UPEC
UNIVERSITÉ PARIS-EST CRÉTEIL
iut Créteil Vitry

iut réseaux & télécoms Créteil-Vitry

TP N°5

SUJET :

SÉCURITÉ ACTIVE DIRECTORY
MODÈLE DE DÉLÉGATION

UE 3.1
ADMINISTRATION SYSTEME

LÉONARD SAVINA
BRICE AUGUSTIN

Durée : 4 heures

Version : 1.2

Création : 12/2020
Révisions : 02/2020

Sommaire

1. Introduction

L'objectif de ce TP est de sécuriser l'administration AD en mettant en place un modèle de délégation d'administration.

Dans un premier temps, la sécurisation va consister à créer l'ossature du modèle de délégation dans l'annuaire Active Directory :

- La création de comptes *nominatifs* pour les administrateurs du domaine
- La création de comptes de type *helpdesk*, permettant de réaliser la plupart des tâches bureautique sans avoir à utiliser un compte administrateur de domaine

Le but étant d'implémenter les bonnes pratiques d'administration de Microsoft avec l'administration en *Tier*. Dans le cas de notre TP nous aurons :

- Un Tier 0 : les administrateurs de domaine et le DC
- Un Tier 2 : le *helpdesk* et les postes de travail

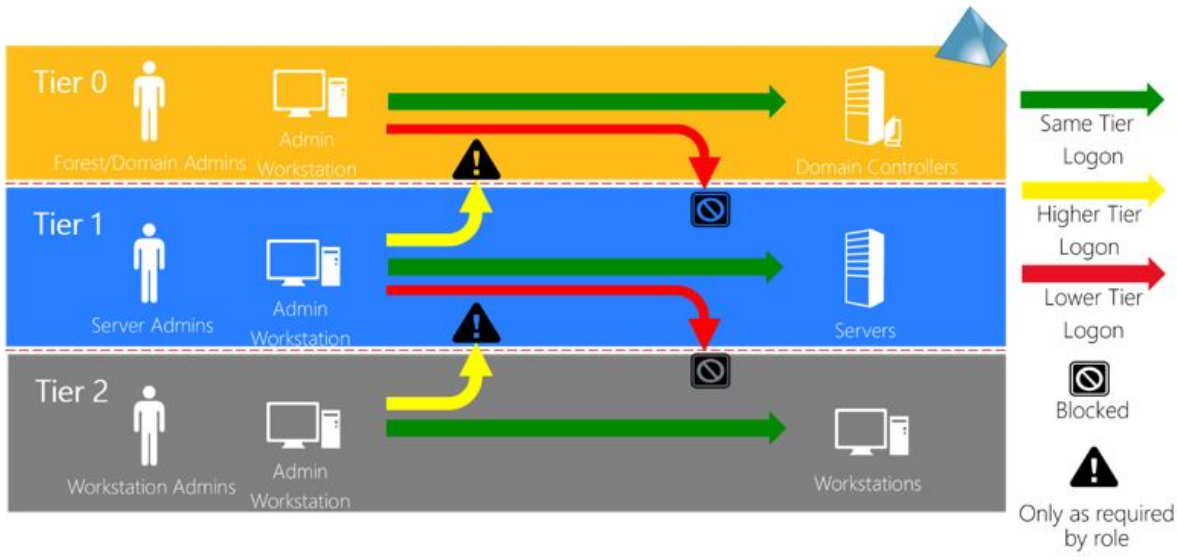

Fig. 1 *Rappel administration en Tier*

Dans un second temps, nous déclinerons ce modèle sur le poste de l'OU `Openspace` et laisserons le poste de l'OU `Bureau` non maitrisé (le modèle d'administration en Tier ne sera pas implémenté sur cette OU).

Dans le prochain TP, vous allez évaluer les bénéfices de ce modèle en réalisant un test d'intrusion et vous améliorerez la détection d'intrusion sur le système d'information.

1.1. Contexte

Pour rappel, vous êtes l'administrateur système de `Blue Sky`, une entreprise de quelques centaines d'employés répartis en trois branches : R&D (*recherche et développement*), Finance (*blanchiment et optimisation fiscale*) et Administrateurs (*gestion du système d'information*).

Les employés disposent de deux espaces de travail :

- Un *openspace* accueille les départements Finance et R&D. Il comporte 70 postes de travail sous `Windows 10`
- L'équipe des administrateurs système et réseau est regroupée dans un grand bureau

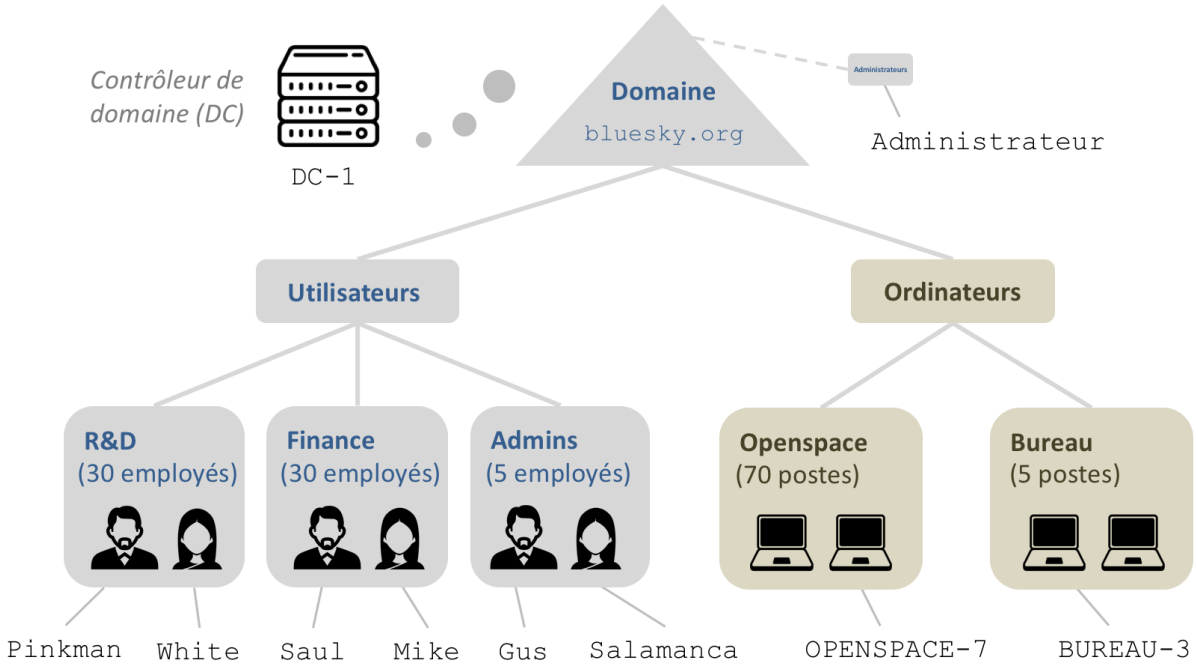

Fig. 2 *Domaine Active Directory de votre entreprise*

1.2. Maquette

Avant de démarrer le TP, vous allez ramener votre maquette dans l'état où elle était, à la fin de la séance précédente.

Pour rappel, la maquette était constituée de :

- Un contrôleur de domaine sous `Windows Server 2016` : vous utiliserez une VM hébergée sur PC3
- Deux postes de travail sous `Windows 10` : un dans l'*openspace*, un dans le bureau des administrateurs. *Utilisez PC1 et PC2, respectivement*
- Deux utilisateurs dans chaque département de l'entreprise (R&D, Finance et Admins)

En plus d'héberger la VM, PC3 (sous `Debian Linux`) vous permettra de visualiser les PDF et rédiger le CR.

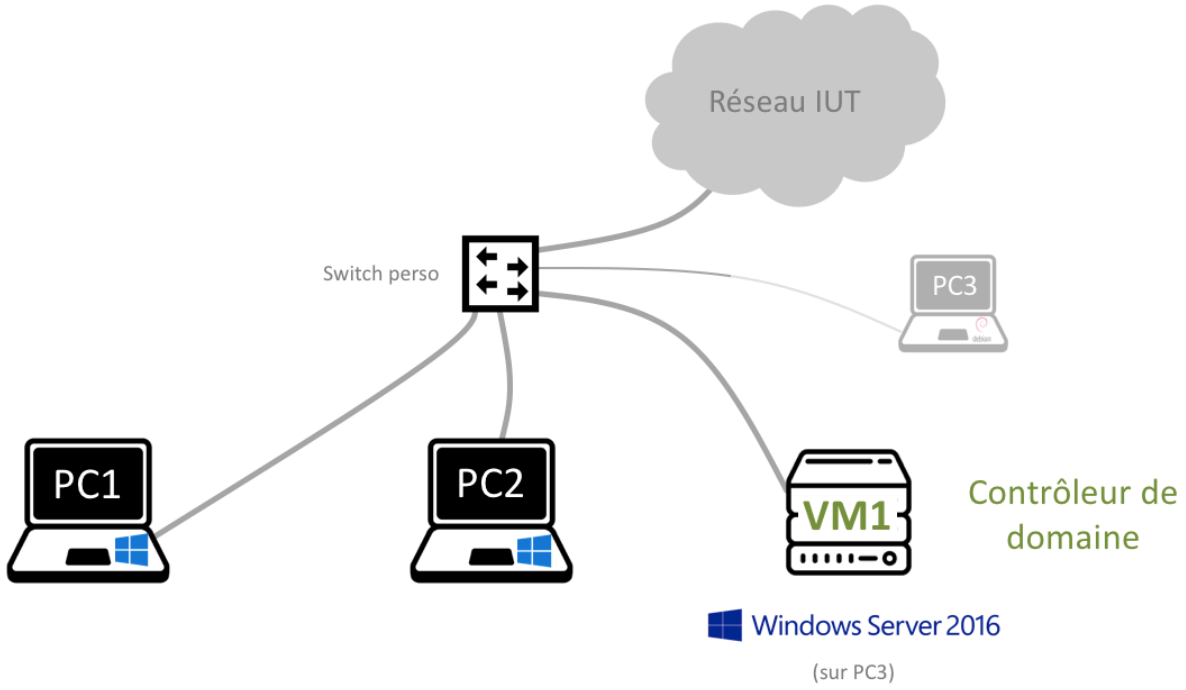

Fig. 3 *Maquette de TP*

PC	Nom	Adresse IP
PC1	`OPENSPACE-7`	`198.51.$t.17/24`[1]
PC2	`BUREAU-3`	`198.51.$t.203/24`

[1] Remplacez `$t` par votre numéro de table.

VM1	DC-1	198.51.$t.3/24
PC3		Dynamique (IUT)

Tableau 1 *Configuration IP des ordinateurs*

Les principales étapes de configuration sont indiquées dans la section `I ♥ PowerShell` du TP précédent :

- **Étape 1** : Nommage et adressage IP du futur DC
- **Étape 2** : Installation et configuration du rôle `ADDS`
- **Étape 3** : Création des utilisateurs et des OU
- **Étape 4** : Nommage, adressage IP des postes de travail et ajout dans le domaine
- **Étape 5** : Déplacement des postes sous la bonne OU (`Openspace` ou `Bureau`)

Si vous disposez encore des scripts `PowerShell` (`step1.ps1` à `step5.ps1`) développés précédemment, utilisez-les.

Dans le cas contraire, utilisez le script fourni par votre chargé de TP :

- Lancez simplement `step1-2-3.ps1` sur l'ordinateur `Windows Server 2016` fraichement restauré, et patientez (l'ordinateur va redémarrer *deux* fois automatiquement)
- Les scripts `step4.ps1` et `step5.ps1` ne sont pas fournis, mais l'utilisation de la GUI ne vous prendra pas beaucoup de temps …

Il ne vous reste plus qu'à créer la GPO* `Afficher les extensions`, et votre maquette est prête !

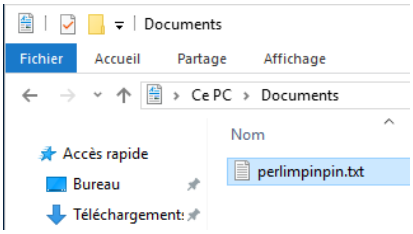

Fig. 4 *Fichier texte dont l'extension est affichée*

Quelle que soit la méthode choisie, vérifiez impérativement que votre nouveau contrôleur de domaine est opérationnel avant de continuer : par exemple ouvrez une session* avec `Pinkman` sur `OPENSPACE-7` et assurez-vous que les extensions de fichiers sont bien affichées (Fig. 4).

Synthèse 1 : Résumez en 4-6 lignes ce que vous avez fait depuis le début de la séance.

Appelez votre chargé de TP pour lui montrer que votre maquette est prête.

2. Préparation du modèle de délégation dans l'AD

Pour créer le modèle de délégation, vous allez légèrement réorganiser l'OU `Admins` :

- `Admin_helpdesk` va contenir les utilisateurs administrateurs réalisant des actions techniques sur l'environnement postes de travail. Ils vont former le Tier 2. Cette OU contient un utilisateur : `adm_h_TRG` où TRG est votre trigramme[2]
- `Admin_domaine` va contenir les comptes administrateurs du domaine (or compte *builtin* `Administrateur`). Ils vont former le Tier 0. Cette OU contient un unique utilisateur : `adm_d_TRG` où TRG est votre trigramme
- `Groupes` contient les groupes d'administration (*groupes de sécurité*) apportés par le modèle de délégation. Le groupe `Admin_helpdesk_pc` va permettre à l'équipe *helpdesk* d'administrer les postes de travail sans être administrateur de domaine. Le groupe `Admin_helpdesk_ad` va permettre à cette équipe de gérer *certains* paramètres de l'environnement utilisateur au niveau Active Directory

[2] Le trigramme est la première lettre de votre prénom suivie des deux premières lettres de votre nom de famille.

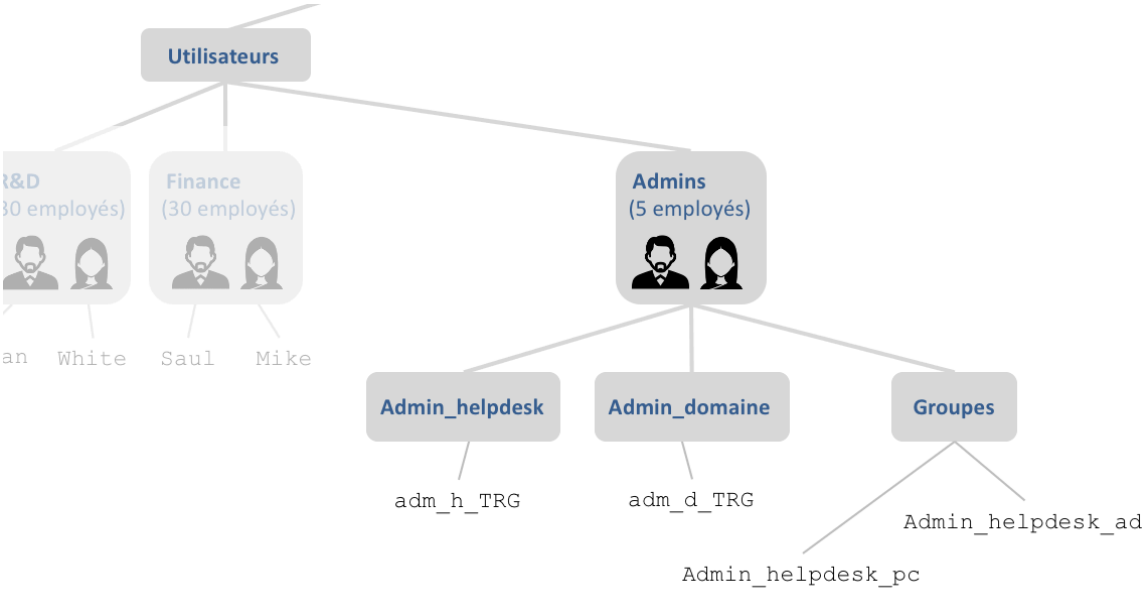

Fig. 5 *Réorganisation des Admins*

Ouvrez une session* sur `DC-1` avec le compte `bluesky\Administrateur`, puis créez les OU* comme indiqué précédemment. Ensuite, créez les deux nouveaux utilisateurs* dans leur OU respective (Fig. 5 et 6).

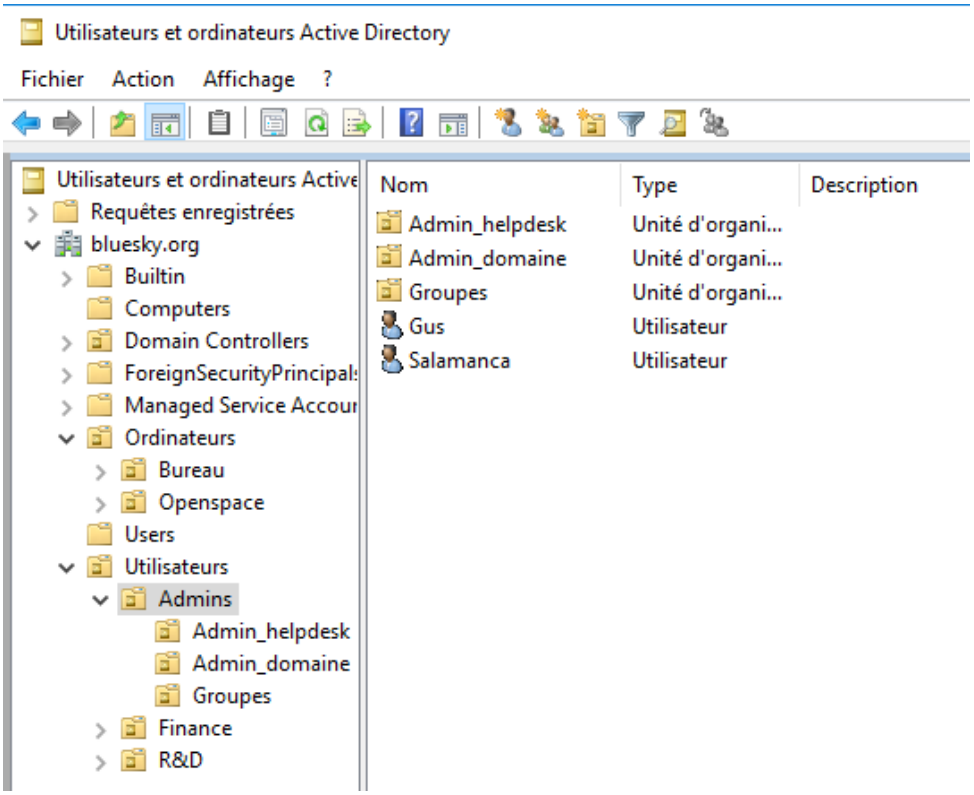

Fig. 6 L'*OU* `Admins` *après réorganisation*

Ajoutez l'utilisateur `adm_d_TRG` au groupe* `Admins du domaine`, puis ouvrez une session* sur `DC-1` avec cet utilisateur.

Vous pouvez à présent désactiver le compte* `bluesky\Administrateur`, devenu inutile et même dangereux. En effet, ce compte non nominatif est souvent la cible d'attaques de type *brute force* et son mot de passe est en général changé trop rarement.

Créez les groupes de sécurité* sous l'OU `Groupes`, conformément à la Fig. 5. Ajoutez l'utilisateur* `adm_h_TRG` à ces deux groupes.

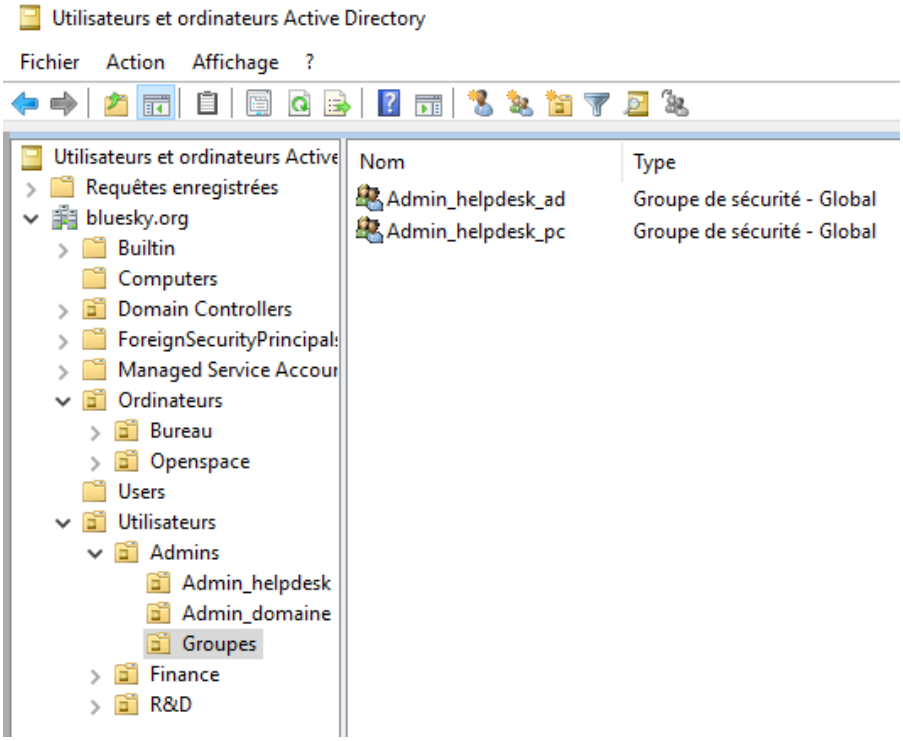

Fig. 7 *Groupes de sécurité pour le helpdesk*

La réorganisation de l'équipe d'administration est maintenant achevée. Il est temps de mettre en place la délégation de certains paramètres utilisateur au niveau Active Directory.

Nous allons permettre au *helpdesk* de gérer la GPO créée précédemment.

Ouvrez le gestionnaire des stratégies de groupe*, sélectionnez la GPO `Afficher les extensions` et déléguez sa modification* au groupe `Admin_helpdesk_ad`.

Connectez-vous sur un des deux postes de travail avec `adm_h_TRG` et réalisez quelques tests pour déterminer si vous êtes administrateur du poste. Faites de même avec `adm_d_TRG`.

Synthèse 2 : Résumez en 4-6 lignes ce que vous avez fait depuis la dernière synthèse.

Appelez votre chargé de TP pour discuter des points suivants :

- Dans un AD non configuré, quels comptes seront utilisés pour dépanner les utilisateurs ? En conséquence quels secrets vont rester en mémoire sur les postes de travail ?
- La méthode de délégation de la GPO au niveau de l'AD est-elle pertinente en termes de sécurité ? Pour répondre à cette question, pensez à qui peut contrôler maintenant cette GPO et sur qui elle s'applique. Que doit on corriger et comment ?

3. Mise en place du modèle de délégation sur les postes de travail

Dans cette partie, l'OU `Bureau` (avec le poste `BUREAU-3`) sera l'exemple de ce qu'il faut faire, avec la mise en place du Tier 2. En revanche, l'OU `Openspace` (avec `OPENSPACE-7`) sera le contre-exemple.

3.1. Mauvaise pratique

Commençons donc par mal faire les choses : ouvrez une session* sur `OPENSPACE-7` avec le compte `adm_d_TRG` et à l'aide du gestionnaire des utilisateurs et groupes locaux*, ajoutez les utilisateurs `adm_h_TRG` et `pinkman` au groupe (local) `Administrateurs`.

La délégation est ainsi réalisée sur `OPENSPACE-7` ! L'équipe *helpdesk* peut administrer le poste, tout comme l'utilisateur `pinkman` qui est un VIP et a exigé d'être administrateur … et peut installer tout ce qu'il veut sur son PC 😊

Ouvrez une session* sur `OPENSPACE-7` avec le compte `adm_h_TRG` et vérifiez que vous êtes administrateur du poste.

3.2. *Bonne pratique*

Voyons à présent comment bien faire les choses pour sécuriser l'accès à `BUREAU-3`. La bonne pratique consiste à créer une GPO* qui va ajouter automatiquement le groupe de sécurité `Admin_helpdesk_pc` au groupe local `Administrateurs`, sur tous les postes de travail de l'OU `Bureau`.

Bien évidemment, il existe une GPO pour gérer les groupes locaux* … *A vous de l'utiliser à bon escient !*

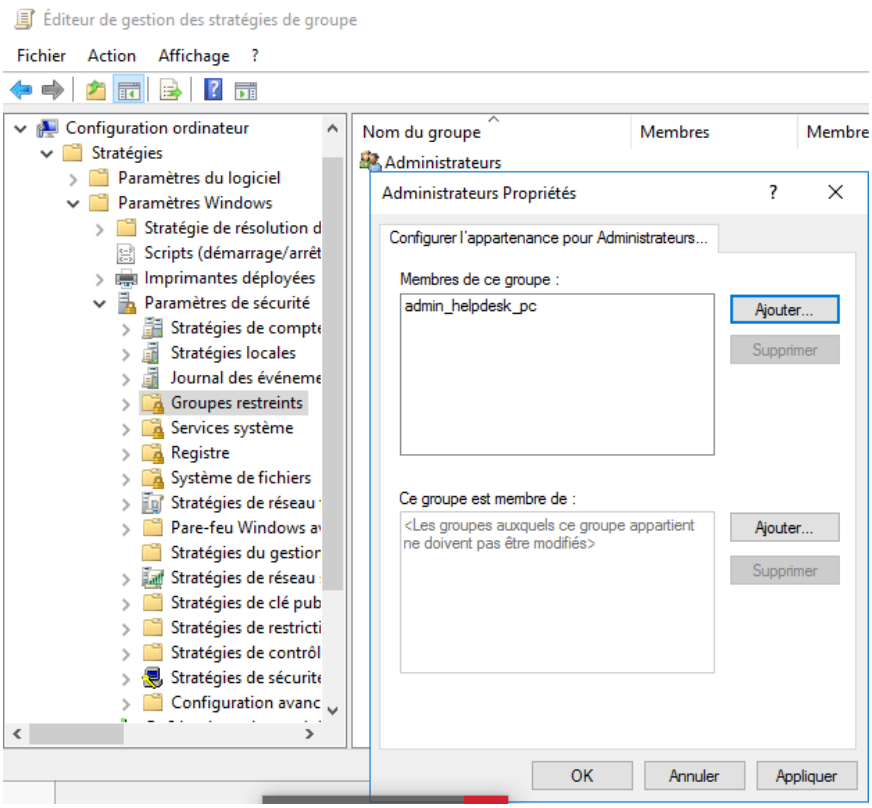

Fig. 8 *Stratégie de groupe restreint*

Quand vous aurez terminé la configuration de cette GPO, seul le groupe `Admin_helpdesk_pc` (en plus du compte par défaut `Administrateur` local et du

groupe Admins du domaine) sera membre du groupe local Administrateurs des postes de travail du Bureau.

Enfin, vous allez empêcher les Admins du domaine d'ouvrir une session sur les postes du Bureau. Pour protéger ces comptes à privilège, il faut éviter de les utiliser pour les interventions courantes, et préférer les comptes *helpdesk*.

Bien évidemment, il existe une GPO pour restreindre l'ouverture de session* … *A vous de l'utiliser à bon escient !*

Redémarrez BUREAU-3 pour que la nouvelle GPO s'applique. Essayez d'ouvrir une session* avec adm_d_TRG, puis avec adm_h_TRG.

Sur les deux postes de travail, ouvrez une session* avec pinkman et affichez la liste des administrateurs locaux*.

Synthèse 3 : Résumez en 4-6 lignes ce que vous avez fait depuis la dernière synthèse.

Appelez votre chargé de TP pour discuter des points suivants :

- Quel est le principal risque sur PC2 si pinkman ouvre une pièce jointe malveillante ?
- Pourquoi est-il préférable d'utiliser une GPO de groupes restreints (méthode utilisée sur BUREAU-3) plutôt que d'éditer directement le groupe local Administrateurs (méthode utilisée sur OPENSPACE-7) ?