Samba 4

Hubert Hollender

X/Stra

2 juin 2016

Sommaire I

Dimension du domaine

- 1 AD (Ver. 4.1.17)
- 7 serveurs de fichiers membres (Ver. 4.1.17)
- 2 serveurs d'impression (Ver. 3.6.6 et 4.1.21)
- 530 clients dans l'AD (Windows, Linux, Mac)
- 473 utilisateurs
- 142 groupes

Evolution

- Version 1.9.x en 1997 en Workgroup sous HP-UX (`smbpasswd`)
- Entre 1997 et 2006 passage à un controleur de domaine avec base de données (`passdb.tdb`)
- Mise en place d'un openldap en mars pour l'annuaire des utilisateur en 2006 sous IRIX
- Passage sous Linux en 2010
- Samba 4 en mars 2015

Que-ce que Samba4

- **DNS** - Un Service de résolution de noms, avec mise à jour dynamique des entrées et localisation des services avec des enregistrements de type SRV (remplace la résolution des noms NETBIOS d'un domaine NT)
- **LDAP** - Active Directory est un annuaire qui peut être interrogé via LDAP (Spécification LDAP RFC 3377)
- **Kerberos** - un protocole d'authentification réseau définit au MIT puis normalisé par IETF
- Simple Network Time Protocol, version 3 (RFC 1769)
- **MSRPC** - Mise en oeuvre Microsoft du standard DCE RPC
- **SMB / CIFS** - Protocole de partage de ressources des domaines Windows
  - Utilisé pour le partage des fichiers et imprimantes.
  - Un des transports possibles pour MSRPC
  - Déploiement des GPO : partage `sysvol`
  - Scripts de connexion : partage `netlogon`

Installation à partir de zéro I

Configuration de kerberos

```
root@testipcms-ad:~# dpkg-reconfigure krb5-config

Default Realm: TESTIPCMS.IPCMS.UNISTRA.FR    (Royaume (« realm ») \
 Kerberos version 5 par défaut :)
Realm: 127.0.0.1                             (
Administrative Server: 127.0.0.1
```

Ajout des bonnes options dans /etc/fstab

```
user_xattr,acl,barrier=1
```

Iniatialisation de l'AD

```
root@testipcms-ad:~# samba-tool domain provision \
 --realm=TESTIPCMS.IPCMS.UNISTRA.FR --domain=TESTIPCMS \
 --adminpass='toto007' --server-role='domain controller'
```

Iniatialisation de l'AD

- S'il y a une erreur ou si on veut recommencer : Il faut purger les dossiers : `/etc/samba`, `/var/lib/samba/private`
- Copie de `/var/lib/samba/private/krb5.conf` dans `/etc`
- Faire pointer le `/etc/resolv.conf` sur l'AD.

Test de la configuration samba I

Execution de samba en single

```
samba -i -M single
```

Test des différents enregistrements du DNS

```
root@ad:~# host -t SRV _kerberos._udp.testipcms.ipcms.unistra.fr
_kerberos._udp.testipcms.ipcms.unistra.fr has SRV \
record 0 100 88 ad.testipcms.ipcms.unistra.fr.

root@ad:~# host -t SRV _ldap._tcp.testipcms.ipcms.unistra.fr
_ldap._tcp.testipcms.ipcms.unistra.fr has SRV \
record 0 100 389 ad.testipcms.ipcms.unistra.fr.

root@ad:~# host -t A ad.testipcms.ipcms.unistra.fr
ad.testipcms.ipcms.unistra.fr has address 130.79.154.219
```

Test de la configuration samba II

Test de Kerberos (récupération d'un ticket kerberos)

```
root@ad:~# kinit administrator@TESTIPCMS.IPCMS.UNISTRA.FR
Password for administrator@TESTIPCMS.IPCMS.UNISTRA.FR:
Warning: Your password will expire in 41 days on Wed Mar 25 13:47:33 2015

root@ad:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@AD.TESTIPCMS.IPCMS.UNISTRA.FR
Valid starting       Expires              Service principal
11/02/2015 14:15:51  12/02/2015 00:15:51  krbtgt/TESTIPCMS.IPCMS.UNISTRA.FR
        renew until 12/02/2015 14:15:45
```

Test du serveur ldap

```
root@ad:~# ldapsearch -x -h localhost -s base -D cn=administrator,\
cn=Users,dc=testipcms,dc=ipcms,dc=unistra,dc=fr -W
Enter LDAP Password:
   ......
```

Attention !!!

- Les postes windows qui se sont connectés à un domaine AD (Samba 4 ou Windows Server) ne se connecteront plus dans un domaine de style NT (Samba 3).
- C'est un point de non retour à moins de sortir tous les postes clients du domaine et les faire rejoindre à nouveau le domaine (Attention aux profils !)

Conseils

- Il faut tester dans un environnement différent de celui de la production.
- L'idéal est de pouvoir cloner les machines en production. Pour tester la migration.
- J'ai construit un "bac à sable" sous VMware avec les mêmes réseaux mais entièrement isolés des réseaux en production.
- Je clone une machine sous VMware et la connecte sur le(s) réseau(x) du bac à sable.

Migration de Samba 3 II

Mettre le serveur ldap d'équerre

- Tous les utilisateurs doivent avoir un `objectClass` `sambaSamAccount` et `posixAccount`
- Pas d'utilisateur et de groupe avec le même nom. Dans l'AD ils se retrouvent dans le même conteneur.
- Pas de SID d'utilisateur en double. Si ça existe !
- ...

Le nom du domaine :

- A l'ipcms c'est `ipcms1` depuis le début.
- On ne peut pas le changer sans casser le domaine et refaire un nouveau domaine (problème des profils locaux sous windows)
- Au nom du domaine samba 3, il faut ajouter un domaine DNS
- `ipcms1.ipcms.unistra.fr`

Recupération des fichiers du pdc samab 3 dans le repertoire `./dbdir`

```
/var/lib/samba/account_policy.tdb
/var/lib/samba/group_mapping.tdb
/var/lib/samba/passdb.tdb
/var/lib/samba/schannel_store.tdb
/var/lib/samba/secrets.tdb
/var/lib/samba/wins.dat
/var/lib/samba/wins.tdb
/var/run/samba/gencache_notrans.tdb
```

Migration proprement dite

Pendant la migration le serveur ldap doit être fonctionnel et accessible.
Commande de migration :

```
samba-tool domain classicupgrade --dbdir ./dbdir/ \
--use-xattrs=yes --realm=ipcms1.ipcms.unistra.fr \
--dns-backend=SAMBA_INTERNAL \
smb-pdc.conf
```

krb5.conf

```
[libdefaults]
        default_realm = IPCMS1.IPCMS.UNISTRA.FR
        dns_lookup_realm = false
        dns_lookup_kdc = true
```

smb.conf

```
[global]
        workgroup = IPCMS1
        realm = IPCMS1.IPCMS.UNISTRA.FR
        netbios name = IPCMS-AD1
        server role = active directory domain controller
        idmap_ldb:use rfc2307 = yes
        dns forwarder = 130.79.155.252
        ntp signd socket directory = /var/lib/samba/ntp_signd
        load printers = no
        printing = bsd
        printcap name = /dev/null
        disable spoolss = yes

[netlogon]
        path = /var/lib/samba/sysvol/ipcms1.ipcms.unistra.fr/scripts
        read only = No

[sysvol]
        path = /var/lib/samba/sysvol
        read only = No
```

Les serveurs membres I

Options de montage

- La gestion des acl : `acl`
- La gestion des attributs étendus : `user_xattr`
- Protection des transactions contre les pannes : `barrier=1`

DNS

- Faire pointer le `/etc/resolv.conf` vers le DNS de l'AD
- Renseigner le domaine de recherche par défaut `search ipcms1.ipcms.unistra.fr`

NTP

Installer un client NTP pour garantir que le système soit à l'heure

Les serveurs membres II

smb.conf 1/2

```
[global]
    workgroup = IPCMS1
    netbios name = ipcms-servgen
    security = ads
    realm = IPCMS1.IPCMS.UNISTRA.FR
    idmap config *:backend              = rid
    idmap config *:range                = 100000-1999999
    idmap config IPCMS1:default         = true
    idmap config IPCMS1:range           = 100-99999
    idmap config IPCMS1:backend         = ad
    idmap config IPCMS1:schema_mode = rfc2307
    idmap config IPCMS1:cache time  = 1800
```

smb.conf 2/2

```
winbind separator = /
winbind nss info = rfc2307
winbind trusted domains only = no
winbind use default domain = yes
winbind enum users  = yes
winbind enum groups = yes
template homedir = /home/%D/%U
template shell = /bin/false

vfs objects = acl_xattr
map acl inherit = Yes
store dos attributes = Yes

dead time = 0
lock directory = /var/cache/samba
registry shares = yes
```

Les serveurs membres IV

Relance des services

```
/etc/init.d/samba restart
/etc/init.d/winbind restart
```

Modification du fichier /etc/nsswitch.conf

```
passwd:         compat winbind
group:          compat winbind
shadow:         compat

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

Intéger la machine au domaine

```
root@member:~# net ads join -Uadministrator
Enter administrator's password:
Using short domain name -- IPCMS1
Joined 'MEMBER' to dns domain 'ipcms1.ipcms.unistra.fr'
```

Vérifie la bonne jonction au domaine

```
root@member:~# wbinfo -t
checking the trust secret for domain IPCMS1 via RPC calls succeeded
```

Tester la conf kerberos (récupère un ticket kerberos)

```
root@member:~# kinit administrator@IPCMS1.IPCMS.UNISTRA.FR
Password for administrator@IPCMS1.IPCMS.UNISTRA.FR:

root@member:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@IPCMS1.IPCMS.UNISTRA.FR

Valid starting       Expires              Service principal
01/06/2016 18:46:16  02/06/2016 04:46:16  krbtgt/IPCMS1.IPCMS.UNISTRA.FR@IPC
renew until 02/06/2016 18:46:11
```

Relance des services

```
/etc/init.d/samba restart
/etc/init.d/winbind restart
```

Vérifier que les utilisateurs sont visibles

```
root@member: # wbinfo -u
<Liste des utilisateurs de l'AD>
```

Vérifier que les groupes sont visibles

```
root@member: # wbinfo -g
<Liste des groupes de l'AD>
```

Vérifier que la couche nssswitch fonctionne

```
root@member: # getent passwd
<Liste des utilisateurs locaux et de l'AD au format /etc/passwd>
root@member: # getent group
<Liste des groupes locaux et de l'AD au format /etc/passwd>
```

Les groupes primaires de l'AD

Les groupes primaires de l'AD n'apparaissent pas dans les serveurs membres ni avec `wbinfo -g` ni avec `getent group`
Solution :
Dans l'AD mettre des groupes primaires spécifiques à windows dont on n'a pas besoin sur les serveurs membres pour la gestion des droits.

Les serveurs d'impressions

- je n'ai pas réussi à migrer le serveur d'impressions
- j'ai gardé le serveur d'impressions en version 3
- Et j'ai installé un nouveau serveur d'impressions en version 4.1.21 à partir de zéro

Installation des outils RSAT

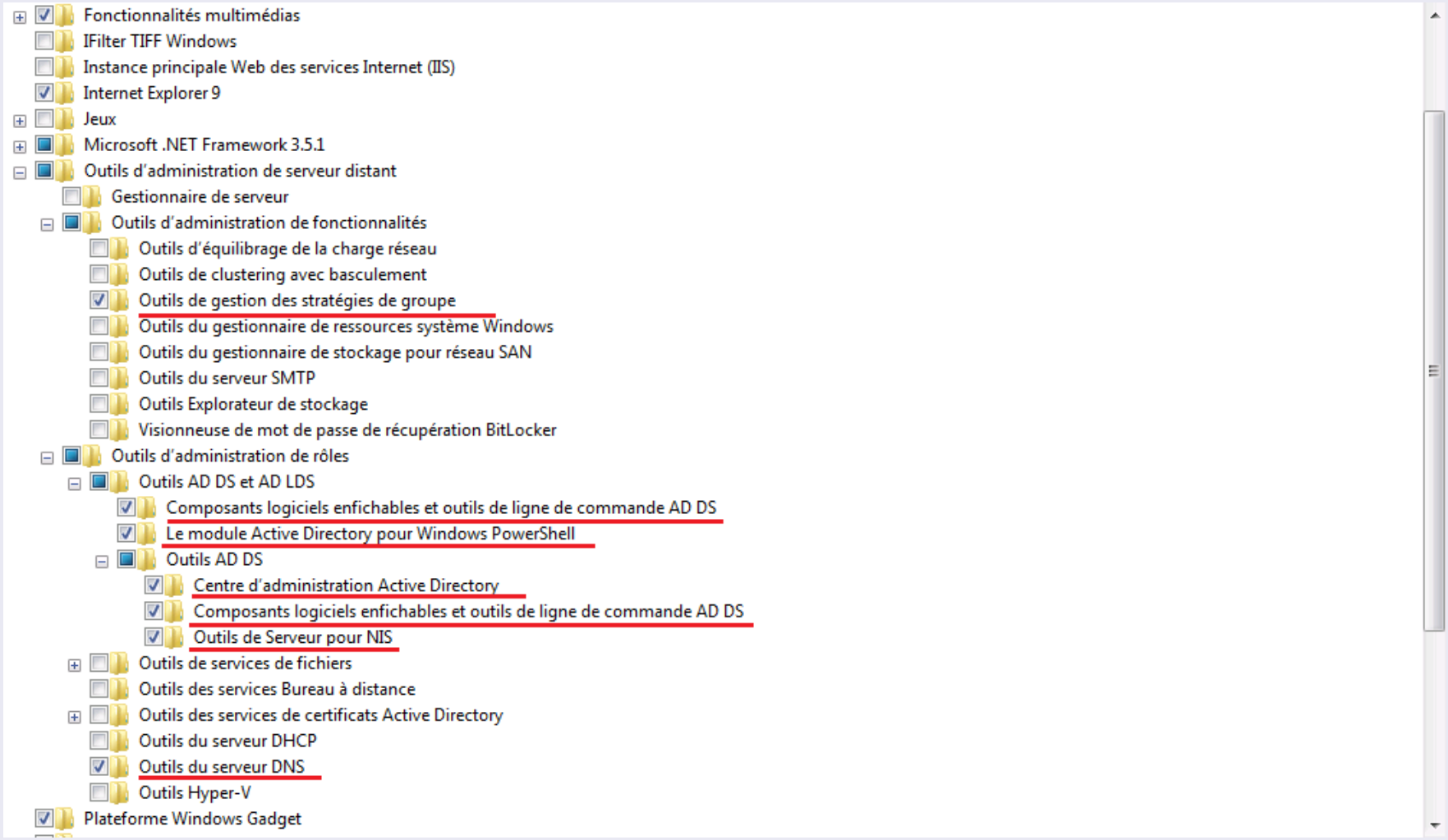
- Installation des outils RSAT (Remote Server Administration Tools)
- Les outils d'administration standard de Microsoft Active Directory peuvent être utilisés pour gérer un Samba4 AD.
- Depuis un poste sous Windows 7 télécharger les Outils d'administration de serveur distant pour Windows 7
- Une fois installé, aller dans Démarrer > Panneau de configuration > Programmes > Activer ou désactiver des fonctionnalités Windows

Activation des outils RSAT

Cocher les fonctionnalités suivantes :

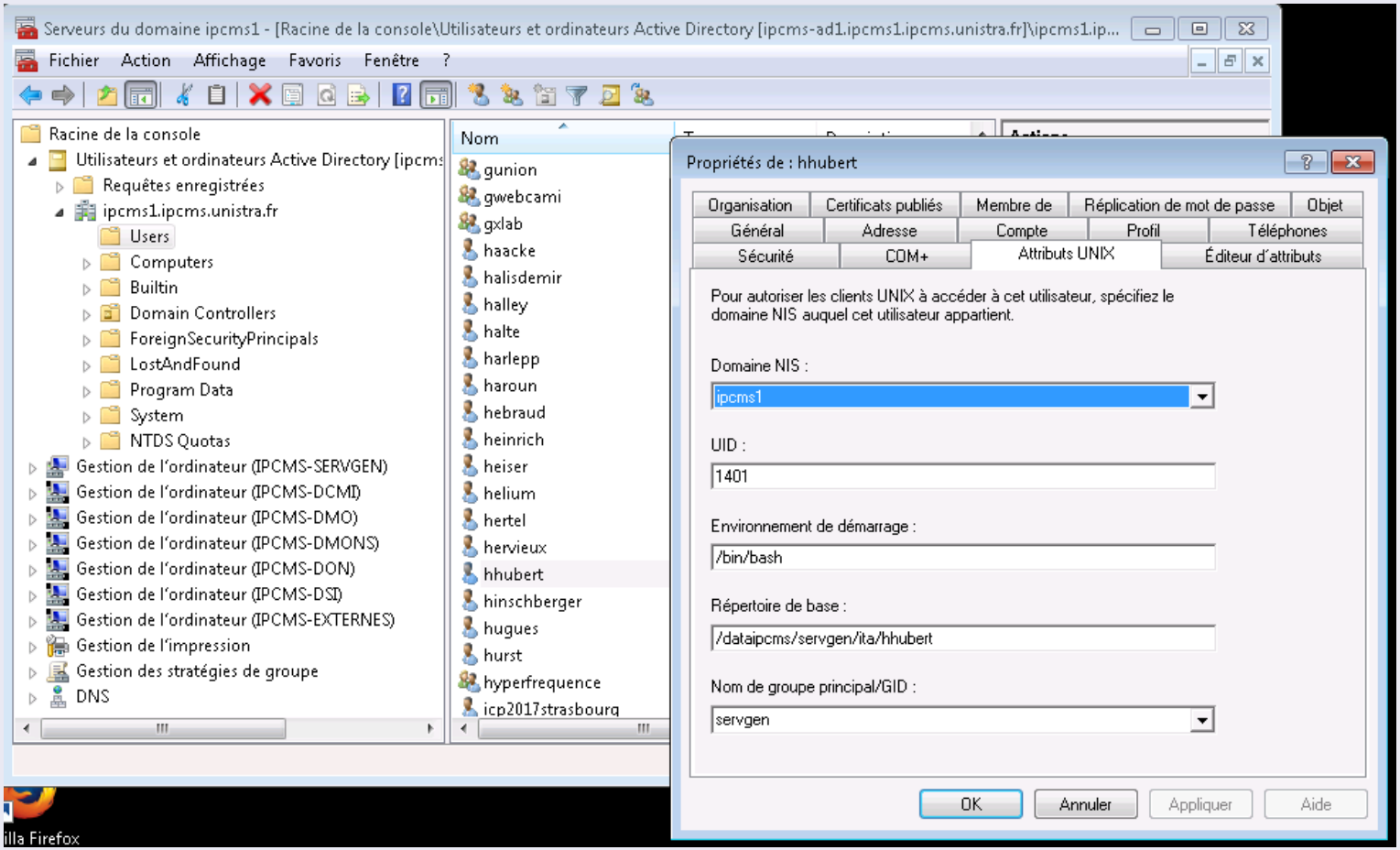
- Outils d'administration de serveur distant > Outils d'administration de fonctionnalités > Outils de gestion des stratégies de groupe
- Outils d'administration de serveur distant > Outils d'administration de rôles > Outils du serveur DNS
- Outils d'administration de serveur distant > Outils d'administration de rôles > Outils AD DS et AD LDS > tout cocher
- Outils d'administration de serveur distant > Outils d'administration de rôles > Outils AD DS et AD LDS > Outils AD DS > tout cocher

Activation des outils RSAT



Les consoles MMC se trouvent dans

Panneau de configuration > Système et sécurité > Outils d'administration



samba-tools

dbcheck	Check local AD database for errors.
delegation	Delegation management.
dns	Domain Name Service (DNS) management.
domain	Domain management.
drs	Directory Replication Services (DRS) management.
dsacl	DS ACLs manipulation.
fsmo	Flexible Single Master Operations (FSMO) roles management.
gpo	Group Policy Object (GPO) management.
group	Group management.
ldapcmp	Compare two ldap databases.
ntacl	NT ACLs manipulation.
processes	List processes (to aid debugging on systems without setproctitle).
rodc	Read-Only Domain Controller (RODC) management.
sites	Sites management.
spn	Service Principal Name (SPN) management.
testparm	Syntax check the configuration file.
time	Retrieve the time on a server.
user	User management.
vampire	Join and synchronise a remote AD domain to the local server.

samba-python

- Un ensemble de modules qui permettent d'administrer tous les aspects d'un serveur Samba
- Le programme incontournable pour l'administration en ligne de commande `samba-tools` est écrit en python et utilise l'API fourni par `samba-python`

Integration des postes linux

- PAM installation de la librairie libpam-winbind et configuration de PAM avec la commande `pam-auth-update` pour debian.
- PBIS `https://www.powerbrokeropen.org/`
- sssd `https://fedorahosted.org/sssd/`

Les limites de Samba 4

- Active Directory Web Services (ADWS) pas implémenté
- => on ne peut pas administrer l'AD avec powershell qui utilise ADWS

Aspects non expérimentés

- migration d'un serveur DC Windows vers Samba 4
- ajout d'un serveur DC secondaire
- Installation Samba 4 comme RODC
- Samba en cluster ctdb
- les versions 4.2 4.3 et 4.4 de Samba

Prochaines étapes

- Upgrade de samba vers la version 4.2 ou 4.3
- Interfacer toutes les applis web avec l'AD (actuellement l'ancien openldap est encore en route => Obligation de maintenir à jour les comptes)
- Changer PBIS vers une solution plus "open"

Pour trouver des infos ...

- https ://www.samba.org/
- https ://wiki.samba.org/index.php/Main_Page
- https ://dev.tranquil.it/wiki/Samba4
- nntp ://news.gmane.org/gmane.network.samba
- nntp ://news.gmane.org/gmane.network.samba-announce
- Implementing Samba 4 By Marcelo Leal Publisher : Packt Publishing Final Release Date : April 2014 Pages : 284