

Permettre Sudo sur Slackware

Sudo, utilisateur de substitution de (Super User) ou Super user de (agissant comme un "super user") Sudo, joue un rôle important sur les système UNIX ; sudo permet aux utilisateurs ordinaires de récupérer temporairement les privilèges d'un autre utilisateur ; il est largement utilisé pour les privilèges du super utilisateur root.

Il y a beaucoup d'avantages et de désavantages d'utiliser sudo à la place de su, par exemple quelquefois nous avons besoin de faire une tâche rapidement, comme mettre à jour le système avec une seule commande , comme 'slackpkg update && slackpkg upgrade-all' ou simplement ouvrir un fichier qui a les permissions de lecture et d'écriture seulement pour root, par exemple.

Mais chaque super héros paie son prix, comme sudo permet à l'utilisateur d'avoir temporairement des super pouvoirs, quelqu'un qui connaît le mot de passe de votre utilisateur ordinaire peut aussi avoir ces super pouvoirs.

C'est pourquoi il est extrêmement important que vous ayez un mot de passe fort pour root et pour votre utilisateur ordinaire afin que vous puissiez utiliser sudo en pleine confiance.

Contrairement à d'autres distributions, Slackware est livrée par défaut sans activer sudo et nous allons voir comment l'activer.

La première étape est de créer un groupe appelé "sudo" ; nous pouvons faire cela de deux façons. La première est de créer manuellement un groupe et la seconde est d'utiliser la commande 'groupadd GROUPName'.

Nous utiliserons la méthode manuelle pour mieux apprendre et comprendre ce que nous faisons.

Il faut tout d'abord se loger en tant que root, pour cela nous utilisons la commande su , et tout de suite après nous ouvrons un fichier de configuration des groupes /etc/group dans notre éditeur favori :

```
$ su
# nano /etc/group
```

Naviguez jusqu'à la dernière ligne du fichier et ajoutez une ligne spéciale pour sudo ; ici la dernière ligne concernait le groupe privoxy mais la vôtre peut être différente :

```
privoxy:x:206:
```

Avec le même format, nous allons créer le groupe sudo : le format s'écrit comme ceci :

```
groupname:x:ID:USERNAME
```

Pour vérifier votre ID d'utilisateur, lancez la commande 'id -u'.

```
$ id -u
1000
```

Finalement nous ajoutons à la fin du fichier /etc/group la ligne :

```
sudo:x:1000:Username
```

Exemple :

```
nobody:x:98:nobody  
nogroup:x:99:  
users:x:100:  
console:x:101:  
tor:x:220:  
privoxy:x:206:  
sudo:x:1000:slackjeff
```

Après avoir fait cela, sauvegardez le fichier et quittez l'éditeur.

Maintenant, il faut éditer le fichier 'sudoers' ; ouvrez le fichier /etc/sudoers dans votre éditeur favori.

```
# nano /etc/sudoers
```

Ouvrez le fichier, trouvez la ligne `##sudo ALL=(ALL)ALL` : cette ligne est commentée par le caractère '#' devant sudo; Il faut décommenter cette ligne en enlevant le '#' qui est devant sudo

Ligne sudo commentée :

```
## Uncomment to allow members of group sudo to execute any command  
# %sudo ALL=(ALL) ALL
```

Ligne sudo décommentée :

```
## Uncomment to allow members of group sudo to execute any command  
%sudo ALL=(ALL) ALL
```

Décommentez la ligne de sudo, sauvegardez et fermez l'éditeur ; pour mettre la cerise sur le gâteau, il faut faire un dernier réglage qui est très important. Nous savons que l'utilisateur ordinaire a un User Id (UID) de 1000, et certaines commandes sont réservées au super utilisateur qui a l'UID de 0 ; lorsque nous lançons une commande, le système cherche la commande dans une liste de répertoires contenue dans la variable PATH.

Il y a des répertoires comme '/sbin' qui n'est accessible que par les utilisateurs d'UID 0 (root par exemple). Qu'arrive t'il si nous essayons d'exécuter une commande comme slackpkg par exemple qui se trouve dans ce répertoire ? Cela ne marche pas.

C'est pourquoi il faut ajouter deux nouvelles lignes à notre PATH.

Pour cela, toujours sous l'identité root, ouvrez le fichier 'profile' qui est situé dans '/ etc / profile' et trouvez la ligne :

```
# Set the default system $PATH:  
PATH="/usr/local/bin:/usr/bin:/bin:/usr/games"
```

Notez qu'il y a déjà un chemin préétabli ; les répertoires ont leurs champs séparés par des ':'. Après

'/usr/games', ajoutez ':', puis '/sbin', puis ':' de nouveau et enfin '/usr/sbin'; Sauvegardez et fermez l'éditeur.

Pour finir, vous devez avoir cette ligne :

```
# Set the default system $PATH:  
PATH="/usr/local/bin:/usr/bin:/bin:/usr/games:/sbin:/usr/sbin"
```



Faites attention que votre utilisateur ordinaire (UID 1000) peut maintenant exécuter des commandes de maintenance qui se trouvent dans /sbin et /usr/sbin, alors qu'auparavant ces commandes dans ces répertoires n'étaient même pas visibles par un utilisateur ordinaire. Mais même en voyant ces commandes, nous avons encore besoin du super utilisateur pour continuer.

Tout simplement, c'est la même chose que mettre une permission de lecture à un fichier ; un utilisateur ordinaire pourra le lire, mais pas l'écrire ou l'exécuter, par exemple.

Redémarrez votre système par la commande shutdown avec le paramètre -r now, ou simplement sortez de votre session utilisateur pour pouvoir exécuter la commande exit ou appuyez simultanément les touches **CTRL + D**

Faites des tests en ajoutant sudo en tête de vos commandes. Testez aussi une mise à jour par slackpkg.

```
$ sudo ls /root/  
$ sudo slackpkg update
```

Sources

- Originally written by [Slackjeff](#)
- Traduction française par [Desiderius](#)

[howtos](#), [misc](#), [sudo on slackware](#), [enabling](#), [author slackjeff](#)

From:
<https://docs.slackware.com/> - **SlackDocs**

Permanent link:
https://docs.slackware.com/fr:howtos:misc:enabling_sudo_on_slackware

Last update: **2021/03/24 09:19 (UTC)**

