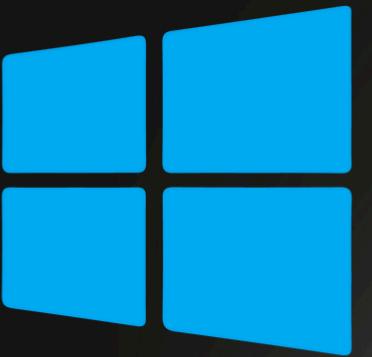




TP-AD DNS WINDOWS SERVER



Microsoft
Active Directory

INSTALLATION DE L'ACTIVE DIRECTORY

PREPARATION DE LA MACHINE WINDOWS SERVER

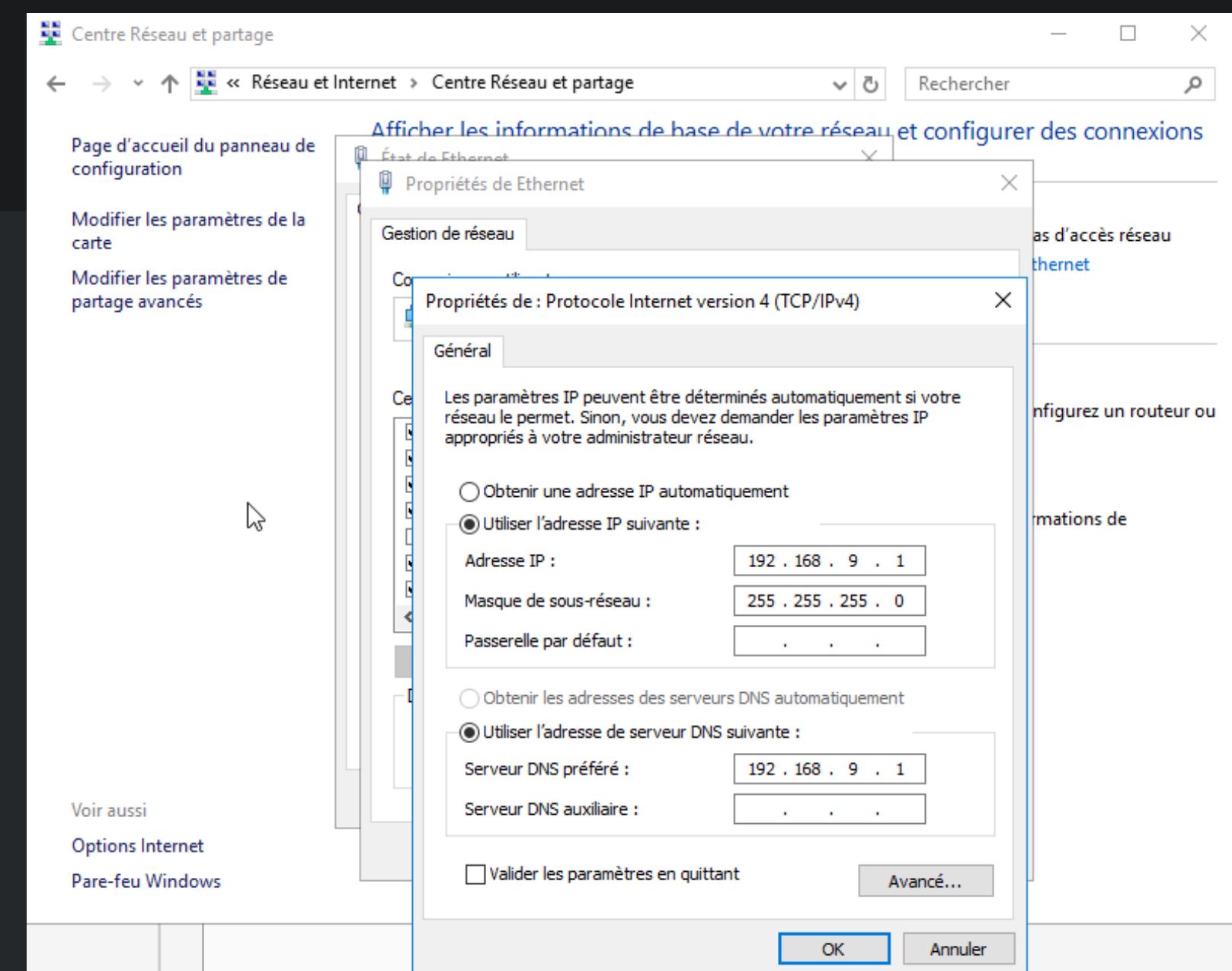
Dans la barre de recherche Windows, tapez « panneau de configuration ». Allez dans réseau et internet -> centre réseau et partage -> Ethernets -> Propriétés -> Protocole internet version 4 -> Propriétés

Configurer l'adresse IP réseau de votre serveur et son DNS :

Adresse IP : 192.168.9.1

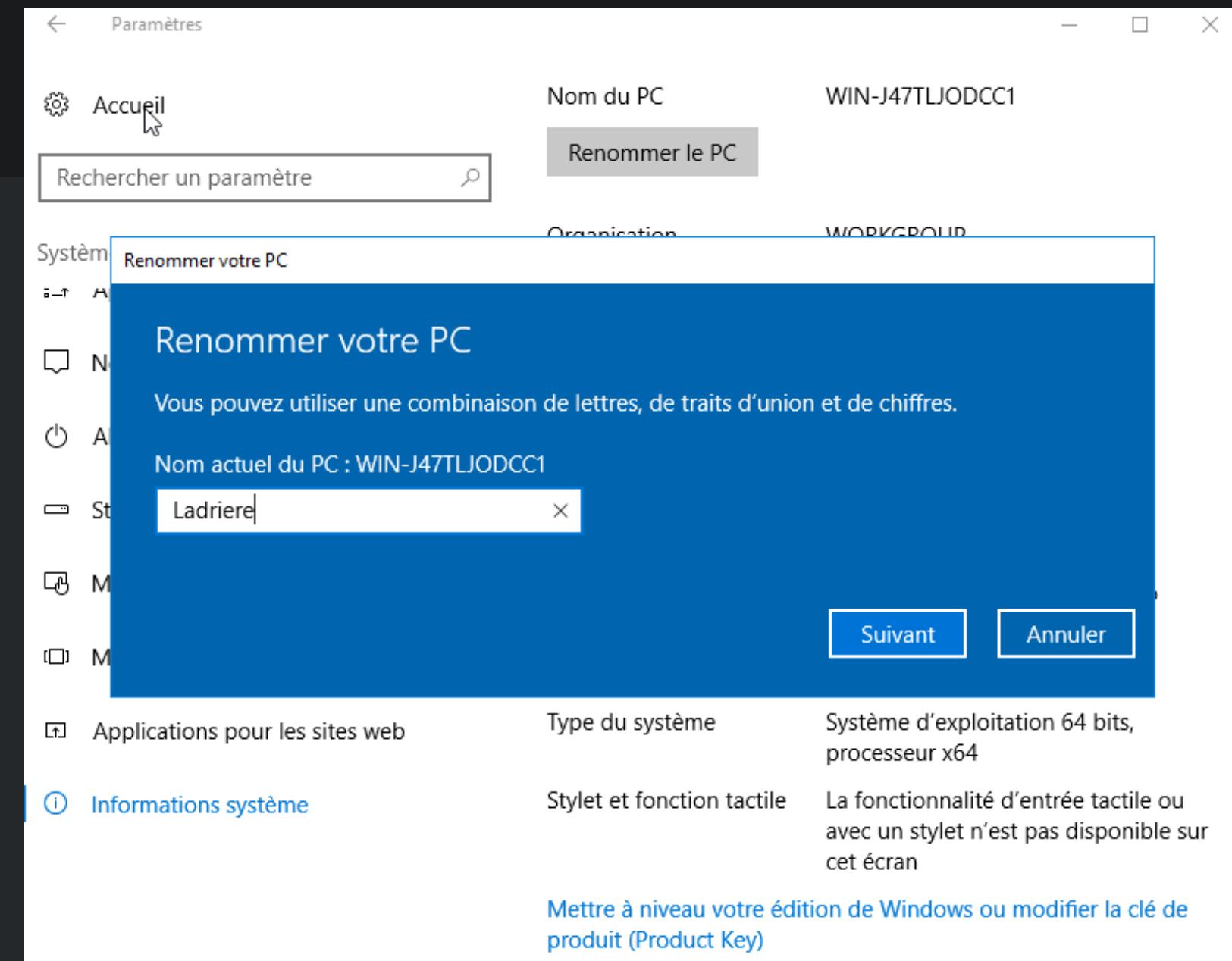
Masque de sous-réseau : 255.255.255.0

Serveur DNS : 192.168.9.1



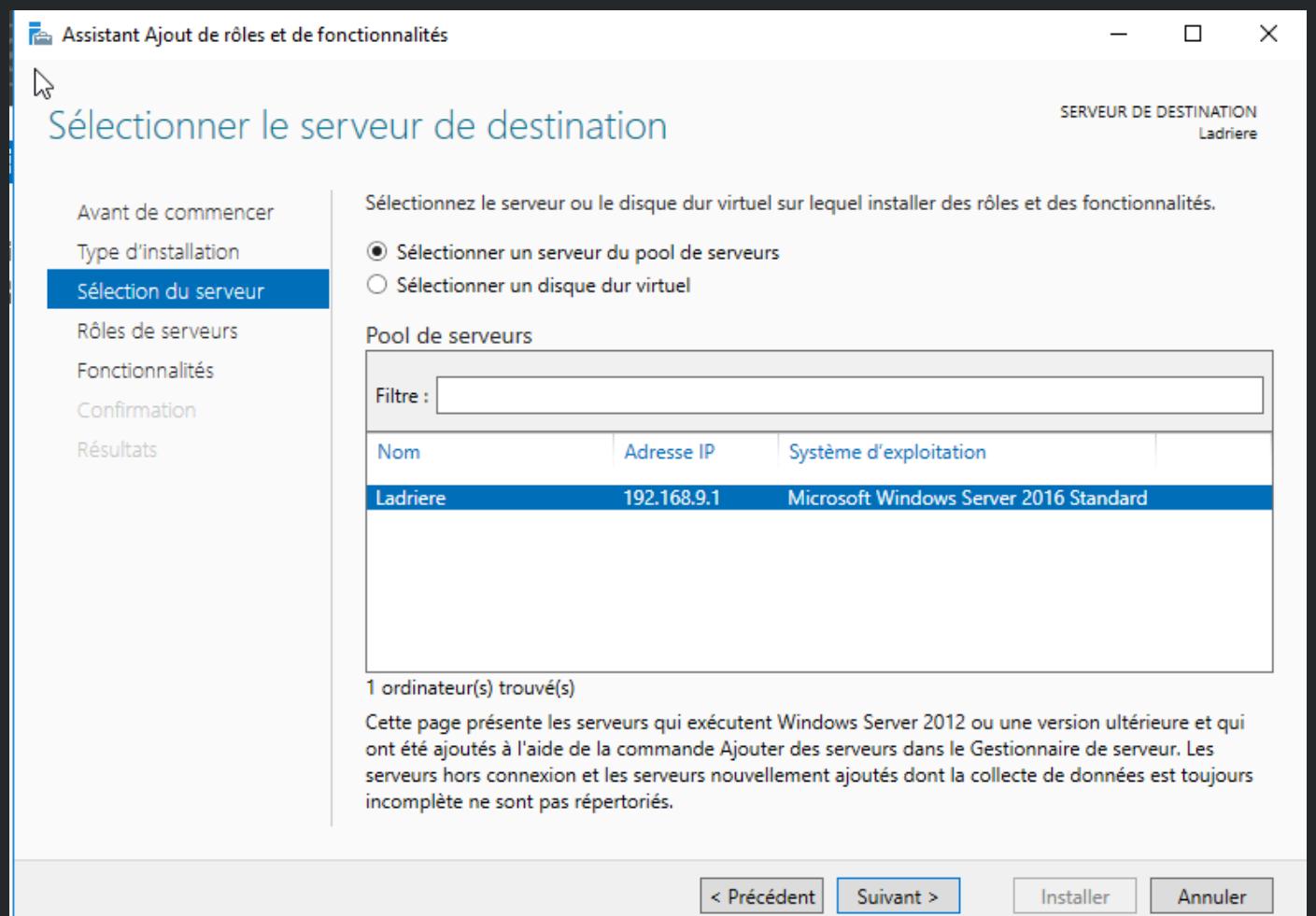
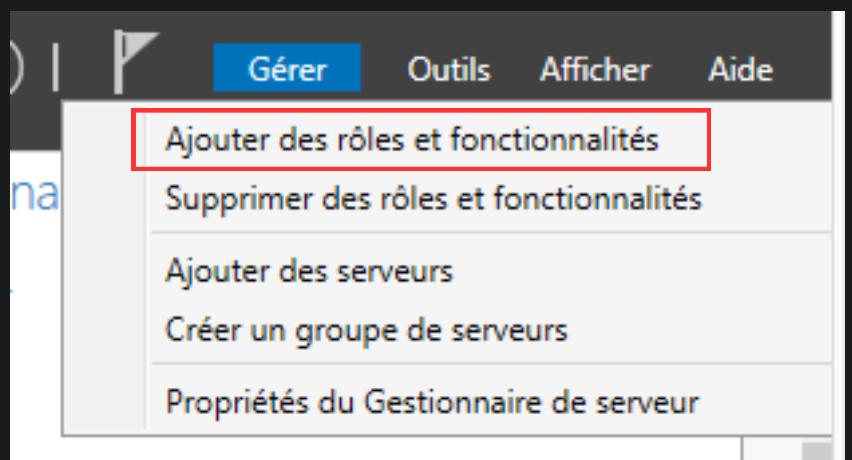
PRÉPARATION DE LA MACHINE WINDOWS SERVER

Pour renommez votre machine vous devez cliquer sur le logo Windows, puis "Paramètres, puis aller dans système puis dans informations système et sélectionnez « renommer ce pc », mettez le nom que vous souhaitez et redémarrer.



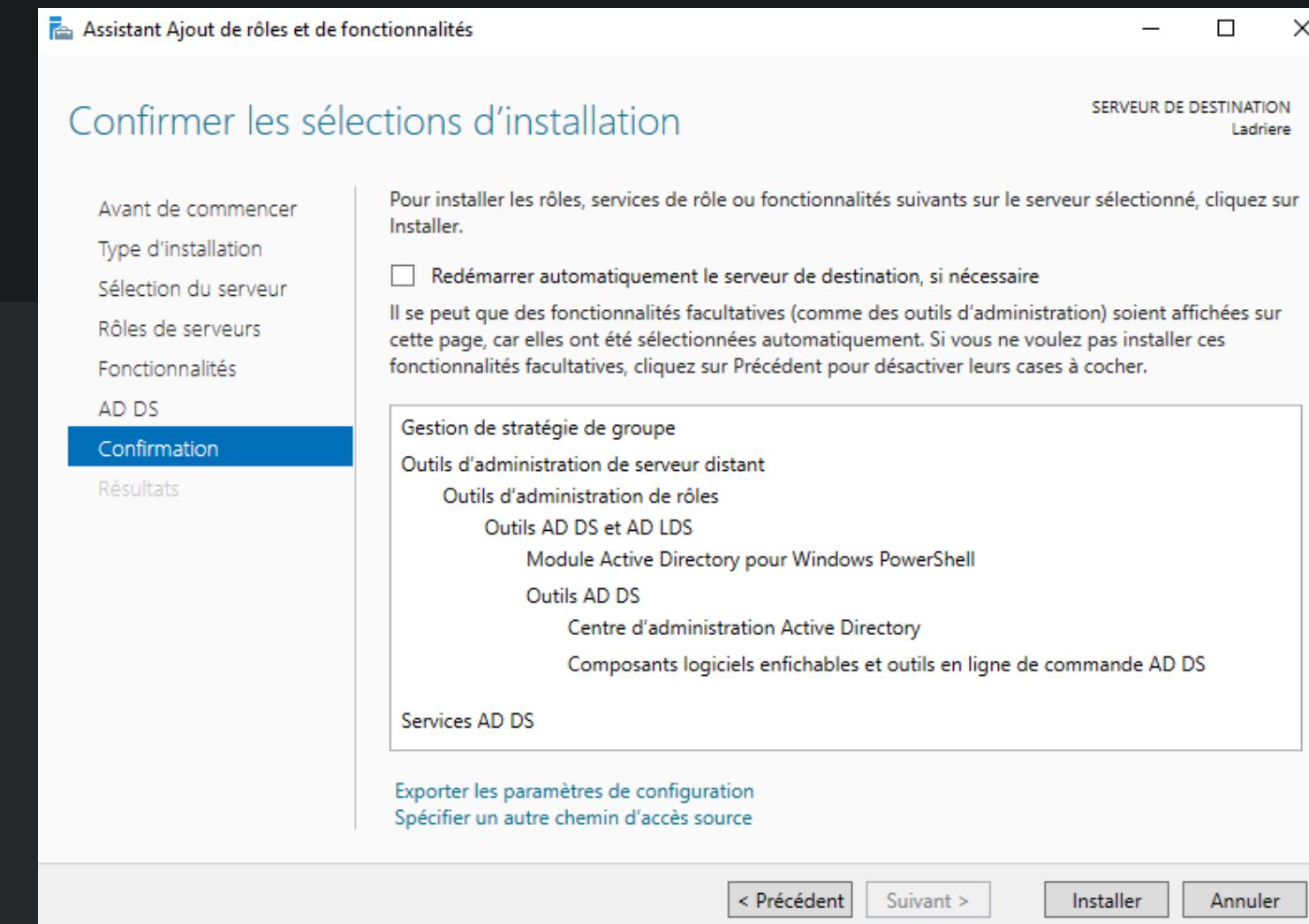
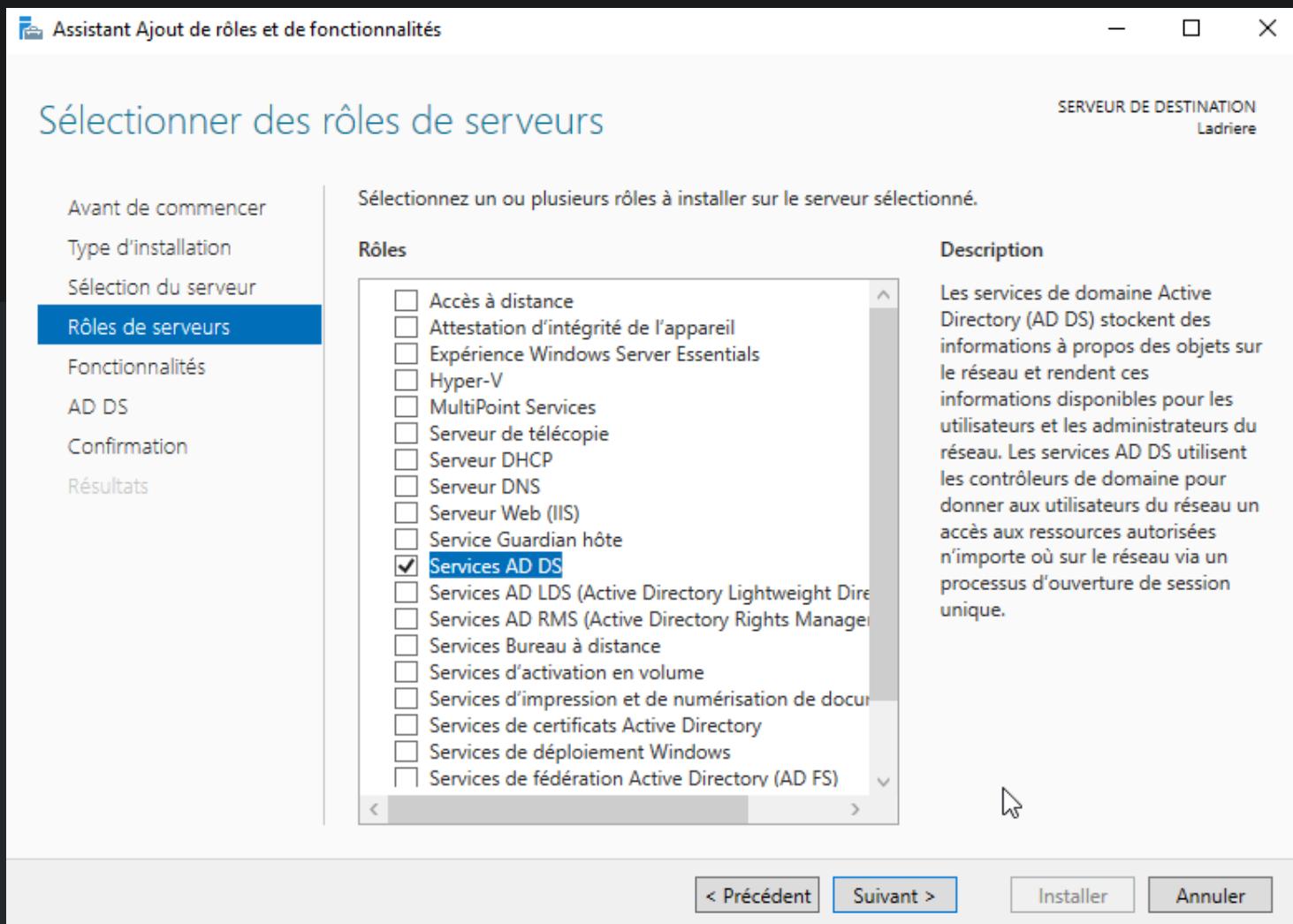
PRÉPARATION DE LA MACHINE WINDOWS SERVER

Pour installer l'Active Directory sur votre Windows serveur sélectionnez en haut à droite "gérer" puis "Ajouter des rôles et fonctionnalités"



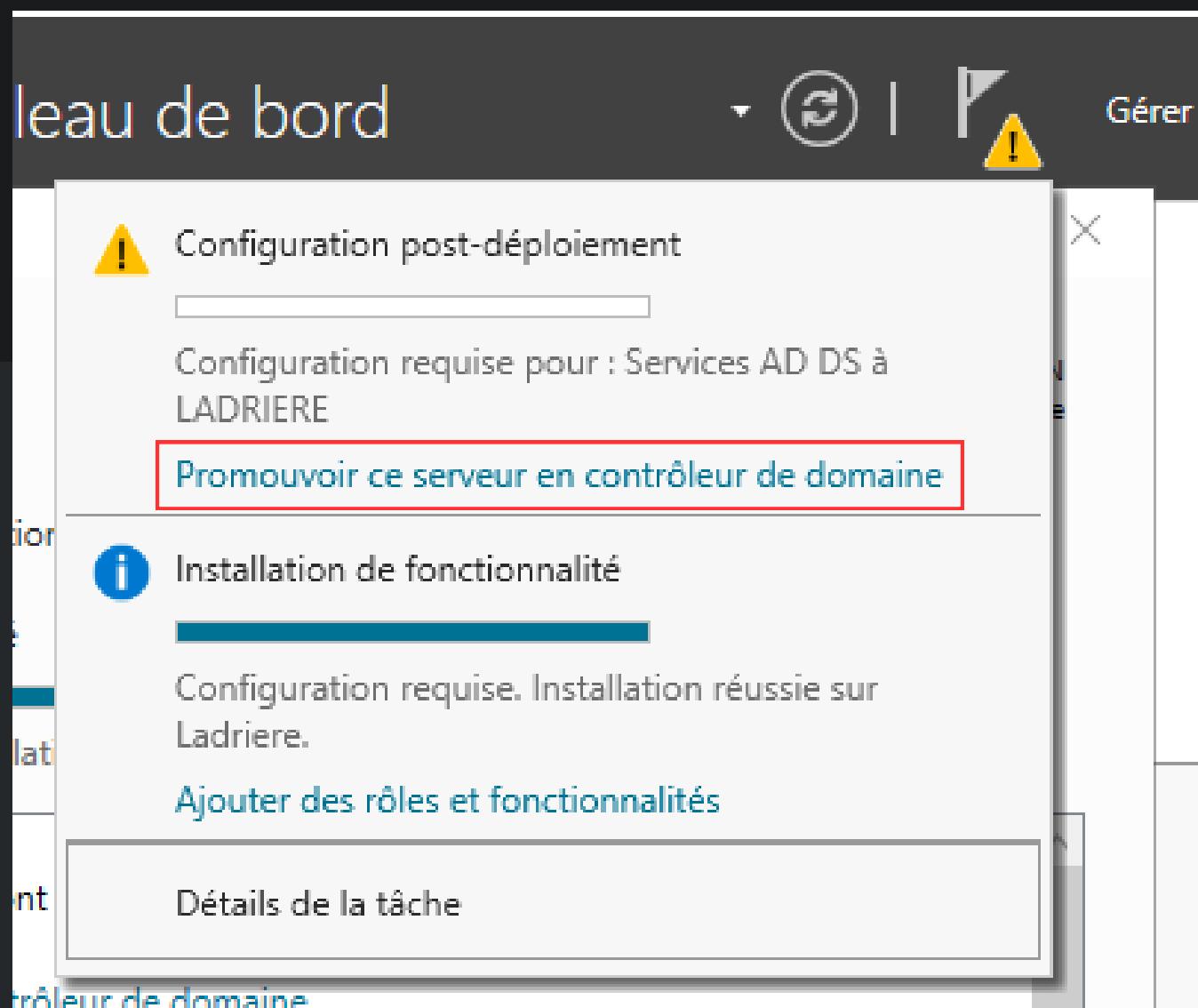
PRÉPARATION DE LA MACHINE WINDOWS SERVER

Ensuite dans “Rôles de serveurs” sélectionnez “Services AD DS” puis faites suivant jusqu'à confirmation et installer



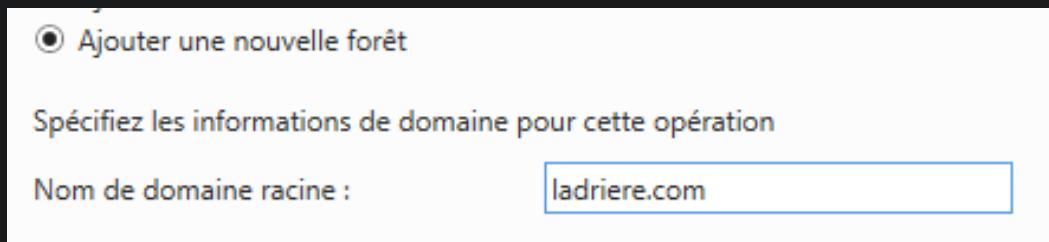
PREPARATION DE LA MACHINE WINDOWS SERVER

Une fois l'installation terminé cliquez sur le drapeau en haut a droite, et cliquez sur "Promouvoir ce serveur en contrôleur de domaine"



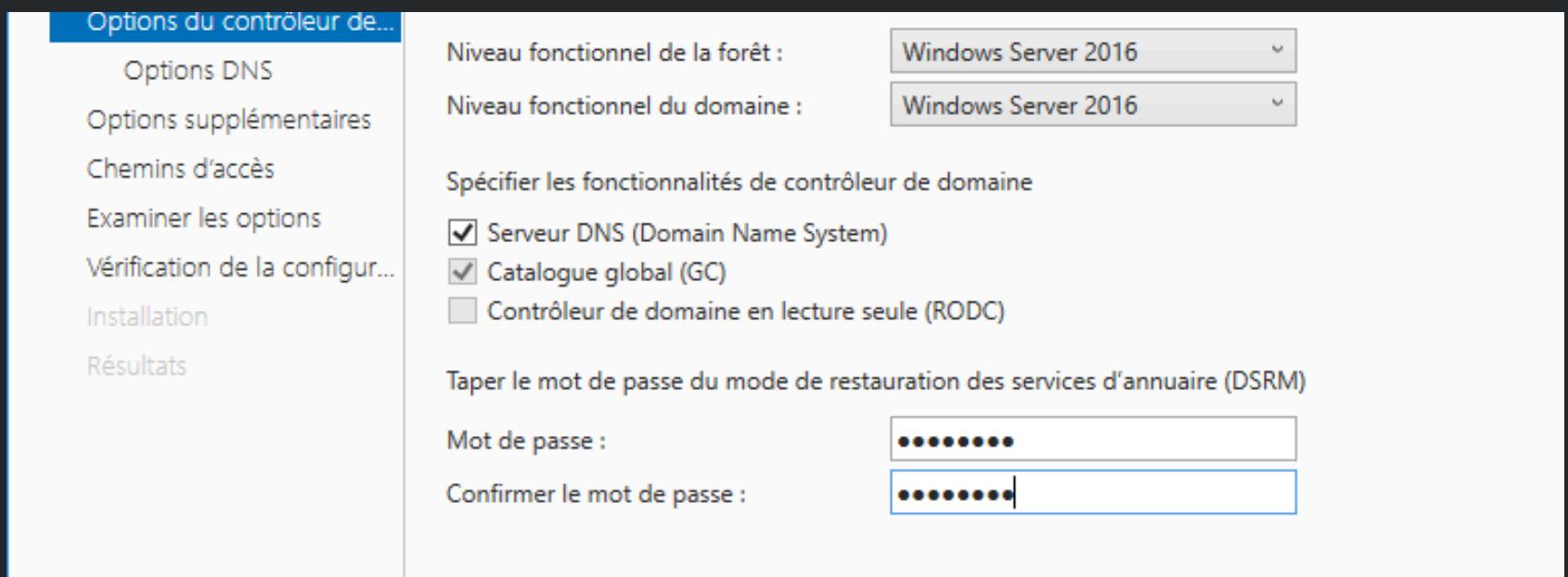
PREPARATION DE LA MACHINE WINDOWS SERVER

Donnez un nom de domaine à votre serveur x.com , ajoutez aussi une nouvelle forêt



Faites suivant

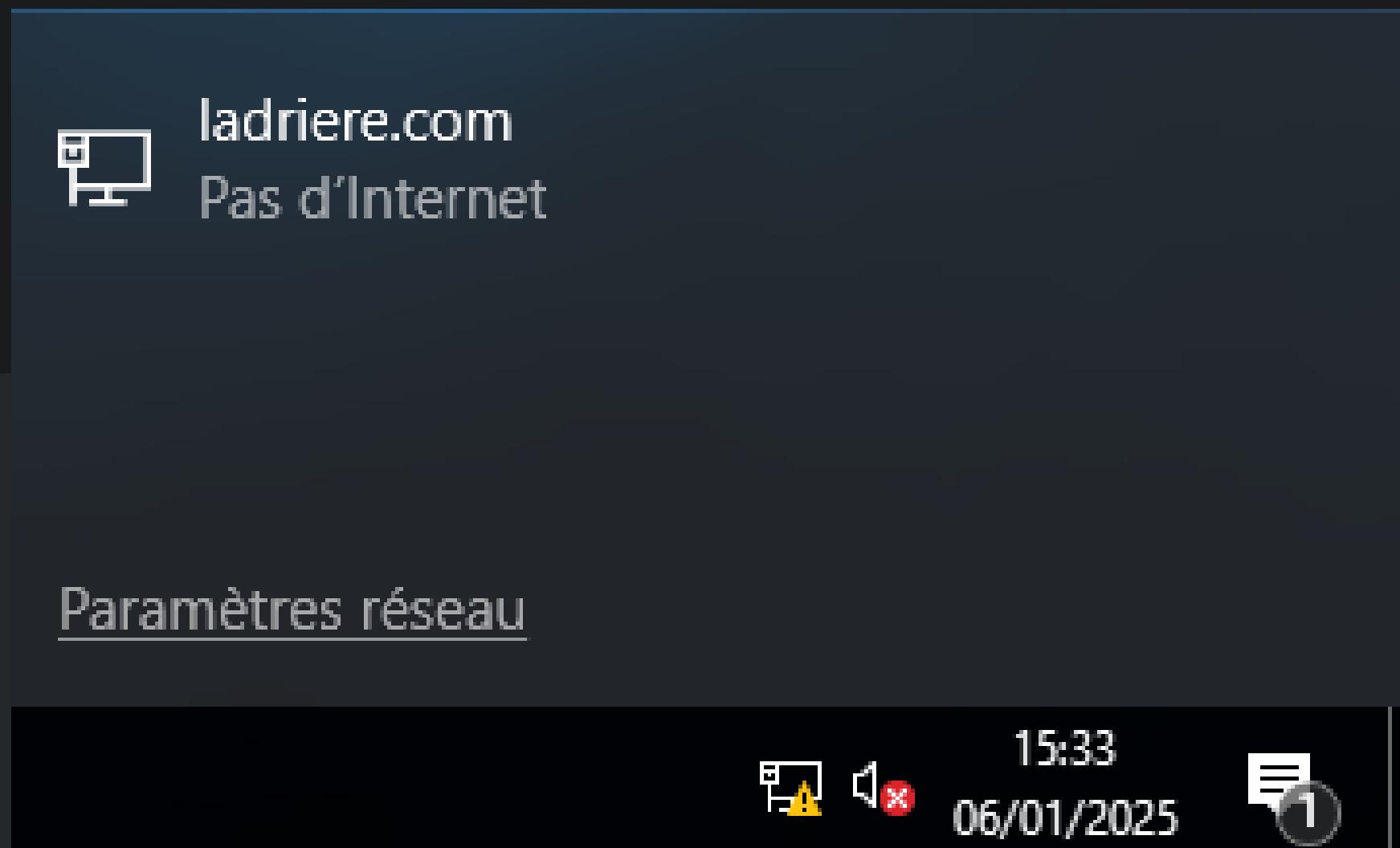
Choisissez comme niveau fonctionnel de la forêt Windows Server 2016 ou 2019
Et mettez aussi un mot de passe



Cliquez ensuite sur "Suivant" jusqu'à arriver à l'installation. Procédez à celle-ci,
votre machine redémarrera ensuite.

PREPARATION DE LA MACHINE WINDOWS SERVER

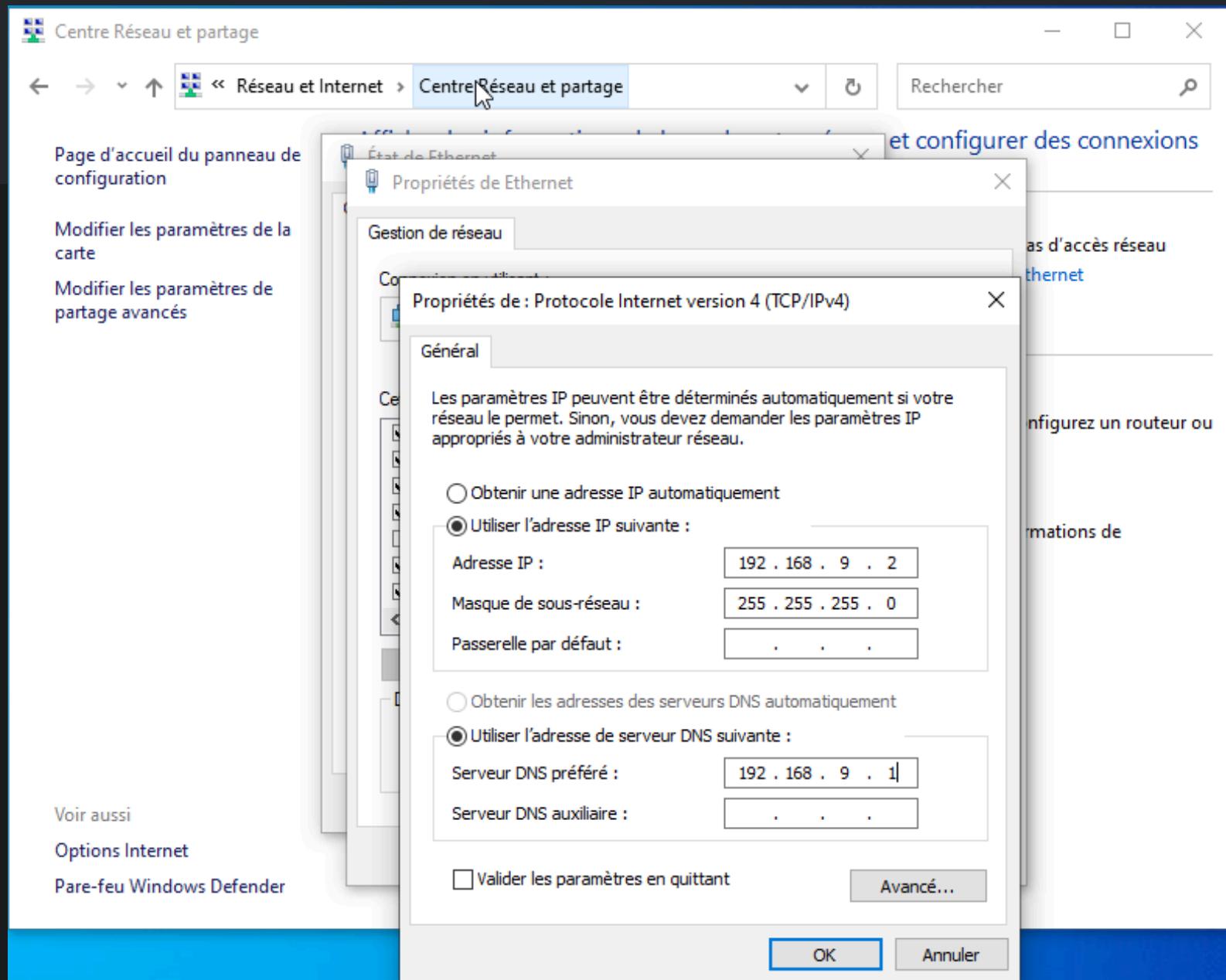
Si le nom de domaine s'affiche correctement en bas à droite au niveau de votre connexion internet, c'est que vous avez effectuez correctement les étapes.



CONFIGURATION DE LA MACHINE WINDOWS

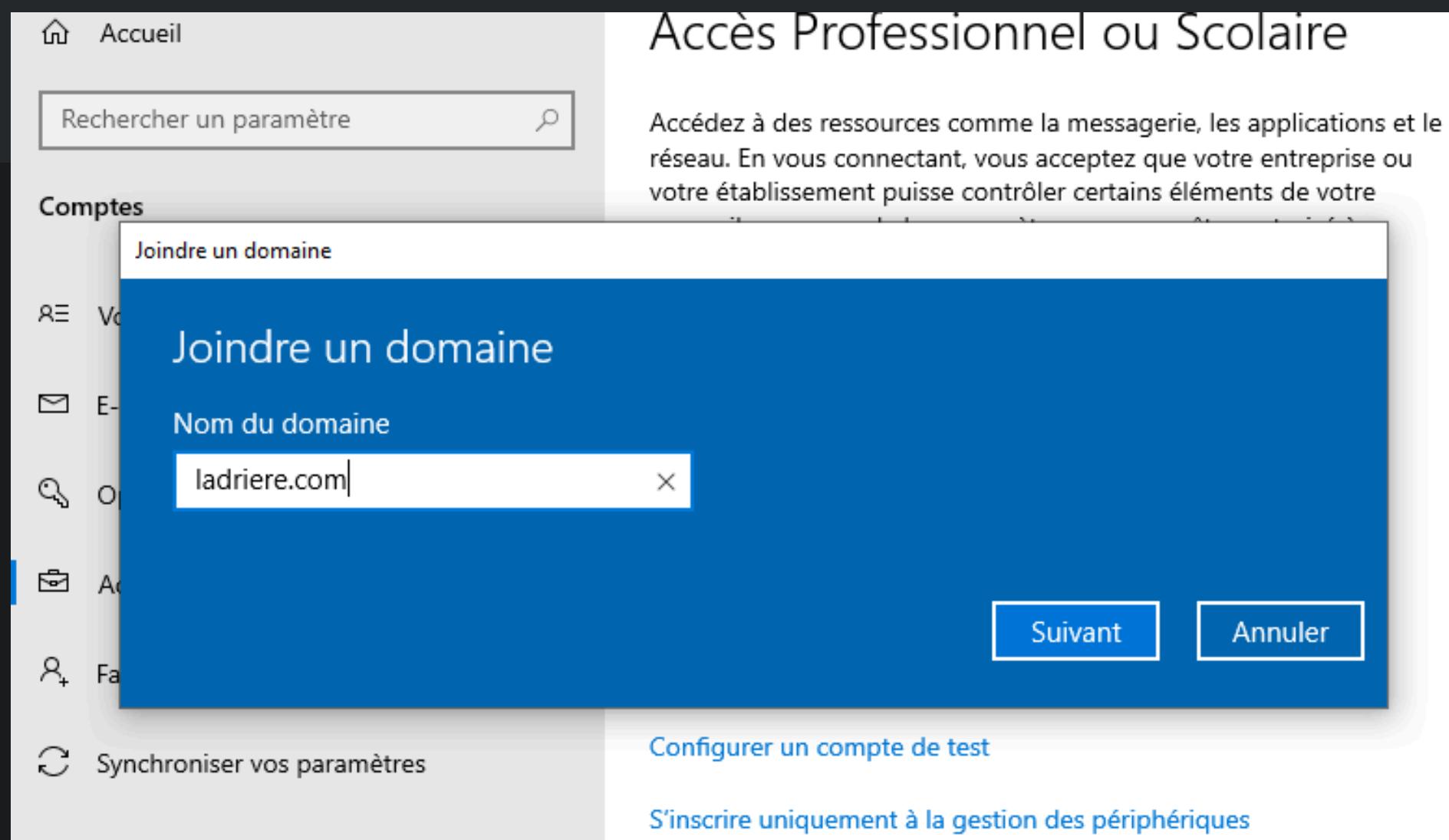
Même principe allez dans le panneau de configuration de votre machine cliente pour y saisir son adresse IP donc 192.168.168.9.2

ATTENTION vous devez saisir une adresse IP cohérente de celle de votre réseau et votre adresse DNS doit être la même que votre Windows serveur



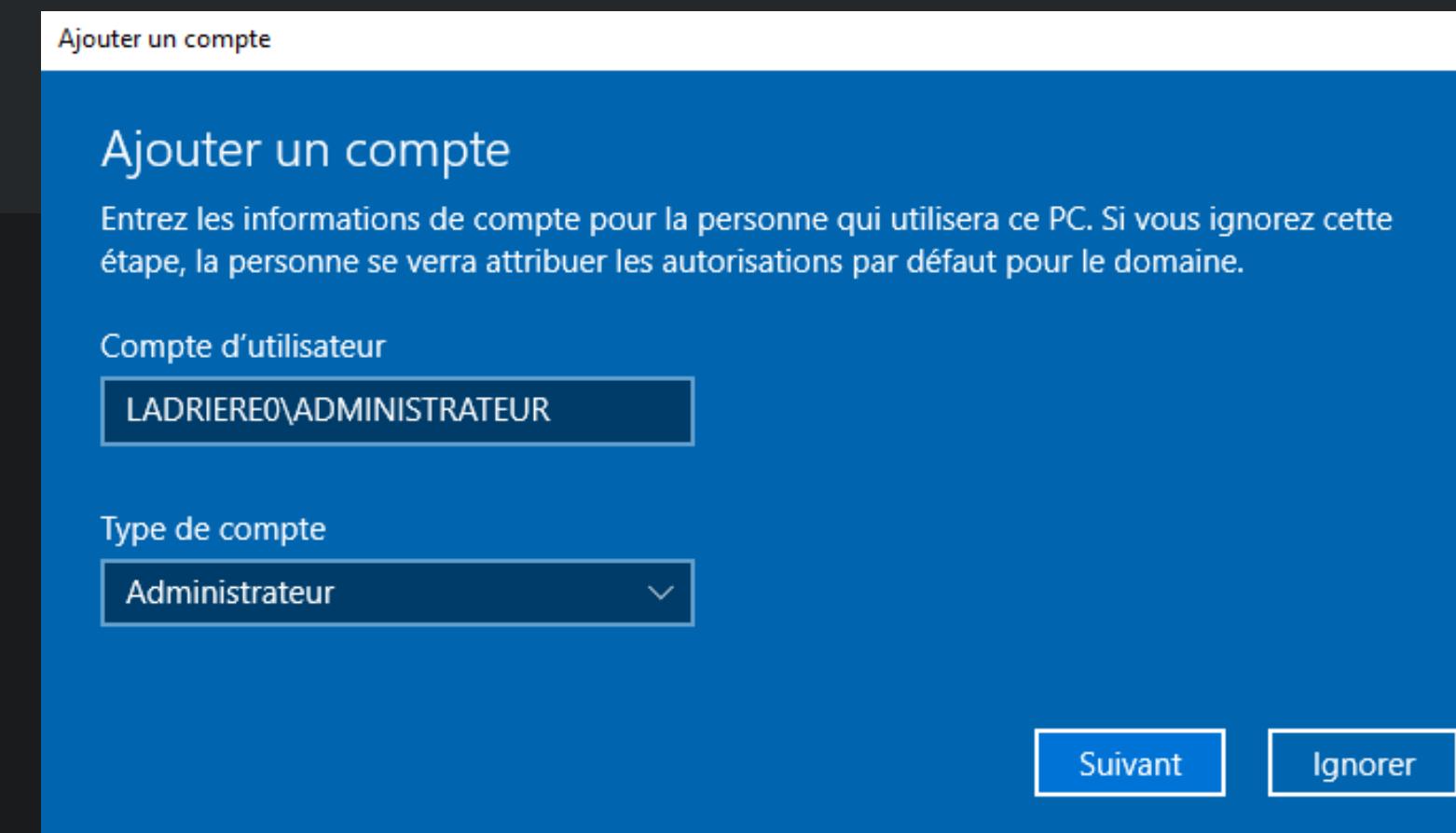
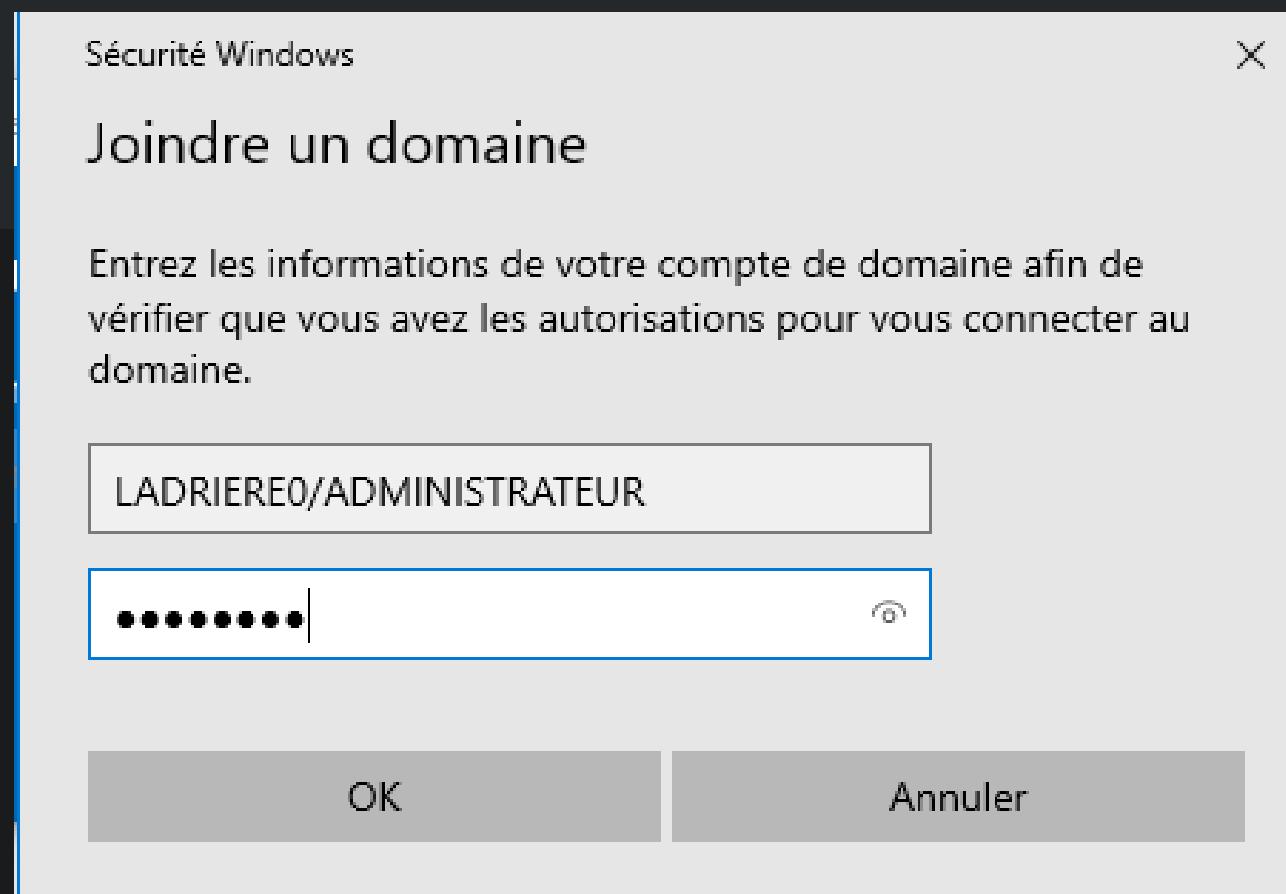
CONFIGURATION DE LA MACHINE WINDOWS

Pour que votre machine cliente soit relié à votre Windows server vous devez dans les paramètres, allez dans Comptes -> Accès professionnel ou Scolaire -> Se connecter -> Rattacher cet appareil à un domaine Active Directory Local et y saisir le nom de domaine de la machine Windows Server :



CONFIGURATION DE LA MACHINE WINDOWS

Maintenant il faudra entrer le nom de votre compte administrateur de votre machine Windows Serveur et définir le compte en tant que Administrateur sur votre machine cliente et redémarrer la Machine



VERIFICATION

Pour vérifier que les machines communiquent bien entre elles, nous pouvons pinger les machines l'une vers l'autre voir si cela fonctionne correctement avec la commande ping 192.168.9.X
Nous pouvons observer que les machines communiquent correctement entre elles

Serveur -> Client

```
C:\Users\Administrateur.WIN-J47TLJODCC1>ping 192.168.9.2

Envoi d'une requête 'Ping' 192.168.9.2 avec 32 octets de données :
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.9.2:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
C:\Users\Administrateur.WIN-J47TLJODCC1>
```

Client -> Serveur

```
Microsoft Windows [version 10.0.19045.2965]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\ADMINISTRATEUR>ping 192.168.9.1

Envoi d'une requête 'Ping' 192.168.9.1 avec 32 octets de données :
Réponse de 192.168.9.1 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.9.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
C:\Users\ADMINISTRATEUR>
```

COMMANDÉ NSLOOKUP

Pour interroger le serveur DNS pour obtenir les informations définies pour un domaine on va utiliser la commande nslookup suivi de notre nom de domaine

```
C:\Users\ADMINISTRATEUR>nslookup ladriere.com
DNS request timed out.
    timeout was 2 seconds.
Server : UnKnown
Address: 192.168.9.1

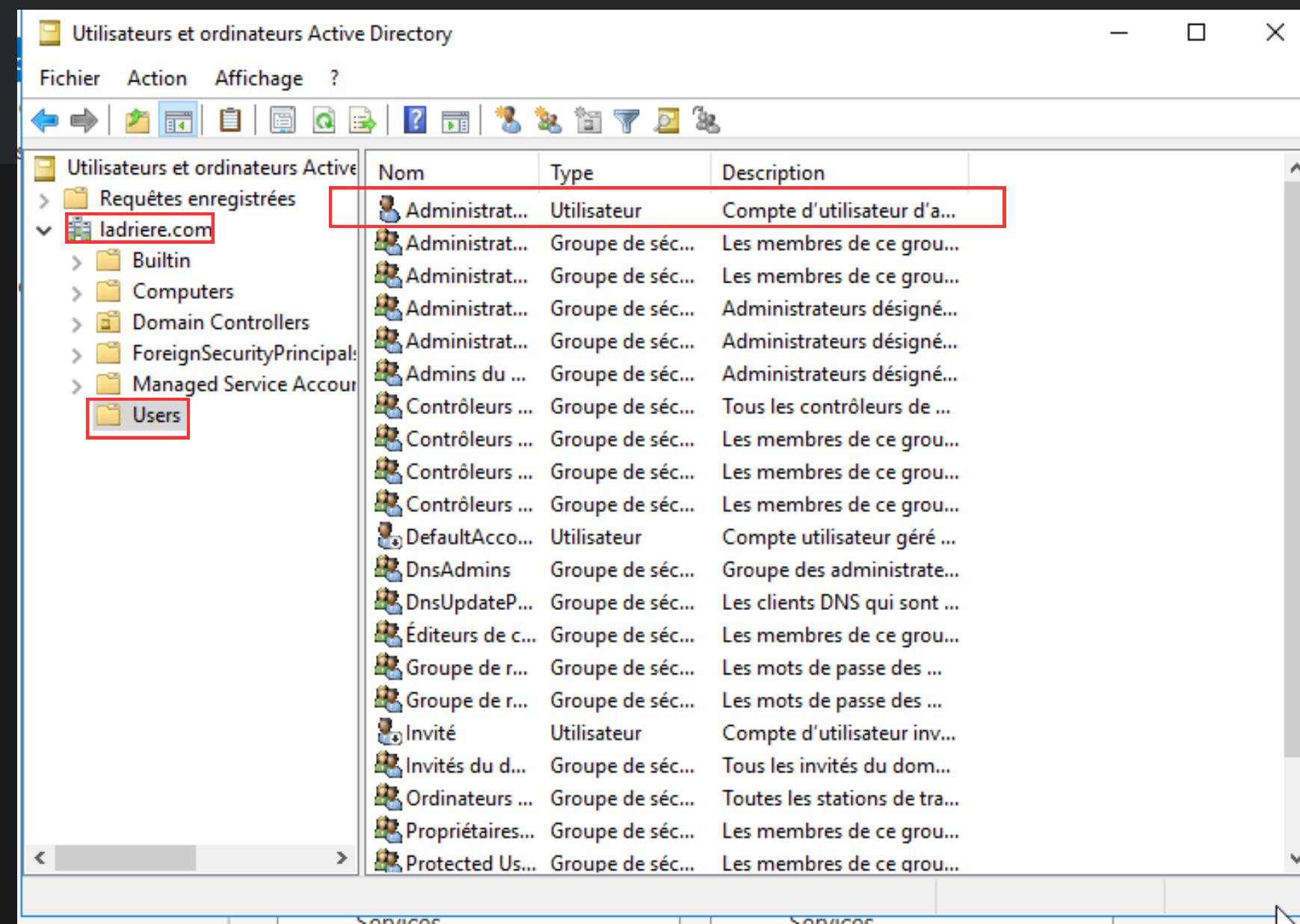
Name : ladriere.com
Address: 192.168.9.1
```

UTILISATEURS ET ORDINATEURS ACTIVE DIRECTORY

Pour savoir qui peut intégrer votre domaine, sur votre machine serveur, allez dans Outils puis aller dans Utilisateurs et ordinateurs Active Directory

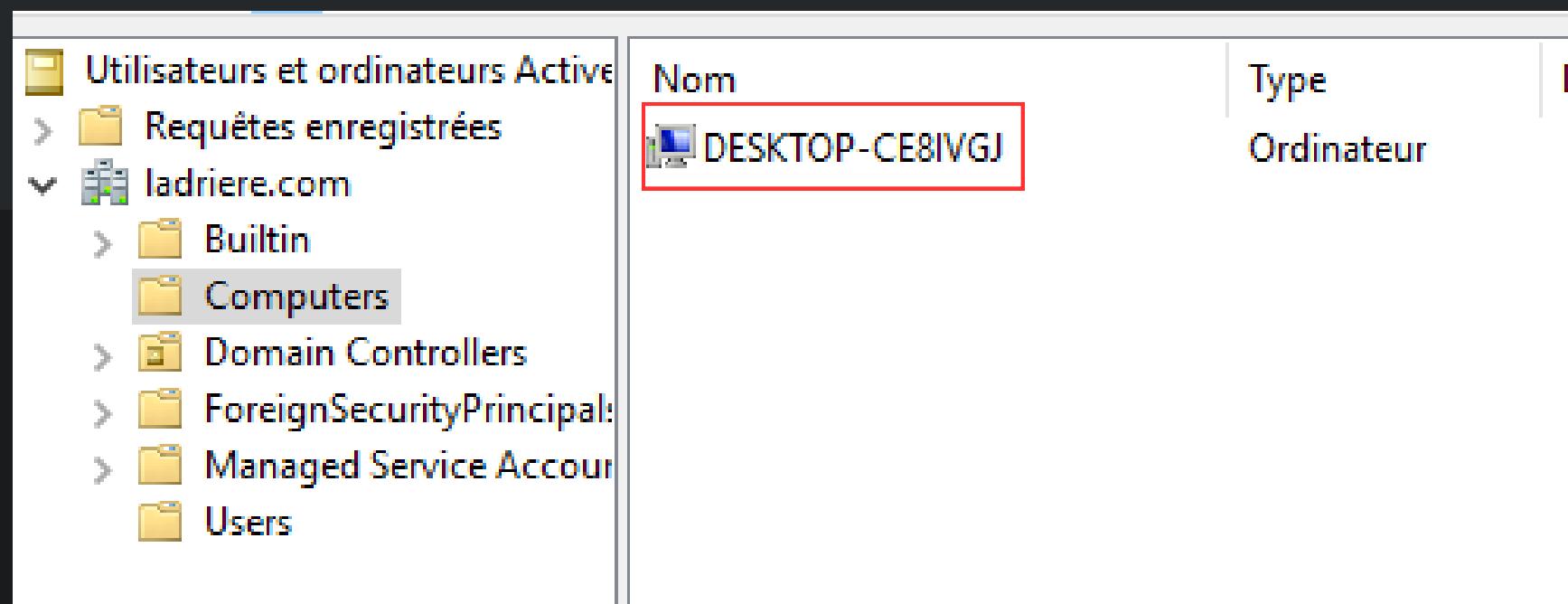
Une fois ceci fait allez sur votre domaine puis dans Users et vous pouvez constater qui a le droit d'intégrer le poste de domaine.

Dans notre cas à nous on peut y trouver le compte Administrateur :



UTILISATEURS ET ORDINATEURS ACTIVE DIRECTORY

Pour voir si une machine est bien raccordé à votre domaine, dans utilisateurs et ordinateurs Active Directory allez dans le domaine puis dans computers vous pouvez observer qu'un poste est connecté, Pour vérifier allez sur votre machine cliente -> paramètres -> système -> à propos de et logiquement le nom de la machine est bien celle écrite dans l'active directory



Spécifications de l'appareil

Nom de l'appareil	DESKTOP-CE8IVGJ
Nom complet de l'appareil	DESKTOP-CE8IVGJ.ladriere.com
Processeur	Intel(R) Core(TM) i3-8300 CPU @ 3.70GHz 3.70 GHz

INTEGRATION DU CLIENT DANS LE DOMAINE

Pour savoir quel poste peut intégrer notre domaine, retourner dans votre machine serveur.

Dans le gestionnaire de serveur allez dans outils -> Utilisateurs et ordinateurs Active Directory

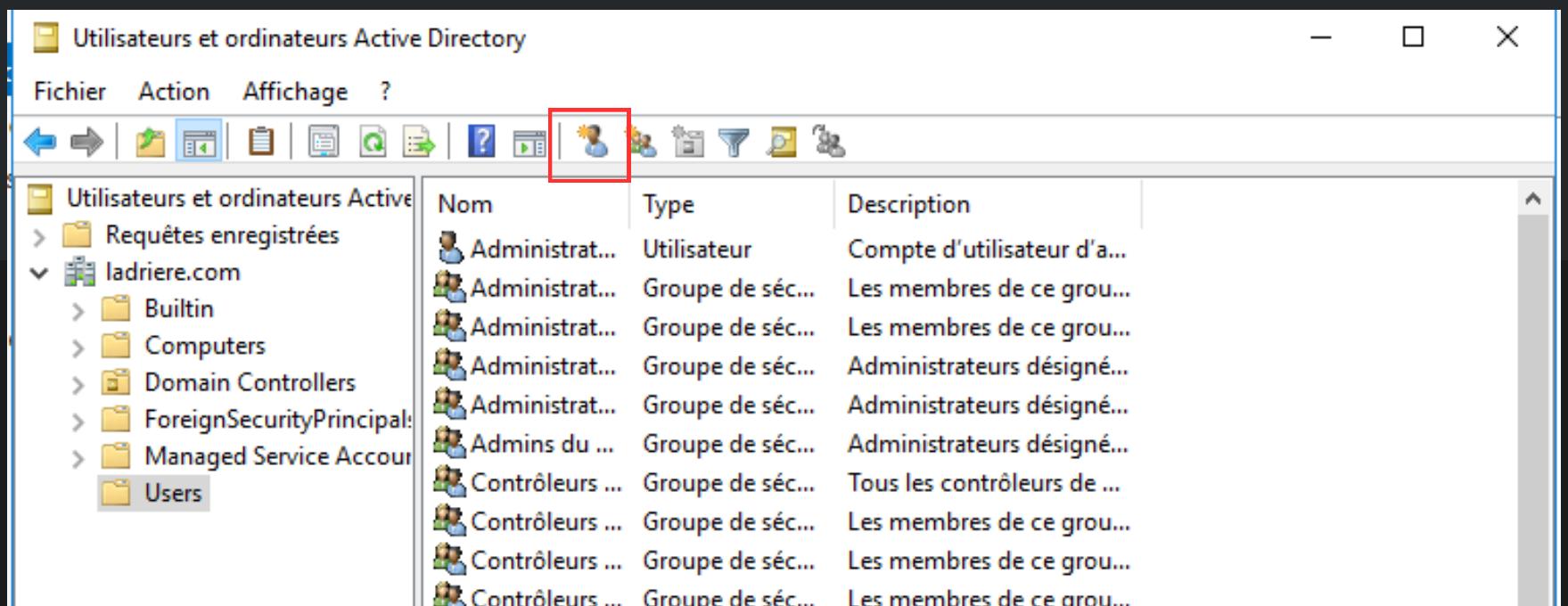
Une fois dedans allez dans votre domaine puis dans Users et vous pouvez observer qui a le droit d'intégrer votre domaine

Ici on peut observer que seul l'administrateur a le droit d'intégrer notre domaine

Nom	Type	Description
Administrat...	Utilisateur	Compte d'utilisateur d'a...
Administrat...	Groupe de séc...	Les membres de ce grou...
Administrat...	Groupe de séc...	Les membres de ce grou...
Administrat...	Groupe de séc...	Administrateurs désigné...
Administrat...	Groupe de séc...	Administrateurs désigné...
Admins du ...	Groupe de séc...	Administrateurs désigné...
Contrôleurs ...	Groupe de séc...	Tous les contrôleurs de ...
Contrôleurs ...	Groupe de séc...	Les membres de ce grou...
Contrôleurs ...	Groupe de séc...	Les membres de ce grou...
Contrôleurs ...	Groupe de séc...	Les membres de ce grou...

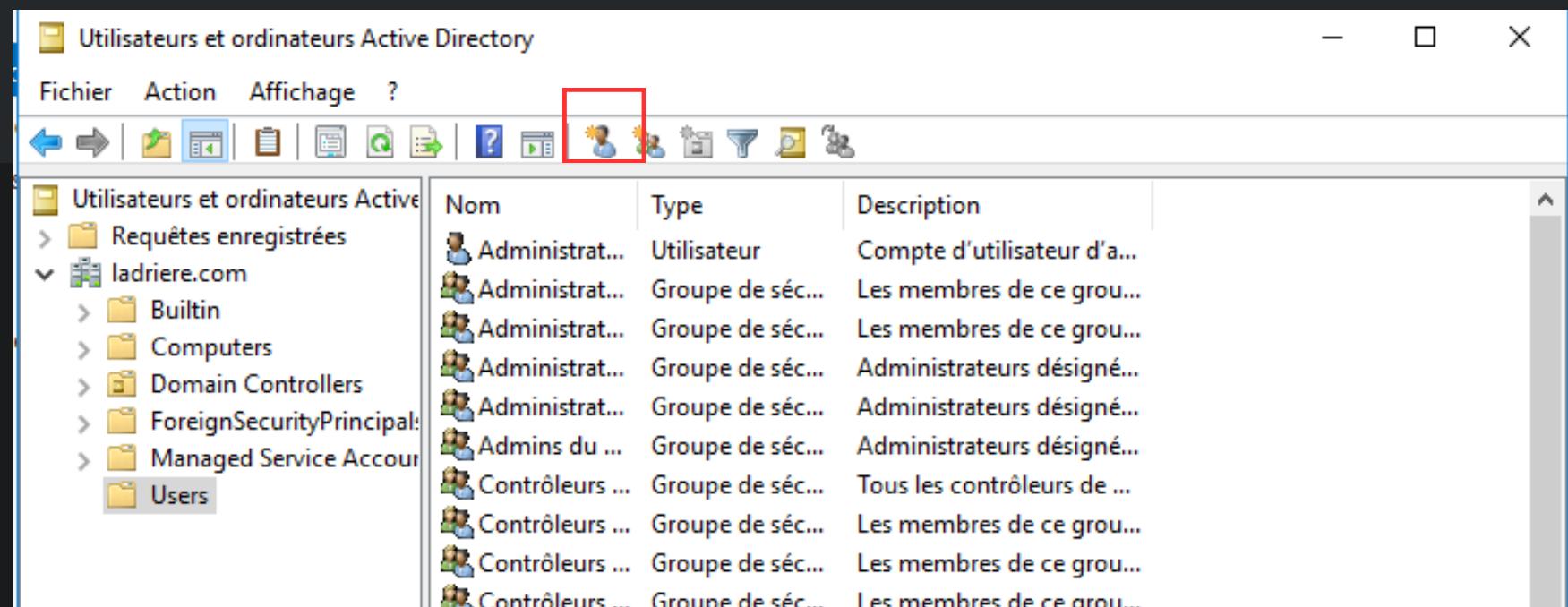
INTEGRATION DU CLIENT DANS LE DOMAINE ACTIVE DIRECTORY

Nous allons maintenant intégrer un Users dans notre domaine, allez dans l'utilisateur et ordinateurs Active Directory et cliquez sur l'icône créer un nouvel utilisateur dans le conteneur actuel



INTEGRATION DU CLIENT DANS LE DOMAINE ACTIVE DIRECTORY

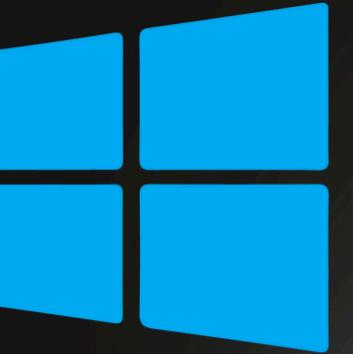
Nous allons maintenant intégrer un Users dans notre domaine, allez dans l'utilisateur et ordinateurs Active Directory et cliquez sur l'icône créer un nouvel utilisateur dans le conteneur actuel
Vous pourrez ensuite saisir les informations de votre nouvel utilisateur ainsi que configurer ses droits, son groupe...



The screenshot shows the 'Nouvel objet - Utilisateur' (New Object - User) dialog box. At the top, it says 'Créer dans : ladriere.com/Users'. The form contains the following fields:

- Prénom :
- Initiales :
- Nom :
- Nom complet :
- Nom d'ouverture de session de l'utilisateur : @ladriere.com
- Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : LADRIERE0\

At the bottom are buttons for '< Précédent' (Previous), 'Suivant >' (Next), and 'Annuler' (Cancel).



Microsoft

Active Directory

UTILISATION DE L'AD

INTÉGRATION DU CLIENT DANS LE DOMAINE

Maintenant ajoutez un Prénom et le nom d'ouverture de session de l'utilisateur et un mot de passe et surtout cocher la case pour que l'utilisateur puisse changer son mot de passe à la première connexion en raison de sécurité

Nouvel objet - Utilisateur

Créer dans : ladriere.com/Users

Prénom : Claire

Initiales :

Nom :

Nom complet : Claire

Nom d'ouverture de session de l'utilisateur

Claire @ladriere.com

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

LADRIERE0\ Claire

< Précédent Suivant > Annuler

Nouvel objet - Utilisateur

Créer dans : ladriere.com/Users

Mot de passe : *****

Confirmer le mot de passe : *****

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

L'utilisateur ne peut pas changer de mot de passe

Le mot de passe n'expire jamais

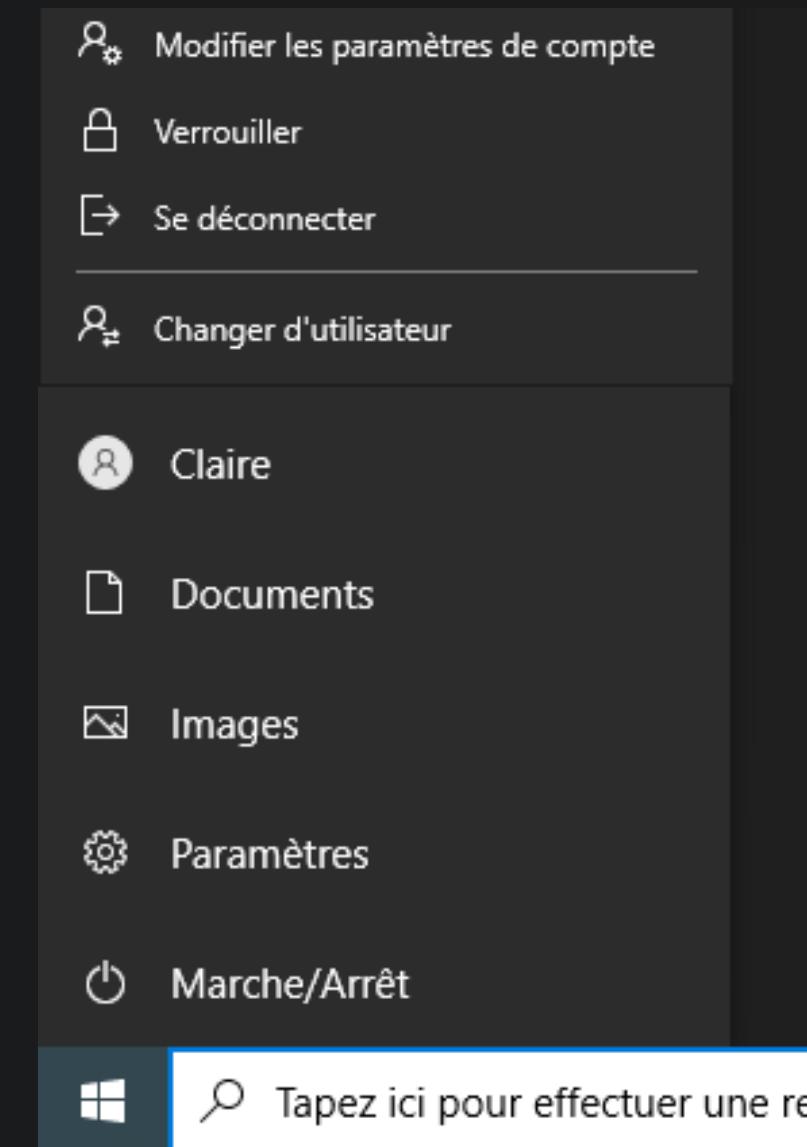
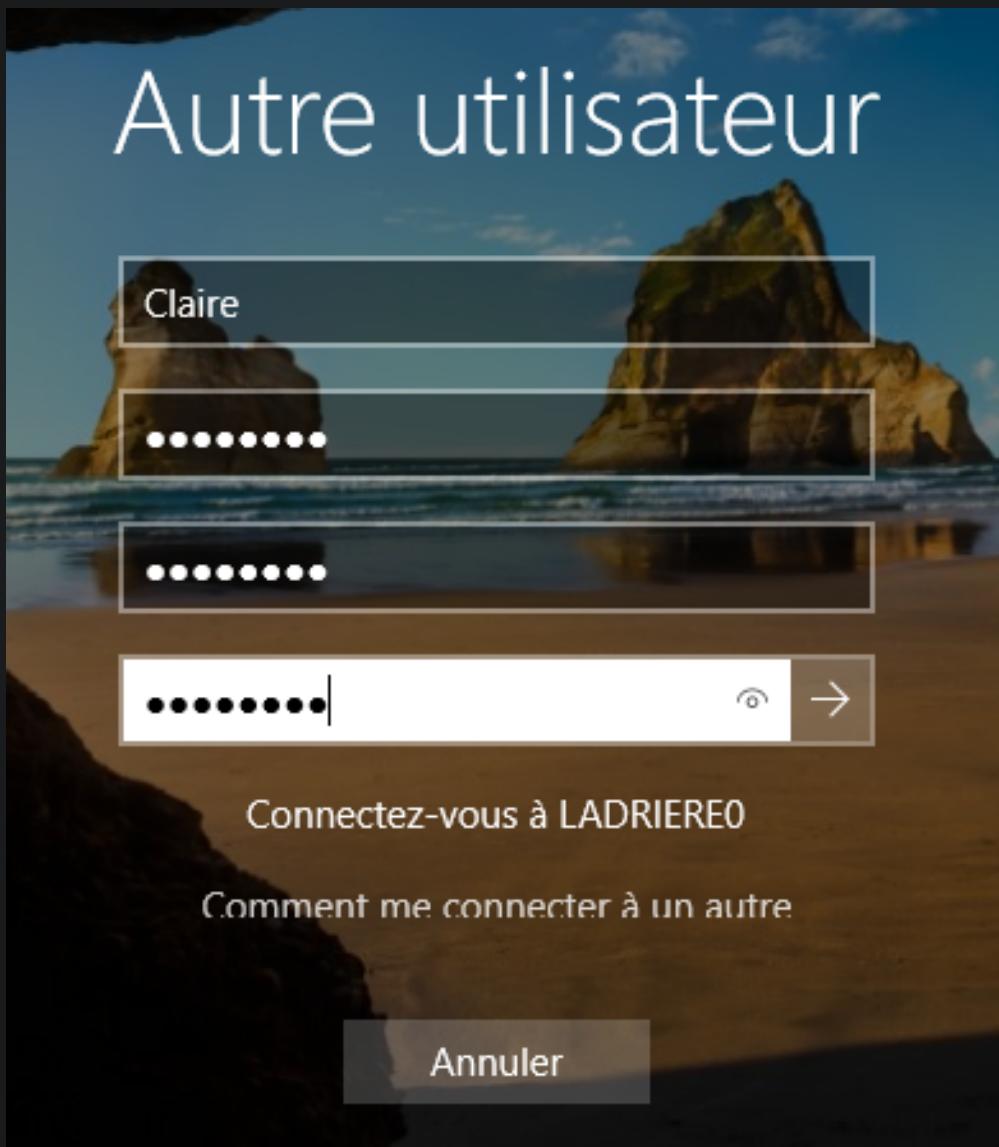
Le compte est désactivé

< Précédent Suivant > Annuler

INTÉGRATION DU CLIENT DANS LE DOMAINE

2032

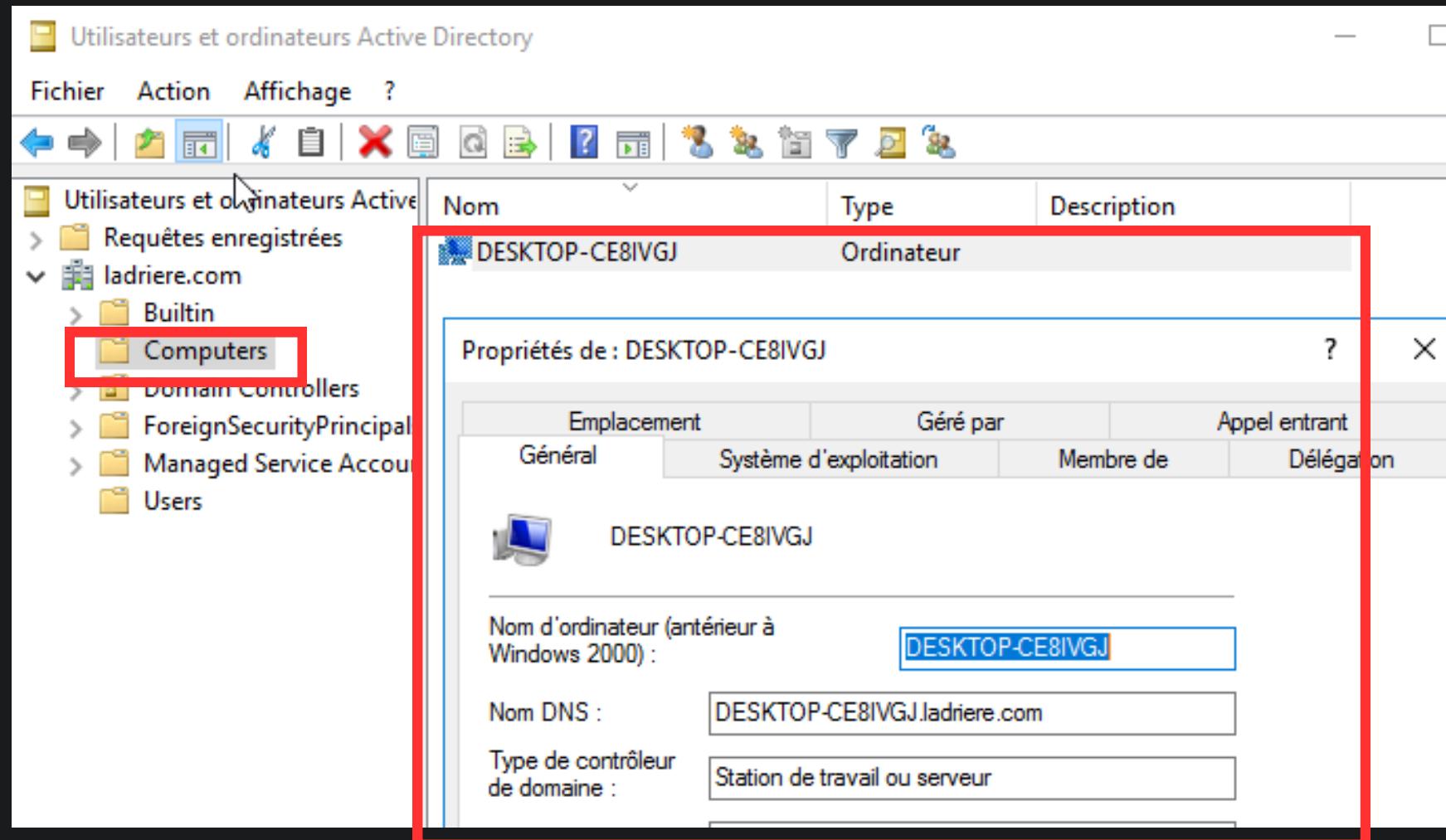
Une fois la création de l'utilisateur terminé retournez sur votre machine cliente, entrez le nom et le mot de passe que vous venez de saisir et changez le. Une fois que vous êtes connecté cliqué sur le logo Windows pour voir si vous êtes connectés sur le bon compte



VERIFICATION DES CLIENTS

Pour savoir quel client est connecté sur notre serveur retournez sur votre machine serveur et retournez dans l'utilisateurs et ordinateurs Active Directory et dans votre domaine

Un nom d'ordinateur est censé apparaître dans Computers , pour être sur que c'est bien un client que vous connaissez vous pouvez : retournez sur la machine cliente -> paramètres -> système -> A propos de et le nom de la machine cliente doit être identique a celle trouvé dans Computers

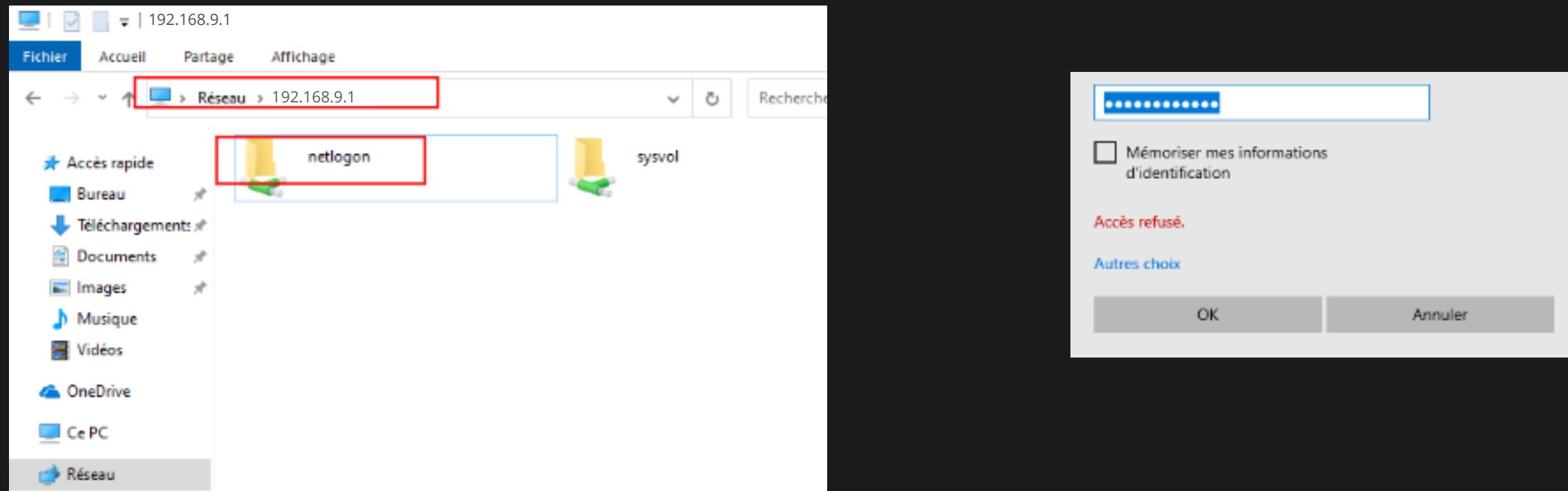


Spécifications de l'appareil

Nom de l'appareil	DESKTOP-CE8IVGJ
Nom complet de l'appareil	DESKTOP-CE8IVGJ.ladriere.com

VERIFICATION CÔTÉ CLIENTS

Depuis la machine cliente allez dans l'explorateur de fichiers puis dans la catégorie réseau
Dans la barre de recherche inscrivez-y l'adresse IP de votre serveur comme ceci \\192.168.x.1 si vous essayez de vous connecter au netlogon on vous demandera les informations d'identifications mais l'accès sera refusé si l'administrateur ne vous donne pas les droits d'accès



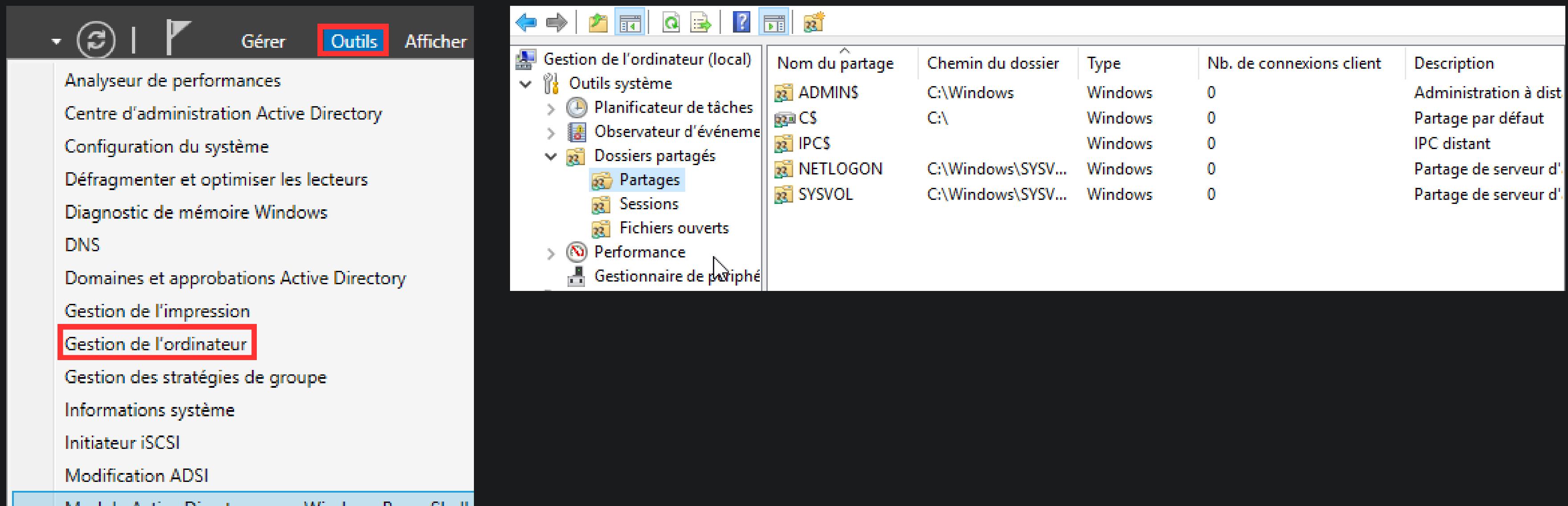
VERIFICATION CÔTÉ CLIENTS

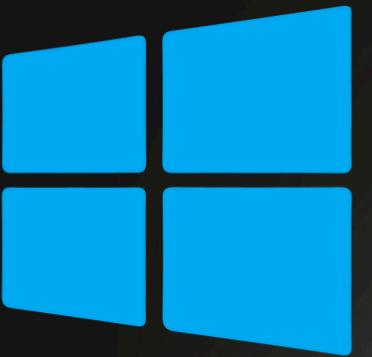
Le service NETLOGON est essentiel au bon fonctionnement du contrôleur de domaine, ce service gère un canal sécurisé pour l'authentification des utilisateurs et des services. Au démarrage, le service NETLOGON à la charge d'ajouter les enregistrements au serveur DNS afin que le contrôleur de domaine puisse être déclaré.

SYSVOL est une collection de dossiers, de points d'analyse du système de fichiers et de paramètres stratégie de groupe répliqués par le service de réPLICATION de fichiers (FRS). La réPLICATION distribue une copie cohérente des paramètres et des scripts stratégie de groupe entre les contrôleurs de domaine d'un domaine.

VERIFICATION CÔTÉ CLIENTS

Les dossiers que vous pouvez observer dans ce chemin d'accès correspondent aux dossiers qui se trouvent dans la machine serveur -> Gestion de l'ordinateur -> Dossiers partagés -> Partages et vous pouvez retrouver les deux fichiers





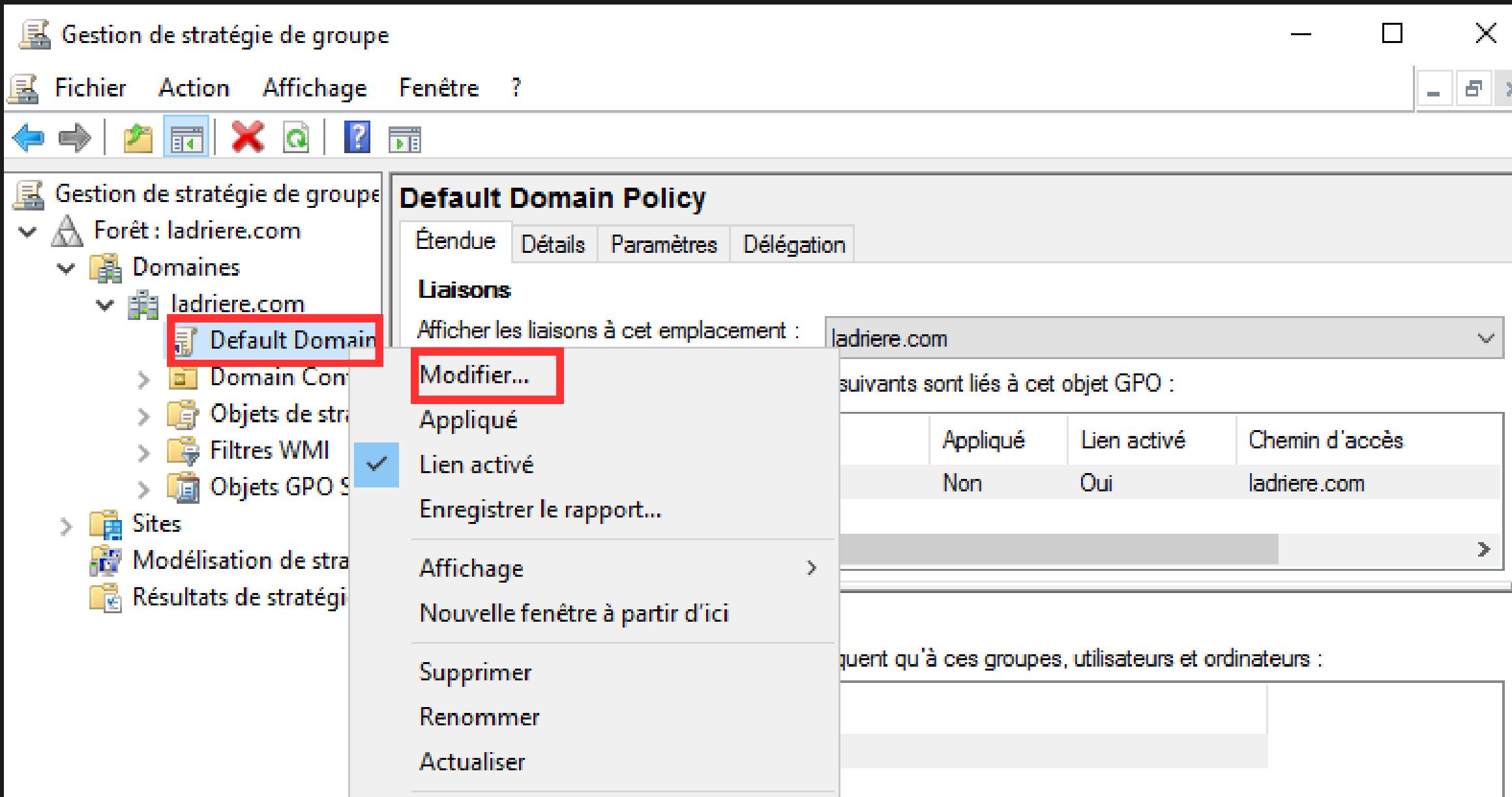
Microsoft
Active Directory

SECURITE DES MOTS DE PASSE

SECURITÉ DES MOTS DE PASSE

Dans la machine Windows Server allez dans l'invite de commande avec la touche Windows+R et tapez la commande gpmc.msc

Allez ensuite sur votre contrôleur de domaine ->clique droit sur Default Domain Policy -> Modifier



SECURITÉ DES MOTS DE PASSE

Maintenant vous devez allez dans Stratégies -> Paramètres Windows -> Paramètres de sécurité -> Stratégies de compte -> stratégie de mot de passe
La fenêtre va maintenant afficher différents paramètres de stratégies :

Stratégie	Paramètres de stratégie
Conserver l'historique des mots de passe	24 mots de passe mémorisés
Durée de vie maximale du mot de passe	30 jours
Durée de vie minimale du mot de passe	1 jours
Enregistrer les mots de passe en utilisant un chiffrement rév...	Désactivé
Le mot de passe doit respecter des exigences de complexité	Désactivé
Longueur minimale du mot de passe	3 caractère(s)

Vous pouvez modifier ces valeurs en double cliquant dessus, dans notre cas à nous j'ai donc appliqué ces paramètres :

SECURITÉ DES MOTS DE PASSE

Vous pouvez modifier ces valeurs en double cliquant dessus, dans notre cas à nous j'ai donc appliqué ces paramètres :

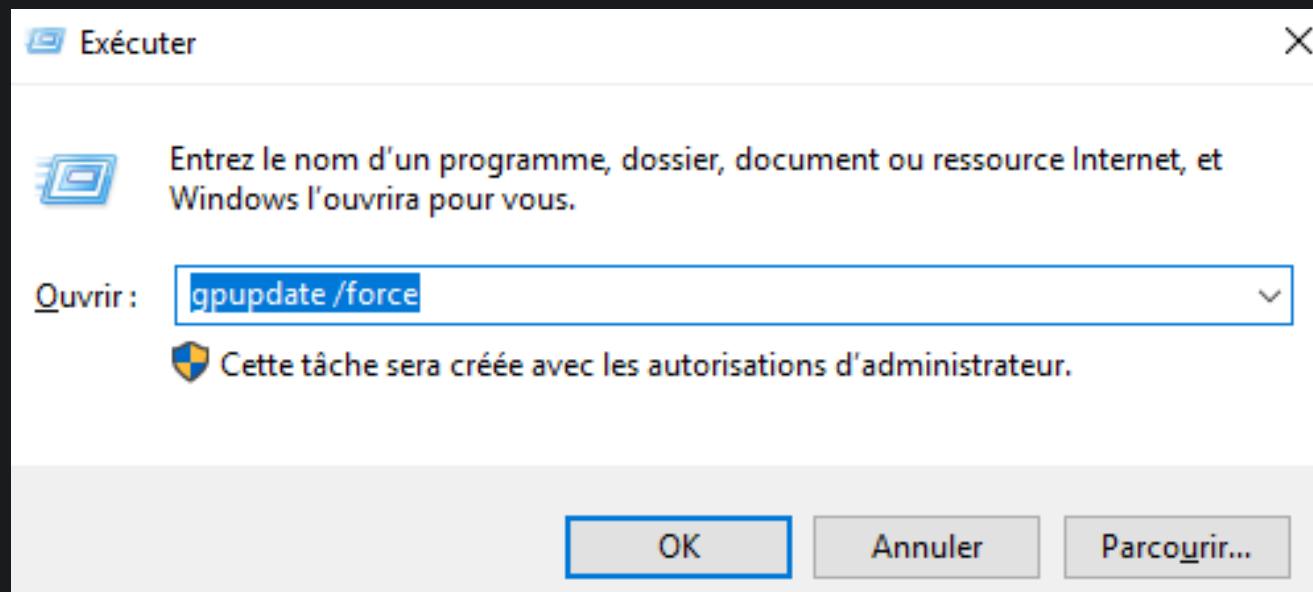
The screenshot shows two windows side-by-side. On the left is a Windows-style dialog box titled 'Propriétés de : Durée de vie maximale du mot de passe'. It has tabs for 'Paramètre de stratégie de sécurité' and 'Expliquer'. Under 'Durée de vie maximale du mot de passe', there is a checked checkbox 'Définir ce paramètre de stratégie' and a field showing 'Le mot de passe expirera dans : 50 jours'. At the bottom are buttons for 'OK', 'Annuler', and 'Appliquer'.

On the right is a table comparing security parameters:

Stratégie	Paramètres de stratégie
Conserver l'historique des mots de passe	24 mots de passe mémorisés
Durée de vie maximale du mot de passe	50 jours
Durée de vie minimale du mot de passe	1 jours
Enregistrer les mots de passe en utilisant un chiffrement rév...	Désactivé
Le mot de passe doit respecter des exigences de complexité	Désactivé
Longueur minimale du mot de passe	3 caractère(s)

SECURITÉ DES MOTS DE PASSE

Pour appliquer ses modifications de paramètres sur votre domaine, retournez dans l'invite de commande avec la commande w+R et entrer la commande gpupdate /force et l'invite de commande mettra à jour la stratégie :



```
C:\Windows\system32\gpupdate.exe
Mise à jour de la stratégie...
La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
```

SECURITÉ DES MOTS DE PASSE

Pour vérifier si cela a correctement fonctionner sur votre Windows serveur retournez dans Utilisateurs et ordinateurs Active Directory et créer un nouvel user.
On va le nommer sio et lui attribuez un mot de passe de trois caractères avec comme instruction qu'à la première connexion l'utilisateur doit changer de mot passe

Nouvel objet - Utilisateur

Créer dans : ladriere.com/Users

Prénom : sio Initials :

Nom :

Nom complet : sio

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

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
LADRIERE0\ sio

< Précédent Suivant > Annuler

Nouvel objet - Utilisateur

Créer dans : ladriere.com/Users

Mot de passe : ***

Confirmer le mot de passe : ***

L'utilisateur doit changer le mot de passe à la prochaine ouverture de session
 L'utilisateur ne peut pas changer de mot de passe
 Le mot de passe n'expire jamais
 Le compte est désactivé

< Précédent Suivant > Annuler

Nom	Type	Description
Utilisateurs du domaine	Groupe de séc...	Tous les utilisateurs du d...
sio	Utilisateur	
Serveurs RAS et IAS	Groupe de séc...	Les serveurs de ce group...
Protected Users	Groupe de séc...	Les membres de ce grou...
Propriétaires créateurs de la st...	Groupe de séc...	Les membres de ce grou...
Ordinateurs du domaine	Groupe de séc...	Toutes les stations de tra...
Invités du domaine	Groupe de séc...	Tous les invités du dom...
Invité	Utilisateur	Compte d'utilisateur inv...
Groupe de réPLICATION dont le ...	Groupe de séc...	Les mots de passe des ...
Groupe de réPLICATION dont le ...	Groupe de séc...	Les mots de passe des ...
Éditeurs de certificats	Groupe de séc...	Les membres de ce grou...
DnsUpdateProxy	Groupe de séc...	Les clients DNS qui sont ...
DnsAdmins	Groupe de séc...	Groupe des administrat...
DefaultAccount	Utilisateur	Compte utilisateur géré ...
Contrôleurs de domaine en le...	Groupe de séc...	Les membres de ce grou...
Contrôleurs de domaine d'en...	Groupe de séc...	Les membres de ce grou...
Contrôleurs de domaine clon...	Groupe de séc...	Les membres de ce grou...

SECURITÉ DES MOTS DE PASSE

Si vous tentez avec deux caractères vous pouvez voir que le Windows ne pas configurer le mot de passe car il ne correspond pas aux critères de stratégie de mot de passe

The image displays two windows from the Windows Active Directory User Creation interface:

Left Window (Nouvel objet - Utilisateur):

- Créer dans : ladriere.com/Users
- Mot de passe : (Two dots)
- Confirmer le mot de passe : (Two dots)
- L'utilisateur doit changer le mot de passe à la prochaine ouverture de session
- L'utilisateur ne peut pas changer de mot de passe
- Le mot de passe n'expire jamais
- Le compte est désactivé

Right Window (Nouvel objet - Utilisateur):

- Créer dans : ladriere.com/Users
- Quand vous cliquerez sur Terminer, l'objet suivant sera créé :
- Nom complet : feur
- Nom de connexion de l'utilisateur
- L'utilisateur doit changer de mot de passe

A modal dialog titled "Services de domaine Active Directory" contains the following message:

Windows ne peut pas définir le mot de passe pour feur car :
Ce mot de passe ne correspond pas aux critères de stratégie de mot de passe. Vérifiez la longueur de mot de passe minimale, la complexité du mot de passe et l'historique des critères de mots de passe.

Buttons at the bottom of the right window include < Précédent, Terminer, Annuler, OK, and Compte utilisateur géré ...

SECURITÉ DES MOTS DE PASSE - VERIFICATION

Sur votre machine cliente identifier vous avec le user que vous venez de créer et regarder si on peut bien changer de mot de passe au démarrage et pour être sur que vous êtes sur le bon compte. Une fois que la session est lancé cliquez sur le logo Windows et vous pouvez vérifier si c'est bien le cas

