

BTS SNIR	Document ressource
Lycée Jean Rostand Villepinte	Commande sudo

Commande sudo

I Présentation

Certaines commandes ne peuvent être exécutées qu'avec les droits de root. La première solution est de se connecter en root et de les exécuter. Mais root a tous les droits et donc si on fait la moindre erreur, on peut mettre en panne notre serveur. Donc cette solution est à proscrire.

La bonne solution est de se connecter avec un compte qui aura des droits limités puis de lancer les commandes système grâce à l'utilitaire sudo, par exemple :

```
snir@debian1:~$ sudo ifconfig
```

Vous pouvez donner les mêmes droits que root à votre utilisateur quand il exécute en précédant la commande de sudo ou bien vous pouvez paramétrer finement l'utilitaire « sudo » pour autoriser ou refuser l'exécution de tâches privilégiées. Plus simplement autoriser l'exécution de toutes les tâches administratives à un groupe d'utilisateurs par l'authentification par mot de passe, sudo peut permettre à un utilisateur particulier ou un groupe d'utilisateurs particulier d'exécuter une ou des tâches bien précises, avec ou sans saisie du mot de passe. D'autres paramètres, tels le délai d'attente avant qu'une ré-authentification soit nécessaire, l'endroit où est enregistré le journal d'événements et le niveau de courtoisie de sudo, sont aussi paramétrables.

II Installation

Pour installer sudo, il suffit de taper la commande suivante en étant root :

```
root@debian1:~# apt-get install sudo
```

III Configuration

Pour pouvoir éditer les autorisations contenues dans le fichier « **/etc/sudoers** », il faut utiliser l'utilitaire : « **visudo** », cela ouvrira l'éditeur de texte configuré par défaut sur le système.

Au début du fichier se trouve les options, puis la possibilité de définir des alias (pour le nom des hôtes, des utilisateurs et des commandes).

Finalement les deux lignes suivantes :

```
root ALL=(ALL:ALL) ALL
%sudo ALL=(ALL:ALL) ALL
```

La première ligne signifie que l'utilisateur « root » depuis n'importe quelle machine peut exécuter n'importe quelle commande comme n'importe quel utilisateur et n'importe quel groupe.

La deuxième ligne signifie que les utilisateurs appartenant au groupe « sudo » depuis n'importe quelle machine peut exécuter n'importe quelle commande comme n'importe quel utilisateur et n'importe quel groupe.

Donc comment est constitué une ligne du fichier sudoers :

```
identifiant ALL = (user) /chemin/commande, /chemin/autrecommande
%groupe ALL = (user) /chemin/commande, !/chemin/autrecommande
```

- x identifiant représente un identifiant utilisateur du système ;
- x %groupe désigne un groupe d'utilisateurs du système ;
- x ALL désigne la ou les machines dans lesquelles les commandes suivantes sont autorisées ou refusées pour cet utilisateur ou ce groupe d'utilisateurs.

BTS SNIR	Document ressource
Lycée Jean Rostand Villepinte	Commande sudo

- x user (entre parenthèses) désigne l'utilisateur dont on prend les droits (peut valoir ALL pour tous)
- x commande et autre commande représentent des commandes pouvant être exécutées par l'utilisateur ou le groupe d'utilisateurs 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.

Les commandes doivent être entrées de manière exacte avec des chemins absolus vers des commandes.

Par exemple si l'on veut que l'utilisateur « util » depuis la machine nommée « serveur » puisse exécuter les commandes « cp » et « mv » en tant que l'utilisateur « root » :

```
util serveur = (root) /bin/cp, /bin/mv
```

Pour pouvoir être utilisé de la sorte :

```
util@serveur:~$ sudo cp source destination
```

Pour connaître le nom de la machine sur laquelle vous vous trouvez, il faut utiliser « hostname ».

Pour connaître le chemin complet d'une commande : « which commande ».

La même chose mais pour le groupe « util » :

```
%util client = (root) /bin/cp, /bin/mv
```

Remarque : les commandes indiquées peuvent prendre des arguments.

Il est possible d'utiliser le caractère « * » pour dire « n'importe quoi », par exemple : « systemctl * networking.service » fonctionnera pour « systemctl [start|stop|restart] networking.service ».

Et si l'on veut que lorsque l'on fait un sudo l'utilisateur n'est pas à entrer son mot de passe, il suffit de mettre comme « flag » « NOPASSWD : », par exemple

```
util serveur = (root) NOPASSWD: /bin/cp, /bin/mv
```

Exemple : création d'un compte admin qui a le droit d'exécuter la commande ifconfig et de relancer les services networking, apache2, mysql et vsFTP

- x Obtention des chemins des commandes :

```
root@debian1:/home/snir# which ifconfig
/sbin/ifconfig
root@debian1:/home/snir# which service
/usr/sbin/service
```

- x Création du compte

```
root@debian1:/home/snir# useradd -m -s /bin/bash admin
```

- x Modification des droits

```
root@debian1:/home/snir# visudo
```

- x Ajout dans le fichier de :

```
admin ALL=(root:root) /usr/sbin/service apache2 *, /usr/sbin/service mysql
*, /usr/sbin/service vsftpd *, /sbin/ifconfig
```

- x Test des modifications, par exemple :

```
admin@debian1:/home/snir$ sudo service vsftpd restart
Stopping FTP server: vsftpd.
Starting FTP server: vsftpd.
```