5 conseils pour les nouveaux administrateurs Linux

Il est généralement assez facile pour les nouveaux administrateurs Linux de maîtriser les bases de l'installation, la configuration et la gestion des systèmes Linux aux niveau de base.
Cependant, il faut des années pour obtenir la connaissance approfondie nécessaire dans de nombreux environnements de serveurs aujourd'hui.
Moi même, je ne connais pas tous, chaque jour j'approfondis.
Une chose que je recommande vraiment d'apprendre dès le début, c'est les bonnes pratiques.
Rappelez-vous, ce sont les bases.
Mais vous devez les saisir dans votre cerveau.
Prier et méditer sur elles, si cela aide.
Quoi que vous fassiez, apprenez ces règles.

1. Ne pas ce lancer en tant que root

Il y a quelques tâches que vous devez faire en tant que login **root**.
Cependant, assurez-vous toujours de saisir “exit” lorsque vous avez terminé ou utiliser d'avantage **sudo**, qui va automatiquement vous obliger à vous authentifier de nouveau en tant que **root**, après une période de temporisation.
Effectuez l'ensemble de vos tâches normales avec un login non administrateur.
Si vous ne possédez pas déjà un login régulier, arrêtez ce que vous faites en ce moment et créer un login, puis connectez vous à ce compte pour faire votre travail.

pour les utilisateurs qui n'auraient pas **sudo** d'installer

```
aptitude install sudo
yum install sudo
```

Pour changer l'éditeur de texte, si comme moi `Vim` est une nécessité

```
update-alternatives  --config editor
```

Puis, sélectionné votre éditeur préféré. Donc pour configurer **sudo** on utilise la commande `visudo`, je vous présente seulement comment ajouté ou retiré des privilèges sur un login ou un groupe de login.

```
<login>   ALL = (login) <commande1>,<commande2>
%<groupe> ALL = (login) <commande1>,!<commande2>
```

- **<login>** : Représente un login du système, un seul login doit être précisé par ligne.
- **%<groupe>** : Désigne un groupe de login du système, le nom du groupe doit donc être précédé d'un symbole de pourcentage (%).
  Un seul groupe doit être précisé par ligne.
- **ALL** : Désigne la ou les machines dans lesquelles les commandes suivantes sont autorisées ou refusées pour ce login ou ce groupe.

Le mot-clé **ALL** désigne l'ensemble des machines de votre parc informatique. Dans le cadre d'une utilisation à domicile, laisser ALL n'est pas un inconvénient. Dans un grand parc d'entreprise, de meilleures stratégies sont à prévoir.

- **(login)** : Désigne le login dont on prend les droits (peut valoir ALL pour tous)
- **<commande1>,<commande2>** : Représentent des commandes pouvant être exécutées par le login ou le groupe désigné en début de ligne.
  Les commandes précédées d'un point d'exclamation (!) sont refusées, alors que celles sans point d'exclamation sont autorisées, les commandes multiples sont séparées par une virgule, sans espace et préférez saisir des chemins absolus vers des commandes plutôt que des chemins relatifs (par exemple, /bin/ls plutôt que ls).

2. Gardez votre système à jour

Le seul programme qui n'a jamais besoin de mise à jour est celui qui n'a pas encore été écrit.
Quasiment chaque morceau de logiciel écrit comporte un bogues.
Je l'ai vu de mes propres yeux, comment il est facile de “pwn” un systèmes d'exploitation non à jour.
L'essentiel ici est de garder votre système à jour!
Pour cela l'utilitaire de gestion des paquets fait l'affaire.

3. Examiner les services et désactiver tous ceux qui sont inutiles

Je ne peux pas vous dire combien de foi je l'ai vu ce conseil.
Exécutez `netstat` (a chacun ces options, j'aime bien `patune` ou `laputen` pour le moyen mémo technique ).
Voyez-vous des services que vous n'avez pas besoin?
Telnet est en cours d'exécution?
Arrêtez-le MAINTENANT, cela vaut pour tout service que vous n'avez pas besoin.
Sérieusement, si vous n'avez pas besoin de certains services, débarrasser vous d'eux.

4. Testez les ports ouverts

`Nmap` permet de savoir si un port est ouvert et potentiellement le service qui écoute derrière.
Il y a d'autres scanners de ports et de vulnérabilité (NESSUS, metasploit, etc).
Arrêtez tous les ports ouverts inutilisés.

exemples de scanne NMAP :

```
nmap -T4 -A <IP> # ou nom de domaine
nmap -T4 -A -v -Pn <IP> #Si un Firewall est actif
```

5. Apprenez à utiliser SELinux, ne le désactivez pas

SELinux est un utilitaire de contrôle d'accès obligatoire à base de règles.
Fondamentalement, il vous donne un contrôle précis sur les logins et la façon dont ils interagissent avec les fichiers et programmes.
Certaines distributions (notamment, Red Hat et Fedora) ont SELinux installé par défaut.
D'autres l'utilisent comme une option d'add-on.
Vous pouvez en apprendre plus sur SELinux sur le projet SELinux Wiki.

Astuce Bonus 1 : les sauvegardes!

Effectuez des sauvegardes régulières permet de garder une certaine sécurité.
Avec les progrès de rançongiciel (dans un cas, les sauvegardes d'une entreprise ont été pris en otage), je vous recommande de mettre ces sauvegardes hors de votre réseau dès que c'est possible.
Bon, si vous n'avez pas fait de sauvegarde récemment, vous connaissez le refrain, arrêter tout de suite et faite le.

Astuce Bonus 2 : les têtes en l'air

Qui n'a jamais oublié en partant de son poste pour un café ou .....(c'est naturel, je m'arrêterai là 😛), laissé trainer une session ssh ouverte, c'est plus grave si celle-ci est ouverte sur le login `root` de plus c'est vraiment grave à mes yeux, si vous oubliez de verrouiller votre session ou que fainéant que vous êtes vous avez désactivé le verrouillage auto de celle-ci (je ne vous pardonne vraiment pas).
Bon, dans la plupart des cas, je vous ferai une blague avec vos icônes caché, votre bureau avec un fond d'écran XXXXX 😛
Mais, dans ma grande mansuétude, je vais être gentil et vous donnez le moyen de fermer les sessions d'un serveur automatiquement au bout d'un timeout.

Éditer, le fichier `bashrc` dans `/etc`

```
vim /etc/bash.bashrc
```

Ajouter, à la fin cela:

```
export TMOUT=tttt
```

avec ttt en seconde.
exemple :

```
export TMOUT=600 #pour 10 minutes.
```

Mais, il est préférable de penser à bien faire `exit`.

Bon, pour certain cela sera du rabâchage, mais pour d'autres, discipline et rigueur sont les 2 mamelles de la réussite (heu, je crois qu'il faut jarrète)

Sources: fossforce.com, ubuntu.org