Intégration GNU/Linux dans un domaine Active Directory

Fix Me! commande en vrac à mettre en forme mais surtout tester la totalité des impacts d'une intégration dans l'AD sur les comptes locaux, les plages d'ID utilisées...

Fix Me! étudier les solutions commerciales ou non qui sont spécialisées sur l'intégration de machines Linux au sein de l'AD.

Pré-requis

- Un serveur Linux standard à intégrer au domaine : srv-linux
- Deux contrôleurs de domaine Active Directory : srv-pdc1 srv-pdc2.
- Domaine nommé : example.local.
- Compte administrateur du domaine : admin-dom.

```
[root@srv-linux ~]# hostname -s
srv-linux
[root@srv-linux ~]# hostname -f
srv-linux.example.local
[root@srv-linux ~]# vi /etc/hosts

[root@srv-linux ~]# chkconfig --level 345 smb on
[root@srv-linux ~]# chkconfig --level 345 winbind on

[root@srv-linux ~]# chkconfig --list smb
smb             0:arrêt 1:arrêt 2:arrêt 3:marche        4:marche
5:marche        6:arrêt
[root@srv-linux ~]# chkconfig --list winbind
winbind         0:arrêt 1:arrêt 2:arrêt 3:marche        4:marche
5:marche        6:arrêt


[root@srv-linux ~]# cat /etc/krb5.conf
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = EXAMPLE.LOCAL
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 forwardable = yes
```

```
[realms]
 EXAMPLE.LOCAL = {
  kdc = srv-pdc1.example.local:88
  kdc = srv-pdc2.example.local:88
  #admin_server = srv-pdc1.example.local:749
  default_domain = example.local
 }

[domain_realm]
 .example.local = EXAMPLE.LOCAL
 example.local = EXAMPLE.LOCAL

[kdc]
 profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
 pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   krb4_convert = false
}

[root@srv-linux ~]# kinit admin-dom
Password for admin-dom@EXAMPLE.LOCAL:

[root@srv-linux ~]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: admin-dom@EXAMPLE.LOCAL

Valid starting     Expires            Service principal
07/08/09 13:57:19  07/08/09 23:57:25  krbtgt/EXAMPLE.LOCAL@EXAMPLE.LOCAL
        renew until 07/09/09 13:57:19


Kerberos 4 ticket cache: /tmp/tkt0
klist: You have no tickets cached

[root@srv-linux ~]# cat /etc/nsswitch.conf | grep winbind
passwd:     files winbind
shadow:     files winbind
group:      files winbind

[root@srv-linux ~]# cp /etc/samba/smb.conf /etc/samba/smb.conf.orig

[root@srv-linux ~]# cat /etc/samba/smb.conf
[global]
        workgroup = EXAMPLE
        realm = EXAMPLE.LOCAL
```

```
        server string = serveur infrastructure srv-linux
        security = ADS
        allow trusted domains = No
        password server = srv-pdc1.example.local
        username map = /etc/samba/smbusers
        idmap backend = rid:example=10000-20000
        idmap uid = 10000-20000
        idmap gid = 10000-20000
        winbind separator = /
        winbind cache time = 60
        winbind enum users = Yes
        winbind enum groups = Yes
        cups options = raw

[root$]
        path = /
        valid users = "@EXAMPLE/admins du domaine"
        admin users = "@EXAMPLE/admins du domaine"
        write list = "@EXAMPLE/admins du domaine"
        read only = No
        browseable = No

[tmp]
        path = /tmp
        valid users = "@EXAMPLE/admins du domaine"
        read only = No

[root@srv-linux ~]#net join ads -U admin-dom

[root@srv-linux ~]# service smb restart
[root@srv-linux ~]# service winbind restart
```

Tests

root@srv-linux tmp]# smbstatus

Quelques commandes pour vérifier que tout fonctionne

Remarque : Avant de saisir les commandes suivantes, il faut vérifier que le serveur Samba est correctement ajouté dans la liste des serveurs du « gestionnaire de serveurs » du contrôleur de domaine Windows. Si ce n'est pas le cas, il faut peut-être attendre quelques minutes pour que la mise à jour se fasse.

La commande suivante doit donner la liste des utilisateurs du domaine.

```
wbinfo -u
```

Celle-ci la liste des groupes du domaine.

```
wbinfo -g
```

Celle-ci permet de vérifier que les utilisateurs du domaine sont ajoutés à la liste des utilisateurs du serveur Linux avec les bons uid.

```
getent passwd
```

La même chose avec les groupes d'utilisateurs.

```
getent group
```

Cette commande permet de vérifier qu'un utilisateur particulier est correctement reconnu.

```
wbinfo -a MonDomaine/tony%LeMotDePasse
```