LP-TP3-AD+-délégation – ECUE31

mercredi 24 mars 2021

Amine ABDOUL-AZID

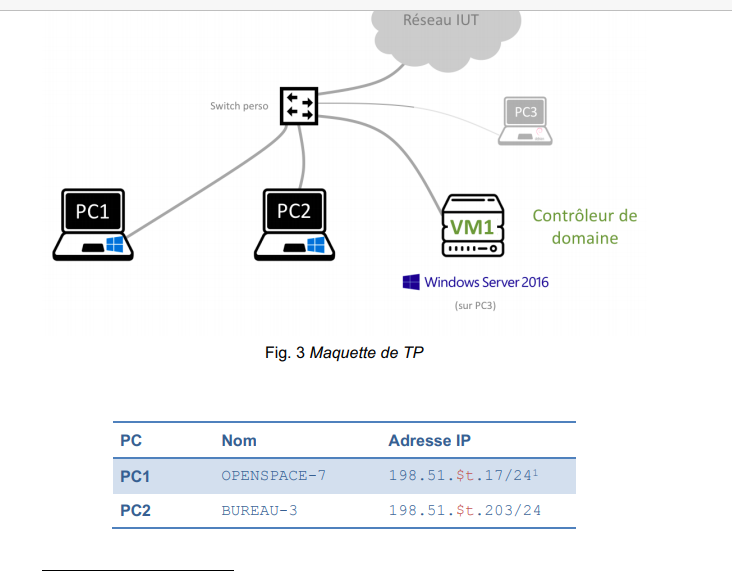
Martial SENE

Kavirajan SARAVANANE

198.51.2.17/24 PC1

198.51.2.203/24 PC2

198.51.2.3/24 VM AD

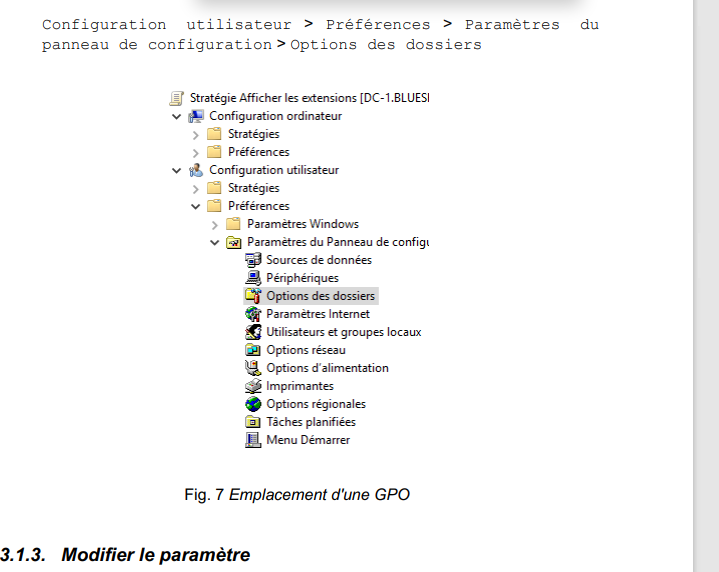
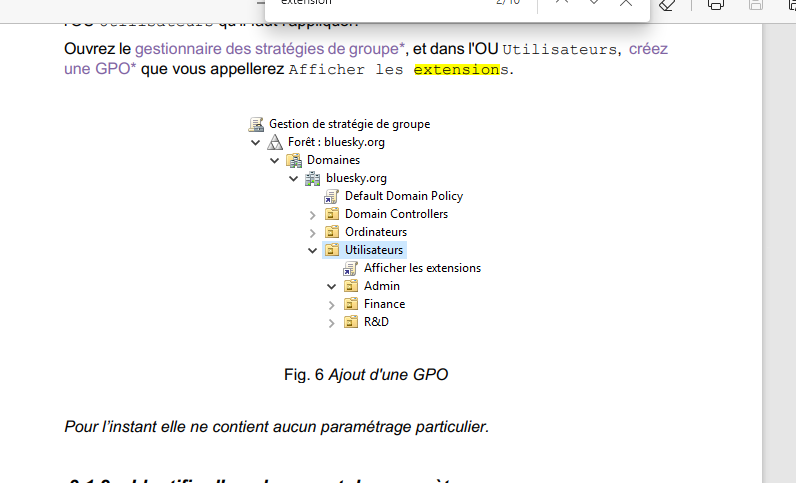


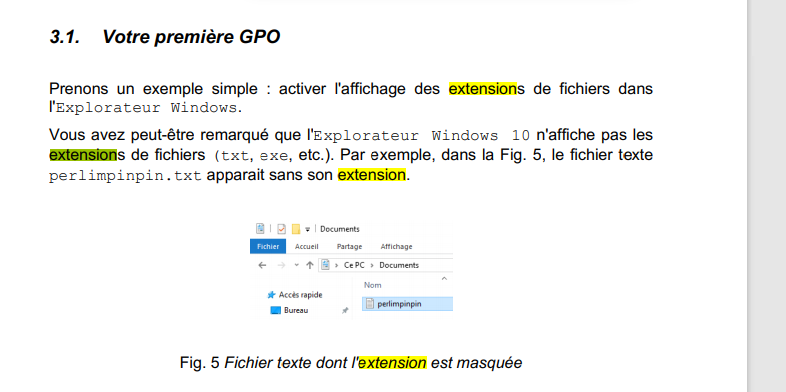
Launch scripts 1-2-3 AD

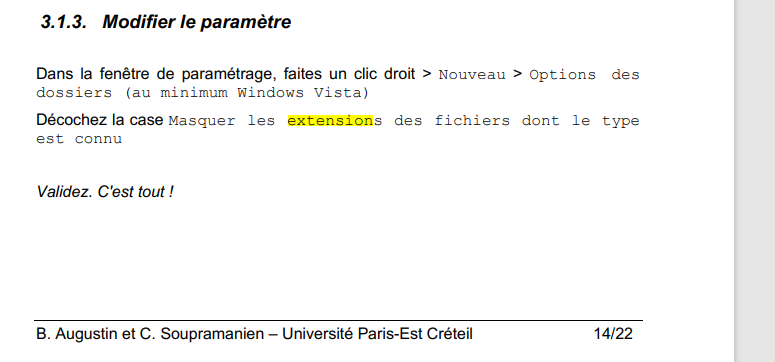
Step4 bureau et openspace

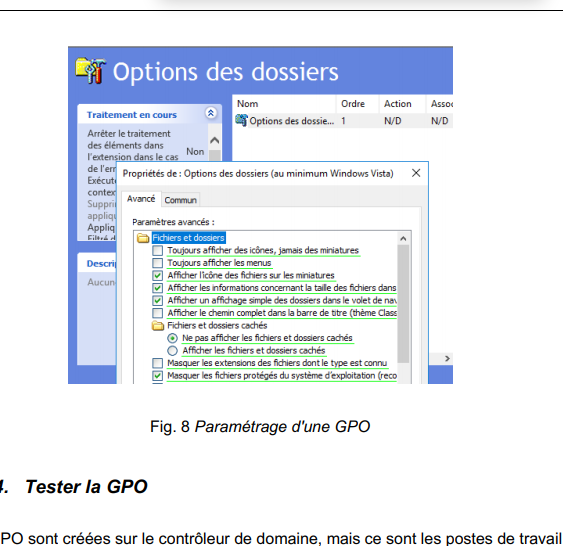
Step 5 par GUI

GPO show\_extension









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.



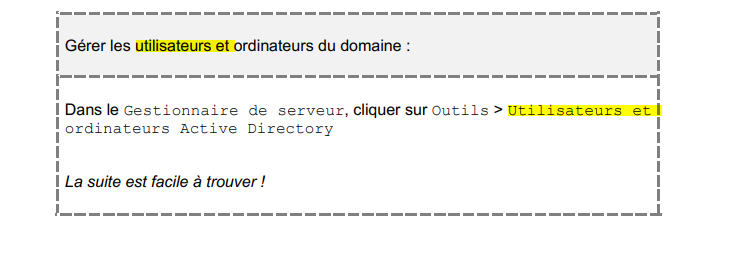
adm\_h\_AAA == user

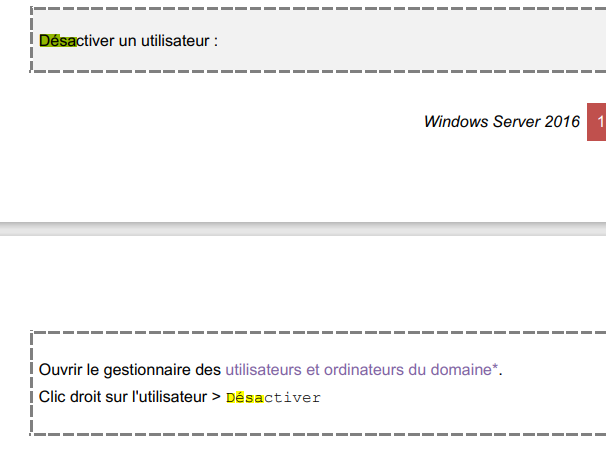
adm\_d\_AAA == user2

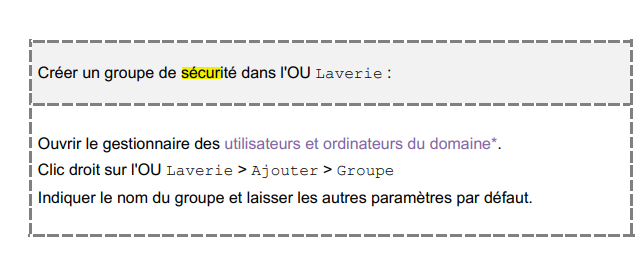
Ouvrez une session\* sur DC-1 avec le compte bluesky\Administrateur, puis créez les OU\* comme indiqué précédemment. Ensuite, créez les deux nouveaux utilisateurs\* dans leur OU respective (Fig. 5 et 6)

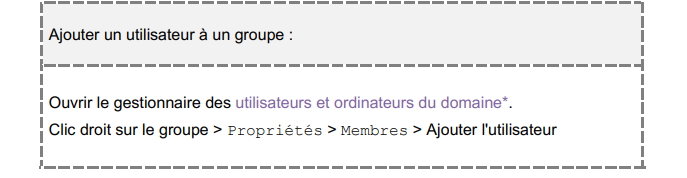
Ouverture de session : adm\_d\_AAA sur VM AD

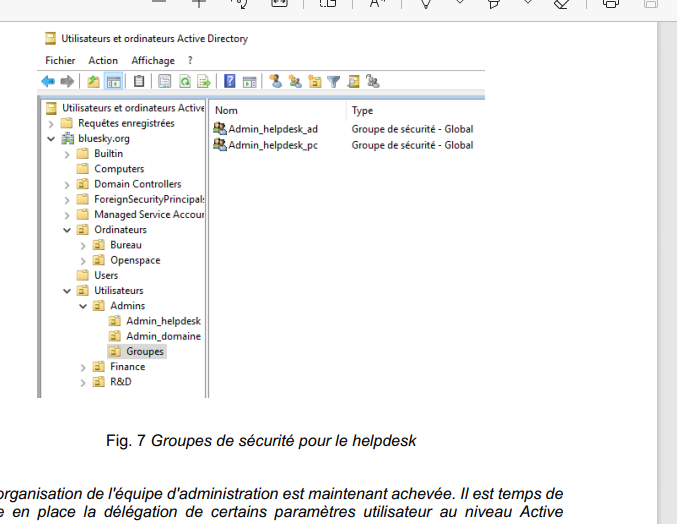
Désactiver l’user adm\_d\_AAA :

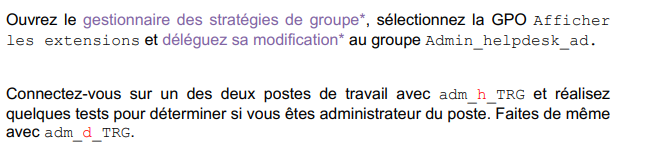






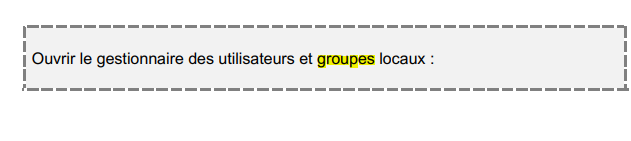


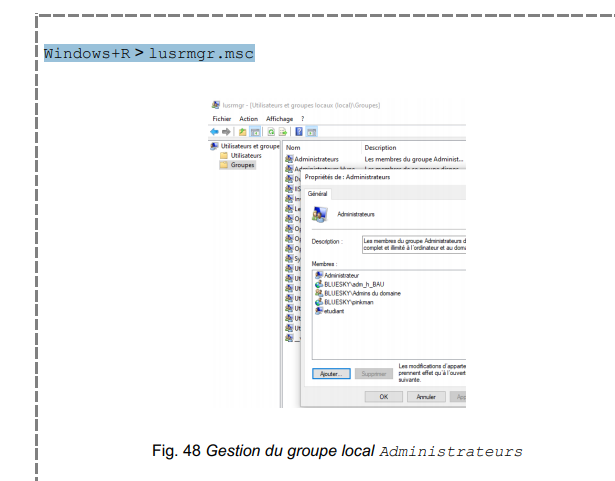




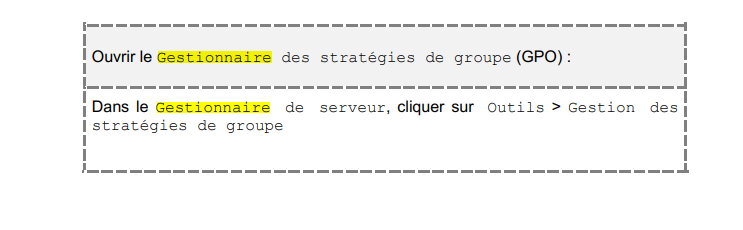
Attention voir + bas :

~~Windows+R > lusrmgr.msc~~

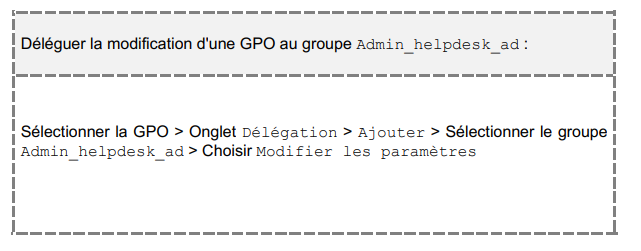




Plutôt celui la



Gpo show\_extension :



**L’user adm\_h\_AAA -> dans le groupe GROUPES/Admin\_helpdesk\_ad.** On arrive à modifier la GPO show\_extension

L’user adm\_d\_AAA 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\_AAA), le groupe admin\_helpdesk\_pc et admin\_helpdesk\_ad avec l’utilisateur adm\_h\_AAA et admin\_domaine du tier1 (l’utilisateur adm\_d\_AAA). 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\_AAA.

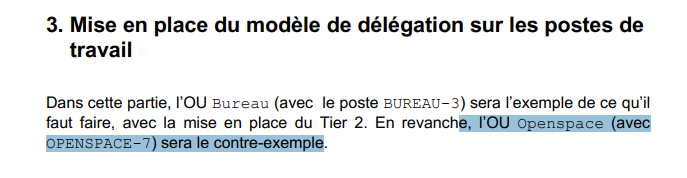
On doit corriger les droits auxquels les postes sont autorisés à se connecter à ce groupe/utilisateurs.

Et le compte adm\_h\_AAA est à la fois dans un OU et dans un groupe.

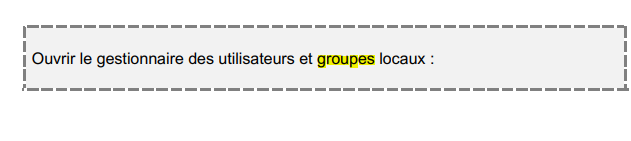
**Synthèse 2 :**

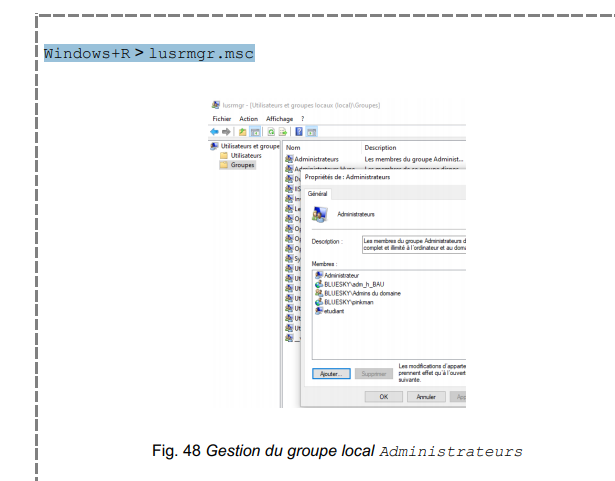
On réorganise l’OU Admins de manière légère selon le cahier des charges avec le groupe et les utilisateurs respectives. On ouvre la session avec le compte admin du tier 1 et on désactive le compte par défaut de BLUESKY. On a créé les groupes de sécurité depuis l’OU groupes et l’user adm\_h\_AAA.

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



~~Windows+R > lusrmgr.msc~~

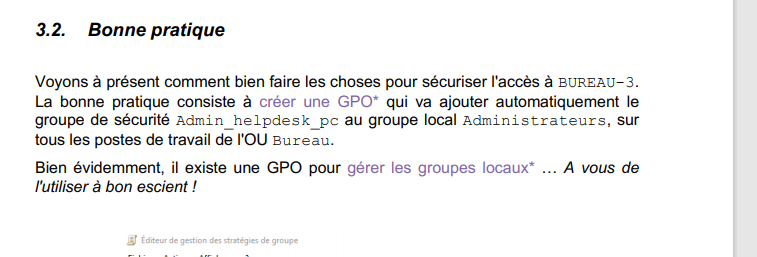


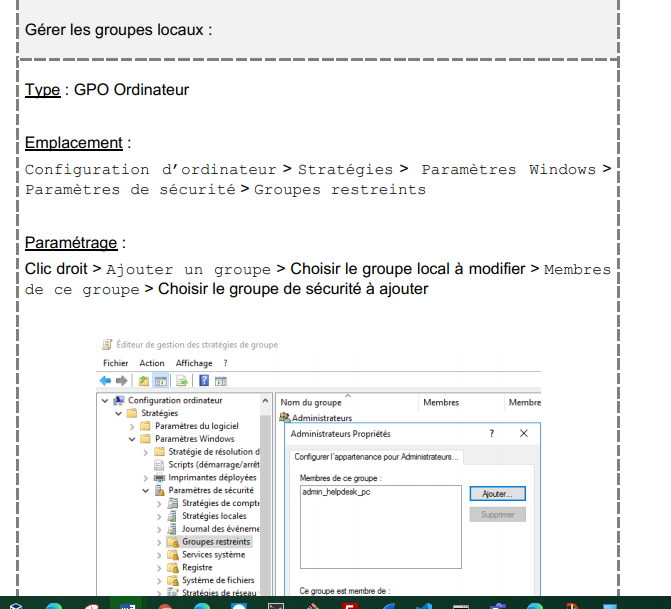


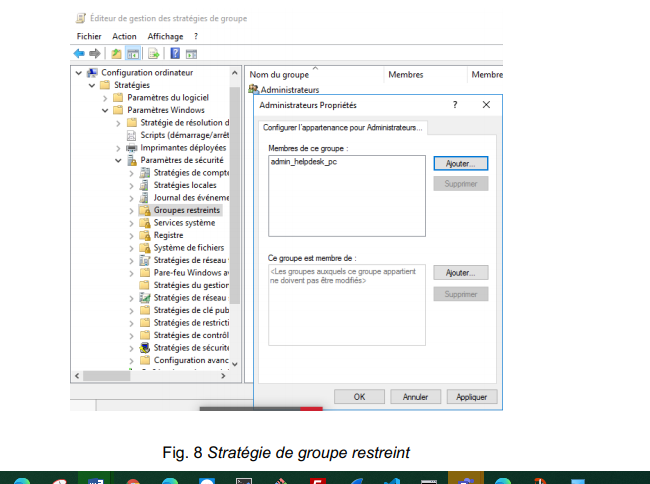
Ajout de pinkman et de **adm\_h\_AAA**

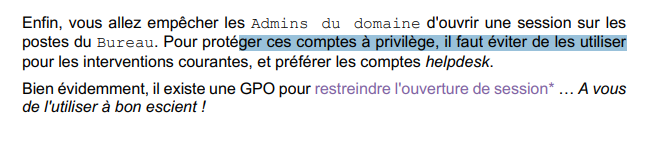
**Avec adm\_h\_AAA sur OPENSPACE-7:PC1, on est administrateurs, quand on a ouvert la session.**

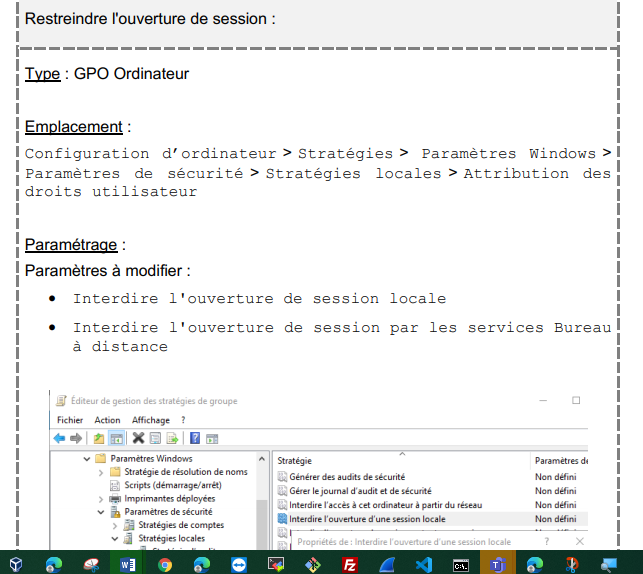
**PR !! Doit-on effacer ces règles ?? précédentes**

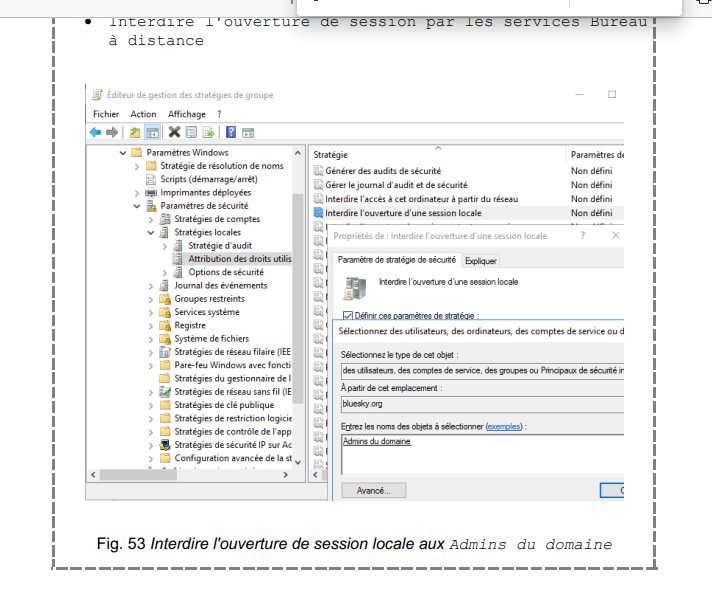
****

****

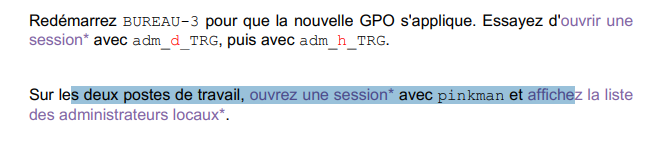
****

****





shutdown /r sur BUREAU3:PC2 afin de redémarrer



adm\_d\_AAA!Admin\_domaine: -BUREAU-3\*PC2 fonctionne peut-être pas

adm\_h\_TRG!Admin\_helpdesk: -BUREAU-3\*PC2 fonctionne

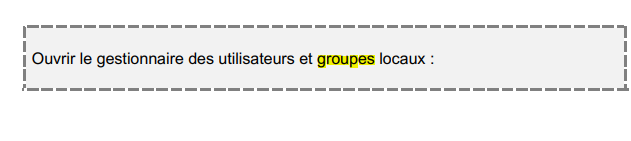
pinkman^R&D:Openspace-7\*PC1-BUREAU-3\*PC2 et on liste les administrateurs locaux

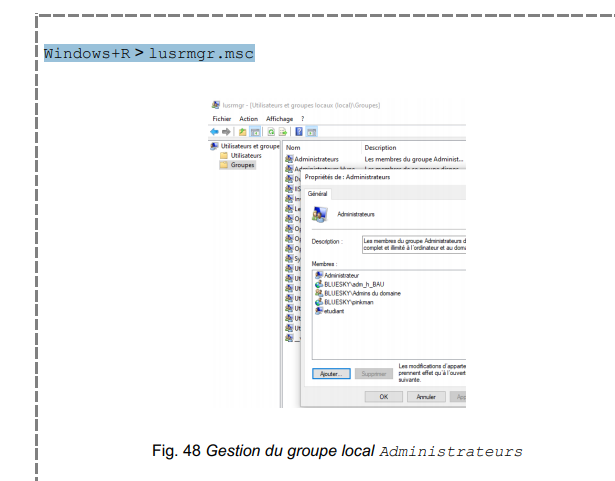


net localgroup Administateurs

ou

~~Windows+R > lusrmgr.msc~~





* 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.