OS Propriétaire Labo – Notes

Grégoire Roumache

Septembre 2020

Table des matières

1 Labo 1 – Active Directory

(a) installer 2 windows server et 1 windows 10

Windows Server n°1	**Windows Server n°2**	**Windows 10**
0. utiliser `sysprep`		
1. nom système = DC1 2. ++ User1, PasswordDC1 3. règle parefeu pour ping 4. config réseau • ip = 192.168.0.2/24 • dns = 192.168.0.130 5. installer l'active directory 6. ++ *Pamela* dans l'AD 7. ++ unité d'organi. *Staff* 8. placer *Pamela* dans *Staff*	1. nom système = MS1 2. ++ User1, PasswordMS1 3. règle parefeu pour ping 4. config réseau • ip = 192.168.0.130/24 • dns = 192.168.0.130 5. intégrer la machine à l'AD	1. nom système = PC1 2. ++ User1, PasswordPC1 3. règle parefeu pour ping 4. config réseau: • ip = 192.168.0.65/24 • dns = 192.168.0.130 5. intégrer la machine à l'AD

(a) tester le ping

(b) se connecter avec *Pamela*, *administrator*, *User1*

2 Labo 2 – Gestion des Group Policy Object (GPO)

<table>
<tr><th>Windows Server n°1</th><th>Windows Server n°2</th></tr>
<tr><td colspan="2">(a) désactiver les règles de trafic entrant de l'icmp dans le firewall
(b) changer le statut de la section domain networks du firewall en connected</td></tr>
<tr><td>1. ++ stratégie GPO log non locally pour Pamela sur DC
2. ++ unité d'organisation batimentA + batimentA/{Floor1,Floor2, Servers} + Femmes
3. placer MS1 dans Servers, PC1 dans Floor2, Pamela dans Femmes
4. ++ stratégie GPO firewall autoriser icmp entrant sur Servers
5. ++ stratégie GPO firewall interdire icmp entrant sur Default Domain Policy
6. ++ stratégie GPO firewall autoriser icmp entrant sur Floor2
7. ++ redirecteurs conditionnels (dns), monsite1.local + monsite2.local = 192.168.0.130
8. ++ préférence GPO page d'accueil IE = monsite1 sur Femmes</td><td>1. installer les rôles DNS et Web
2. ++ 2 zones primaires, dedans: enregistrement A = www
3. ++ monsite1 & monsite2 (config IIS)
4. se connecter avec l'administrateur de l'AD
5. installer le rôle DHCP, l'activer pour l'AD</td></tr>
<tr><td colspan="2">(a) forcer l'adoption immédiate des GPO
(b) vérifier les GPO dans le Group Policy Management
(c) aller sur www.monsite1.local et www.monsite2.local
(d) se connecter en Pamela et ouvrir internet explorer
(e) tester le ping</td></tr>
</table>

3 Labo 3 – Mise en place du NAT

Windows Server n°1	**Windows Server n°2**
1. ++ disque de 50 GB (+ initialiser le disque) 2. ++ nouveau volume & share de type SMB 3. ++ stratégie GPO, réduire l'intervalle d'actualisation des GPO 4. ++ stratégie GPO, interdire notepad aux utilisateurs 5. ++ unité d'organisation *no_ notepad_ OU*, y placer l'UO *no_ notepad_ OU_ child* 6. ++ utilisateurs, dans les UO correspondantes: *no_ notepad*, *no_ notepad_ child* 7. ++ GPO *lock_ taskbar*, enforcer la GPO 8. bloquer l'héritage pour *no_ notepad_ OU* 9. ++ filtre WMI: mémoire libre > 2Go 10. ++ GPO déployement d'application, ex: chrome (.msi) 11. ++ modèle d'administration de l'application (.adm) 12. ++ GPO page d'accueil du navigateur	1. ++ carte réseau en nat 2. la configurer en dhcp, dns = 192.168.0.2 3. ++ rôle *remote access* (nat)
(a) tester le ping vers internet (b) accéder au *share* dans l'explorateur de fichiers (c) tester l'accès à notepad pour les différents utilisateurs (d) vérifier si la barre des tâches est vérouillée pour les différents utilisateurs (e) réduire la ram, rebooter la machine et vérifier que l'application n'est pas déployée (f) augmenter la ram, rebooter la machine et vérifier que l'application est bien installée (g) tester la page d'accueil du navigateur	

Exercice supplémentaire:

- les utilisateurs des groupes *firefox_ group* et *chrome_ group* ont leurs navigateurs respectifs installés
- les utilisateurs des groupes *monsite1* et *monsite2* ont leurs page d'accueil respectives mises en place

4 Labo 4 – Gestion des profils et des environnements

Windows 10

1. ++ répertoires *C:\programmes\allowed*, et *C:\programmes\denied*
2. copier dans ces répertoires *C:\Windows\System32\calc.exe*
3. copier *C:\Windows\System32\mspaint.exe* sur le share

Windows Server n°1

1. ++ OU *roaming_ OU*
2. ++ utilisateur itinérant *itinerant-test1*
3. ++ OU *Profils_ Oblig_ OU*
4. ++ utilisateur obligatoire *oblig-test1*
5. ++ OU *Folder_ redirect_ OU*
6. ++ utilisateur *moreels*
7. ++ GPO *Folder_ redirect_ GPO*, uniquement pour *moreels*, rediriger les dossiers personnels vers *users_ folders*
8. ++ OU, y placer le pc windows 10
9. ++ GPO, interdire *...\denied\calc.exe*
10. ++ GPO, interdire le hash de *mspaint.exe*

Windows Server n°2

1. ++ dossier share invisible *Profiles*
2. ++ accès écriture sur *Profiles* aux membres du domaine
3. ++ full control sur *Profiles* aux admins
4. ++ dossier *users_ folders* dans le share
5. ++ full control sur *users_ folders* aux membres du domaine

Debian

1. installer la machine, la placer dans le réseau, vérifier qu'elle reçoit une configuration du dhcp
2. configurer un hostname, procéder à un upgrade de la base de données d'aptitude
3. installer *dnsutils, sssd, sssd-tools, realmd, samba, samba-common-bin, krb5-config, winbind, smbclient, libnss-sss, libpam-sss, adcli, policykit-1*
4. configurer l'authentification kerberos (realm = `DOMAINE<nb>.LOCAL`)
5. joindre le domaine
6. permettre aux utilisateurs de l'AD de se logger sur la debian

Remarque: dans l'énoncé, il est mis que le share est dans *ms1* mais dans le labo 3, on a créé le share sur *dc1*.

(a) se connecter avec *itinerant-test1* pour vérifier que son profil est bien un type itinérant

(b) avec *itinerant-test1*, créer un fichier sur le bureau, puis se reconnecter sur une autre machine pour voir si il y est aussi

(c) idem avec *oblig-test1* mais le fichier ne devrait pas être présent

(d) se connecter avec *moreels* et vérifier que le dossier *documents* est dans le share

(e) avec *moreels* créer un document dans *documents*, et vérifier qu'il est accessible après reconnexion sur une autre machine

(f) essayer de lancer les programmes de calculatrice sur la machine windows 10

(g) se connecter en admin sur le pc windows 10, essayer de lancer ...*denied**calc.exe*, ça devrait échouer

(h) renommer *mspaint.exe* et essayer de le lancer, ça devrait échouer

(i) vérifier que la machine debian est bien présente dans l'*active directory users and computers*

(j) vérifiez qu'on peut se logger avec un utilisateur de l'AD sur la console du serveur Linux

(k) vérifier qu'on peut se connecter au serveur en ssh sur windows (`ssh pamela@domaine<nb>.local@<ip>`)

A Comment faire le labo 1

A.1 Changer le nom système

1. taper *control panel* dans la barre de recherche windows
2. cliquer sur la section *system and security*, puis sur la section *system*
3. à droite, cliquer sur *change settings*, puis sur le bouton *change*
4. changer le nom de l'ordinateur et cliquer sur *ok*

A.2 Activer la règle de pare-feu pour ping

1. taper *firewall.cpl* dans la barre de recherche windows
2. (sur windows 10, à droite, cliquer sur *advanced settings*)
3. à gauche, cliquer sur *inbound rules*
4. activer la/les règles: *file and printer sharing (echo request - icmpv4-in)*

A.3 Ajouter un compte local

1. taper *settings* dans la barre de recherche windows
2. cliquer sur *accounts*
3. à gauche, cliquer sur:
   - *family & other users* (sur windows 10)
   - *other users* (sur windows server)
4. cliquer sur *add someone else to this pc*
5. (sur windows 10, ajouter l'username et le mot de passe)
6. cliquer sur *users*
7. faire un clic-droit, puis cliquer sur *new user*
8. entrer l'username, le mot de passe et désactiver l'option *user must change password at next logon*

A.4 Modifier la config réseau

1. taper *ncpa.cpl* dans la barre de recherche windows
2. cliquer sur *ethernet*, puis sur *properties*
3. cliquer sur *internet protocol version 4*
4. changer la config

A.5 Intégrer une machine à l'Active Directory

1. taper *control panel* dans la barre de recherche windows
2. cliquer sur la section *system and security*, puis sur la section *system*
3. à droite, cliquer sur *change settings*, puis sur le bouton *change*
4. sélectionner le bouton radio *domain*
5. entrer le nom du domaine (a priori: *domaine<num_pc>.local*)
6. appuyer sur *ok*
7. se connecter avec un compte de la machine sur laquelle est installé l'AD (ex: *Pamela*, *Tigrou007*)

Remarque: l'active directory doit être déjà installé sur le serveur (les 2 machines doivent entrer en contact).

A.6 Utiliser `sysprep`

1. ouvrir le navigateur de fichiers, aller dans le dossier *C:\Windows\System32\Sysprep*
2. double-cliquer sur *sysprep.exe*
3. cocher l'option *generalize*
4. appuyer sur *ok*

A.7 Installer l'active directory

1. ouvrir le *server manager*
2. en haut à droite, cliquer sur *manage*, puis sur *add roles and features*
3. à gauche dans *server roles*, sélectionner *active directory domain services*
4. cliquer sur *add features* dans la popup, puis continuer jusqu'à l'installation
5. quand un signe danger apparaît en haut à droite, cliquer dessus
6. cliquer sur *promote this server to a domain controller*
7. sélectionner l'option *add a new forest*, et ajouter le nom de domaine (a priori *domaine<num_pc>.local*)
8. ensuite, ajouter le mot de passe DSRM: *Tigrou007*, et terminer la configuration

A.8 Ajouter un compte dans l'active directory

1. ouvrir le *server manager*
2. à gauche, cliquer sur *AD DS*
3. faire un clic-droit sur *users*, puis cliquer sur *new*, puis sur *user*
4. compléter le formulaire

A.9 Ajouter une unité d'organisation

1. ouvrir le *server manager*
2. à gauche, cliquer sur *AD DS*
3. faire un clic-droit sur DC1, puis cliquer sur *active directory users and computers*
4. dans la nouvelle fenêtre, clic-droit sur le nom de domaine (*xxx.local*)
5. cliquer sur *new*, puis sur *organizational unit*
6. donner un nom et appuyer sur *ok*

A.10 Déplacer un compte dans une unité d'organisation

1. ouvrir le *server manager*
2. à gauche, cliquer sur *AD DS*
3. faire un clic-droit sur DC1, puis cliquer sur *active directory users and computers*
4. à gauche, cliquer sur *user*
5. faire un clic-droit sur l'utilisateur et cliquer sur *move*
6. sélectionner l'unité d'organisation dans laquelle la déplacer et cliquer sur *ok*

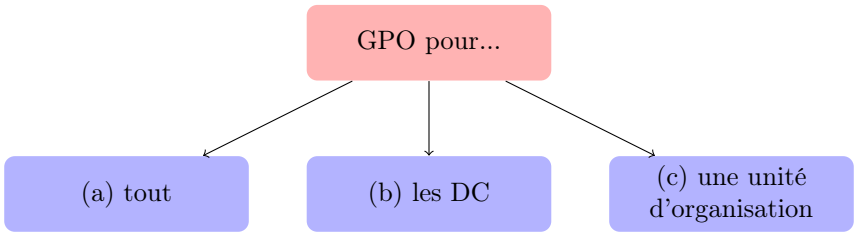
B Comment faire le labo 2

B.1 Changer le statut de la section *domain networks* du firewall en *connected*

1. taper *ncpa.cpl* dans la barre de recherche windows
2. faire un clic droit sur la carte réseau, puis cliquer sur *disable*
3. faire un clic droit sur la carte réseau, puis cliquer sur *enable*

B.2 Ouvrir le *Group Policy Management Editor*

1. taper *gpmc.msc* dans la barre de recherche windows



2. dans le menu de gauche, clic droit sur:
   (a) *forest: domaine.local/default domain policy*
   (b) *forest: domaine.local/domains/domaine.local/domain controllers/default domain controllers policy*
   (c) une *policy* dans l'unité d'organisation (dans *forest: domaine.local/domains/domaine.local/*)

   > Si il n'y a pas encore de *policy* dans l'unité d'organisation:
   > - clic droit sur l'unité d'organisation
   > - cliquer sur *create a gpo in this domain and link it here*

3. après le clic droit sur la policy, cliquer sur *edit*

Remarque: différence entre *default domain policy* et *default domain controller policy* (= *default DC policy*):

- les paramètres configurés dans *default domain policy* s'appliquent à toutes les machines du domaine
- les paramètres dans *default domain controller policy* ne s'appliquent qu'aux serveurs DC du domaine

B.3 Ajouter une GPO *log on locally*

1. ouvrir le *Group Policy Management Editor* (voir section B.2)
2. dans le menu de gauche, cliquer sur *computer configuration/policies/windows settings/security settings/local policies/user rights assignment*
3. doucle-cliquer sur *allow logon locally*
4. cliquer sur *add user or group*, puis sur *browse*
5. écrire *Pamela* en bas, puis cliquer sur *check names*, puis sur *ok*

B.4 Ajouter une GPO pour autoriser/refuser le ping avec le firewall

1. ouvrir le *Group Policy Management Editor* (voir section B.2)
2. dans le menu de gauche, clic droit sur *computer configuration/policies/windows settings/security settings/windows defender firewall/inbound rules*, puis cliquer sur *new rule*
3. sélectionner l'option *predefined*, puis l'option *file and printer sharing*
4. cliquer sur *next*, puis sélectionner l'option permettant le ping en ipv4
5. cliquer sur *next*, puis sélectionner l'option *allow the connection*

B.5 Ajouter une GPO pour changer la page d'accueil de internet explorer (IE)

1. ouvrir le *Group Policy Management Editor* (voir section B.2)
2. dans le menu de gauche, cliquer sur *User Configuration/Policies/Administrative Template/Windows Components/Internet Explorer*
3. clic droit sur *disable changing home page settings*, puis cliquer sur *edit*
4. choisir l'option *enabled*, et taper l'adresse dans *home page*: http://www.<site>.<wtv>

B.6 Ajouter un redirecteur conditionnel (dns)

1. taper *dns manager* dans la barre de recherche windows
2. dans le menu de gauche, faire un clic droit sur *dns/dc1/conditionnal forwarders*
3. cliquer sur *new conditionnal forwarder*
4. dans *dns domain*, taper: <site>.<wtv>
5. dans *ip addresses of the master servers*, taper l'adresse ip du serveur web

B.7 Ajouter une zone primaire et un enregistrement A (dns)

Ajouter une zone primaire:

1. taper *dns manager* dans la barre de recherche windows
2. dans le menu de gauche, faire un clic droit sur *dns/dc1/forward lookup zone*, puis cliquer sur *new zone*

Ajouter un enregistrement A:

1. taper *dns manager* dans la barre de recherche windows
2. dans le menu de gauche, faire un clic droit sur *dns/dc1/forward lookup zone/<zone>*
3. cliquer sur *new host (A or AAAA)*
4. dans *name*, taper: www
5. dans *ip address*, taper l'adresse ip du serveur web

B.8 Activer le rôle DHCP pour l'AD (pendant l'installation du rôle)

Lors de la configuration post-installation du rôle DHCP, dans *autorization*, sélectionner l'option *use the following user's credentials*, avec *user name* mis en *domaine\administrator*.

B.9 Ajouter une default gateway dans le dhcp

1. ouvrir le dhcp manager
2. dans le menu de gauche, faire un clic droit sur *dhcp/ms1.domaine14.local/ipv4/scope[<ip>] labo2/scope option*
3. cliquer sur *configure options*
4. cliquer sur *003 router*, et ajouter l'adresse ip de la default gateway

B.10 Forcer l'adoption immédiate des GPO

ATTENTION ! À faire sur toutes les machines, pas uniquement DC.

1. ouvrir CMD
2. taper la commande `gpupdate /force`

B.11 Vérifier les GPO dans le *Group Policy Management*

1. taper *gpmc.msc* dans la barre de recherche windows
2. cliquer sur la stratégie à vérifier
3. aller dans l'onglet *settings*
4. vérifier que les GPO sont bien configurées

Remarque: la fenêtre *group policy management* en se rafraîchit pas, il faut la fermer et la rouvrir si nécessaire.

C Comment faire le labo 3

C.1 Ajouter un disque et l'initialiser

Dans VirtualBox:

1. cliquer sur la VM, puis sur *configuration*, puis sur *Stockage*
2. dans *unités de stockage*, cliquer sur *ajouter un disque dur*
3. choisir les options du disque

Dans la VM:

1. taper *computer management* dans la barre de recherche windows
2. dans le menu de gauche, cliquer sur *disk management*
3. une fenêtre *initialize disk* devrait s'ouvrir, cliquer sur *ok*

C.2 Créer un volume et un share de type SMB

Créer un volume:

1. taper *server manager* dans la barre de recherche windows
2. dans le menu de gauche, cliquer sur *file and storage server*, puis sur *disks*
3. faire un clic droit sur le dernier disque, puis cliquer sur *new volume*
4. choisir les options du volume et changer la *drive letter* à *F*

Créer un share de type SMB:

1. dans la même fenêtre (*server manager*), dans le menu de gauche, cliquer sur *shares*
2. en haut, à droite de *shares*, cliquer sur *tasks*, puis sur *new share*
3. dans *share location*, sélectionner le volume *F*
4. donner le nom *MyShare* dans *share name*

Remarque: si il n'y a pas *shares* dans le menu de gauche de *server manager*, aller dans *computer management* pour créer le share.

C.3 Ajouter une GPO pour réduire l'intervalle d'actualisation des GPO

1. ouvrir le *Group Policy Management Editor* (voir section B.2)
2. dans le menu de gauche, cliquer sur *computer configuration/policies/administrative templates/system/group policy*
3. double-cliquer sur *set group policy refresh interval for computers*
4. activer l'option *enabled*, puis configurer l'intervalle d'actualisation, ensuite appuyer sur *apply*

C.4 Ajouter une GPO pour interdire notepad aux utilisateurs

1. ouvrir le *Group Policy Management Editor* (voir section B.2)
2. dans le menu de gauche, cliquer sur *user configuration/policies/administrative templates/system*
3. double-cliquer sur *don't run specified windows applications*
4. sélectionner l'option *enabled*
5. dans *options*, cliquer sur *show*
6. dans la fenêtre qui vient de s'ouvrir, ajouter les deux valeurs *notepad*, et *notepad.exe*
7. appuyer sur *ok*, puis *apply*

C.5 Ajouter une GPO *lock_ taskbar*

1. ouvrir le *Group Policy Management Editor* (voir section B.2)
2. dans le menu de gauche, cliquer sur *user configuration/policies/administrative templates/start menu and taskbar*
3. double-cliquer sur *lock the taskbar*
4. sélectionner l'option *enabled*, puis cliquer sur *apply*

C.6 Ajouter un filtre WMI: mémoire libre > 2Go

Créer un filtre WMI:

1. taper *gpmc.msc* dans la barre de recherche windows
2. dans le menu de gauche, faire un clic droit sur *wmi filter*, puis cliquer sur *new*
3. changer le nom et la description, puis cliquer sur *add* et taper la query

> exemple – filtre mémoire libre > 2Go:
> `select * from Win32_OperatingSystem where FreePhysicalMemory > 2150000000`

Ajouter un filtre WMI à une GPO:

1. taper *gpmc.msc* dans la barre de recherche windows
2. dans le menu de gauche, cliquer sur la GPO pour laquelle il faut ajouter le filtre WMI
3. à droite, dans *wmi filtering*, sélectionner le filtre WMI à appliquer

C.7 Ajouter une GPO de déployement d'application

Base:

1. placer le fichier *.msi* de l'application dans le share SMB

   > - ouvrir le *server manager*, cliquer sur *local server*
   > - désactiver les paramètres de *internet explorer enhanced security configuration*
   > - télécharger le fichier *.msi* dans IE, ex: `https://chromeenterprise.google/browser/download`

2. ouvrir le *Group Policy Management Editor* (voir section B.2)
3. dans le menu de gauche, faire un clic gauche puis un clic droit sur *computer configuration/policies/software settings/software installation*
4. cliquer sur *new*, puis sur *package*, ensuite sélectionner le fichier *.msi* placé dans le share SMB

Complément (pas obligatoire) – installer uniquement sur une machine:

1. dans la fenêtre *group policy management*, dans le menu de gauche, cliquer sur la GPO de déployement d'application
2. à droite, en-dessous de *security filtering*, retirer le groupe des utilisateurs authentifiés
3. ensuite, cliquer sur *add*, puis sur *object types*, et ajouter les ordinateurs
4. ensuite, taper le nom de machine, puis cliquer sur *check names*

Après avoir appliqué les GPO sur la machine, il faut la redémarrer pour lancer l'installation.

C.8 Ajouter un modèle d'administration

1. ouvrir le *Group Policy Management Editor* (voir section B.2)
2. dans le menu de gauche, faire un clic droit sur *computer management/administrative templates*
3. cliquer ensuite sur *add/remove templates*, puis sur *add*
4. sélectionner le fichier *.adm* qui doit être situé dans le Share SMB

C.9 Installer le rôle *remote access*

1. ouvrir le *server manager*, en haut à droite, cliquer sur *manage*, puis sur *add roles and features*
2. dans *server roles*, cliquer sur *remote access*, dans *role services*, cliquer sur *routing*
3. une fois l'installation terminée, dans le menu de gauche de *server manager*, cliquer sur *remote access*
4. au centre de la fenêtre, faire un clic droit sur le serveur, puis cliquer sur *remote access management*
5. dans le menu de gauche, cliquer sur *directaccess and vpn*
6. ensuite après le chargement, dans le menu de droite, cliquer sur *open rras management*
7. dans la nouvelle fenêtre, clic droit sur le serveur, puis sur *configure and enable routing and remote access*
8. dans *configuration*, sélectionner l'option *network address translation (nat)*

Attention !

- Mettre le DNS sur DC1.
- Mettre la default gateway sur MS1.
- En cas de problème, ouvrir *RRAS management*:
    1. dans le menu de gauche, supprimer *ms1/ipv4/nat*
    2. dans le menu de gauche, faire un clic droit sur *ms1/ipv4/general*, puis sur *new routing protocol*
    3. ajouter le *nat*
    4. dans le menu de gauche, faire un clic droit sur *ms1/ipv4/nat*, puis sur *new interface*
    5. ajouter l'interface sur réseau interne en *private interface connected to private network*
    6. ajouter l'interface en réseau externe en *public interface connected to the internet*, **et** *enable nat on this interface*

D Comment faire le labo 4

D.1 Créer un dossier invisible et changer les accès

1. Créer le dossier (directement dans le filesystem, pas dans le share).
2. Pour modifier les accès au dossier, faire un clic droit sur le dossier, cliquer sur *properties*, puis aller dans l'onglet *security*.
3. Dans le menu de gauche de *server manager*, cliquer sur *file and storage service*, puis sur *shares*.
4. À droite du menu *shares*, cliquer sur *tasks*, puis sur *new share*.
5. Dans *share name*, ajouter un $ à la fin du nom.

Remarque: il faudra taper le $ dans l'explorateur de fichiers pour accéder au share.

D.2 Créer un utilisateur itinérant

1. ouvrir la fenêtre *active directory users and computers*
    (a) ouvrir le *server manager*
    (b) à gauche, cliquer sur *AD DS*
    (c) faire un clic droit sur *DC1*, puis cliquer sur *active directory users and computers*
2. faire un clic droit sur l'utilisateur, puis cliquer sur *properties*, ensuite sélectionner l'onglet *profile*
3. dans *profile path*, donner un lien vers le share (ex: `\\ms1\profiles$\%username%`)

D.3 Créer un utilisateur obligatoire

1. créer un utilisateur itinérant (section: D.2)
2. se connecter avec l'utilisateur et aller dans le dossier qui contient les dossiers de profils de l'utilisateur
3. faire un clic droit sur son dossier, puis cliquer sur *properties*
4. aller dans l'onglet *security*, cliquer sur *edit*, et ajouter l'administrateur du domaine en *full control*
5. se reconnecter en administrateur du domaine, et aller dans le dossier de l'utilisateur
6. modifier l'extension du fichier *ntuser.dat*, dans le dossier du profil de l'utilisateur, en *.man*

Remarques:

- l'administrateur du domaine doit avoir *full control* sur le dossier de l'utilisateur
- pour voir le fichier, il faut activer l'affichage des fichiers cachés

D.4 Vérifier le type d'un profil (itinérant, obligatoire)

1. taper *panneau de configuration* dans la barre de recherche windows
2. cliquer sur *système et sécurité*, puis sur *système*, puis sur *paramètres système avancés*
3. en-dessous de *profil des utilisateurs*, cliquer sur *paramètres*

D.5 Ajouter une GPO pour rediriger les dossiers personnels

1. ouvrir le *Group Policy Management Editor* (voir section B.2)
2. dans le menu de gauche, faire un clic droit sur *user configuration/policies/windows settings/folder redirection/documents*
3. cliquer sur *properties*, dans *setting*, sélectionner *basic*
4. dans *target folder location*, sélectionner *create a folder for each user under the rooth path*
5. *root path*, donner un dossier dans le share (ex: *\\ms1\user_folders*)

Modifier le filtre de sécurité:

1. dans la fenêtre *group policy management*, cliquer sur la GPO
2. à droite, enlever *authenticated users*, et ajouter les utilisateurs pour lesquels on veut que la GPO s'applique
3. aussi ajouter *domain computers*, sinon l'ordinateur ne pourra pas récupérer cette GPO

D.6 Ajouter une GPO pour interdire toutes les applications dans un dossier

1. ouvrir le *Group Policy Management Editor* (voir section B.2)
2. dans le menu de gauche, faire un clic droit sur *computer configuration/policies/windows settings/security settings/software restriction policies*
3. faire un clic droit sur *additional rule*, puis cliquer sur *new path rule*
4. cliquer sur *browse*, puis sélectionner le dossier à bannir

D.7 Ajouter une GPO pour interdire une application avec son hash

1. ouvrir le *Group Policy Management Editor* (voir section B.2)
2. dans le menu de gauche, faire un clic droit sur *computer configuration/policies/windows settings/security settings/software restriction policies*
3. cliquer sur *new software restriction policies*
4. faire un clic droit sur *additional rule*, puis cliquer sur *new hash rule*
5. cliquer sur *browse*, puis sélectionner l'application à bannir

D.8 Joindre le serveur Debian au domaine et permettre aux utilisateurs de s'y logger

1. `realm join domaine<nb>.local --user=administrator --install='/' --verbose`
2. `nano /etc/ssh/sshd_config`

```
KereberosAuthentification yes
KereberosOrLocalPasswd yes
KereberosTicketCleanup yes
KereberosGetASFToken yes
KereberosUseKuserok yes # pour debian 9, pas debian 10
GSSAPIAuthentification yes
GSSAPICleanupCredentials yes
```

Vérification:

1. `login pamela@domaine<nb>.local`
2. `id`