

04/03/2025

# Compte rendu

Active Directory

Amine LAOUAR

ECORIS

## TABLE DES MATIERES

Introduction .....	2
Prérequis.....	2
Configuration de l'active directory .....	3
Création des Unités Organisationnelles (OU).....	4
Création des Utilisateurs.....	6
Création GPO .....	7
Empêcher l'accès à l'invite de commandes (CMD) et à l'éditeur de registre .....	8
Bloquer l'installation de logiciels.....	8
Fond d'écran .....	9
Préparer l'image du fond d'écran.....	9
Créer et appliquer une GPO pour imposer le fond d'écran .....	9
Délégation des droits d'administration sur les OU .....	11
Délégation des droits aux administrateurs locaux .....	11
Accorder un accès total aux administrateurs principaux.....	13
Configuration des politiques de mots de passe et restrictions d'accès aux postes .....	14
Création de deux politiques de mots de passe .....	14
Activer les FGPP dans Active Directory .....	14
Configuration des profils itinérants avec restrictions d'accès .....	19
Création et application des profils itinérants .....	19
Définition des profils itinérants dans Active Directory .....	21
Conclusion.....	21

## 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 :

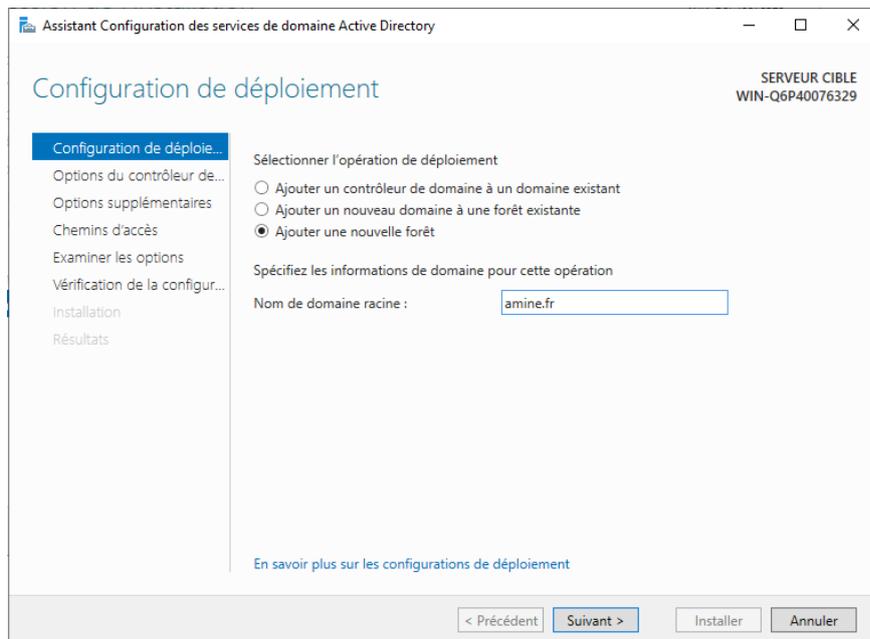
- Trois machines virtuelles sous Windows (1 serveur et 2 postes clients)
- VirtualBox avec réseau privé configuré
- Une adresse IP fixe pour le serveur
- Installation des add-ons invités pour une compatibilité optimale

### Objectif

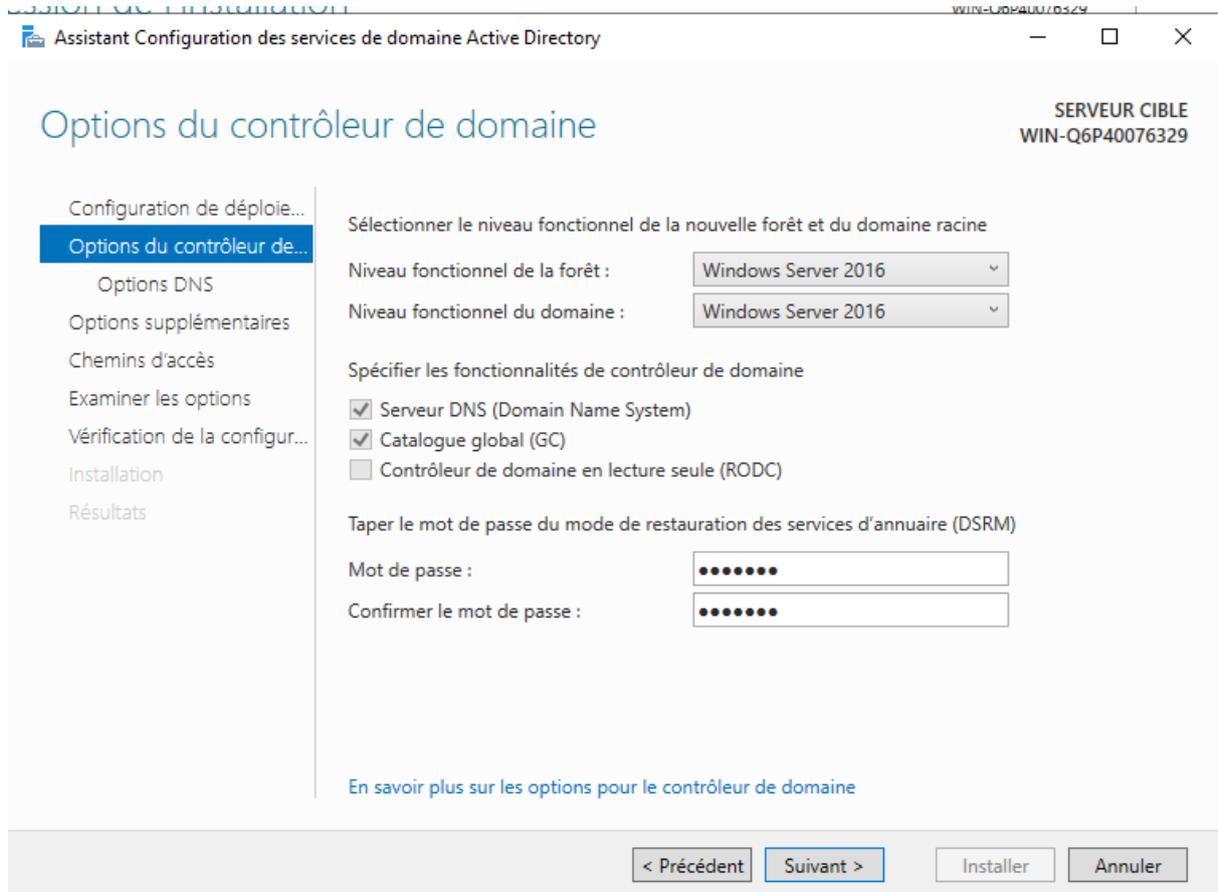
Mettre en place les services essentiels au bon fonctionnement d'Active Directory.

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

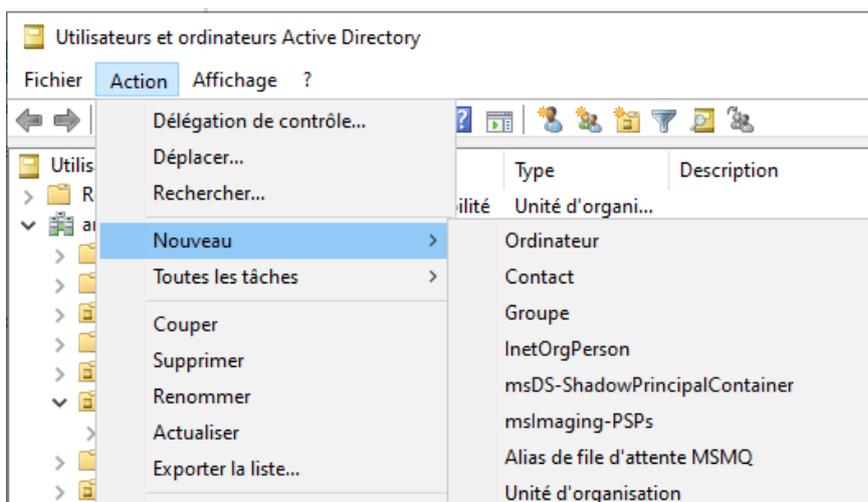


Définissez un mot de passe pour le mode de récupération des services d'annuaire.



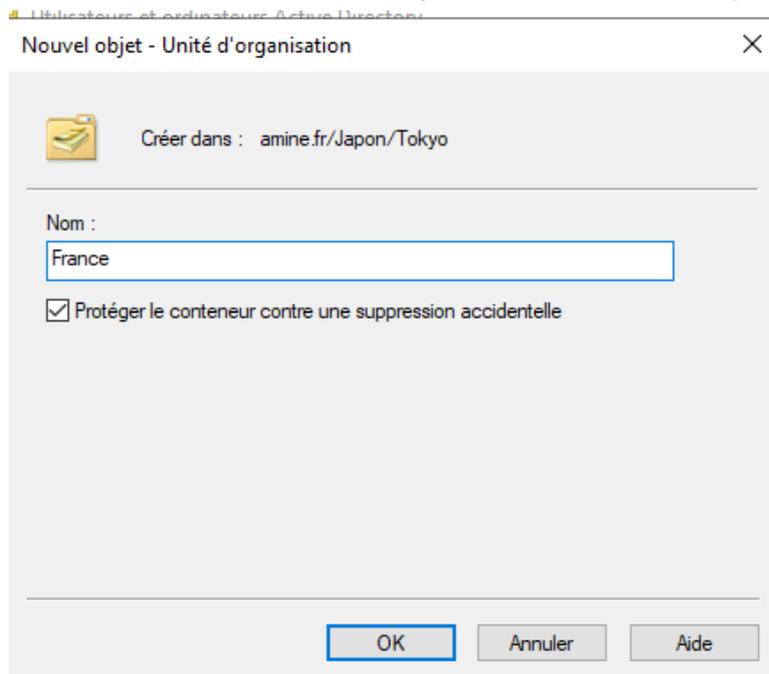
Cliquez sur Suivant jusqu'à Installer. Le serveur redémarrera automatiquement après l'installation.

## CREATION DES UNITES ORGANISATIONNELLES (OU)

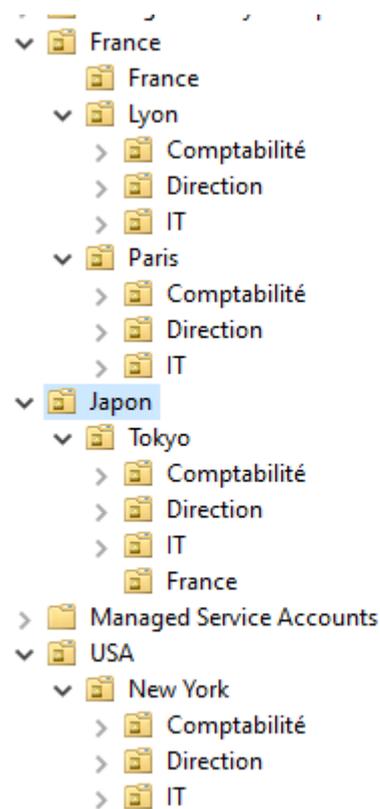


Faites un clic droit sur le nom de domaine, puis sélectionnez Nouveau → Unité d'organisation

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.

Nouvel objet - Utilisateur

Créer dans : amine.fr/France/Paris/Direction

Prénom : Stéphane      Initiales :

Nom : depanam

Nom complet : Stéphane depanam

Nom d'ouverture de session de l'utilisateur : s.depanam@amine.fr

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : AMINE\s.depanam

< Précédent    Suivant >    Annuler

Nouvel objet - Utilisateur

Créer dans : amine.fr/France/Paris/Direction

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

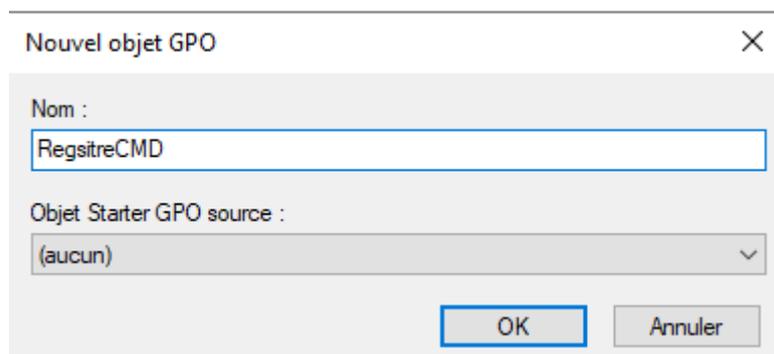
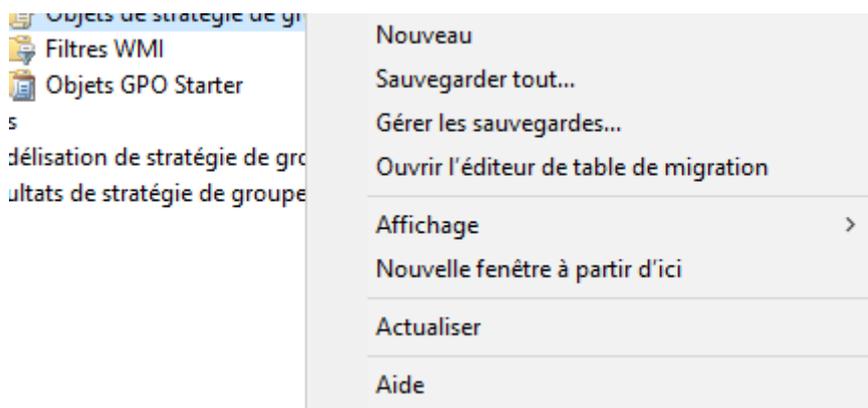
Définissez un mot de passe et configurez les options souhaitées (ex: l'utilisateur doit changer son mot de passe à la première connexion)

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

Configuration utilisateur

- Stratégies
  - Paramètres du logiciel
  - Paramètres Windows
  - Modèles d'administration :
    - Bureau
    - Composants Windows
    - Dossiers partagés
    - Menu Démarrer et barre
    - Panneau de configuration
    - Réseau
    - Système
      - Accès au stockage amovible
      - Affichage
      - Gestion de l'alimentation
      - Gestion de la communication Internet
      - Installation de pilotes
      - Options Ctrl+Alt+Suppr
      - Options d'atténuation
      - Ouverture de session
      - Profils utilisateur
      - Redirection de dossiers
      - Scripts
      - Services Paramètres régionaux
      - Stratégie de groupe
        - Télécharger les composants manquants
        - Interprétation du siècle pour l'an 2000
        - Restreindre l'exécution de ces programmes à partir de l'aide
        - Ne pas afficher l'écran de démarrage Mise en route à l'ouverture de session
        - Interface utilisateur personnalisée
        - Désactiver l'accès à l'invite de commandes**

Modifier le paramètre de stratégie

Configuration requise :  
Au minimum Windows 2000

Description :  
Ce paramètre de stratégie empêche les utilisateurs d'exécuter l'invite de commandes interactive, Cmd.exe. Ce paramètre de stratégie indique également s'il est permis d'exécuter ou non les fichiers de commandes (.cmd et .bat) sur l'ordinateur.

Si vous activez ce paramètre de stratégie et que l'utilisateur essaie d'ouvrir une fenêtre de commande, le système affiche un message signalant qu'un paramètre bloque l'action.

Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les utilisateurs peuvent exécuter l'invite de commandes.

Paramètre	État	Commentaire
Télécharger les composants manquants	Non configuré	Non
Interprétation du siècle pour l'an 2000	Non configuré	Non
Restreindre l'exécution de ces programmes à partir de l'aide	Non configuré	Non
Ne pas afficher l'écran de démarrage Mise en route à l'ouverture de session	Non configuré	Non
Interface utilisateur personnalisée	Non configuré	Non
<b>Désactiver l'accès à l'invite de commandes</b>	<b>Non configuré</b>	<b>Non</b>

Stratégie RegistreCMD [WIN-Q6P40076]

- Configuration ordinateur
  - Stratégies
  - Préférences
  - Configuration utilisateur
    - Stratégies
      - Paramètres du logiciel
      - Paramètres Windows
      - Modèles d'administration :
        - Bureau
        - Composants Windows
        - Dossiers partagés
        - Menu Démarrer et barre
        - Panneau de configuration
        - Réseau
        - Système
          - Accès au stockage amovible
          - Affichage
          - Gestion de l'alimentation
          - Gestion de la communication Internet
          - Installation de pilotes
          - Options Ctrl+Alt+Suppr
          - Options d'atténuation
          - Ouverture de session
          - Profils utilisateur
          - Redirection de dossiers
          - Scripts
          - Services Paramètres régionaux
          - Stratégie de groupe
            - Télécharger les composants manquants
            - Interprétation du siècle pour l'an 2000
            - Restreindre l'exécution de ces programmes à partir de l'aide
            - Ne pas afficher l'écran de démarrage Mise en route à l'ouverture de session
            - Interface utilisateur personnalisée
            - Désactiver l'accès à l'invite de commandes
            - Empêcher l'accès aux outils de modifications du Registre**

Modifier le paramètre de stratégie

Configuration requise :  
Au minimum Windows 2000

Description :  
Désactive l'éditeur de Registre Windows Regedit.exe.

Si vous activez ce paramètre de stratégie et que l'utilisateur essaie de démarrer Regedit.exe, un message s'affiche pour expliquer qu'un paramètre de stratégie bloque l'action.

Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les utilisateurs peuvent exécuter Regedit.exe normalement.

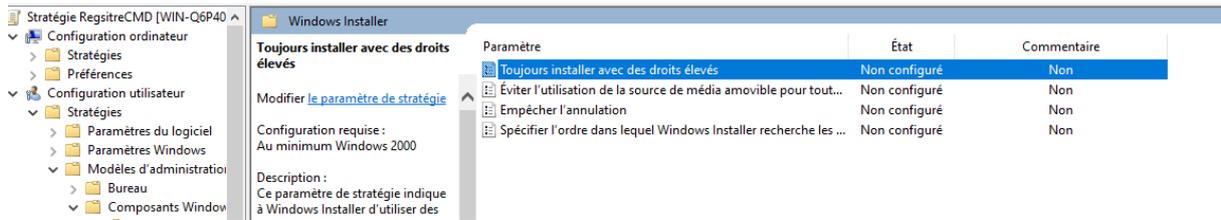
Pour empêcher les utilisateurs d'utiliser d'autres outils d'administration, utilisez le paramètre de stratégie de groupe.

Paramètre	État	Commentaire
Accès au stockage amovible	Non configuré	Non
Affichage	Non configuré	Non
Gestion de l'alimentation	Non configuré	Non
Gestion de la communication Internet	Non configuré	Non
Installation de pilotes	Non configuré	Non
Options Ctrl+Alt+Suppr	Non configuré	Non
Options d'atténuation	Non configuré	Non
Ouverture de session	Non configuré	Non
Profils utilisateur	Non configuré	Non
Redirection de dossiers	Non configuré	Non
Scripts	Non configuré	Non
Services Paramètres régionaux	Non configuré	Non
Stratégie de groupe	Non configuré	Non
Télécharger les composants manquants	Non configuré	Non
Interprétation du siècle pour l'an 2000	Non configuré	Non
Restreindre l'exécution de ces programmes à partir de l'aide	Non configuré	Non
Ne pas afficher l'écran de démarrage Mise en route à l'ouverture de session	Non configuré	Non
Interface utilisateur personnalisée	Non configuré	Non
Désactiver l'accès à l'invite de commandes	Non configuré	Non
<b>Empêcher l'accès aux outils de modifications du Registre</b>	<b>Non configuré</b>	<b>Non</b>

## BLOQUER L'INSTALLATION DE LOGICIELS

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

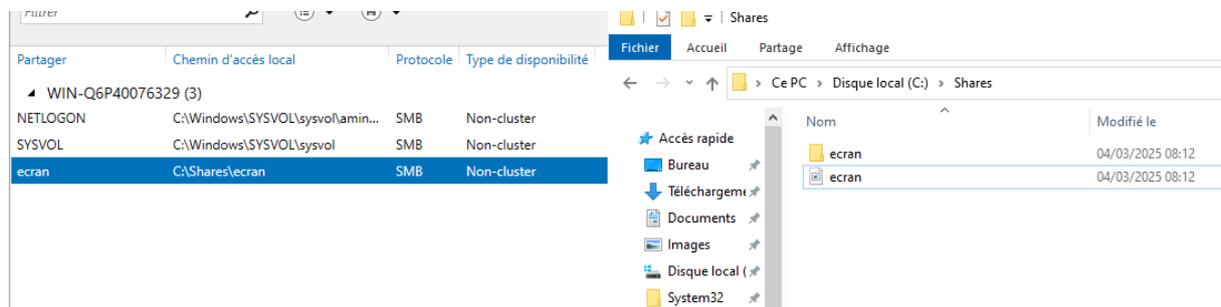
ACTIVER LA STRATEGIE : TOUJOURS INSTALLER AVEC DES DROITS ELEVES



## FOND D'ECRAN

### PREPARER L'IMAGE DU FOND D'ECRAN

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



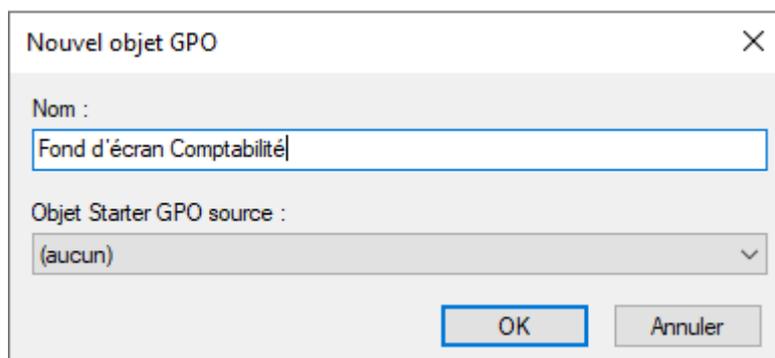
Stocker l'image sur un dossier partagé accessible aux utilisateurs :

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.

**Domaines**

- amine.fr
  - Default Domain Policy
  - Domain Controllers
    - Default Domain Controllers Policy
  - France
    - RegistreCMD
    - Lyon
      - Comptabilité
      - Direction
      - IT
    - Paris
      - Comptabilité
      - Direction
      - IT
  - Japon
    - RegistreCMD
    - Tokyo
      - Comptabilité
      - Direction
      - IT
  - USA
    - RegistreCMD
    - New York
      - Comptabilité
      - Direction
      - IT
  - Objets de stratégie de groupe
    - Default Domain Controllers Policy
    - Default Domain Policy
    - Fond d'écran Comptabilité

**Liaisons**

Afficher les liaisons à cet emplacement : amine.fr

Les sites, domaines et unités d'organisation suivants sont liés à cet objet GPO :

Emplacement	Appliqué	Lien activé
Comptabilité	Non	Oui

**Filtrage de sécurité**

Les paramètres dans ce GPO s'appliquent uniquement aux groupes, utilisateurs et ordinateurs suivants :

Nom
Utilisateurs authentifiés

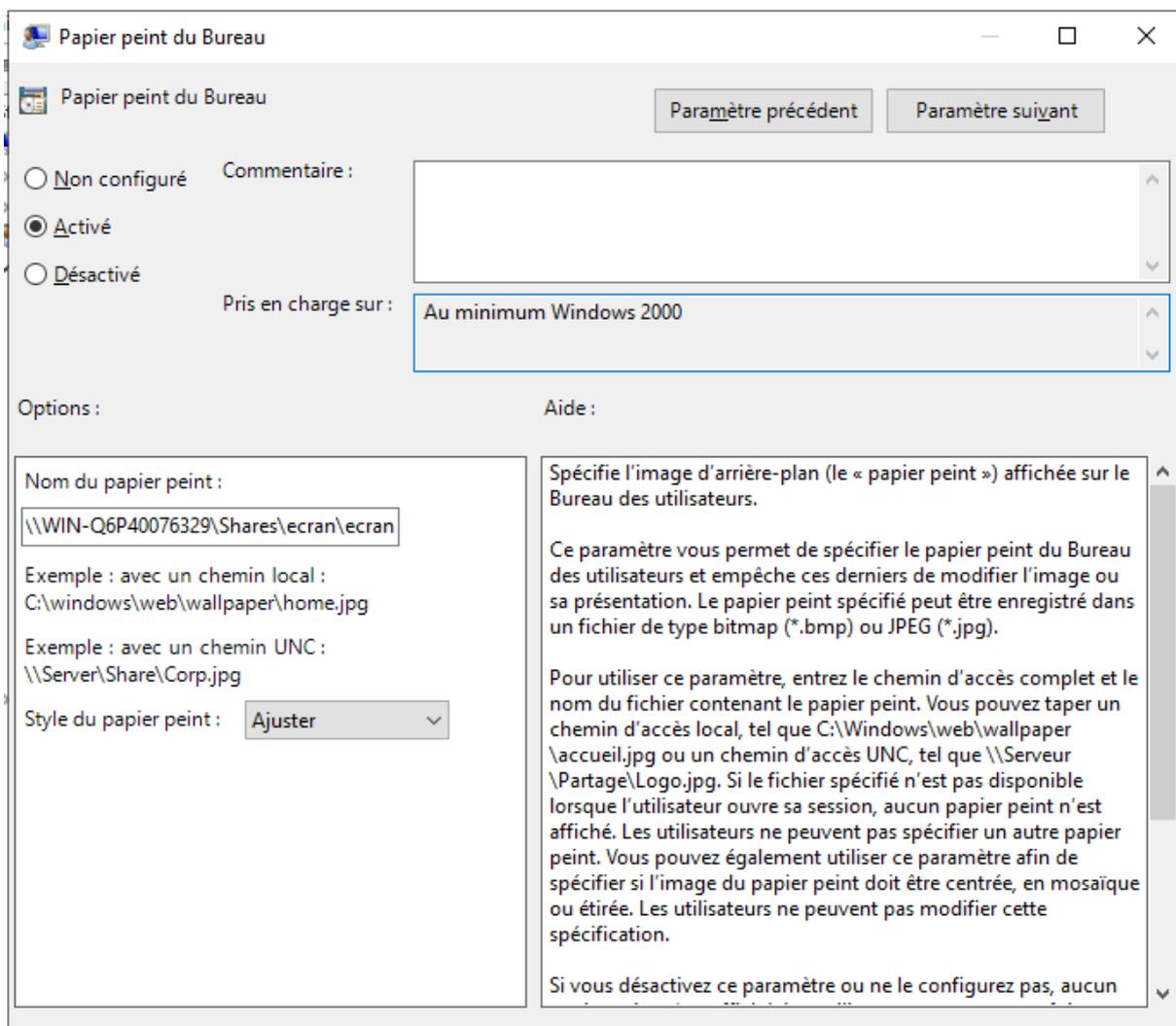
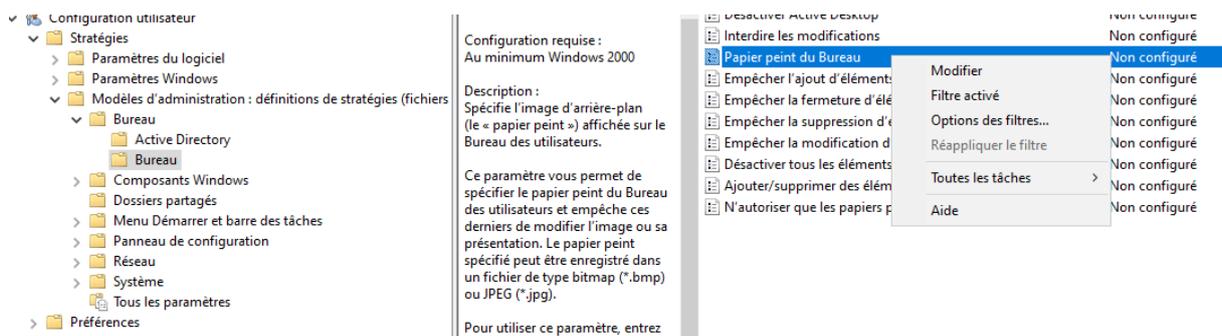
Ajouter... Supprimer Propriétés

Modifier le GPO et aller dans :

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

Activer la stratégie :

"Fond d'écran Active Desktop" → Activé



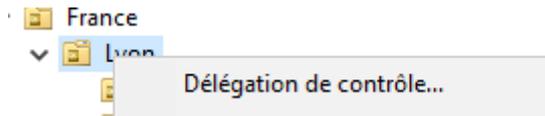
## DELEGATION DES DROITS D'ADMINISTRATION SUR LES OU

### DELEGATION DES DROITS AUX ADMINISTRATEURS LOCAUX

Ouvrir la console "Utilisateurs et ordinateurs Active Directory"

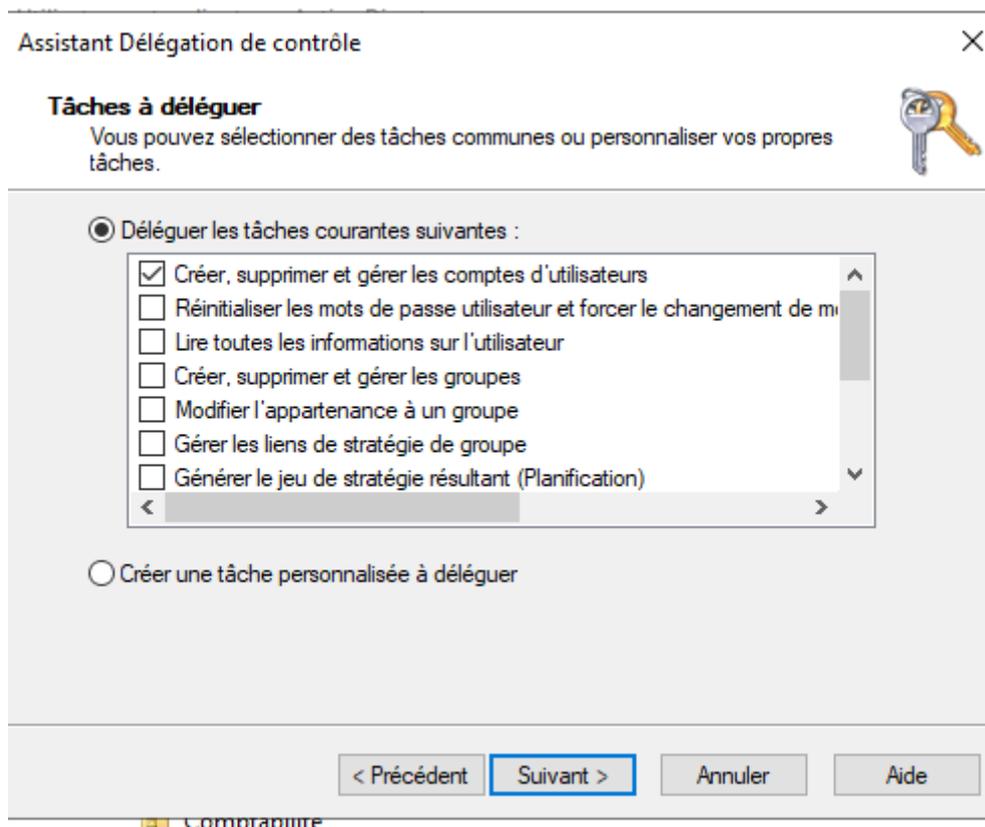
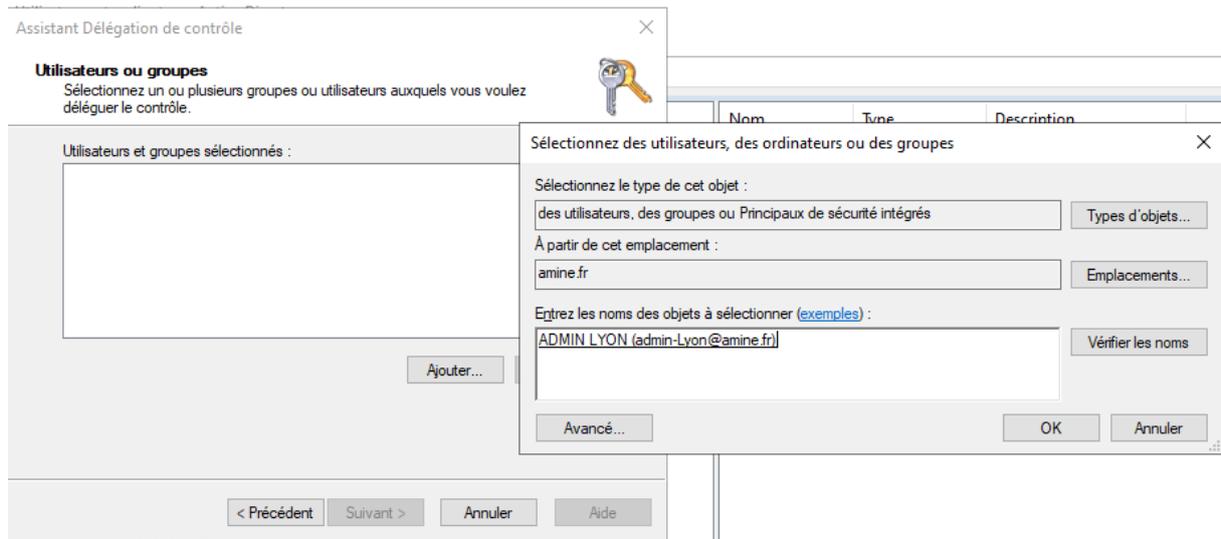
Faire un clic droit sur l'OU du site concerné (ex: France/Lyon).

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".

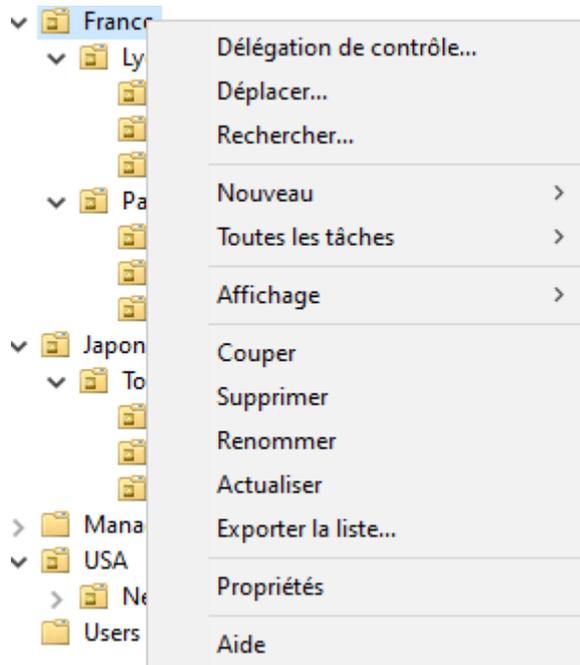


Terminer l'assistant, puis tester avec un compte admin local pour vérifier qu'il peut gérer uniquement son OU.

#### 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).

Propriétés de : France

Général Géré par COM+

Nom : amine.fr/France/Admin\_Principal\_France

Modifier... Propriétés Effacer

Bureau :

Adresse :

Ville :

Département ou région :

Pays/région :

Numéro de téléphone :

Numéro de télécopie :

OK Annuler Appliquer

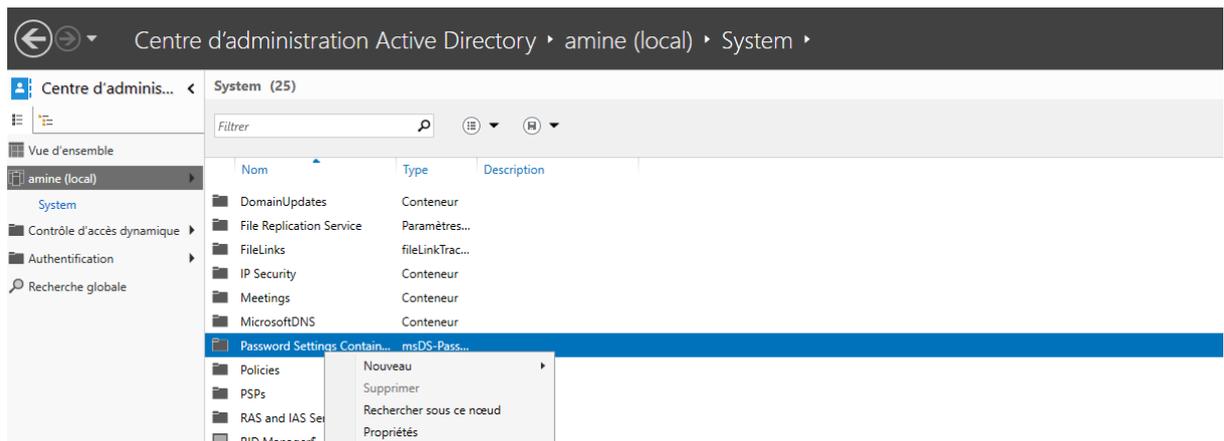
Appliquer et fermer.

## 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**

**Créer Paramètres de mot de passe : Complexe\_Utilisateurs**

**\* Paramètres de mot de passe**

S'applique directement à

Paramètres de mot de passe

Nom : \* Complexe\_Utilisateurs

Priorité : \*

Appliquer la longueur minimale du mot de passe  
Longueur minimale du mot de passe (caractères) : \* 12

Appliquer l'historique des mots de passe  
Nombre de mots de passe mémorisés : \* 24

Le mot de passe doit respecter des exigences de complexité

Stocker le mot de passe en utilisant un chiffrement réversible

Protéger contre la suppression accidentelle

Description :

Options d'âge du mot de passe :

Appliquer l'âge minimal de mot de passe  
L'utilisateur ne peut pas changer le mot de passe d'i... \* 1

Appliquer l'âge maximal de mot de passe  
L'utilisateur doit changer le mot de passe après (jour... \* 90

Appliquer la stratégie de verrouillage des comptes :

Nombre de tentatives de connexion échouées autorisé : \* 5

Réinitialiser le nombre de tentatives de connexion écho... \* 30

Le compte va être verrouillé

Pendant une durée de (mins) : \* 30

Jusqu'à ce qu'un administrateur déverrouille manuellement le compte

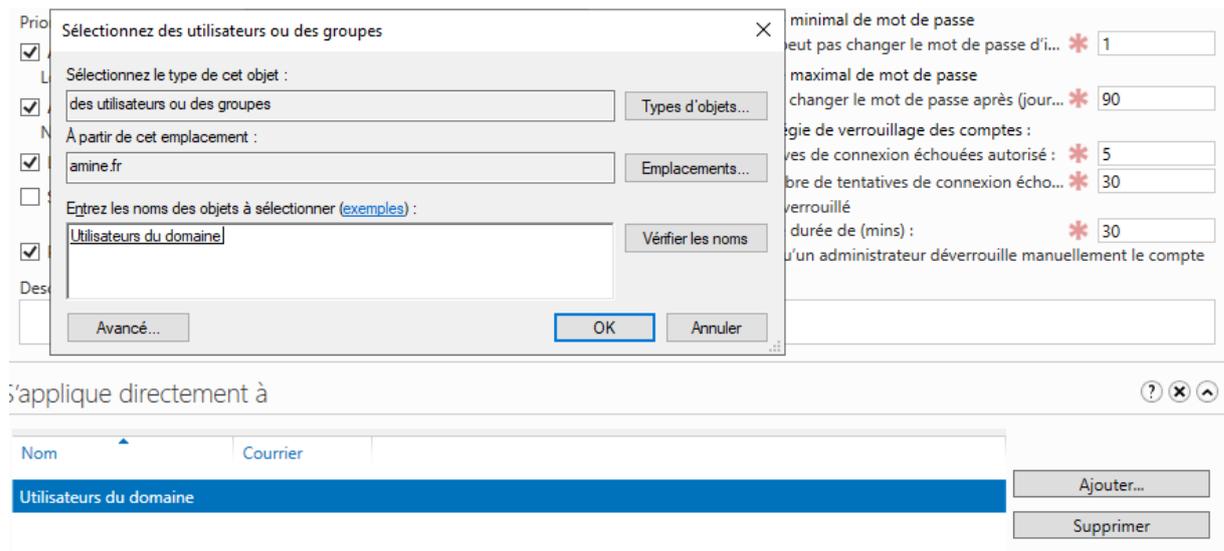
S'applique directement à

Nom	Courrier

Ajouter...  
Supprimer

Informations supplémentaires... OK Annuler

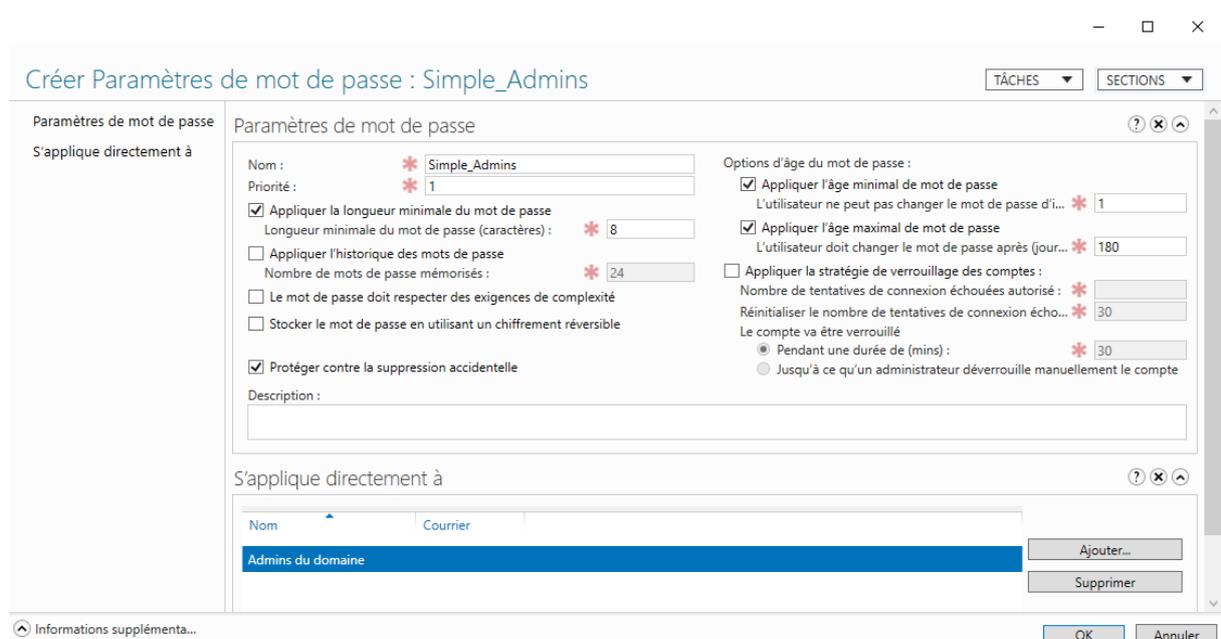
4. Dans **Attributs appliqués à**, ajouter le **groupe des utilisateurs standards** (ex: Utilisateurs\_Domaine).



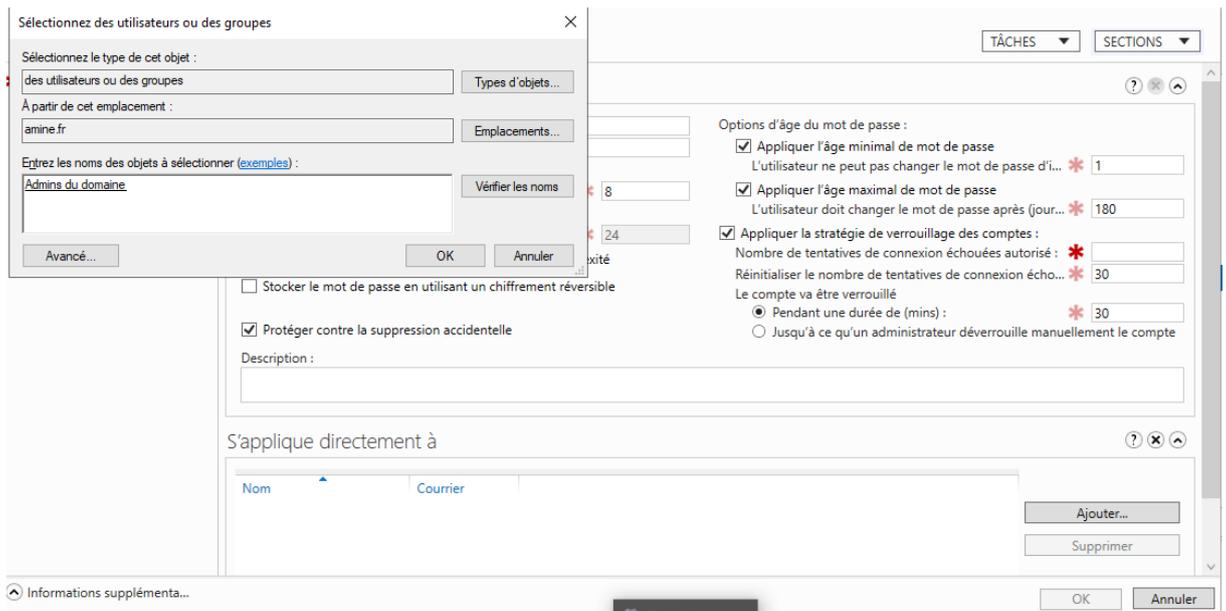
## 5. Enregistrer.

## 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



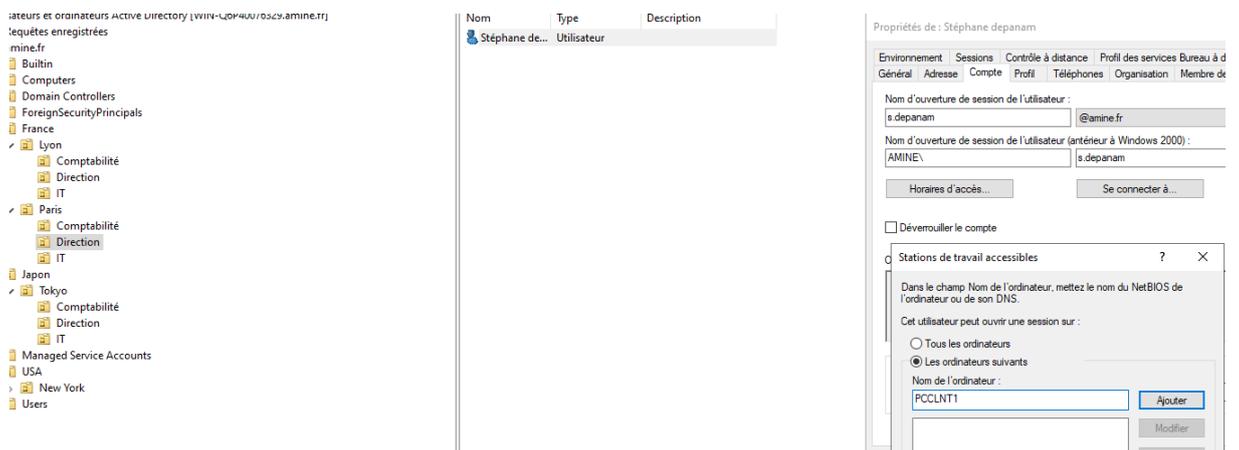
3. Dans **Attributs appliqués à**, ajouter le **groupe des administrateurs** (ex: Admins\_Domaine).



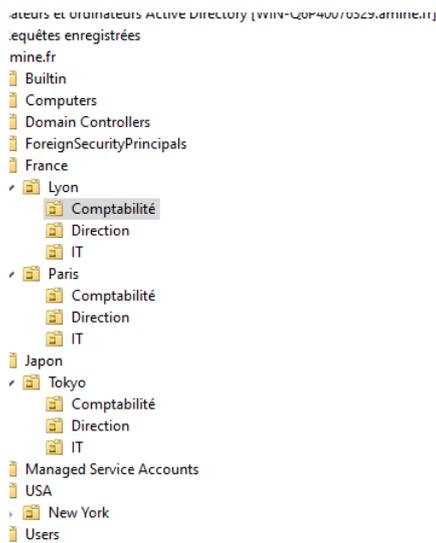
#### 4. Enregistrer.

## RESTRICTION DES CONNEXIONS POUR DIRECTION ET COMPTABILITE

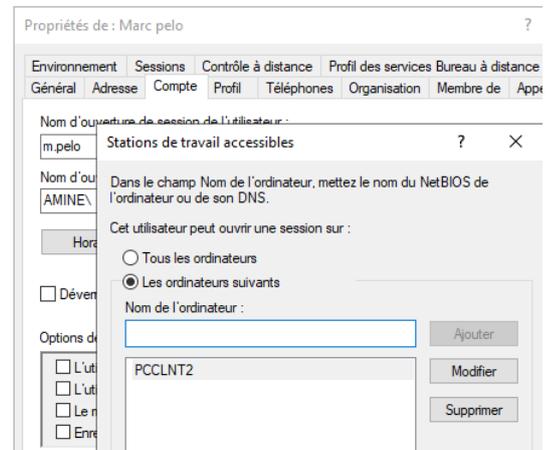
1. Ouvrir "**Utilisateurs et ordinateurs Active Directory**" (dsa.msc).
2. Sélectionner un utilisateur de l'OU **Direction**.
3. **Ouvrir ses propriétés** → Onglet **Compte** → Bouton **Se connecter à...**
4. Sélectionner uniquement **PCCLNT1**, puis **Appliquer**.



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

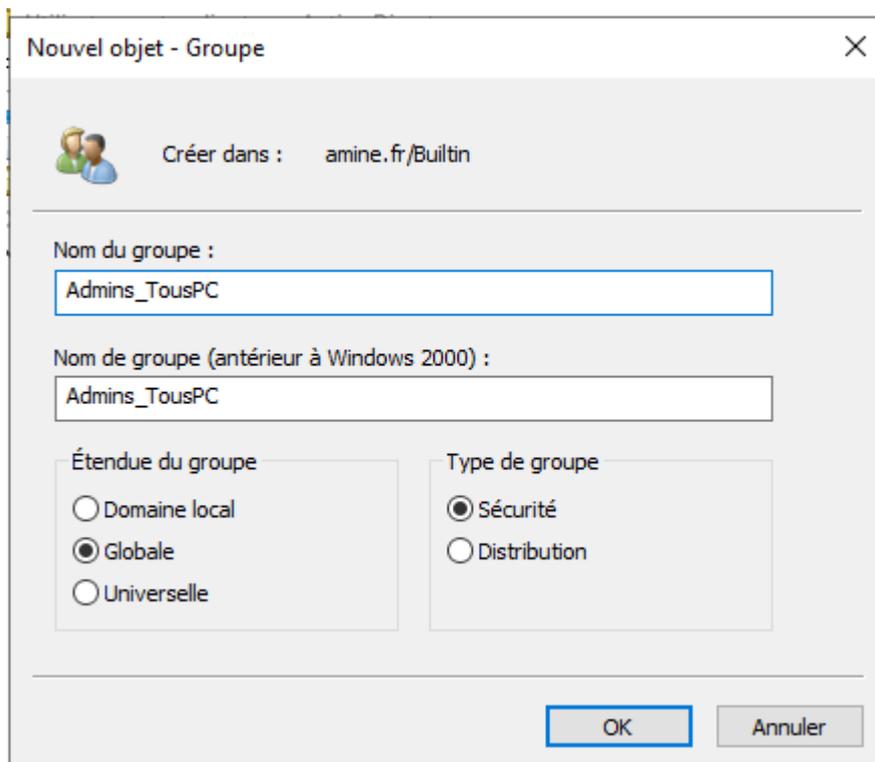


Nom	Type	Description
Marc pelo	Utilisateur	

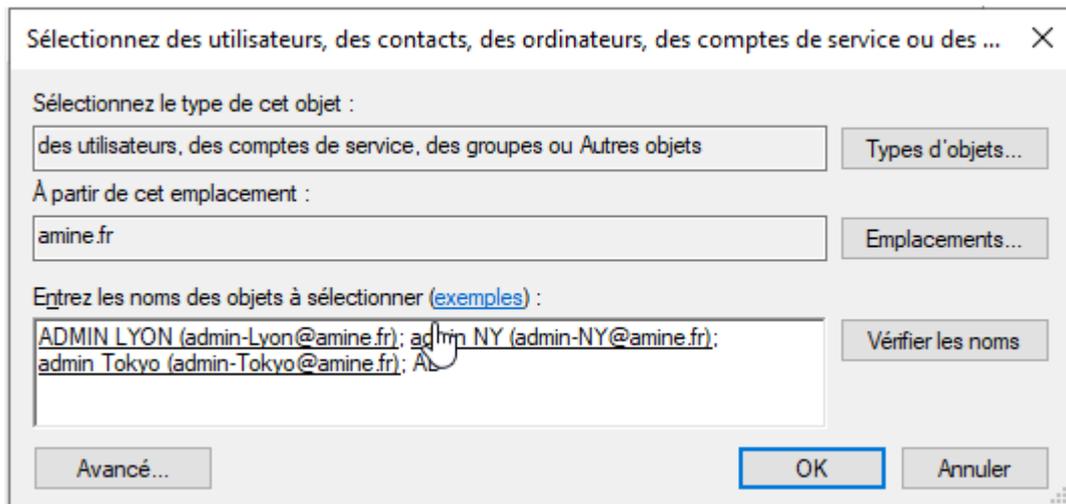


## AUTORISER LES ADMINISTRATEURS A SE CONNECTER PARTOUT

### 1. Créer un groupe **Admins\_TousPC**.



### 2. Ajouter les administrateurs à ce groupe.

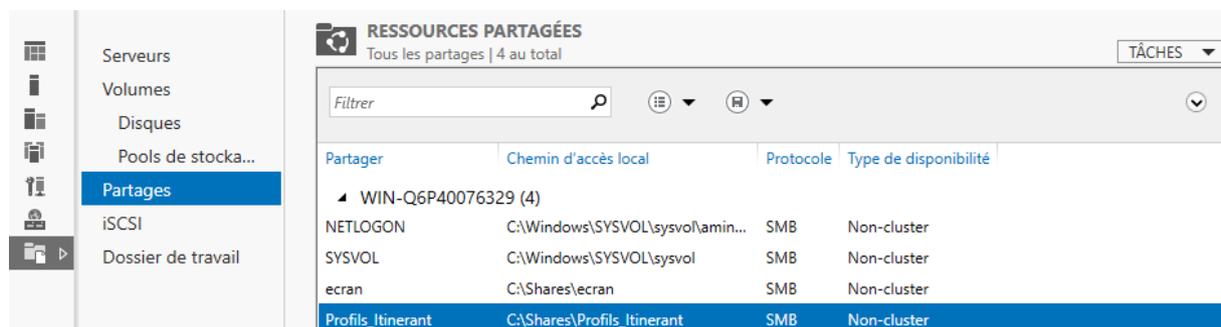


## CONFIGURATION DES PROFILS ITINERANTS AVEC RESTRICTIONS D'ACCES

### CREATION ET APPLICATION DES PROFILS ITINERANTS

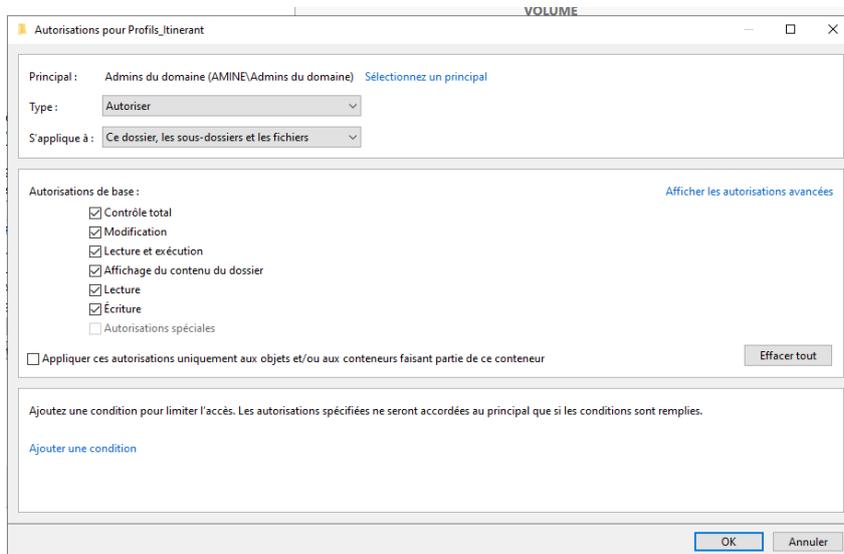
#### CREATION DU DOSSIER PARTAGE POUR LES PROFILS

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

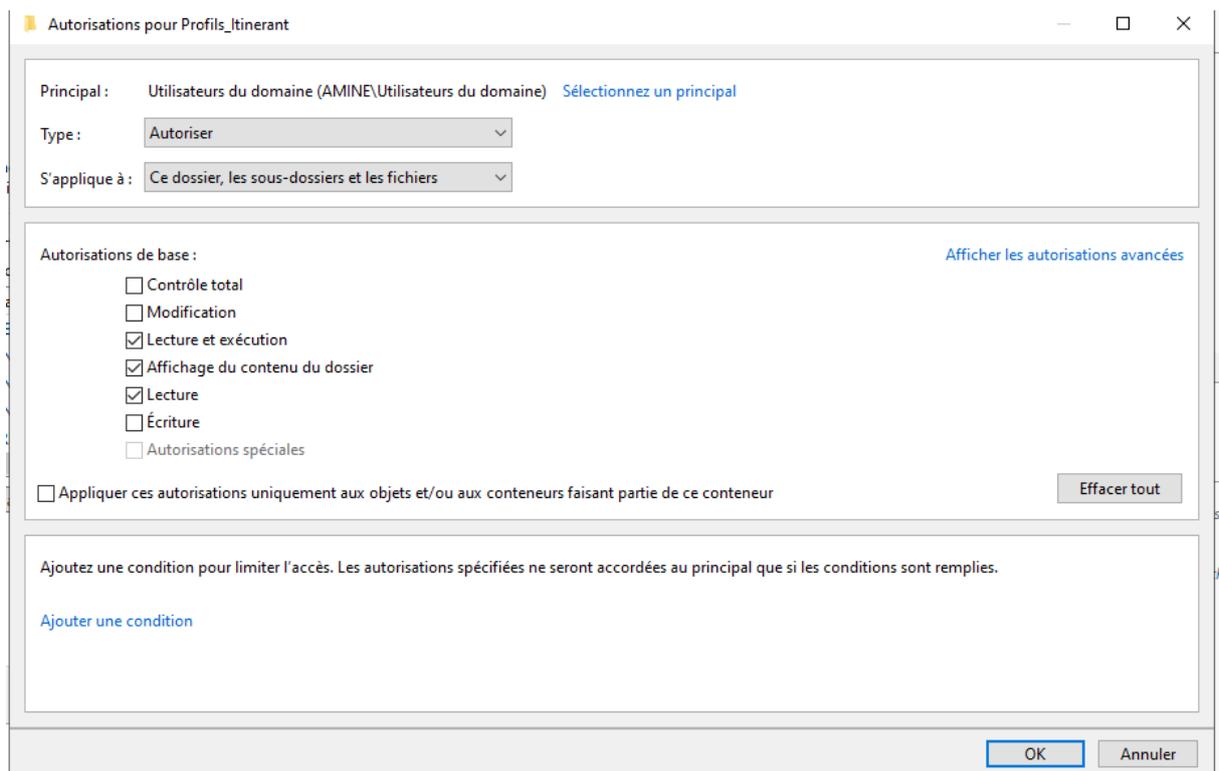


## Configurer les permissions NTFS :

### Administrateurs du domaine → Contrôle total



### Utilisateurs du domaine → Lecture & Écriture



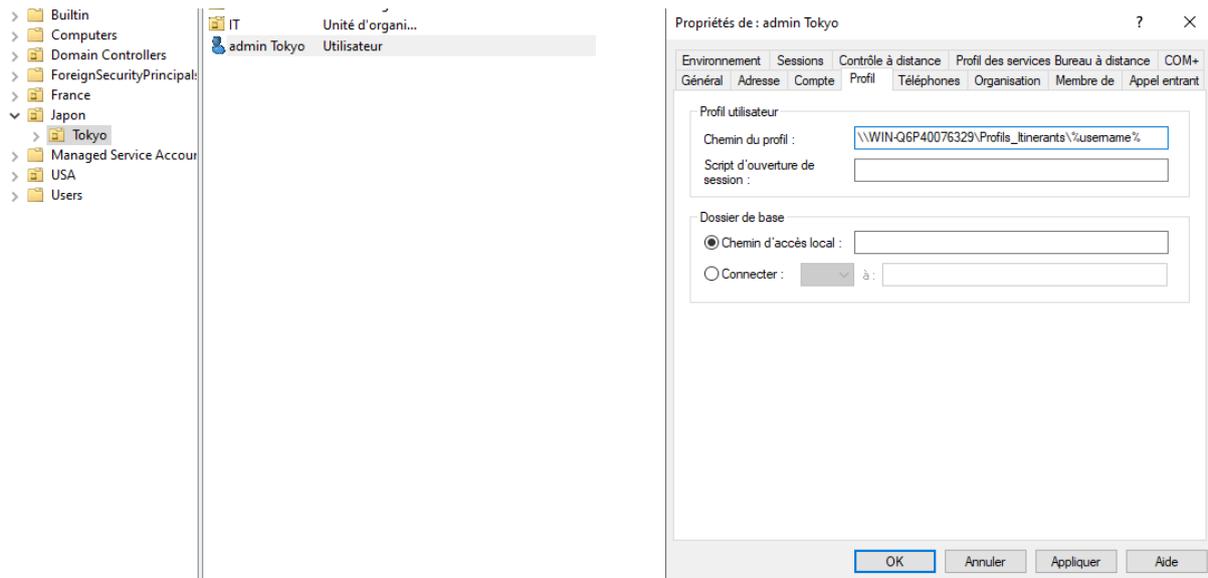
## DEFINITION DES PROFILS ITINERANTS DANS ACTIVE DIRECTORY

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**.