Clients légers et authentification Active Directory

Contexte

- Milieu d'enseignement (salles machines)
- Utilisation de Linux et Windows
- Solution classique :
  - PCs avec des installations sur le disque local

Problèmes

- Administration pénible :
  - les étudiants « bidouillent »
  - les disques « lachent »
  - il faut installer, réinstaller, renouveler les machines, maintenir à jour

Proposition

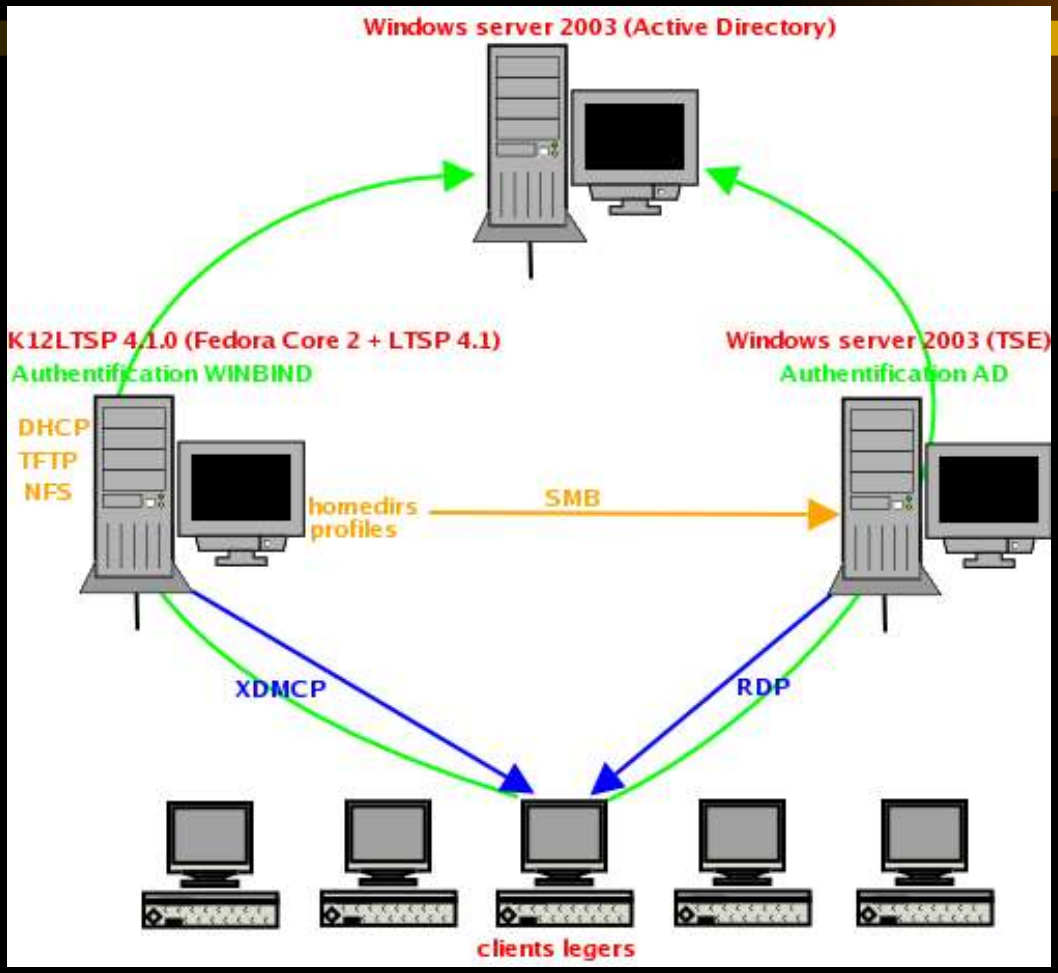
- Clients légers

Contraintes

- Réutiliser le matériel existant
- Continuer à créer les comptes sur le contrôleur de domaine

- Ne pas perdre de vue le fait que Windows est utilisé majoritairement
- Pouvoir utiliser les périphériques locaux

Solution


Windows server 2003 (Active Directory)
K12LTSP 4.1.0 (Fedora Core 2 + LTSP 4.1)
Authentification WINBIND
Windows server 2003 (TSE)
Authentification AD
DHCP
TFTP
NFS
homedirs
profiles
SMB
XDMCP
RDP
clients legers

Mise en oeuvre

- Serveurs :
  - Installation de Windows server 2003 (AD)
  - Installation de K12LTSP
  - Installation de Windows server 2003 (TSE)
- Clients légers :
  - Vérifier que les cartes réseau sont PXE
  - Relever les caractéristiques (@MAC, type souris, résolution, fréquences écran)
  - Enlever les DD

Serveur AD

- Installation de W2K3
- Windows update
- Dans "Gérer votre serveur"
  - "Ajouter ou supprimer un rôle"
  - "Contrôleur de domaine (Active Directory)"
  - si nécessaire, faire en sorte que le contrôleur de domaine soit serveur DNS

Serveur K12LTSP

- Installation de K12LTSP
  - /opt/ltsp/templates/k12linux/K12Linux-LTSP-initialize
  - yum -y update
  - reboot

Serveur K12LTSP (suite)

- Dans /opt/ltsp/i386/etc/lts.conf

```
[nom_client_léger_ou_IP_ou_adrMAC]
        # clavier fr
        XkbSymbols        = "fr(pc105)"
        XkbModel          = "pc105"
        XkbLayout         = "fr"

        # souris à molette
        X_MOUSE_PROTOCOL   = "PS/2"
        X_MOUSE_DEVICE     = "/dev/psaux"
        X_MOUSE_RESOLUTION = 400
        X_MOUSE_BUTTONS    = 3
        X_ZAxisMapping     = "4 5"

        # résolution
        X_COLOR_DEPTH      = 16
        X_MODE_0           = 1024x768

        # session X
        SCREEN_01          = startx
```

Serveur K12LTSP (suite)

- Configuration de Winbind (fait partie de Samba)
  - Active Directory = LDAP + Kerberos
  - Vérifier donc que samba est compilé avec ce qu'il faut

    smbd -b | grep KRB
    smbd -b | grep LDAP
  - Exécuter « authconfig »

    * dans "User Information" cocher "Use Winbind"
    * dans "Authentication" cocher "Use Winbind Authentication"
      - Security Model = ads
      - Domain = EXEMPLE
      - Domain Controllers = IP_CONTROLEUR_DOMAINE
      - ADS Realm = EXEMPLE.MATHRICE.COM
      - Template Shell = /bin/bash

    * cliquer sur "Join Domain" pour ajouter la machine k12ltsp dans le domaine active directory

    net ads join -w EXEMPLE -S IP_CONTROLEUR_DOMAINE -U Administrateur

    * cliquer sur "Ok" pour lancer le service winbind

Serveur K12LTSP (suite)

- Configuration de Winbind (fichiers modifiés)
  - /etc/pam_smb.conf
  - /etc/nsswitch.conf
  - /etc/pam.d/system-auth
  - /etc/krb5.conf
  - /etc/krb.conf
  - /etc/samba/smb.conf

Serveur K12LTSP (suite)

- Tests de Winbind

  wbinfo -p wbinfo -t
  net ads info
  net ads status -U Administrateur
  tdbdump /etc/samba/secrets.tdb

  tdbdump /var/cache/samba/winbindd_idmap.tdb
  tdbdump /var/cache/samba/winbindd_cache.tdb

  wbinfo -u wbinfo -g
  getent passwd getent group

  Dans /etc/samba/smb.conf (suppression de « Nom_Domaine\ ») :
  winbind use default domain = yes

Serveur K12LTSP (suite)

- Tests de connexion utilisateur

gdm-restart ; service sshd restart

mkdir /home/EXEMPLE

Créer un user sur AD puis son répertoire de base sur linux (script createhome.sh)

```
#! /bin/sh
usage() {
        echo "usage: $0 nom_de_compte_utilisateur_AD" ; exit 1
}
[ $# -ne 1 ] && usage
if id $1 > /dev/null 2>&1; then
        mkdir /home/EXEMPLE/$1
        chmod 700 /home/EXEMPLE/$1
        (cd /etc/skel ; find . -depth -print | cpio -dump /home/EXEMPLE/$1)
        chown -R `id -u $1`.`id -g $1` /home/EXEMPLE/$1
else
        echo "le compte \"$1\" n'existe pas"
fi
```

Autres possibilités : cron, pam_mkhomedir

Serveur TSE

- Installation de W2K3
- Windows update
- Dans "Gérer votre serveur"
  - "Ajouter ou supprimer un rôle"
  - "Terminal Server"

Serveur TSE (suite)

- Configuration de TSE
  - Pour faire simple, ajouter le groupe "Utilisateurs du domaine" dans le groupe "Utilisateurs du Bureau à distance"
  - Exécuter « gpedit.msc »
    Dans :
    Configuration ordinateur
    Modèles d'administration
    Composants Windows
    Services Terminal Server
    Double-cliquer sur "Répertoire de base utilisateur Terminal Server"
    - cocher "Activé"
    - Emplacement = Sur le réseau
    - Chemin d'accès à la racine du répertoire = \\nom_srvLinux_ou_IP
    - Lettre du lecteur = H:

Configuration de LTSP pour utiliser TSE

- Dans /opt/ltsp/i386/etc/lts.conf

```
# session Windows
SCREEN_02          = rdesktop
RDP_SERVER         = nom_srvTSE_ou_IP
RDP_OPTIONS        = -f -k fr -d EXEMPLE
```

- rdesktop de lbe est « bug »é. Le remplacer

  cf http://www.mail-archive.com/ltsp-discuss@lists.sourceforge.net/msg20143.html

- Dans /etc/samba/smb.conf

```
[homes]
  comment = Home Directories
  browseable = no
  writable = yes
```

- chkconfig smb on ; service smb start

Profils itinérants

- Dans /etc/samba/smb.conf

```
[Profiles]
   comment = Profiles dir
    path = /home/profiles
    browseable = no
    guest ok = yes
   writable = yes
```

```
mkdir /home/profiles
chmod a+rwxt /home/profiles
service smb restart
```

Profils itinérants (suite)

- Sur TSE
  - Exécuter « gpedit.msc »

    Dans :

    Configuration ordinateur
    Modèles d'administration
    Composants Windows
    Services Terminal Server
    Double-cliquer sur "Définir le chemin d'accès des profils itinérants Terminal Server"

    - cocher "Activé"
    - Chemin du profil = \\nom_srvLinux_ou_IP\Profiles

Périphériques locaux

- Sous LTSP :
  - Principe :
    - supermount + samba sur les clients légers
    - automounter + mount.smbfs sur le serveur

    Supermount :
    - Pas de montage/démontage
    - Pas de timeout
    - Le média peut être éjecté à tout moment

Périphériques locaux (suite)

- Sous LTSP (suite):
  - Installer/mettre à jour ltsp_localdev via ltspadmin
  - Dans /opt/ltsp/i386/etc/lts.conf

```
# Lecteur CDROM IDE
    LOCAL_DEVICE_01    = /dev/hdc:cdrom

# Lecteur de disquette
    LOCAL_DEVICE_02    = /dev/fd0:floppy

# Périphériques USB
    RCFILE_01          = "usb"
    MODULE_01          = usbcore
    MODULE_02          = usb-uhci
    MODULE_03          = usb-storage
    LOCAL_DEVICE_03    = /dev/sda1:usbkey
    LOCAL_DEVICE_03    = /dev/sr0:usbcdrom
    LOCAL_DEVICE_03    = /dev/sdb:usbfloppy
```

Périphériques locaux (suite)

- Sous LTSP (suite):
  - Dans /etc/auto.master
    /misc /etc/auto.misc --timeout=60
  - Dans /etc/auto.misc
    ws001cdrom -fstype=smbfs,workgroup=LTSP,guest ://ws001/cdrom
    ws001floppy -fstype=smbfs,workgroup=LTSP,fmask=666,dmask=777,guest,username=nobody,rw ://ws001/floppy
    ws001usbkey -fstype=smbfs,workgroup=LTSP,fmask=666,dmask=777,guest,username=nobody,rw ://ws001/usbkey
    ws001usbcdrom -fstype=smbfs,workgroup=LTSP,guest ://ws001/usbcdrom
    ws001usbfloppy -fstype=smbfs,workgroup=LTSP,fmask=666,dmask=777,guest,username=nobody,rw ://ws001/usbfloppy
  - chkconfig autofs on ; service autofs start

Périphériques locaux (suite)

- Sous TSE:
  - Problème : avec rdesktop, pas de « local drive mapping »
  - Mais, comme les clients légers font tourner samba, un « net view \\ws001 (sous Windows)» ou « smbclient -L ws001 -N (sous Linux)» nous montre les « shares » déclarés dans lts.conf. Il suffit donc de connecter les « shares » sur des lecteurs logiques

quid de la sécurité ? confidentialité ?

Résolution de problèmes

- Si « kinit failed: Clock skew too great » alors problème de synchronisation qui peut empêcher Kerberos de fonctionner correctement

  Sous Windows, il est possible de se synchroniser avec une source NTP. Dans une fenêtre DOS :

  w32tm /config /syncfromflags:manual /manualpeerlist:IP1,IP2
  w32tm /config /update

Résolution de problèmes (suite)

- Si « tdb(/var/cache/samba/winbindd_idmap.tdb): rec_read bad magic 0x42424242 at offset=262512 » alors probablement une corruption dans les bases Winbind

  Solution : arrêter winbind, arrêter smb, supprimer le contenu de /var/cache/samba, relancer winbind, relancer smb

  Attention : le mapping change

Résolution de problèmes (suite)

- Parfois, le mapping uid/sid change ce qui cause des problèmes d'accès aux homedirs

  Solution : faire tourner un cron qui vérifie que les homedirs, le répertoire des profils et certains fichiers/répertoires dans /tmp correspondent aux logins.

Pour aller plus loin

- Optimisation et administration de TSE
- Gestion des licences sous TSE
- Installation des applications sous TSE
- ...

The Definitive Guide to Windows Server 2003 Terminal Services (http://www.realtimepublishers.com/)

Perspectives

- Citrix Metaframe

Conclusion

- ça a l'air de marcher
- Autre alternative : remplacer le serveur AD par un serveur Linux (NIS/LDAP) + contrôleur de domaine (samba)