Fiche Linux

# Démarrage

## Bypass le mot de passe root sur un GRUB non-protégé

* Appuyer sur ‘Echap’ au démarrage puis sur ‘e’ sur la ligne de la distribution voulue
* Ajouter ‘single’ à la fin de la ligne « kernel » puis appuyer sur ‘b’
* Modifier le mot de passe root avec passwd
* Redémarrer pour ne pas rester dans le mode mono-utilisateur bridé

## Protéger son GRUB

* grub-crypt >> /boot/grub/grub.conf
* Taper le mot de passe voulu
* vim /boot/grub/grub.conf
* Copier la ligne apparue à la fin du fichier sous « hiddenmenu »
* Ajouter « password –encrypted » avant le mot de passe chiffré
* Mettre « lock » sous chaque ‘title’ que l’on veut protéger avec ce même mot de passe
* On peut aussi faire un mot de passe local pour chaque ‘title’ en ajoutant un « password –encrypted [XXX] » différent sous chaque ‘title’ mais c’est un besoin plutôt rare

# Réseau

## /etc/sysconfig/network

# Début

HOSTNAME=machine.domaine

NETWORKING=yes

# Fin

## /etc/hosts

# Début

1.2.3.4 machine.domaine machine

# Fin

## /etc/sysconfig/network-scripts/ifcfg-eth0

# Début

DEVICE=eth0

ONBOOT=yes

BOOTPROTO=none

IPADDR=1.2.3.4

NETMASK=255.255.255.0

GATEWAY=1.2.3.1

DNS1=100.0.0.1

DNS2=100.0.0.2

DOMAIN=domaine.com

# Fin

# Fichiers

## Ajout d’un nouveau disque

* fdisk –l
* fdisk /dev/xxx
* mkfs –t ext4 /dev/xxx
* mount /dev/xxx /mon/dossier

## Fichiers importants

* /etc/mtab = Liste des points actuellement montés
* /etc/fstab = Liste des points montés au démarrage
* « tail –n X /etc/mtab >> /etc/fstab » pour monter des points de manière permanente (X = nombre de lignes)

## Liens

* « ln source destination » => Lien physique, pas grave si la source est supprimée
* « ln -s source destination » => Lien symbolique, équivalent d’un raccourci Windows

## Trouver tous les fichiers avec des permissions SUID

* « find / -user root –perm -4000 –exec ls –ldb {} \; »
* Pratique pour rapidement trouver certaines faiblesses de configuration

## Droits

* User, Group, Others
* Read, Write, Execute <=> 4, 2, 1
* SUID => ‘rws------‘ au lieu de ‘rwx------‘ et chmod sous le format ‘4XXX’ (donc « chmod u+s » pour le mettre)
* SGID => Même fonctionnement que le SUID mais avec le groupe à la place de l’utilisateur
* Le SUID s’applique seulement sur des fichiers, le SGID peut s’appliquer partout
* Sticky bit = Interdiction de supprimer le dossier si on n’en est pas propriétaire
  + Format ‘1XXX’ et ‘drwxrwxrwt’, ‘t’ au lieu de ‘x’ sur Others
  + Si on le met sur un fichier exécutable, ce dernier restera en mémoire après son exécution

# Services

## Activer un service au démarrage

* « chkconfig [service] on »

# SELinux (Security Enhanced Linux)

## Modes

* “Enforcing” = 1 = Activé
* “Permissive” = 0 = Silencieux
* “Disabled” = Totalement éteint

# Utilisateurs

## Exemple de création assez détaillée

* useradd –u 501 –g 650 –G 651,652 –d /home/users/timothe –c “Commentaire” timothe
  + Création d’un utilisateur timothe avec l’UID 501, appartenant au groupe principal 650 et aux groupes secondaires 651 et 652
  + Créer le dossier /home/users si nécessaire
  + Mais ne surtout pas créer /home/users/timothe, il doit être généré par la commande
  + Éviter les nombres sous 500 pour l’UID, quasiment tout est réservé pour le système

## Modifier un GID proprement

* usermod –g X timothe
* find / -gid Y –exec chgrp X
  + Cette commande sert à reloger les fichiers de timothe dans le bon groupe
  + X = Nouveau GID
  + Y = Ancien GID

## Exemple pour les paramètres de sécurité

* chage -E 2026-08-09 -m 30 -M 60 -d0 -W 10 -I 45 timothe
  + Date d’expiration le 9 août 2026
  + Durée de vie du mot de passe entre 30 et 60 jours
  + Changement de mot de passe obligatoire à la prochaine connexion
  + Avertissement 10 jours avant l’expiration
  + Expiration du compte automatique 45 jours après l’expiration du mot de passe

## Template

* Le template utilisé pour les futurs répertoires de connexion se trouve dans /etc/skel
* On peut y ajouter des choses ou modifier les fichiers, notamment le .bashrc et le .bash\_profile
* Il y a aussi les fichiers /etc/default/useradd et /etc/login.defs qui contiennent pas mal de paramètres

## /etc/default/useradd

# Début

GROUP=100 # Groupe par défaut si non-précisé à la création.

HOME=/home # Répertoire de connexion par défaut si non-précisé à la création.

INACTIVE=-1 # Nombre de jours avant expiration du compte si mot de passe expiré (-1 = +∞).

EXPIRE= # Date d'expiration du compte (vide = pas d'expiration).

SHELL=/bin/bash # Shell par défaut si non-précisé à la création.

SKEL=/etc/skel # Emplacement du squelette de /home/ par défaut. Outil très puissant.

# Fin

## Substitution et environnement

* « su – timothe » permet de prendre le profil de l’utilisateur timothe en chargeant son environnement
* L’environnement est principalement composé du .bashrc et du .bash\_profile
* Si on utilise cette commande sans être root il faudra évidemment le mot de passe du compte cible

# Tâches planifiées

## Exemple : sauvegarde en relatif toutes les 4 heures les lundis du mois d’août

* crontab –e
* « \* \*/4 \* 8 1 tar cvf /sauvegardes/dossier.`date \+\%j`.tar /home/dossier » sur la première ligne
  + Ne surtout pas oublier les ‘\’ pour isoler le ‘+’ et le ‘%’, grosse source d'erreurs
  + Tester la tâche en mettant cinq ‘\*’ pour l’exécuter toutes les minutes
  + ‘/x’ = Tous les x
  + ‘1-9’ = De 1 à 9
  + ‘1,9’ = 1 et 9
* Enregistrer et quitter
* service crond start

# Dépôts

## Créer un dépôt local contenant tous les .rpm de la machine

* find / -name \*.rpm -exec cp {} /depot/rpm/ \ ;
* createrepo /depot/rpm/
* vim /etc/yum.repos.d/depot\_rpm.repo
* « yum clean all » pour vider le cache au cas où
* « yum list available » pour vérifier que le dépôt marche, montre tous les paquets disponibles.
* « yum install [paquet] »

## /etc/yum.repos.d/depot\_rpm.repo

# Début

[dp] # Nom court

name=Dépôt RPM # Nom long

baseurl=file:///depot/rpm/ # Il y a bien 3 / (protocole + racine), 'http://' pour du distant

enable=1 # Pour désactiver ce dépôt, mettre 0 (assez rare puisqu’on dégage souvent tout)

gpgcheck=0 # Mettre 1 pour qu'il y ait une vérification par GPG, inutile en local.

# gpgkey=file:///chemin/vers/la/clé/publique

# Fin

# VIM

## Configuration

* Éditer le fichier $HOME/.vimrc pour changer les options de Vim
* Taper « :set nu » en mode Normal pour afficher les numéros de ligne
* Taper « :set ic » en mode Normal pour ignorer la casse lors des recherches
* Taper « :syntax on » en mode Normal pour activer la coloration syntaxique

## Commandes en mode Normal

### Modification

* dd => Effacer une ligne entière
* dXd => Effacer X lignes
* dw => Effacer un mot
* dXw => Effacer X mots
* d$ => Effacer jusqu’à la fin de la ligne en partant de la position du curseur
* y{motion} => Copier (yank), {motion} = Toutes les options utilisables avec les autres commandes (comme ‘d’)
  + Exemples : ‘y4’ copie 4 lignes, ‘yy’ en copie 1, ‘y$’ copie jusqu’à la fin de la ligne, etc.
* p => Coller quelque chose copié par y ou effacé par d
* u => Annuler la dernière modification sur un caractère
* U => Annuler toutes les dernières modifications que l’on a effectuées consécutivement sur une ligne
* c{motion] = « Changer jusqu’à ».
  + Exemple : ‘c$’ va nous mettre en mode remplacement jusqu’à la fin de la ligne

### Déplacement

* % => Permet de se téléporter au [, ( ou { correspondant
* gg => Aller au début du fichier
* G => Aller à la fin du fichier
* xxxG => Aller à la ligne xxx du fichier
* $ => Aller à la fin de la ligne
* 0 => Aller au début de la ligne

### Recherche et remplacement

* /texte => Rechercher « texte » dans le fichier
* n => Prochaine occurrence (next)
* N => Précédente occurrence (shift n)
* / ? => Directement chercher en direction opposée
* « :s/ancien/nouveau » => Remplace « ancien » par « nouveau » sur la première occurrence trouvée
* « :s/ancien/nouveau/g » remplace sur toutes les occurrences présentes dans la ligne
* « :s/ancien/nouveau/gc » remplace sur toutes les occurrences présentes dans la ligne en demandant une confirmation à chaque fois
* « :#,#s/ancien/nouveau/g » remplace sur toutes les occurrences présentes dans la plage de lignes indiquée par les # (« 1,10 » => Lignes 1 à 10, etc)
* « :%s/ancien/nouveau » remplace les occurrences dans tout le fichier

### Données, commandes et autres fichiers

* :5,56w FICHIER => Enregistrer les lignes de 5 à 56 dans le fichier FICHIER
* :! COMMANDE => Exécuter une commande externe qui s’affichera temporairement
* :r FICHIER => Récupérer le fichier FICHIER et l’insérer dans le fichier courant à partir de la position du curseur
* :r! COMMANDE => Insérer le résultat de la commande COMMANDE à partir de la position du curseur
* Ctrl-W => Sauter d’un fichier à l’autre lorsque plusieurs sont ouverts en même temps
* F1 => Ouvrir le fichier d’aide de Vim. Quitter avec :q!
* Ctrl-D => Autocompléter une commande