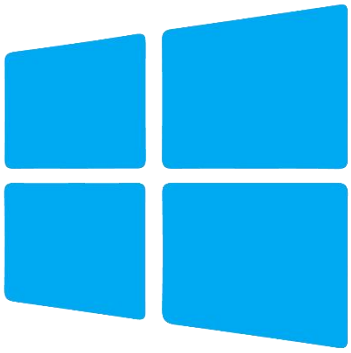
11/11/2023

Atelier :Active Directory

Cyber Management School



Microsoft Active Directory

AKAZAF ABDELLAH ; ADJAHOUISSO JEAN-BAPTISTE ; PORTIER JORIS

Introduction :

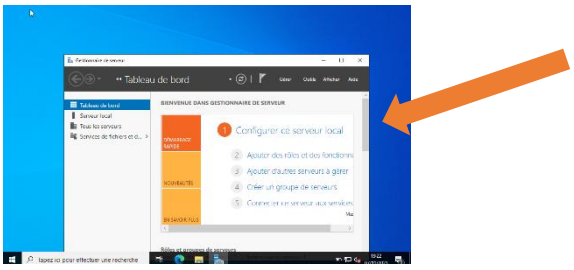
Dans le cadre de notre mission en tant qu'Ingénieur cyber sécurité, votre entreprise vous demande de mettre en place un Active Directory. Pour ce faire, nous avons utiliser un domaine Windows. En termes simples, un domaine Windows est un groupe d'utilisateurs et d'ordinateurs sous l'administration d'une entreprise donnée. L'idée principale derrière un domaine est de centraliser l'administration des composants communs d'un réseau d'ordinateurs Windows dans un référentiel unique appelé Active Directory (AD). Le serveur qui exécute les services Active Directory est appelé Contrôleur de Domaine (DC)

Les principaux avantages d'avoir un domaine Windows configuré sont les suivants :

Gestion centralisée de l'identité : Tous les utilisateurs à travers le réseau peuvent être configurés depuis Active Directory avec un minimum d'effort.

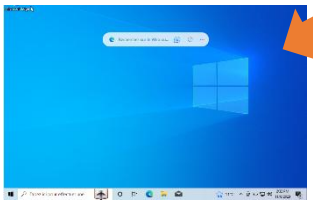
Gestion des politiques de sécurité : Vous pouvez configurer des politiques de sécurité directement depuis Active Directory et les appliquer aux utilisateurs et aux ordinateurs du réseau selon les besoins.

Installation de Windows Server et deux clients Windows au choix :

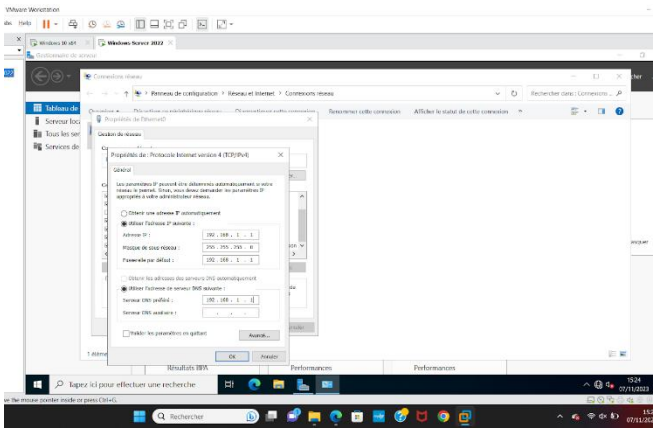


Windows Server

Windows Client

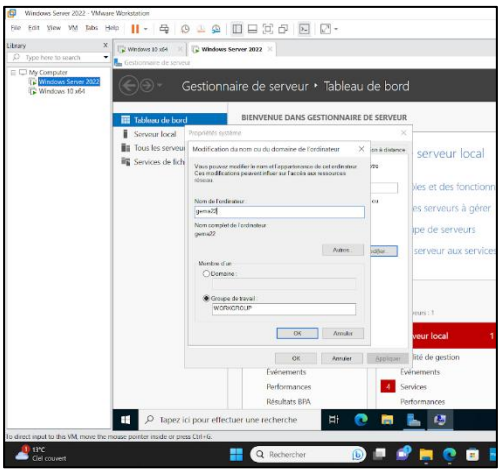


En utilisant l'exécution de la commande "ncpa.cpl", nous accéderons aux paramètres réseau de la machine, ce qui nous permettra de configurer une adresse IP. Cette configuration nous permettra ensuite de détecter et d'envoyer des requêtes de Ping entre les différentes machines du réseau. L'adresse IP du domaine DNS est 192.168.1.1



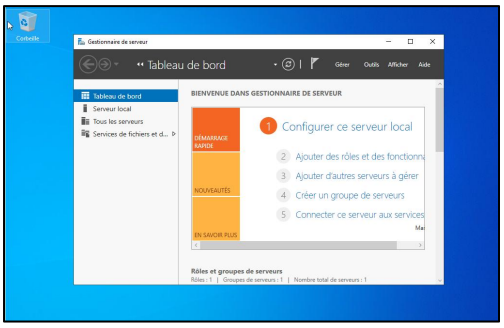
```
Carte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::acc6:c5c9:ee3e:8d1d%4
   Adresse IPv4. . . . . . . . . . . . . : 192.168.1.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 0.0.0.0
```

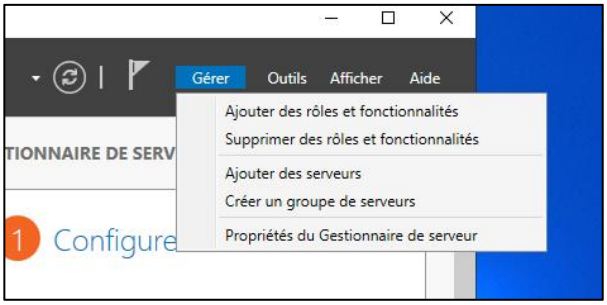
Une fois que nous avons défini une adresse IP pour la machine, nous devons également modifier le nom par défaut, que nous avons changé pour "gema22".

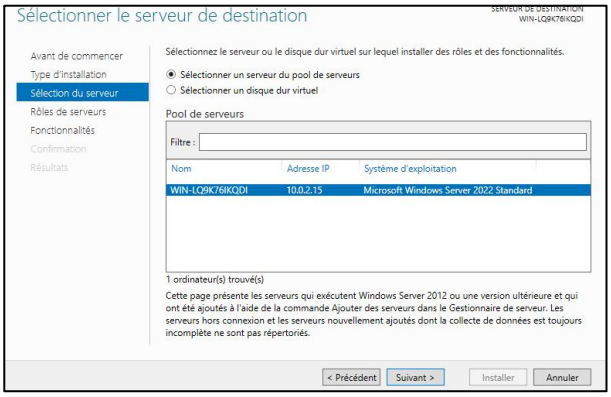


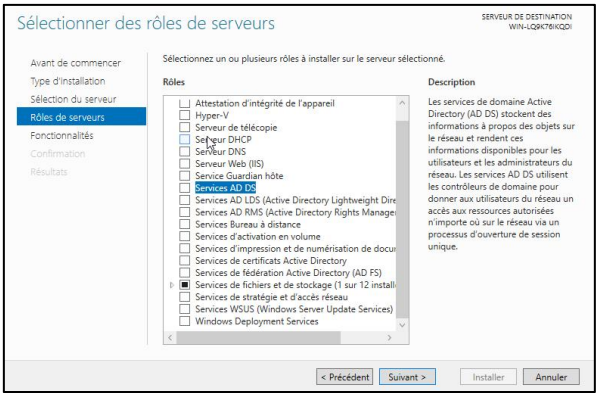
Créer un AD dans votre Windows Server :

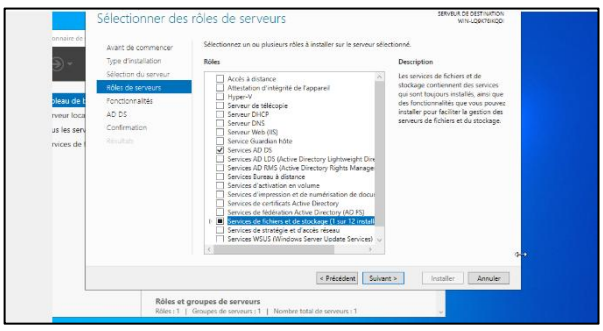
Notre objectif est de créer un domaine AD spécifique à l'entreprise. Une fois créé, nous configurerons des groupes

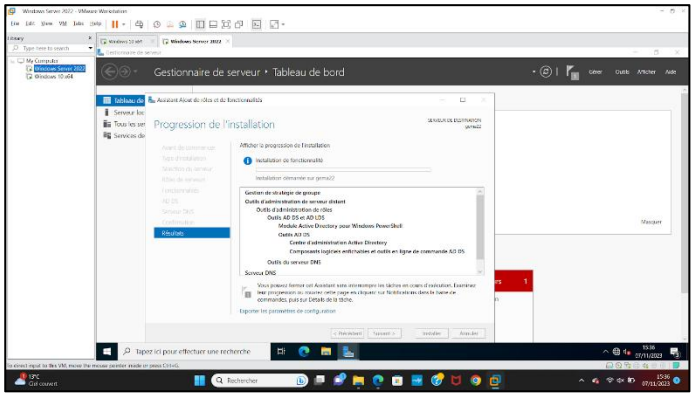




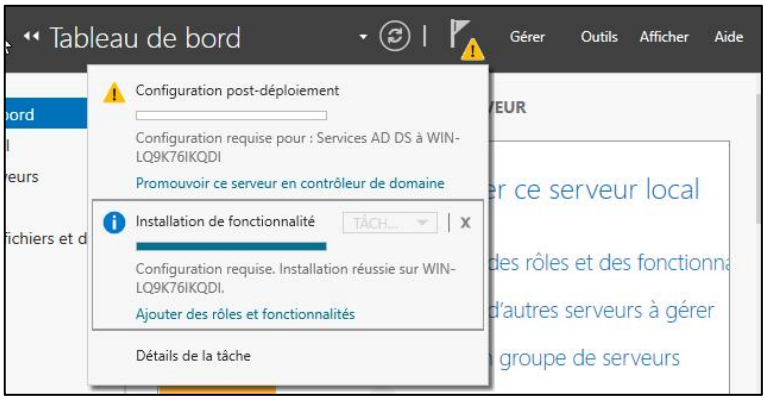




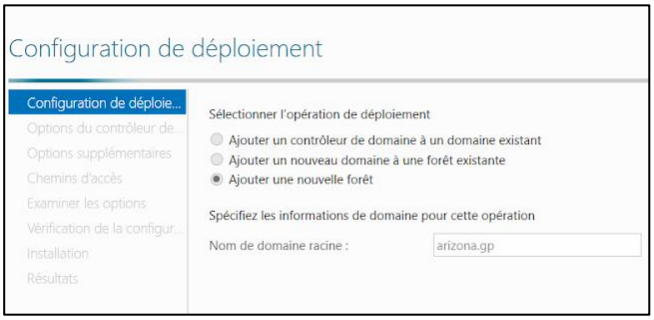




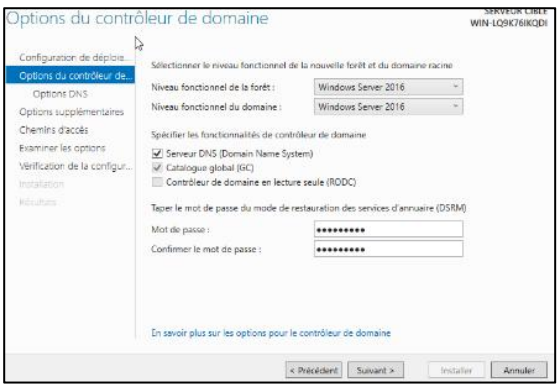
On vient de configurer et d'installer les rôles mais il faudra installer notre domaine

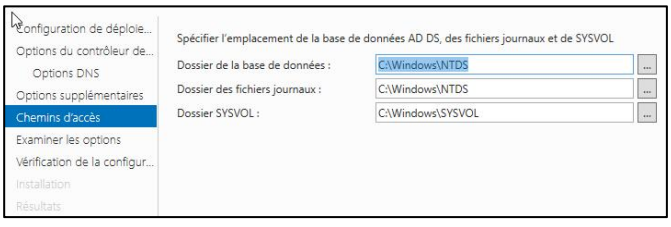


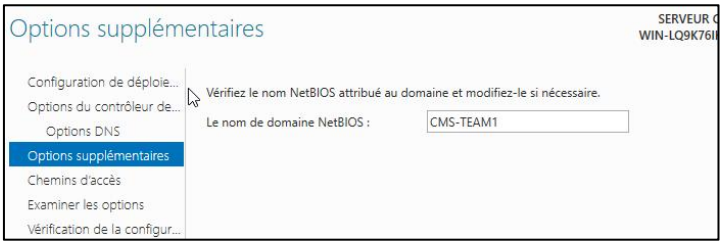
Cette notification nous redirige vers le panneau de la configuration de déploiement. Ici, nous allons ajouter une nouvelle foret AD car il n'en existe pas, plus le nom de domaine.



Par la suite, Nous allons sélectionner les path pour certains répertoires qui vont nous être utiles plus tard pour le logs, les journaux. Pour la partie deux du TP sur le fait de remonter des alertes. Nous avons finalisé la configuration reste plus qu'à passer à la partie vérification, installation et la machine



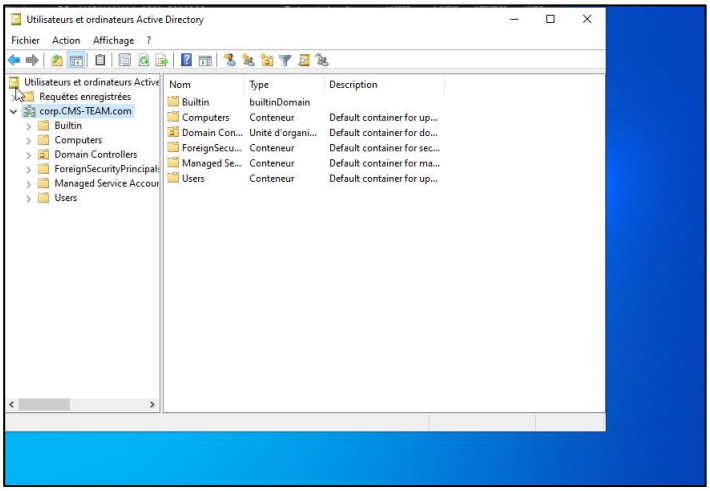




Une fois installer, le serveur redémarre et notre Domain AD est créé

Création de groupes d'utilisateurs sur l'AD

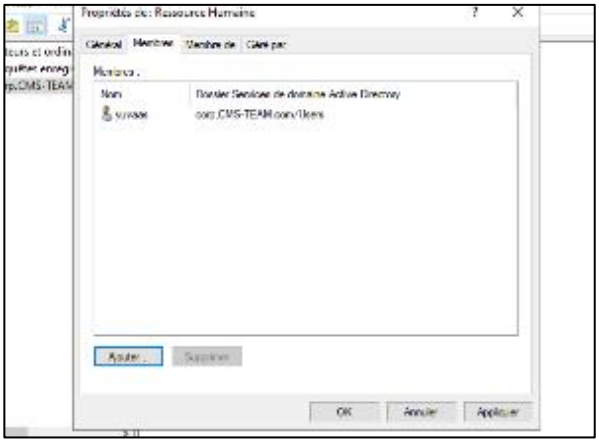
Dans les outils, nous allons choisir
Utilisateurs et ordinateurs active Directory



On remarque qu'il existe des conteneurs par défaut alors qu'on a rien créé. Ces conteneurs sont créés automatiquement par Windows et contiennent ce qui suit :

- Builtin : Contient les groupes par défaut disponibles pour n'importe quel hôte Windows.
- Computers : Toute machine rejoignant le réseau sera placée ici par défaut. Vous pouvez les déplacer si nécessaire.
- Domain Controllers : OU par défaut qui contient les contrôleurs de domaine (DC) de votre réseau.
- Users : Utilisateurs et groupes par défaut qui s'appliquent à l'ensemble du domaine.
- Managed Service Accounts : Contient des comptes utilisés par les services dans votre domaine Windows."

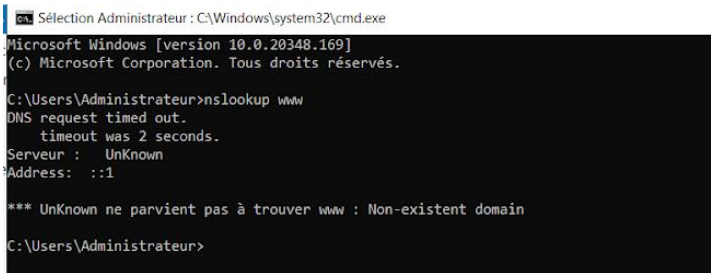
Nous allons créer des groupes pour faciliter la gestion des utilisateurs grâce aux stratégies groupes. De plus, pour ajouter un membre dans un groupe il faut que le membre soit déjà inscrit en tant qu'utilisateur, un membre qui n'est pas déjà inscrits ne pourra pas être ajouter à un groupe



Intégrez deux clients Windows à votre AD

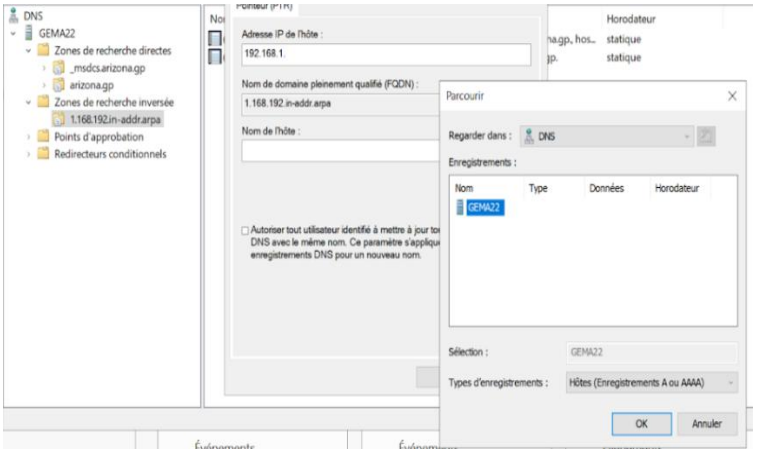
Nous allons maintenant intégrez deux clients Windows à notre domaine AD.Pour pouvoir le faire , il faudra verifier que notre Serveur AD et les systemes du client sont connectés et sont sur le meme reseau. En effet , il doit etre connecté pour communiquer .

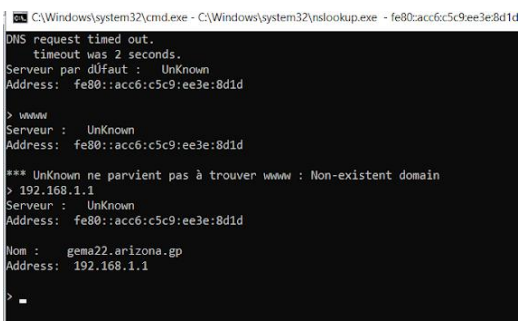
Pour commencer nous allons configurer le DNS. Cette configuration est importante pour le bon fonctionnement du serveur. Grace à la commande **« nslookup www »**, on se rend compte que le serveur n'est toujours pas reconnu.

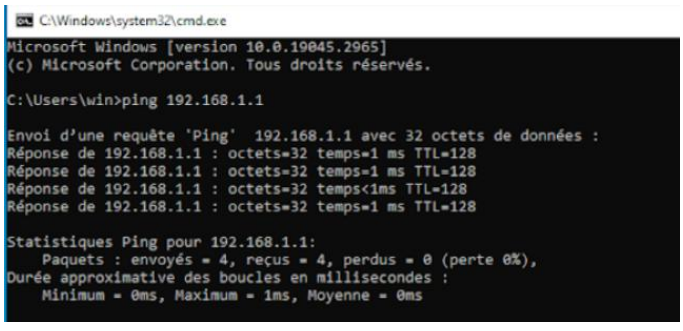


Nous avons utilisé une zone inverse pour que notre serveur soit identifiable et qu'il puisse faire une recherche inverse de l'IP a un nom de domaine, pour une zone directe c'est l'inverse avec un nom de domaine on trouve un IP. Nous avons créé un nouveau pointeur dans lequel nous lui avons attribué l'IP de notre machine.

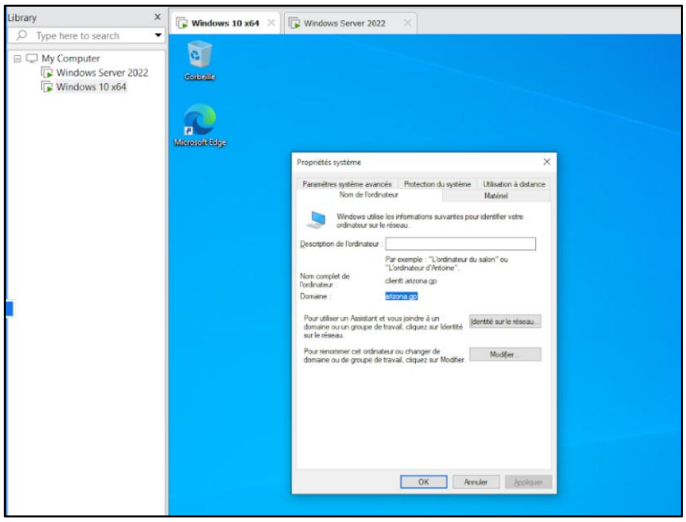
Nous avons vu si le serveur et la machine client communiquait (Commande : ping et nslookup www). Ensuite nous avons créé un nouvel alias dans la zone de recherche direct sur le serveur nous allons lui attribuer le nom www et allons lui attribuer le domaine de gema que nous avons créé au préalable.







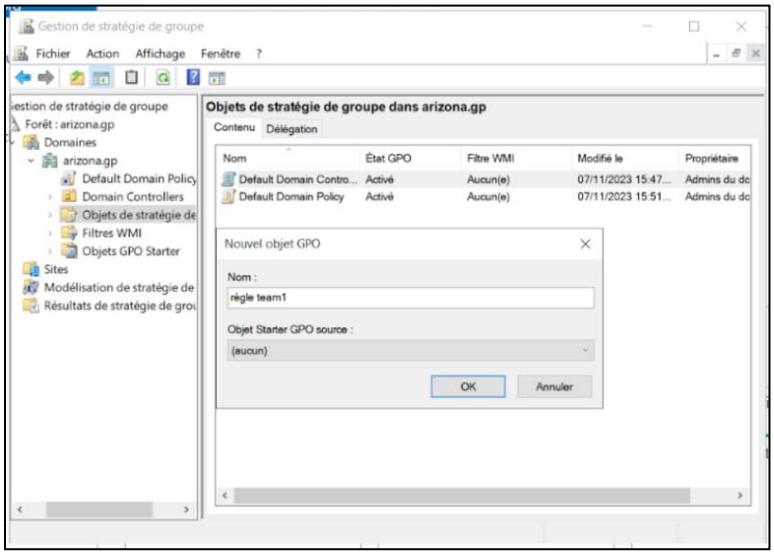
On voit que les machine communique bien entre elle avec PING et de qu'avec une requet www l'IP de la machine nous pointe sur le nom de notre domaine gema22.arizona.gp.

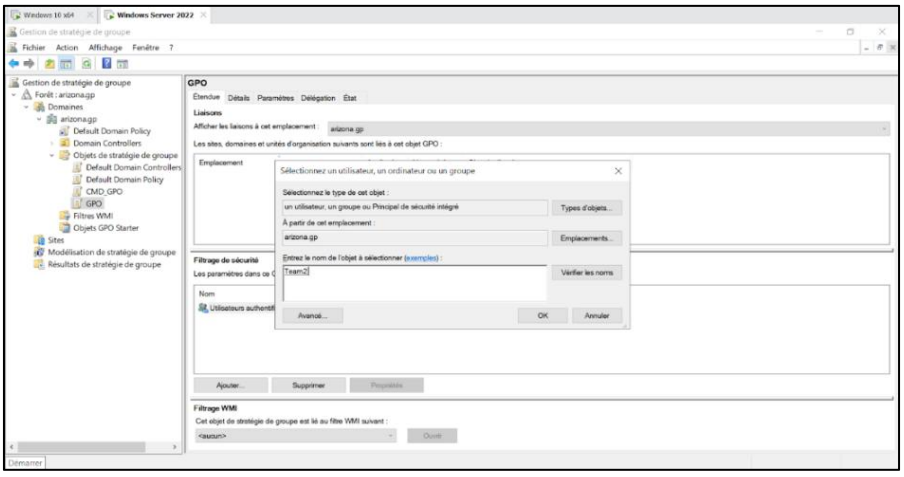


Des politiques de sécurité locales (mot de passe/comptes/application…) via GPO

Pour la gestion des stratégies de groupe, nous disposons de plusieurs options. Tout d'abord, nous avons créé deux groupes, Team1 et Team2, dans lesquels un ou plusieurs utilisateurs sont assignés. Nous avons identifié plusieurs restrictions à prendre en considération :

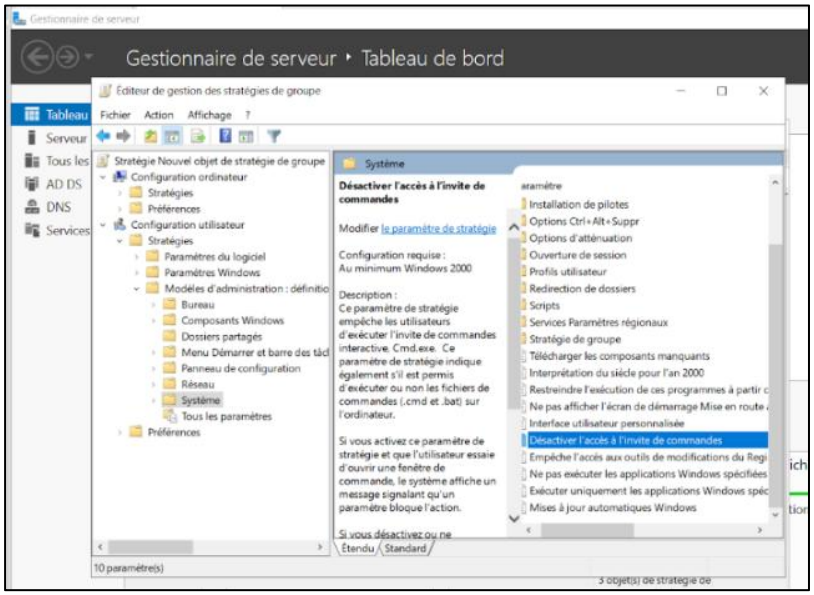
- Limiter l'utilisation de l'invite de commente a un groupe
- Crée une politque de mots de passe complexe
- Crée une politique de mots de passe a 12 caracter
- Crée un verou de l'utilisation de compte au bout 3 tentative



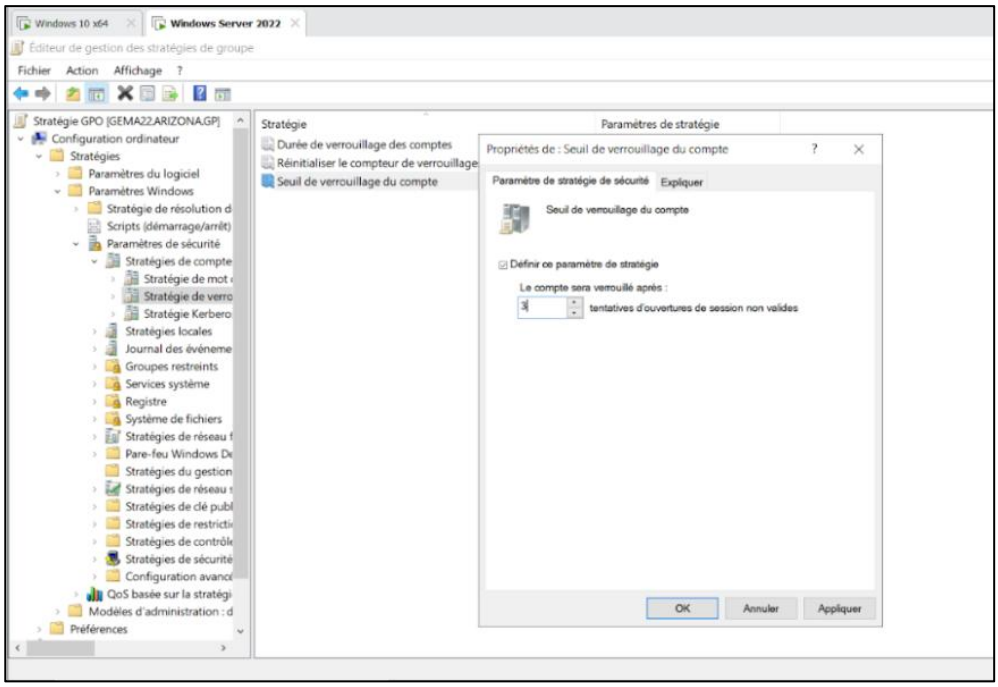


Chaque GPO doit avoir un nom qui nous permettra de les reconnaître, afin de leur attribuer une ou plusieurs règles et un ou plusieurs groupes.

Nous avons choisi, pour la Team2, de restreindre l'utilisation de l'invite de commande. Sur la capture ci-dessous, son état était désactivé, et nous l'avons activé

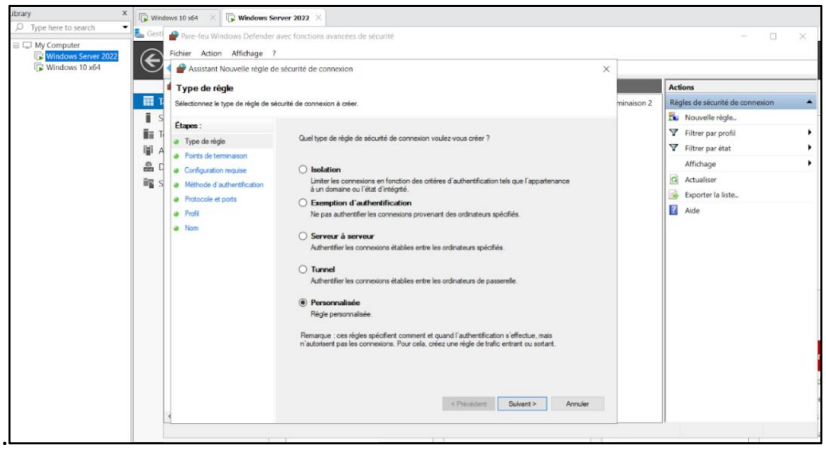


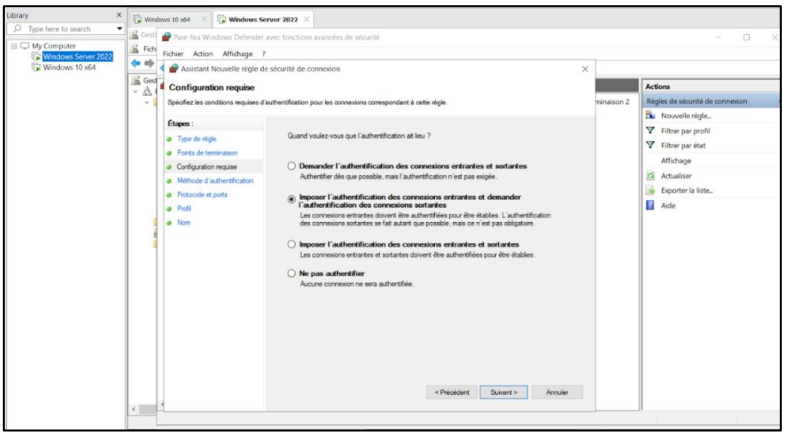
Pour la deuxième GPO, nous avons appliqué une stratégie sur la sécurité des sessions et des mots de passe. Dans l'arborescence des stratégies de compte, nous avons activé deux stratégies de mots de passe et une stratégie de verrouillage. Sur la capture ci-dessous, nous avons paramétré trois tentatives non valides pour bloquer le compte, douze caractères pour le mot de passe, et activé l'utilisation de mots de passe forts. Sur cette politique, nous n'avons pas pu apporter d'option car Windows considère par défaut qu'un mot de passe fort doit inclure une majuscule, un chiffre et un caractère special



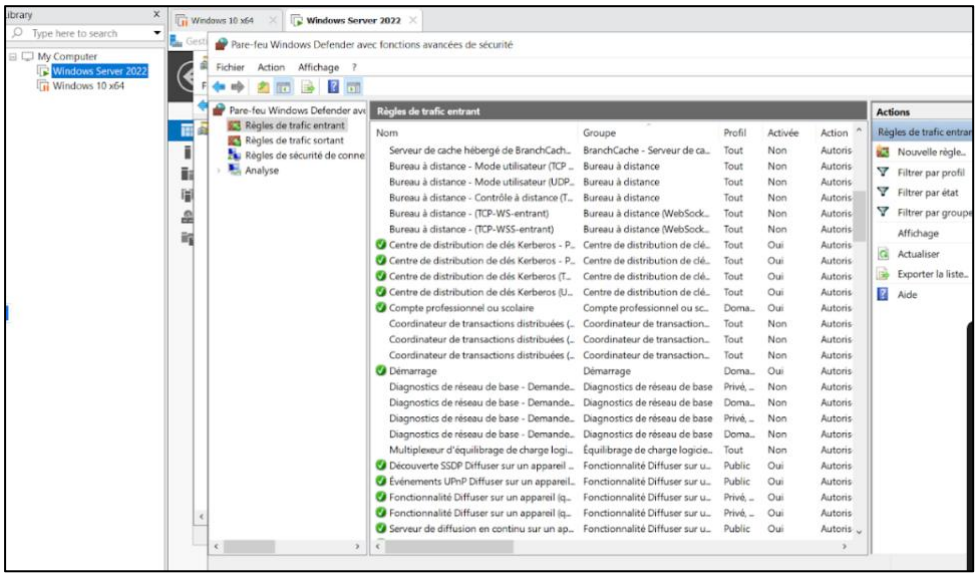
<u>Des règles de flux entrant/sortant sur le pare-feu (blocage de ports, d'adresses…) directement sur une machine Window.</u>

Sur les règles du pare-feu, nous avons tout d'abord, dans le typage des règles personnalisées, défini les nôtres. Nous avons plusieurs possibilités, l'une d'entre elles se trouve dans l'onglet de droite "ACTION", où l'on peut ajouter une nouvelle règle et/ou désactiver ou activer une règle déjà existante



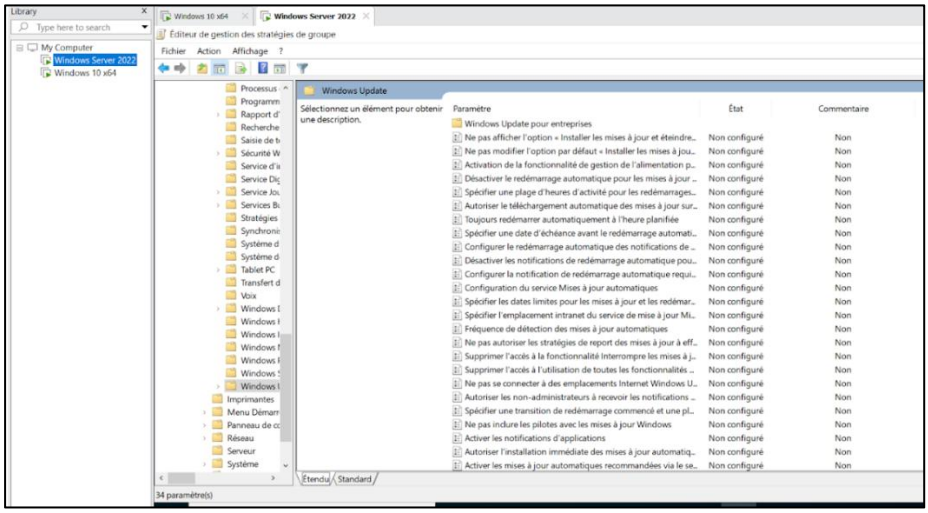


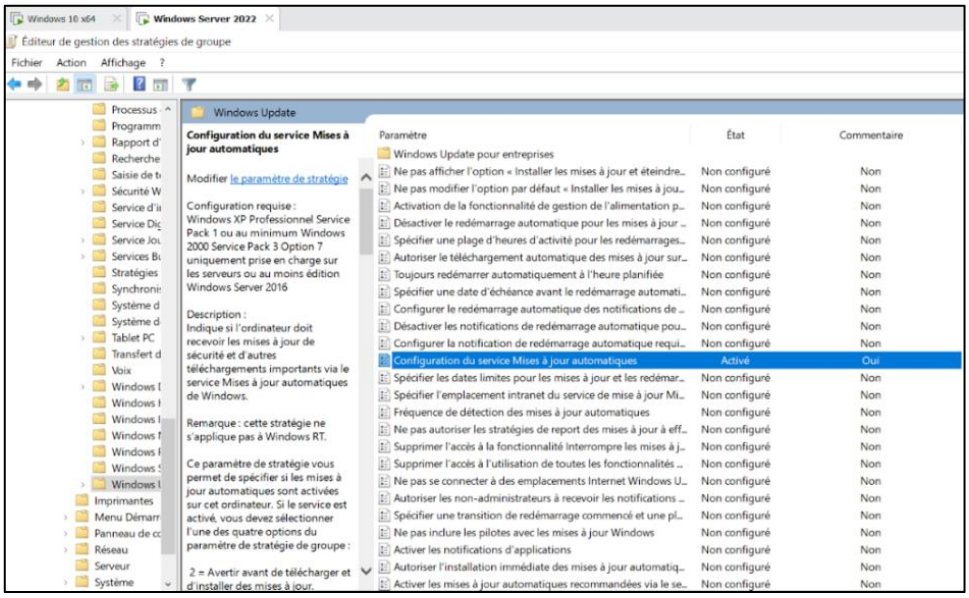
Pour notre groupe, nous avons désactivé toutes les utilisations du Bureau à distance pour renforcer la sécurité en cas d'attaque informatique. Le pare-feu bloque tout le trafic entrant du Bureau à distance sur les protocoles TCP/UDP.



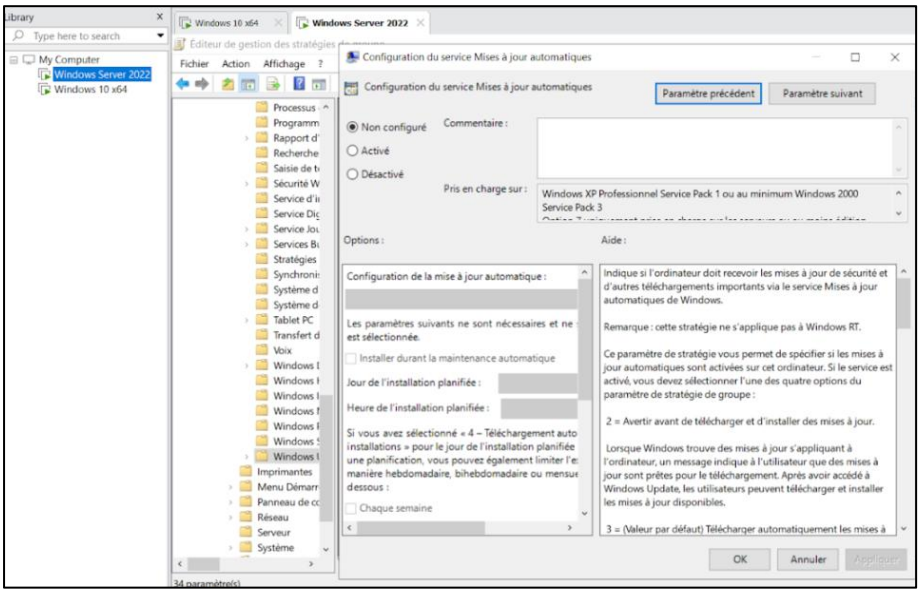
Une politique sur les MAJ Windows (sur la machine client)

En premier lieu, pour configurer le paramètre de mise à jour des machines, sur la barre de recherche Windows, nous allons taper gpedit.msc. Pour la configuration des mises à jour, la démarche est similaire à celle d'une Stratégie de groupe locale que nous avons effectuée un peu plus tôt. Celle qui nous intéresse se trouve dans Configuration Ordinateur local/Modèles d'administration/Composant Windows/Windows Update : le paramètre qui nous intéresse est "Configuration de service de Mise à jour automatique".



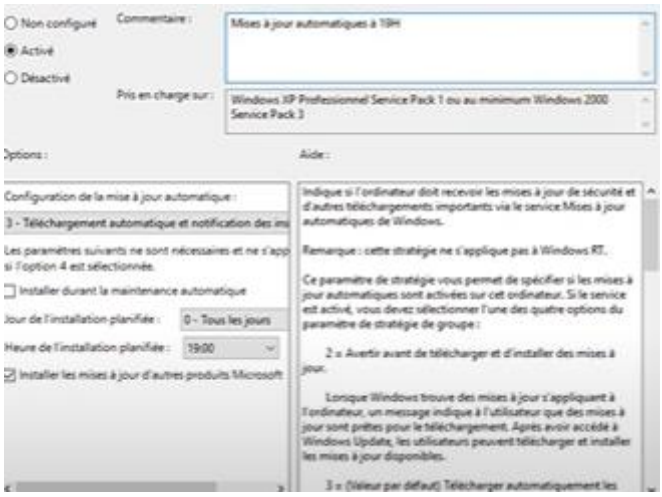


Dessus, nous pouvons donc l'activer, ajouter un commentaire au moment de la mise à jour, spécifier une heure à laquelle elle devrait se faire et définir quand elle devrait se produire.



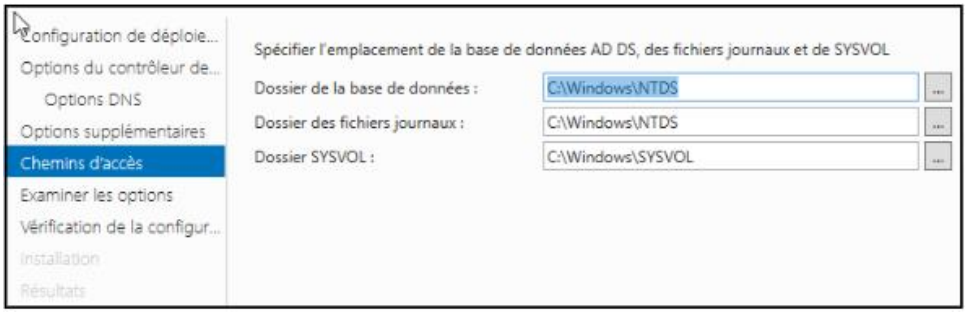
Nous avons apporté pour un paramétrage :

- Tous les jours
- A 19h00
- L'installations des autres produits microsoft
- Avec le commenter "Mise a jours automatiques a 19h"

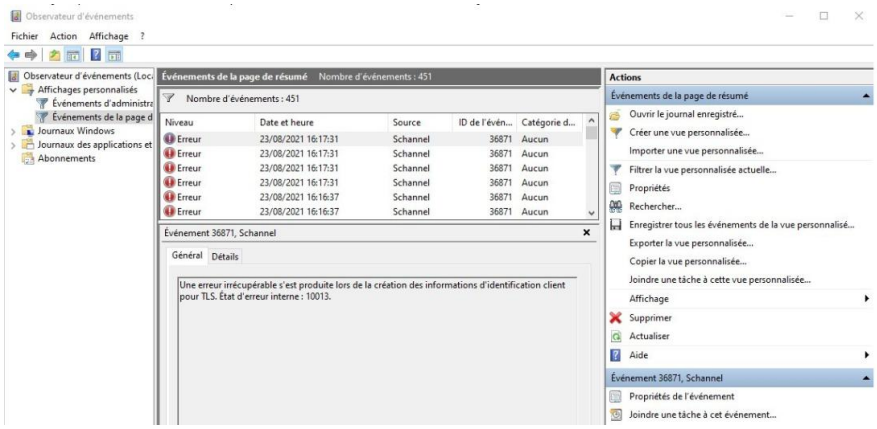


Gestion des évènement Windows :

Sur le point suivant, nous allons jeter un coup d'œil sur les événements de sécurité. Nous avons essayé trois mots de passe incorrects pour faire apparaître l'erreur dans les journaux de la machine. Dans les points précédents sur la création de l'AD, nous avons parlé d'un chemin qui nous mène aux journaux des événements.



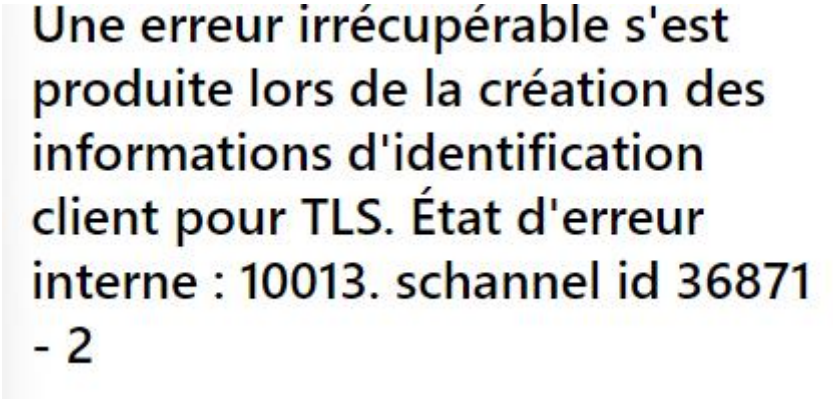
Nous sommes parties jeter un œil sur les fichiers et les dossiers mais les logs étaient chiffrés. Alors nous sommes parties voir sur l'observateur d'évènements pour nous restituer tous les évènements passé sur notre AD



Nous avons plusieurs infos :

- Niveau d’erreur qui peut varier de 1 à 6
- La date de l’évènement
- Sa source
- Son ID

Pour comprendre l’ID de l’évènement 36871 nous sommes parties sur le site de Microsoft qui nous indique ceci.



Nous avons plusieurs possibilités dans l'Observateur d'événements, telles que la possibilité de filtrer les événements en fonction de leurs informations, ou mieux encore, de créer une vue personnalisée pour suivre les événements qui nous sont importants.