GESTION D'UTILISATEUR/ORDINATEUR

- Ajout d'un serveur à l'active directory

Ajout d'un serveur à l'active directory

Prérequis

- Avoir un serveur linux
- Mettre les serveur active directory en tant que serveur DNS
- Mettre le domaine de recherche
- Avoir un nom de serveur respectant la bonne nomenclature

Installation des paquets nécessaire

- Installer le serveur de temps NTP:

```
apt -y install realmd sssd sssd-tools libnss-sss libpam-sss adcli samba-common-bin
oddjob oddjob-mkhomedir packagekit
```

- Interroger l'active directory

```
root@linux-test:~# realm discover megaproduction.local
megaproduction.local
  type: kerberos
  realm-name: MEGAPRODUCTION.LOCAL
  domain-name: megaproduction.local
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
```

- Joindre le domain

```
root@linux-test:~# realm join megaproduction.local
Password for Administrator:
root@linux-test:~#
```

> Le serveur est ajouté sur l'active directory !!

- Parfois l'ajout de fonctionne pas alors on peut ajouter le serveur de la façon suivante

```
➜  ~ realm join -v --membership-software=samba megaproduction-gr2.local -U
Administrateur


 * Resolving: _ldap._tcp.megaproduction-gr2.local
 * Performing LDAP DSE lookup on: 192.168.201.4
 * Successfully discovered: MEGAPRODUCTION-GR2.LOCAL
Password for Administrateur:
 * Unconditionally checking packages
 * Resolving required packages
 * LANG=C LOGNAME=root /usr/bin/net --configfile /var/cache/realmd/realmd-smb-
conf.9AYTJ3 -U Administrateur --use-kerberos=required ads join MEGAPRODUCTION-
GR2.LOCAL
Password for [MEG-G2\Administrateur]:
Using short domain name -- MEG-G2
Joined 'BST-G2-FRONT-01' to dns domain 'MEGAPRODUCTION-GR2.LOCAL'
 * LANG=C LOGNAME=root /usr/bin/net --configfile /var/cache/realmd/realmd-smb-
conf.9AYTJ3 -U Administrateur ads keytab create
Es * /usr/sbin/update-rc.d sssd enable
p * /usr/sbin/service sssd restart
oir * Successfully enrolled machine in realm
```

- Voire les infos d'un utilistateur en particulier:

```
root@linux-test:~# id kvega@megaproduction.local
uid=683401106(kvega@megaproduction.local) gid=683400513(domain
users@megaproduction.local) groups=683400513(domain
users@megaproduction.local),683401103(gg-admin-
domain@megaproduction.local),683401104(gg-admin-sys@megaproduction.local)
```

- Pour se connecter sans mettre le nom de domaine derrière le nom de l'utilisateur
  - Éditer le fichier */etc/sssd/sssd.conf*
  - Modifier la ligne contenant `use_fully_qualified_names = False`
  - Redémarrer le service sssd
- Pour qu'à la première connexion de l'utilisateur sur le serveur son Home de créé

- Éditer le fichier */etc/pam.d/common-session*
- Ajouter à la fin

```
session optional        pam_mkhomedir.so skel=/etc/skel umask=077
```

- Tester la connexion en tant qu'utilisateur de l'active directory

```
root@linux-test:~# su - kvega
Creating directory '/home/kvega@megaproduction.local'.
kvega@linux-test:~$ pwd
/home/kvega@megaproduction.local
```

> **LISTE des PORTS a autoriser: 389, 88, 464 et 53**