



-Installation sur Windows Server 2019 des fonctionnalités suivantes :

- Active Directory (AD)
- DNS
- Stratégie de groupe (GPO)

Qu'est-ce que l'Active directory ? DNS ?

En informatique, [Active Directory \(AD\)](#), est un système serveur centralisé 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. 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 de l'AD. En effet est le service informatique distribué utilisé pour traduire les noms de domaine Internet en adresse IP ou autres enregistrements.

Pourquoi avons-nous besoin de tout cela ?

La fonctionnalité la plus importante de l'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.



Sommaire :

1) Conseil de pré-installation.....	3
1. Sécurité.....	3
2) Installation de l'Active Directory, Serveur DNS.	6
1. Active Directory	6
2. Configuration du contrôleur de domaine	11
3. Configurer le DNS	16
3) Création d'un utilisateur sur le contrôleur de domaine	22
4) Configurer la machine de l'utilisateur sur le domaine	26
5) Mettre en place une stratégie de groupe	30
1. Création de l'objet de stratégie de groupe	31
2. Modification de l'objet de stratégie.....	32
3. Application de l'objet de stratégie	34
4. Vérification de la stratégie	35

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 « PC Utilisateur » (Win 10 vers.20H22)

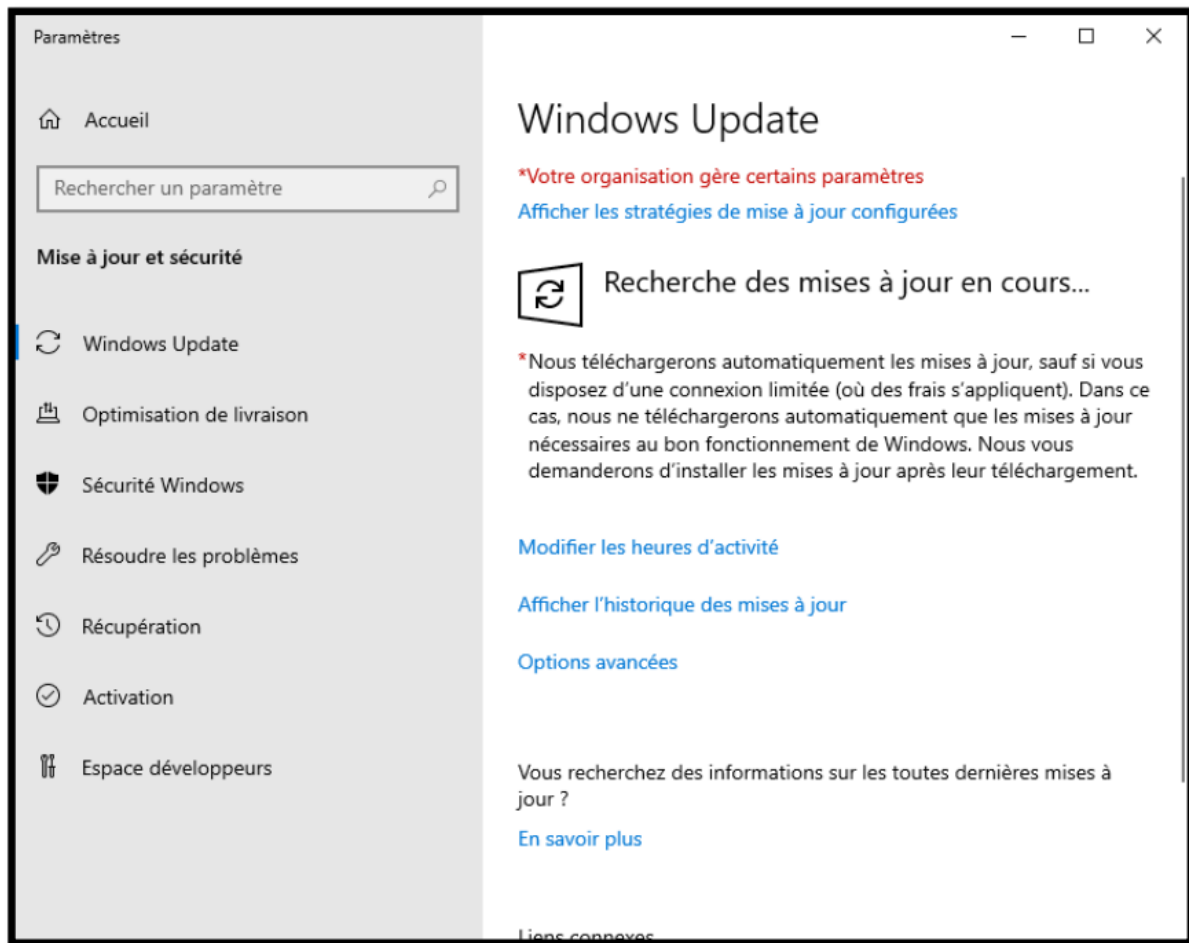
Raccourci	Explication
IP	Internet Protocol
Mask	Masque de sous-réseau
MAC	Media access control address
DNS	Domain Name System
AD DS	Active Directory Domain Service
GPO	Group Policy Object
PC	Personal Computer



1) Conseil de pré-installation.

1. Sécurité

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.

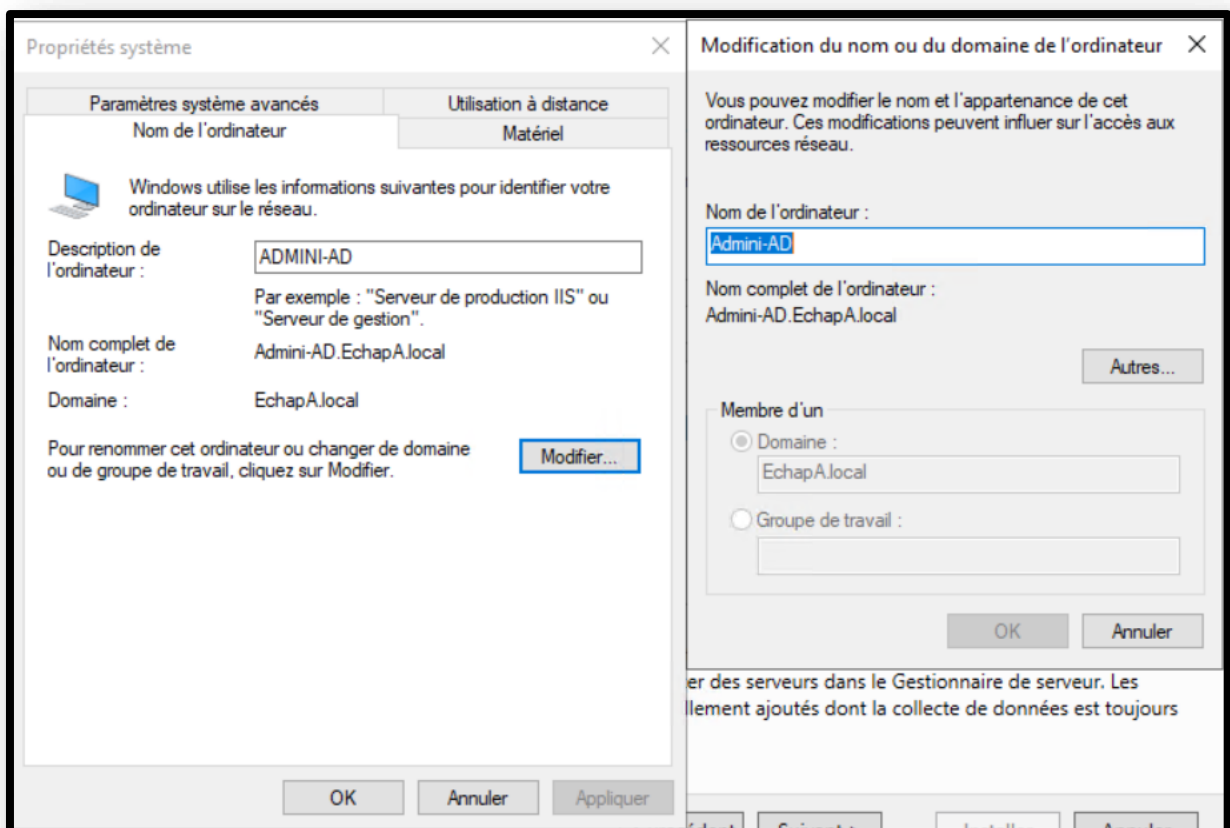
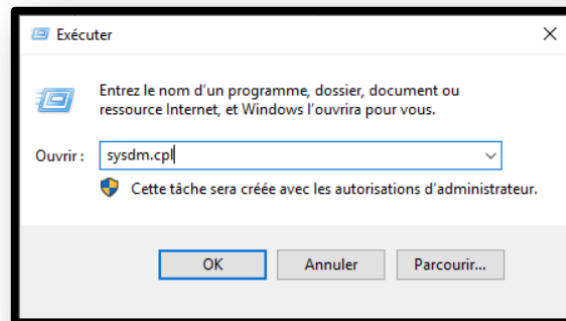


Il est également possible de mettre à jour le système d'exploitation en cliquant avec le bouton gauche de la souris, sur le menu avec l'icône Windows en bas à gauche, puis cliquez sur "Paramètres" (icône d'engrenage), puis "Mise à jour et sécurité" puis cliquez sur "Recherche des mises à jour".

Nous avons défini un nom personnalisé pour le serveur, dans ce cas je l'ai appelé : « ADMINI-AD »

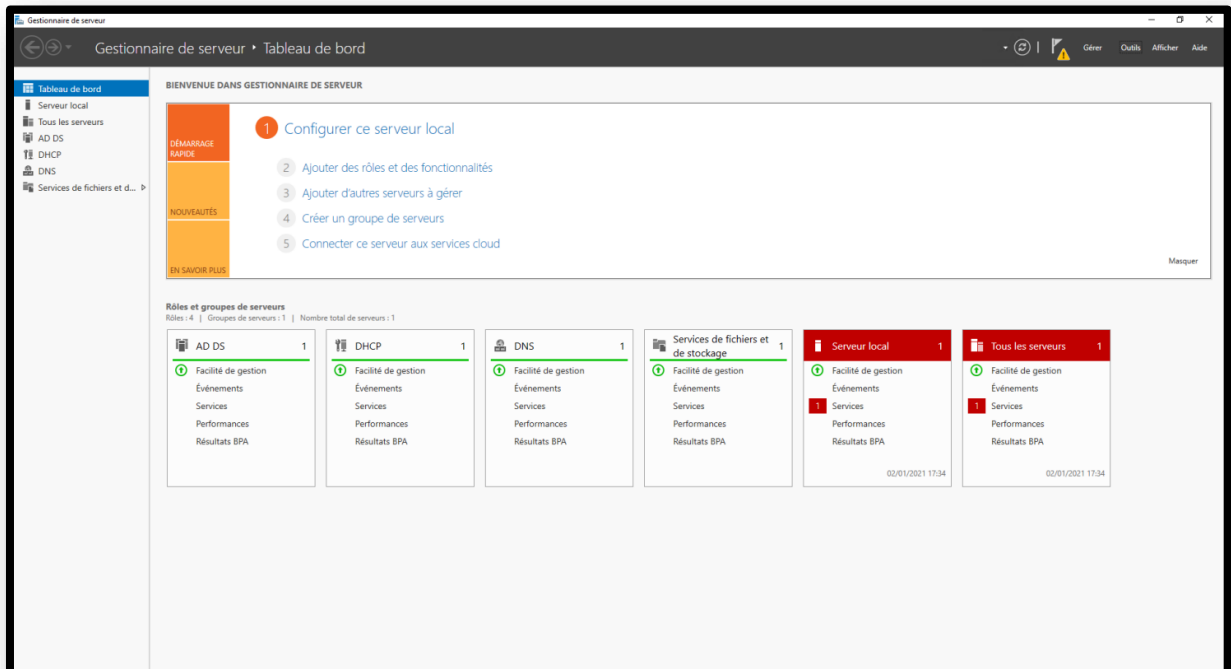
Après avoir changé le nom de la machine, il est fortement recommandé de redémarrer le serveur, pour des raisons évidentes.

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..." ou plus simplement en ouvrant la fenêtre « Exécuter » et rentre la commande « sysdm.cpl ».



De là, nous pouvons voir la nouvelle interface graphique (GUI Graphics Users Interface) du gestionnaire de serveur. C'est une console qui sera souvent utilisée pour gérer le serveur.

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



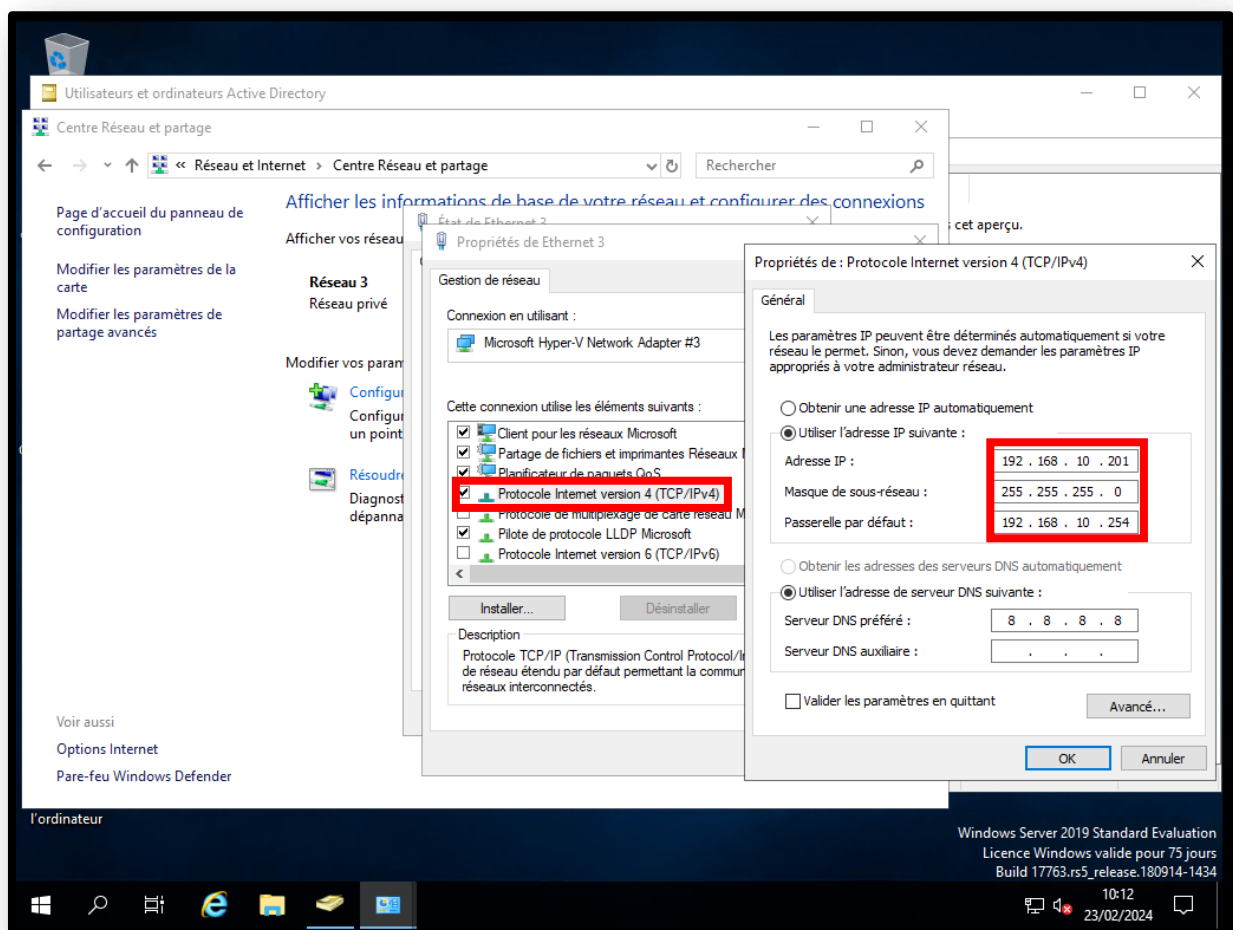
2) *Installation de l'Active Directory, Serveur DNS.*

1. *Active Directory*

À partir de là, nous définirons une adresse IP fixe sur notre serveur.

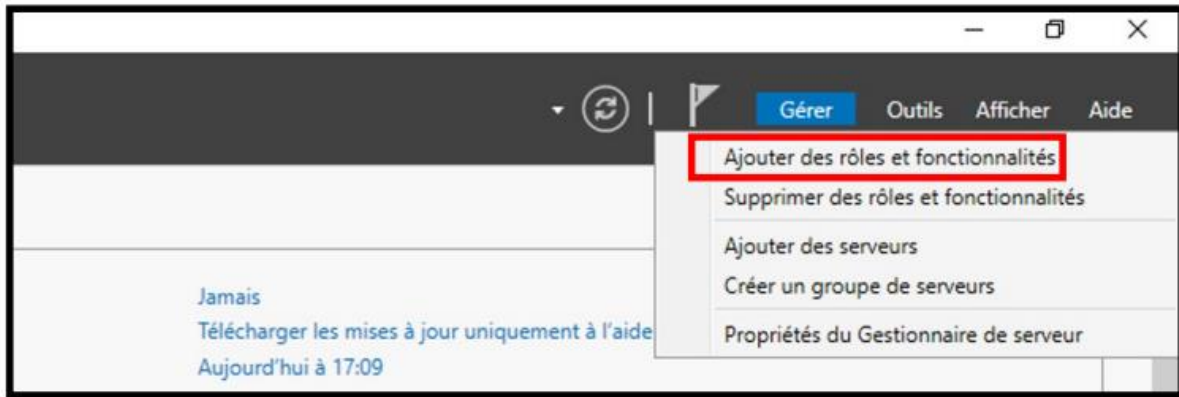
Il faut aussi définir une adresse IP statique dans le sous-réseau, dans notre cas, nous définissons les paramètres affichés dans la capture d'écran. Dans ce cas, nous allons tout configurer, via le protocole ipv4, mais la procédure est absolument réalisable même en ipv6.

Dans ce cas par exemple, je suis allé définir une IP statique 192.168.10.201, avec un masque de sous-réseau (MAC Address) 255.255.255.0, une passerelle : 192.168.10.254 et le DNS classique de Google (8.8.8.8).



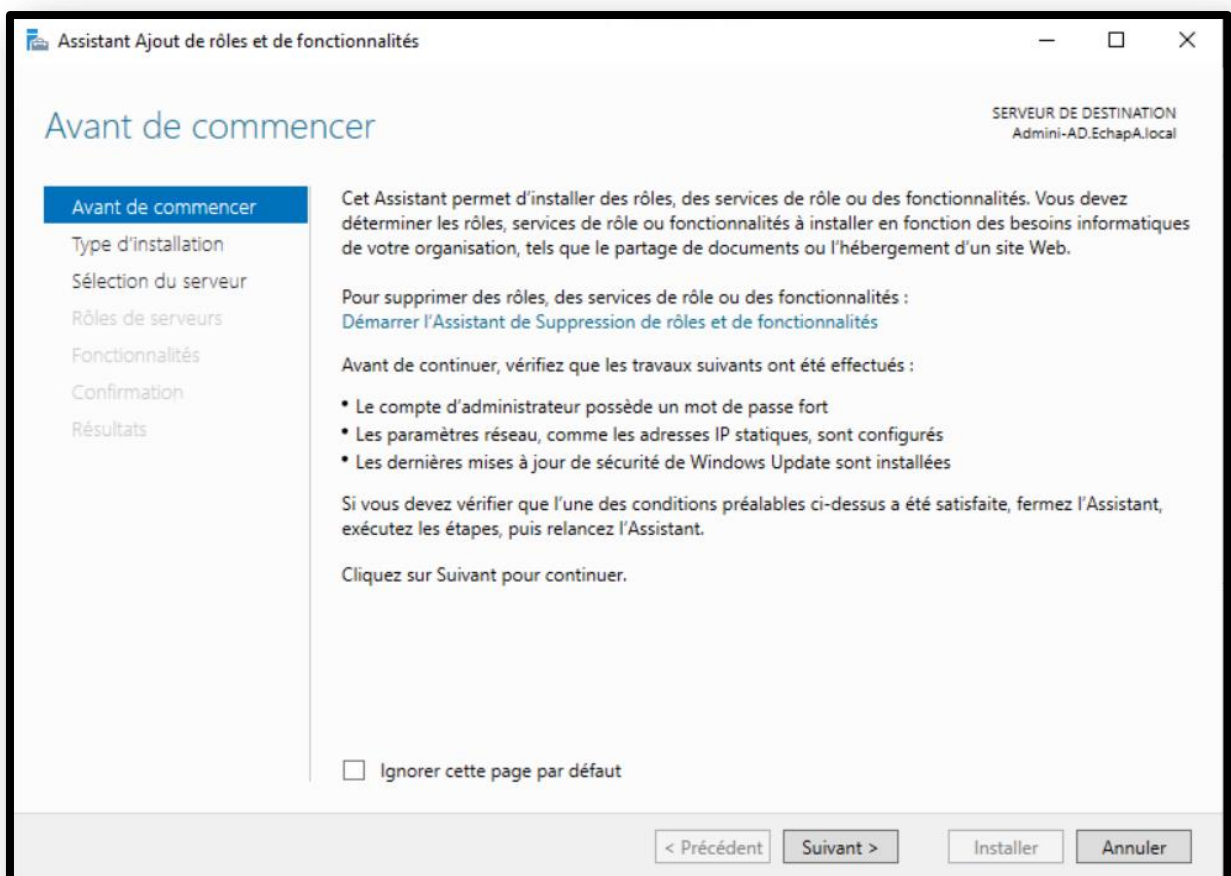
Une fois la carte réseau configurée, ajoutons les rôles et fonctionnalités, donc les services que nous souhaitons installer, dans ce cas nous installerons les fonctionnalités listées :

- Active Directory
- Serveur DNS
- DHCP

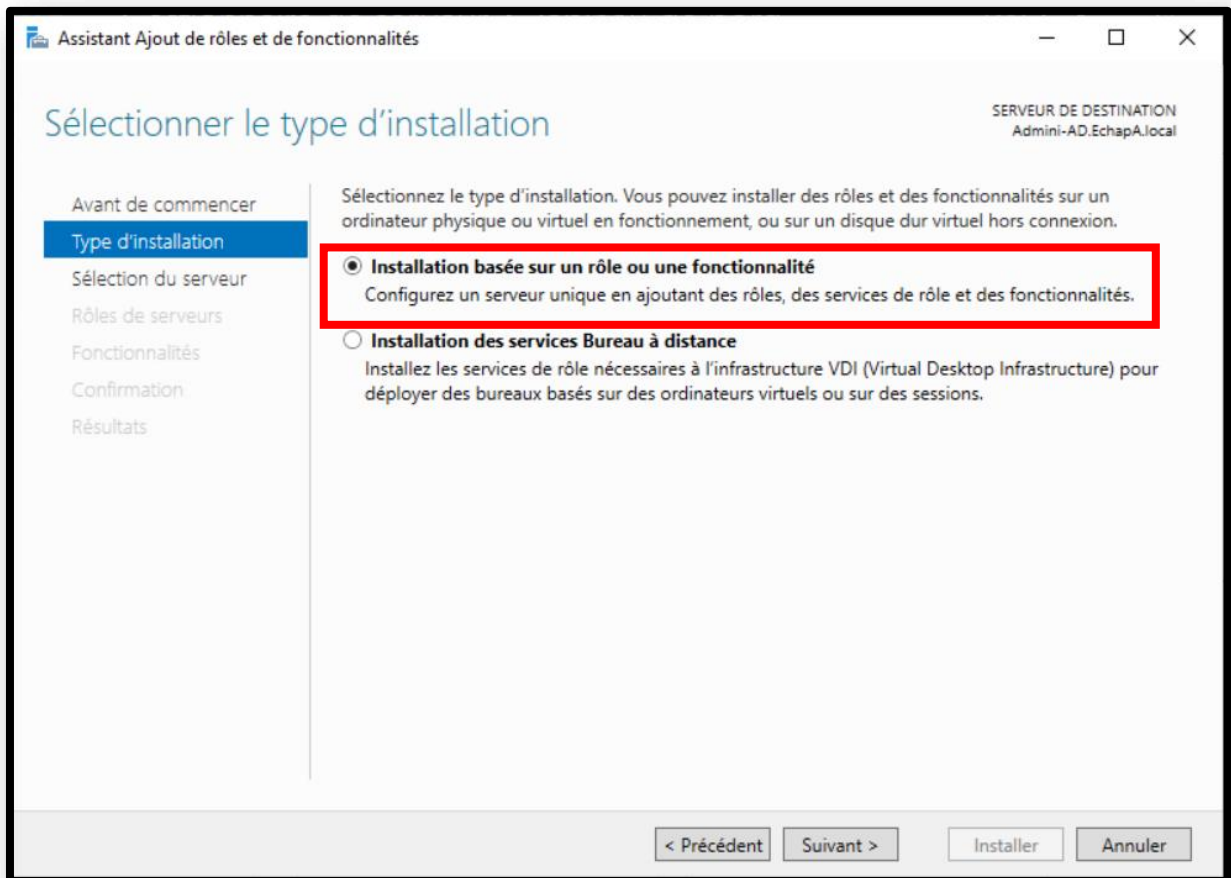


Donc à partir de là, nous suivons la procédure d'installation des services :

Cliquez ensuite sur le bouton "Suivant >".

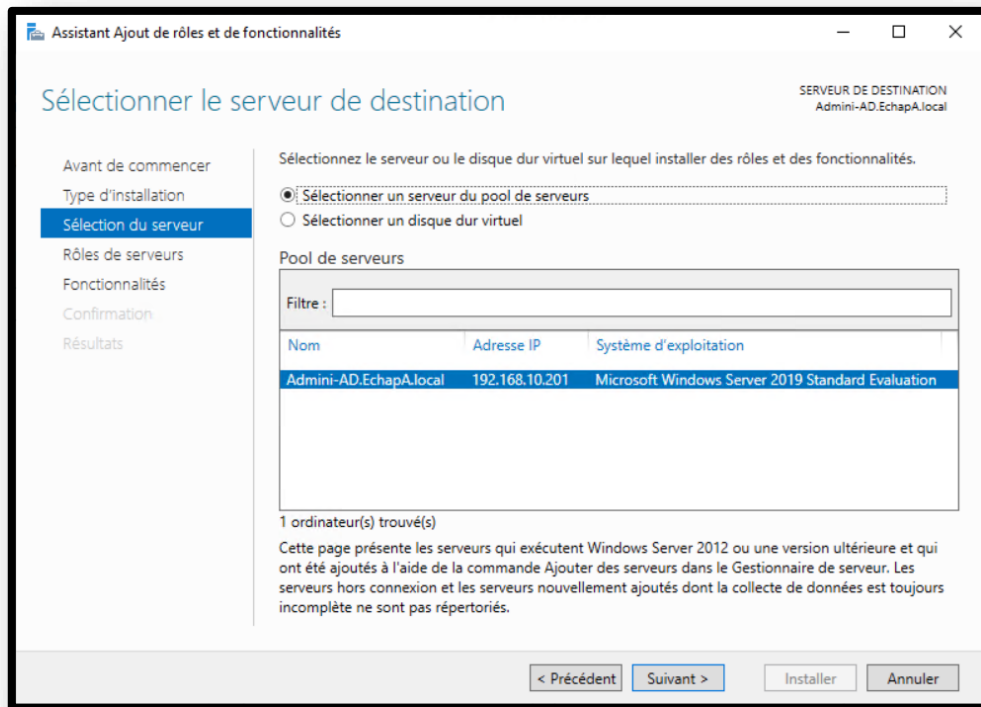


Assurez-vous que l'option est cochée : "Installation basée sur un rôle ou une fonctionnalité".

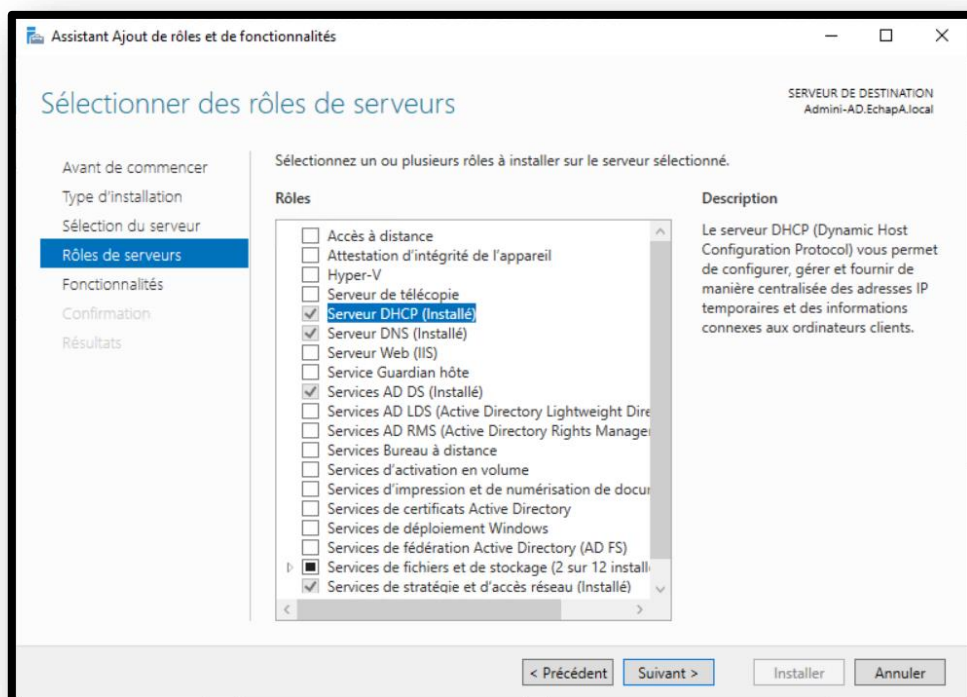


Vous pouvez choisir le serveur sur lequel installer.

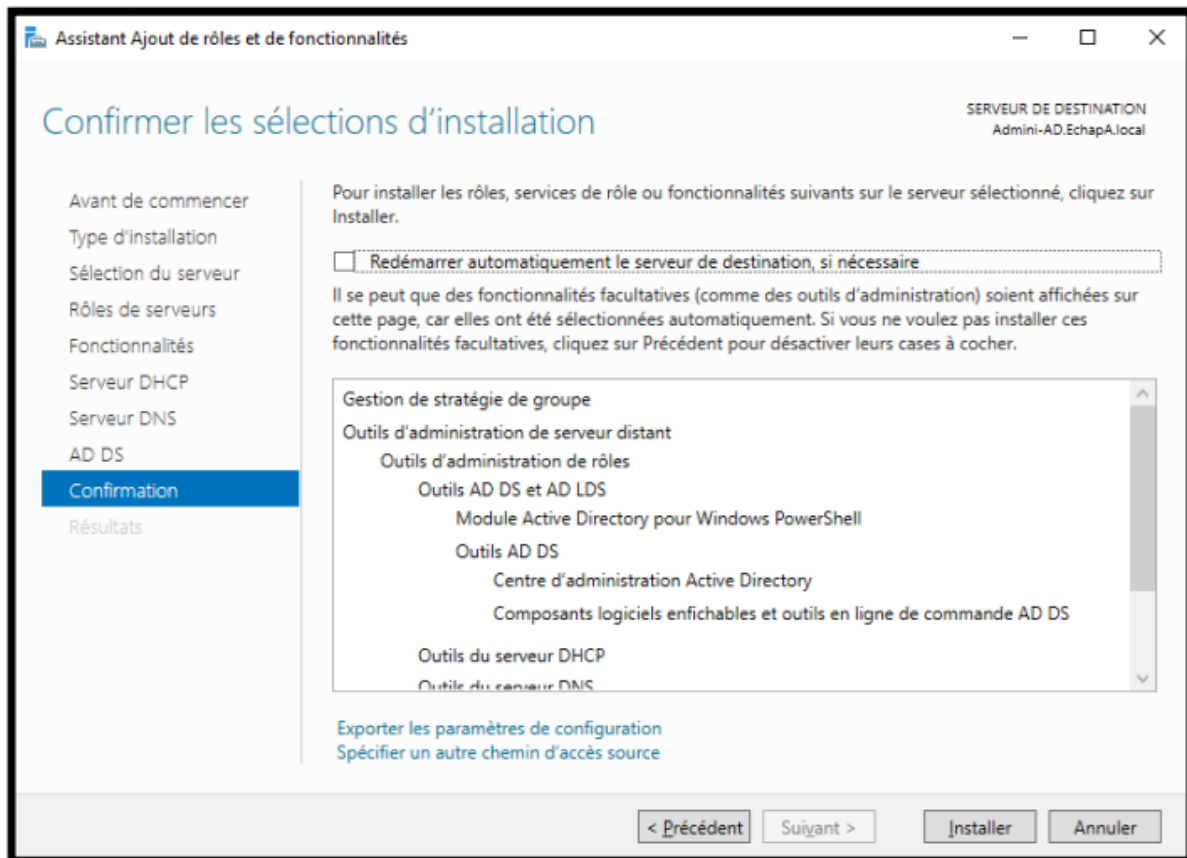
Dans ce cas, nous avons le serveur local « ADMINI-AD ».



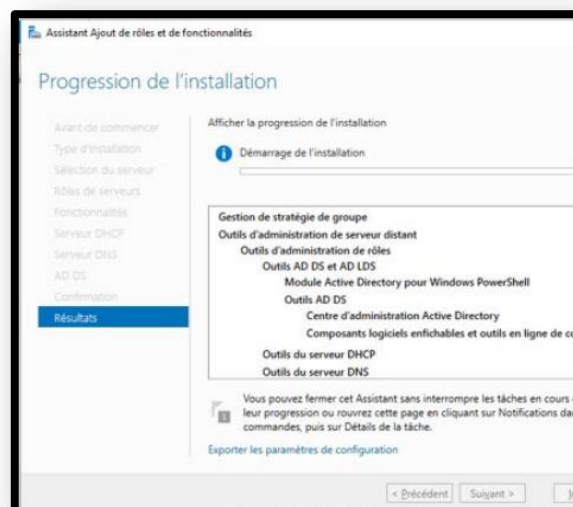
Dans cette fenêtre, nous choisirons d'installer le service AD DS (Active Directory) DNS et DHCP. Evidemment nous irons choisir les fonctionnalités dont nous aurons besoin.



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



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

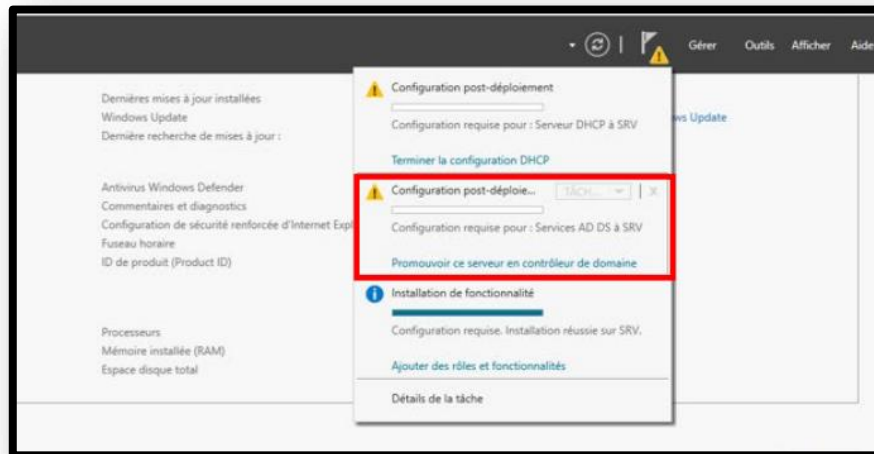




2. Configuration du contrôleur de domaine

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".

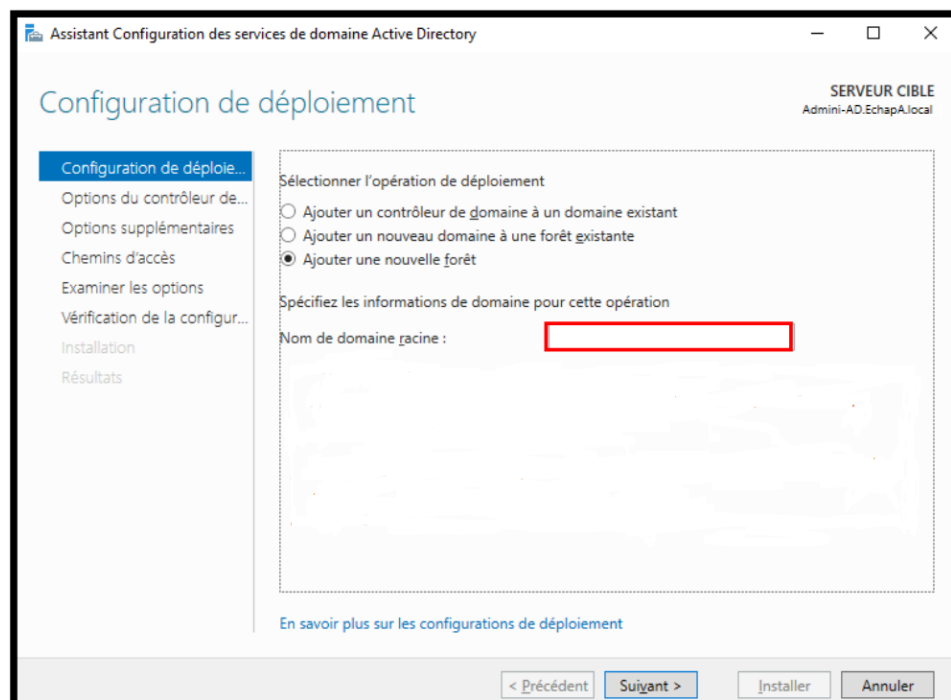


Ici, nous allons définir une option spécifique ;

- Ajouter une nouvelle forêt.

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





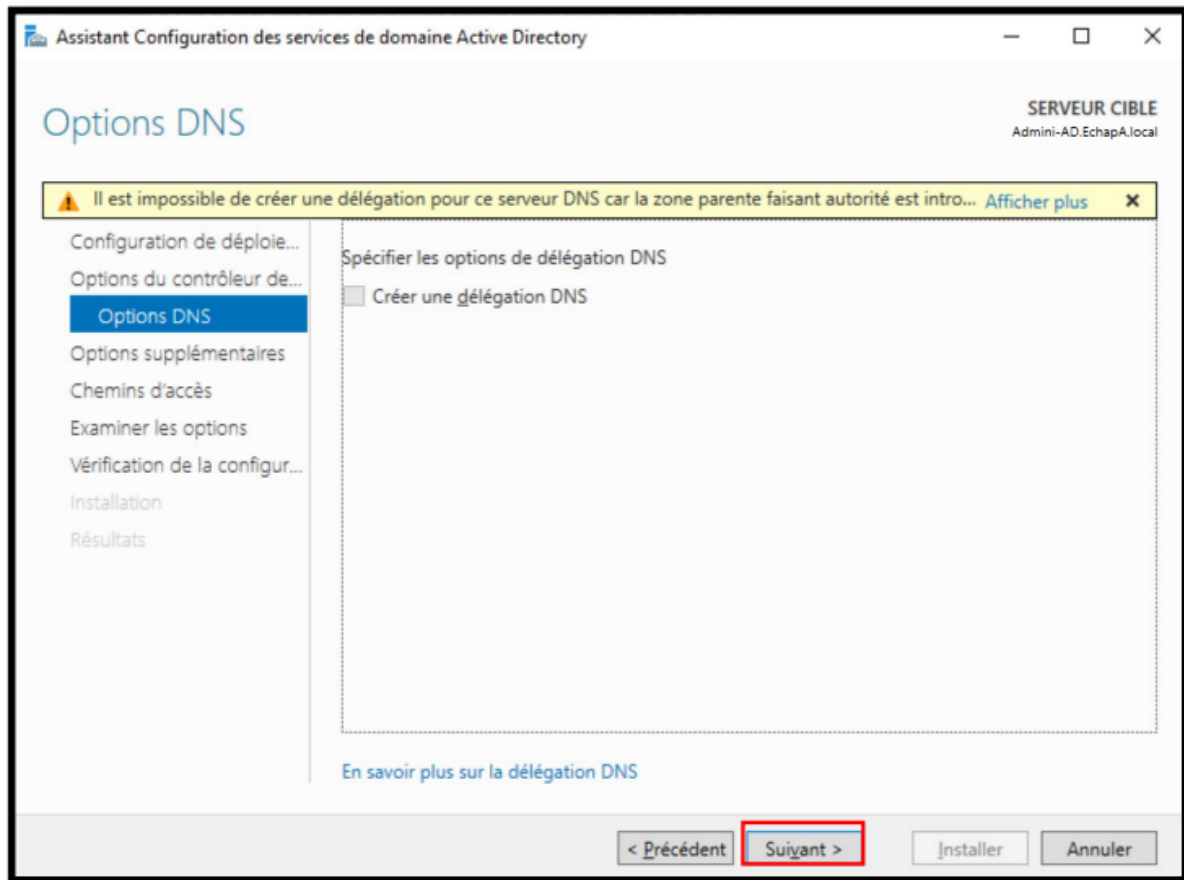
Depuis cette fenêtre, il sera nécessaire d'installer le serveur DNS, car il remarque que le serveur DNS n'est pas installé.

Il y a la possibilité de ne pas l'installer, mais dans notre cas c'est nécessaire, car les machines des utilisateurs ne seraient pas en mesure de joindre le domaine.

Le mot de passe demandé est le mot de passe que nous devons 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.

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).

Dans cette fenêtre, une "alerte" s'affiche, ce qui est tout à fait normal, puisqu'il n'y a pas encore de serveur DNS.



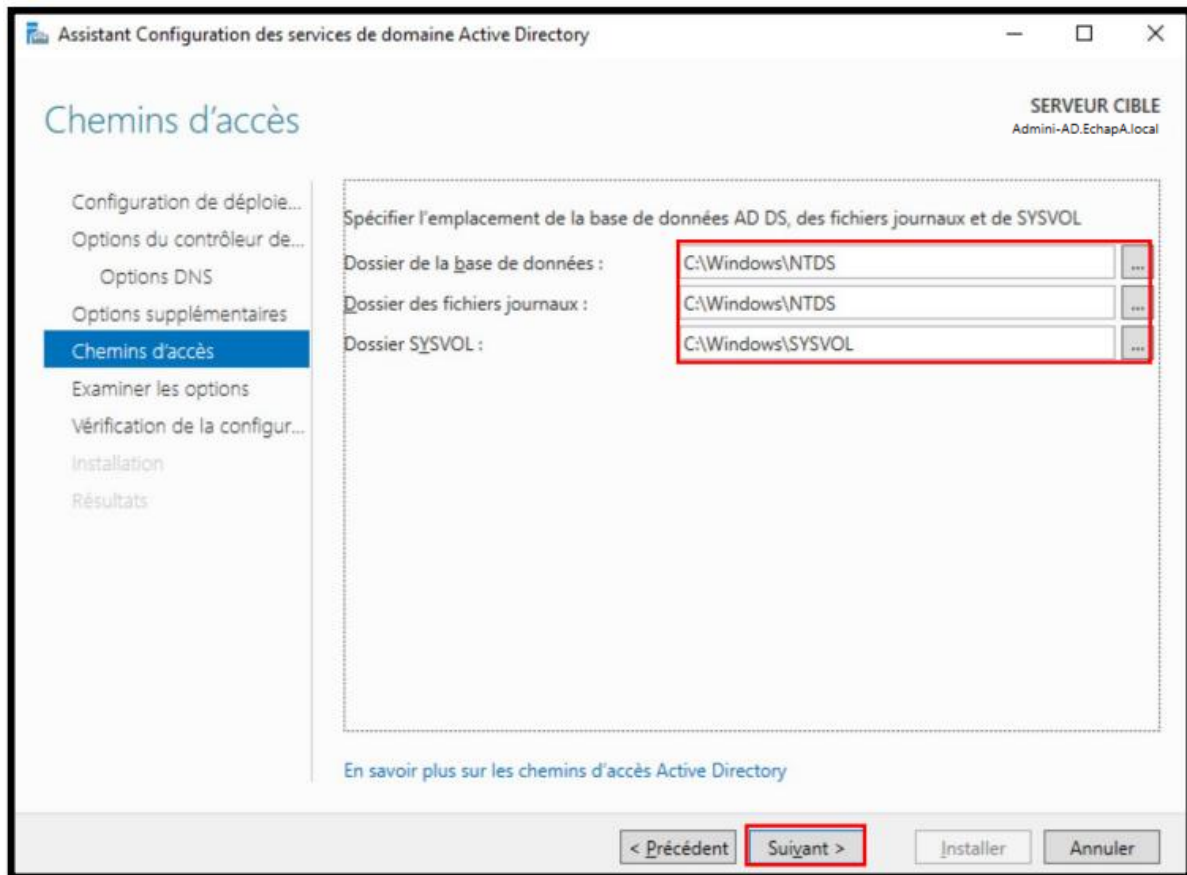
Dans l'onglet « Options supplémentaires », le nom NetBios est défini automatiquement, ce n'est rien d'autre que le nom de domaine sans l'extension.



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

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

Par défaut, les dossiers affichés dans la capture d'écran sont automatiquement choisis, mais il est possible de changer le chemin.



Dans « Examiner les options », nous avons un petit résumé de tous les paramètres.

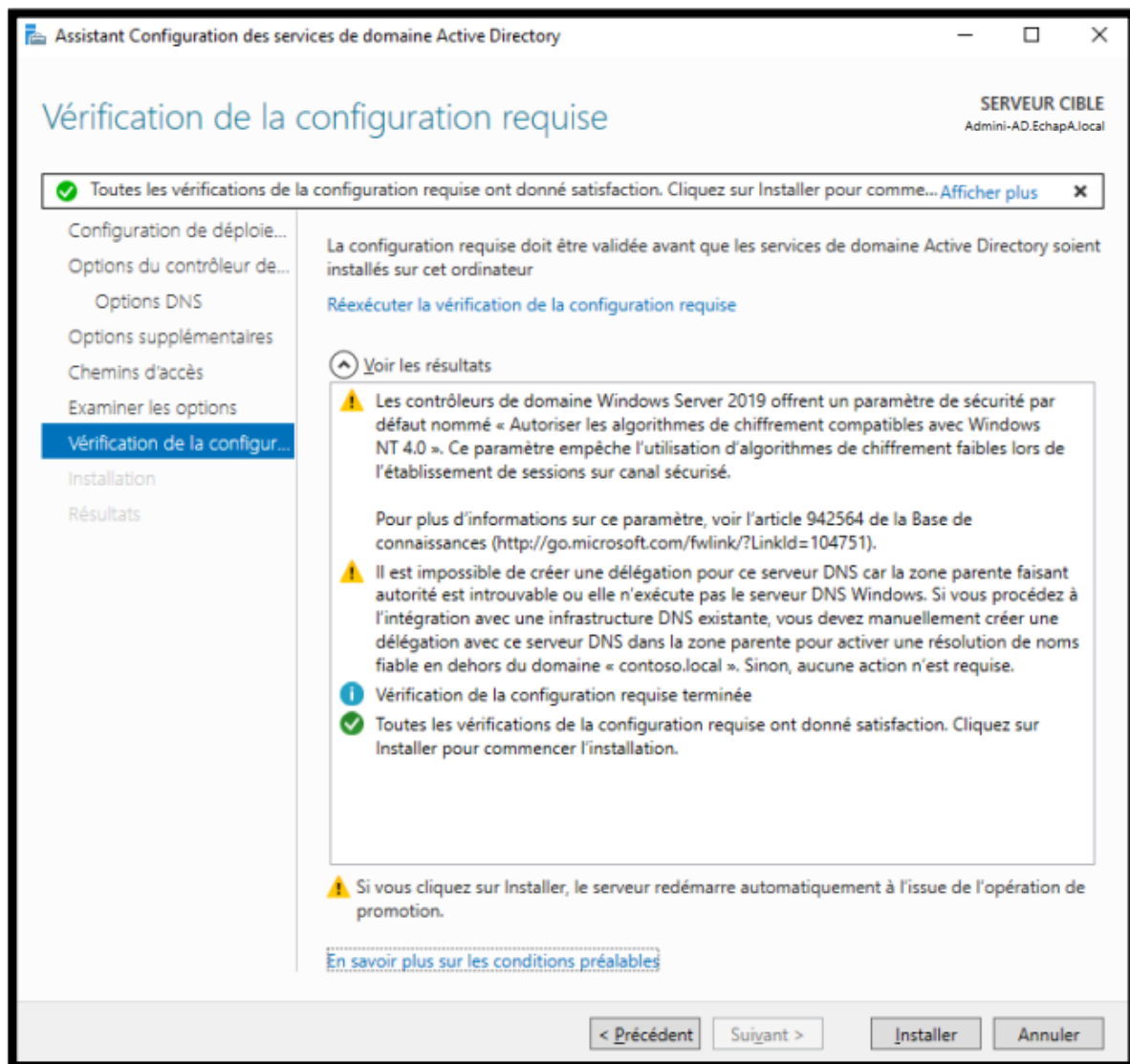
Un bref diagnostic des prérequis sera fait.



Nous aurons certainement des "alertes".

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.



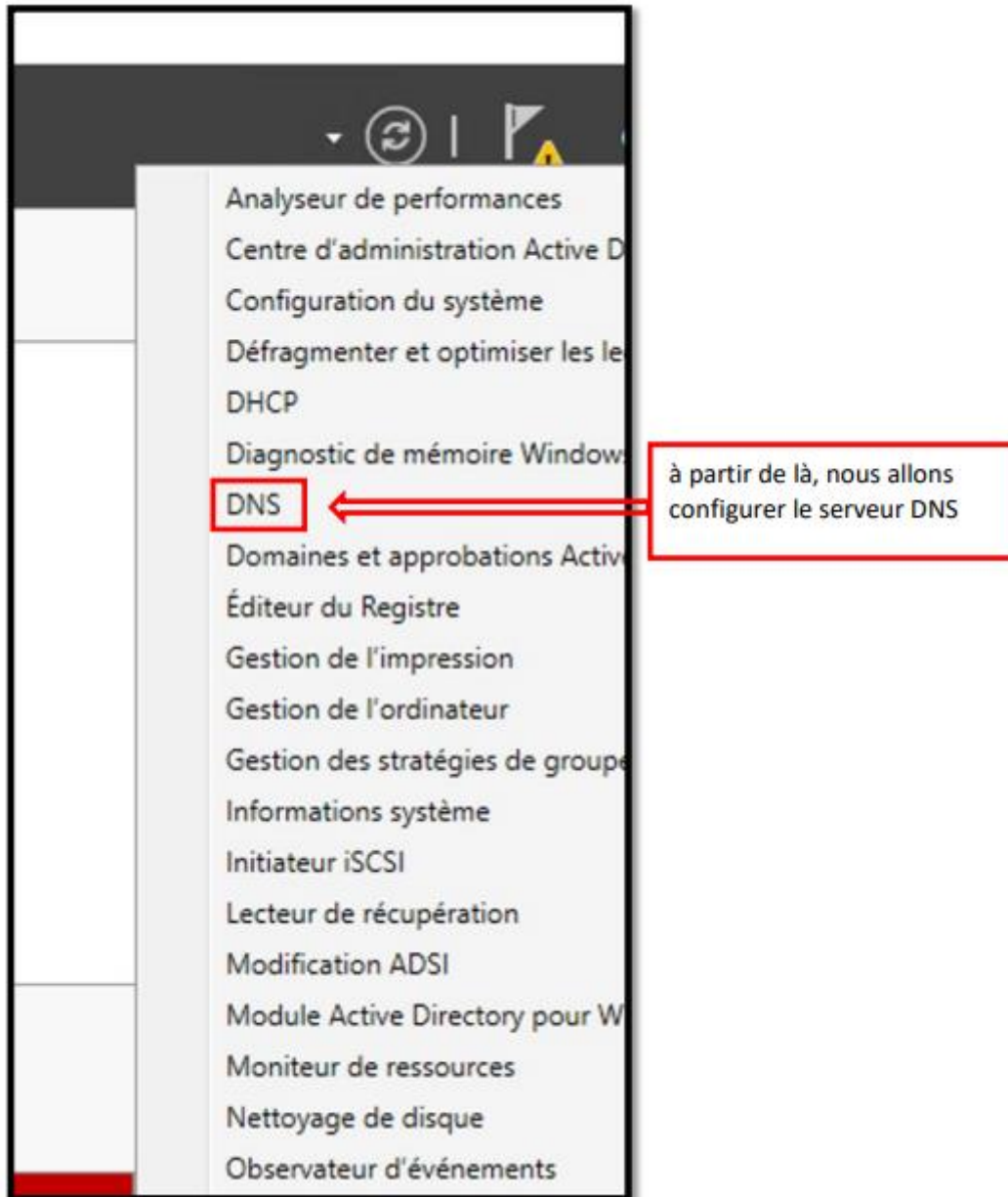
Par conséquent, le rôle de contrôleur de domaine sera installé, en l'associant aux cinq rôles typiques de contrôleur de domaine.

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.

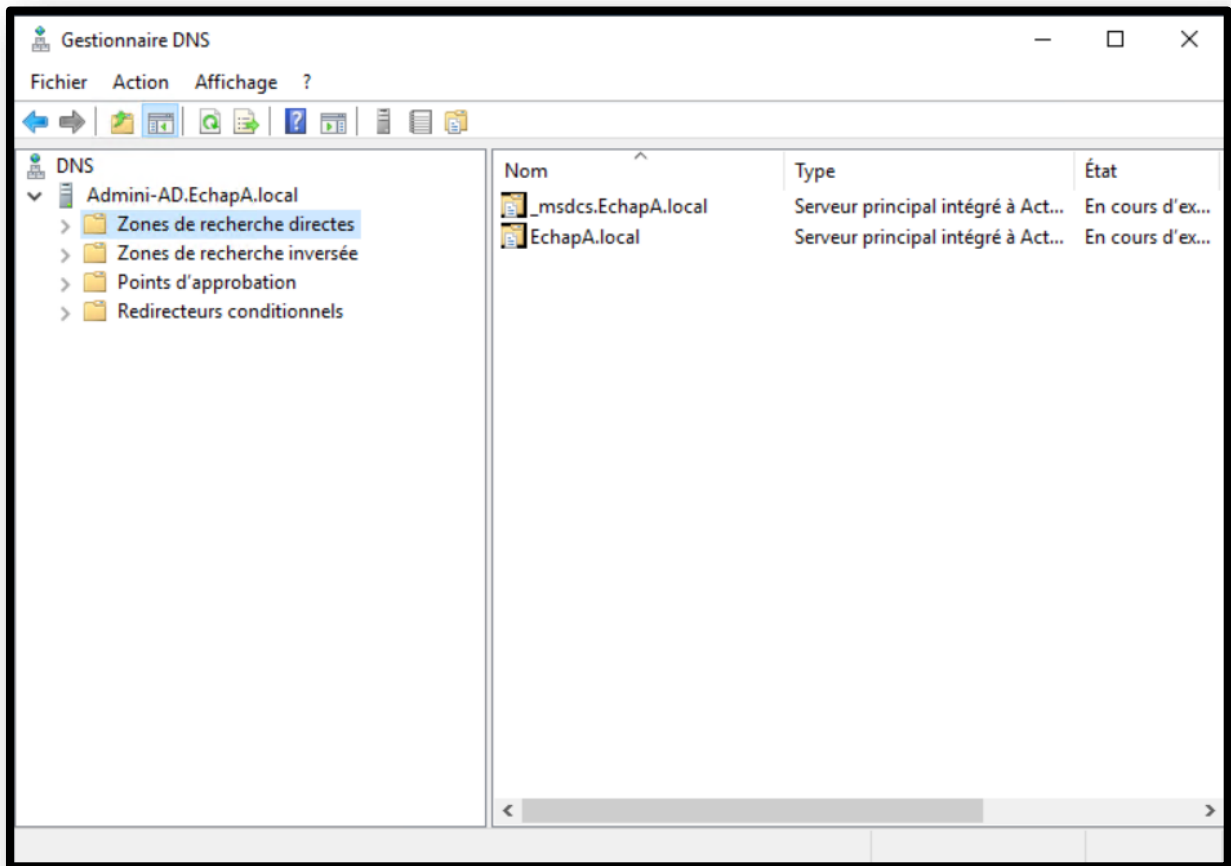
3. Configurer le DNS



De là, nous allons configurer le serveur DNS



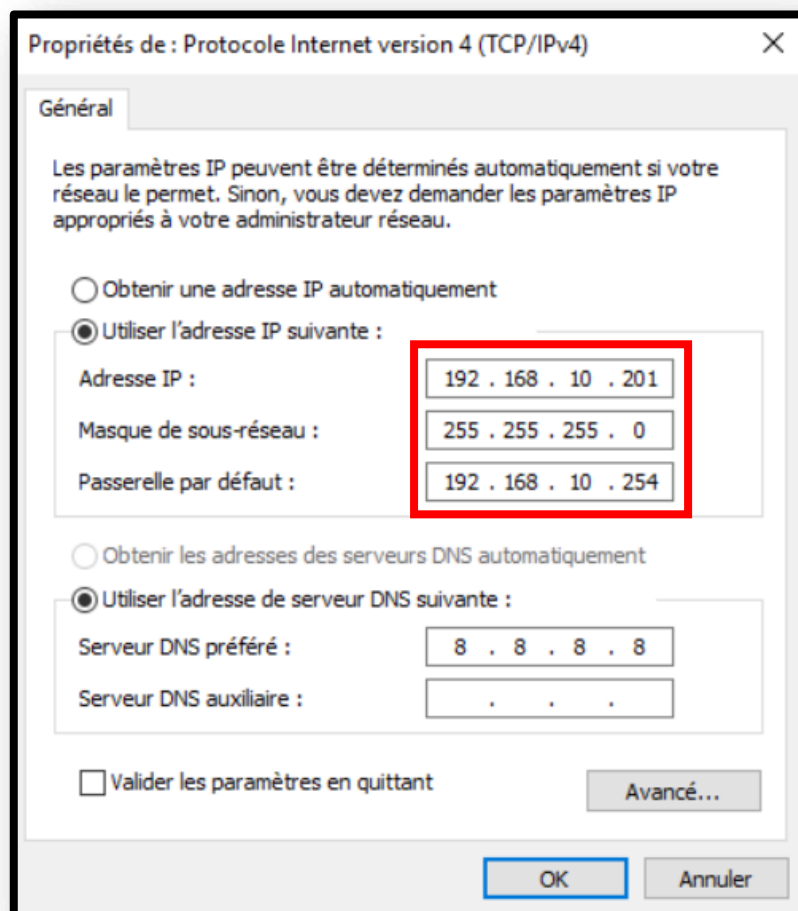
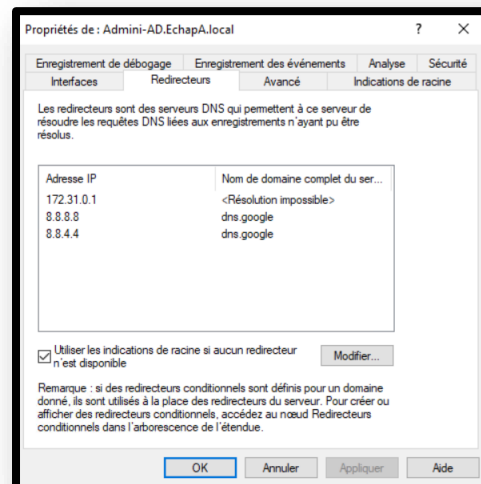
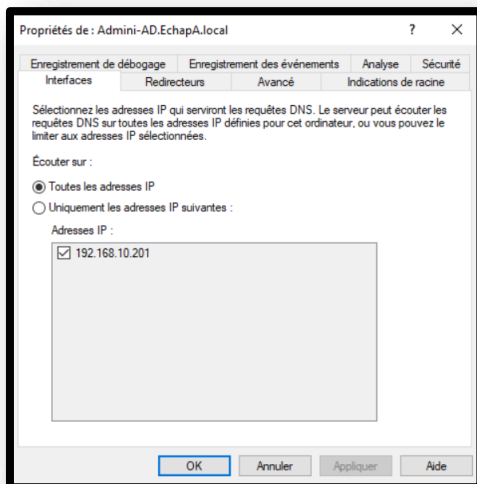
Depuis cette console dans la capture d'écran ci-dessous, vous pouvez gérer tous les serveurs DNS du réseau. En cela, nous n'avons que le serveur précédemment créé.





En cliquant avec le bouton droit de la souris sur "propriétés" sur notre serveur DNS (dans notre cas Admini-AD), 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.



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

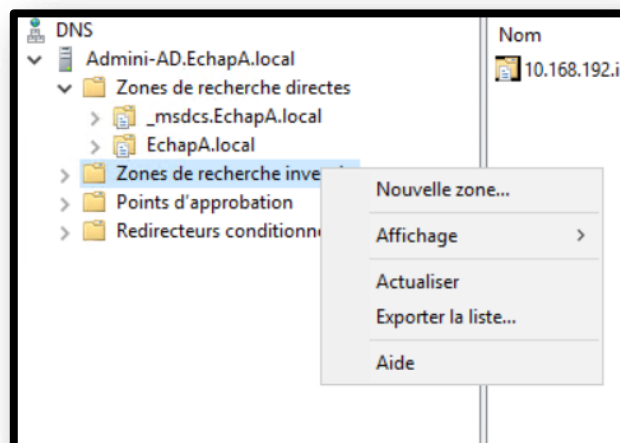


Dans cette fenêtre, nous verrons automatiquement toutes les machines qui seront ajoutées au réseau et au domaine "Echapa".

Nom	Type	Données	Horodateur
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(identique au dossier parent)	Source de nom (SOA)	[86], admini-ad.echapa.lo...	statique
(identique au dossier parent)	Serveur de noms (NS)	admini-ad.echapa.local.	statique
(identique au dossier parent)	Hôte (A)	172.31.254.127	21/11/2023 10:00:00
admini-ad	Hôte (A)	192.168.10.201	statique

La zone inversée n'a pas encore été créée ! C'est en effet une chose à faire !

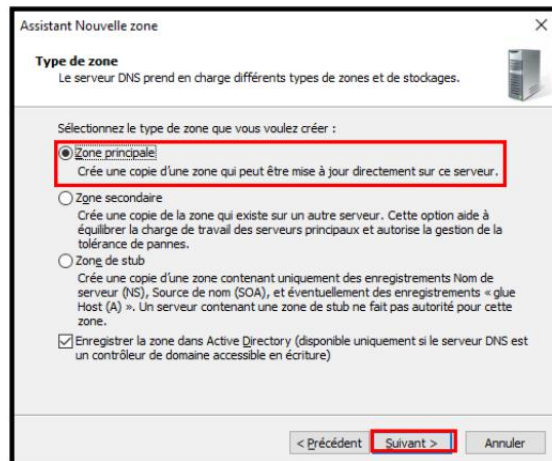
Cliquez ensuite avec le bouton droit de la souris sur "nouvelle zone ...".



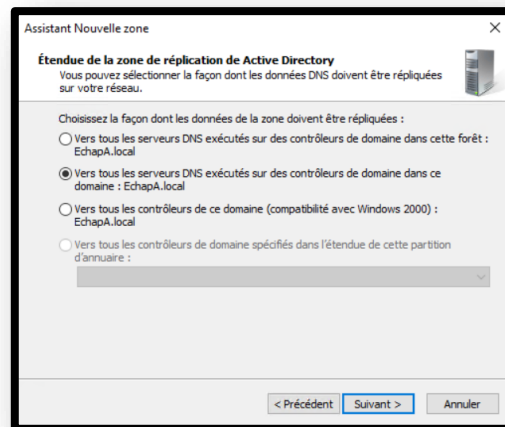
Cliquez ensuite sur « Suivant > »



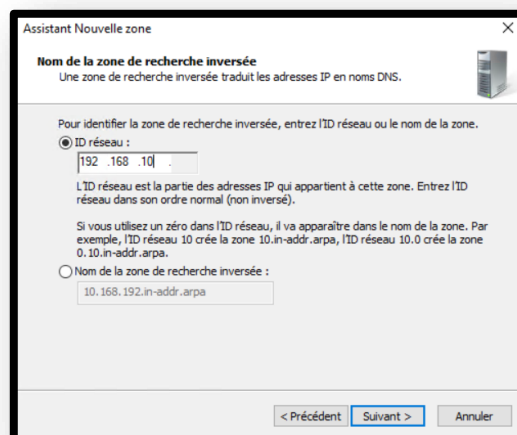
Nous allons donc créer une zone principale.



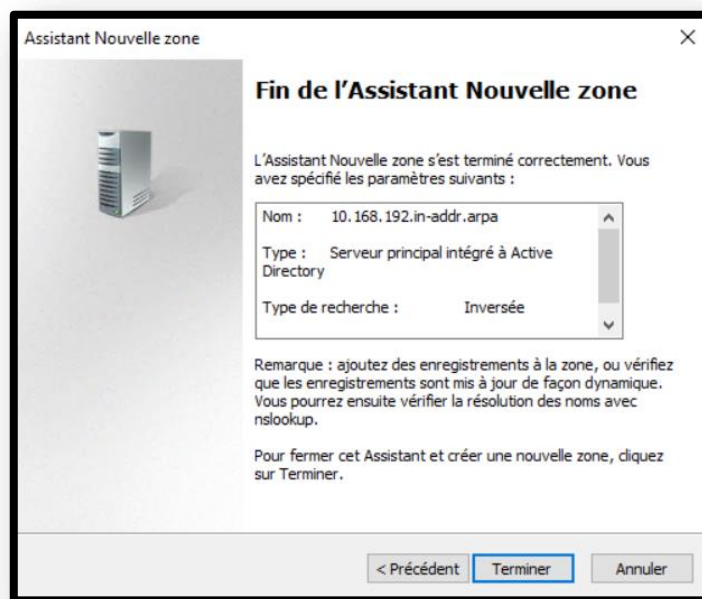
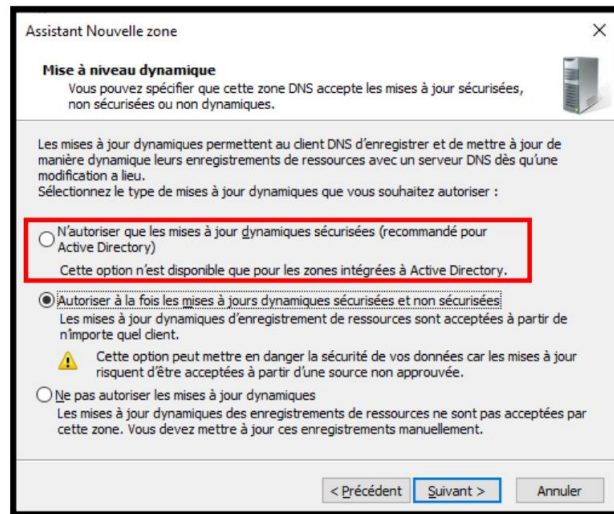
Nous autoriserons la réplication de tous les serveurs DNS dans le domaine « Echapa.local ».



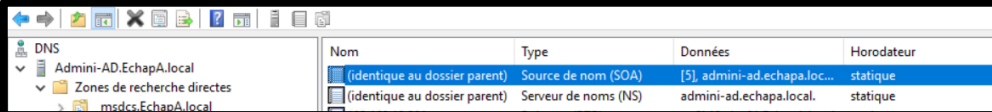
Ici, nous allons entrer l'ID du réseau. Le dernier octet est implicite, vous n'avez donc pas besoin de l'insérer. Dans ce cas, l'ID à saisir est donc les trois premiers octets de l'adresse IP précédemment définie dans la carte réseau.



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.



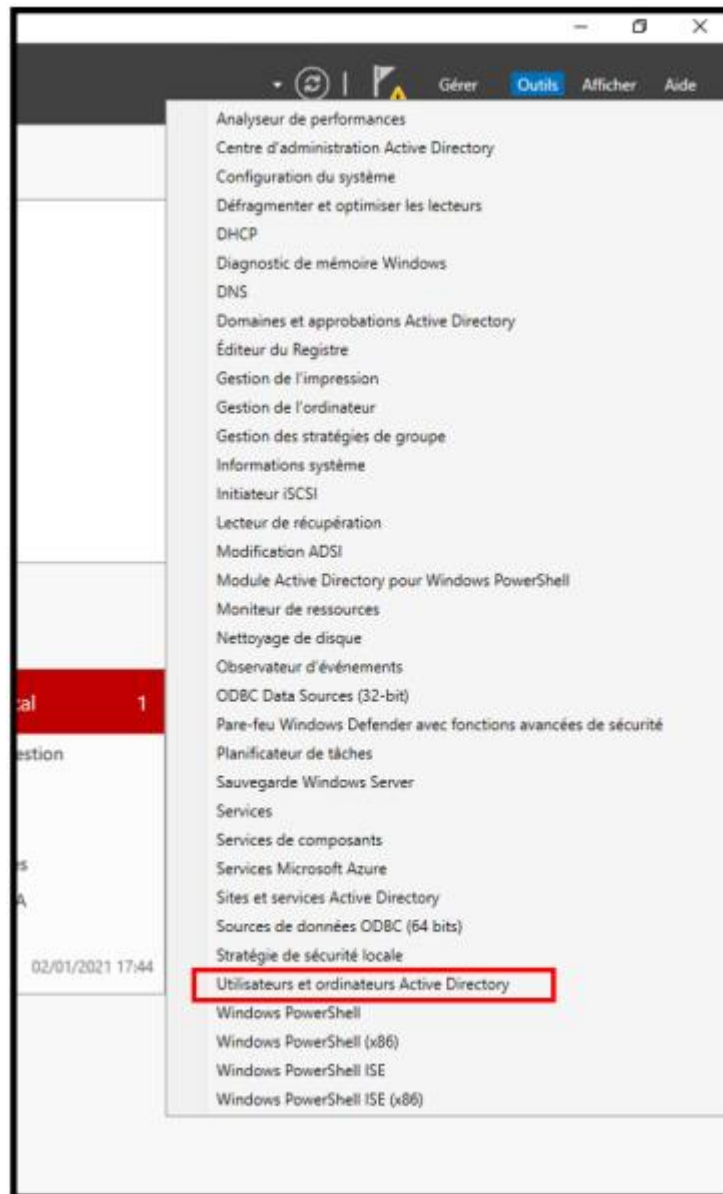
Nous avons déjà le premier "Record" qui est le contrôleur de domaine. Nous avons donc terminé la configuration du serveur DNS ici.



Nom	Type	Données	Horodateur
(identique au dossier parent)	Source de nom (SOA)	[5], admini-ad.echapA.loc...	statique
(identique au dossier parent)	Serveur de noms (NS)	admini-ad.echapA.local.	statique

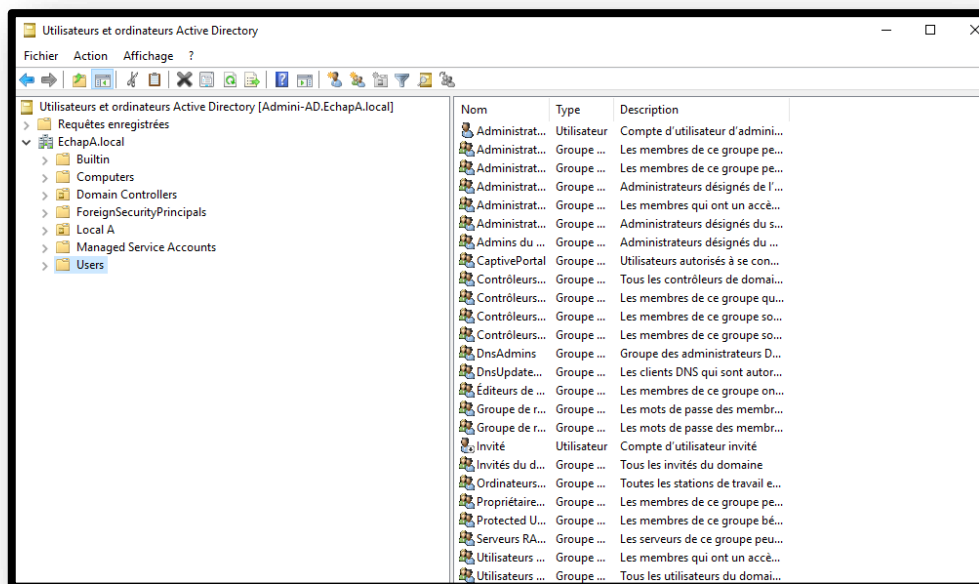
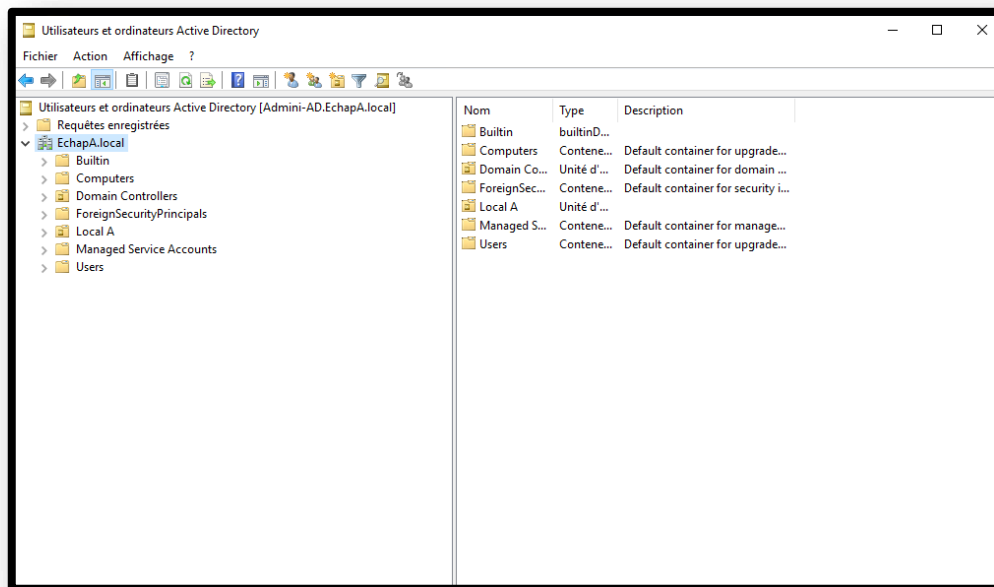
3) *Création d'un utilisateur sur le contrôleur de domaine*

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 "users", 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 « Michel » dans l'OU « Commercial ».

Il suffit alors de créer un nouvel utilisateur 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).

A screenshot of the 'Nouvel objet - Utilisateur' (New Object - User) dialog box in the Active Directory console. The dialog has a title bar with a close button. Below the title bar is a header area with a user icon and the text 'Créer dans : Echapa.local/Local A/Utilisateurs/Commercial'. The main area contains several input fields: 'Prénom :' with 'Michel' entered, 'Initiales :' with an empty field, 'Nom :' with 'Mich' entered, 'Nom complet :' with 'Michel Mich' entered, 'Nom d'ouverture de session de l'utilisateur :' with 'mmich' entered and a dropdown menu showing '@Echapa.local', and 'Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :' with 'ECHAPA\' and 'mmich' entered. At the bottom are three buttons: '< Précédent' (disabled), 'Suivant >' (active/highlighted), and 'Annuler' (disabled).



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.

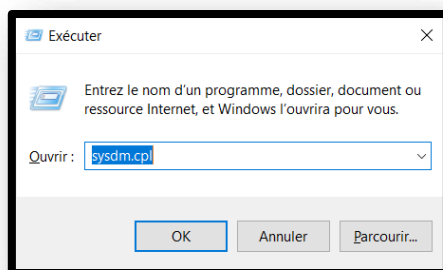
L'icône d'un utilisateur est un "petit homme" tandis que l'icône du groupe est composée de "2 petits hommes".

Nom	Type
Administrateur	Utilisateur
Administrateurs clés	Groupe de sécurité - Global
Administrateurs clés Entreprise	Groupe de sécurité - Universel
Administrateurs de l'entreprise	Groupe de sécurité - Universel
Administrateurs DHCP	Groupe de sécurité - Domaine local
Administrateurs du schéma	Groupe de sécurité - Universel
Admins du domaine	Groupe de sécurité - Global
CaptivePortal	Groupe de sécurité - Global
Contrôleurs de domaine	Groupe de sécurité - Global
Contrôleurs de domaine clonables	Groupe de sécurité - Global
Contrôleurs de domaine d'entreprise en lecture seule	Groupe de sécurité - Universel
Contrôleurs de domaine en lecture seule	Groupe de sécurité - Global
DnsAdmins	Groupe de sécurité - Domaine local
DnsUpdateProxy	Groupe de sécurité - Global

4) Configurer la machine de l'utilisateur sur le domaine

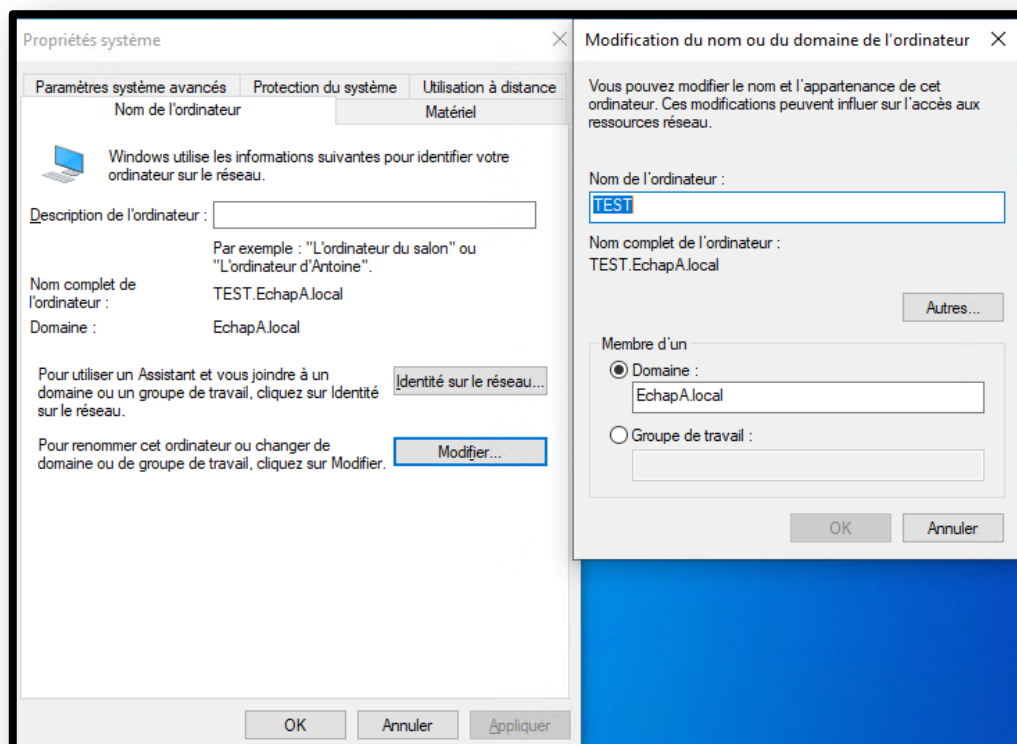


Pour ajouter une machine au domaine vous devez : cliquez sur l'icône Windows en bas à gauche, puis allez dans "paramètres" puis "à propos de votre pc" "renommer ce pc" puis cliquez sur "modifier" et entrez dans le groupe de travail précédemment créé. Vous pouvez aussi accéder à ces paramètres avec un raccourci « Windows + R » et écrire « sysdm.cpl ».

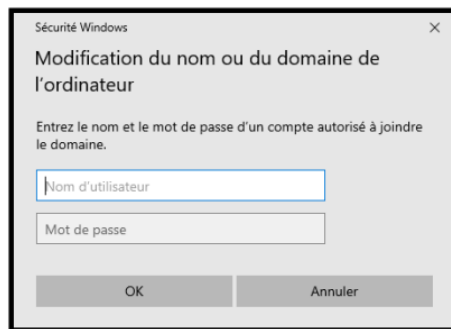


Avant d'effectuer cette opération, il est nécessaire de définir l'adresse IP du serveur précédemment définie comme DNS.

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 « Benoit Matiez » a été utilisé.

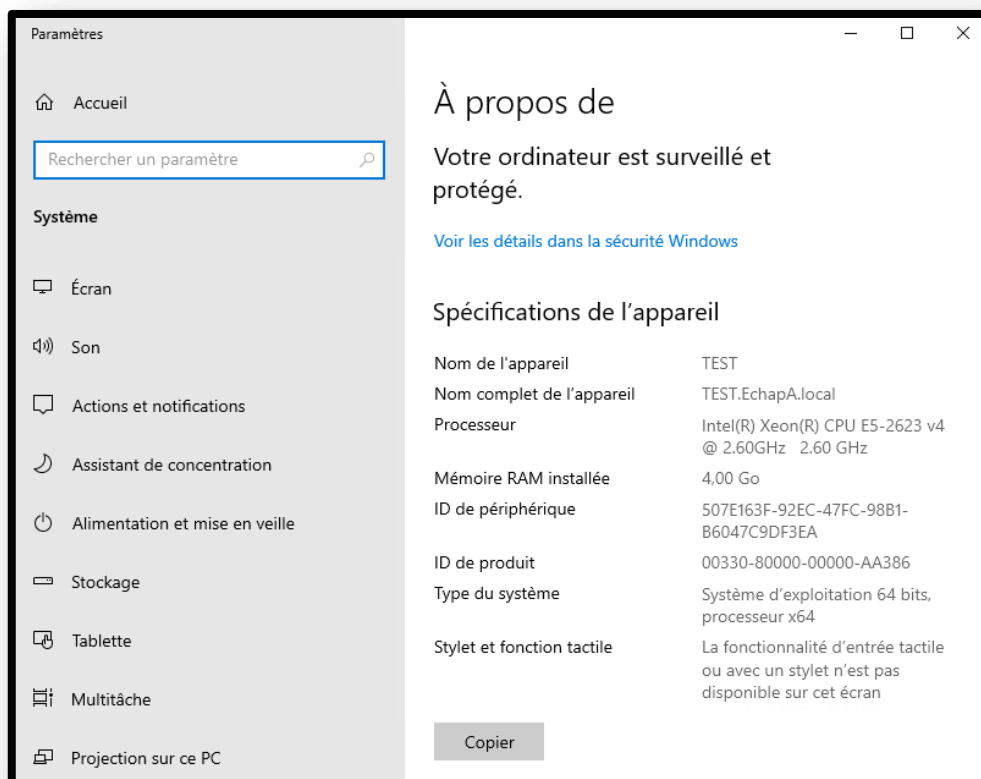


A ce stade, nous devons simplement entrer les informations d'identification pour ajouter ce PC au contrôleur de domaine



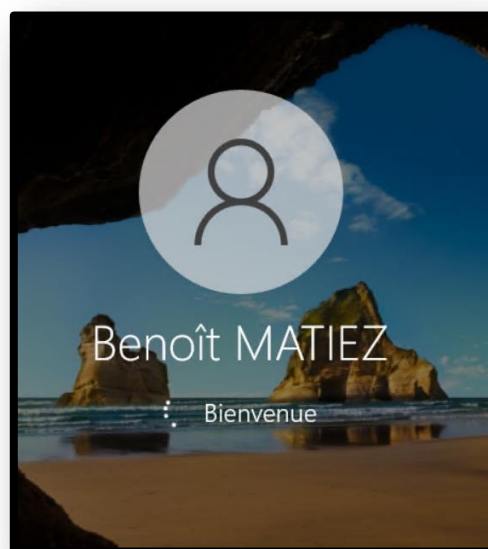
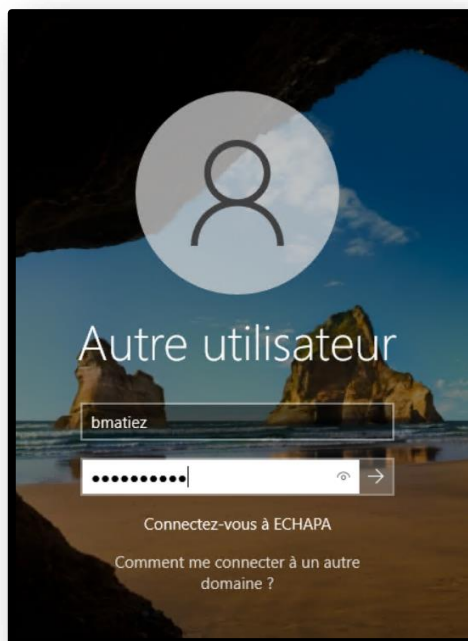
Une fenêtre de confirmation s'affichera ensuite.

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.

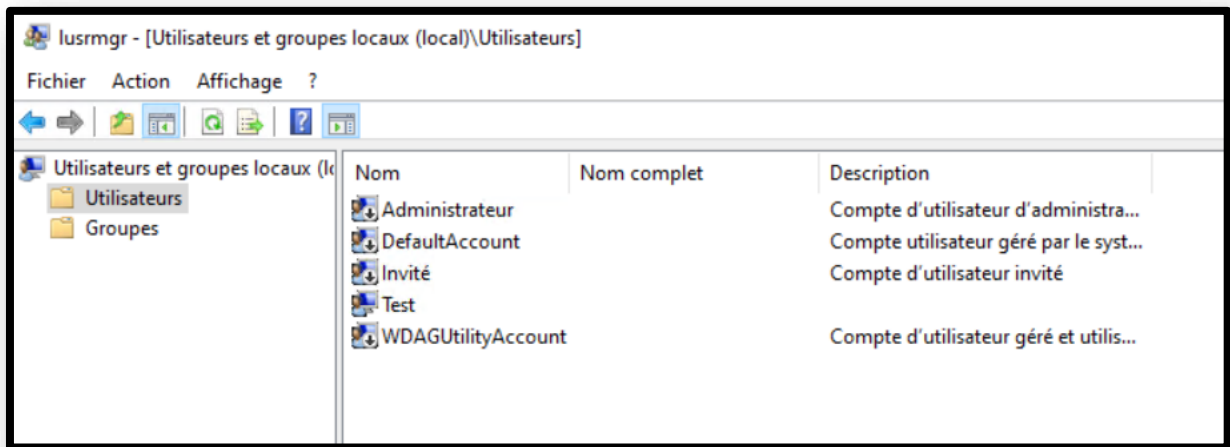


Au redémarrage, vous pouvez accéder en vous connectant directement avec l'utilisateur souhaité. Donc, dans ce cas, nous nous connecterons avec le compte :

- bmatiez : nom de l'utilisateur



Et voici les différents comptes locaux sur la machine :



5) *Mettre en place une stratégie de groupe*

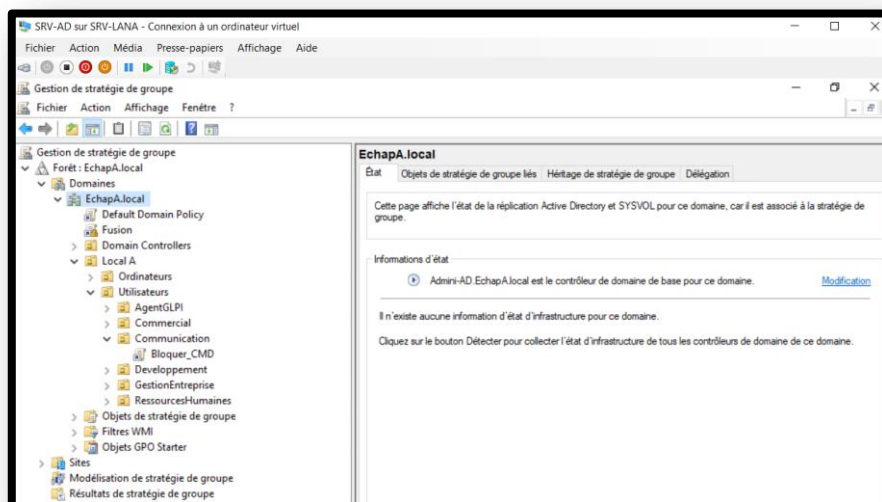
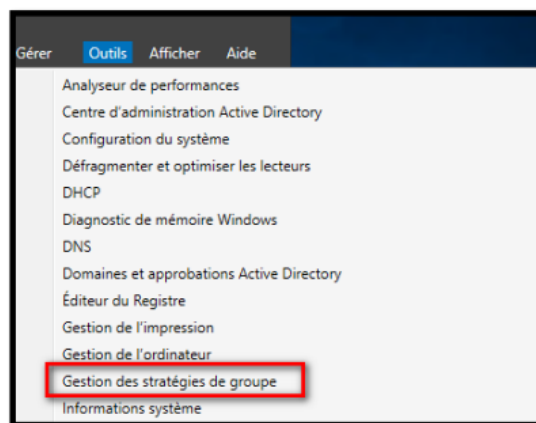


Les stratégies de groupe (en anglais, Group Policy ou GP) sont un ensemble de règles qui contrôlent l'environnement de travail des utilisateurs et des ordinateurs. Ils fournissent une gestion et une configuration centralisées des systèmes d'exploitation, des applications et des paramètres utilisateur 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 ce cas ces opérations ont déjà été effectuées :

- Active Directory et le service DNS (Domain Name Service) ont déjà été configurés,
- La machine de l'utilisateur a été jointe au domaine.

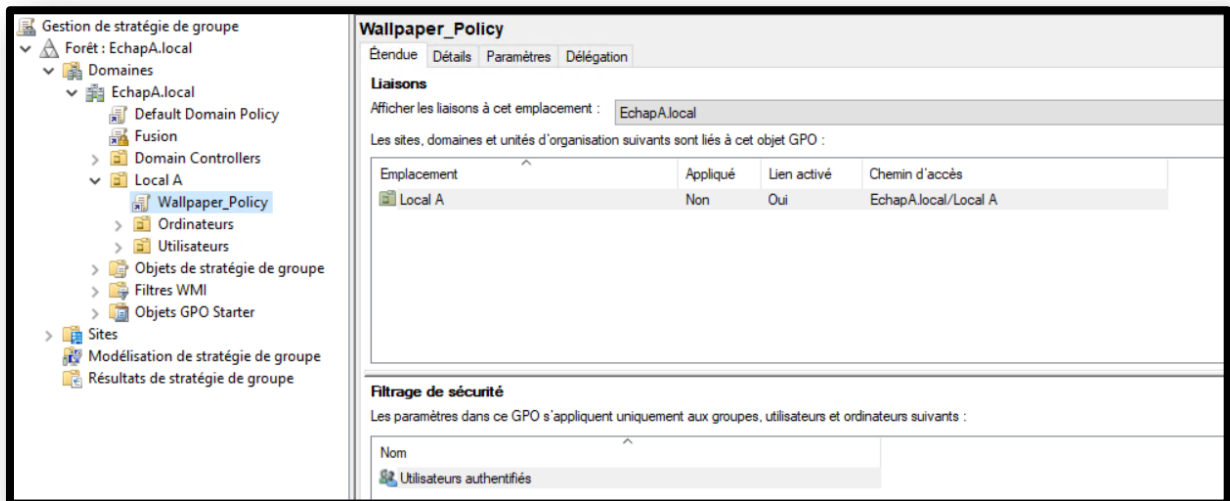




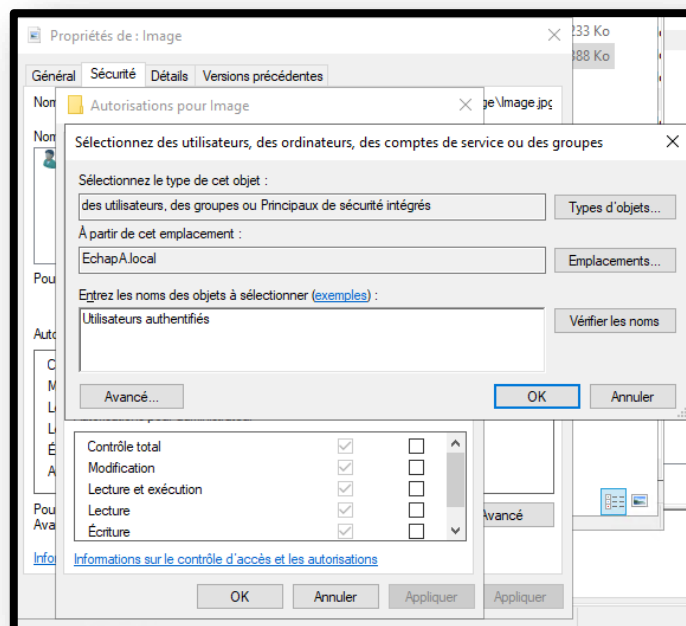
1. Création de l'objet de stratégie de groupe

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 ».

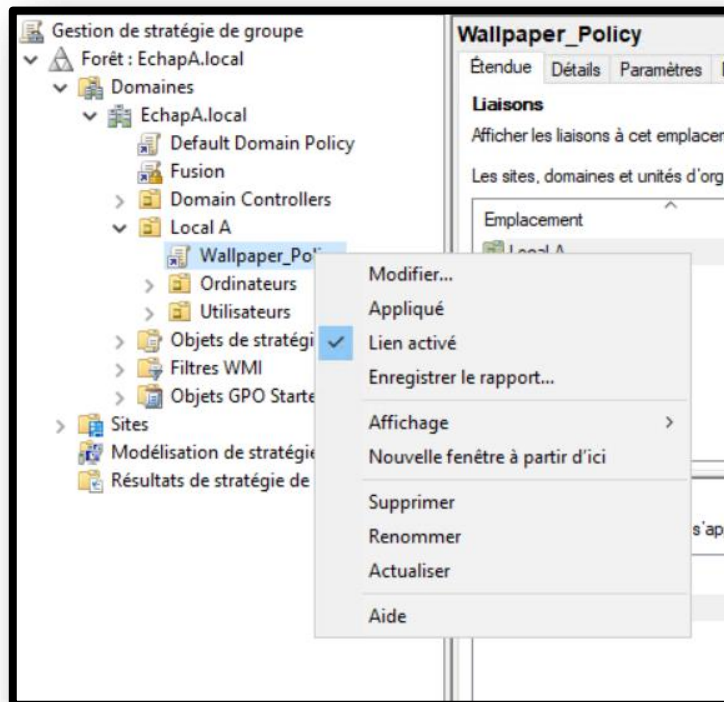


Avant toute chose bien modifier les paramètres de sécurité de l'Image pour que l'utilisateur puisse le voir !

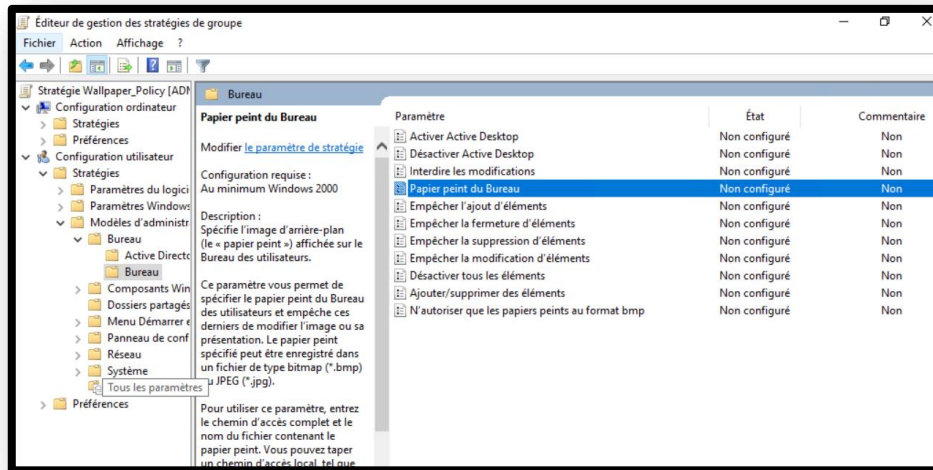


2. Modification de l'objet de stratégie

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

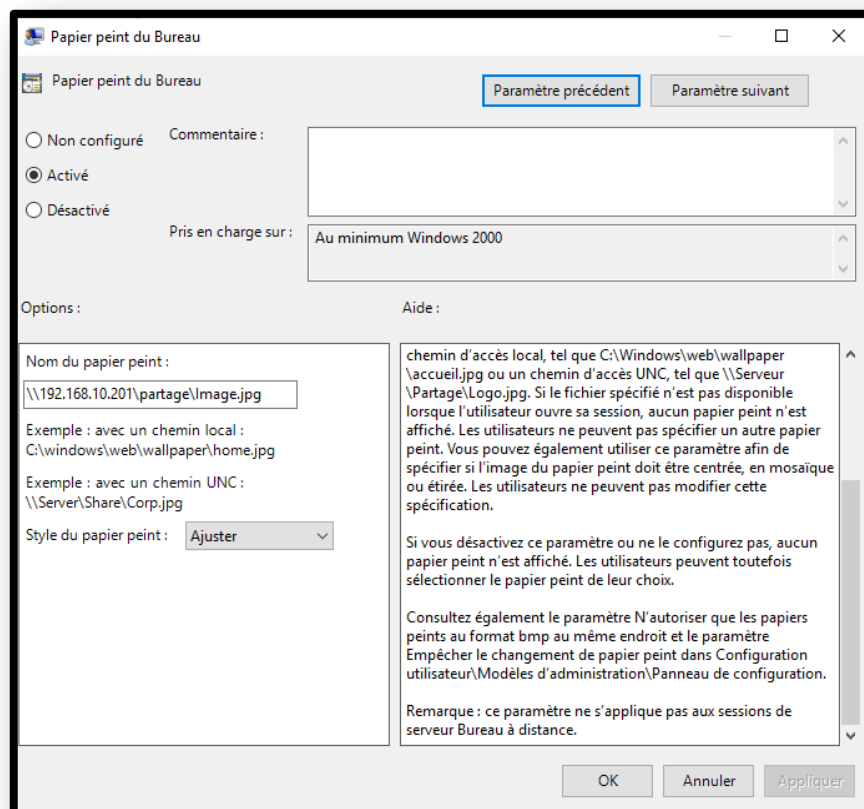


Une fenêtre d'édition apparaîtra. Dans le volet de gauche, sélectionnez Configuration de l'utilisateur> Modèles d'administration> Bureau> Bureau. Dans le volet de droite, double-cliquez sur le paramètre Papier peint du bureau.

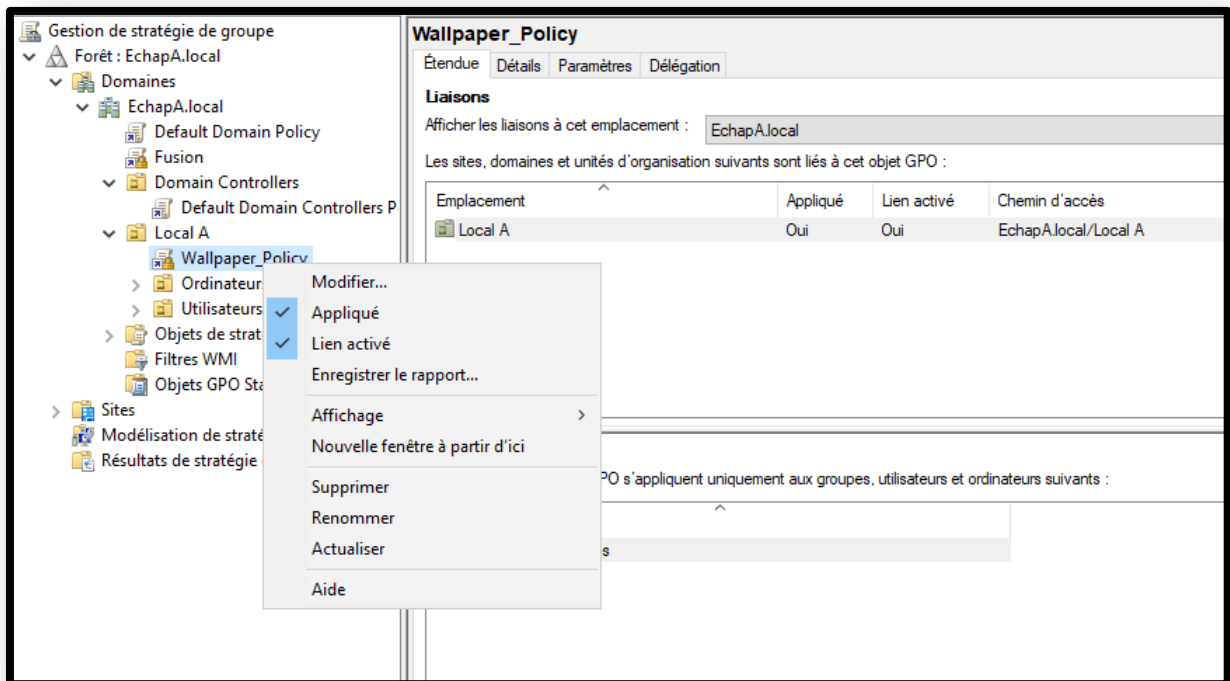


Définissez l'option sur **Activé**, puis spécifiez l'emplacement et le style du papier peint. Dans cet exemple, nous spécifions un chemin local parce que le fichier image pour le fond d'écran du bureau est stocké sur le lecteur local du serveur du contrôleur de domaine et que le style de papier peint 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 « **Activer Active Desktop** » (puis définir l'option sur « **Activé** »)



3. Application de l'objet de stratégie





4. Vérification de la stratégie

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 « gpupdate / 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: Invite de commandes
Microsoft Windows [version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur.WIN-L4K7LTQNFEL>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.

C:\Users\Administrateur.WIN-L4K7LTQNFEL>
```

