

Qu'est-ce que sudo?

sudo (abréviation de *superuser do*, en anglais : « super utilisateur fait ») est une **commande et un utilitaire informatique** utilisé dans les systèmes d'exploitations de type Unix et Linux tels que FreeBSD, MacOS, Solaris, Ubuntu...etc.

A quoi sert sudo?

sudo permet à un administrateur système de donner à un utilisateur (ou un groupe d'utilisateurs) la possibilité d'exécuter une ou plusieurs commandes en tant que super utilisateur, tout en gardant une trace des commandes tapées et en demandant un mot de passe à l'utilisateur avant d'exécuter sa commande.

Ainsi, sudo peut empêcher l'exécution *libre* de commandes critiques (généralement des commandes d'administration) pouvant gravement affecter le système.

Installation de l'utilitaire sudo

Lorsqu'il n'est pas fourni de base dans le système d'exploitation, il est possible d'installer sudo en le téléchargeant via <ftp://ftp.sudo.ws/pub/sudo/> ou en faisant appel à une commande d'installation de paquets spécifique au système d'exploitation utilisé (ex : *apt-get install sudo* pour debian ou ubuntu). L'installation de sudo doit se faire en mode super utilisateur.

Configuration de l'utilitaire sudo

La configuration de l'utilitaire sudo passe par l'exécution de la commande **visudo** en tant qu'administrateur.

visudo permet en fait d'éditer le fichier de configuration de sudo (se trouvant à */etc/sudoers*) de manière beaucoup plus sûre qu'une édition manuelle de ce fichier, dans la mesure où visudo peut :

- bloquer une multiple édition du fichier
- effectuer une vérification basique de la syntaxe du fichier de configuration

Le fichier de configuration est divisé en 4 champs que nous allons étudier...

Host alias specification

Cette section sert à définir quelles machines (distantes ou locales) pourront lancer les commandes gérées par sudo. A un groupe de machines est associé un alias permettant d'associer un nom générique au groupe. Ce concept d'alias est également utilisé dans les autres sections de configurations de sudo.

La syntaxe de configuration de cette section est la suivante :

Host_Alias <alias groupe machine> = <adresse des machines>

Exemple d'utilisation :

```
# Host alias specification
Host_Alias    ICI = localhost, 127.0.0.1, ma.machine.fr
Host_Alias    LABAS = 192.168.1.2, sa.machine.fr
```

User alias specification

Cette section permet de définir les utilisateurs ou groupes d'utilisateurs pouvant exécuter les commandes gérées par sudo. La syntaxe de configuration de cette section est la suivante :

User_Alias <alias groupe users> = utilisateur1, utilisateur2, ...

Exemple d'utilisation :

```
# User alias specification
User_Alias    groupe1 = toto, bob, axel
User_Alias    groupe2 = dieu
```

Cmnd alias specification

Cette section permet de définir quelles commandes devront être gérées par sudo. La syntaxe de configuration de cette section est la suivante :

```
Cmnd_Alias <alias groupe commande> = commande1, commande2, ...
```

Exemple d'utilisation :

```
# Cmnd alias specification
Cmnd_Alias    SHUTDOWN=/sbin/shutdown
Cmnd_Alias    SYSLOGD=/etc/syslogd
```

User privilege specification

Cette section finale permet de définir quel groupe d'utilisateurs peut exécuter quel groupe de commande et sur quelles machines... La syntaxe de configuration de cette section est la suivante :

```
<alias grpe user> <alias grpe machine> = NOPASSWD <alias grpe commande1> , <alias grpe commande2> , ...
```

Le paramètre NOPASSWD permet d'éviter à l'utilisateur de devoir taper un mot de passe lorsqu'il utilise la commande. Si NOPASSWD n'est pas explicitement spécifié, alors un mot de passe sera requis.

Le mot clé ALL permet l'exécution de n'importe quelle commande au groupe d'utilisateur spécifié. Le symbole « ! » permet d'interdire explicitement l'exécution de commande.

Exemple d'utilisation :

```
# User privilege specification
root ALL=(ALL) ALL
groupe1 ICI=NOPASSWD:SYSLOGD
groupe2 LABAS=SHUTDOWN
groupe2 ALL = !/usr/bin/su, !/usr/bin/su root
```

Ici,

- root a tous les droits sur toutes les machines
- groupe1, sur "ICI", peut se servir de syslogd sans avoir à rentrer de mot de passe
- groupe2, sur "LABAS", peut se servir de "shutdown"
- groupe2, sur toutes les machines, ne peut pas lancer la commande "su", ni "su root".

Utilisation de la commande sudo

L'utilisation standard de la commande sudo en console s'effectue généralement de la manière suivante : **sudo <commande>**. Un mot de passe vous sera alors éventuellement demandé selon la configuration de sudo. La commande sudo possède beaucoup d'options explicitées dans le manuel en ligne (man).

Liens annexes - documentation

Site officiel de sudo : <http://www.sudo.ws>

Documentation Française :

<http://fr.wikipedia.org/wiki/Sudo>

http://www.lea-linux.org/cached/index/Admin-admin_env-sudo.html

<http://doc.ubuntu-fr.org/sudo>

<http://ustilago.free.fr/sudo.html>

man sudo