LP-TP5-AD+-délégation – ECUE31
lundi 29 mars 2021

Amine ABDOUL-AZID
Martial SENE
Kavirajan SARAVANANE

198.51.2.17/24 PC1
198.51.2.203/24 PC2
198.51.2.3/24 VM AD

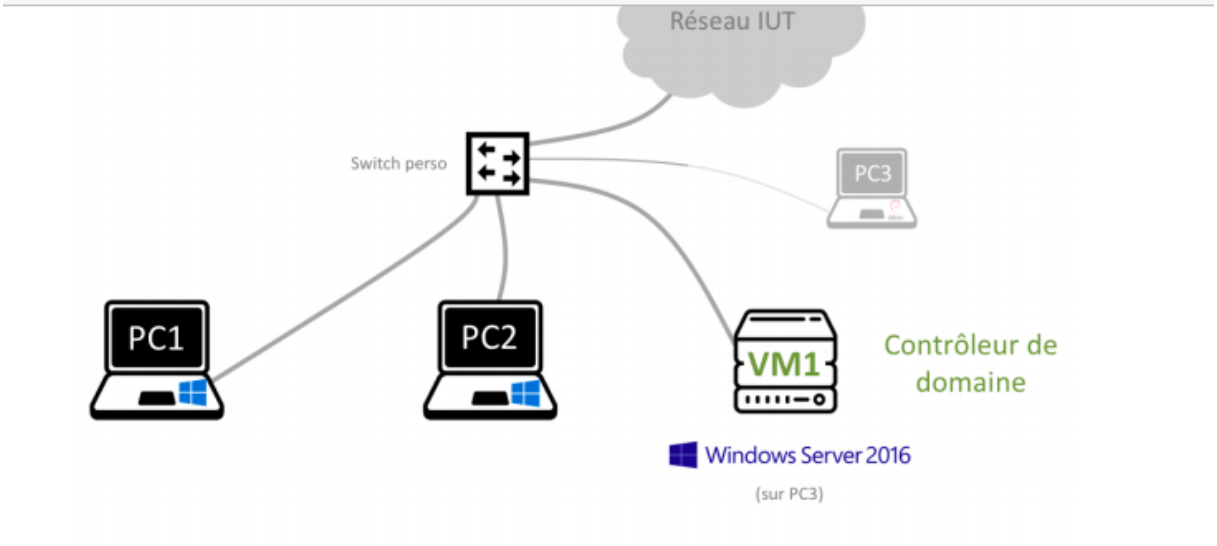


Fig. 3 *Maquette de TP*

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

Launch scripts 1-2-3 AD
Step4 bureau et openspace
Step 5 par GUI

GPO show_extension

Ouvrez le gestionnaire des stratégies de groupe*, et dans l'OU `Utilisateurs`, créez une GPO* que vous appellerez `Afficher les extensions`.

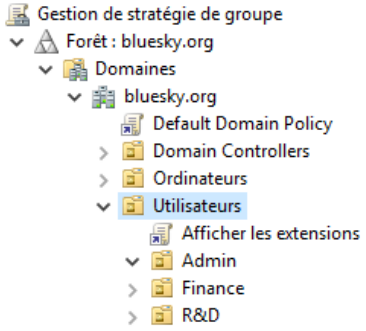


Fig. 6 *Ajout d'une GPO*

Pour l'instant elle ne contient aucun paramétrage particulier.

`Configuration utilisateur > Préférences > Paramètres du panneau de configuration > Options des dossiers`

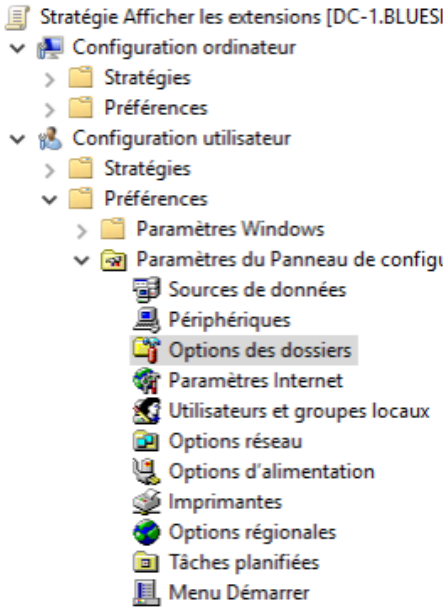


Fig. 7 *Emplacement d'une GPO*

3.1.3. Modifier le paramètre

3.1. Votre première GPO

Prenons un exemple simple : activer l'affichage des extensions de fichiers dans l'`Explorateur Windows`.

Vous avez peut-être remarqué que l'`Explorateur Windows 10` n'affiche pas les extensions de fichiers (`txt`, `exe`, etc.). Par exemple, dans la Fig. 5, le fichier texte `perlimpinpin.txt` apparait sans son extension.

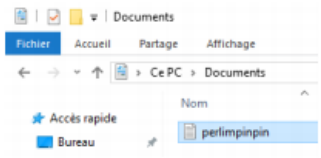


Fig. 5 *Fichier texte dont l'extension est masquée*

3.1.3. Modifier le paramètre

Dans la fenêtre de paramétrage, faites un clic droit > `Nouveau` > `Options des dossiers (au minimum Windows Vista)`

Décochez la case `Masquer les extensions des fichiers dont le type est connu`

Validez. C'est tout !

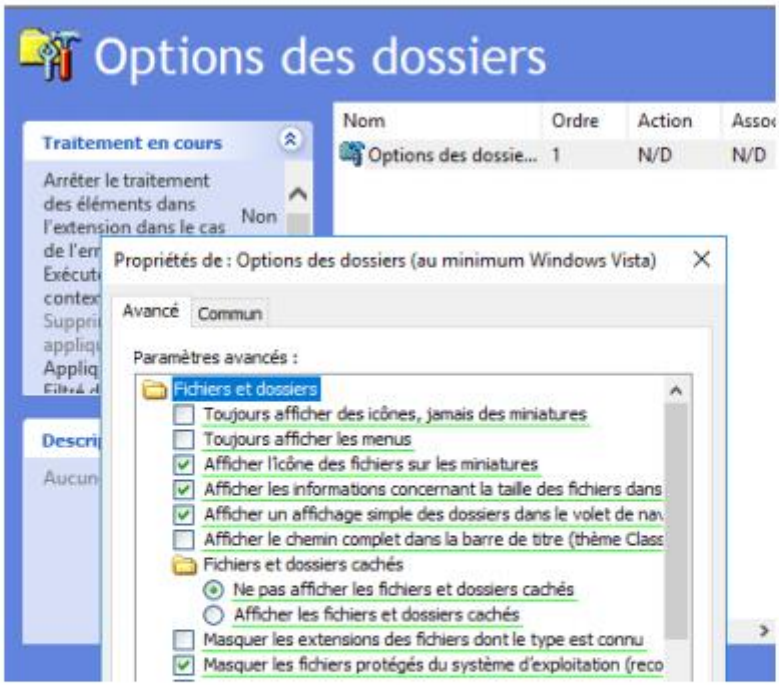


Fig. 8 *Paramétrage d'une GPO*

I. *Tester la GPO*

PO sont créées sur le contrôleur de domaine, mais ce sont les postes de travail

gpupdate /force && gpresult /v

test pinkman sur openspace-7PC1
test white sur bureau-3PC2

Synthèse 1 :

Après avoir restauré, configuré les IP, le DNS sur les clients PC1-PC2 comme adresse de la VM AD.

J'ai réalisé les différentes étapes 1-5. Pour configurer le contrôleur et les clients AD.

J'ai réalisé une GPO. J'ai testé les différents utilisateurs et cela fonctionne.

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

adm_h_AAB == user

adm_d_AAB == user2

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)

Ouverture de session : adm_d_AAB sur VM AD

Désactiver l'user ~~adm_d_AAB~~ bluesky\Administrateur :

> Gérer les utilisateurs et ordinateurs du domaine :
>
> Dans le `Gestionnaire de serveur`, cliquer sur `Outils` > `Utilisateurs et ordinateurs Active Directory`
>
> *La suite est facile à trouver !*

Désactiver un utilisateur :

Windows Server 2016 1

Ouvrir le gestionnaire des utilisateurs et ordinateurs du domaine*.
Clic droit sur l'utilisateur > `Désactiver`

Créer un groupe de sécurité dans l'OU `Laverie` :

Ouvrir le gestionnaire des utilisateurs et ordinateurs du domaine*.
Clic droit sur l'OU `Laverie` > `Ajouter` > `Groupe`
Indiquer le nom du groupe et laisser les autres paramètres par défaut.

Ajouter un utilisateur à un groupe :

Ouvrir le gestionnaire des utilisateurs et ordinateurs du domaine*.
Clic droit sur le groupe > `Propriétés` > `Membres` > Ajouter l'utilisateur

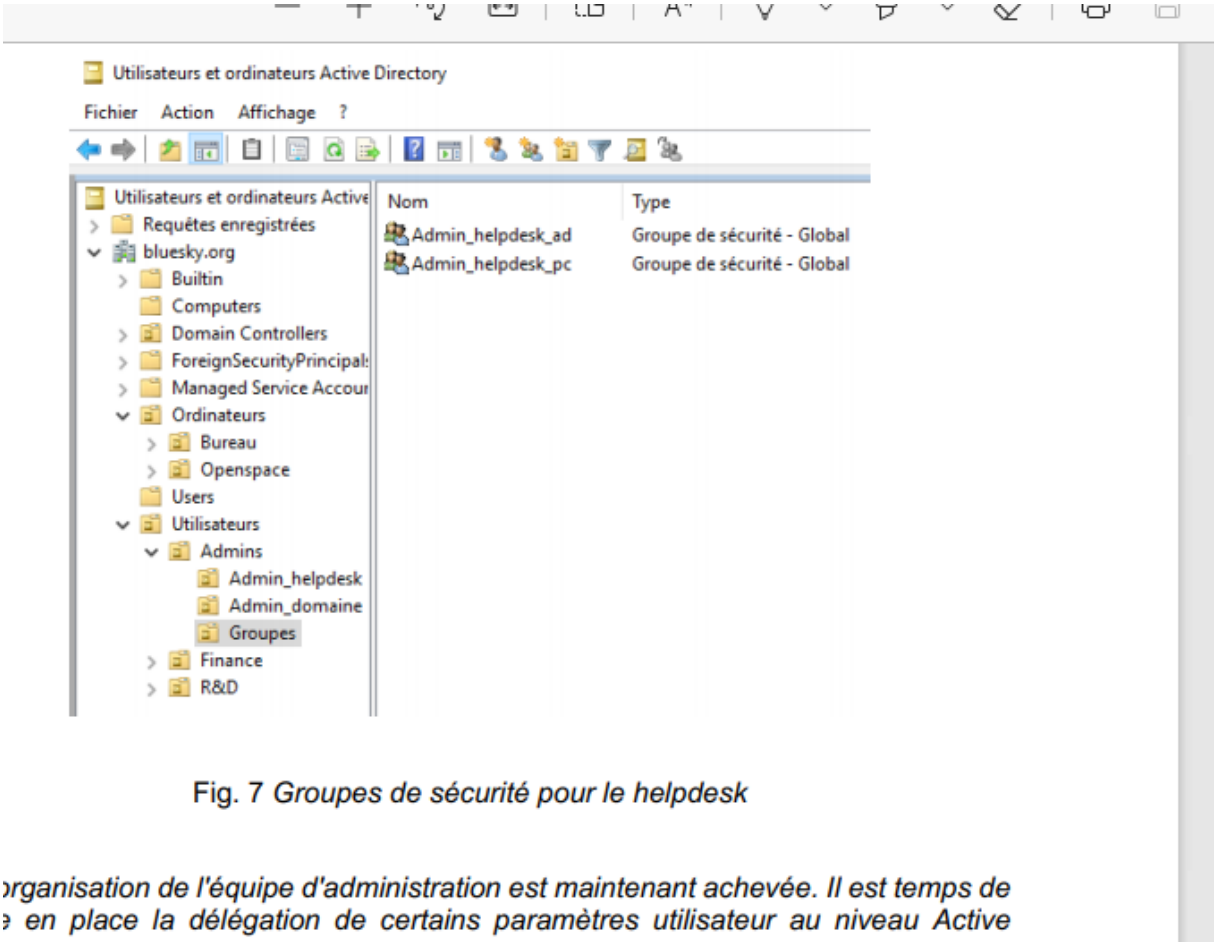


Fig. 7 *Groupes de sécurité pour le helpdesk*

rganisation de l'équipe d'administration est maintenant achevée. Il est temps de
e en place la délégation de certains paramètres utilisateur au niveau Active

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`.

Attention voir + bas :

~~Windows+R > lusrmgr.msc~~

Ouvrir le gestionnaire des utilisateurs et groupes locaux :

```
Windows+R > lusrmgr.msc
```

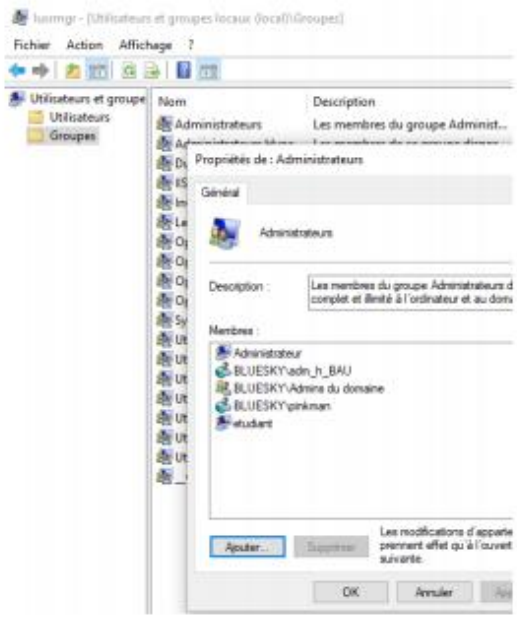
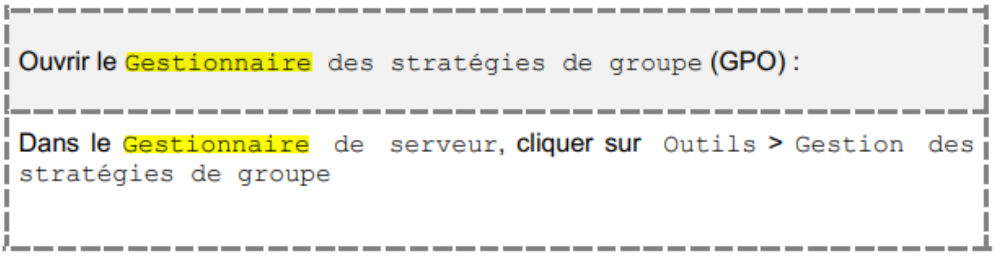
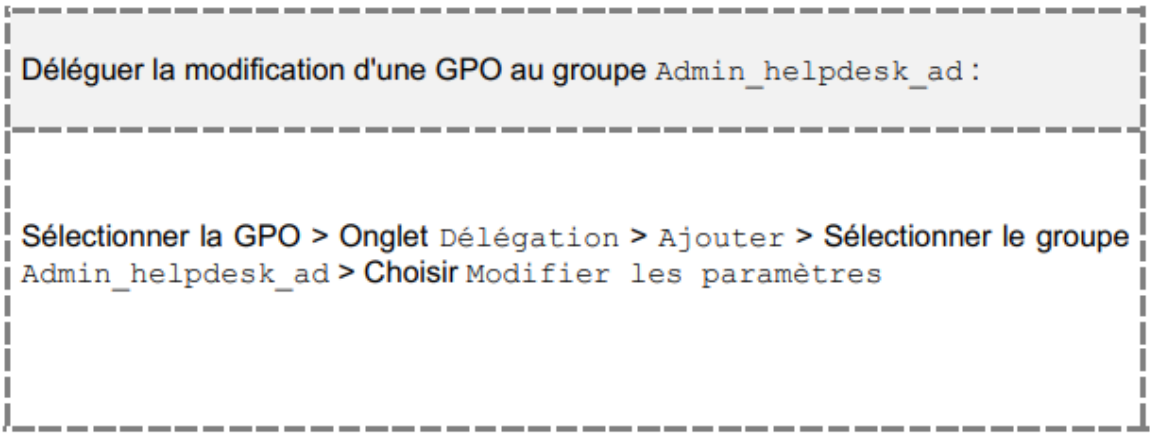


Fig. 48 *Gestion du groupe local* `Administrateurs`

Plutôt celui la



Gpo show_extension :



L'user adm_h_AAB -> dans le groupe GROUPES/Admin_helpdesk_ad. On arrive à modifier la GPO show_extension

L'user adm_d_AAB fait partie du groupe admins du domaine par conséquent cela ne fonctionne pas.

- 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 ?

Dans un AD mal configuré, le secret qui va rester est le condensat, c'est-à-dire l'équivalent d'un token qui permettrait d'ouvrir la session vu qu'elle reste sur la ROM ou RAM avant Windows 2012R2 cette faille était exploitable.

A partir d'une faille, en effet l'élévation de privilège sera possible.

Les conséquences peuvent êtres, faux log, des heures fausses avec le NTP, un ransomware, des fuites de données, attaque du SSO qui est stocké dans lsass.exe, modification des registres, demande TGT type attaque par golden ticket…

- 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 ?

La délégation de l'AD permet de contrôler les droits et le couplé à la méthode des tiers permettra d'éviter que des attaquants ont un haut de niveau de privilège.

La GPO peut-être contrôler par l'admin_helpdesk du Tier2 (l'utilisateur adm_h_AAB), le groupe admin_helpdesk_pc et admin_helpdesk_ad avec l'utilisateur adm_h_AAB et admin_domaine du tier1 (l'utilisateur adm_d_AAB). Elle s'applique sur le tier 2 le groupe admin_helpdesk , le groupe admin_helpdesk_pc et admin_helpdesk_ad avec l'utilisateur adm_h_AAB.

On doit corriger les droits auxquels les postes sont autorisés à se connecter à ce groupe/utilisateurs.

Et le compte adm_h_AAB est à la fois dans un OU et dans un groupe.

Synthèse 2 :

On réorganise l'OU Admins de manière légère selon le cahier des charges avec le groupe et les utilisateurs respectives. On ouvre la session avec le compte admin du tier 1 et on désactive le compte par défaut de BLUESKY. On a créé les groupes de sécurité depuis l'OU groupes et l'user adm_h_AAB.

Enfin on a délégué à l'admin helpdesk la modification de la GPO.

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.

~~Windows+R > lusrmgr.msc~~

Ouvrir le gestionnaire des utilisateurs et groupes locaux :

```
Windows+R > lusrmgr.msc
```

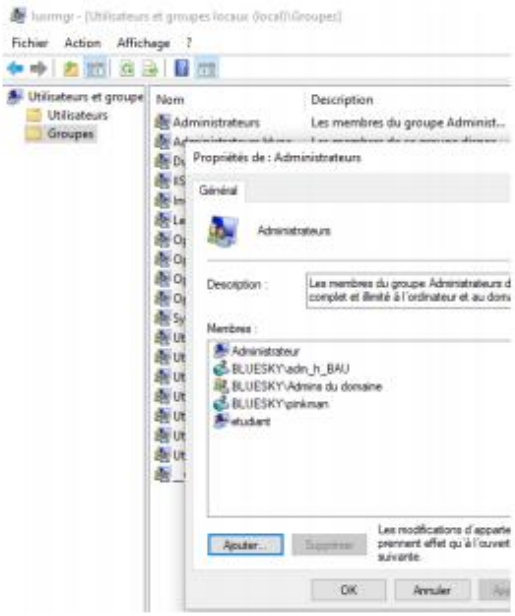


Fig. 48 *Gestion du groupe local* `Administrateurs`

Ajout de pinkman et de **adm_h_AAB**

Avec adm_h_AAB sur OPENSPACE-7:PC1, on est administrateurs, quand on a ouvert la session.

PR !! Doit-on effacer ces règles ?? précédentes

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 !*

Gérer les groupes locaux :

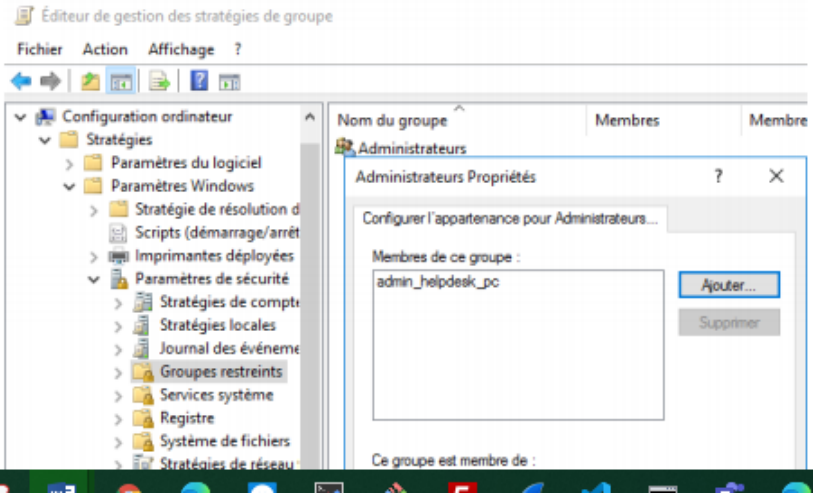
Type : GPO Ordinateur

Emplacement :

`Configuration d'ordinateur` > `Stratégies` > `Paramètres Windows` > `Paramètres de sécurité` > `Groupes restreints`

Paramétrage :

Clic droit > `Ajouter un groupe` > Choisir le groupe local à modifier > `Membres de ce groupe` > Choisir le groupe de sécurité à ajouter



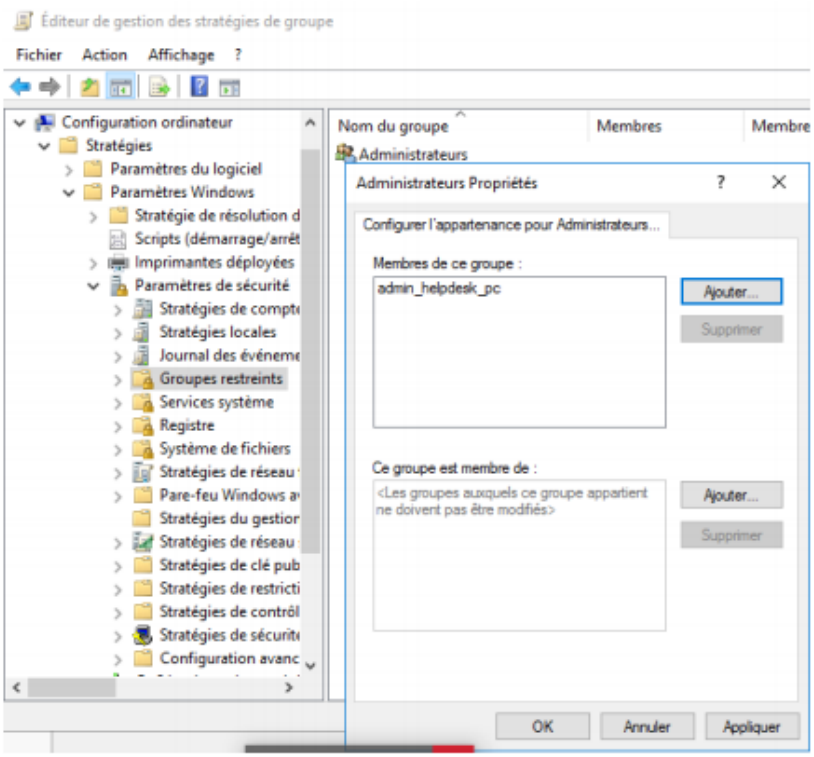


Fig. 8 *Stratégie de groupe restreint*

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 !*

Restreindre l'ouverture de session :

Type : GPO Ordinateur

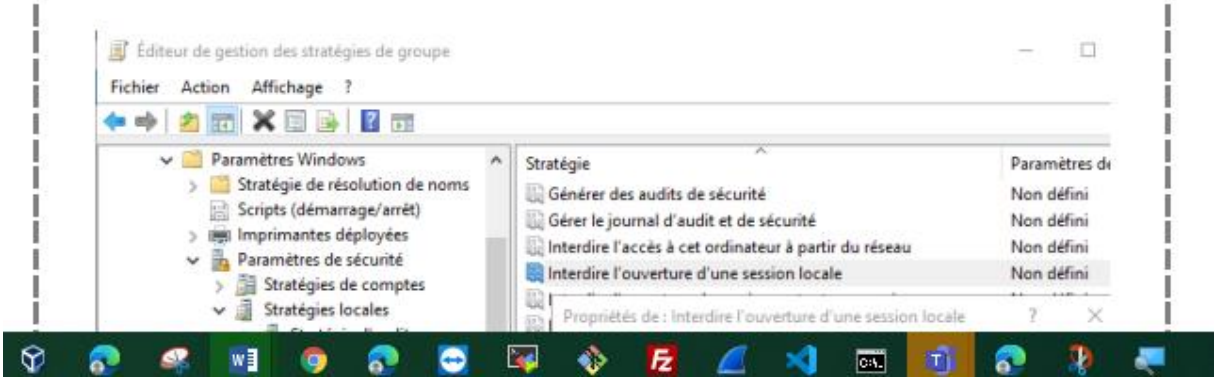
Emplacement :

Configuration d'ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur

Paramétrage :

Paramètres à modifier :

- Interdire l'ouverture de session locale
- Interdire l'ouverture de session par les services Bureau à distance



- Interdire l'ouverture de session par les services Bureau à distance

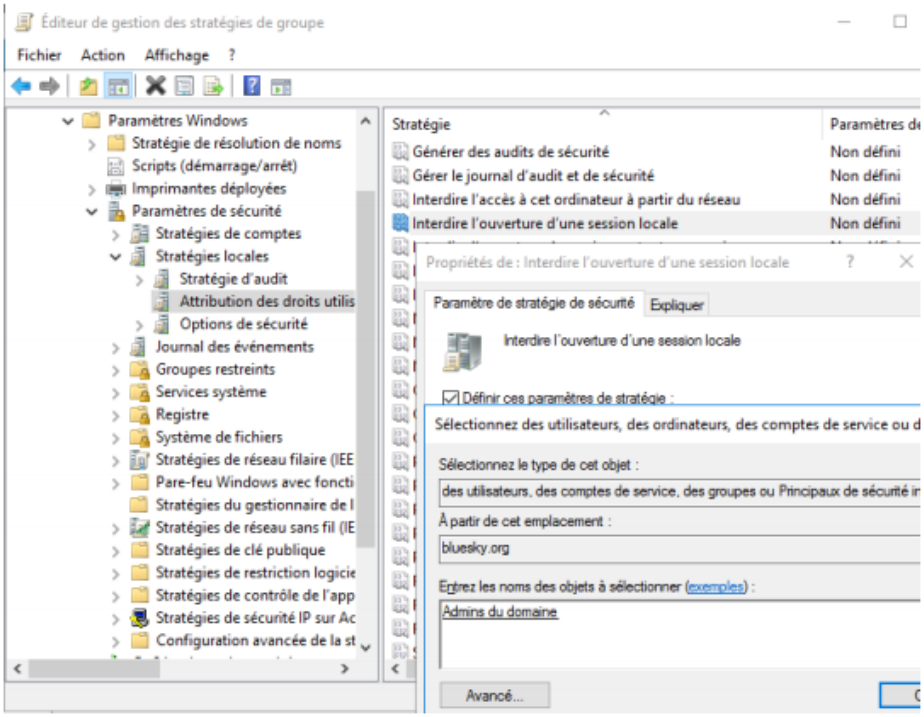


Fig. 53 *Interdire l'ouverture de session locale aux* `Admins du domaine`

shutdown /r sur BUREAU3:PC2 afin de redémarrer

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*.

adm_d_AAB!Admin_domaine: -BUREAU-3*PC2 fonctionne peut-être pas

adm_h_TRG!Admin_helpdesk: -BUREAU-3*PC2 fonctionne

pinkman^R&D:Openspace-7*PC1-BUREAU-3*PC2 et on liste les administrateurs locaux

```
net localgroup Administrateurs
```

Dans cet exemple, les `Administrateurs` locaux sont :

- Les utilisateurs locaux `Administrateur` et `etudiant`
- Les utilisateurs Active Directory `adm_h_BAU` et `pinkman`
- Le groupe Active Directory `Admins du domaine`

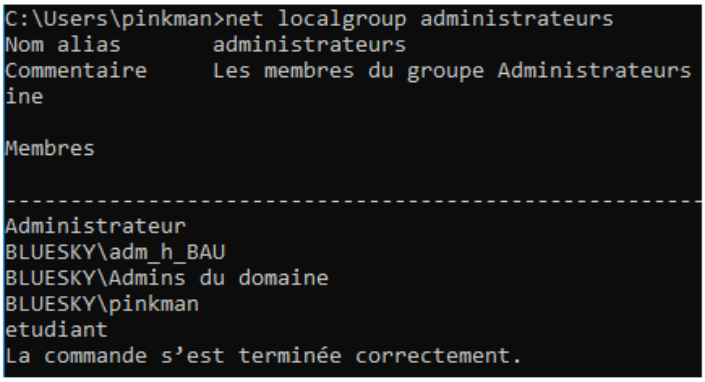


Fig. 49 *Gestion du groupe local* `Administrateurs`

net localgroup Administateurs

ou

~~Windows+R > lusrmgr.msc~~

Ouvrir le gestionnaire des utilisateurs et groupes locaux :

Windows+R > lusrmgr.msc

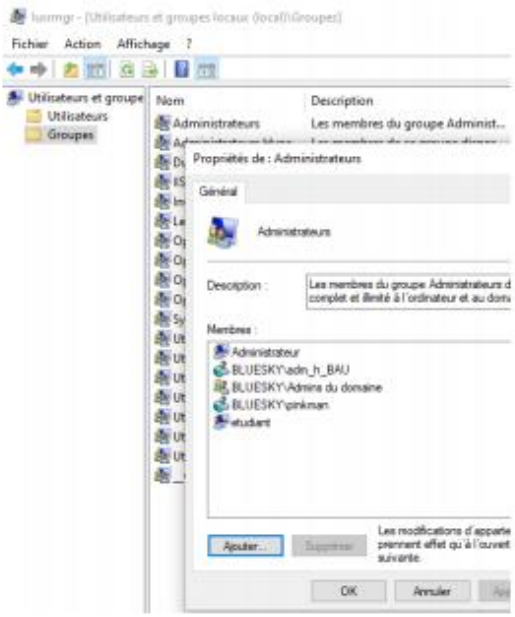


Fig. 48 *Gestion du groupe local* `Administrateurs`

- Quel est le principal risque sur PC2 si pinkman ouvre une pièce jointe malveillante ?

Pinkman infecte le compte administrateurs et par conséquent l'ensemble du réseau, il y a un risque d'exploitation des failles pour saboter l'ACTIVE Directory et les PC.

- 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) ?

Les groupes restreints sont partiellement administrateurs et ont une partie des GPO qui sont délégués dans notre cas : Le helpdesk peut gérer la GPO show_extension mais plus souvent dans les cas réel ils gèrent la réinitialisation des mots de passes. L'édition du groupe local est à bannir car cette méthode est dangereuse. D'ailleurs il faudrait bloquer l'accès à partir d'une GPO pour le groupe local.

Synthèse 3 :

J'ai vu les bonnes pratiques sur PC2 et les mauvaises pratiques sur PC1, cela nous sensibilise à éviter les portes dérobés.
Par conséquent les GPO, sont plus + pratiques pour gérer les groupes locaux et ajouter l'administrateur_helpdesk_pc et retsreindre l'ouverture de session et par bureau à distance par conséquent cela évite de désactiver le compte et de passer par le helpdesk sur le BUREAU-3:PC2

Synthèse 4 :

Au cours de ce TP, nous avons travaillé sur l'ACTIVE DIRECTORY, à partir des scripts du précédent TP, nous avons eu un gain de temps.

Désormais on a mis une arborescence sous le modèle tier et j'ai privilégié les groupes au lieu des OU. On a vu la délégation des rôles, les groupes de sécurité. Et le gestionnaire de groupes locaux. OPENSPACE-7:PC1 peut faire une « escalation of privileges » ainsi pinkman est un admin VIP. Enfin on a mis des GPO afin de restreindre les droits.