

# Atelier Professionnel



Alesio ARAPI  
BTS SIO 2025

## **Description du système informatique**

Le système informatique de cette petite entreprise d'assurance est centralisé au sein d'un unique étage de bureaux, où travaillent 15 employés. L'entreprise gère ses activités principales, notamment la gestion des contrats, le suivi des sinistres, la relation client, ainsi que la comptabilité et l'administration.

Une salle serveur de taille modeste est installée dans un local sécurisé, accessible uniquement aux administrateurs système via badge d'accès. Ces serveurs gèrent les services de base tels que le réseau interne (DHCP, DNS, annuaire Active Directory), la messagerie professionnelle et les applications métier essentielles (édition et gestion des contrats d'assurance, base de données clients et sinistres, suivi des indemnisations, et un logiciel de gestion comptable simplifié). L'entreprise utilise également un système de sauvegarde quotidienne sur un cloud sécurisé.

Le réseau est segmenté en différents accès pour garantir la sécurité des données sensibles. Une attention particulière est portée à la protection contre les cyberattaques, avec des solutions de pare-feu et d'antivirus centralisées.

## **L'équipement informatique**

Chaque employé dispose d'un ordinateur fixe connecté au réseau interne. Le parc informatique comprend 15 postes de travail standard ainsi que deux serveurs physiques hébergeant plusieurs machines virtuelles.

Les employés en charge du suivi client et des sinistres disposent d'un double écran pour améliorer leur productivité. Le directeur et les commerciaux sont dotés d'ordinateurs portables pour leurs déplacements professionnels.

L'entreprise a mis en place une politique d'équipement homogène afin de faciliter la maintenance informatique et la gestion des mises à jour. Chaque employé dispose d'une adresse de messagerie professionnelle sous la forme nom.prenom@assurances-pme.com.

## **Organisation du réseau**

L'ensemble du réseau est centralisé sur un unique étage. Une baie de brassage assure la connexion de tous les postes de travail et équipements au réseau de l'entreprise via des connexions filaires et un réseau Wi-Fi sécurisé.

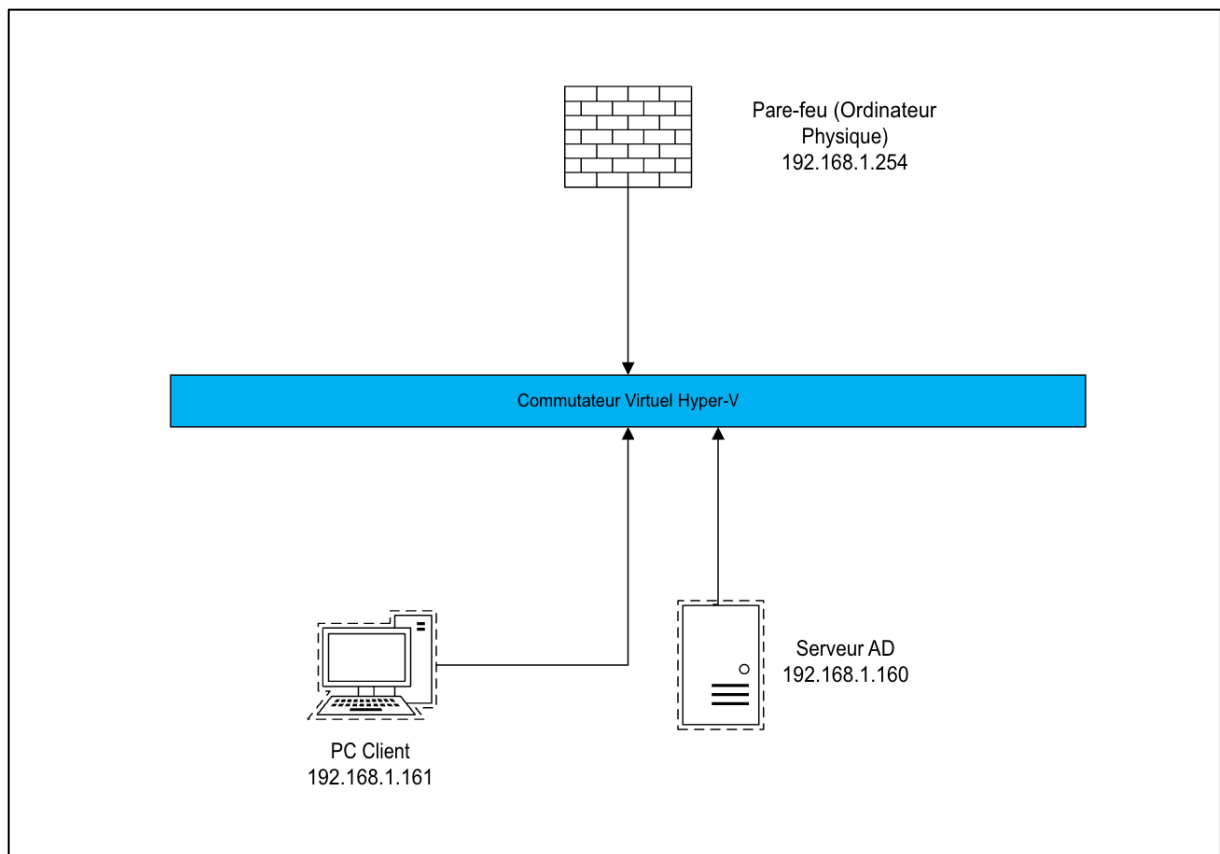
La salle de réunion est équipée d'un vidéoprojecteur, d'un système de visioconférence et d'un tableau interactif pour les présentations et les réunions à distance avec les partenaires et clients.

## Salle serveur et connexion internet

L'organisation des serveurs et des équipements réseaux est la suivante :

- Le serveur principal est virtualisé sous Hyper-V

### Environnement virtuel :



# **Rapport technique du projet**

## **L'équipe du Pôle Projet :**

- Alesio ARAPI – Étudiant BTS SIO option SISR.

Profil : Technicien Système & Réseau

## **Introduction :**

Ce projet vise à restreindre certaines fonctionnalités et applications sous Azure AD afin de renforcer la sécurité et le contrôle des accès, en limitant l'utilisation de paramètres sensibles comme le panneau à distance.

## **Objectifs du Projet :**

Les objectifs du projet sont :

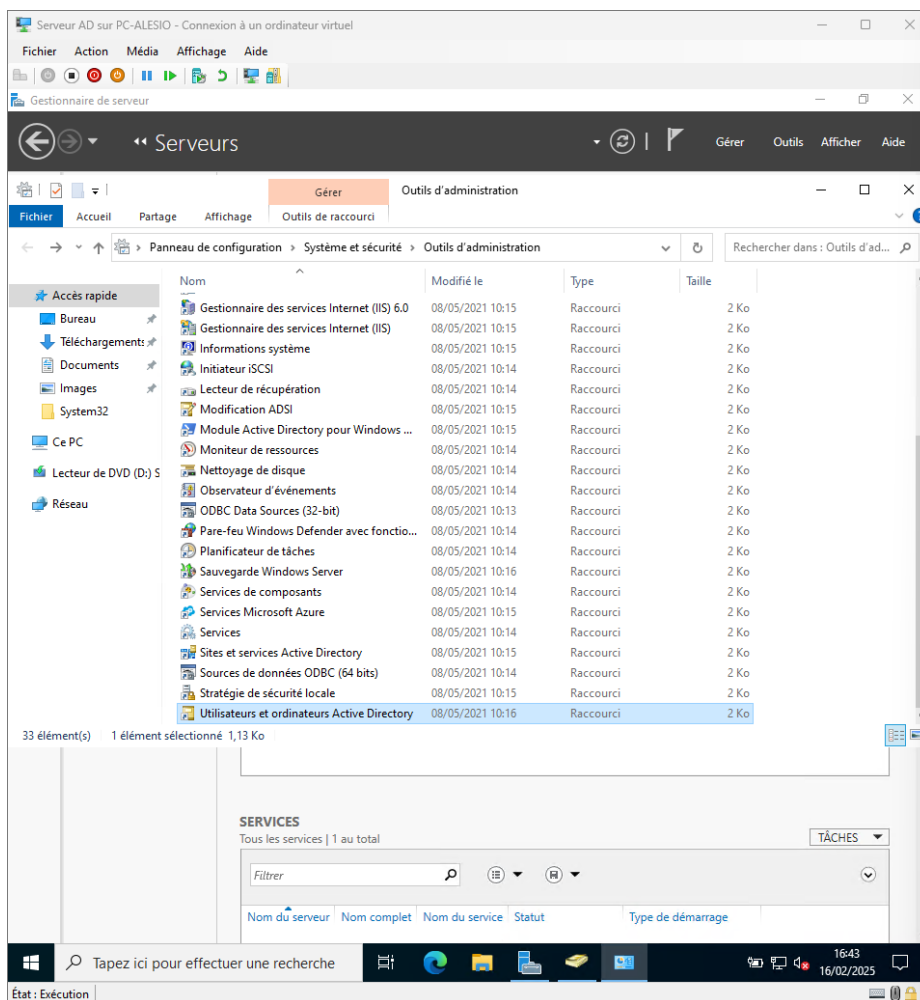
- Phase 1 : Installation + configuration de l'Azure AD
- Phase 2 : Mise en place des utilisateurs et de la stratégie de groupe
- Phase 3 : Tests finaux

# Installation et configuration de l'Azure AD

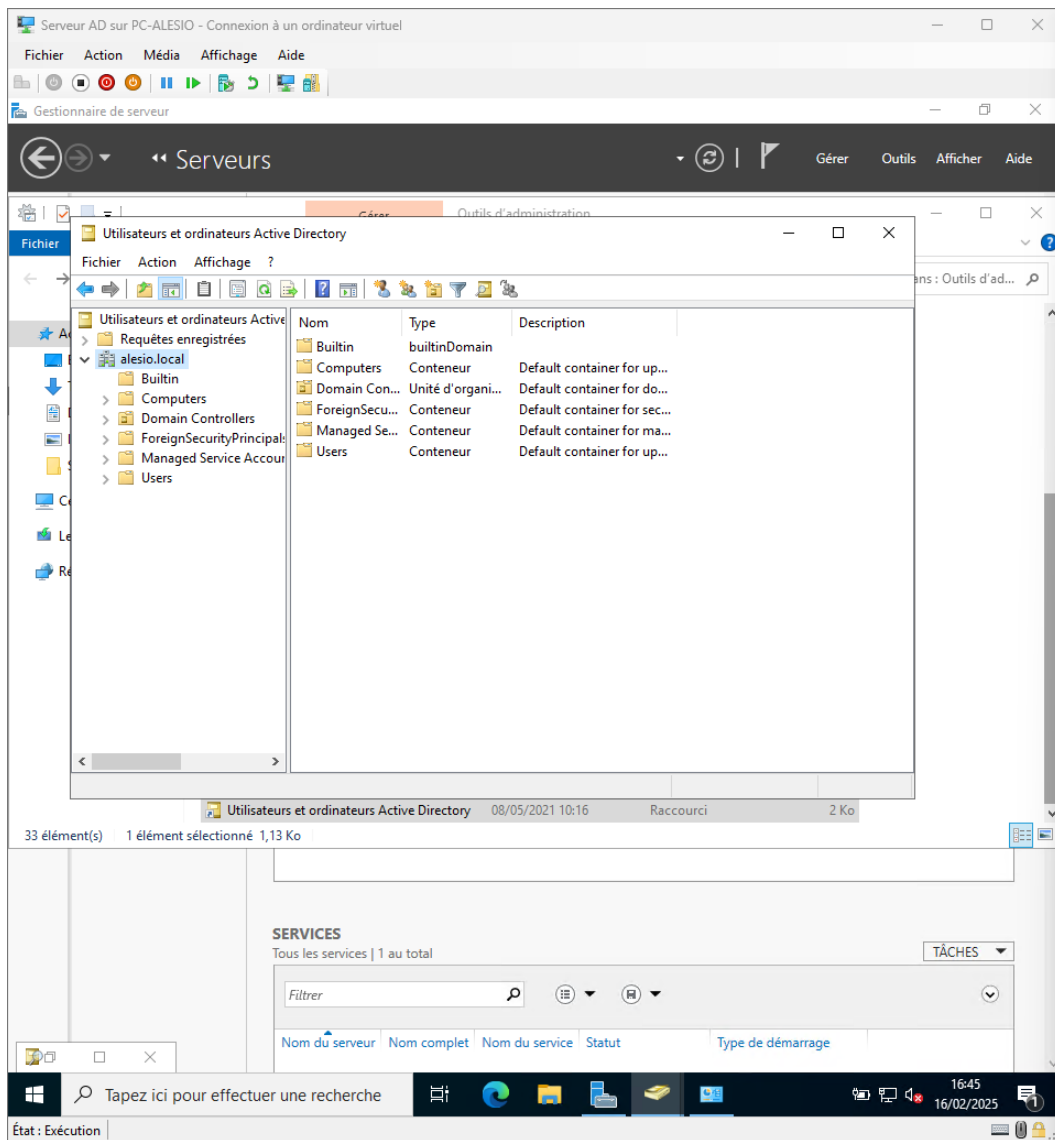
Après avoir configuré le domaine **alesio.local** et mis en place l'infrastructure Active Directory, nous passons à l'intégration des utilisateurs et des groupes. Cette étape permet de centraliser la gestion des comptes, d'attribuer des permissions spécifiques et de sécuriser l'accès aux ressources du réseau.

## Mise en place des utilisateurs

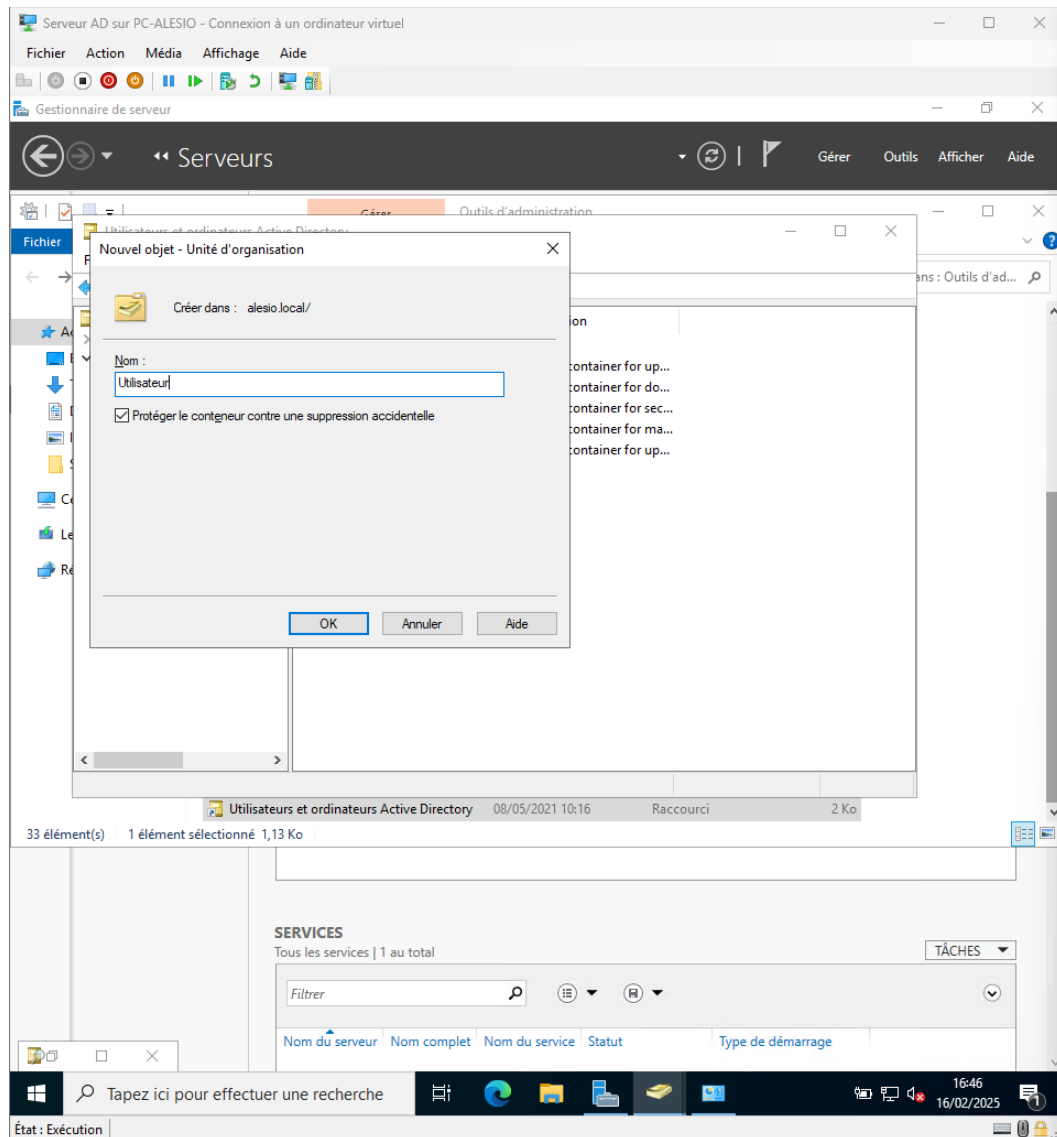
Pour cela, il faut accéder aux outils d'administration du serveur.



Ouvrir la console « Utilisateurs et Ordinateurs Active Directory ».

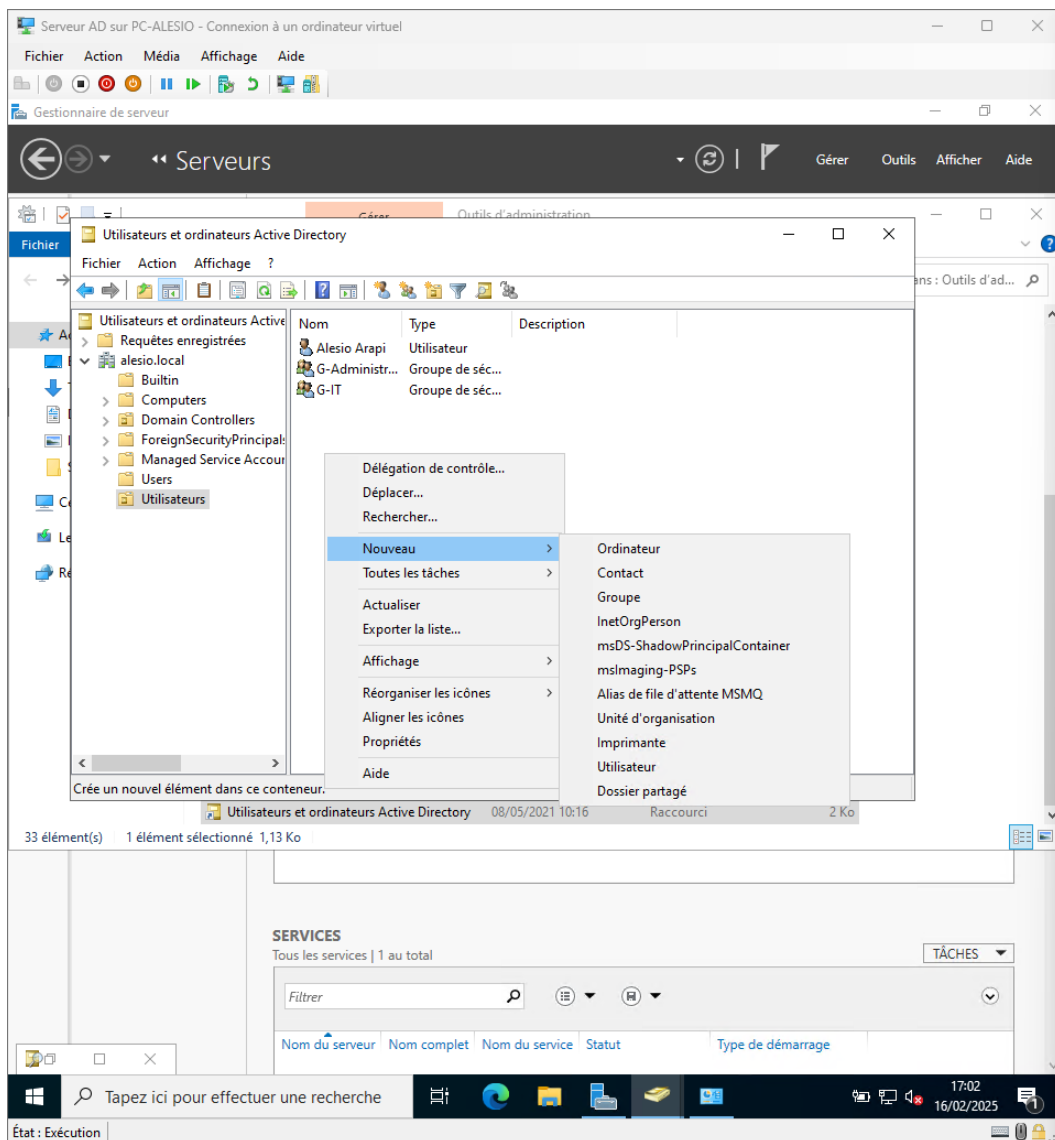


Créer une nouvelle unité d'organisation pour regrouper les utilisateurs (optionnel).

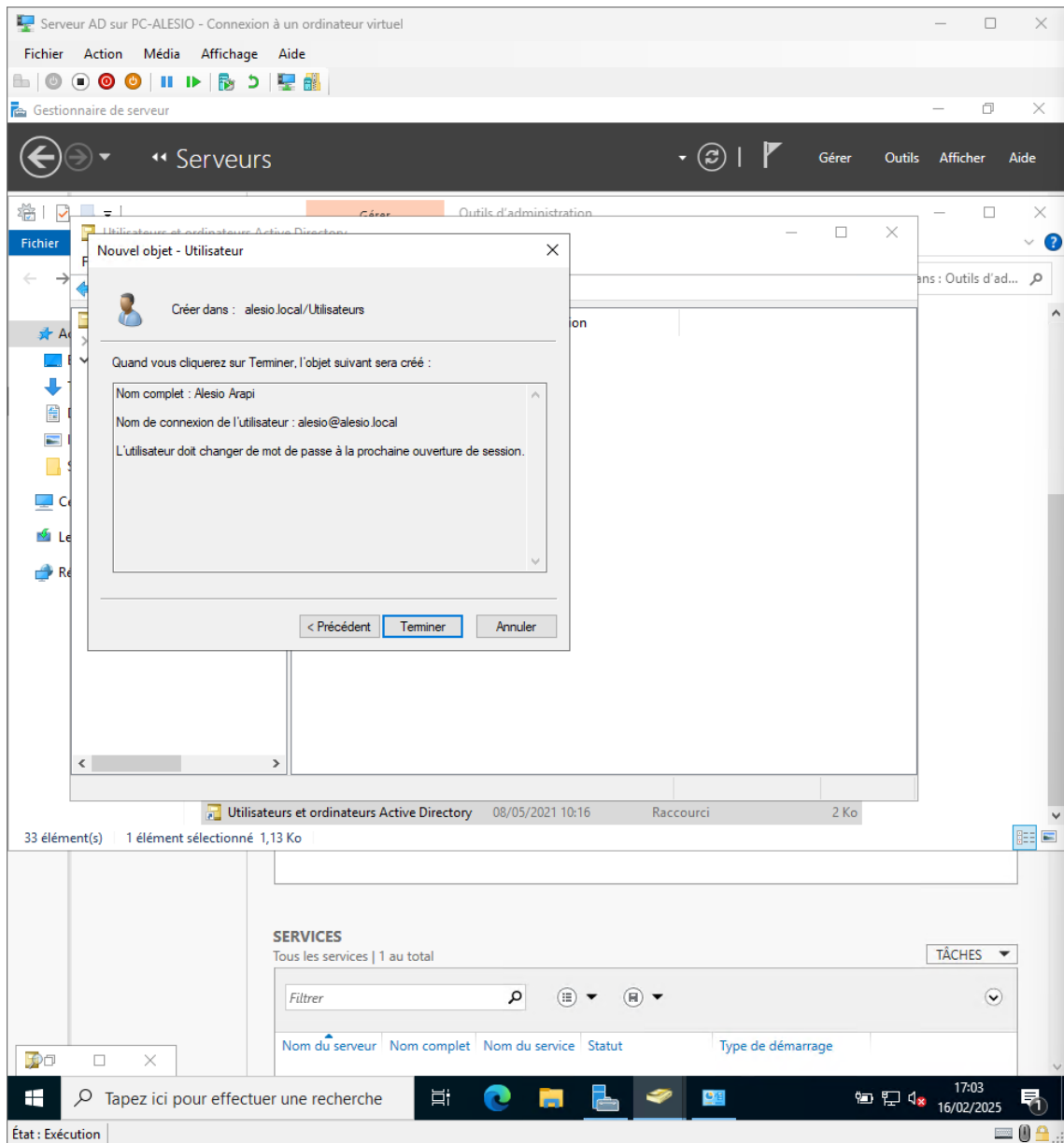




Ajouter un nouvel utilisateur dans l'unité d'organisation créée.

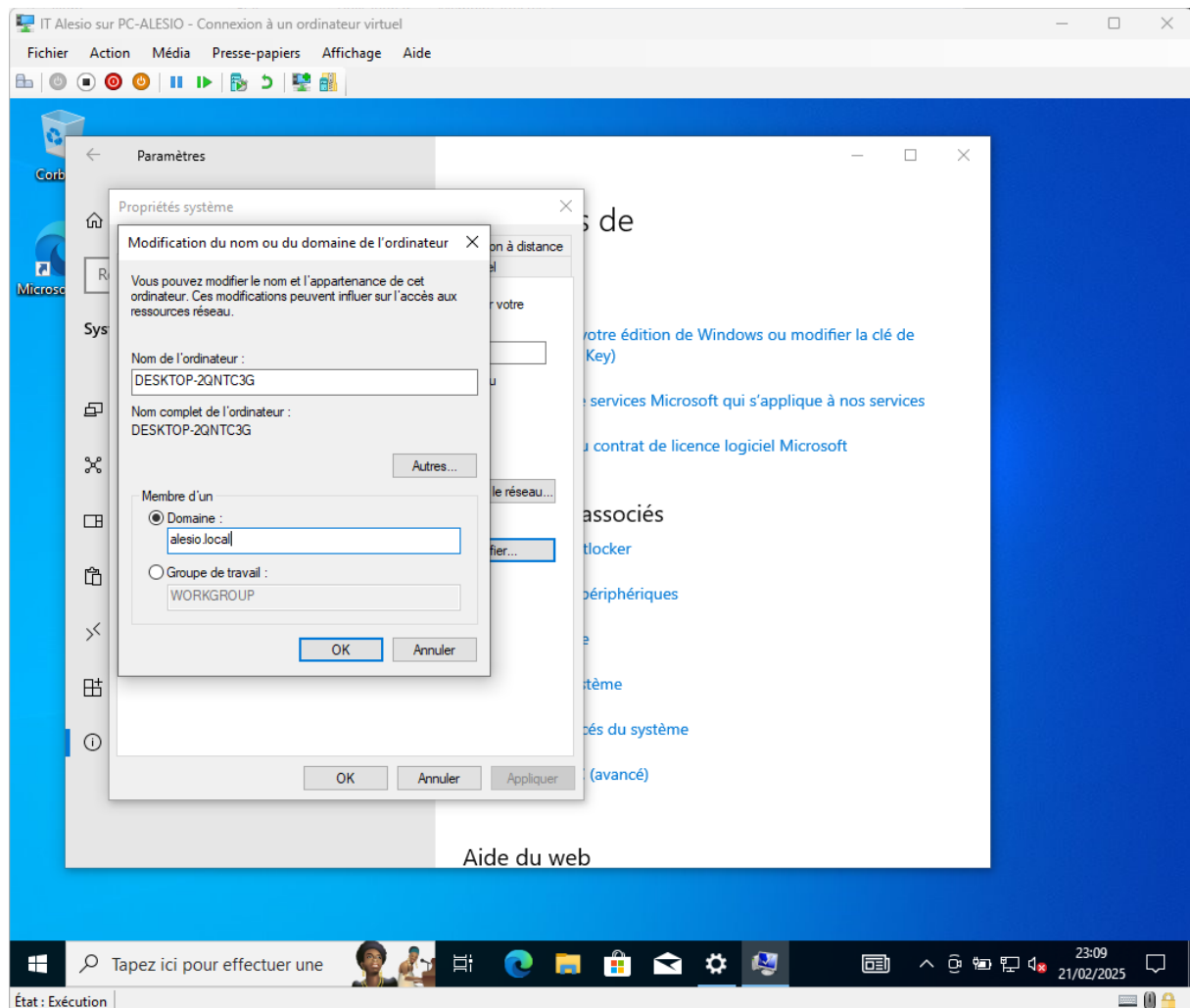


Définir les informations de connexion de l'utilisateur et confirmer la création.

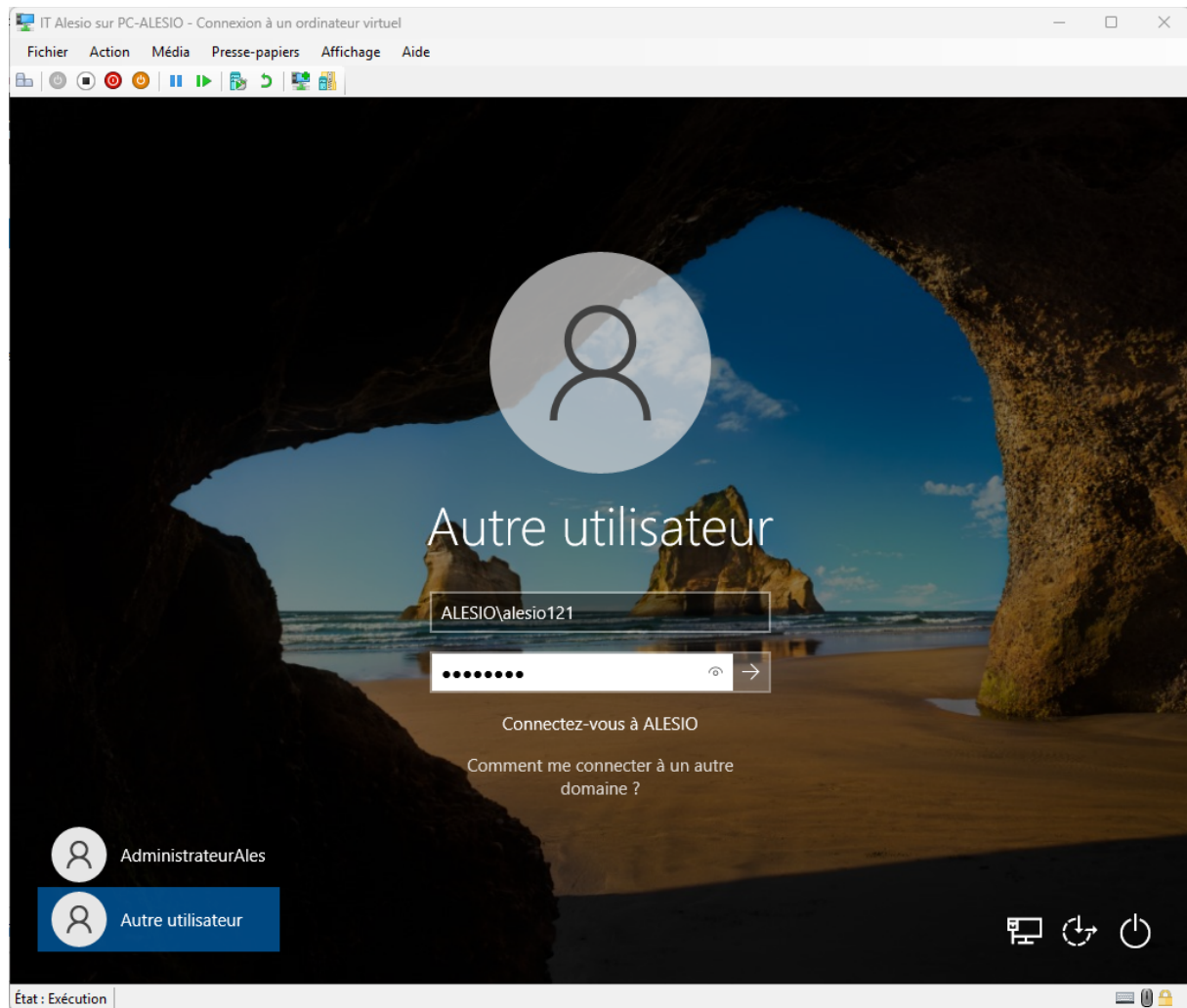


Après avoir créé l'utilisateur, on ajoute l'ordinateur au domaine.

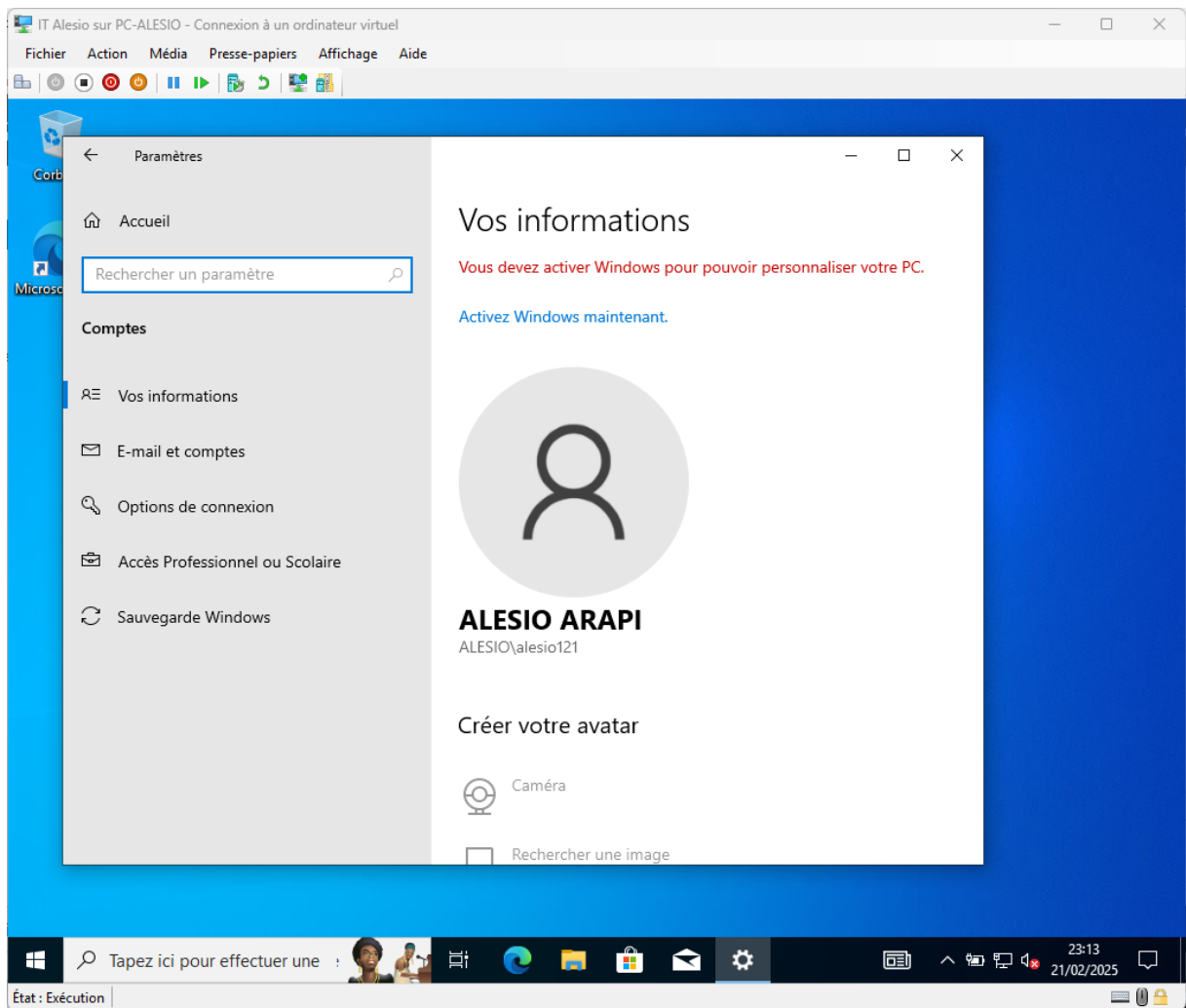
Pour cela, il faut se rendre dans les paramètres système de l'ordinateur, cliquer sur « Domaine », puis ajouter le nom de notre domaine : alesio.local.



Une fois les informations confirmées, on peut déconnecter cet utilisateur et ajouter l'utilisateur du domaine.

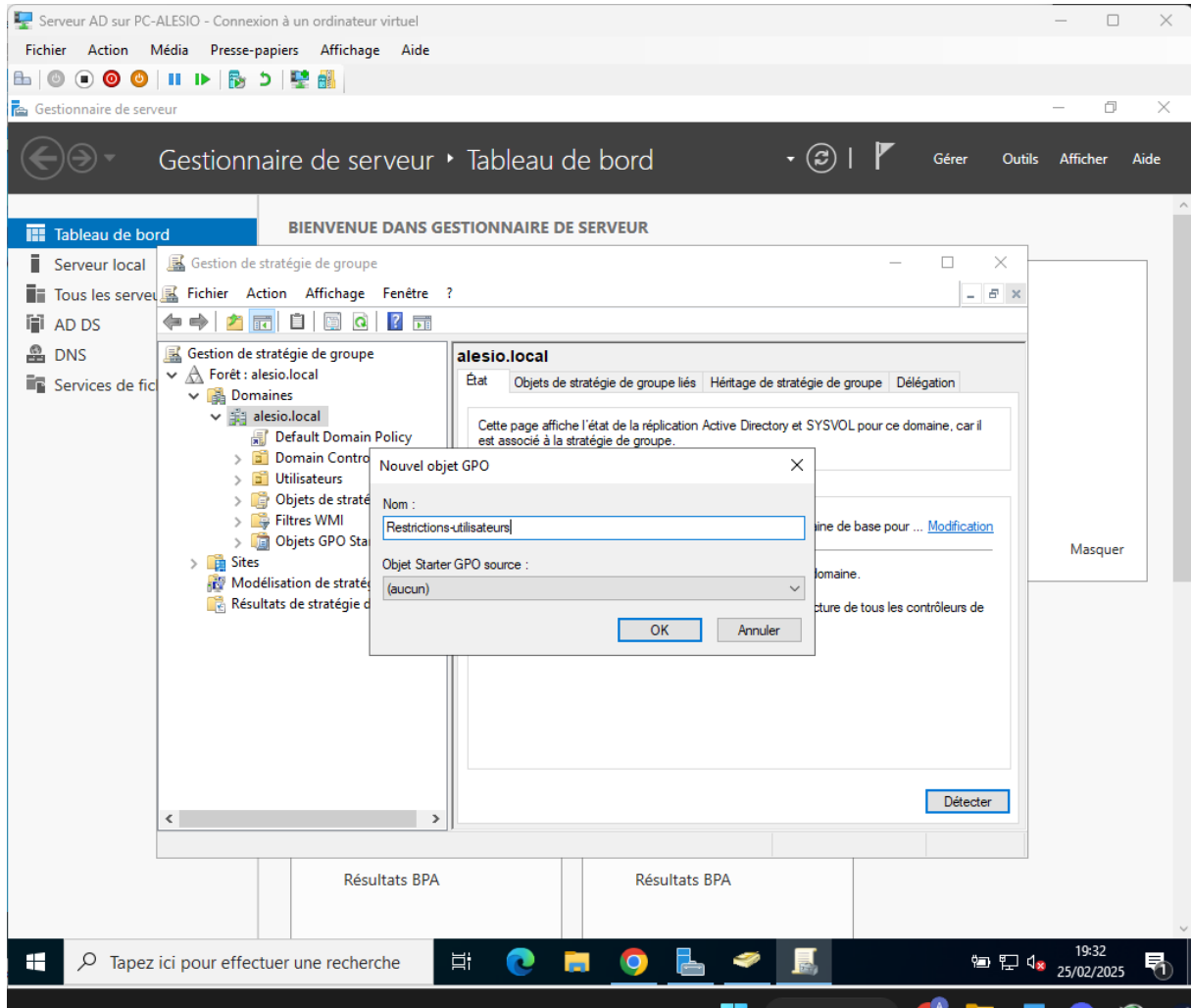


Puis, on peut voir dans les paramètres que le PC a bien rejoint le domaine.

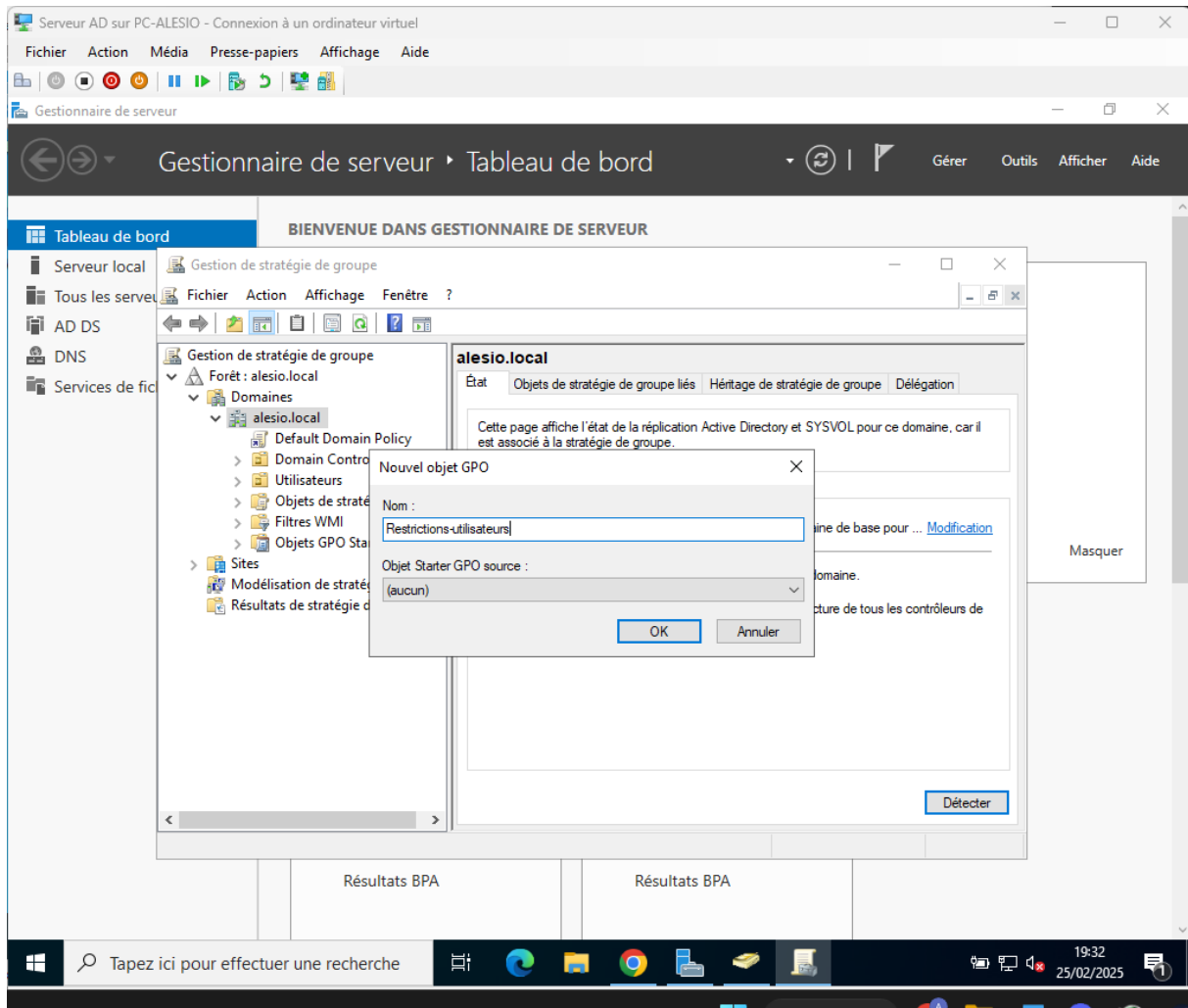


## Création de la stratégie de restriction

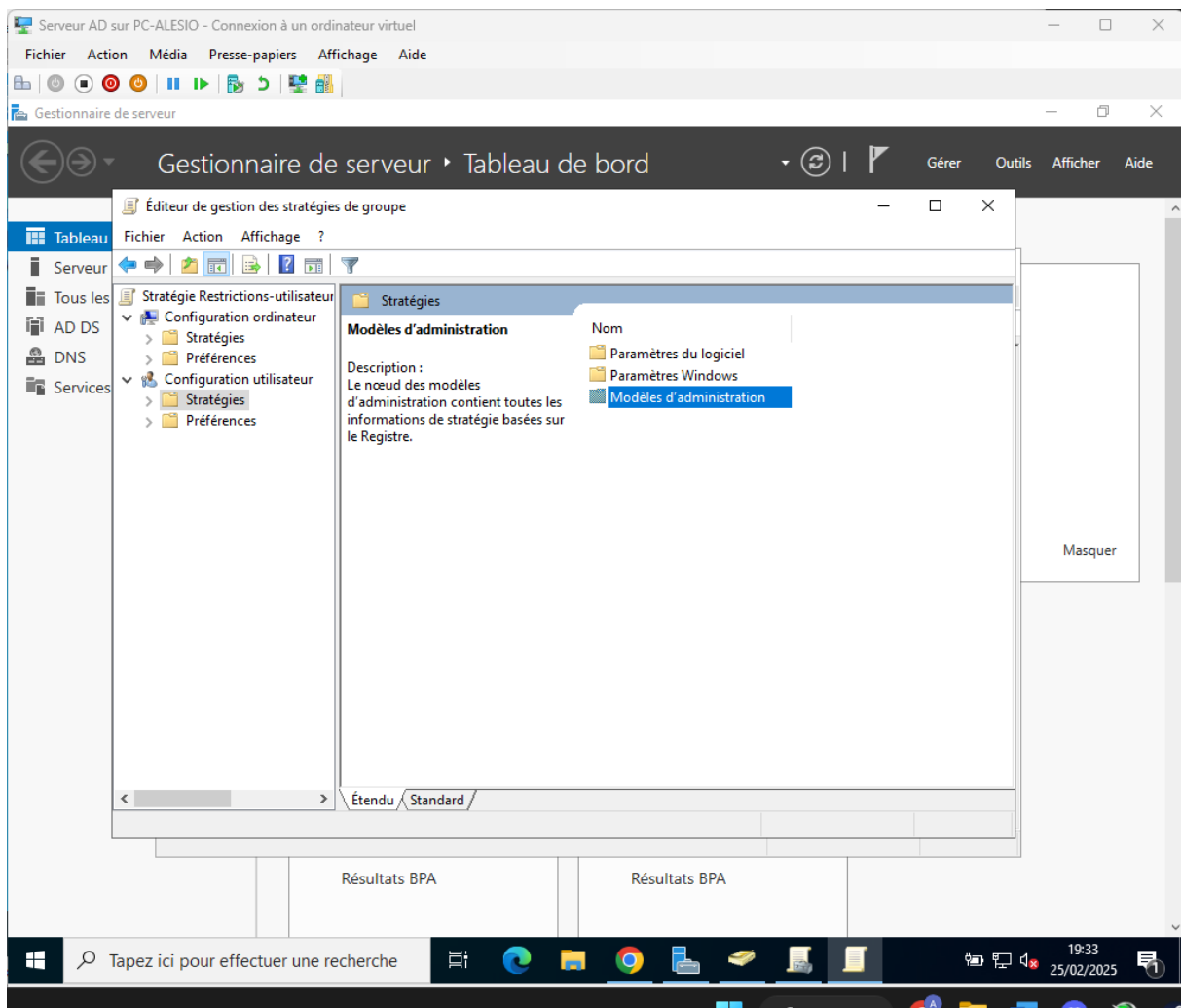
Pour créer une stratégie de groupe, je me rends dans « Gestion de la stratégie de groupe » et je crée une nouvelle GPO.



Ensuite, on peut entrer à l'intérieur de la stratégie et la modifier.  
Dans mon cas, je vais bloquer l'accès au panneau de configuration. Pour cela, il faut aller dans « Configuration utilisateur », puis cliquer sur « Stratégie ».

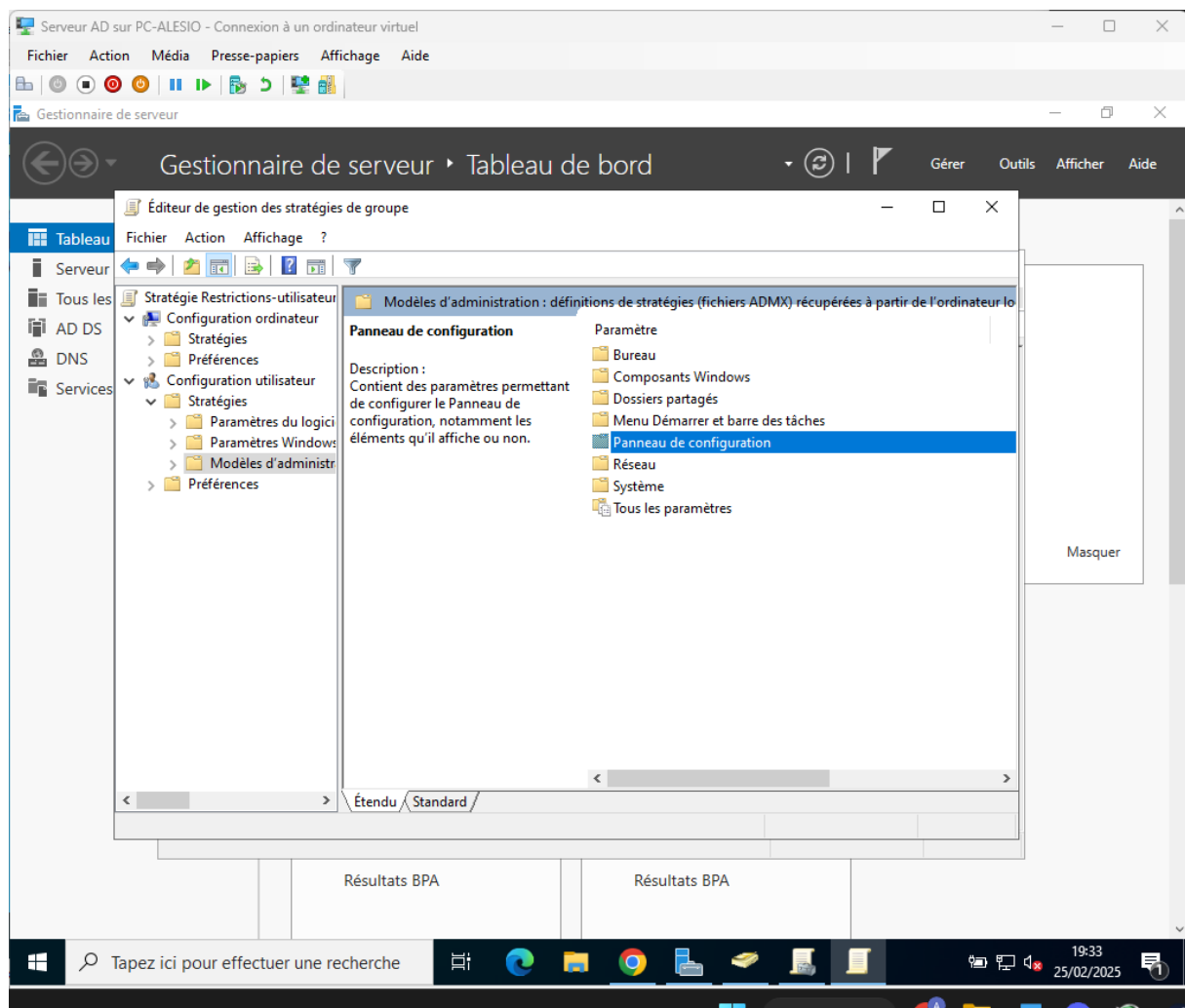


Ensuite, on clique sur modèle d'administration.

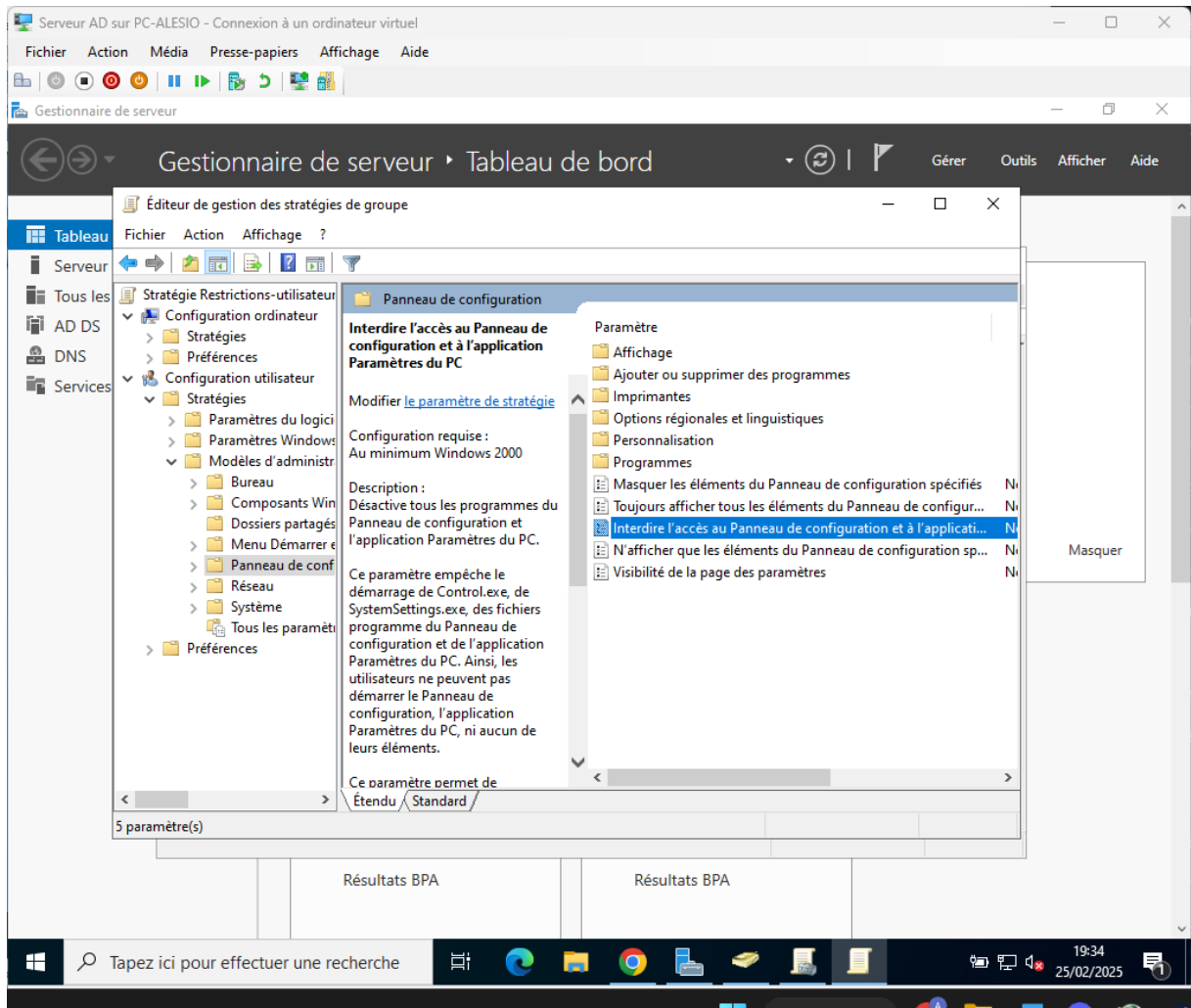




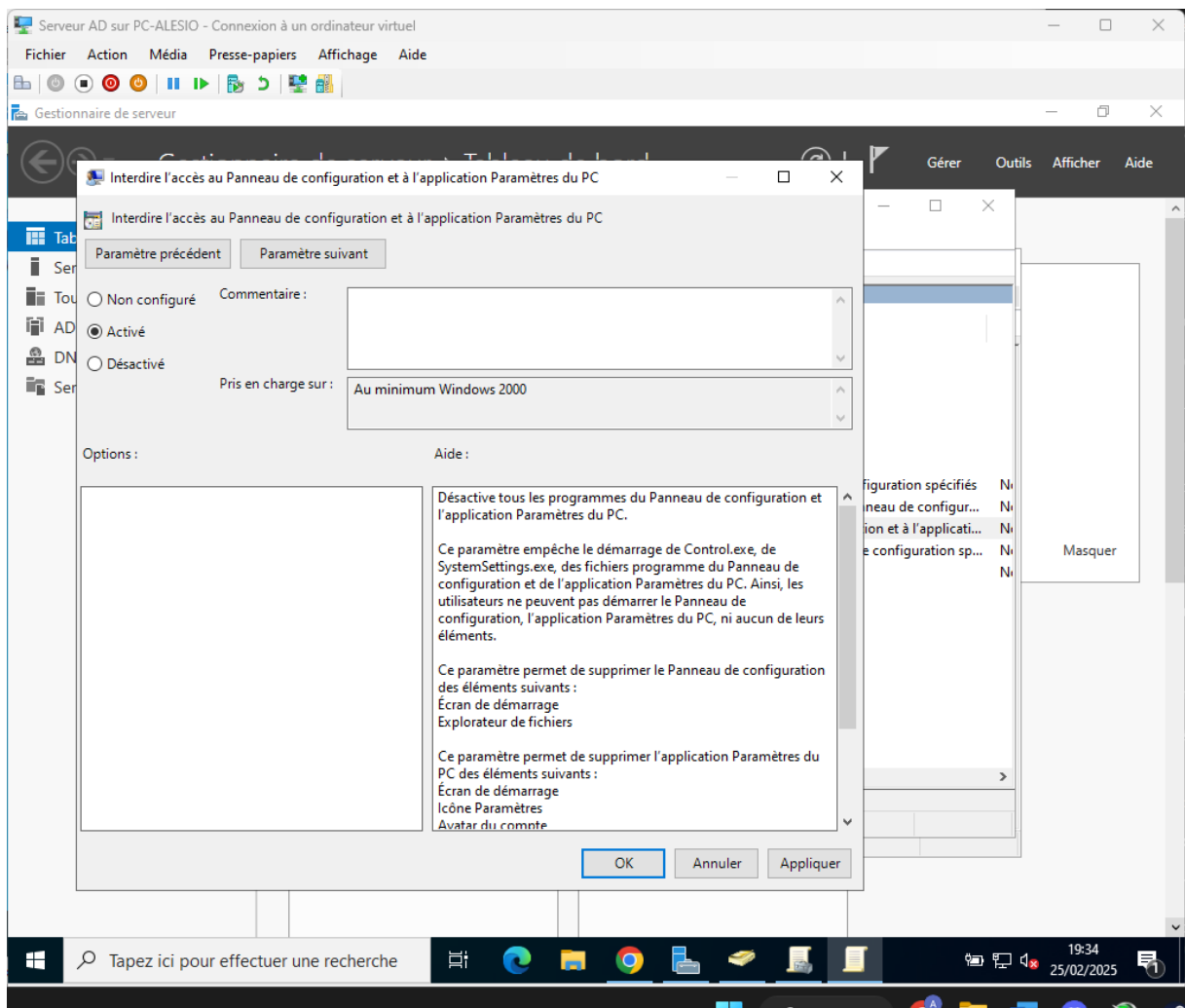
Puis, on sélectionne « Panneau de configuration ».



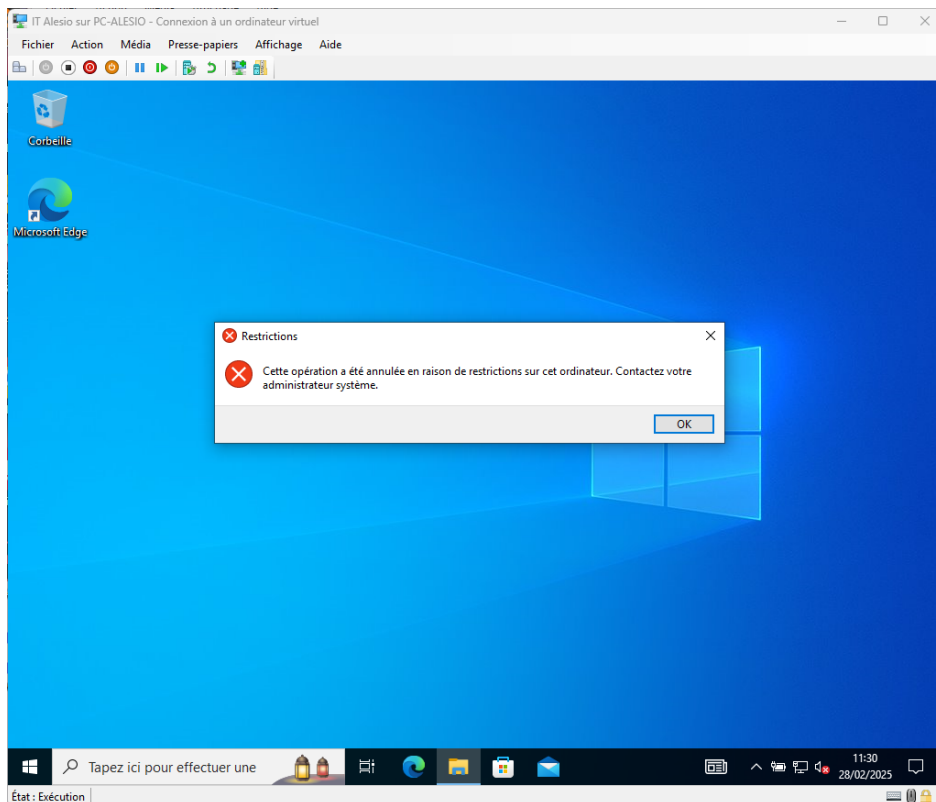
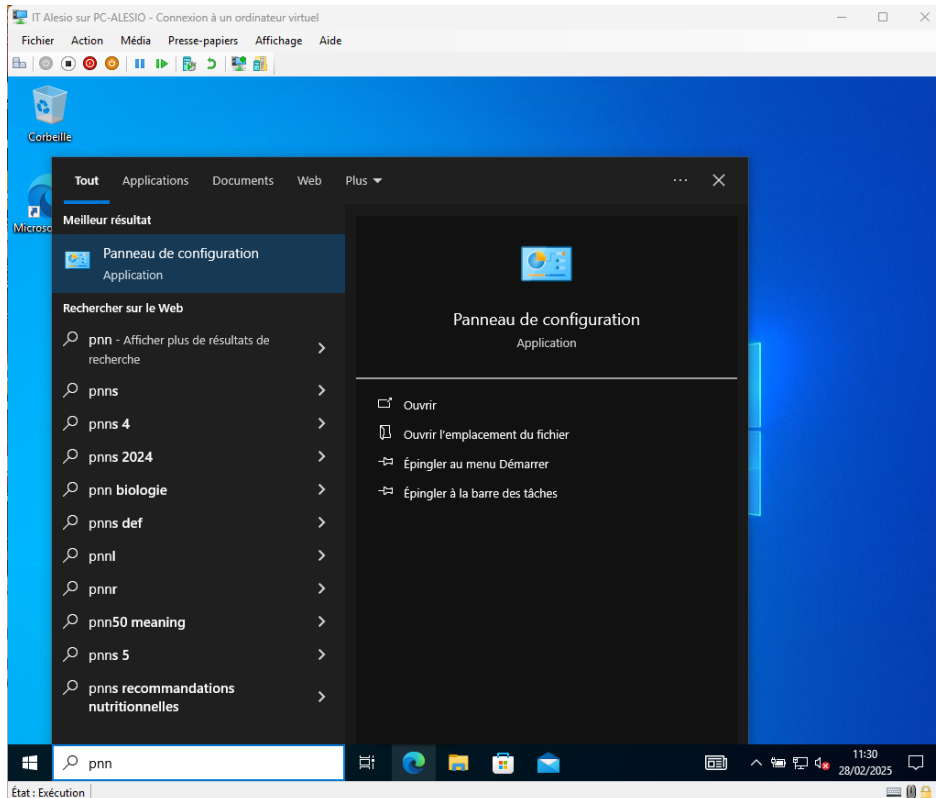
Une fois à l'intérieur, il faut aller dans « Interdire l'accès au Panneau de configuration ».



Et sélectionner « Activé ».



Et voilà ! Maintenant, lorsqu'on essaie d'accéder au Panneau de configuration depuis le poste utilisateur, ce message s'affiche.



## **Conclusion**

Les stratégies de groupe (GPO) sont très utiles pour gérer facilement plusieurs ordinateurs et utilisateurs. Elles permettent par exemple d'installer des logiciels, bloquer certaines fonctions ou appliquer des règles automatiquement. C'est un vrai gain de temps pour les administrateurs, tout en gardant un bon contrôle sur le réseau.