LP-TP5-AD+-délégation – ECUE31

mardi 30 mars 2021

Amine ABDOUL-AZID

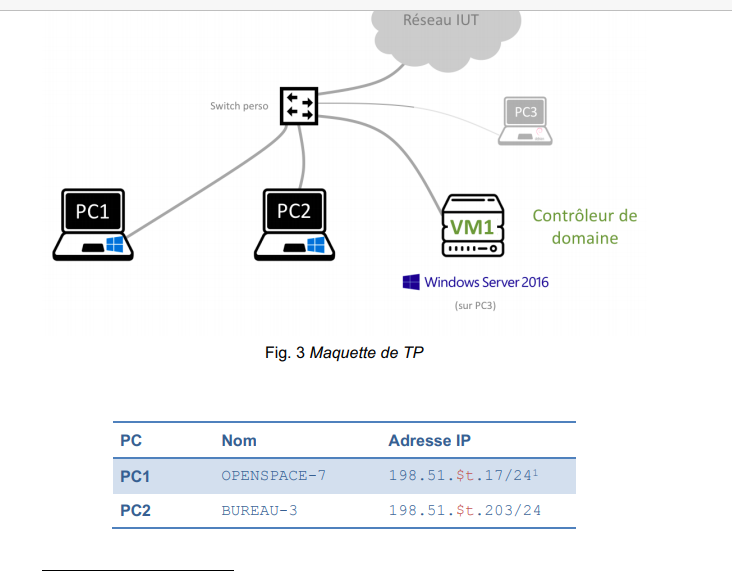
~~Martial SENE~~

~~Kavirajan SARAVANANE~~

198.51.2.17/24 PC1

198.51.2.203/24 PC2

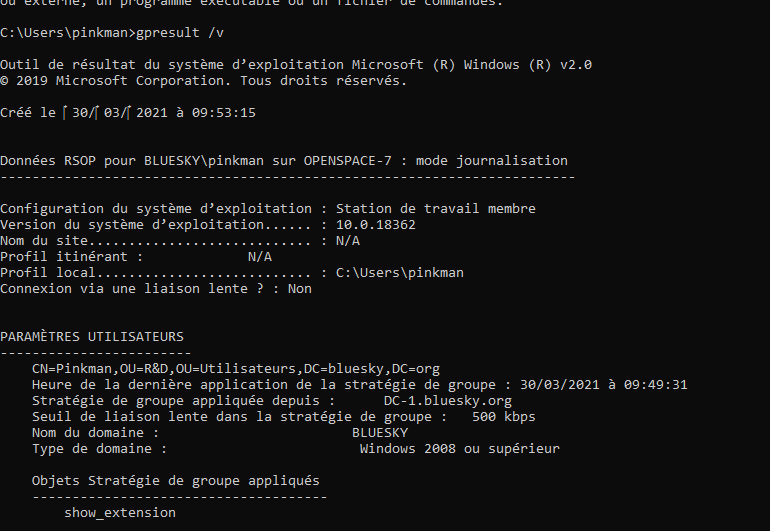
198.51.2.3/24 VM AD

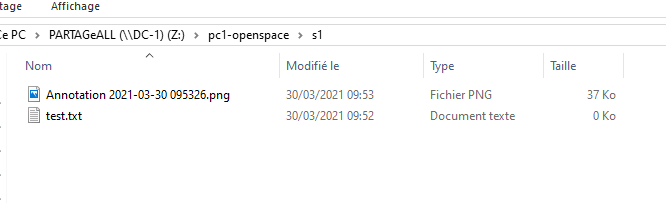


On a lancé : gpupdate /force && gpresult /v

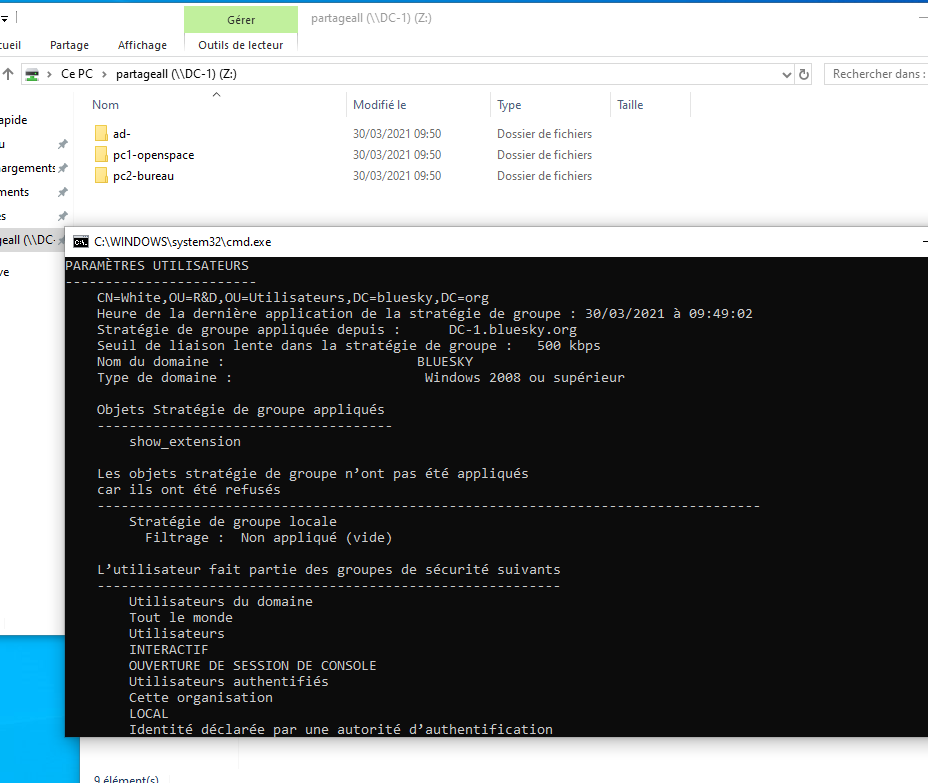
On a testé avec :

pinkman sur openspace-7(PC1) :





Sur white sur bureau-3(PC2) :



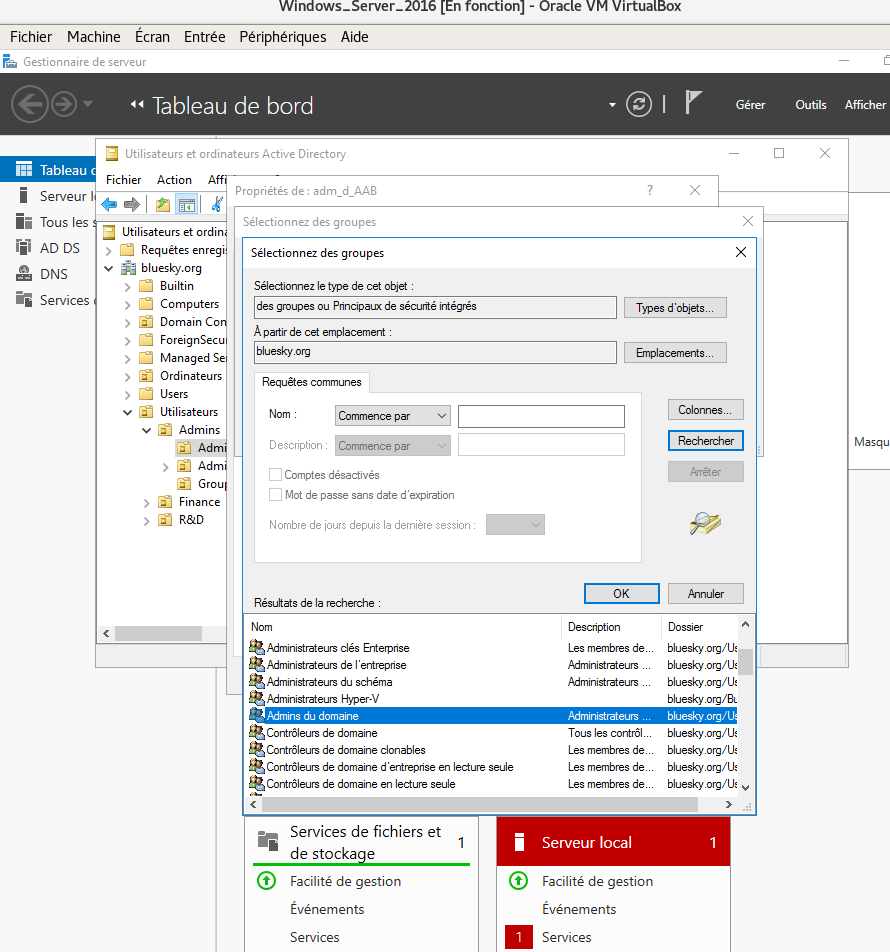
**Synthèse 1 :**

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

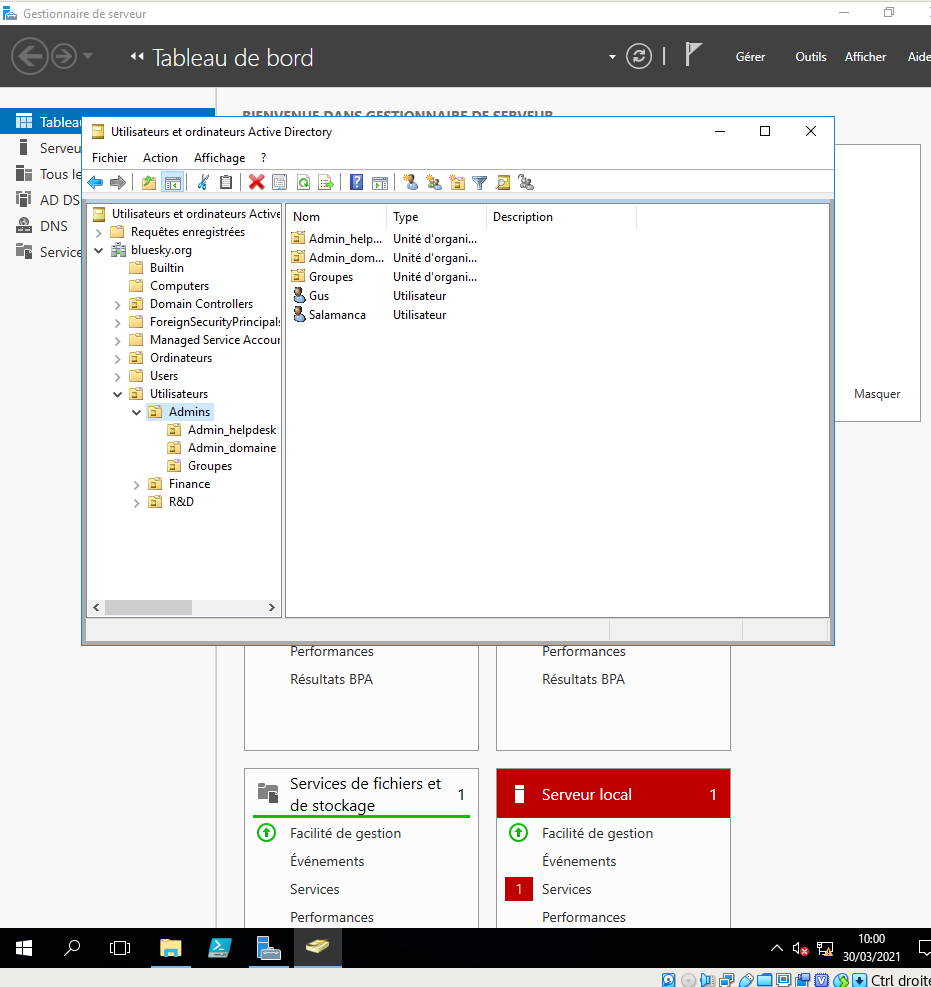
J’ai réalisé les différentes étapes 1-5. Pour configurer le contrôleur et les clients AD.

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

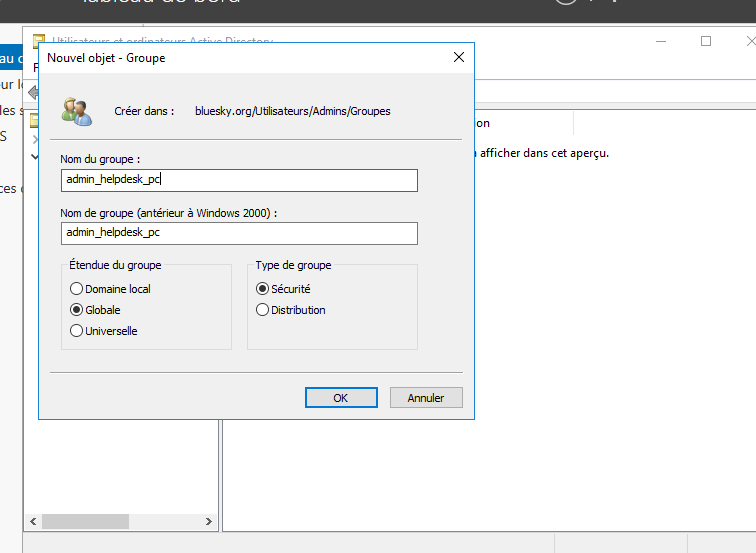
Ajout du compte adm\_d\_AAA au groupe Admins du domaine :



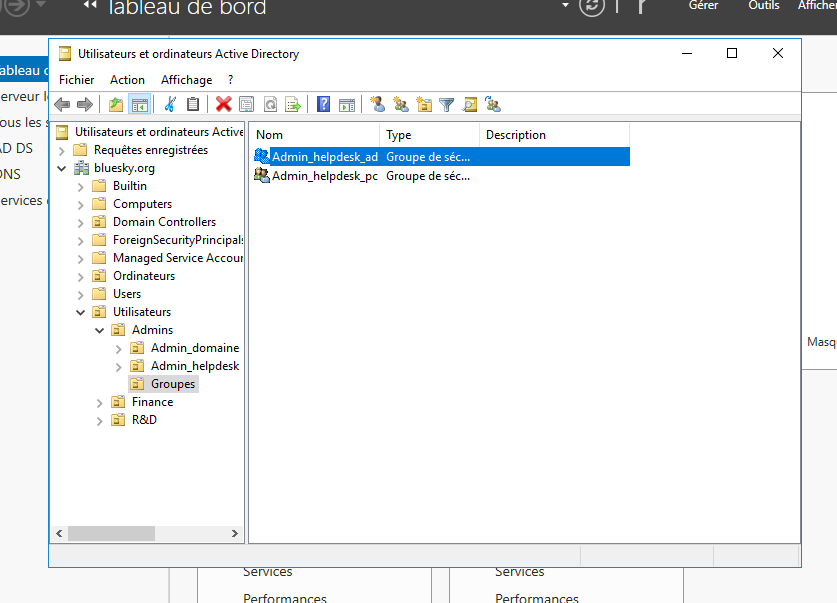
Listes OU Admins :



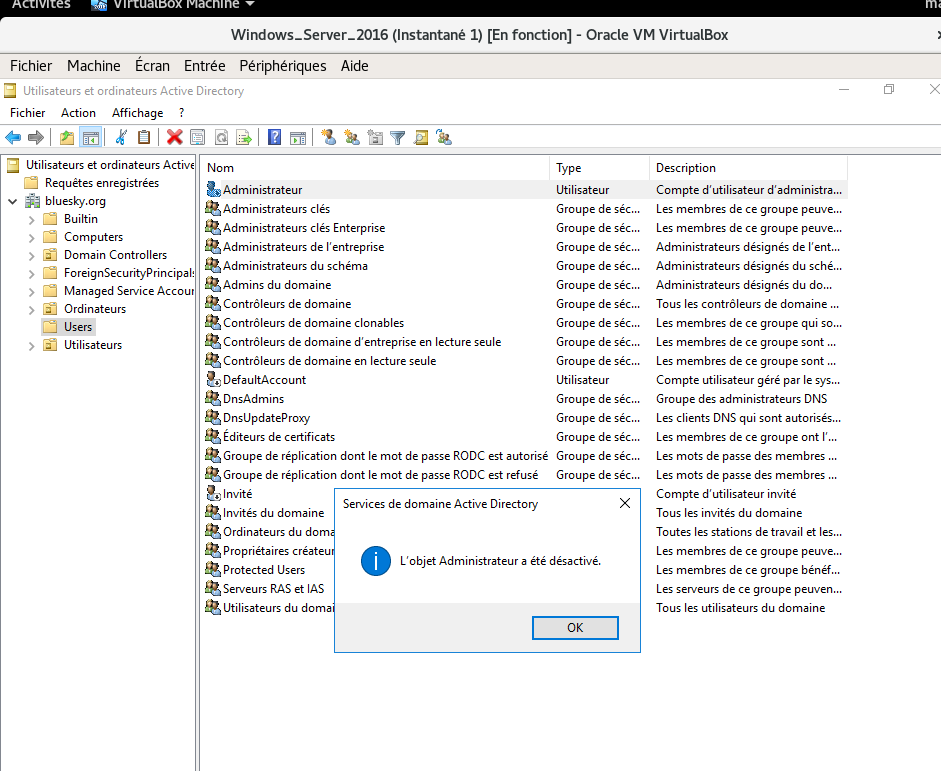
Avec le groupe :



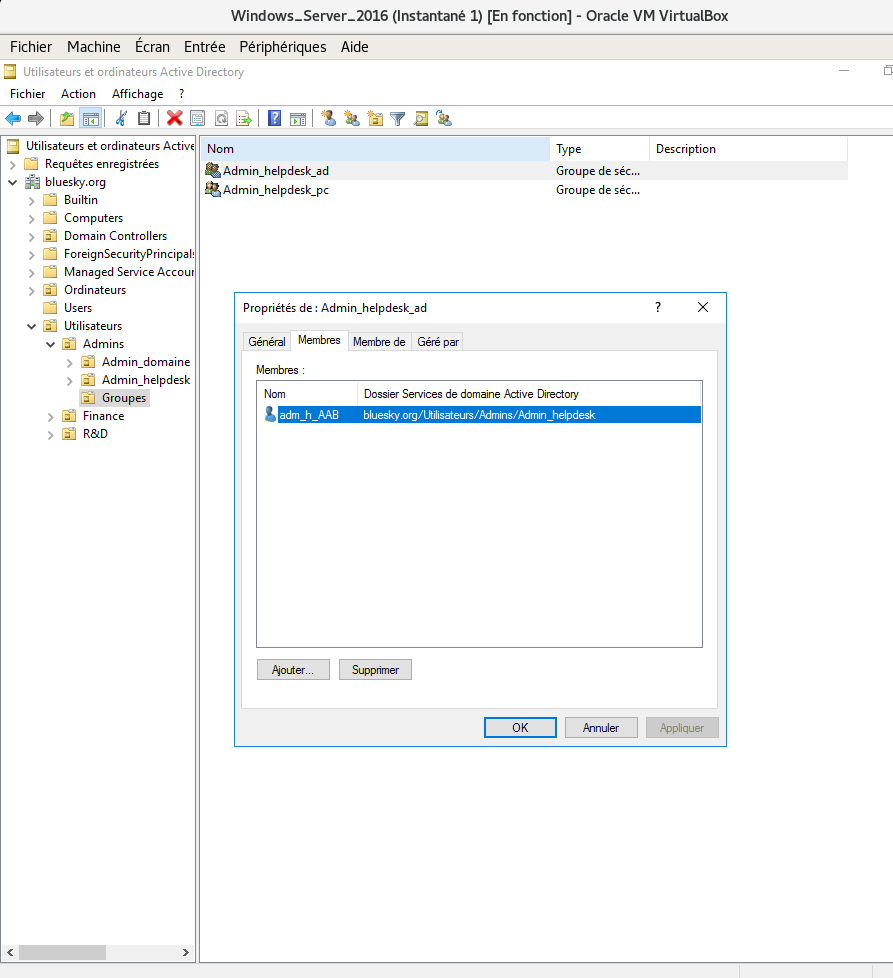
Liste de l’OU Groupes :



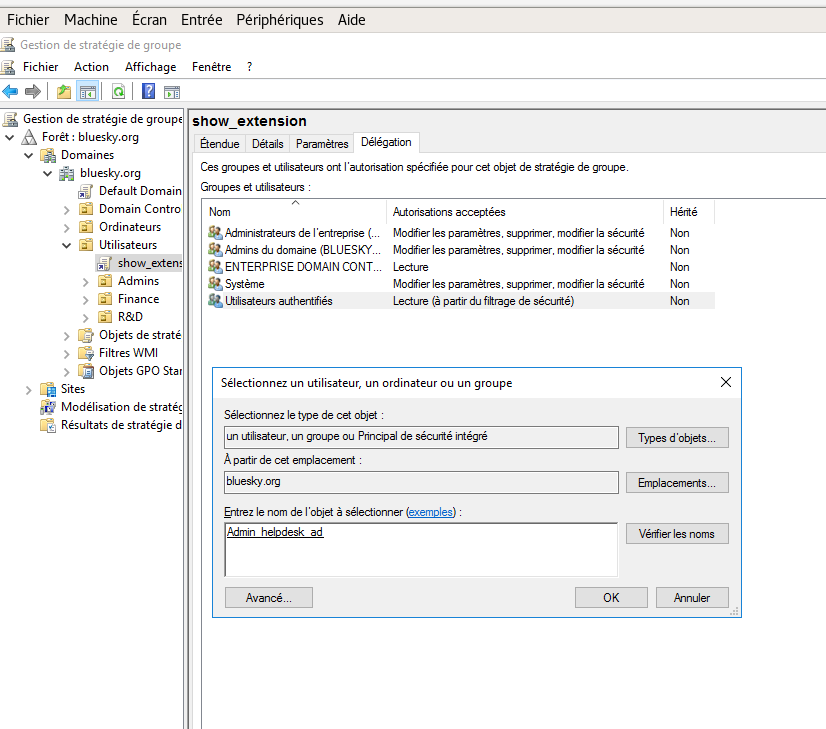
Désactivation du compte Administrateurs sur DC-1 :



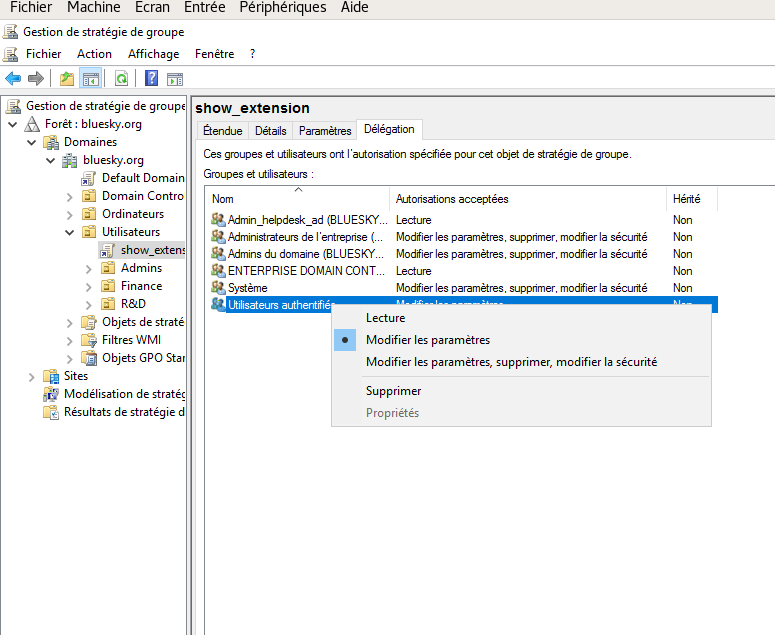
Ajout du compte dans le groupe de sécurités Admin\_helpdesk\_pc :



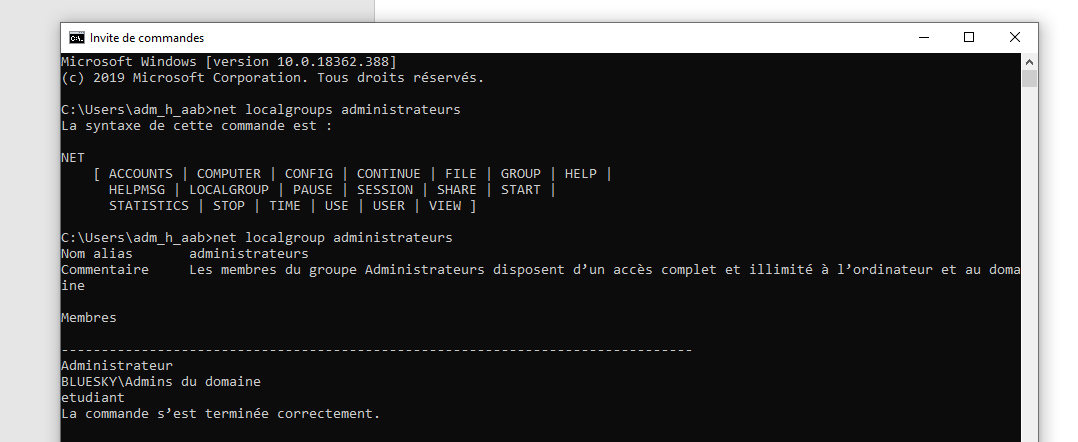
Gpo : Afficher les extensions :



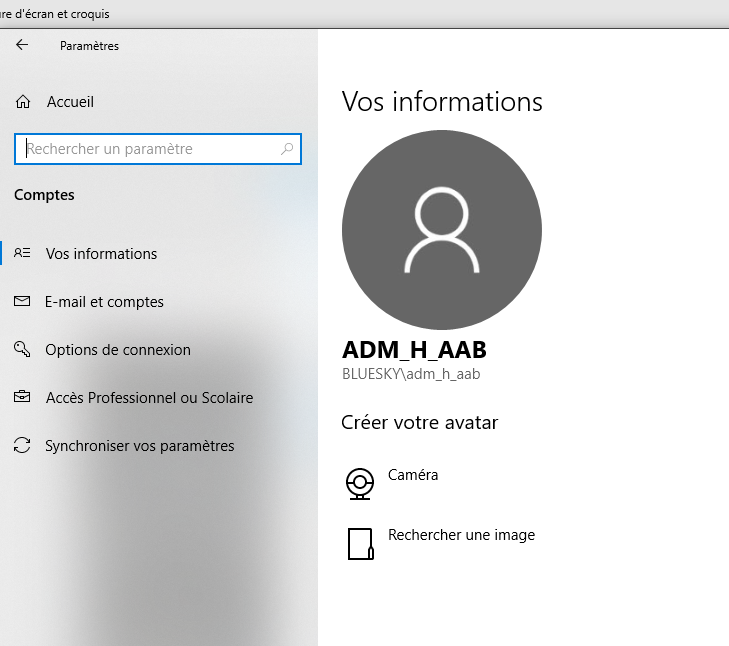
Ne pas oublier modifier les paramètres :



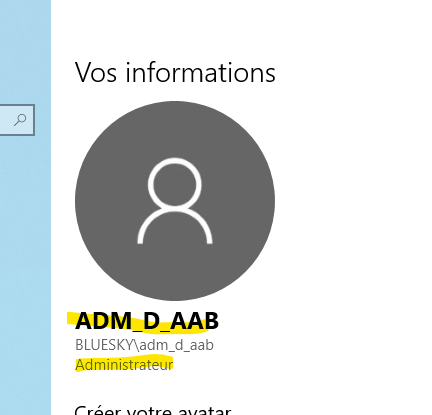
Listes des administrateurs sur PC2 :



**L’user adm\_h\_AAB -> dans le groupe GROUPES/Admin\_helpdesk\_ad.** On arrive à modifier la GPO show\_extension mais n’est pas pour autant administrateur.

****

L’user adm\_d\_AAB fait partie du groupe admins du domaine par conséquent, il a le droit de modifier la GPO et les droits Administrateurs.

****

* 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 non configuré, les comptes pour dépanner les utilisateurs ont souvent les droits admins et font partie d’où au lieu de faire partie de groupe.*

*Par conséquent 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 niveau de privilège élevé.*

*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. De plus, le compte est utilisé dans 2 groupes différents.*

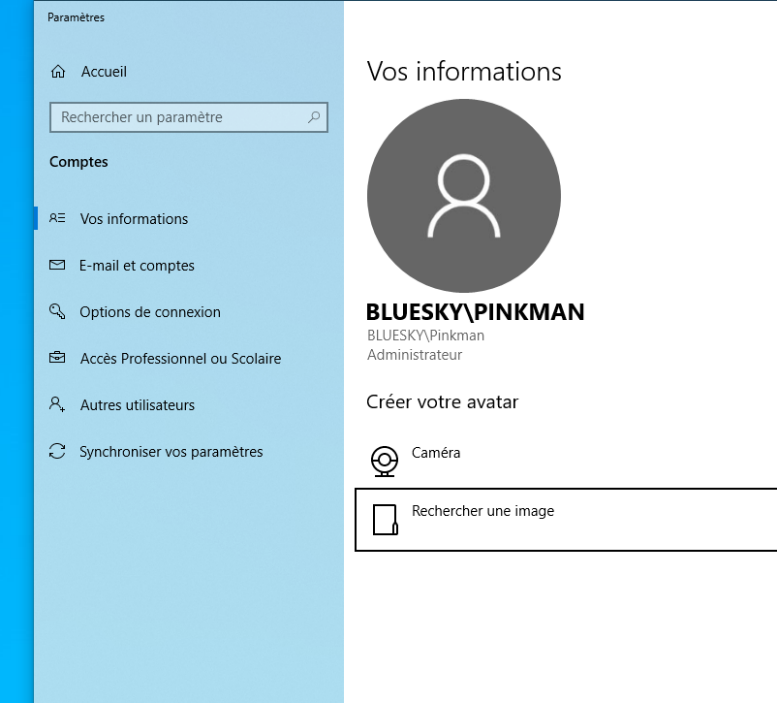
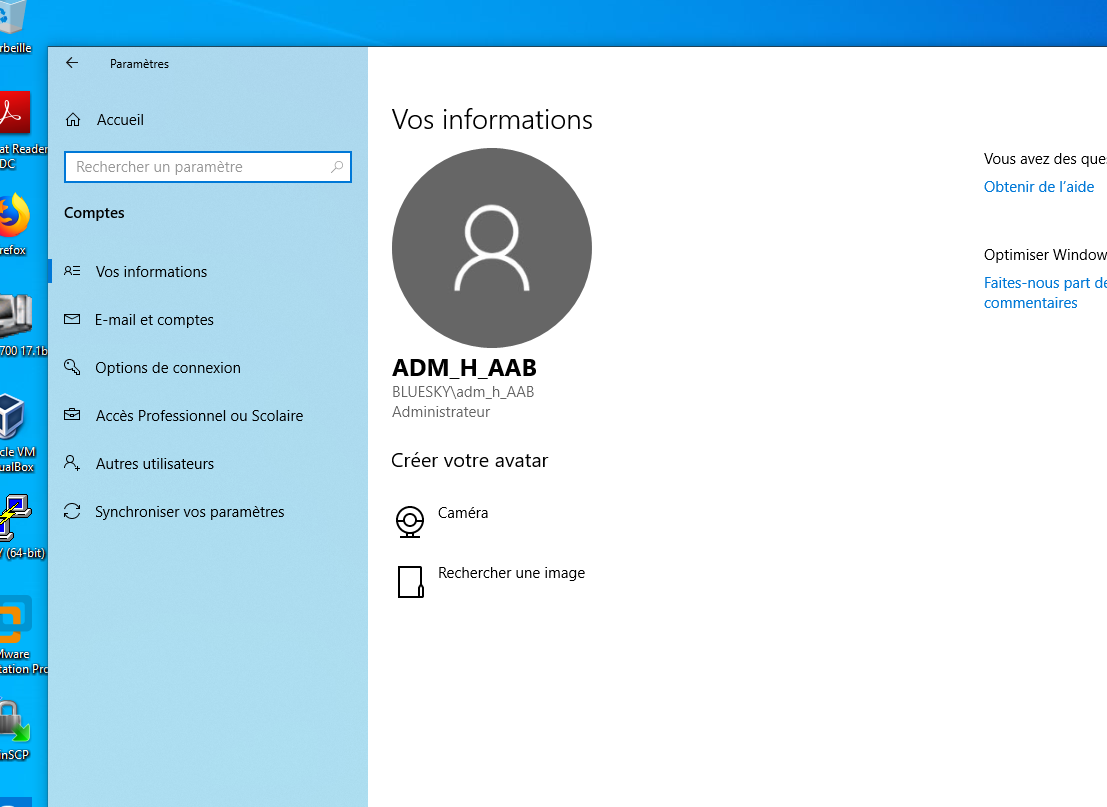
*On doit surtout en* déplaçant l’admin du domaine pour éviter que la GPO(afficher extension s’exécute) sur ces comptes administrateurs.

**Synthèse 2 :**

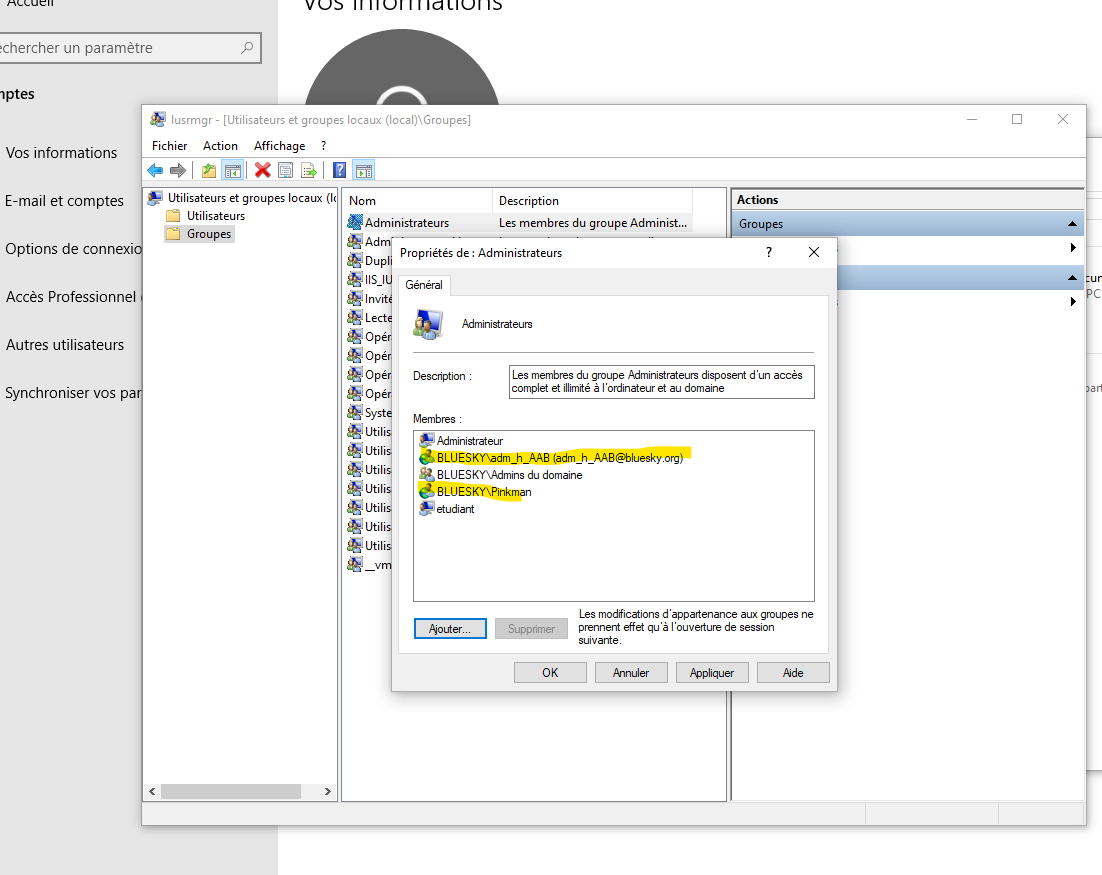
On réorganise l’OU Admins de manière légère selon le cahier des charges avec le groupe et les utilisateurs respectives. On ouvre la session avec le compte admin du tier 1 et on désactive le compte par défaut de BLUESKY. On a créé les groupes de sécurité depuis l’OU groupes et l’user adm\_h\_AAB.

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

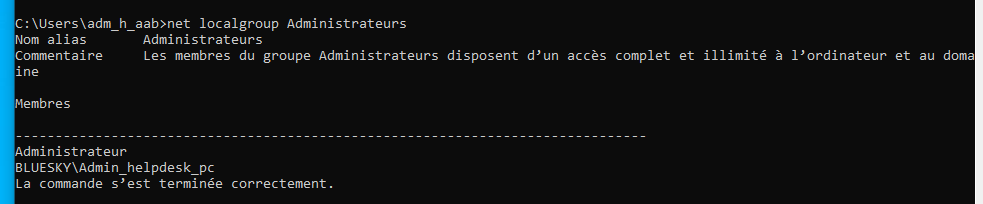
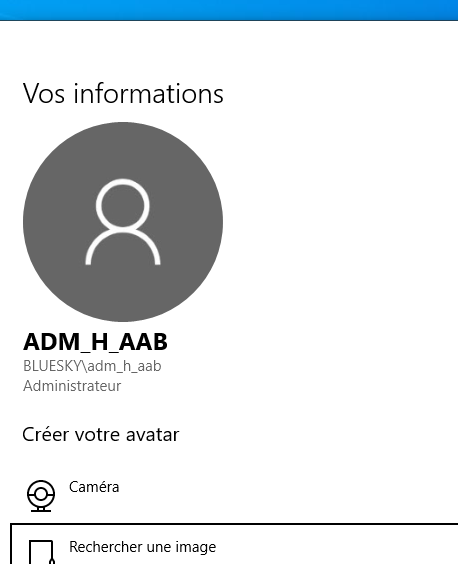
Ajout de pinkman et de **adm\_h\_AAB en tant qu’administrateurs locale du PC1**

**** **** 

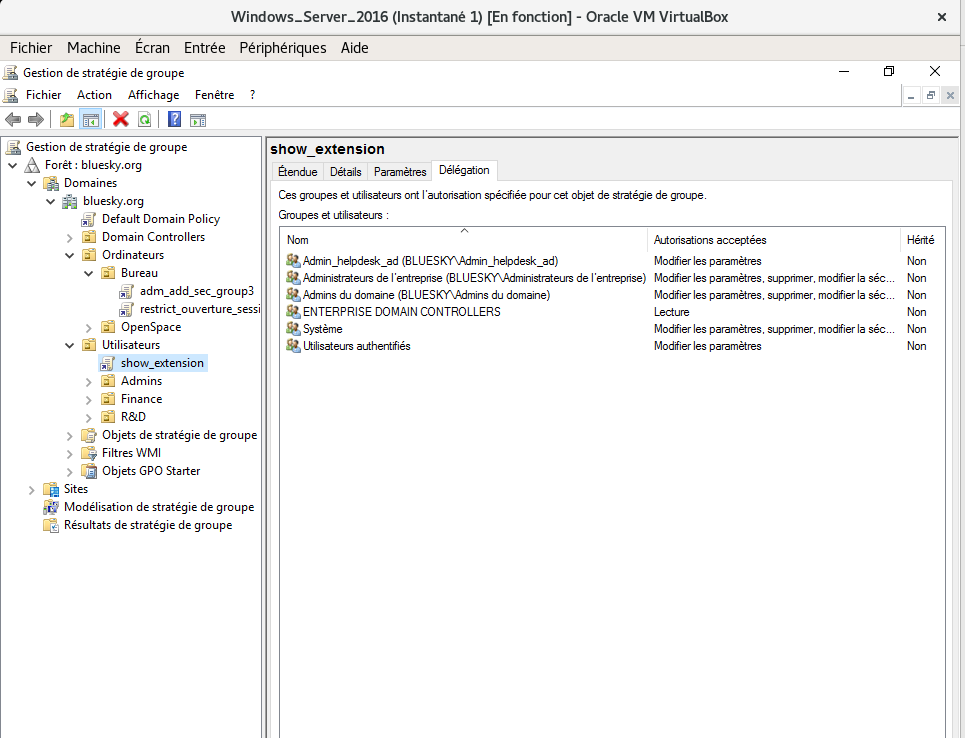
**En faisant :**

****

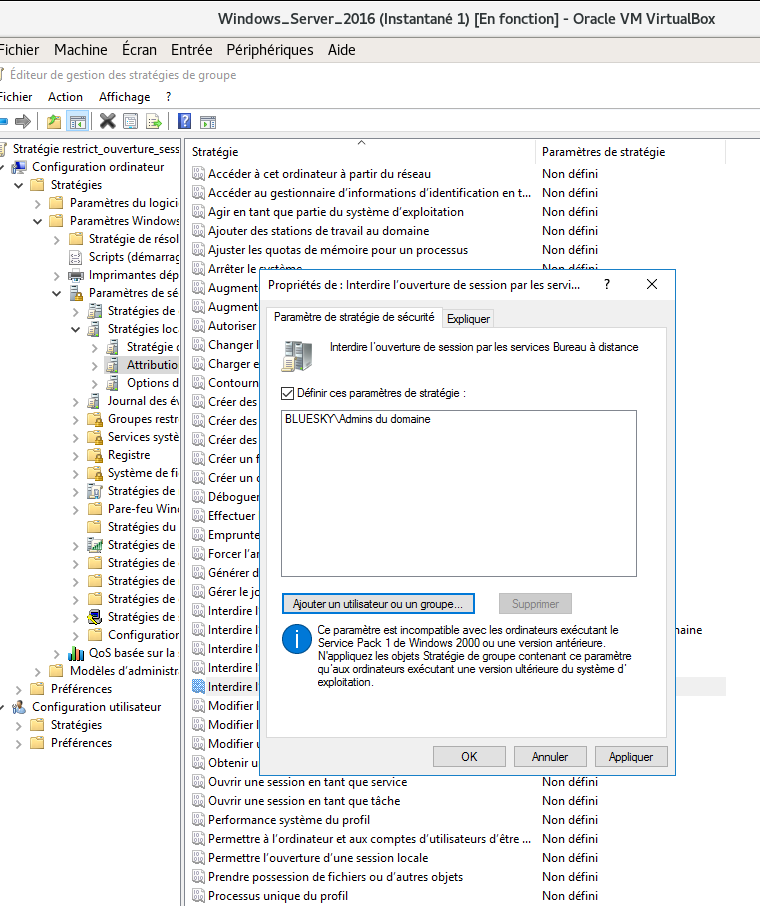
**Avec adm\_h\_AAB sur OPENSPACE-7(PC1), on est administrateurs, quand on a ouvert la session.**

Listes des GPO sur DC-1 :



Restreindre le RDP et l’ouverture de session :



shutdown /r sur BUREAU3(PC2) afin de redémarrer

adm\_d\_AAB en tant qu’Admin\_domain sur le BUREAU-3 ne peut plus se connecter car le groupe Admins du domaine est désactivé seul le groupe Admin\_helpdesk\_PC est autorisée et est administrateur.

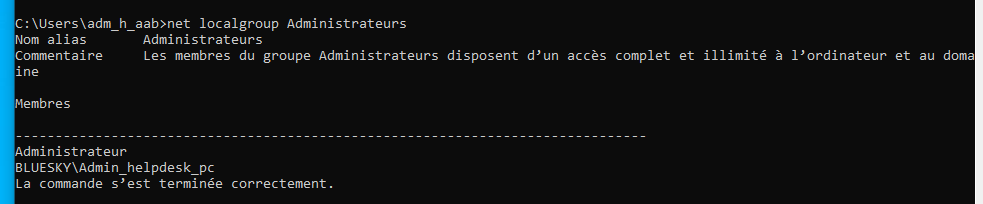
adm\_h\_TRG en tant qu’Admin\_helpdesk sur le PC2 ce compte fonctionne

J’ai listé les administrateurs locaux sur :

Openspace-7 :



Sur pc2 :



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

*Pinkman infecte son compte utilisateurs et n’infecte pas l’ensemble du réseau sauf s’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.*

*Il est plus facile de déléguer ou d’attribuer plusieurs GPO à un groupe et de restreindre leurs accès.*

**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 restreindre 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.

Récap :

On devrait déplacer l’admin du domaine pour éviter que la GPO(afficher extension s’exécute) sur ces comptes administrateurs.