04/03/2025

Compte rendu

Active Directory

Amine LAOUAR

ECORIS

TABLE DES MATIERES

INTRODUCTION

L’objectif de ce TP est de se familiariser avec l’annuaire LDAP via Active Directory et d’administrer un environnement Windows en créant une infrastructure complète. L’ensemble des configurations et tests réalisés permettront de simuler un environnement professionnel structuré et sécurisé.

PREREQUIS

Avant de commencer, il est nécessaire de disposer des éléments suivants :

- Trois machines virtuelles sous Windows (1 serveur et 2 postes clients)
- VirtualBox avec réseau privé configuré
- Une adresse IP fixe pour le serveur
- Installation des add-ons invités pour une compatibilité optimale

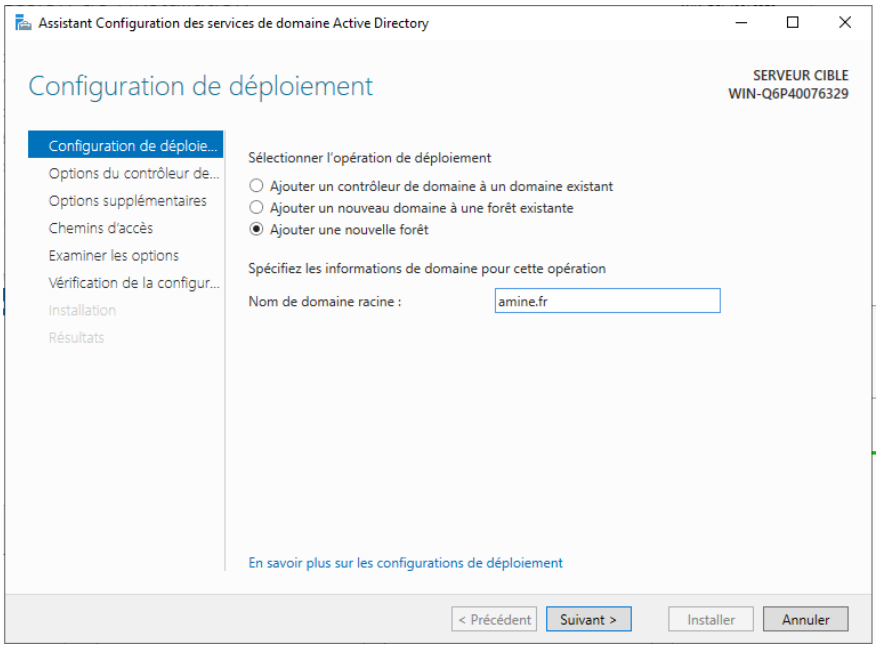
CONFIGURATION DE L'ACTIVE DIRECTORY

Objectif

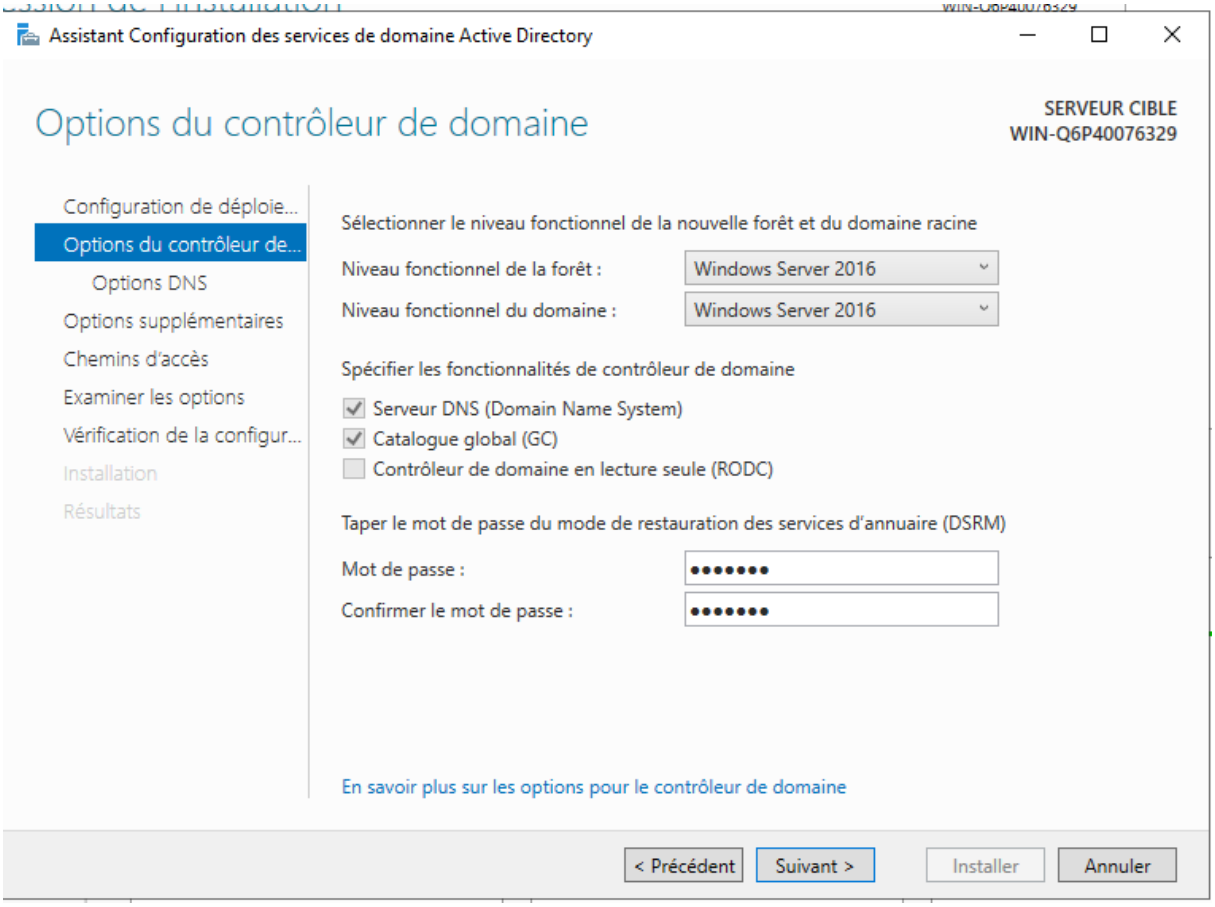
Mettre en place les services essentiels au bon fonctionnement d'Active Directory.

Dans le Gestionnaire de serveur, cliquez sur la notification et sélectionnez Promouvoir ce serveur en contrôleur de domaine.

Choisissez Ajouter une nouvelle forêt, puis saisissez le nom de domaine

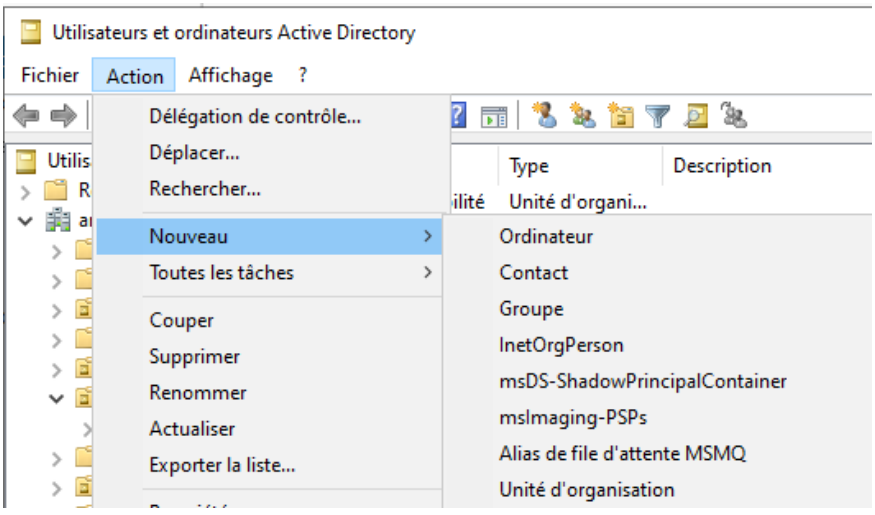


Définissez un mot de passe pour le mode de récupération des services d'annuaire.



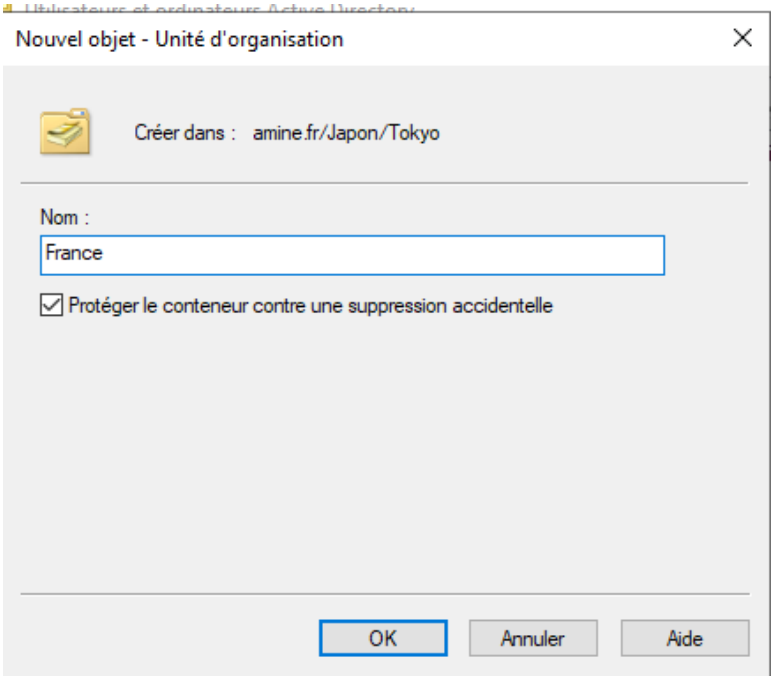
Cliquez sur Suivant jusqu'à Installer. Le serveur redémarrera automatiquement après l'installation.

CREATION DES UNITES ORGANISATIONNELLES (OU)

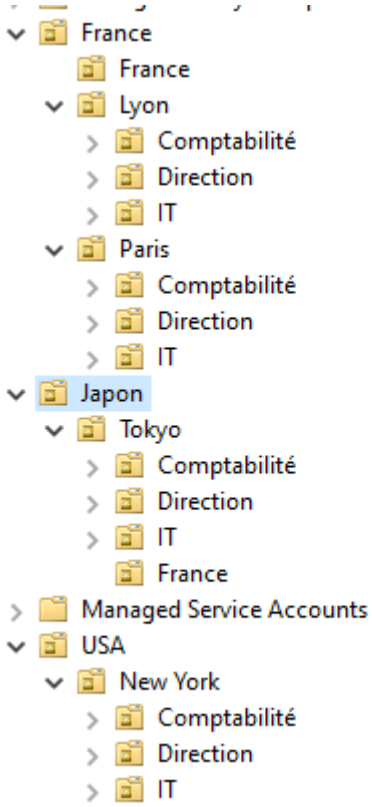


Faites un clic droit sur le nom de domaine, puis sélectionnez Nouveau → Unité d'organisation

Saisissez le nom de l’OU (ex: France, USA, Japon) et validez avec OK



Créez les OU internes : Direction, Comptabilité, IT sous chaque sous-OU correspondante

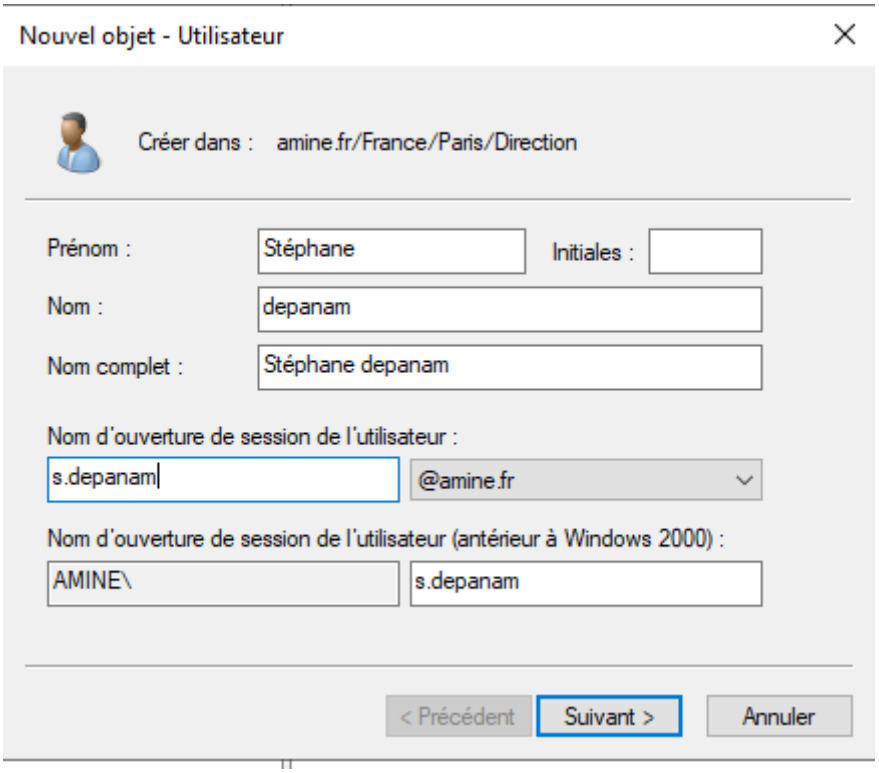


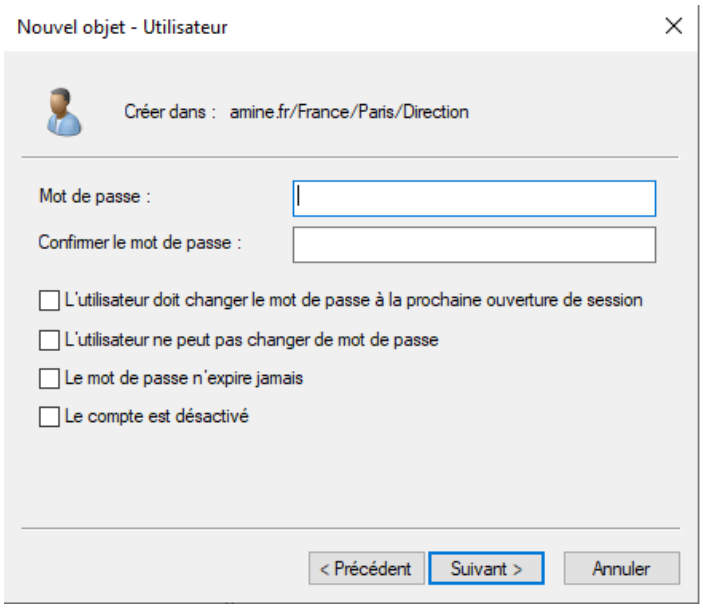
CREATION DES UTILISATEURS

Dans Utilisateurs et ordinateurs Active Directory, accédez à l'OU où vous souhaitez créer un utilisateur.

Faites un clic droit sur l'OU et sélectionnez Nouveau → Utilisateur.

Renseignez le prénom, nom et nom de connexion de l'utilisateur.





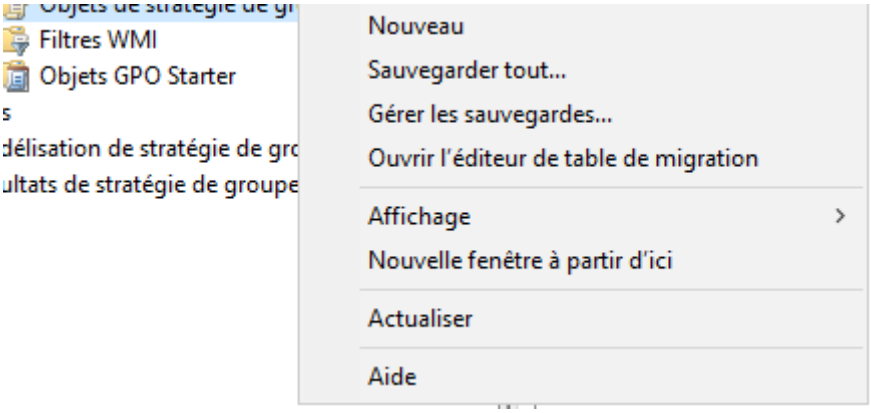
Définissez un mot de passe et configurez les options souhaitées (ex: l'utilisateur doit changer son mot de passe à la première connexion)

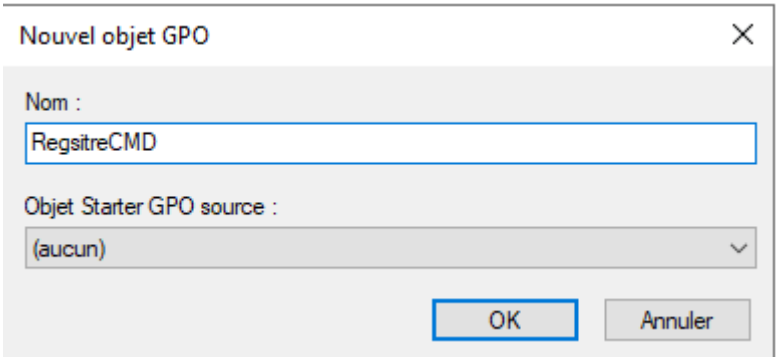
Cliquez sur Suivant, puis sur Terminer.

Répétez l'opération pour chaque utilisateur dans les OU Direction, Comptabilité et IT.

CREATION GPO

Créer un nouveau GPO et le lier aux OU Direction et Comptabilité

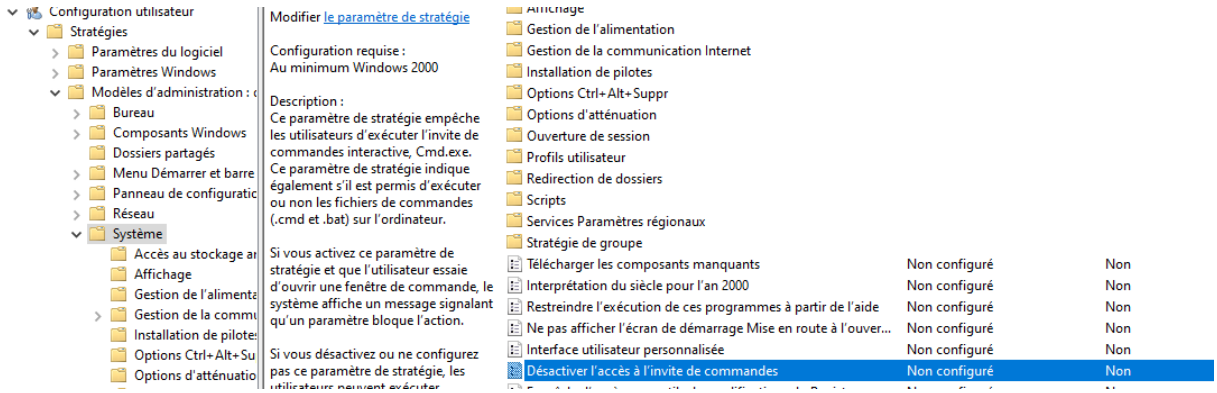


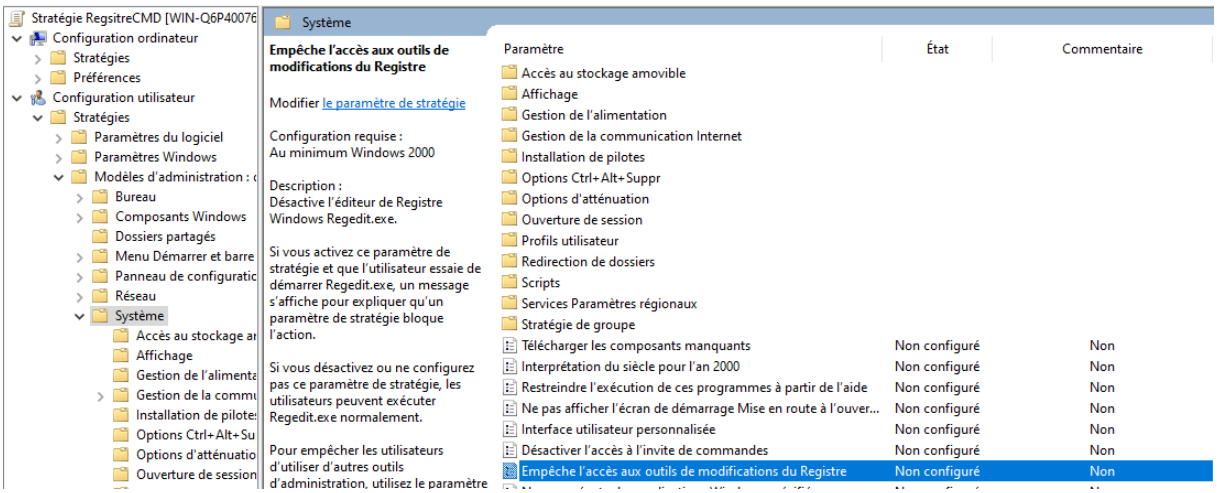


EMPECHER L'ACCES A L'INVITE DE COMMANDES (CMD) ET A L'EDITEUR DE REGISTRE

Modifier le GPO et aller dans :
Configuration utilisateur → Modèles d'administration → Système

Activer les stratégies :
Empêcher l'accès à l'invite de commandes → Activé
Empêcher l'accès à l'éditeur du Registre → Activé

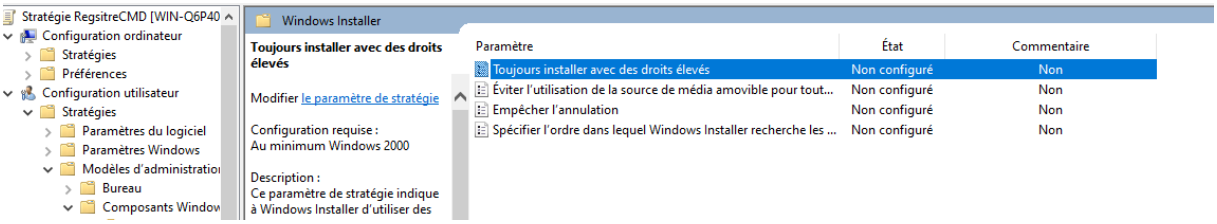




BLOQUER L'INSTALLATION DE LOGICIELS

CONFIGURATION UTILISATEUR → MODELES D'ADMINISTRATION → Composants Windows/Windows Installer

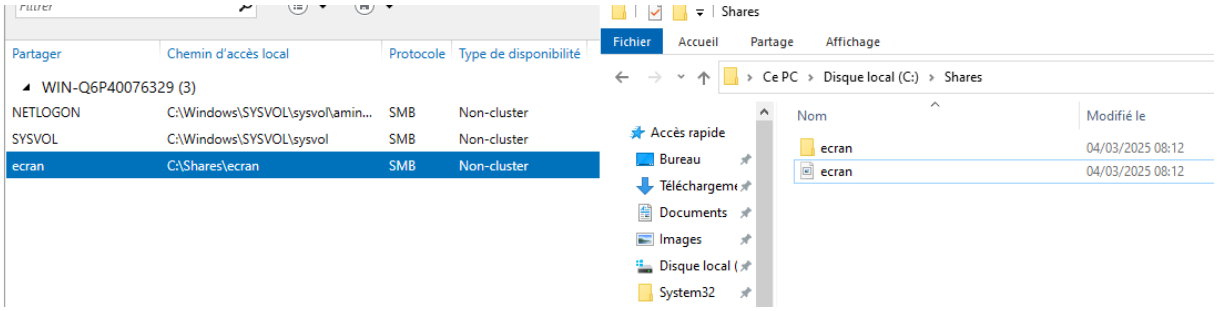
ACTIVER LA STRATEGIE : TOUJOURS INSTALLER AVEC DES DROITS ELEVES



FOND D'ECRAN

PREPARER L'IMAGE DU FOND D'ECRAN

Créer une image (ex: compta.jpg) avec le fond d'écran souhaité.



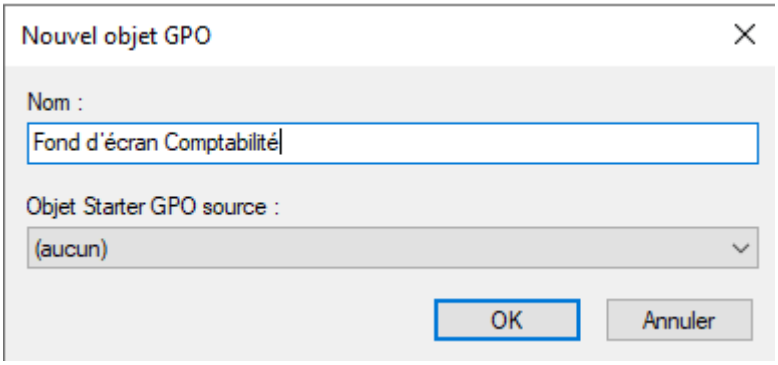
Stocker l'image sur un dossier partagé accessible aux utilisateurs :

Ex : \\SRVAD\Share\ecran.jpg

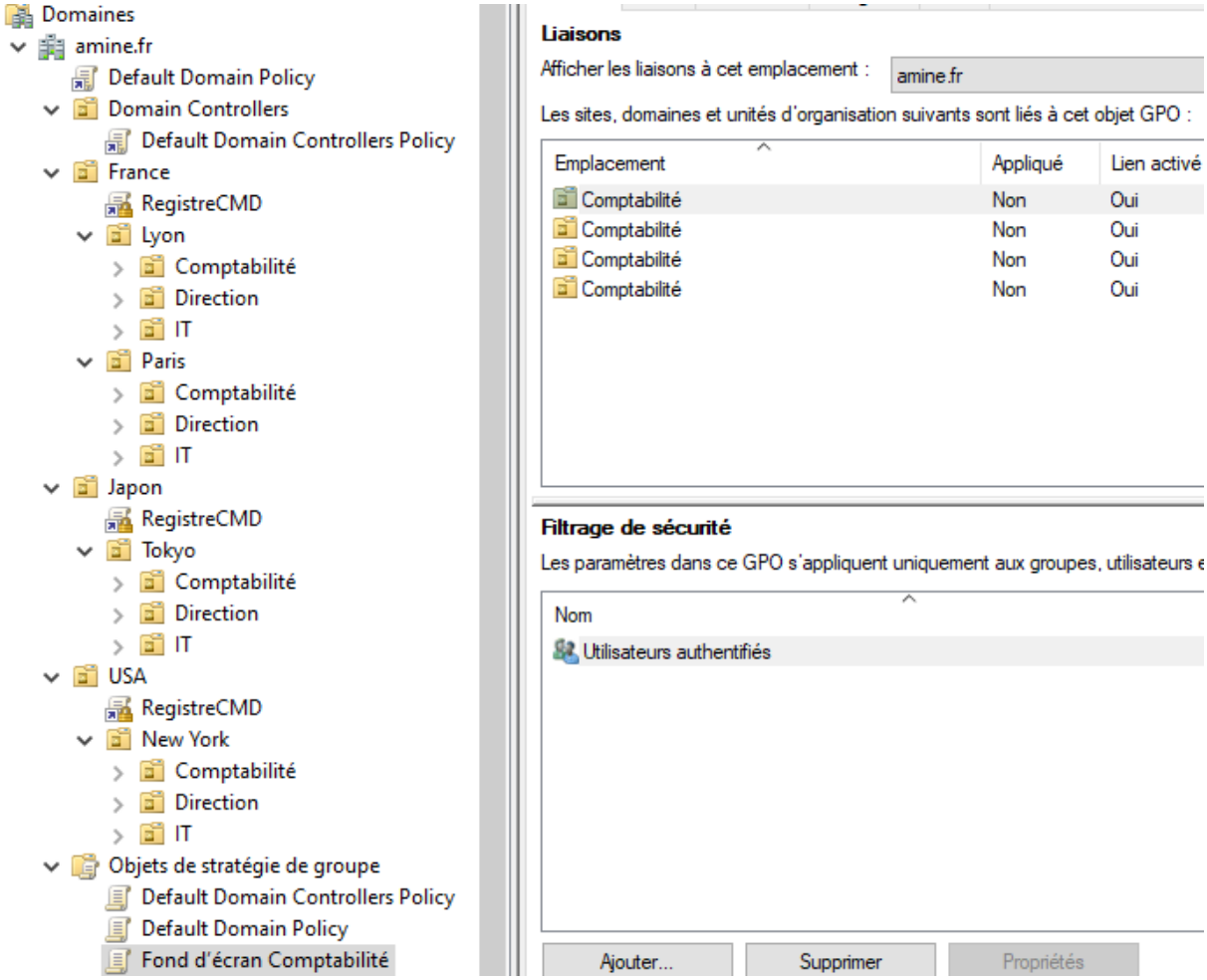
CREER ET APPLIQUER UNE GPO POUR IMPOSER LE FOND D'ECRAN

Ouvrir la **Console de gestion des stratégies de groupe (GPMC**

Créer un nouveau GPO nommé "Fond d'écran Comptabilité".



Lier ce GPO à l’OU Comptabilité.

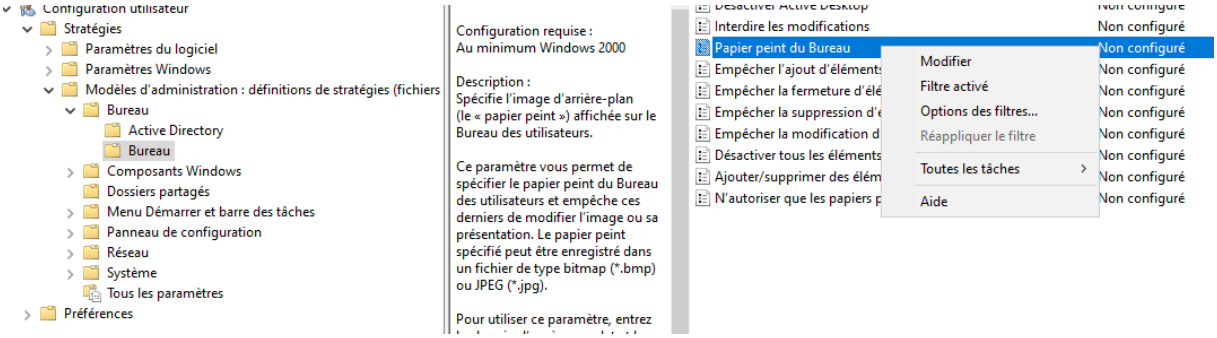


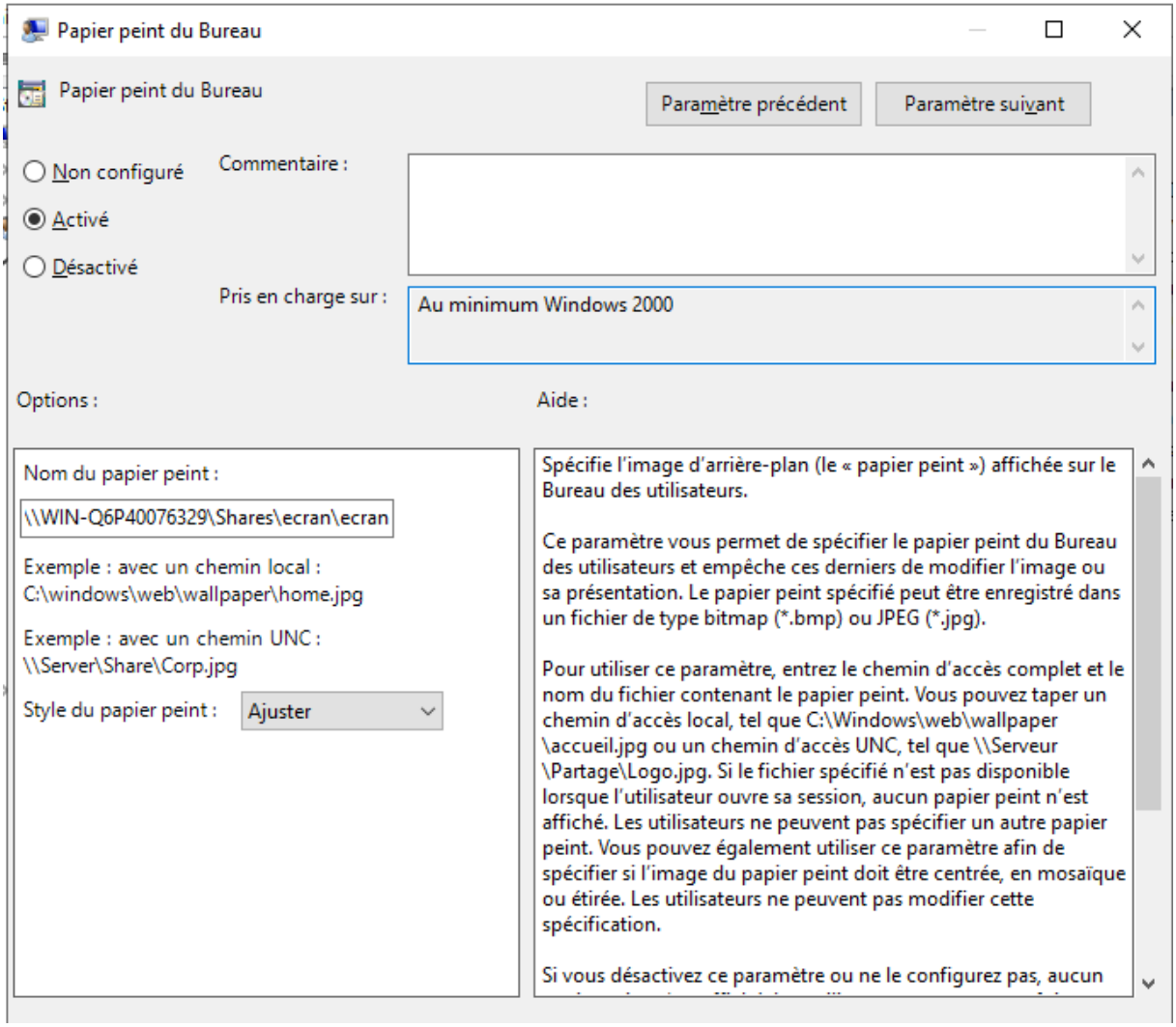
Modifier le GPO et aller dans :

Configuration utilisateur → Stratégies → Modèles d'administration → Bureau → Active Desktop

Activer la stratégie :

"Fond d’écran Active Desktop" → Activé





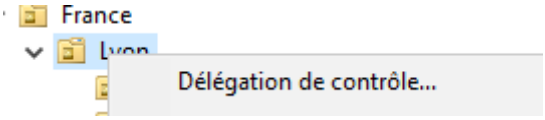
DELEGATION DES DROITS D'ADMINISTRATION SUR LES OU

DELEGATION DES DROITS AUX ADMINISTRATEURS LOCAUX

Ouvrir la console "Utilisateurs et ordinateurs Active Directory"

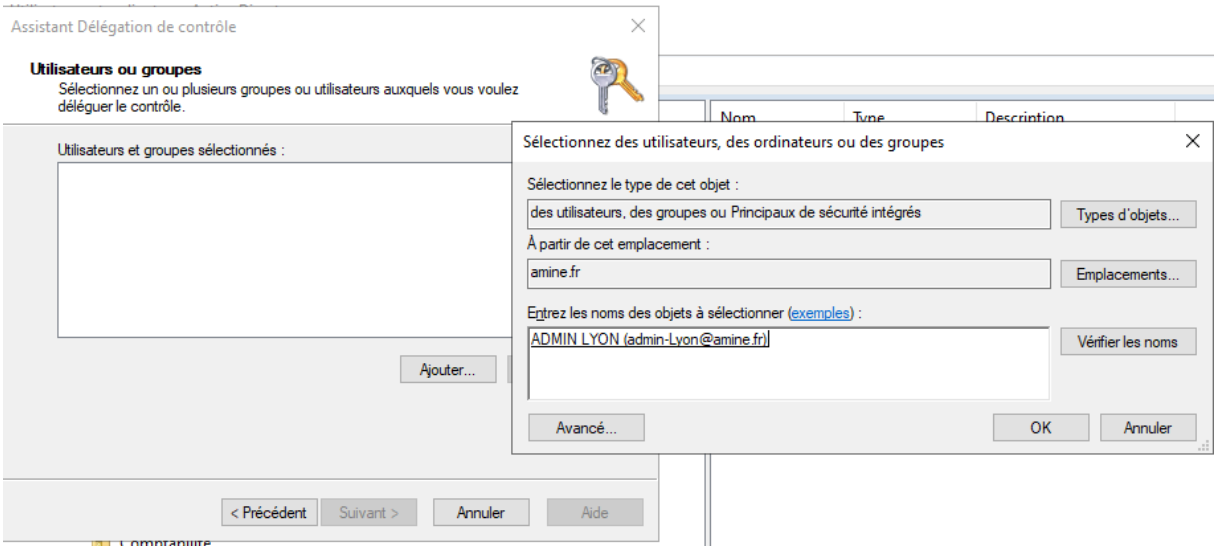
Faire un clic droit sur l'OU du site concerné (ex: France/Lyon).

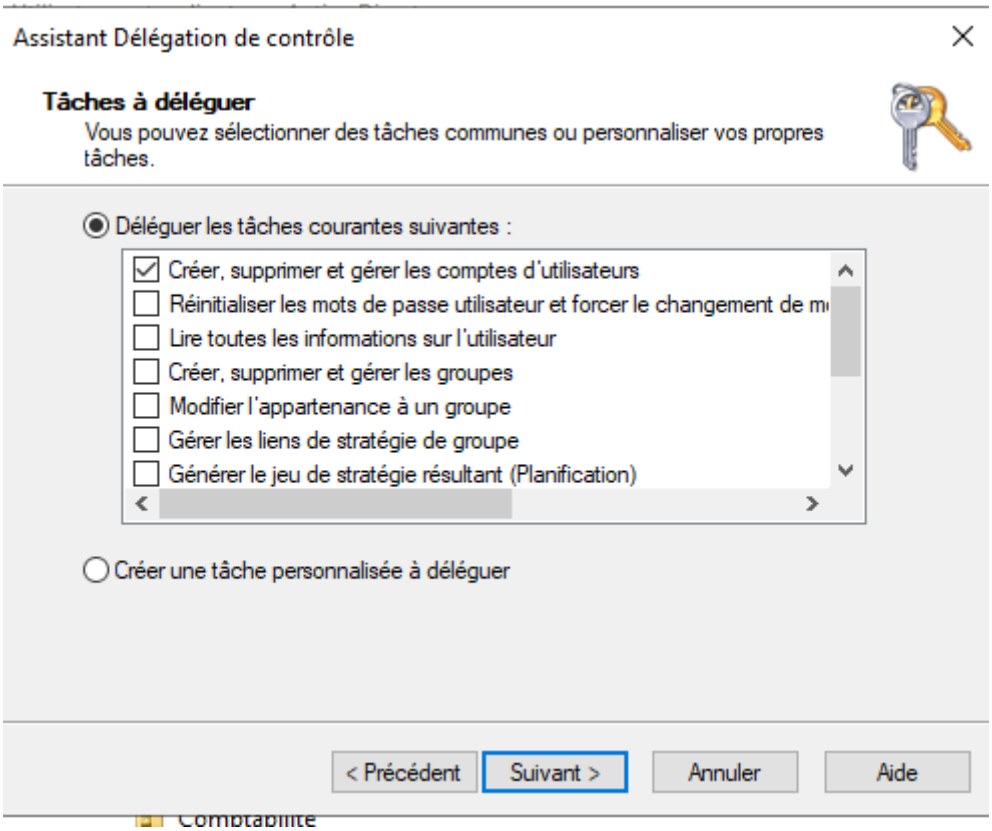
Cliquer sur "Délégation de contrôle".



Ajouter l’utilisateur ou le groupe d’administrateurs locaux correspondant à ce site (ex: IT_Lyon).

Suivre l’assistant, puis sélectionner "Créer, modifier et supprimer des comptes utilisateur".



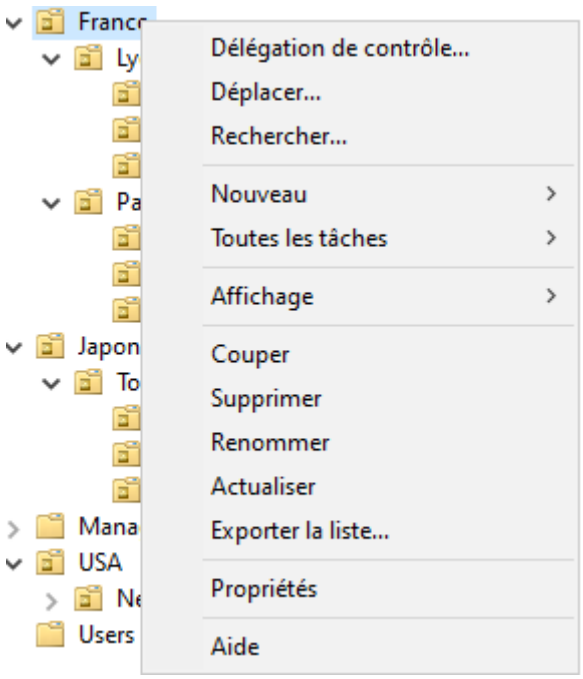


Terminer l’assistant, puis tester avec un compte admin local pour vérifier qu'il peut gérer uniquement son OU.

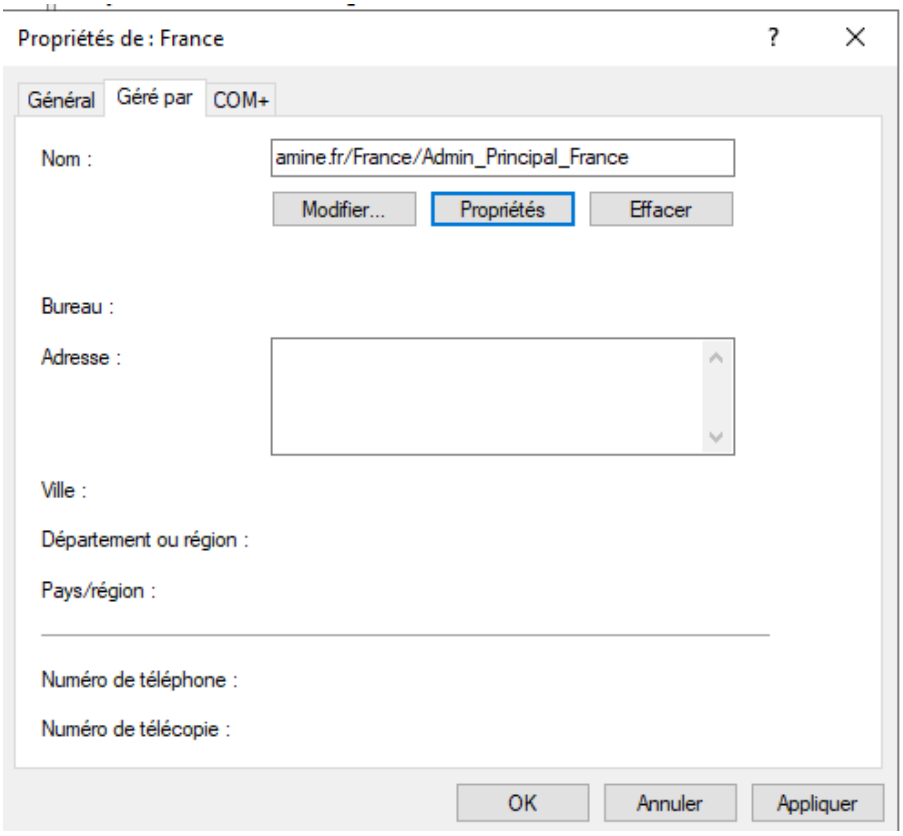
ACCORDER UN ACCES TOTAL AUX ADMINISTRATEURS PRINCIPAUX

Ouvrir la console "Utilisateurs et ordinateurs Active Directory".

Faire un clic droit sur l’OU principale (ex: France).



Aller dans l'onglet "Sécurité", puis Ajouter les administrateurs principaux (ex: Admin_Principal_France).



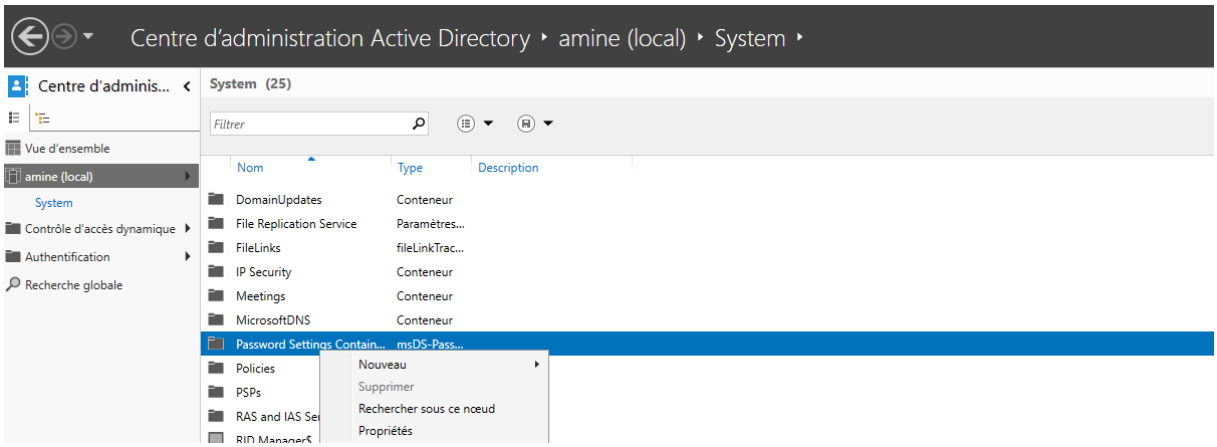
Appliquer et fermer.

CONFIGURATION DES POLITIQUES DE MOTS DE PASSE ET RESTRICTIONS D'ACCES AUX POSTES

CREATION DE DEUX POLITIQUES DE MOTS DE PASSE

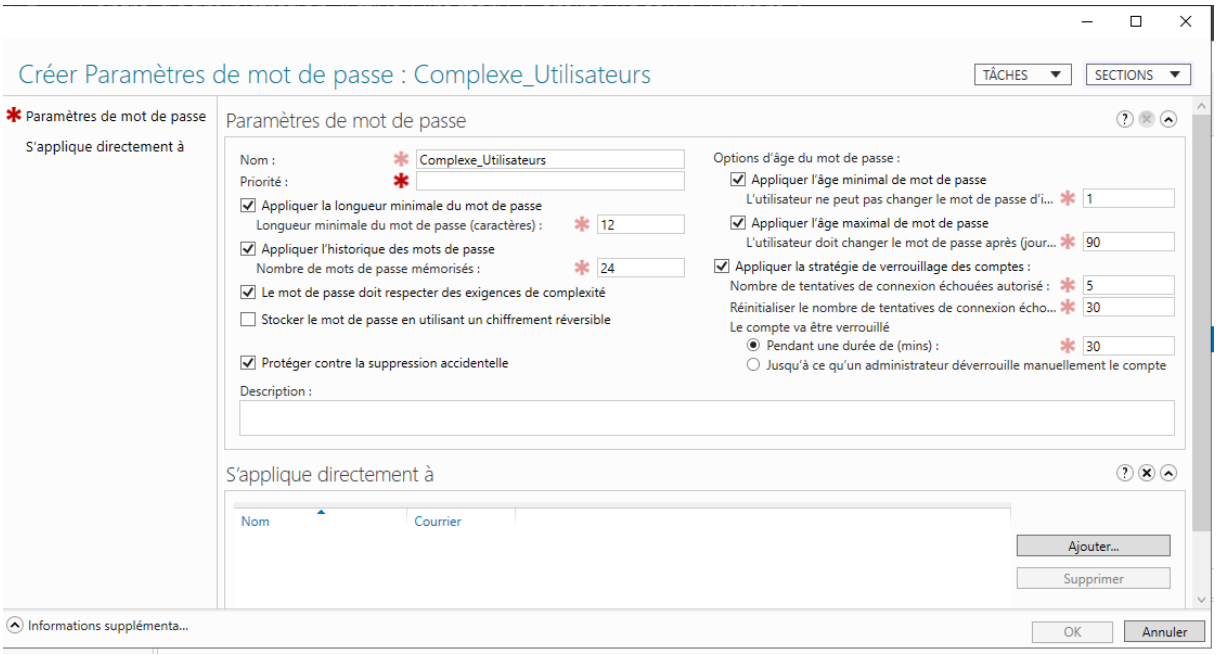
ACTIVER LES FGPP DANS ACTIVE DIRECTORY

1. **Ouvrir la console "Active Directory Administrative Center"** (dsac.msc).
2. Dans le panneau de gauche, aller dans **Système → Password Settings Container**.

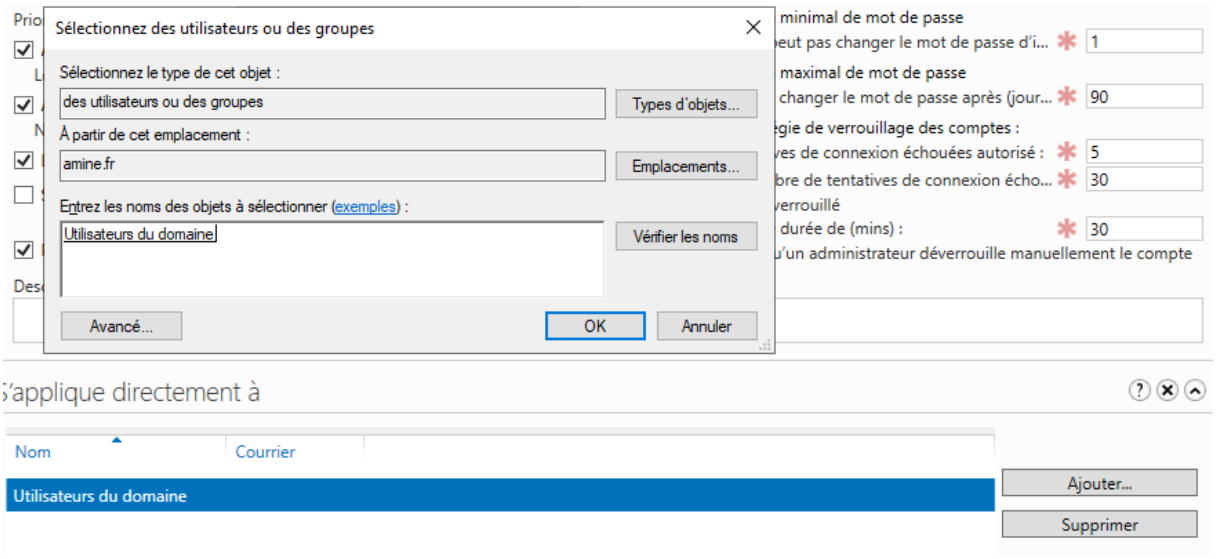


CREER LA POLITIQUE DE MOT DE PASSE COMPLEXE POUR LES UTILISATEURS

1. **Clic droit sur "Password Settings Container" → Nouveau → Paramètres de mot de passe**.
2. Donner un nom explicite, ex: **"Complexe_Utilisateurs"**.
3. Définir les critères :
   - Longueur minimale : **12 caractères**
   - Complexité activée : **Oui**
   - Historique des mots de passe : **24 anciens mots interdits**
   - Expiration : **90 jours**
   - Verrouillage après **5 tentatives**



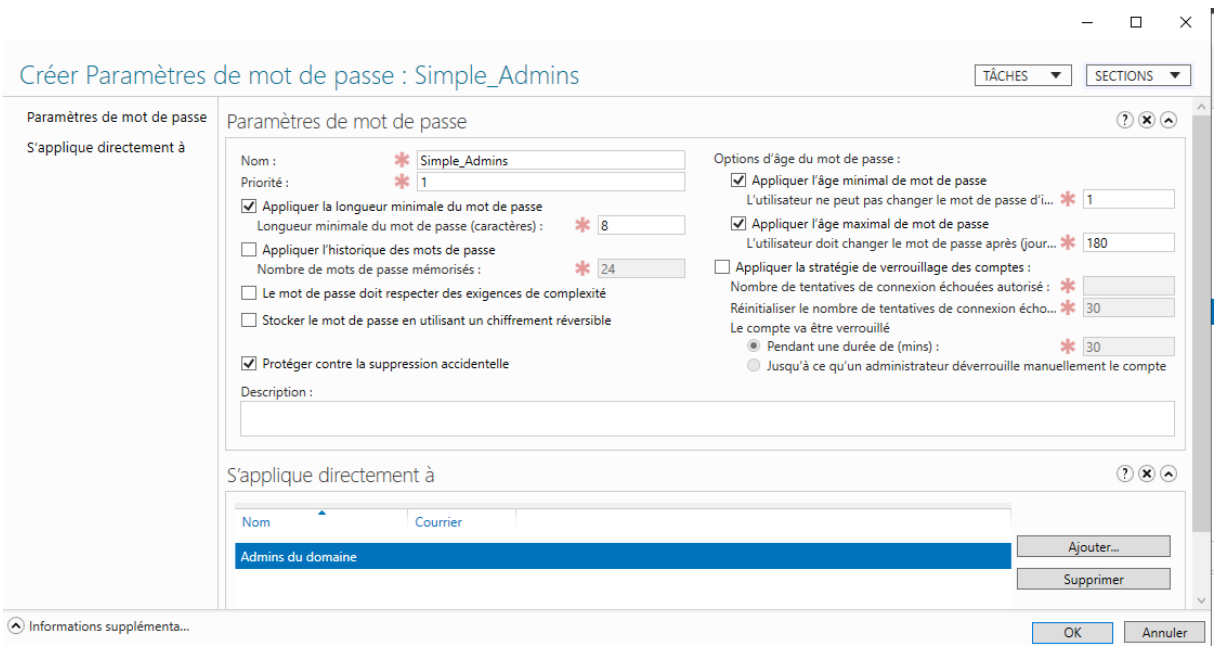
4. Dans **Attributs appliqués à**, ajouter le **groupe des utilisateurs standards** (ex: Utilisateurs_Domaine).



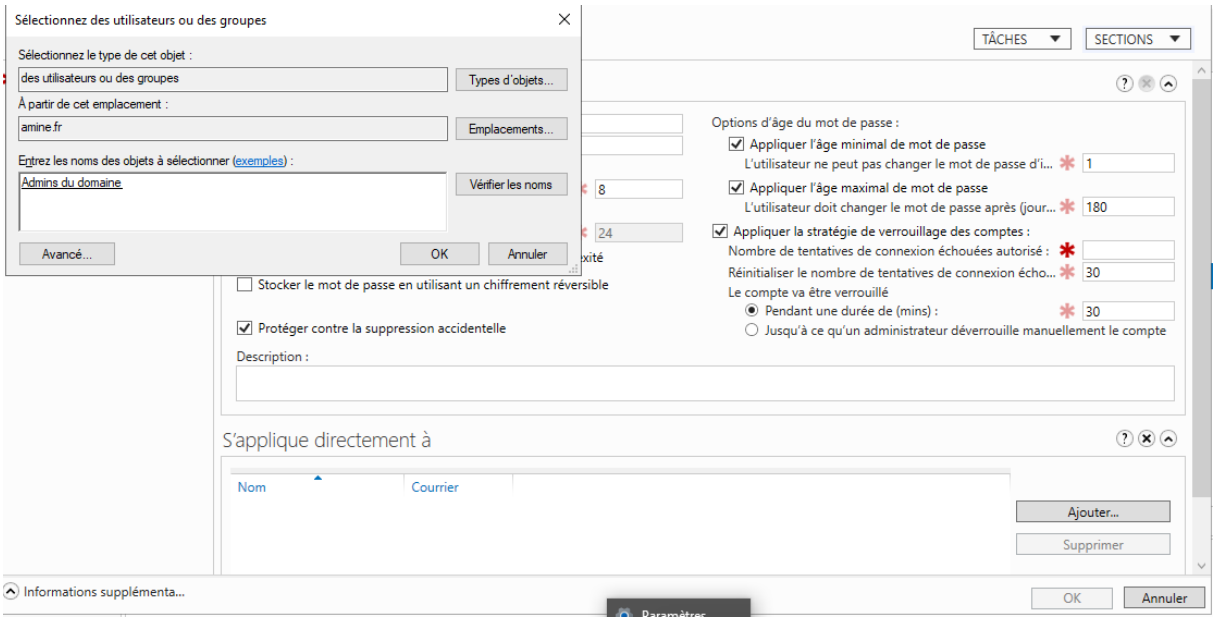
5. **Enregistrer**.

CREER LA POLITIQUE DE MOT DE PASSE SIMPLE POUR LES ADMINS

1. Refaire la procédure précédente avec un autre nom, ex: **"Simple_Admins"**.
2. Paramètres plus souples :
   - Longueur minimale : **8 caractères**
   - Complexité activée : **Non**
   - Expiration : **180 jours**
   - Aucune restriction sur l'historique des mots de passe



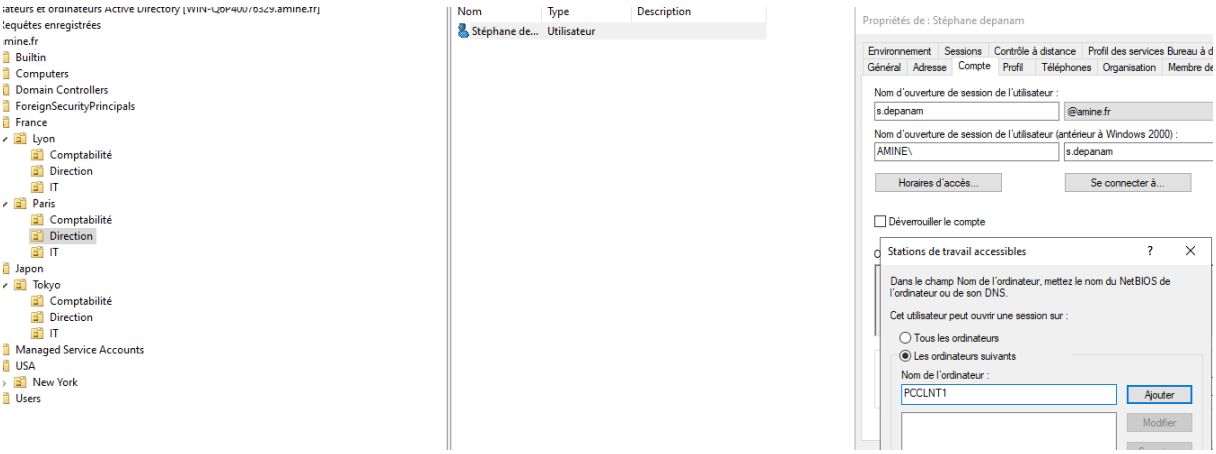
3. Dans **Attributs appliqués à**, ajouter le **groupe des administrateurs** (ex: Admins_Domaine).



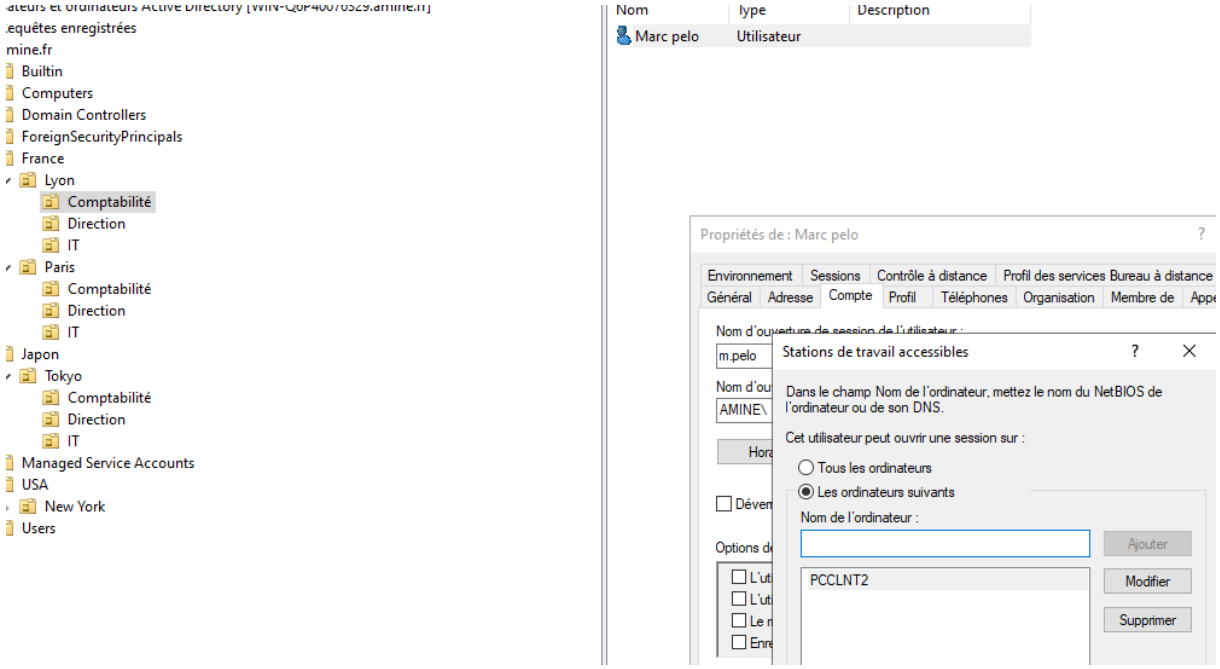
4. **Enregistrer**.

RESTRICTION DES CONNEXIONS POUR DIRECTION ET COMPTABILITE

1. Ouvrir **"Utilisateurs et ordinateurs Active Directory"** (dsa.msc).
2. Sélectionner un utilisateur de l'OU **Direction**.
3. **Ouvrir ses propriétés** → Onglet **Compte** → Bouton **Se connecter à...**.
4. Sélectionner uniquement **PCCLNT1**, puis **Appliquer**.

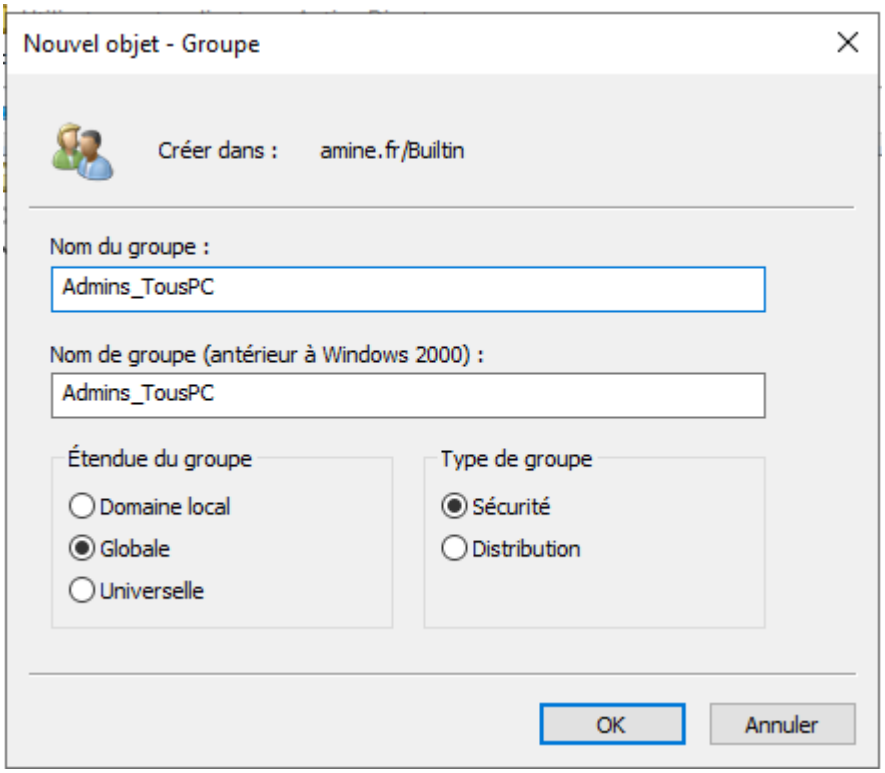


5. Répéter l'opération pour les utilisateurs de **Comptabilité** en leur assignant **PCCLNT2**.

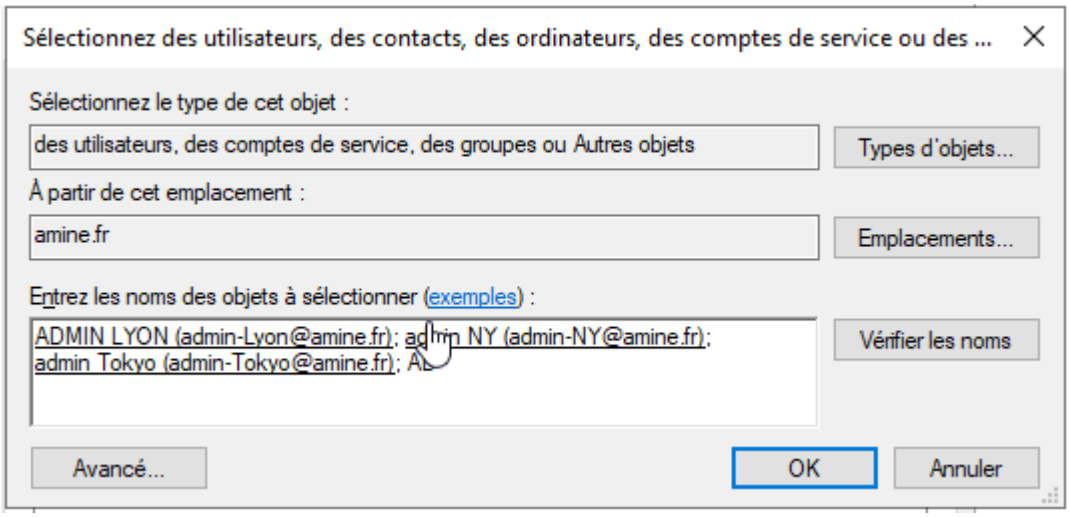


AUTORISER LES ADMINISTRATEURS A SE CONNECTER PARTOUT

1. Créer un **groupe Admins_TousPC**.



2. Ajouter les administrateurs à ce groupe.

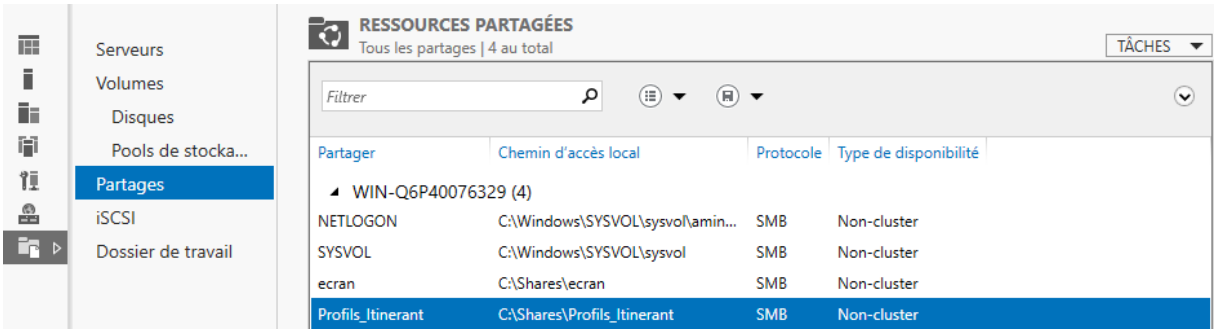


CONFIGURATION DES PROFILS ITINERANTS AVEC RESTRICTIONS D'ACCES

CREATION ET APPLICATION DES PROFILS ITINERANTS

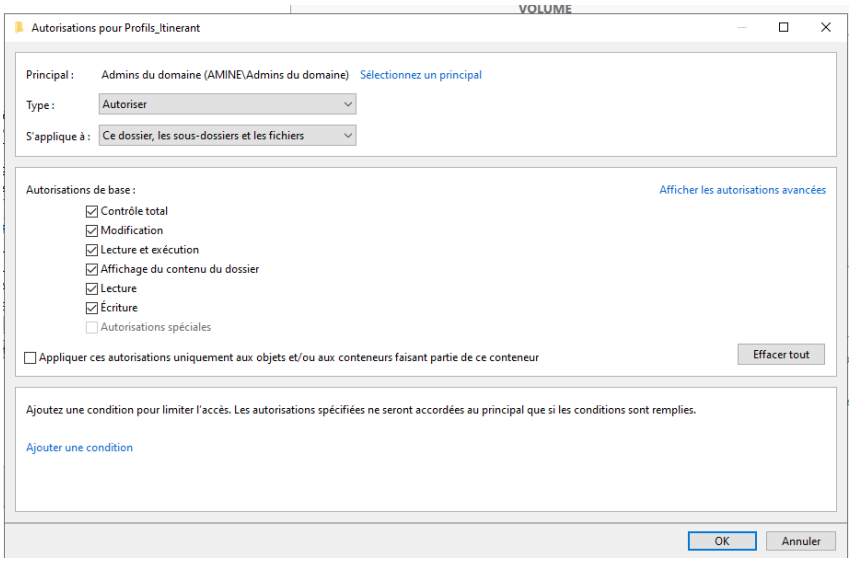
CREATION DU DOSSIER PARTAGE POUR LES PROFILS

Sur le serveur AD, créer un dossier, ex: C:\Profils_Itinerants

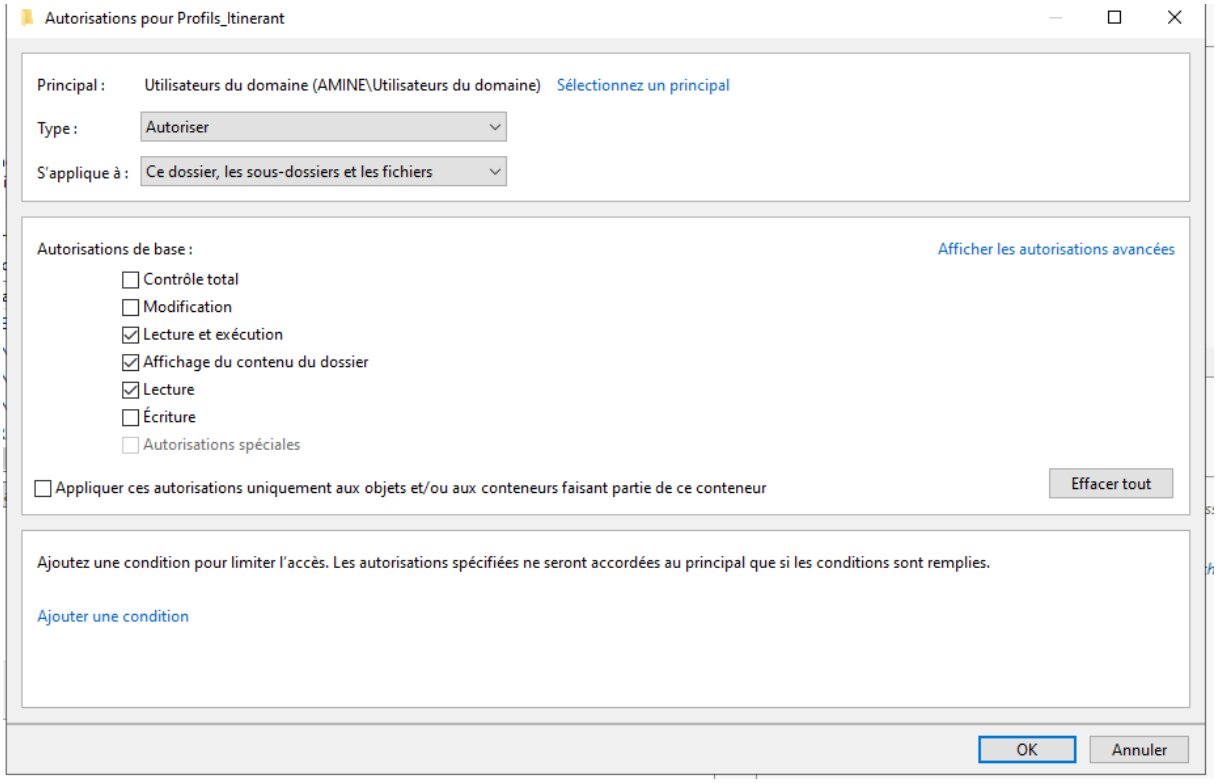


Configurer les permissions NTFS :

Administrateurs du domaine → Contrôle total



Utilisateurs du domaine → Lecture & Écriture



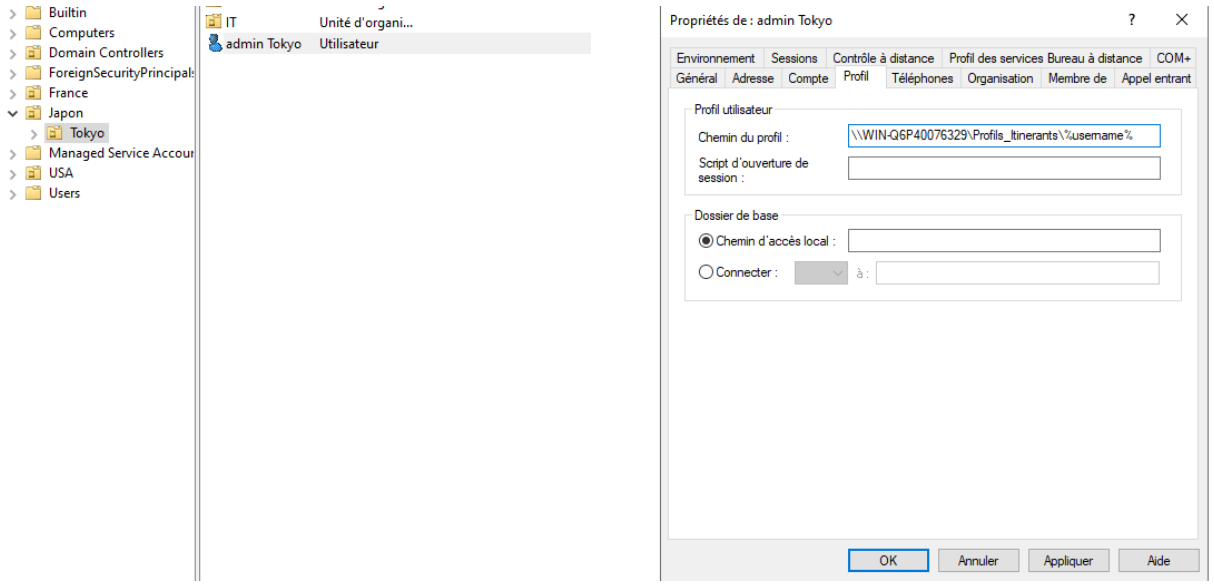
DEFINITION DES PROFILS ITINERANTS DANS ACTIVE DIRECTORY

Ouvrir "Utilisateurs et ordinateurs Active Directory"

Sélectionner un utilisateur, clic droit → Propriétés.

Aller dans l'onglet Profil.

Dans **Chemin du profil**, entrer le chemin UNC avec `%username%`



CONCLUSION

Ce TP a permis de mettre en place un environnement Active Directory structuré avec une gestion efficace des utilisateurs et des ressources. Nous avons configuré une **forêt AD**, créé des **OU organisées**, attribué des **profils itinérants**, appliqué des **restrictions d'accès aux postes**, et mis en place des **GPO pour sécuriser et restreindre les actions des utilisateurs**.