

## 0.1 Lancer des commandes avec les droits de root : Sudo

>Sudo<sup>1</sup> (Superuser do) est un programme permettant aux administrateurs systèmes de donner à certains utilisateurs ou groupes d'utilisateurs, la possibilité d'exécuter une ou plusieurs commandes en tant que root ou en tant qu'un autre utilisateur.

### 0.1.1 1. Installation de Sudo :

Sudo est certainement disponible sur les CD d'installation de votre distribution. Il vous suffira de l'installer selon la méthode spécifique à votre distribution.

– **Pour Mandriva :**

```
# urpmi sudo
```

– **Pour Debian :**

```
# apt-get install sudo
```

– **Pour RedHat :** Récupérez le paquetage sudo-x.x.x-x.i386.rpm sur les CD d'installation de RedHat et installez le ainsi :

```
# rpm -Uvh sudo-1.6.6-1.i386.rpm
```

– **Pour les autres :** Récupérez les sources de Sudo >ici<sup>2</sup> et installez le comme suit :

```
$ tar xvzf sudo-1.6.6.tar.gz
$ ./configure --prefix=/usr/bin
$ make
$ su
Password
# make install
```

### 0.1.2 2. Configuration de Sudo :

La configuration de Sudo s'effectue via la commande **visudo** en root qui va éditer le fichier */etc/sudoers* : Ce fichier de configuration nécessite l'utilisation d'une syntaxe spécifique dont le principe général est le suivant :

- Définition des groupes d'utilisateurs à qui on veut donner des droits particuliers via la syntaxe **User\_Alias**,
- Définition des groupes de machines à partir desquelles il est possible d'exécuter les commandes définies via la syntaxe **Host\_Alias**,
- Définition des commandes que les utilisateurs vont pouvoir exécuter via la syntaxe **Cmnd\_Alias**.

Prenons un exemple pour faciliter la compréhension de la configuration de Sudo. Je veux autoriser les utilisateurs kernel, tuffgong et le groupe d'utilisateurs test à gérer la création et la suppression des comptes utilisateurs via les commande **adduser** et **userdel** depuis la machine locale et la machine d'ip 192.168.0.4

```
# sudoers file.
#
```

---

<sup>1</sup><http://www.courtesan.com/sudo/>

<sup>2</sup><http://www.courtesan.com/sudo/www.html>

```
# This file MUST be edited with the 'visudo' command as
  root.
#
# See the man page for details on how to write a sudoers
  file.
# Définition du groupe de machines à partir desquelles
  les actions sont possibles (localhost et 192.168.0.4) :
Host_Alias MACHINES = localhost, 192.168.0.4
# Définition du groupe Administrateurs contenant les utilisateurs
  kernel, tuffgong et le groupe d'utilisateurs test :
User_Alias ADMINISTRATEURS = kernel, tuffgong, %web
# Définition du groupe de commandes autorisées à être
  exécutées (adduser, userdel) :
Cmnd_Alias GESTION_USERS = /usr/sbin/adduser, /usr/sbin/userdel
# Définition des autorisations :
ADMINISTRATEURSMACHINES = NOPASSWD : GESTION_USERS
```

Notez que dans l'exemple ci-dessus, le paramètre **NOPASSWD** évite à l'utilisateur de devoir taper son mot de passe pour utiliser Sudo. Les options possibles de Sudo étant nombreuses, je vous renvoie aux pages de manuels de ce programme pour une utilisation plus avancée (**man sudo**). Enfin, remarquez également qu'une mauvaise configuration de Sudo peut être une menace pour la sécurité de votre système. Par exemple, il est tout à fait possible via Sudo d'autoriser un utilisateur à changer les mots de passe des utilisateurs mais veillez à inclure une exception concernant celui de Root afin de le rendre inaccessible.