

LP-TP5-AD+-délégation – ECUE31
mardi 30 mars 2021

Amine ABDOUL-AZID
~~Martial SENE~~
~~Kavirajan SARAIVANANE~~

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

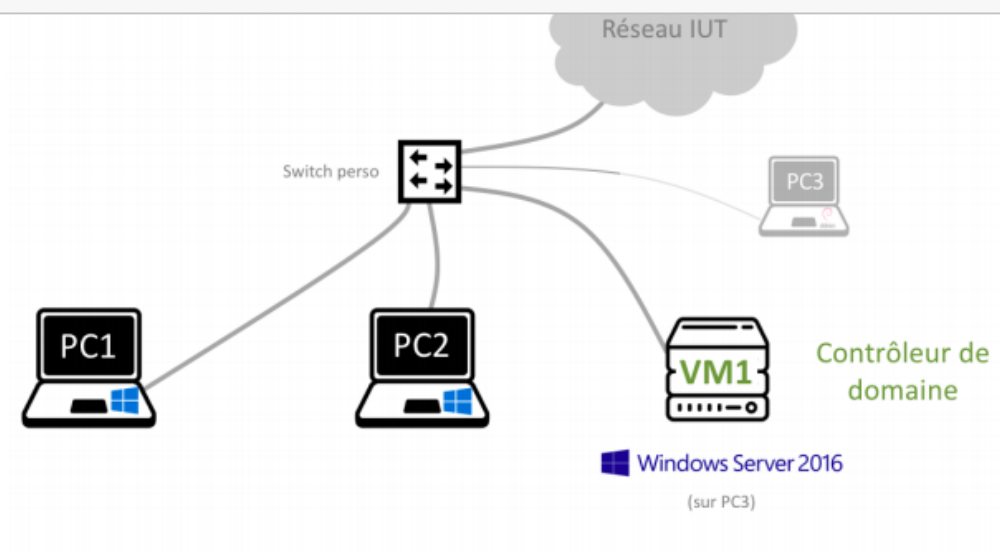


Fig. 3 Maquette de TP

PC	Nom	Adresse IP
PC1	OPENSOURCE-7	198.51.51.17/24 ¹
PC2	BUREAU-3	198.51.51.203/24

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

On a testé avec :

pinkman sur openspace-7(PC1) :

```
ou externe, un programme exécutable ou un fichier de commandes.

C:\Users\pinkman>gpresult /v

Outil de résultat du système d'exploitation Microsoft (R) Windows (R) v2.0
© 2019 Microsoft Corporation. Tous droits réservés.

Créé le 30/03/2021 à 09:53:15

Données RSOP pour BLUESKY\pinkman sur OPENSOURCE-7 : mode journalisation
-----

Configuration du système d'exploitation : Station de travail membre
Version du système d'exploitation..... : 10.0.18362
Nom du site..... : N/A
Profil itinérant : N/A
Profil local..... : C:\Users\pinkman
Connexion via une liaison lente ? : Non



PARAMÈTRES UTILISATEURS
-----

CN=Pinkman,OU=R&D,OU=Utilisateurs,DC=bluesky,DC=org
Heure de la dernière application de la stratégie de groupe : 30/03/2021 à 09:49:31
Stratégie de groupe appliquée depuis : DC-1.bluesky.org
Seuil de liaison lente dans la stratégie de groupe : 500 kbps
Nom du domaine : BLUESKY
Type de domaine : Windows 2008 ou supérieur

Objets Stratégie de groupe appliqués
-----
show_extension
```

Page Affichage

le PC > PARTAGEALL (\\DC-1) (Z:) > pc1-openspace > s1

Nom	Modifié le	Type	Taille
 Annotation 2021-03-30 095326.png	30/03/2021 09:53	Fichier PNG	37 Ko
 test.txt	30/03/2021 09:52	Document texte	0 Ko

Sur white sur bureau-3(PC2) :

Ce PC > partageall (\\DC-1) (Z:)

Nom

Modifié le

Type

Taille

ad-

30/03/2021 09:50

Dossier de fichiers

pc1-openspace

30/03/2021 09:50

Dossier de fichiers

pc2-bureau

30/03/2021 09:50

Dossier de fichiers

C:\WINDOWS\system32\cmd.exe

PARAMÈTRES UTILISATEURS

CN=White,OU=R&D,OU=Utilisateurs,DC=bluesky,DC=org

Heure de la dernière application de la stratégie de groupe : 30/03/2021 à 09:49:02

Stratégie de groupe appliquée depuis : DC-1.bluesky.org

Seuil de liaison lente dans la stratégie de groupe : 500 kbps

Nom du domaine : BLUESKY

Type de domaine : Windows 2008 ou supérieur

Objets Stratégie de groupe appliqués

show_extension

Les objets stratégie de groupe n'ont pas été appliqués

car ils ont été refusés

Stratégie de groupe locale

Filtrage : Non appliqué (vide)

L'utilisateur fait partie des groupes de sécurité suivants

Utilisateurs du domaine

Tout le monde

Utilisateurs

INTERACTIF

OUVERTURE DE SESSION DE CONSOLE

Utilisateurs authentifiés

Cette organisation

LOCAL

Identité déclarée par une autorité d'authentification

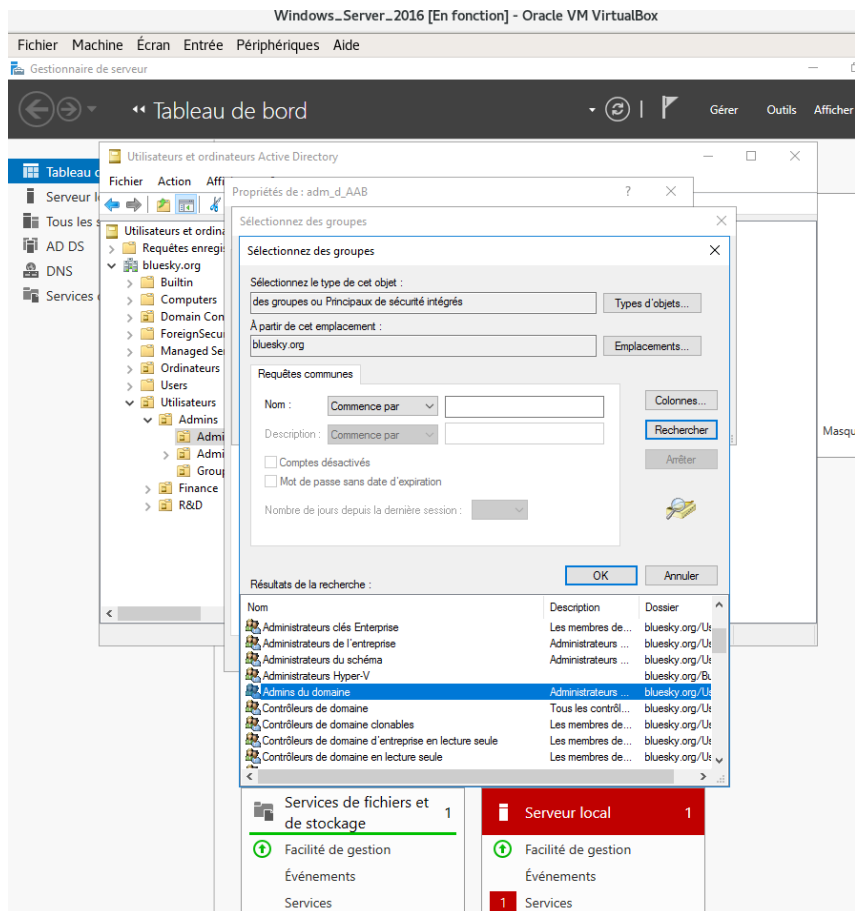
Synthèse 1 :

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

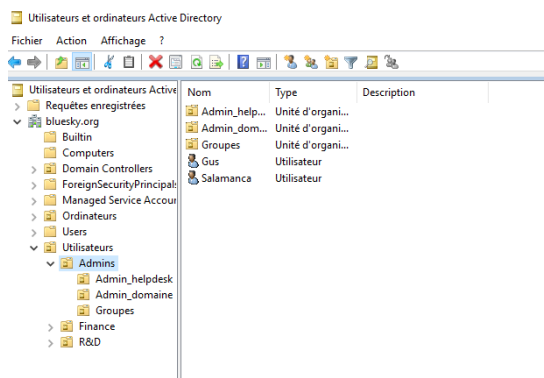
J'ai réalisé les différentes étapes 1-5. Pour configurer le contrôleur et les clients AD.

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

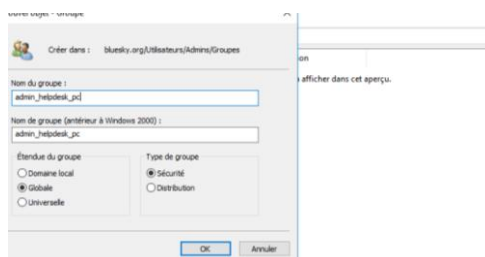
Ajout du compte adm_d_AAA au groupe Admins du domaine :



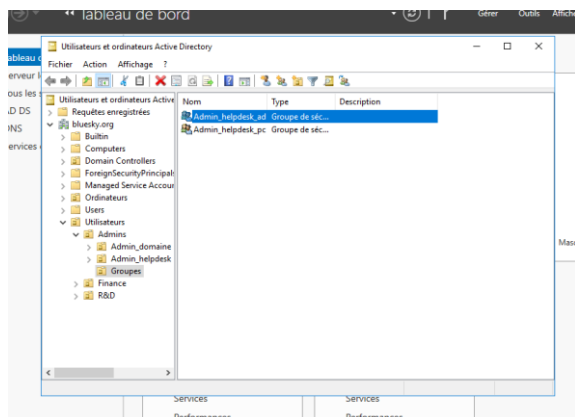
Listes OU Admins :



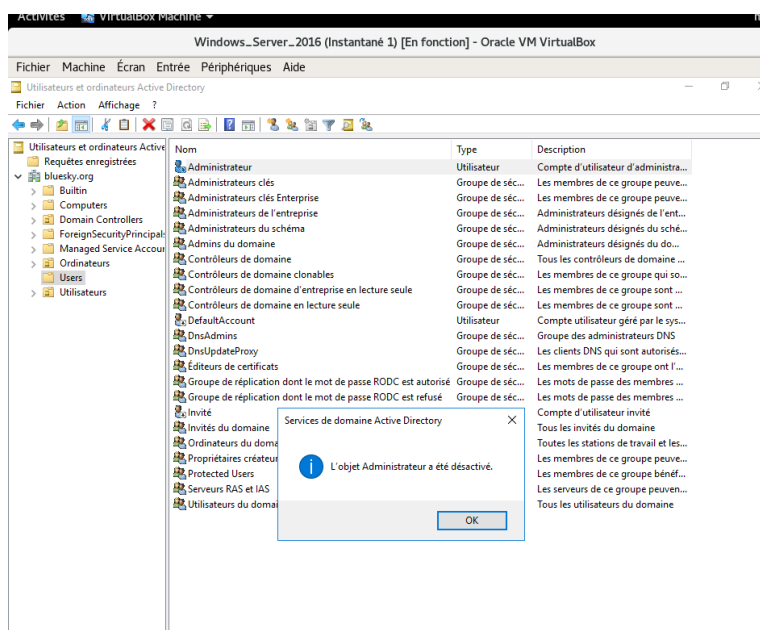
Avec le groupe :



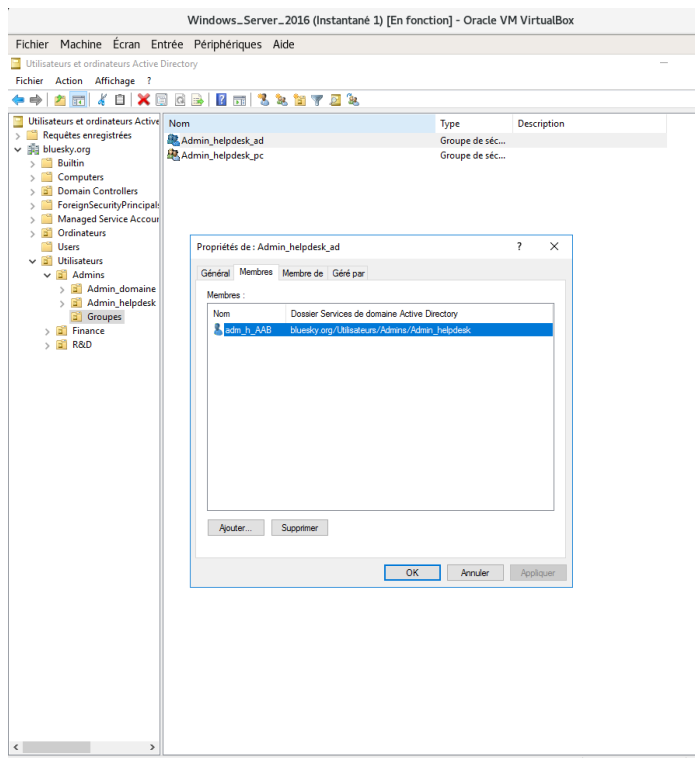
Liste de l'OU Groupes :



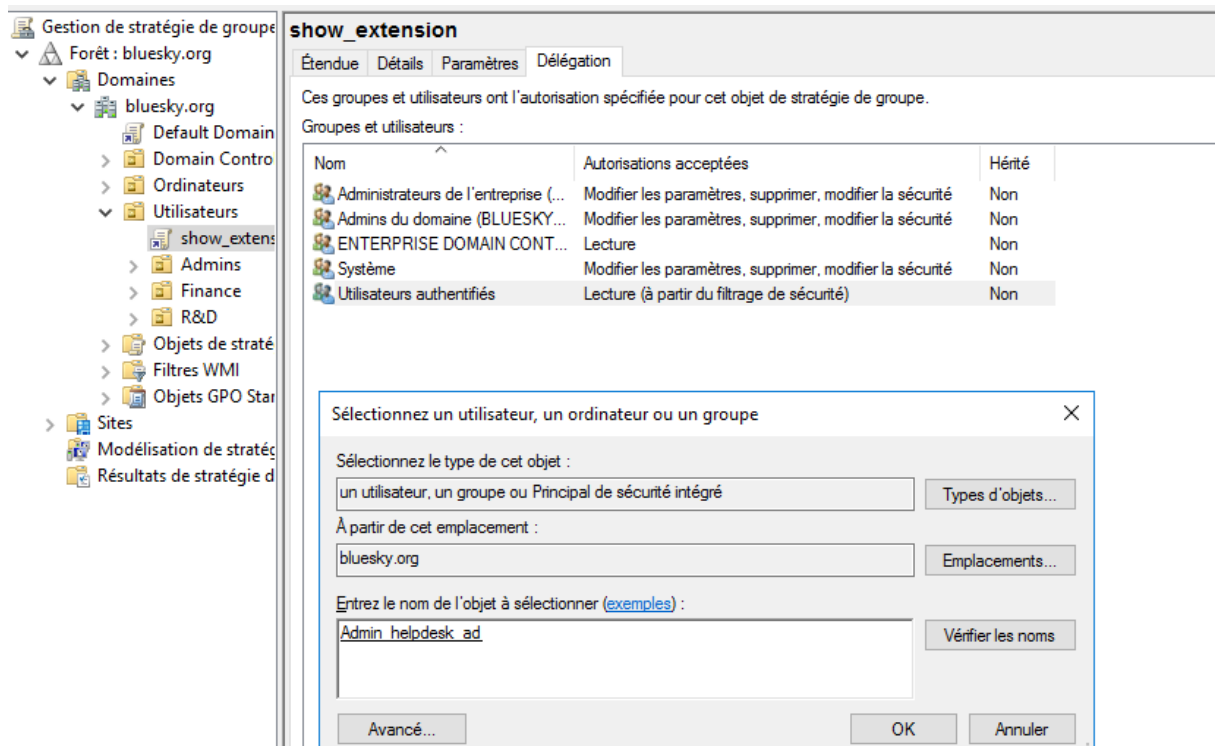
Désactivation du compte Administrateurs sur DC-1 :



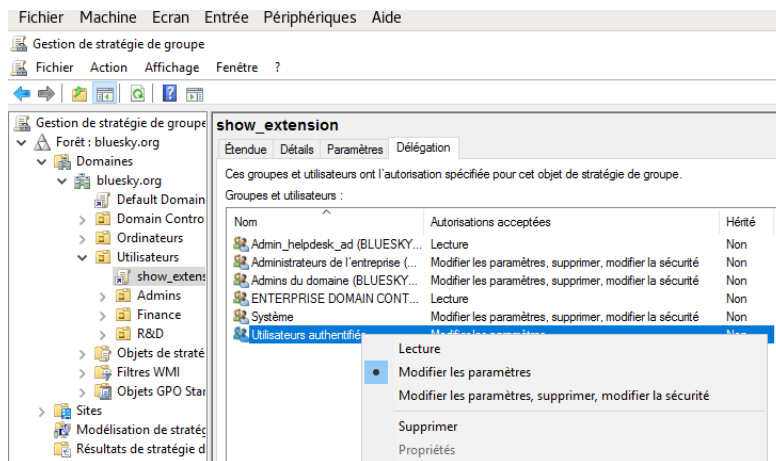
Ajout du compte dans le groupe de sécurités Admin_helpdesk_pc :



Gpo : Afficher les extensions :



Ne pas oublier modifier les paramètres :



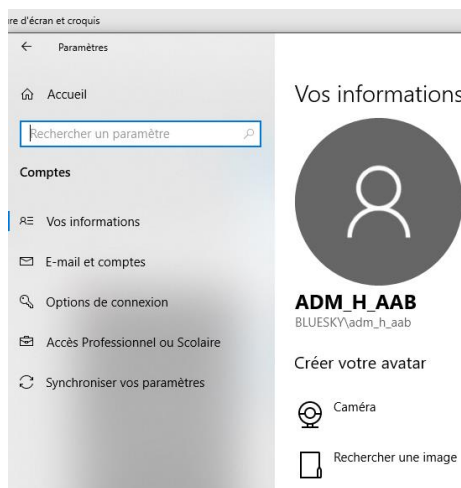
Listes des administrateurs sur PC2 :

```
C:\Users\adm_h_aab>net localgroups administrateurs
La syntaxe de cette commande est :

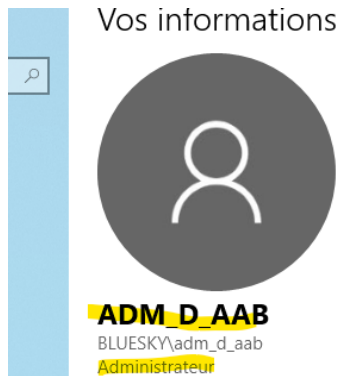
NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
  HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
  STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Users\adm_h_aab>net localgroup administrateurs
Nom alias          administrateurs
Commentaire        Les membres du groupe Administrateurs disposent d'un accès complet et illimité à l'ordinateur et au domaine
Membres
-----
Administrateur
BLUESKY\Admins du domaine
etudiant
La commande s'est terminée correctement.
```

L'utilisateur **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'utilisateur **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 être, 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 contrôlée 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.

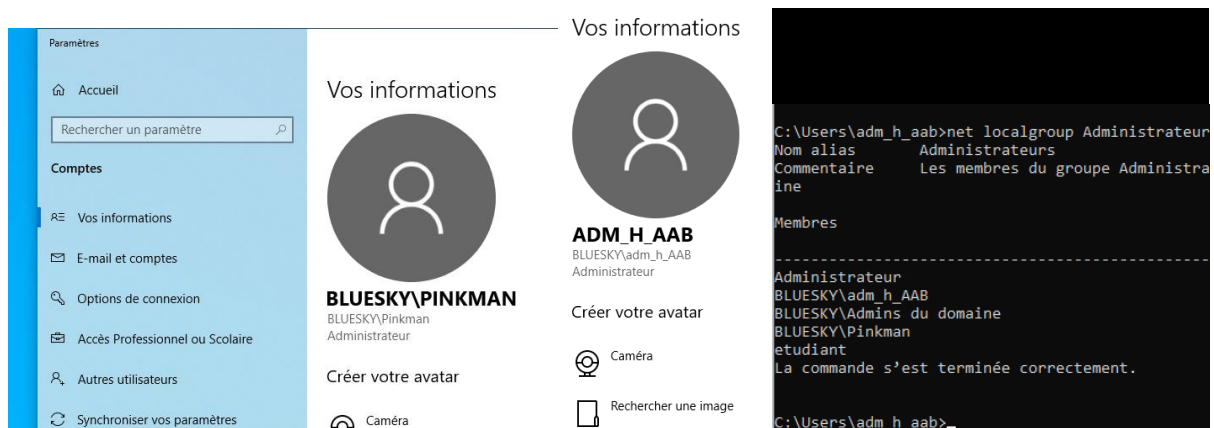
On doit surtout en déplaçant l'admin du domaine pour éviter que la GPO (afficher extension s'exécute) sur ces comptes administrateurs.

Synthèse 2 :

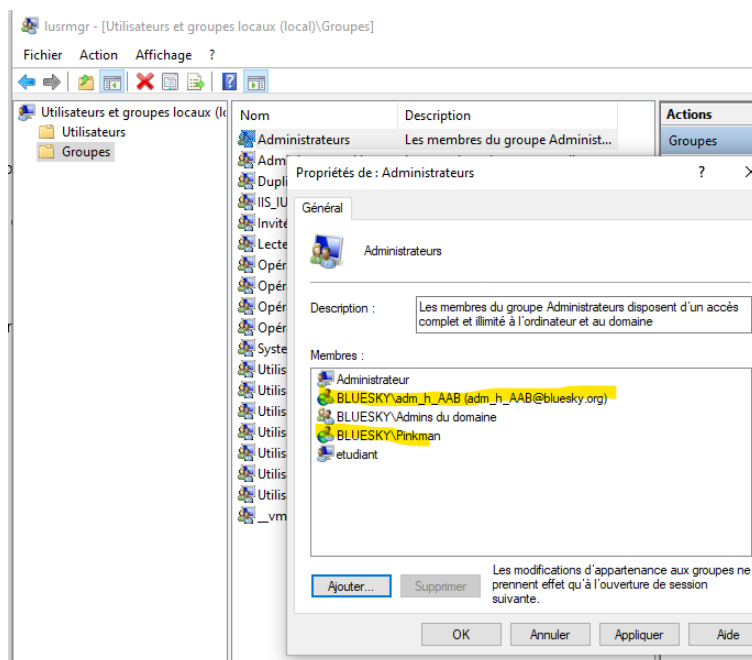
On réorganise l'OU Admins de manière légère selon le cahier des charges avec le groupe et les utilisateurs respectives. On ouvre la session avec le compte admin du tier 1 et on désactive le compte par défaut de BLUESKY. On a créé les groupes de sécurité depuis l'OU groupes et l'utilisateur adm_h_AAB.

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

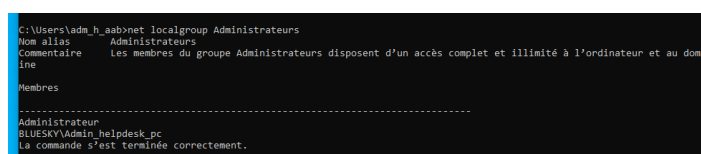
Ajout de pinkman et de adm_h_AAB en tant qu'administrateurs locale du PC1



En faisant :

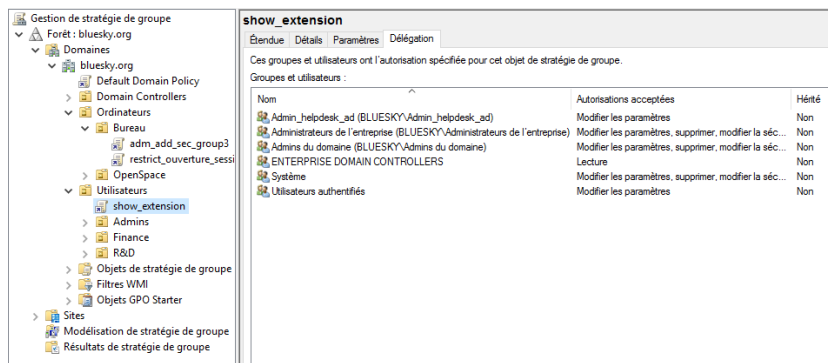


Avec adm_h_AAB sur OPENSOURCE-7(PC1), on est administrateurs, quand on a ouvert la session.

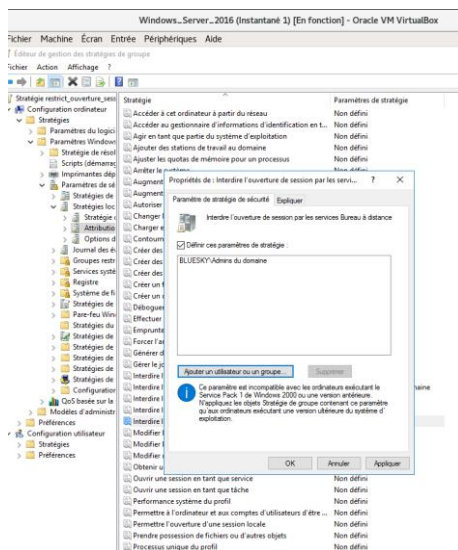


ADM_H_AAB
BLUESKY\adm_h_aab
Administrateur

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 :

```
C:\Users\adm_h_aab>net localgroup Administrateur
Nom alias      Administrateurs
Commentaire    Les membres du groupe Administra
ine
Membres
-----
Administrateur
BLUESKY\adm_h_AAB
BLUESKY\Admins du domaine
BLUESKY\Pinkman
etudiant
La commande s'est terminée correctement.
C:\Users\adm_h_aab>
```

Sur pc2 :

```
C:\Users\adm_h_aab>net localgroup Administrateurs
Nom alias      Administrateurs
Commentaire    Les membres du groupe Administrateurs disposent d'un accès complet et illimité à l'ordinateur et au doma
ine
Membres
-----
Administrateur
BLUESKY\Admin_helpdesk_pc
La commande s'est terminée correctement.
```

- 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 OPENSOURCE-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 dérobées.

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. OPENSOURCE-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.