Version du : dimanche 12 janvier 2014

Machine cible : IBM thinkcentre (MT-M 8183-QVG) (RAM : 512 Mo DDR1)

Objectif : Installer une machine exploitée par un OS Debian GNU/Linux (stable, testing, sid) qui s'intègre dans un domaine SCRIBE : dans le cadre de ce tutoriel, l'OS choisi est wheezy.

Interface graphique : MATE (fork de GNOME 2)
Gestionnaire de session : lightdm

Préliminaires :

(1) Schéma de partionnement (non automatique) du disque dur de 40 Go (le système de fichiers formaté en ext3 permet l'utilisation d'un OS *BSD si besoin !):

/dev/sda1	ext3	/	1 Go
/dev/sda2	swap		2 Go
/dev/sda3	ext3	/	10 Go
/dev/sda5	ext3	/var/cache/apt	2 Go
/dev/sda6	ext3	/home	reste

(2) Les fichiers nécessaires seront automatiquement copiés à la racine du répertoire du compte root de l'OS debian (sda3). Le fichier qui doit être modifié est « intranet.sh ».

Commentaires :

- 3 partitions primaires + 2 partitions logiques pour la 4ème primaire
- /dev/sda1 → racine de l'OS Debian qui permettra de sauver et de réinstaller l'OS principal = OS2
- /dev/sda2 → partition swap commune aux deux OS GNU/Linux
- /dev/sda3 → racine de l'OS principal Debian GNU/Linux = OS1
- /dev/sda5 → système de fichiers qui contient les packages dans /var/cache/apt/archives/ (copie sur d'autres machines via ssh ou un disque dur externe ou clef USB ou protocole NFS ou création d'un « mirroir » local) → avantage : dans l'hypothèse d'une ré-installation, ce serait inutile de télécharger tous les paquets !
- /dev/sda6 → système de fichiers monté sur /home de l'OS1 (cette partition contiendra l'image de la partition sda3 de la racine de l'OS1 et les comptes locaux/ldap des utilisateurs + /home/wine)

Les étapes :

(1) On télécharge l'ISO du DVD multi-arch de la Debian GNU/Linux wheezy.

URL : http://cdimage.debian.org/debian-cd/7.3.0/multi-arch/iso-dvd/

Dans un xterm, on vérifie les différentes signatures cryptographiques :

$ md5sum -c MD5SUMS
$ sha1sum -c SHA1SUMS
$ sha256sum -c SHA256SUMS
$ sha512sum -c SHA512UMS

Puis, on grave ou on teste via VirtualBox.

(2) Installation d'un 1er système minimal (OS2) Debian (pas d'interface graphique) sur /dev/sda1 + grub + reboot → création d'un compte prof (pour les transferts éventuels via ssh d'images sur le réseau)

(3) Installation d'un 2ème système minimal (OS1) Debian (pas d'interface graphique) (via dhcp + compte adminprof créé + infos ci-dessus + café !) + reboot → boot automatique sur l'OS1 !

(4) (a) Se connecter avec le compte root créé de l'OS1

(b) Lancer le script et reboot automatique de la machine :

 # bash integrdom_debian.sh

ou

 # bash prepalin.sh && bash integrdom.sh

(5) Avec GRUB, choisir l'OS2 et se connecter en root :

(a) Monter le système de fichiers de la partition sda6 sous /mnt/sda6 :

mkdir -p /mnt/sda{3,6} && mount /dev/sda6 /mnt && cd /mnt/sda6

(b) Sauvegarde de la racine de l'OS1 à coup de 50 Mo, démontage puis reboot automatique (sauf si il y a des erreurs → un café !) :

 # dd if=/dev/sda3 of=.debian_wheezy_sda3.img bs=50M && chmod 700 .debian_wheezy_sda3.img && cd && umount /mnt/sda6 && reboot

(6) Boot automatique sur l'OS1 puis :

(a) Vérifications et tests à partir du compte adminprof

(b) Création de deux comptes locaux (au cas où...) :

 # adduser prof && adduser invite (pour les élèves !) → le profil des comptes (locaux et ldap) est créé à partir de « /etc/skel/ ».

(c) Paramétrer l'extinction automatique tous les jours à 21 h 00 :

crontab -e
00 21 * * * /sbin/shutdown -h now

(7) Quand tout fonctionne, on clone le disque **entier** (lourd !) en lançant en RAM le DVD de Debian GNU/Linux (ou autre !) à l'aide de la commande « dd ». L'image est sauvegardée sur un disque dur externe via USB (/dev/sdb1 + café !) :

Sans compression :

 # mount /dev/sdb1 /mnt && cd /mnt
 # dd if=/dev/sda of=ibm_debian_debian.img bs=50M && cd && umount /mnt && init 0

Ou en compressant l'image :

 # mount /dev/sdb1 /mnt && cd /mnt
 # dd if=/dev/sda | gzip -v6 | dd of=ibm_debian_debian.img.gz bs=25M && cd && umount /mnt && init 0

(8) Puis on clone (restauration) des machines identiques en lançant en RAM le DVD de Debian GNU/linux (café !) :

Sans compression :

 # mount /dev/sdb1 /mnt && cd /mnt
 # dd if=ibm_debian_debian.img of=/dev/sda bs=50M && cd && umount /mnt && init 0

Ou en décompressant l'image :

 # mount /dev/sdb1 /mnt && cd /mnt
 # zcat ibm_debian_debian.img.gz | dd of=/dev/sda bs=50M && cd && umount /mnt && init 0

(9) Reboot et boot sur les deux OS pour :

(a) changer le nom de la nouvelle machine (sous debian : /etc/hostname)

(b) changer éventuellement le nom de la carte réseau (eth0 vers eth1 ou autre) (sous Debian : /etc/network/interfaces)

(c) changer les mots de passe de root, de prof (OS2) et d'adminprof (OS1) : ils sont donnés en fonction du nom de la machine !

(d) Sauvegarder par clonage la partition sda3 de l'OS1 en un fichier caché sur la partition sda6 :

 # mount /dev/sda6 /mnt/sda6 && cd /mnt/sda6
 # dd if=/dev/sda3 of=.debian_wheezy_sda3.img bs=50M && chmod 700 .debian_debian_sda3.img && cd && umount /mnt/sda6 && init 0

ANNEXE N°1 : un script modulaire

licence.txt

GNU GPL

readme.txt

```
################################################################################
# Jean-François Mai - Conseiller TICE (collège République Cholet)
# Académie : Nantes
#
# Script "d'intégration" d'un client Debian GNU/Linux dans le domaine contrôlé par un serveur SCRIBE 2.*
#
# version 0.3 (avec proxy system)
# début : jeudi 27 décembre 2013
# fin : mercredi 1 janvier 2014
# --> testé et validé avec un serveur Scribe 2.3 (archi : amd64) virtualisé à l'aide de VirtualBox et deux clients virtuels Debian GNU/Linux wheezy (stable, archi : x86) virtualisés à l'aide de VirtualBox
#
################################################################################

# todo
(0) À tester sur le terrain !!!!
(1) Création d'un serveur local de paquets
(2) Éléments de sécurité -> notamment avec les serveurs ldap et samba; users.txt --> password à crypter
(3) wine et/ou playonlinux
```

(4) Création de scripts pour sortir du domaine
(5) Automatiser le nettoyage du /home via "nettoyer.sh"
(6) Paramétrer le pare-feu Netfilter
(7) Création de conditions pour des ré-installations multiples sur le même système Debian (ex : si arrêt des scripts pour cause d'erreurs, pour des tests ultérieurs, actuellement les fichiers *old créés la 1ère fois sont écrasés lorsque les scripts sont relancés une 2ème fois...
todo

Préliminaire : avoir une Debian GNU/Linux de base installée sur une partition --> pas d'interface graphique

Informations concernant l'architecture réseau de l'EPLE : à modifier (si besoin) avant de lancer les scripts les fichiers du répertoire "config"

(1) config/intranet.sh
(2) config/users.txt

intranet.sh

```
#!/bin/bash

# Informations concernant l'architecture réseau de l'EPLE : à modifier (si besoin) avant de lancer les scripts les fichiers du répertoire "config"
# (1) intranet.sh (ce fichier)
# (2) users.txt (dans le même répertoire)

export ip_scribe="10.149.46.65" && # IP de src-dc1 dans la zone DMZ privée
export ip_proxy="10.149.46.126" && # IP Amon dans la zone DMZ privée
export port_proxy="3128" #&&
#export ent="www.republique.e-lyco.fr"
```

integrdom_debian.sh

```
#!/bin/bash

# Préliminaire : avoir une Debian GNU/Linux de base installée sur une partition --> pas d'interface graphique

./prepalin.sh &&
./integrdom.sh
```

prepalin.sh

```
#!/bin/bash

# Ce script installe automatiquement un système Debian GNU/Linux fonctionnel et autonome :
# (1) gestionnaire de session LIGHTDM
# (2) environnemnt graphique : MATE --> à voir enlightenment, lxde

source config/intranet.sh &&

touch ~/report.txt &&
echo "Partie n°1" > ~/report.txt &&
scripts/./01.sh | tee ~/report.txt &&
echo "Partie n°2" >> ~/report.txt &&
```

scripts/./02.sh | tee -a ~/report.txt

01.sh

```
#!/bin/bash

# Partie n°1 : téléchargement et installation des logiciels

# Copie des scripts sur la racine du compte root + "renommage"

cd &&
mv debian_gnu_linux/ integrdom &&
cd integrdom/ &&

# Paramétrage des sources des paquets --> todo : créer un dépôt local !

mv /etc/apt/sources.list /etc/apt/sources.list.old &&
cp -f data/sources.list /etc/apt/ &&

# Synchronisation de la liste des paquets de la machine locale

apt-get update && # des avertissements sur les clés cryptographiques non reconnues

# Importation des signatures de clés cryptographiques

wget -q -O - https://dl-ssl.google.com/linux/linux_signing_key.pub | apt-key add - &&
apt-get --yes --quiet --allow-unauthenticated install mate-archive-keyring &&
apt-get --yes --quiet --allow-unauthenticated install pkg-mozilla-archive-keyring &&
apt-get --yes --quiet --allow-unauthenticated install deb-multimedia-keyring &&

# Re-synchronisation de la liste des paquets de la machine locale

apt-get update && # cette fois-ci, les signatures sont reconnues

# debconf en mode silencieux

export DEBIAN_FRONTEND="noninteractive" &&
export DEBIAN_PRIORITY="critical" &&

# paquets binaires téléchargés et installés --> serveur local de paquets --> café !

apt-get -y install xorg xterm vim openssh-server mate-core mate-desktop-environment lightdm flashplugin-
nonfree geogebra iceweasel iceweasel-l10n-fr vlc audacity pinta mplayer libdvdcss2 wine winetricks
google-chrome-stable google-earth-stable ntpdate xscreensaver xscreensaver-gl-extra xscreensaver-data-
extra gimp sweethome3d &&
apt-get -t wheezy-backports -y install libreoffice libreoffice-l10n-fr &&
apt-get -y install libnss-ldap libpam-mount cifs-utils numlockx &&

# Interface graphique de apt --> bof !

#apt-get install synaptic &&

# Pour wine

#apt-get -y install curl p7zip-full playonlinux mono-complete donf-editor &&
```

```
# Pour rendre automatique le mises à jour de sécurité --> bof !

#apt-get -y unattended-upgrades &&
#cp -f data/20auto-upgrades /etc/apt/apt.conf.d/ &&

# debconf remis dans sa configuration initiale (mode "verbeux")

export DEBIAN_FRONTEND="dialog" &&
export DEBIAN_PRIORITY="high"
```

02.sh

```
#!/bin/bash

# Partie n°2 : paramétrage du client

#source config/intranet.sh &&

# "Blacklister" pcspkr --> erreurs au boot !

cp -f data/blacklist.conf /etc/modprobe.d/ &&

# Paramétrage de iceweasel : ajout de Firefox Mozilla dans le menu "Logiciels" de MATE (changement d'icône en réalité)...

cp -f data/firefox.desktop /usr/share/applications/ &&
cp -f data/firefox.png /usr/share/pixmaps/ &&

# ... paramétrage de l'URL de l'ENT de l'établissement (ici l'ENT e-lyco du collège République de Cholet)

cp -f data/elyco.desktop /usr/share/applications/ &&
#cp -f data/elyco.desktop data/elyco.desktop.tmp &&
#sed -i "s/arg1/$ent/" data/elyco.desktop.tmp &&
#sed -i -e "s/Exec=iceweasel/Exec=iceweasel $ent/" data/elyco.desktop.tmp &&
#mv data/elyco.desktop.tmp /usr/share/applications/elyco.desktop &&
cp -f data/elyco.png /usr/share/pixmaps/ &&

# Faire en sorte de pouvoir utiliser avec MATE les économiseurs d'écran provenant des paquets xscreensaver, xscreensaver-gl-extra et xcreensaver-data-extra  --> choix par défaut : XMATRIX !

cp -rf /usr/share/applications/screensavers/ /usr/share/applications/screensavers.old &&
find /usr/share/applications/screensavers -name "*.desktop" -print | xargs sed -i
's/OnlyShowIn=GNOME;/OnlyShowIn=GNOME;MATE;/g' &&

# Désactiver le changement d'utilisateur lors d'un verrouillage d'écran
# ne fonctionne pas !

#gsettings set org.mate.lockdown disable-user-switching true &&

# Pour vérifier, valider dans un xterm : gsettings list-recursively org.mate.lockdown

# Supprimer les options "Mettre en veille" et "Hiberner"

mv /usr/share/polkit-1/actions/org.freedesktop.upower.policy /usr/share/polkit-
```

```
1/actions/org.freedesktop.upower.policy.old &&
cp -f data/org.freedesktop.upower.policy /usr/share/polkit-1/actions/ &&

# Création du profil local dans /etc/skel/

cd /home &&
mv adminprof/ adminprof.old &&
tar xzpfv ~/integrdom/skel/skel.tar.gz &&
mv skel/ adminprof &&
chown -R adminprof:adminprof adminprof/ &&
cd /etc &&
mv skel/ skel.old &&
tar xzpfv ~/integrdom/skel/skel.tar.gz &&
chown -R root:root skel/ &&

# Création de trois comptes locaux supplémentaires :

cd ~/integrdom &&
scripts/./addusers.sh &&
useradd -d /home/prof -g prepalin -s /bin/bash -k /etc/skel -m prof &&

# Paramétrage de l'extinction automatique tous les jours à 21 h 00 :
# crontab -e --> 00 21 * * * /sbin/shutdown -h now
# /var/spool/cron/crontabs

crontab data/root &&

# On commente les lignes relatives à "Google Chrome" et "Google Earth" dans /etc/apt/sources.list
# --> raison : doublon avec les informations de /etc/apt/apt.d/
# --> évite donc les avertissements

sed -i -e 's/^deb http:\/\/dl.google.com\/linux\/chrome\/deb\/ stable main/#&/' /etc/apt/sources.list &&
sed -i -e 's/^deb http:\/\/dl.google.com\/linux\/earth\/deb\/ stable main/#&/' /etc/apt/sources.list &&

update-rc.d -f exim4 remove &&
apt-get update &&
#apt-get -y upgrade &&
apt-get -y dist-upgrade &&
#apt-get clean &&
apt-get -y autoremove --purge #&&

#reboot
```

addusers.sh

```
#!/bin/bash

cible="config/users.txt" &&

cat $cible | while true ; do
read idn grp mdp &&
if [ "$idn" == "stop" ] ; then break ; fi &&
if ! grep -i $grp "/etc/group" ; then groupadd $grp ; fi &&
if ! grep -i $idn "/etc/passwd"
 then
```

```
  useradd -d /home/$idn -g $grp -s /bin/bash -k /etc/skel -m $idn &&
  (echo $mdp;echo $mdp) | passwd $idn
fi
done
```

users.txt

```
adminskel adminprof *QuatrE6!TroiS5?
prof prepalin alpha_ibm
invite prepalin beta
stop
```

integrdom.sh

```
#!/bin/bash

# Ce script "intègre" un système Debian GNU/Linux dans un domaine contrôlé par un serveur eole SCRIBE

source config/intranet.sh &&

echo "Partie n°3" >> ~/report.txt &&
cd ~/integrdom/ &&
scripts/./03.sh | tee -a ~/report.txt &&
reboot
```

03.sh

```
#!/bin/bash

# Partie n°3 : "intégration" dans un domaine contrôlé par un serveur eole SCRIBE
# Synchronisation du client avec le serveur de temps

#ntpdate $ip_scribe &&

cp -f data/ldap.conf data/ldap.conf.tmp &&
sed -i -e "s/arg1/$ip_scribe/" data/ldap.conf.tmp &&
mv /etc/ldap/ldap.conf /etc/ldap/ldap.conf.old &&
mv data/ldap.conf.tmp /etc/ldap/ldap.conf &&

mv /etc/security/group.conf /etc/security/group.conf.old &&
cp -f data/group.conf /etc/security/ &&

cp -f data/libnss-ldap.conf data/libnss-ldap.conf.tmp &&
sed -i -e "s/arg1/$ip_scribe:389/" data/libnss-ldap.conf.tmp &&
mv data/libnss-ldap.conf.tmp /etc/libnss-ldap.conf &&
cp -f data/pam_ldap.conf data/pam_ldap.conf.tmp &&
sed -i -e "s/arg1/$ip_scribe:389/" data/pam_ldap.conf.tmp &&
mv data/pam_ldap.conf.tmp /etc/pam_ldap.conf &&

mv /etc/nsswitch.conf /etc/nsswitch.conf.old &&
cp -f data/nsswitch.conf /etc/ &&

mv /etc/pam.d/common-account /etc/pam.d/common-account.old &&
mv /etc/pam.d/common-auth /etc/pam.d/common-auth.old &&
```

```
mv /etc/pam.d/common-password /etc/pam.d/common-password.old &&
mv /etc/pam.d/common-session /etc/pam.d/common-session.old &&
mv /etc/pam.d/common-session-noninteractive /etc/pam.d/common-session-noninteractive.old &&
cp -f data/common-* /etc/pam.d/ &&

mv /usr/share/pam-configs/ /usr/share/pam-configs.old &&
cp -rf data/pam-configs/ /usr/share/ &&

mv /etc/security/pam_mount.conf.xml /etc/security/pam_mount.conf.xml.old &&
cp -f data/pam_mount.conf.xml data/pam_mount.conf.xml.tmp &&
sed -i -e "s/arg1/$ip_scribe/g" data/pam_mount.conf.xml.tmp &&
mv data/pam_mount.conf.xml.tmp /etc/security/pam_mount.conf.xml &&

# /etc/profile --> français encodé en UTF8

mv /etc/profile /etc/profile.old &&
cp -f data/profile /etc/ &&

# Ne pas créer les dossiers par defaut dans home

cp -f data/user-dirs.* /etc/xdg/ &&

# Seul l'admin et les membres administrateurs du domaine peuvent utiliser la commande "sudo" --> à revoir niveau sécurité

mv /etc/sudoers /etc/sudoers.old &&
cp -f data/sudoers /etc/ &&

# Paramétrage de lighdm : activer numlockx + logon et logoff

mv /etc/lightdm/lightdm.conf /etc/lightdm/lightdm.conf.old &&
cp -f data/{lightdm.conf,logo*} /etc/lightdm/ &&

# Script qui permettra de nettoyer le /home/* --> à automatiser

cp -f scripts/nettoyer.sh ~ &&

service nscd restart &&

# Paramétrage du proxy http squid pour tout le système

# (1) Paramétrage du proxy pour MATE

cp -f data/scribe.gschema.override data/scribe.gschema.override.tmp &&
sed -i -e "s/arg2/$ip_proxy/g" data/scribe.gschema.override.tmp &&
sed -i -e "s/arg3/$port_proxy/g" data/scribe.gschema.override.tmp &&
mv data/scribe.gschema.override.tmp /usr/share/glib-2.0/schemas/scribe.gschema.override &&

# Prise en compte des modifications apportées

glib-compile-schemas /usr/share/glib-2.0/schemas &&

# (2) Paramétrage du proxy pour le système

cp -f data/environment data/environment.tmp &&
```

```
sed -i -e "s/arg1/$ip_proxy:$port_proxy/g" data/environment.tmp &&
mv /etc/environment /etc/environment.old &&
mv data/environment.tmp /etc/environment &&

# (3) Paramétrage du proxy pour apt

cp -f data/20proxy data/20proxy.tmp &&
sed -i -e "s/arg1/$ip_proxy:$port_proxy/g" data/20proxy.tmp &&
mv data/20proxy.tmp /etc/apt/apt.conf.d/20proxy &&

# Désactiver le changement d'utilisateur lors d'un verrouillage d'écran
# ne fonctionne pas !

gsettings set org.mate.lockdown disable-user-switching true

# Pour vérifier, valider dans un xterm : gsettings list-recursively org.mate.lockdown
```

nettoyer.sh

```
#!/bin/bash

REP=/home &&

for rep in a b c d e f g h i j k l m n o p q k r s t v w x y z ;
do
  if [ -e "$REP/$rep/" ] ; then
    echo "Destruction de $REP/$rep !" &&
    rm -rf $REP/$rep/
  fi
done
```

04.sh

todo

ANNEXE N°2 : explications rapides

(1) Le fichier « intranet.sh » est à éditer et à modifier en fonction du réseau de l'établissement.

(2) Le script « integrdom_debian.sh » permet l'intégration d'une Debian GNU/Linux automatiquement. Pour le lancer (dans un xterm et sur la racine du compte root) :

```
# cd && tar xvfzp debian_gnu_linux.tar.gz && cd debian_gnu_linux/ && ./integrdom_debian.sh
```

(3) Les scripts (modulaires) « prepalin.sh » et « integrdom.sh » permettent d'effectuer la même manipulation en deux temps (création d'une image intermédiare de la racine / de Debian). De plus, la maintenance des scripts est plus facile ainsi : erreurs à corriger, ajout/suppression de fonctionnalités...

Pour les lancer (dans un xterm et sur la racine du compte root) :

```
# cd && tar xvfzp debian_gnu_linux.tar.gz && cd debian_gnu_linux/ && ./prepalin.sh
```

Après le reboot, on crée une image de la racine / de Debian + reboot.

```
# cd && ./integrdom.sh
```