il fait donc partie de la plage d'adresses IP précédemment créée)

Depuis cette fenêtre, nous pouvons ensuite vérifier quelques détails :

- ✓ Notre adresse IP 10.10.10.101
- ✓ Adresse DNS (de notre serveur DHCP)
- ✓ Les détails du BAIL (date d'obtention et d'expiration)
- ✓ L'adresse Mac de notre PC
- ✓ Notre adresse MAC



## Mettre en place de stratégie de groupe

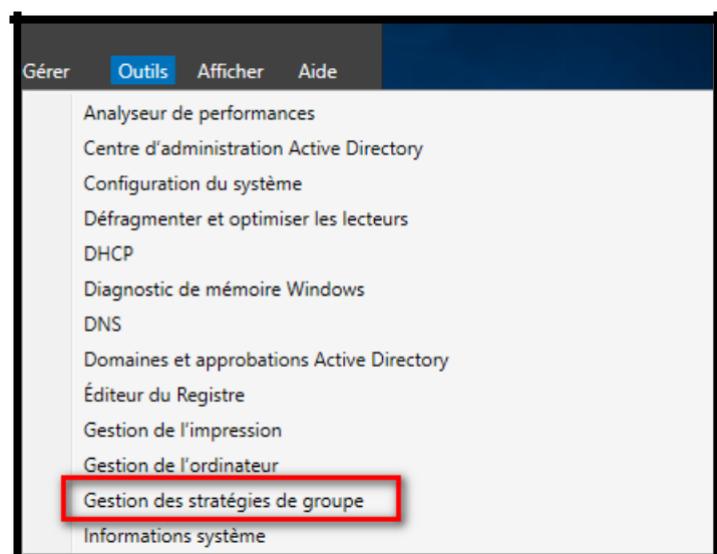
Les stratégies de groupe (en anglais, Group Policy ou GP) sont un ensemble de règles qui contrôlent l'environnement de travail des utilisateurs et des ordinateurs. Ils fournissent une gestion et une configuration centralisées des systèmes d'exploitation, des applications et des paramètres utilisateur dans un environnement Active Directory.

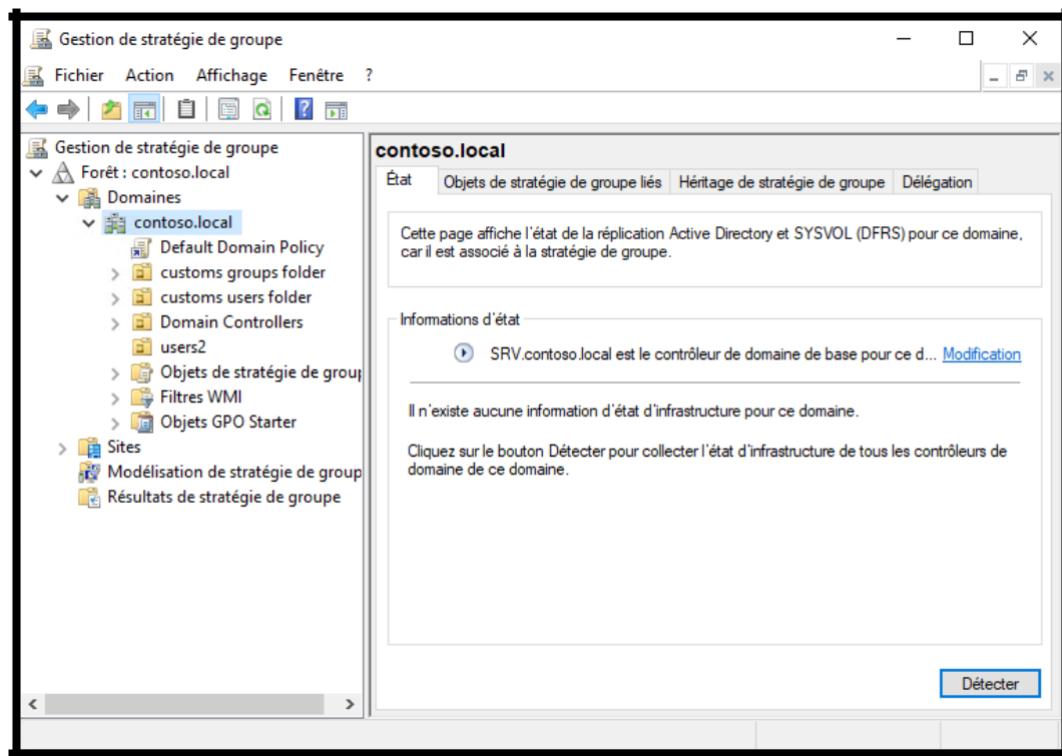
En d'autres termes, les stratégies de groupe contrôlent en partie ce que les utilisateurs peuvent et ne peuvent pas faire sur un système informatique. Bien que les stratégies de groupe soient le plus souvent utilisées pour les environnements d'entreprise, elles sont également courantes dans d'autres contextes tels que les écoles, les petites entreprises et d'autres types d'organisations. La stratégie de groupe est souvent utilisée pour restreindre certaines actions qui peuvent poser des risques de sécurité potentiels, par exemple : pour bloquer l'accès au gestionnaire de tâches, restreindre l'accès à certains dossiers, désactiver les téléchargements de fichiers exécutables, désactiver l'utilisation lecteurs externes (clés USB, disques optiques), etc.

Dans cet exemple, nous allons essayer de changer l'arrière-plan du bureau Windows à l'aide de la stratégie de groupe.

Dans ce cas ces opérations ont déjà été effectuées :

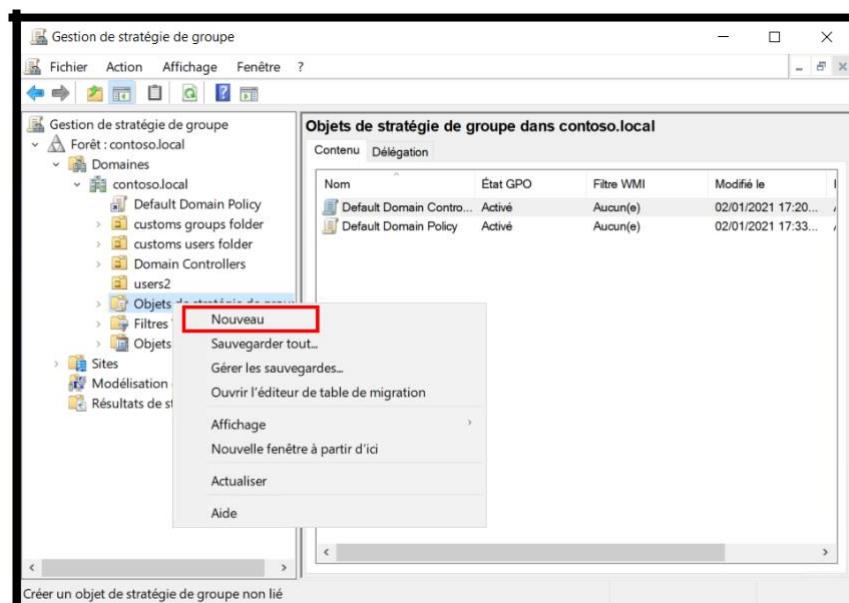
- ✓ Active Directory et le service DNS (Domain Name Service) ont déjà été configurés
- ✓ La machine client a été jointe au domaine
- ✓ La politique sera appliquée au niveau de l'utilisateur BTS Sio
- ✓ Le fichier image de papier peint est stocké sur. Un dossier partagé sur le réseau local. (`\|SRV\shared`)
- ✓ Le nom d'utilisateur cible est "BTS Sio" se trouve dans une unité d'organisation nommée : "Custom Policy".



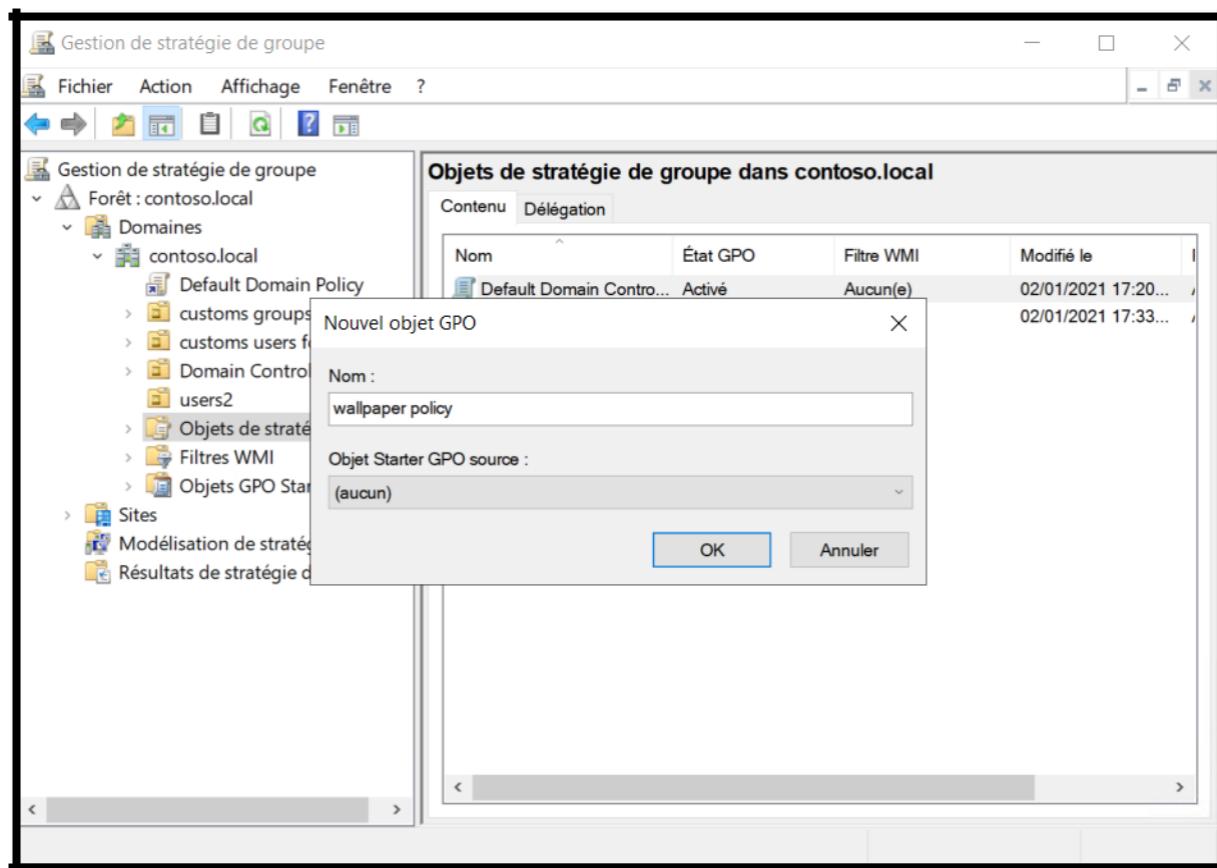


### Création de l'objet de stratégie de groupe :

Sur la console de gestion des stratégies de groupe, développez la forêt et le domaine, cliquez avec le bouton droit sur Objets de stratégie de groupe et sélectionnez "Nouveau"

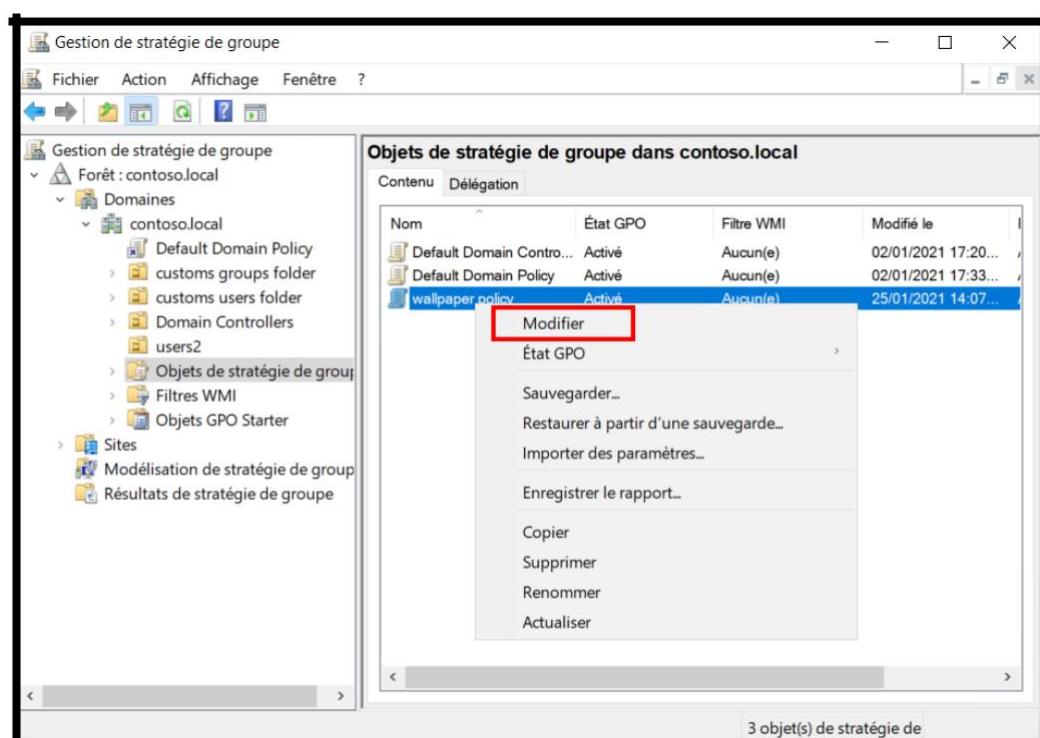


Nommez le nouvel objet de stratégie. Dans cet exemple, le nom de la politique est «Wallpaper Policy».

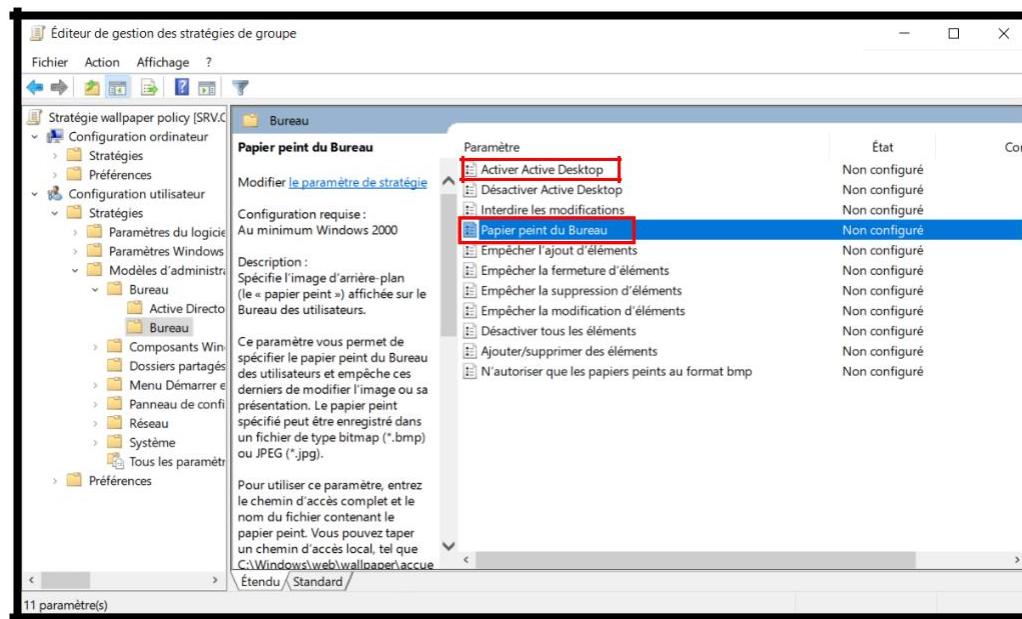


## Modification de l'objet de stratégie

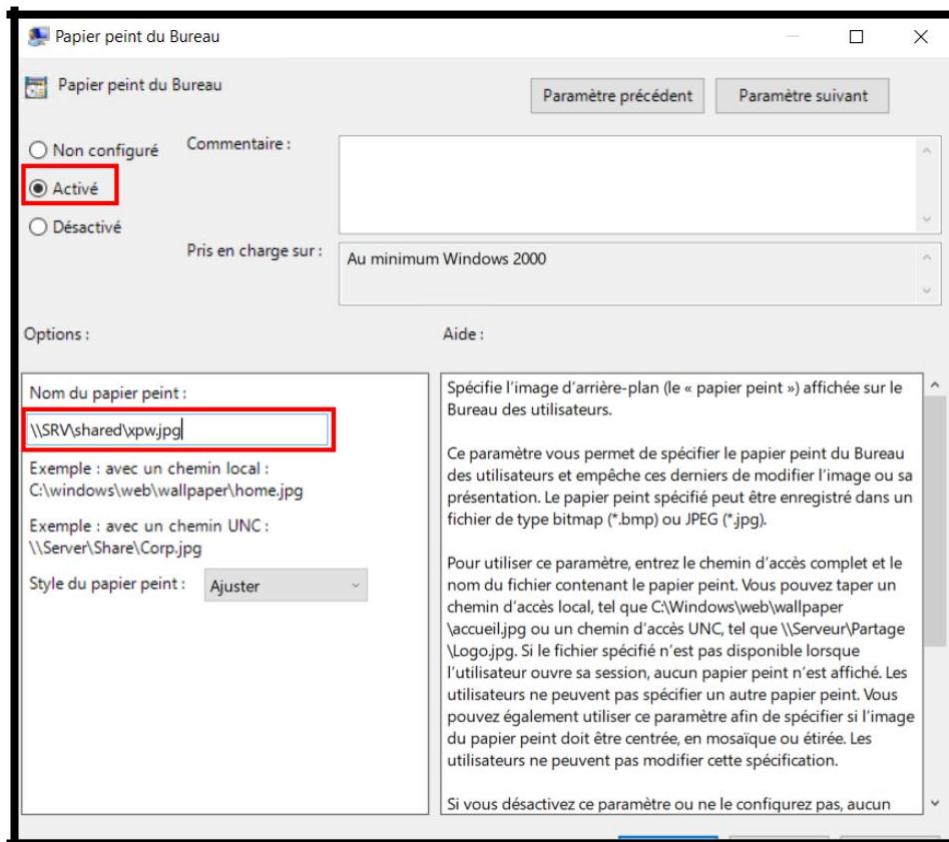
La stratégie nouvellement créée sera répertoriée dans les listes d'objets de stratégie de groupe. Cliquez un clic droit dessus et sélectionnez "Modifier"



Une fenêtre d'édition apparaîtra. Dans le volet de gauche, sélectionnez Configuration de l'utilisateur> Modèles d'administration> Bureau> Bureau. Dans le volet de droite, double-cliquez sur le paramètre Papier peint du bureau.



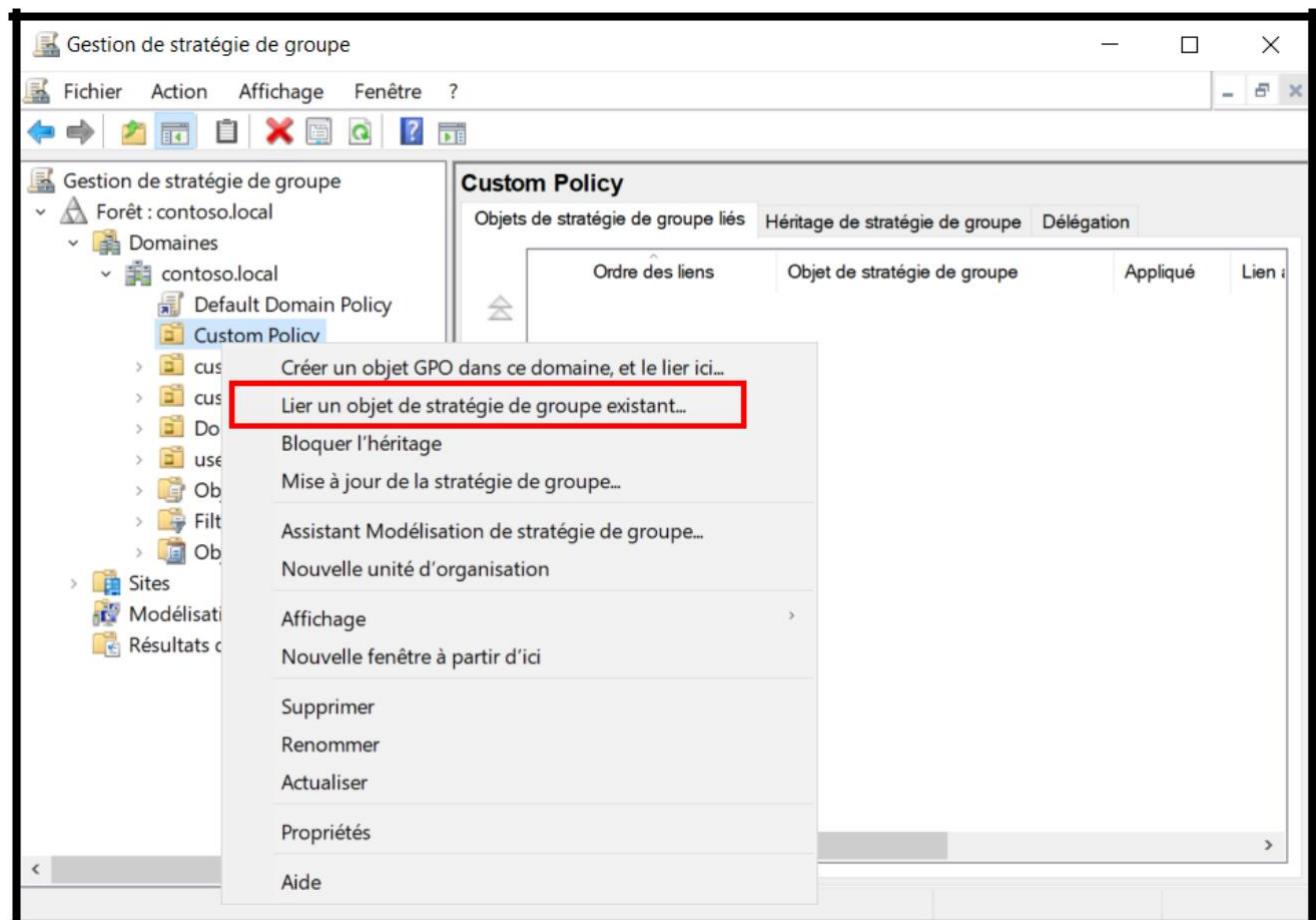
Définissez l'option sur Activé, puis spécifiez l'emplacement et le style du papier peint. Dans cet exemple, nous spécifions un chemin local parce que le fichier image pour le fond d'écran du bureau est stocké sur le lecteur local du serveur du contrôleur de domaine et que le style de papier peint que nous avons utilisé est « Ajuster ». Une fois configuré, cliquez sur OK et fermez la fenêtre de l'éditeur.  
La même opération doit être effectuée sur « Active Desktop » (puis définir l'option sur « Activé »)



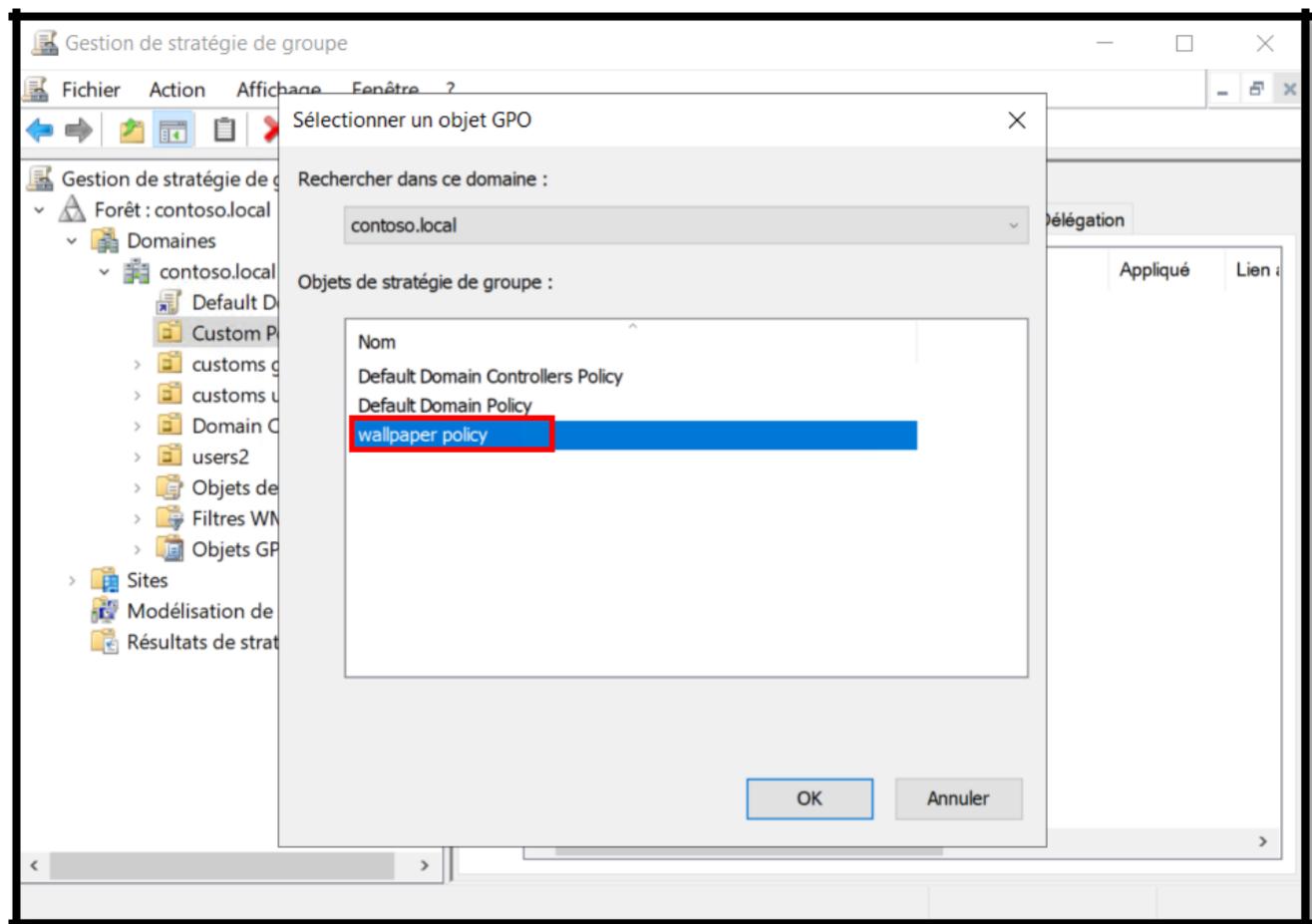
[Retour au  
Sommaire](#)

## Application de l'objet de stratégie

De retour dans la fenêtre de la console de gestion des stratégies de groupe, cliquez avec le bouton droit de la souris sur l'unité d'organisation "Custom Policy" et sélectionnez "Lier un objet de stratégie de groupe existant".



Sélectionnez la stratégie de papier peint et cliquez sur OK.



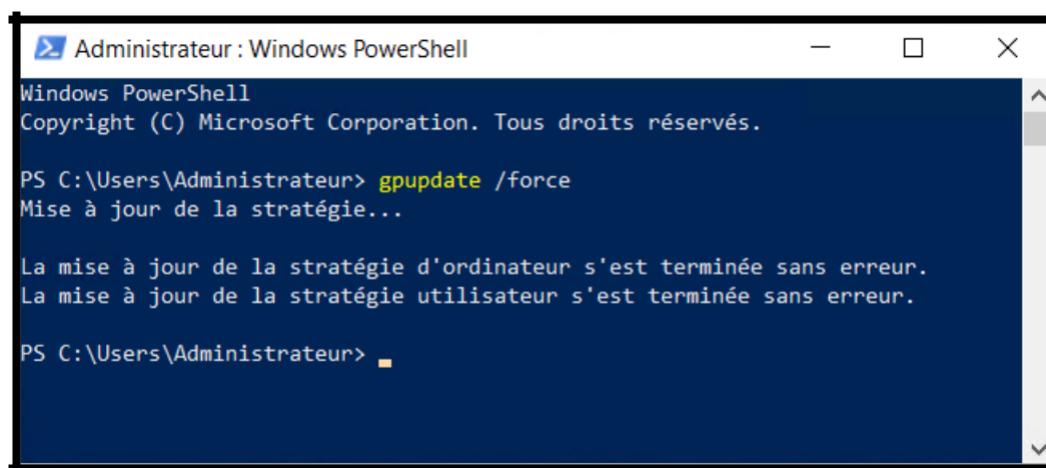
Enfin, insérez l'endroit où vous voulez que l'objet de stratégie de groupe opère. Donc si je veux que ce GPO opère sur l'utilisateur "BTS" je vais entrer le GPO dans le dossier où l'utilisateur "BTS" est présent.

### Vérifier les résultats sur la machine client

Une fois que la machine client a reçu la politique mettre à jour, le fond d'écran va changer. La mise à jour de la politique est un processus qui se produit périodiquement en arrière-plan, de sorte qu'elle ne nécessite aucune action de la part de l'utilisateur. Cependant, dans cette démonstration, nous souhaitons accélérer le processus afin de forcer la mise à jour de la politique à s'exécuter immédiatement en ouvrant CMD et en utilisant la commande « **gp update /force** »

Pour vérifier que la stratégie a été appliquée, l'utilisateur peut exécuter la commande « **gpresult /r** » sur le CMD. Recherchez la stratégie nommée « Stratégie de papier peint » dans la section « Objets de stratégie de groupe appliqués ».

Une fois la stratégie appliquée, ce sera nécessaire. Redémarrer le PC.  
Ainsi, au prochain redémarrage, le fond d'écran sera changé.



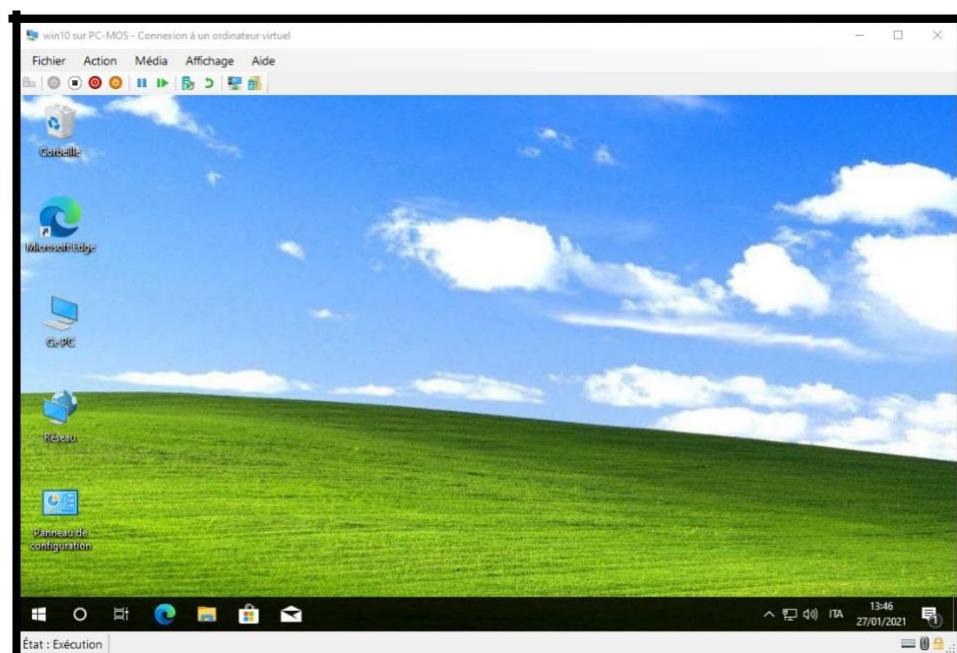
```
Administrator : Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

PS C:\Users\Administrateur> gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

PS C:\Users\Administrateur>
```

Dans ce cas (peut-être par nostalgie du bon vieux temps), nous avons inséré l'ancien fond d'écran de Windows XP.



[Retour au Sommaire](#)

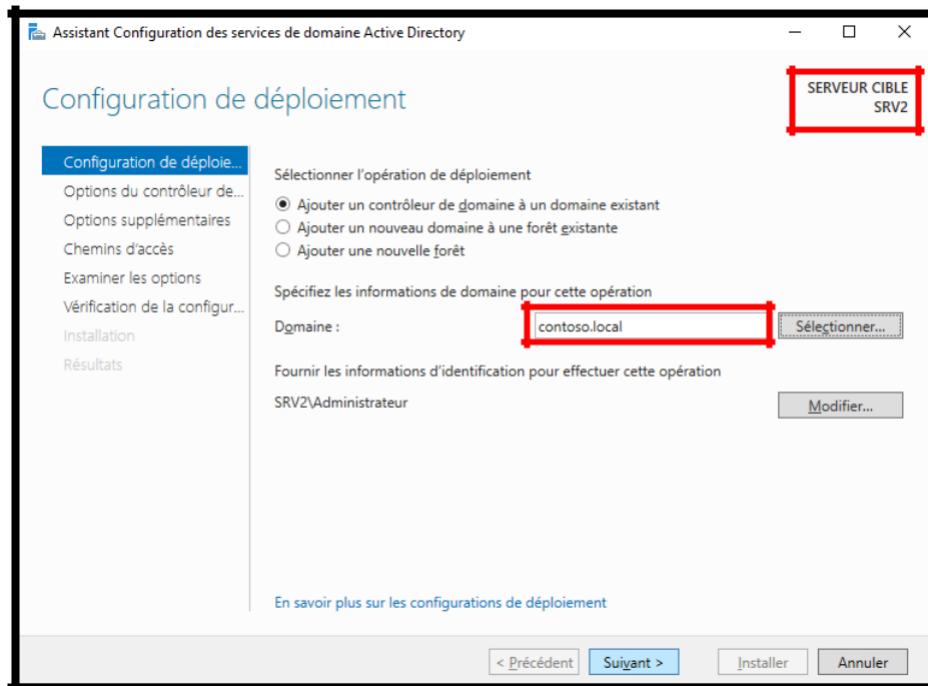
## Active directory secondaire (bonus)

Dans l'environnement d'entreprise, il est toujours recommandé d'avoir au moins deux contrôleurs de domaine, de sorte que si le premier tombe en panne pour une raison quelconque, il y ait un deuxième contrôleur de domaine qui peut s'activer sans laisser tout le réseau en difficulté.

Tout d'abord nous allons configurer la carte réseau, puis nous spécifierons dans la carte réseau une adresse IP statique, ayant comme DNS principal, l'adresse IP du premier contrôleur de domaine. Afin qu'il puisse se connecter au contrôleur de domaine principal.

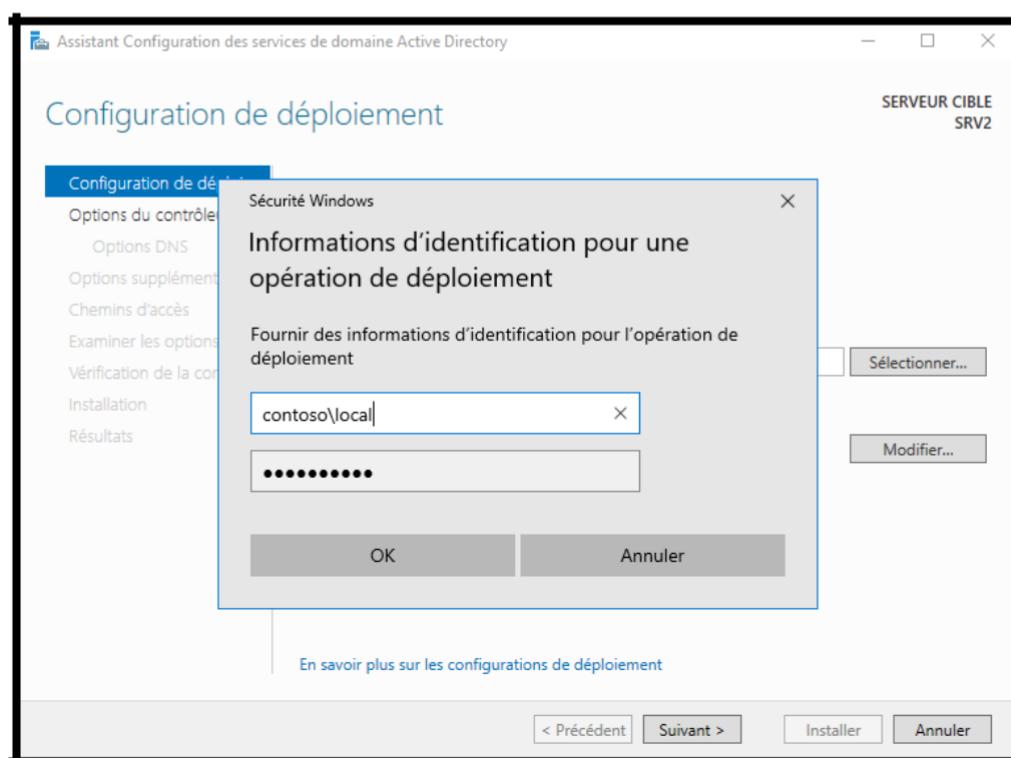
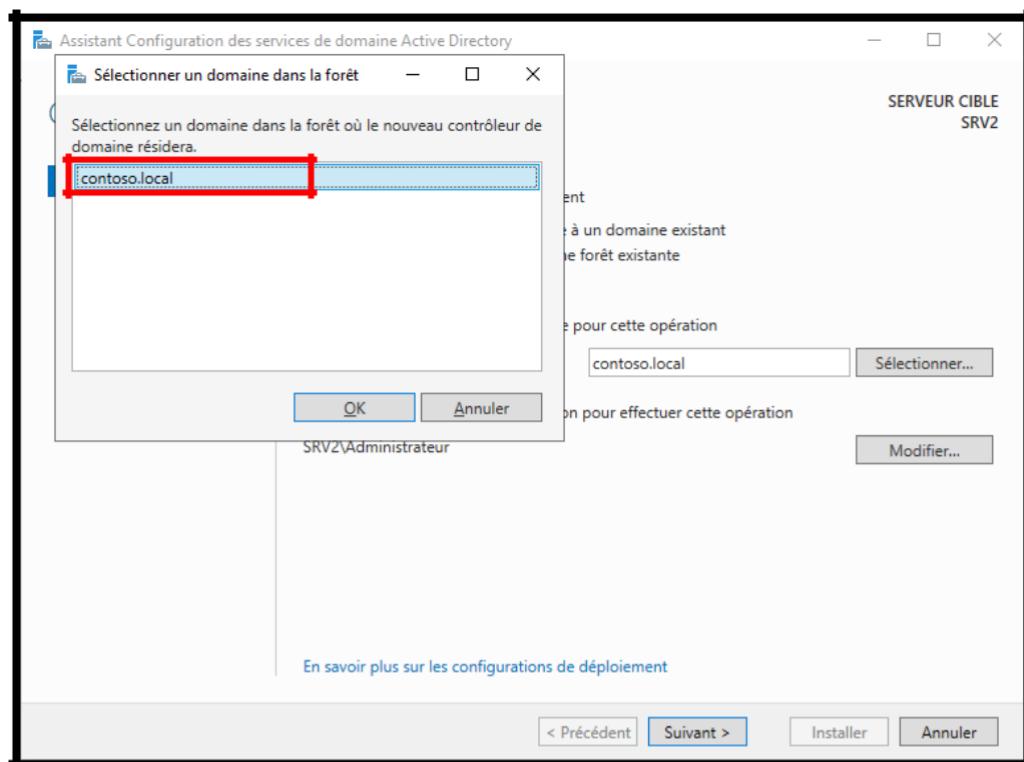
Sur ce serveur, nous avons déjà installé la fonctionnalité AD DS précédemment (vous pouvez voir le tutoriel d'installation [ici](#))

Dans ce cas, notre serveur s'appelait SRV2, comme vous pouvez le voir sur la capture d'écran ci-dessous.



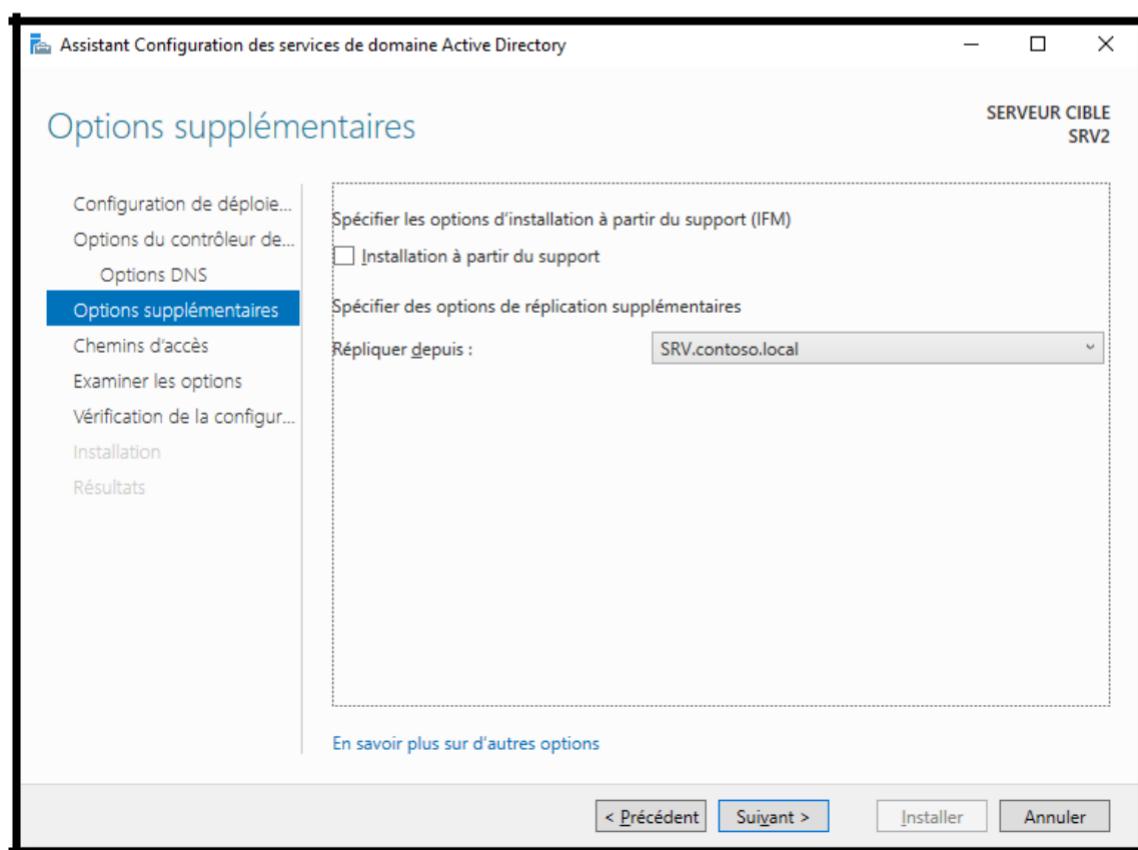
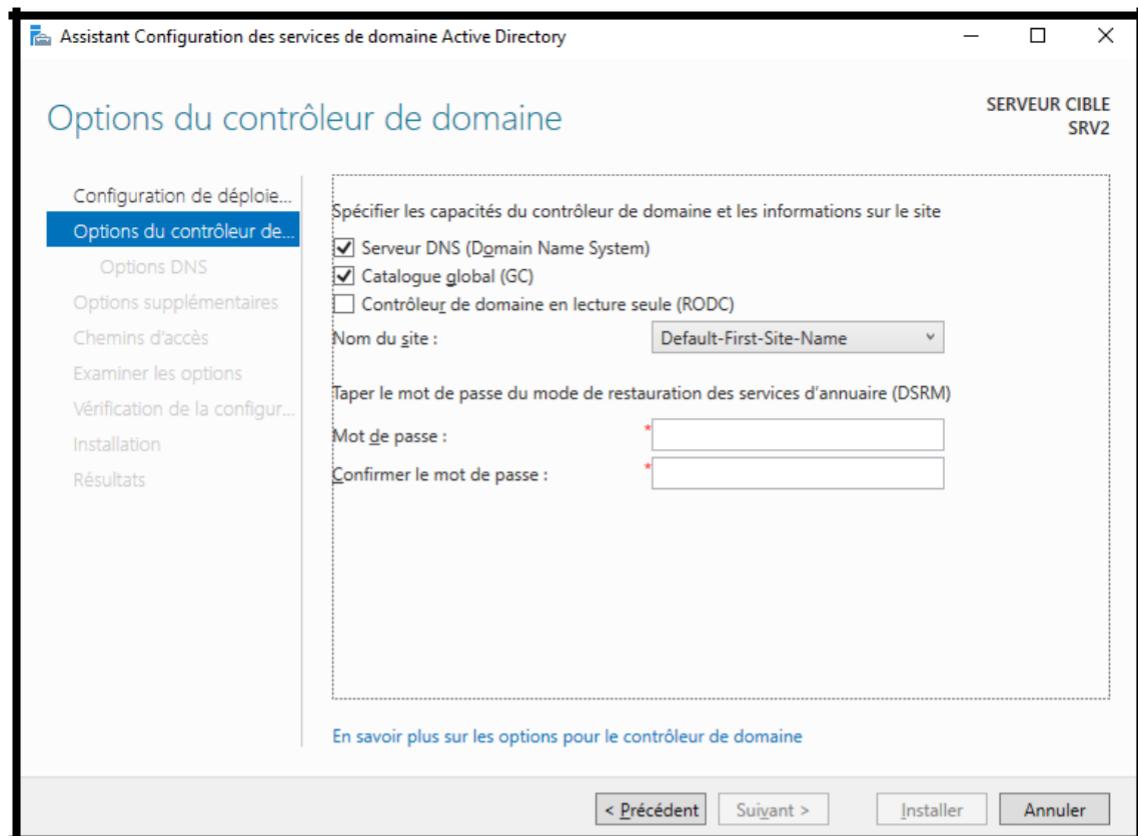
[Retour au Sommaire](#)

Ensuite, il suffira de sélectionner le domaine, puis de saisir les identifiants pour continuer.





Comme vous pouvez le voir également dans ce cas, le serveur DNS sera installé afin que le contrôleur de domaine puisse fonctionner correctement.



Dans ce cas également, il est possible de sauvegarder le script à utiliser ultérieurement sur d'autres serveurs via PowerShell.

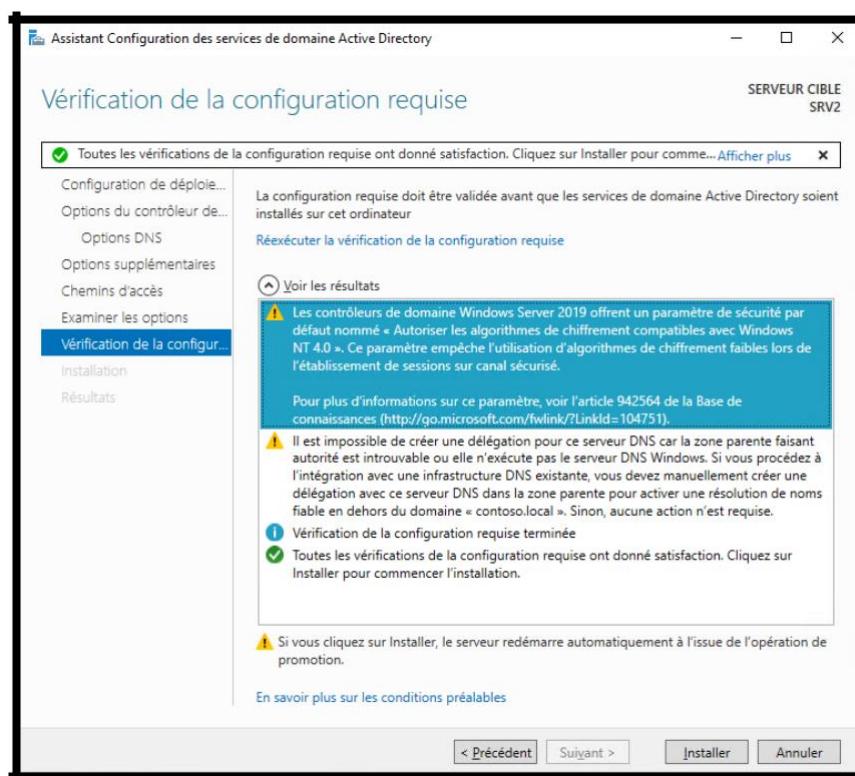


```

tmpF73A.tmp - Bloc-notes
Fichier Edition Format Affichage Aide
#
# Script Windows PowerShell pour le déploiement d'AD DS
#
Import-Module ADDSDeployment
Install-ADDSDomainController `-
-NoGlobalCatalog:$false `-
-CreateDnsDelegation:$false `-
-Credential (Get-Credential) `-
-CriticalReplicationOnly:$false `-
-DatabasePath "C:\Windows\NTDS" `-
-DomainName "contoso.local" `-
-InstallDns:$true `-
-LogPath "C:\Windows\NTDS" `-
-NoRebootOnCompletion:$false `-
-ReplicationSourceDC "SRV.contoso.local" `-
-SiteName "Default-First-Site-Name" `-
-SysvolPath "C:\Windows\SYSVOL" `-
-Force:$true

```

Dans ce cas également, nous recevons des erreurs qui peuvent être ignorées.



On peut donc vérifier sur le serveur principal que les contrôleurs de domaine sont en fait deux :

- **SRV** : (le premier contrôleur de domaine créé)
- **SRV2** : (le deuxième contrôleur de domaine créé en tant que sauvegarde)

The screenshot shows the Windows Server Management Console with the title "Console1 - [Racine de la console]\Utilisateurs et ordinateurs Active Directory [SRV.contoso.local]". The left pane displays a tree view of Active Directory objects under "contoso.local", including "BuiltIn", "Computers", "customs groups folder", "customs users folder", "Domain Controllers" (which is selected), "ForeignSecurityPrincipals", "Managed Service Accounts", "Users", and "users2". The right pane is a table showing two entries:

Nom	Type	Typ...	Site
SRV	Ordinateur	GC	Default-Fir...
SRV2	Ordinateur	GC	Default-Fir...

The "Actions" pane on the right contains "Domain C..." and "Autre...".

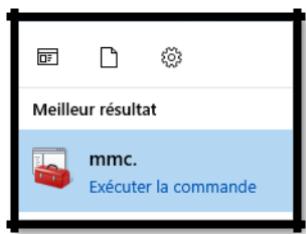
## Implémenter une console MMC (partie extra)

### Définition :

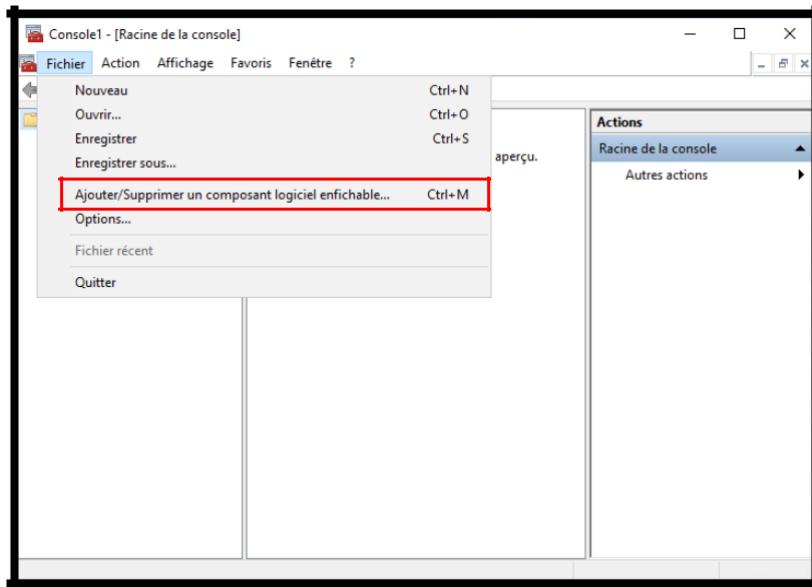
*Microsoft Management Console (MMC)* est un gestionnaire de console virtuelle incorporé dans Microsoft Windows, qui sert de conteneur pour des interfaces graphiques de configuration.

Il est possible de mémoriser une console MMC personnalisé pour avoir plusieurs panneaux de configuration en un coup d'œil. Par exemple, dans cet exemple, nous allons stocker une console personnalisée avec plusieurs composants.

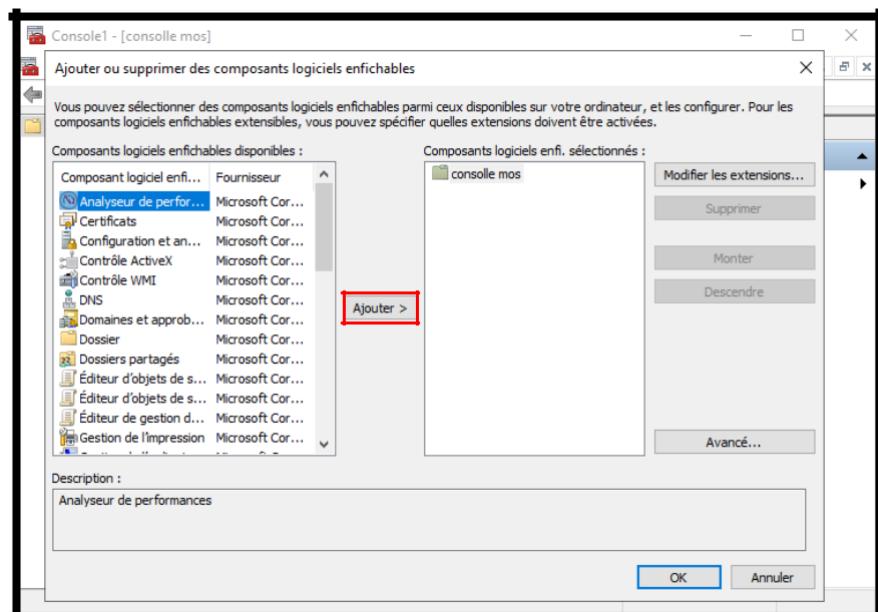
Donc, cliquez sur l'icône Windows en bas à gauche et recherchez ce qui suit : "**mmc.**"



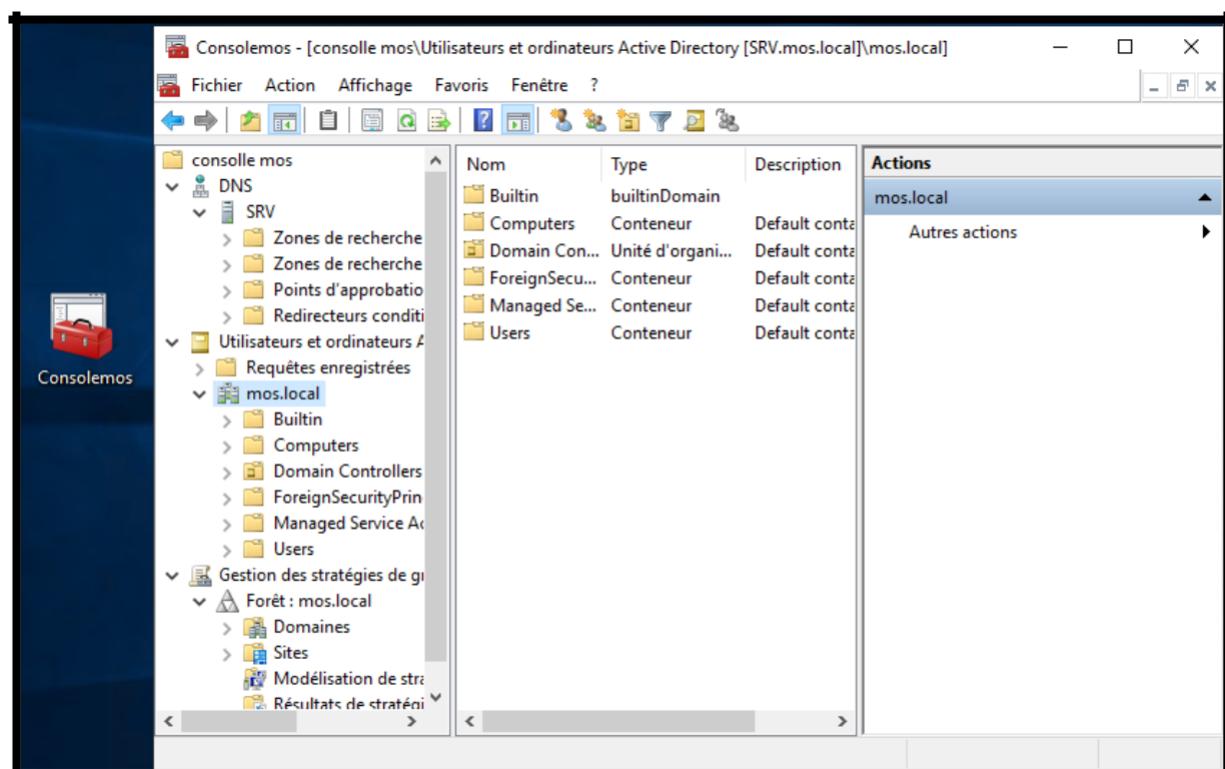
Cliquez ensuite sur l'icône. Après ça ce sera nécessaire cliquer sur "**Ajouter / Supprimer un composant logiciel enfichable...** »



Donc à partir de ce panneau il sera possible d'ajouter toutes nos composants.  
Nous pouvons ensuite ajouter plusieurs composants à notre console.



Nous pouvons ensuite sauvegarder notre "console" en cliquant sur le bouton "**Registre sous**" du menu "**Fichier**". Enfin, vous devriez avoir un résultat similaire :



[Retour au Sommaire](#)

## Conclusion

Ça répond aux besoins de qui ?

AD DS peut grandement faciliter la gestion de réseaux simples, mais aussi de réseaux très complexes. Bien sûr, c'est une bonne règle de pouvoir trouver le bon équilibre pour simplifier les opérations à effectuer. A titre d'exemple, dans le cas d'une vingtaine de postes de travail sur un même site, pour faciliter la gestion, il est possible de créer un seul domaine et peut-être plusieurs unités organisationnelles.

Sinon, face à la présence de centaines de postes de travail sur de nombreux sites, la meilleure chose à faire pour simplifier la gestion est de créer un nombre de sous-domaines égal au nombre de sites. Toutes les stratégies utiles pour optimiser les travaux et tirer le meilleur parti des technologies mises à disposition par les outils Windows Server.

En effet, AD DS est fonctionnel pour toute réalité, il suffit d'utiliser les outils appropriés en les contextualisant aux architectures en question.

Sans ces systèmes et les fonctionnalités qu'ils offrent, la sécurité informatique serait sérieusement compromise.

Aujourd'hui, il est quasiment impossible pour une entreprise de se passer de ces systèmes fondamentaux.

## Contraintes

AD DS n'est pas gratuit. C'est indéniable. Il faut donc acheter des licences, des ordinateurs et des équipements de réseau qui ont certainement un coût. Il faut. Alors **avoir un ou des serveurs.**

Il faut **avoir des compétences d'administration.**

Le technicien qui vient réparer ou mettre en œuvre de nouvelles fonctionnalités a également un coût, et il doit avoir des compétences spécifiques

Il faut avoir **une bonne réflexion à la création de l'organisation**

Il faut avoir **une bonne réflexion à la création de l'arborescence de fichiers et des droits d'accès**

***Junior gafarou  
sadate***

[Retour au  
Sommaire](#)