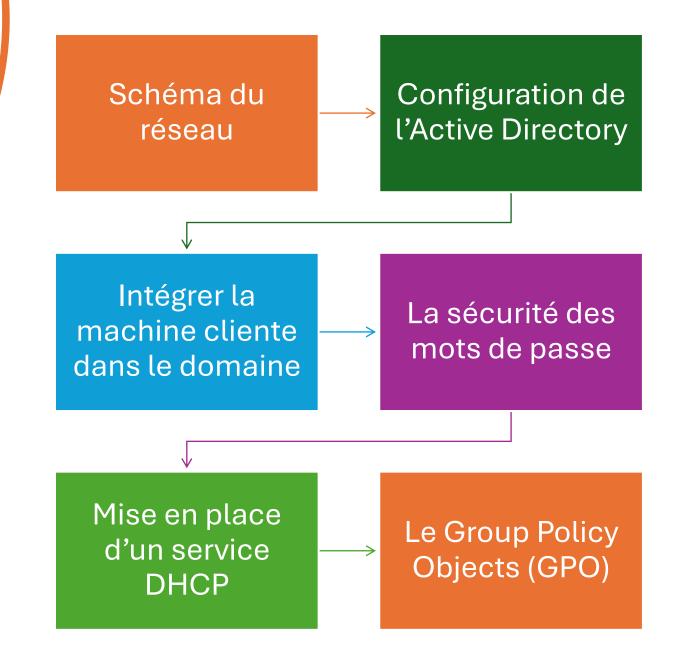
TP-AD DNS



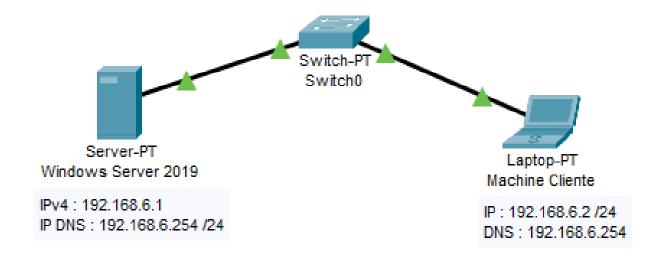




Sommaire











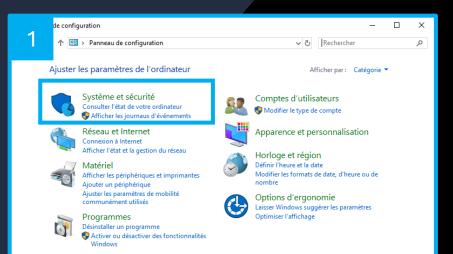
Active Directory

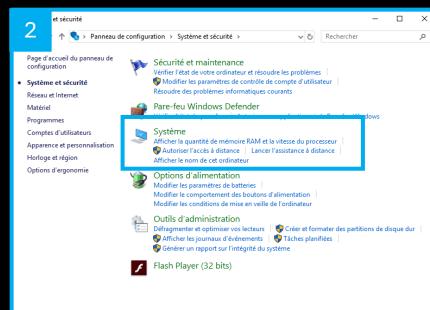
Paramétrage de l'IP du serveur

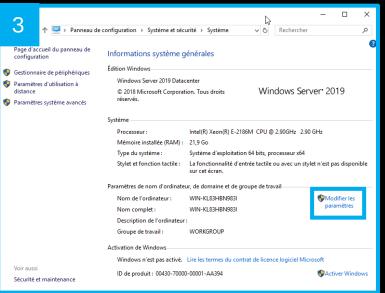
Propriétés de : Protocole Internet version 4 (TCP/IPv4)			
Général			
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.			
Obtenir une adresse IP automatiquement			
Utiliser l'adresse IP suivante :			
Adresse IP :	192 . 168 . 6 . 1		
Masque de sous-réseau :	255 . 255 . 255 . 0		
Passerelle par défaut :			
Obtenir les adresses des serveurs DNS automatiquement			
Utiliser l'adresse de serveur DNS suivante :			
Serveur DNS préféré :	192 . 168 . 6 . 1		
Serveur DNS auxiliaire :			
☐ Valider les paramètres en quittant Avancé			
	OK Annuler		

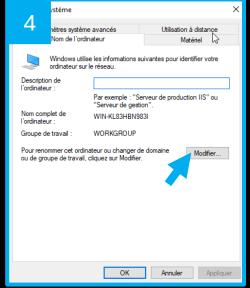
Depuis la machine serveur, aller dans les paramètres de votre carte réseau puis assigner une IP fixe qui sera la même adresse comme serveur DNS.

Panneau de configuration → Réseau et Internet → Centre Réseau et partage → Modifier les paramètres de la carte → « votre carte réseau » → Clic droit + « Propriétés » → Sélectionner « Protocole Internet version 4 (TCP/IPv4).









ion du nom ou du domaine de l'ordinateur	
	vez modifier le nom et l'appartenance de cet ir. Ces modifications peuvent influer sur l'accès aux es réseau.
Nom de l'	'ordinateur :
Nom com TRIOUX	plet de l'ordinateur :
	Autres
Membre	e d'un
○ D o	omaine :
● Gro	oupe de travail :
W	ORKGROUP
	OK Annuler

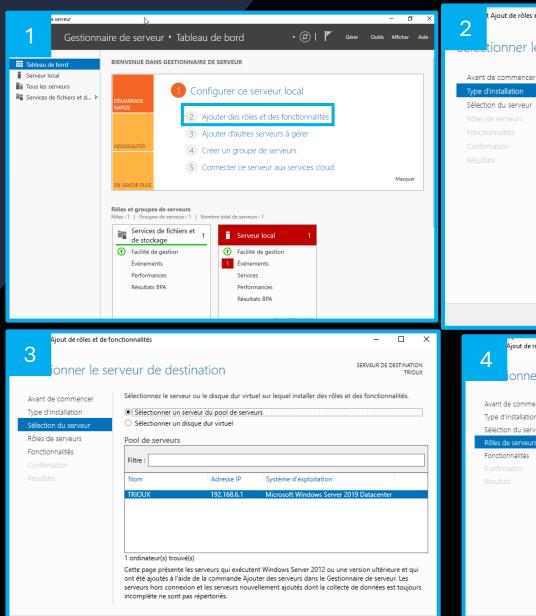
Modifier le NetBios

Pour changer votre nom d'ordinateur (NetBios), aller dans le panneau de configuration puis « **Système et sécurité** ».

Dans la page « **Système et sécurité** », cliquer sur « **Système** » puis « **Modifier les paramètres** ».

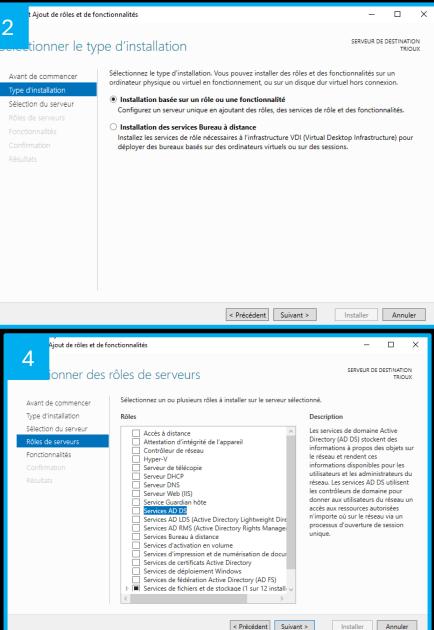
Une fenêtre va s'ouvrir, cliquer sur « **Modifier...** » et vous accéderez à une autre fenêtre qui cette fois-ci vous permettra de modifier le nom de l'ordinateur ainsi que de le rattacher à un serveur DNS.

Il faudra toutefois redémarrer l'ordinateur afin de prendre en compte les modifications.



< Précédent Suivant >

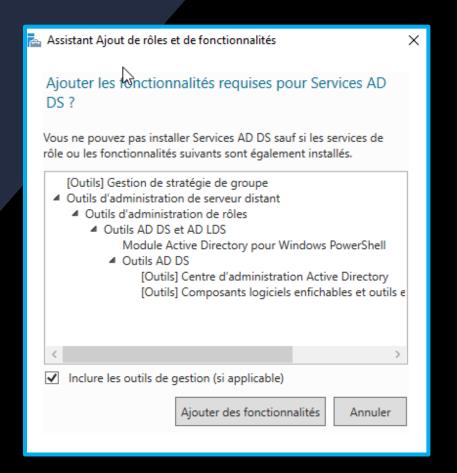
Installer

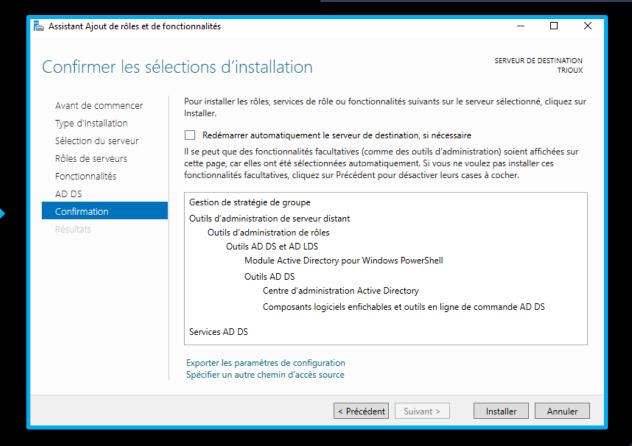


Installation de l'Active Directory

Pour installer l'Active Directory, depuis le tableau de bord, cliquer sur « **Ajouter des rôles et des fonctionnalités** », une fenêtre d'installation va s'ouvrir.

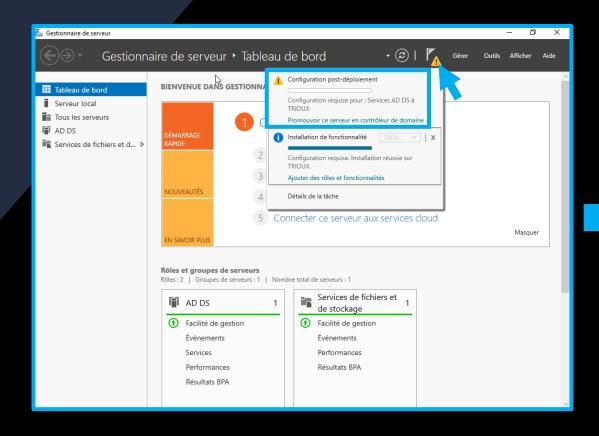
Pensez à bien sélectionner votre serveur puis cocher « **Services AD DS** » dans la page « **Rôles de serveurs** » et faites suivant.



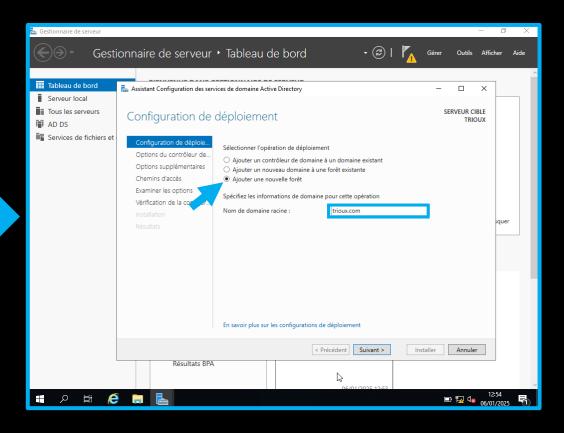


Ensuite, on vous demandera si vous souhaitez ajouter toutes les fonctionnalités requises pour faire fonctionner le service.

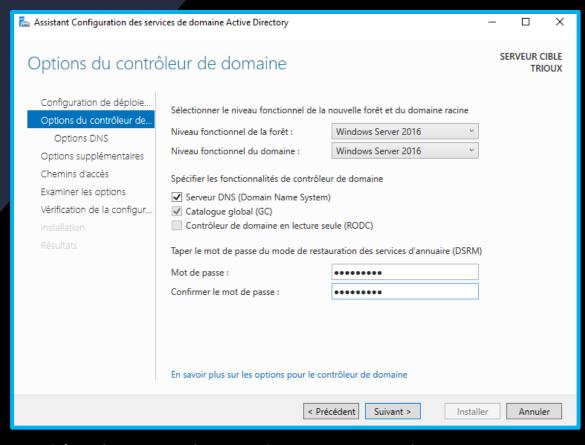
Puis laissez vous guider en faisant « **Suivant** » jusqu'à arriver à cette page où vous cliquerez sur « **Installer** ».



Retourner sur le tableau de bord, puis cliquer sur le drapeau avec un panneau d'avertissement. Faites « **Promouvoir ce serveur en contrôleur de domaine** ».



La fenêtre suivante s'ouvre, nous créerons une nouvelle forêt avec comme nom de domaine « **trioux.com** » et faites <u>suivant</u>.



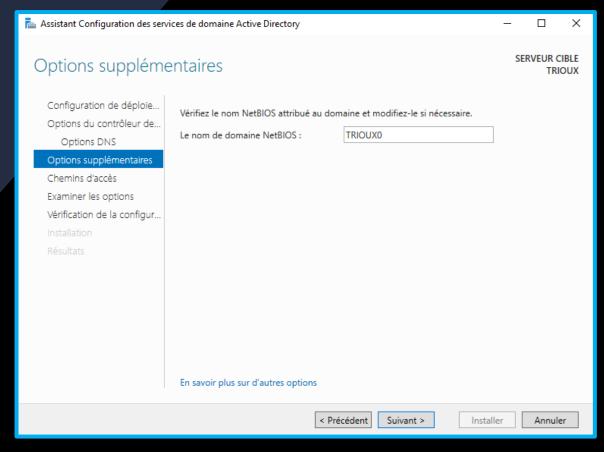
SERVEUR CIBLE **Options DNS** TRIOUX 🛦 Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est intro... Afficher plus Configuration de déploie. Spécifier les options de délégation DNS Options du contrôleur de.. Créer une délégation DNS Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur. En savoir plus sur la délégation DNS < Précédent Suivant > Installer Annuler

Sélectionner « **Windows Server 2016** » qui est le niveau fonctionnel maximale utilisé par Windows Server 2019 et 2022.

Rentrer un mot de passe de restauration et faites suivant.

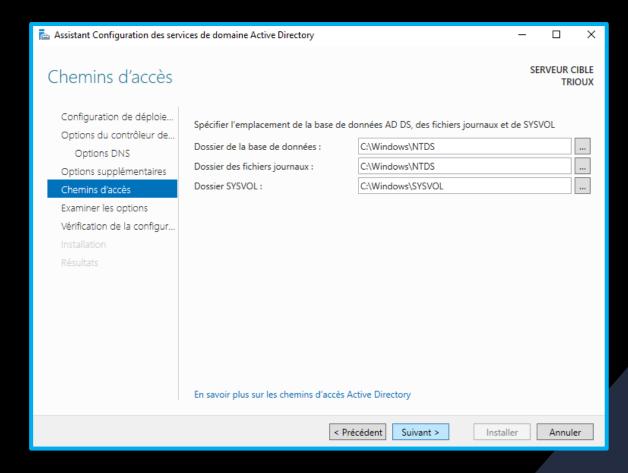
Nous ne créerons pas de délégation donc suivant.

Assistant Configuration des services de domaine Active Directory



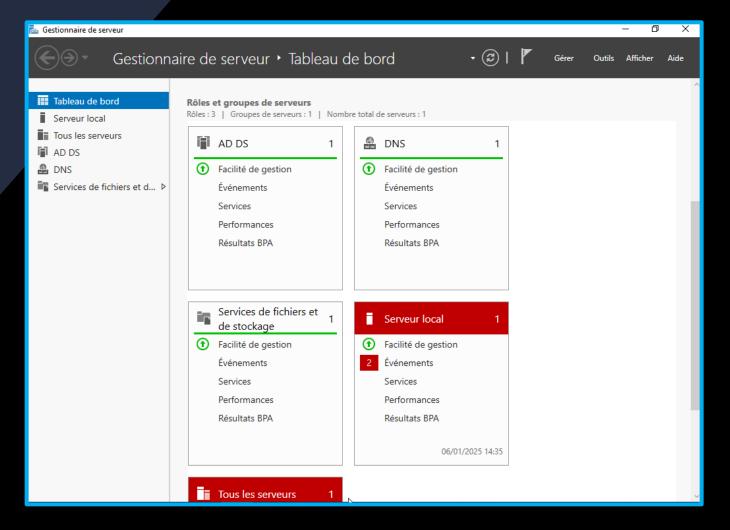
Donner un nom de domaine Netbios à votre serveur.

Attention, il ne peut pas être identique au Netbios de votre ordinateur, ce pourquoi j'ai rajouté un 0 derrière TRIOUX.



Nous laisserons par défaut les chemins.

A quoi correspondent les deux services installés?

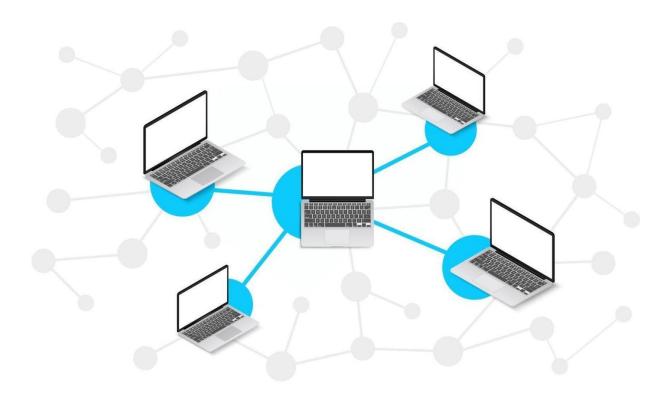


Au sein du tableau de bord, nous retrouvons divers services y compris l'Active Directory que nous venons d'installer.

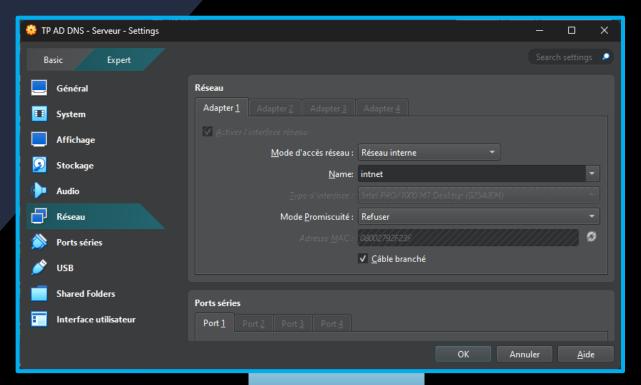
AD DS: C'est un service d'annuaire qui propose des méthodes pour stocker des données d'annuaire et rendre ces données disponibles aux utilisateurs et administrateurs du réseau.

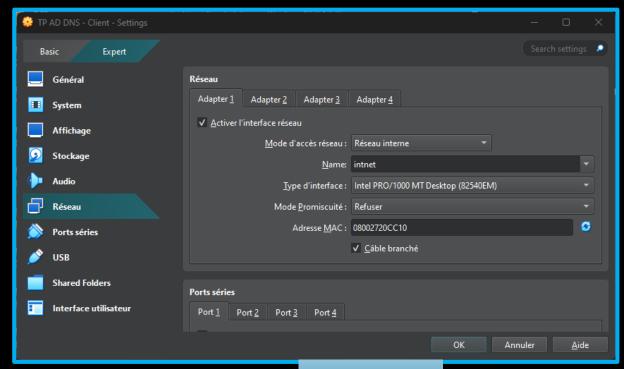
DNS : Le Domain Name System sert à faciliter la recherche d'un site sur Internet. Ainsi, il permet d'associer un nom à une adresse IP.

Intégrer la machine cliente dans le domaine



Réseau interne

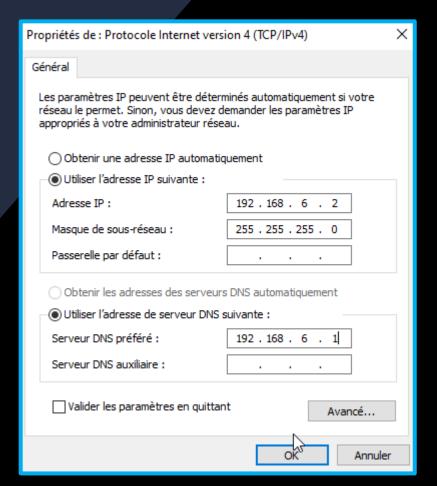




Serveur

Client

Sur VirtualBox, mettez en réseau interne vos deux VMs afin qu'elles puissent communiquer entre elle.



Pour connecter la machine cliente au domaine, il faut que vous alliez dans les propriétés du protocole IPv4 et affecter lui une adresse IP en « 192.168.votreposte.2 » par exemple.

Connecter la machine cliente au domaine

```
C:\Users\Client SIO>ping 192.168.6.1
Envoi d'une requête 'Ping' 192.168.6.1 avec 32 octets de données :
Réponse de 192.168.6.1 : octets=32 temps<1ms TTL=128
Statistiques Ping pour 192.168.6.1:
    Paquets: envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
C:\Users\Client SIO>ping trioux.com
Envoi d'une requête 'ping' sur trioux.com [192.168.6.1] avec 32 octets de données :
Réponse de 192.168.6.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.6.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.6.1 : octets=32 temps=3 ms TTL=128
Réponse de 192.168.6.1 : octets=32 temps<1ms TTL=128
Statistiques Ping pour 192.168.6.1:
   Paquets: envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 3ms, Moyenne = 0ms
```

J'essaie de pinger ma machine serveur depuis ma machine cliente en testant avec l'adresse IP puis son nom de domaine.

Les paquets sont envoyés donc la communication entre les deux postes est opérationnelle.

C:\Users\Client SIO>nslookup trioux.com

DNS request timed out.

timeout was 2 seconds.

Serveur : UnKnown

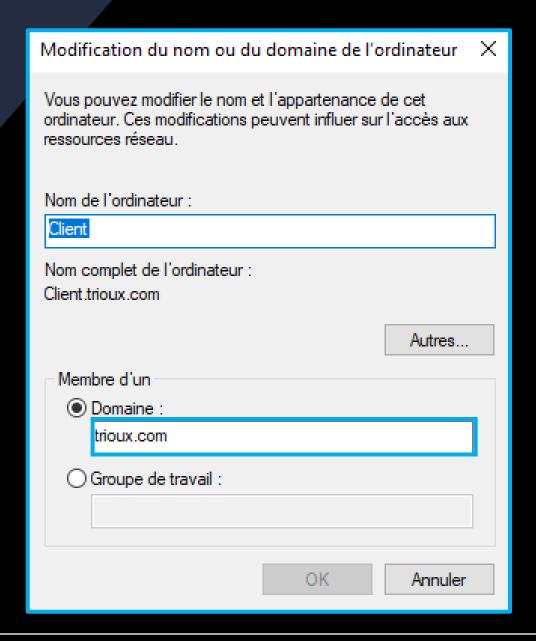
Address: 192.168.6.1

Nom : trioux.com

Address: 192.168.6.1

La commande « **nslookup** votredns » est une commande intégrée à tous les systèmes d'exploitation Windows/Windows Server.

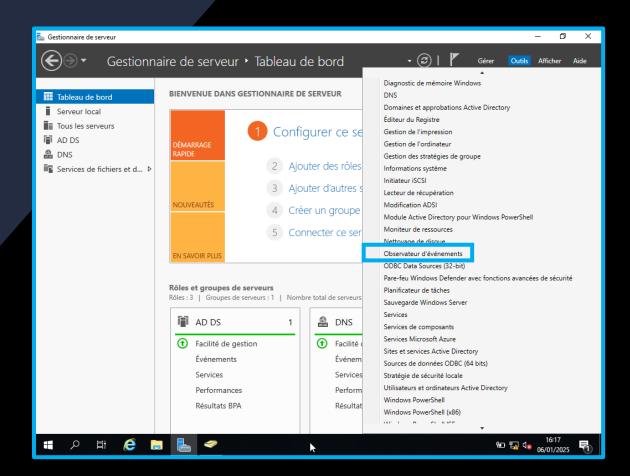
En effet, cette commande permet de vérifier quelles adresses sont associés à un nom de domaine, de vérifier le serveur de messagerie ou encore de vérifier que le serveur que nous venons de créer est bien inscrit dans la zone DNS du domaine Active Directory.



Connecter la machine cliente au domaine

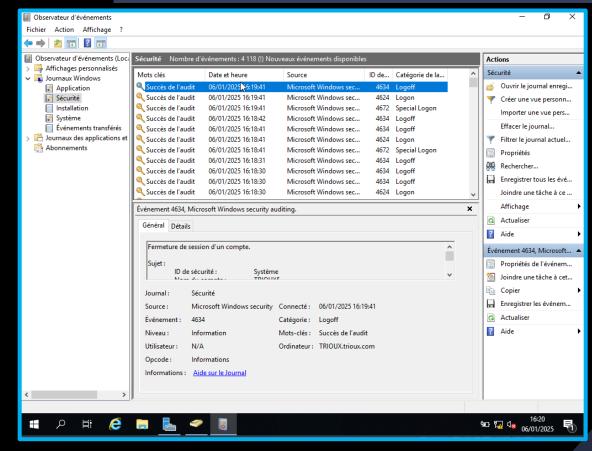
Il est nécessaire de rattacher sa machine cliente à son serveur DNS.

Pour ce faire, nous retournerons dans la fenêtre où nous avions changé le Netbios sur la partie serveur et puis nous affecterons le DNS « **trioux.com** » pour l'ordinateur « **Client** ».



Dans « Outils », cliquer sur « Observateur d'événements ».

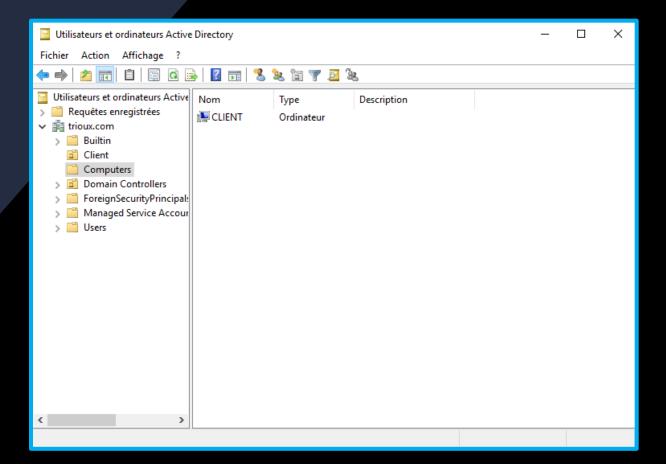
Trouver les utilisateurs connectés au serveur



Ensuite, dérouler « **Journaux Windows** » puis Cliquer sur « **Sécurité** ».

C'est ici que vous pourrez retrouver la trace des connexions de vos utilisateurs.

2^{nde} méthode:

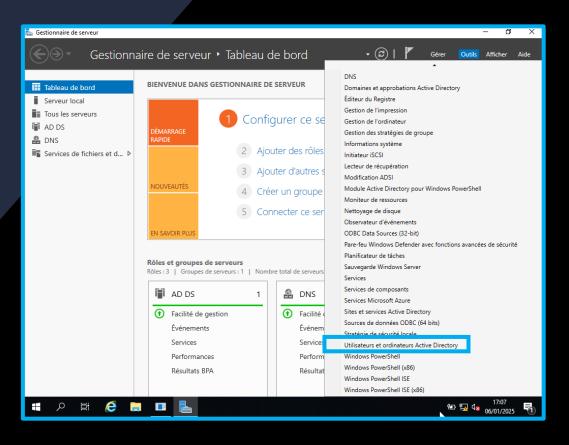


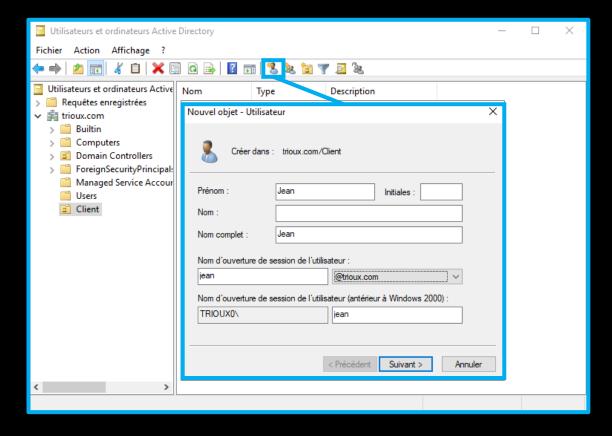
Trouver les utilisateurs connectés au serveur

Spécifications de l'appareil		
Nom de l'appareil	Client	
Nom complet de l'appareil Processeur	Client.trioux.com Intel(R) Xeon(R) E-2186M CPU	
	@ 2.90GHz 2.90 GHz	
Mémoire RAM installée	8,00 Go	
ID de périphérique	283E203A-7382-427F- A2D6-292FED474D25	
ID de produit	00330-80000-00000-AA756	
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	

Retourner dans l'interface « **Utilisateurs et ordinateurs Active Directory** » et sélectionner l'unité organisationnelle « **Computers** » et vous pourrez voir les postes connectés au serveur.

Créer un utilisateur dans l'Active Directory

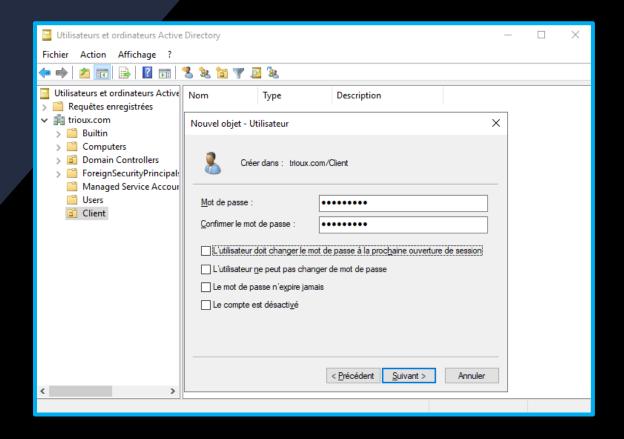


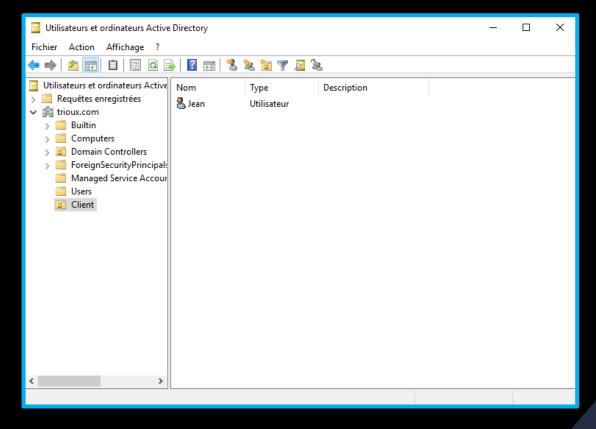


Dans « Outils », cliquer sur « Utilisateurs et ordinateurs Active Directory ».

Vérifier que vous êtes bien dans le répertoire de votre DNS, et après avoir créé une unité organisationnelle, nous créerons un utilisateur nommé « Jean ».

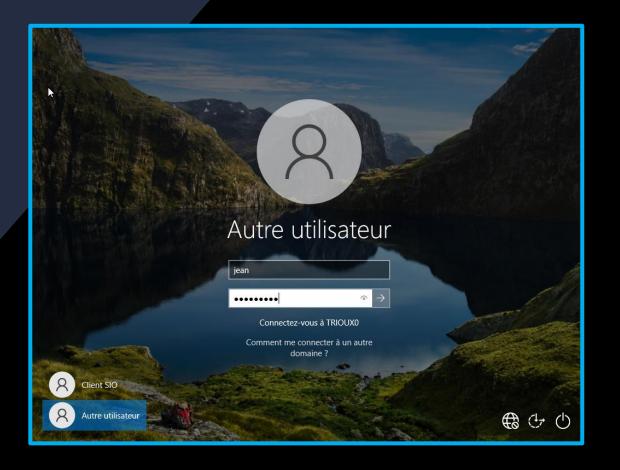
Créer un utilisateur dans l'Active Directory

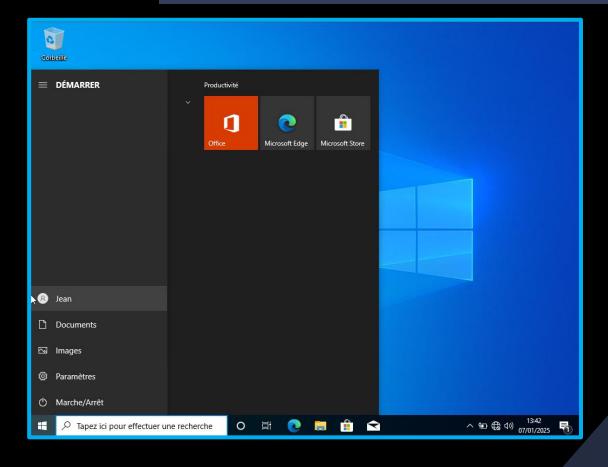




Je décoche l'option pour l'utilisateur de choisir son mot de passe à l'ouverture de sa session puisque c'est un compte de test. L'utilisateur est créé et nous pouvons dès à présent le tester sur la machine cliente.

Test du compte depuis la machine cliente

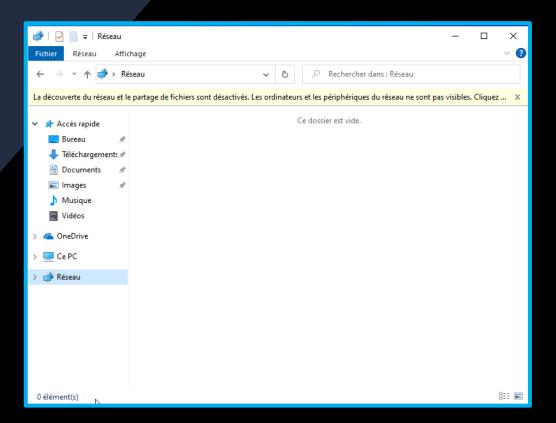


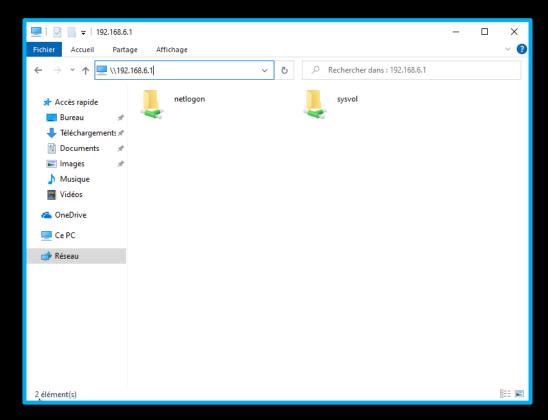


Depuis la machine cliente, rentrons les informations de connexion de l'utilisateur Jean.

La session de l'utilisateur « Jean » est fonctionnelle et accessible.

L'explorateur de fichier et les réseaux





Par défaut, lorsque l'on se rend dans l'explorateur de fichier celui-ci demande d'activer la découverte du réseau. Hors, si nous activons cette découverte alors nous sommes déconnectés du domaine. A la place, nous rentrerons l'adresse IP du serveur DNS qui donne un visuel sur deux dossiers nommés « **netlogon** » et « **sysvol** ».

Netlogon: Gère l'authentification des utilisateurs dans le domaine.

Sysvol: Dossier partagé qui a pour utilité de stocker et répliquer les données liées aux stratégies de groupe.

La sécurité des mots de passe



La politique de sécurité des mots de passe

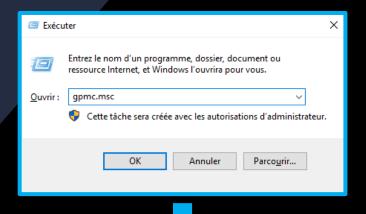
Afin de restreindre le niveau de sécurité des postes informatiques, il est necessaire de mettre en place une politique de mot de passe fort.

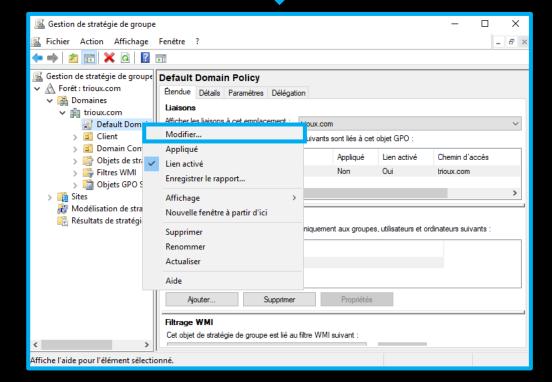
Dans le cadre de ce TP, nous ne respecterons pas les bonnes pratiques afin d'expérimenter.

Nous mettrons en place ces exigences pour les mots de passe :

- Historique des mots de passe : 30 jours
- Durée de vie maximale : 30 jours
- Durée de vie minimale : 1 jour
- Enregistrer les mots de passe : Désactivé
- Mot de passe doit respecter des exigences de complexité: Désactivé
- Longueur minimale de mot de passe : 3 caractères





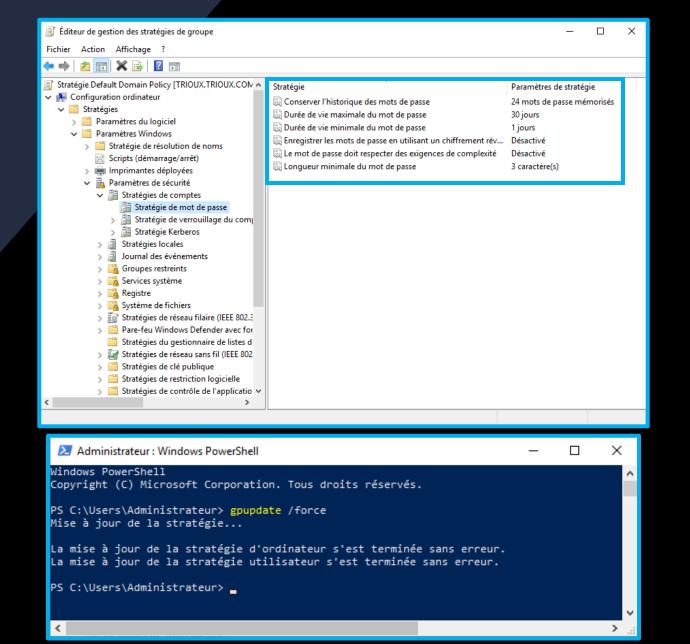


La stratégie de mot de passe

Il est nécessaire de modifier les règles établis par défaut concernant la sécurité des mots de passe.

Pour se faire depuis la machine cliente :

- Windows + R
- Dans Exécuter : gpmc.msc
- Dans la fenêtre stratégie de groupe dérouler jusqu'à Default Domain Policy (Forêt: nomdevotreserveur -> Domaines -> votre serveur -> clic droit sur "Default Domain Policy" -> Modifier...

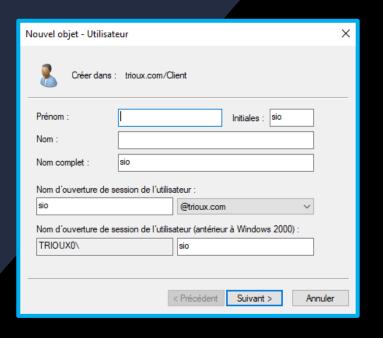


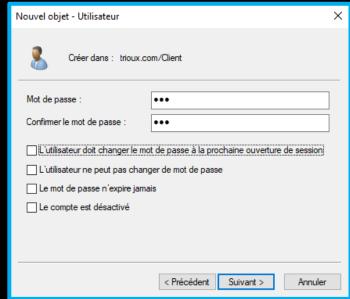
La stratégie des mots de passe

Pour accéder au repertoire de stratégie de mot de passe :

- 1. Configuration ordinateur
- 2. Stratégies
- 3. Paramètres Windows
- 4. Paramètres de sécurité
- 5. Stratégies de comptes
- 6. Stratégie de mot de passe

Ensuite en double cliquant sur les stratégies, nous pouvons modifier les valeurs.

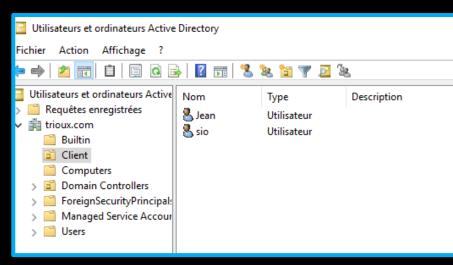


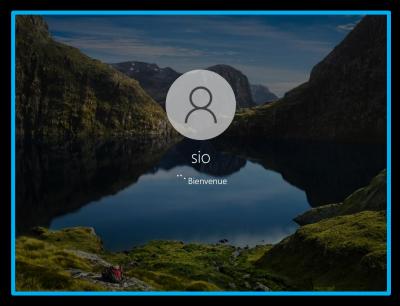


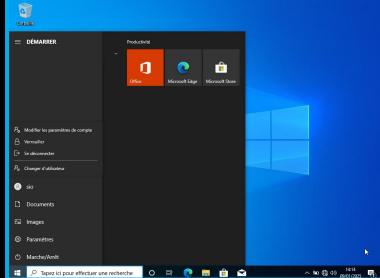
Création du user sio

Afin de verifier si les paramètres de stratégie de mot de passe ont bien été pris en compte, nous allons créer un utilisateur "sio" et pour mot de passe "sio".

L'utilisateur peut être créé et la session s'initialise, tout est ok.







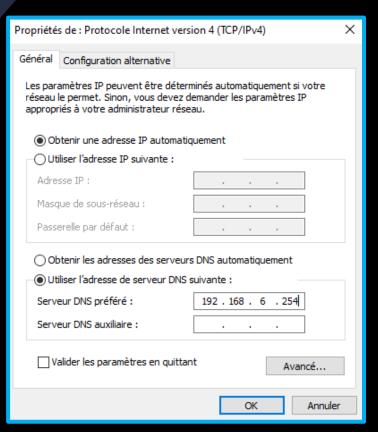
Mise en place d'un service DHCP



Mise en place du DHCP

Concernant le paramétrage d'un service DHCP, vous pouvez vous réitérez à ce $\frac{TP}{T}$ (à partir de la page 22) qui explique comment le mettre en place.

Pinger votre serveur DNS afin de vérifier la liaison entre votre poste client et le serveur.



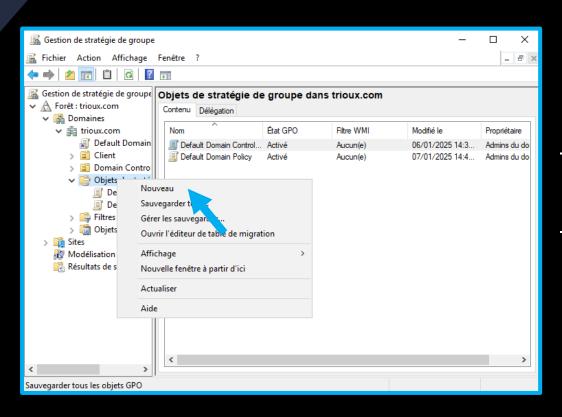
```
Invite de commandes
Microsoft Windows [version 10.0.19043.928]
(c) Microsoft Corporation. Tous droits réservés.
C:\Users\sio>ipconfig /all
Configuration IP de Windows
  Nom de l'hôte . . . . . . . . : Client
  Suffixe DNS principal . . . . . : trioux.com
  Type de noeud. . . . . . . : Hybride
  Routage IP activé . . . . . . : Non
  Proxy WINS activé . . . . . . : Non
  Liste de recherche du suffixe DNS.: trioux.com
Carte Ethernet Ethernet :
  Suffixe DNS propre à la connexion. . . : trioux.com
  Description. . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
  DHCP activé. . . . . . . . . . . . . . . . Oui
  Configuration automatique activée. . . : Oui
  Adresse IPv6 de liaison locale. . . . : fe80::b18c:fca3:1128:313f%8(préféré)
  Masque de sous-réseau. . . . . . . : 255.255.255.0
  Bail obtenu. . . . . . . . . . : jeudi 9 janvier 2025 14:28:17
  Bail expirant. . . . . . . . . . . . . jeudi 16 janvier 2025 14:51:30
  Passerelle par défaut. . . . . . . :
  Serveur DHCP . . . . . . . . . . . . . . . . . 192.168.6.254
  IAID DHCPv6 . . . . . . . . . : 101187623
  DUID de client DHCPv6. . . . . . . : 00-01-00-01-2F-0D-99-F6-08-00-27-20-CC-10
  Serveurs DNS. . . . . . . . . . . . . . . 192.168.6.254
  NetBIOS sur Tcpip. . . . . . . . . . . . Activé
C:\Users\sio>
```



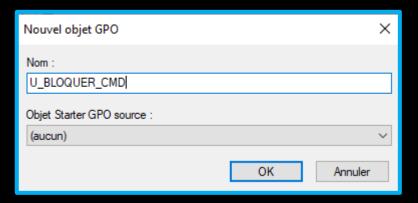


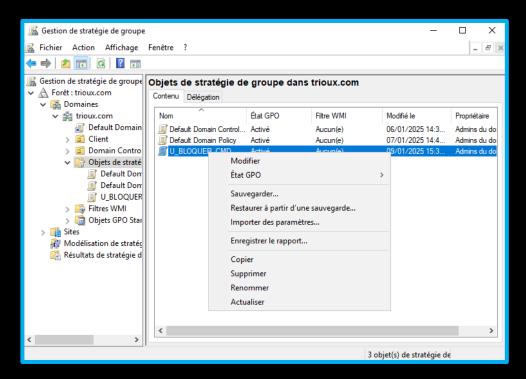
Group Policy Objects (GPOs)

Dans cette partie du TP, nous allons voir comment créer une politique dans une stratégie de groupe. Tout d'abord le **Group Policy Objects** (GPOs), ou en français "stratégie de groupe", est un ensemble d'outils intégrés à Windows Server permettant au service informatique de **centraliser la gestion de l'environnement utilisateur** et la configuration des machines grâce à l'application de **politiques**.

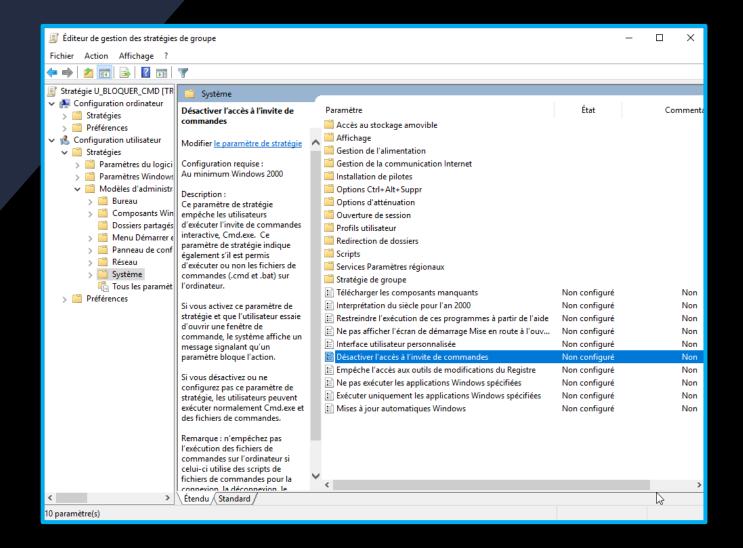


- Windows + R : "gpmc.msc", vous arrivez dans la fenêtre de gestion de stratégie de groupe;
- Dérouler votre domaines et faites clic droit sur "**Objets** de stratégie de groupe" et "**Nouveau**".



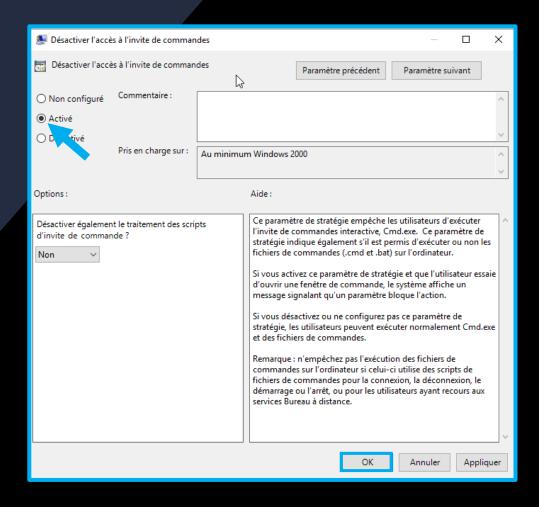


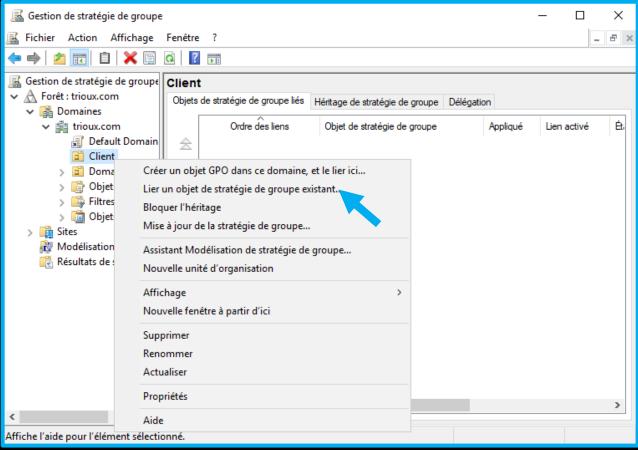
- Nommer votre GPO, ici, nous allons bloquer l'accès à l'invite de commande pour tous les utilisateurs (d'où le préfixe "**U**" pour **User**);
- Clic droit sur votre GPO et cliquer sur "Modifier".



La fenêtre "Editeur de gestion des strategies de groupe" s'ouvre, c'est ici que l'on peut configurer les paramètres à appliquer sur les utilisateurs ou bien les ordinateurs.

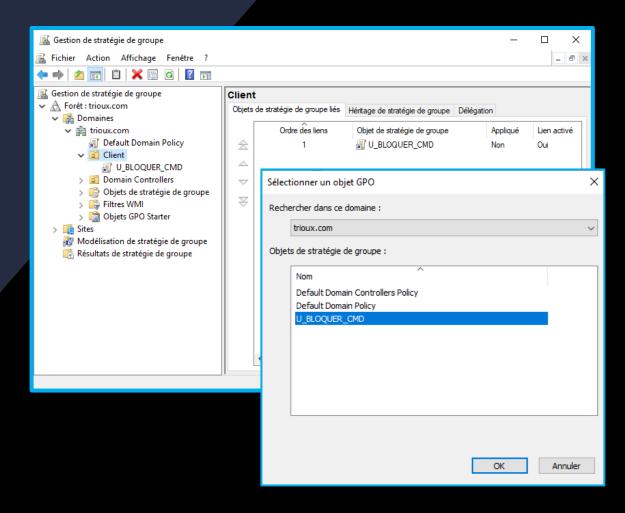
Pour désactiver l'accès à l'invite de commande à tous les utilisateurs, rejoignez le chemin "Système" et faites un clic droit sur "Désactiver l'accès à l'invite de commandes"

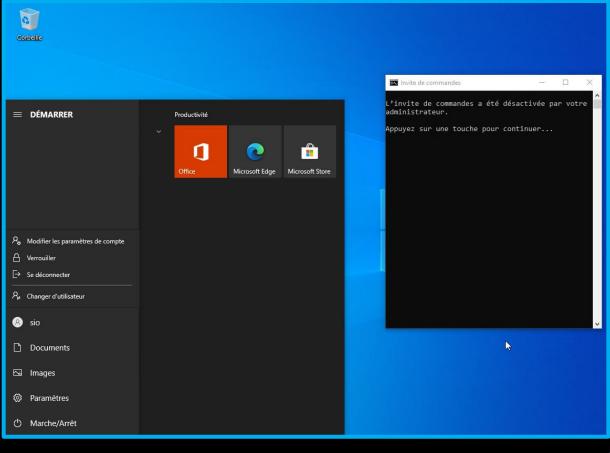




Cocher "Activé" et faites "OK".

Retournez dans la gestion des stratégies de groupe, faites un clic droit et sélectionnez "Lier un objet de stratégie de groupe existant..."





Sélectionner votre GPO puis "**OK**". Nous pouvons voir qu'il est bien affecté à l'unité organisationnelle "**Client**" donc pour les deux utilisateurs "**Jean**" et "**sio**". Les utilisateurs de l'U.O "Client" ne peuvent plus utiliser l'invite de commande et un message d'erreur s'affiche lorsque l'utilisateur essayera d'y accéder.