Dois-je utiliser su ou sudo pour lancer mes commandes en root ?

- Objet : Bien comprendre les différences entre su et sudo dans le contexte d'une administration simple de sa machine
- Niveau requis : débutant
- Commentaires : *Quelle commande utiliser pour passer root et exécuter des tâches d'administration ?*
- Retours sur le forum: ici
- Débutant, à savoir : Utiliser GNU/Linux en ligne de commande, tout commence là !.

Introduction

Dans la suite, `ma_commande` désigne n'importe quelle commande, que ce soit `apt update` ou `rm /root/bla.log`.

Je veux exécuter `ma_commande` en *root*.

Je peux utiliser différents moyens. Mais tous ne se valent pas. Voici les différentes méthodes que nous allons comparer:

- se connecter en `root` depuis le TTY ([Ctrl]+[Alt]+[F1]/[F2]/etc. puis entrer `ma_commande`
- `su -` puis entrer `ma_commande`
- `su -c "ma_commande"`
- `su -l` puis entrer `ma_commande`
- `su -l -c "ma_commande"`
- `sudo ma_commande`
- `sudo -s` puis entrer `ma_commande`
- `sudo -i ma_commande`
- `sudo -i` puis entrer `ma_commande`

Version courte

Il ne faut jamais utiliser `su` et `su -c "ma_commande"`.

Si vous êtes membre du groupe *sudo* (tappez `groups` dans le terminal pour vérifier), alors utilisez `sudo ma_commande` ou ouvrez un shell *root* avec `sudo -s` (dans le dossier courant) ou `sudo -i` (dans `/root`) en entrant le mot de passe de votre utilisateur lorsque demandé.

Sinon, vous avez défini un mot de passe *root* lors de l'installation, alors utilisez `su -l -c "ma_commande"` ou ouvrez un shell *root* avec `su -l`, en saisissant dans les deux cas ce mot de passe.

Version longue

Authentification et mot de passe

su et sudo donnent des droits importants, mais avant cela, ils s'assurent que l'utilisateur en a bien le droit. Le mode d'authentification est paramétrable (voir `man pam_unix` et `man sudoers` par exemple), mais nous parlerons ici du comportement par défaut.

Mot de passe root

Lorsque l'on utilise su sans spécifier d'utilisateur, c'est implicitement les droits de *root* que l'on demande à obtenir. Et c'est également le mot de passe de l'utilisateur *root* qui nous est demandé.

Dans certains cas, l'utilisateur *root* s'est vu désactiver son mot de passe (c'est le cas par défaut sous ubuntu, ou sous debian si l'on laisse le mot de passe *root* vide lors de l'installation). Dans ce cas, on ne peut ni se connecter en root depuis le TTY, ni taper utiliser une des méthodes su ci-dessus.

Il est toujours possible de créé un mot de passe pour *root*, ce qui permettra alors d'utiliser ces commandes.

Mot de passe ''sudo''

Lorsque l'on utilise sudo, c'est le mot de passe de l'utilisateur courant qui est demandé.

Sous debian, par défaut, seuls les utilisateurs membres du groupe sudo sont autorisés à utiliser la commande sudo pour obtenir les droits *root*. En particulier, si vous avez installé Debian sans mettre de mot de passe *root*, le premier utilisateur que vous avez créé a été ajouté automatiquement au groupe sudo et a donc le droit d'utiliser la commande.

Pour savoir à quels groupes vous appartenez, tapez la commande

```
groups
```

Vous pouvez à tout moment ajouter ou retirer un membre du groupe sudo. Cette modification nécessite une déconnexion/reconnexion pour être prise en compte. Attention cependant à ne pas scier la branche sur laquelle vous êtes assis !

Shell ou pas shell

Une première différence entre ces différentes commandes est que certaines ouvrent un *shell* en tant

que *root*, dans lequel vous pouvez taper autant de commandes que vous voulez et qui seront exécutées avec les droits *root*. D'autres se contentent d'exécuter une seule commande avec les droits *root* puis vous ramènent dans votre *shell* utilisateur.

On note que chaque commande a sa duale

Version avec shell interactif	Version one-line
su	su -c “…”
su -l	su -l -c “…”
sudo -s	sudo …
sudo -i	sudo -i …

L'environnement d'exécution de la commande sera identique dans ces deux cas. La différence étant l'ouverture d'un shell interactif ou non.

Lorsque vous avez plusieurs commandes à taper, ou que vous ne savez pas forcément à l'avance toutes les commandes que vous avez à taper, privilégiez une commande de la première liste. Si vous savez que vous n'avez qu'une commande à taper, la seconde liste peut offrir une alternative intéressante.

Environnement

Outre les droits d'exécution d'un programme, un point que l'on néglige souvent ou que l'on oublie de mentionner, c'est l'importance des variables d'environnement et du dossier de travail.

Dossier de travail

Afin de savoir depuis quel dossier seront exécutées les différentes commandes, faisons un test avec pwd, qui est une commande affichant le dossier courant (*print work directory*). Et avant de lancer les commandes, nous allons nous placer dans `/tmp` avec `cd`

Méthode utilisée	pwd
connexion `root` depuis le TTY + `ma_commande`	`/root`
`su` + `ma_commande`	`/tmp`
`su -c “ma_commande”`	`/tmp`
`su -l` + `ma_commande`	`/root`
`su -l -c “ma_commande”`	`/root`
`sudo ma_commande`	`/tmp`
`sudo -s` + `ma_commande`	`/tmp`
`sudo -i ma_commande`	`/root`
`sudo -i` + `ma_commande`	`/root`

Vous voyez que certaines commandes vous ramènent dans `/root`, ce qui n'est pas forcément ce que vous voulez et peut-être dangereux, alors que certaines vous laissent dans le dossier courant, ce qui n'est pas forcément ce que vous voulez et

peut-être dangereux... aussi

PATH

Le PATH est une variable d'environnement très importante. C'est une liste de dossiers séparés par des `:`. Lorsque vous tapez une commande dans le terminal, par exemple `rm`, le shell va chercher dans les dossiers du PATH un par un, pour voir s'ils contiennent un binaire exécutable `rm`. C'est le fichier du premier dossier (de gauche à droite) qui sera sélectionné.

En revanche, si aucun des dossiers du PATH ne contient `rm`, le shell renverra l'erreur suivante :

```
rm: Aucun fichier ou dossier de ce type
```

Vous pouvez tester en ouvrant un nouveau terminal et en tapant

```
PATH=""
rm /tmp/un-fichier-qui-nexiste-pas
```

Tout ceci serait inconséquent si *root* et utilisateurs avaient le même PATH. Mais ce n'est pas le cas.

Le PATH d'un utilisateur est habituellement: `/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games`, parfois on trouve également `$HOME/.local/bin` ou `$HOME/bin`.

Le PATH de root est: `/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin`

On voit que par exemple `/sbin` n'est pas dans le PATH de l'utilisateur, alors que `/usr/games` n'est pas dans le PATH de *root*.

Ainsi, `ip` renverra une erreur dans le shell de l'utilisateur, alors que `/sbin/ip` l'exécutera sans problème.

Si un programme s'attend à être exécuté en *root* avec un PATH de *root*, alors il ne fonctionnera pas si le PATH n'est pas celui de *root*.

En remplaçant `ma_commande` par `sh -c 'printf %s\\n $PATH'` , vous pouvez obtenir les différents PATH.

Méthode utilisée	$PATH
connexion `root` depuis le TTY + `ma_commande`	celui de *root*
`su` + `ma_commande`	celui de l'utilisateur
`su -c “ma_commande”`	celui de l'utilisateur
`su -l` + `ma_commande`	celui de *root*
`su -l -c “ma_commande”`	celui de *root*
`sudo ma_commande`	celui de *root*
`sudo -s` + `ma_commande`	celui de *root*
`sudo -i ma_commande`	celui de *root*
`sudo -i` + `ma_commande`	celui de *root*

Voilà déjà une première raison de ne jamais utiliser `su` ou `su -c` , sauf si l'on ne veut pas exécuter de commande propre à *root*.

env

Pour vous rendre compte des différences entre les environnements des différentes commandes, je vous invite à taper la commande « env » via les différentes méthodes ci-dessus.

Pour synthétiser:

Méthode utilisée	env
connexion `root` depuis le TTY + `ma_commande`	celui de *root*
`su` + `ma_commande`	celui de l'utilisateur
`su -c “ma_commande”`	celui de l'utilisateur
`su -l` + `ma_commande`	celui de *root* + morceaux de celui de l'utilisateur
`su -l -c “ma_commande”`	celui de *root* + morceaux de celui de l'utilisateur
`sudo ma_commande`	celui de *root* + morceaux de celui de l'utilisateur
`sudo -s` + `ma_commande`	celui de *root* + morceaux de celui de l'utilisateur
`sudo -i ma_commande`	celui de *root* + morceaux de celui de l'utilisateur
`sudo -i` + `ma_commande`	celui de *root* + morceaux de celui de l'utilisateur

Voici en exemple ce que j'ai chez moi...

```
==> su <==
(gros bazar)

==> sudo <==
COLORTERM=rxvt-xpm
DISPLAY=:0
HOME=/root
LANG=fr_FR.utf8
LC_ALL=fr_FR.utf8
LOGNAME=root
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;0
1:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42
:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;
31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:
*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01
;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*
.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=
01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;3
1:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.s
wm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjp
eg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=0
1;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;3
5:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:
*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.webp=01;35:*.ogm=01;35:*.mp4=01;35:*.
m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=
```

```
01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;3
5:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.em
f=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00
;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36
:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
MAIL=/var/mail/root
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SHELL=/bin/bash

==> sudo -i <==
COLORTERM=rxvt-xpm
DISPLAY=:0
HOME=/root
LANG=fr_FR.utf8
LC_ALL=fr_FR.utf8
LOGNAME=root
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;0
1:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42
:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;
31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:
*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01
;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*
.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=
01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;3
1:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.s
wm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjp
eg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=0
1;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;3
5:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:
*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.webp=01;35:*.ogm=01;35:*.mp4=01;35:*.
m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=
01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;3
5:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.em
f=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00
;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36
:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
MAIL=/var/mail/root
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
PWD=/root

==> sudo -s <==
COLORTERM=rxvt-xpm
DISPLAY=:0
HOME=/root
LANG=fr_FR.utf8
LC_ALL=fr_FR.utf8
LOGNAME=root
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;0
1:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42
:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;
31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:
```

```
*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01
;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*
.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=
01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;3
1:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.s
wm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjp
eg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=0
1;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;3
5:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:
*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.webp=01;35:*.ogm=01;35:*.mp4=01;35:*.
m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=
01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;3
5:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.em
f=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00
;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36
:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
MAIL=/var/mail/root
OLDPWD=/tmp
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

==> su -l <==
HOME=/root
LANG=fr_FR.UTF-8
LOGNAME=root
MAIL=/var/mail/root
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
PWD=/root
SHELL=/bin/bash
SHLVL=1
TERM=screen-256color
USER=root
```

Vous remarquerez de subtiles différences entre chacun des environnements.

Sécurité

Lorsque qu'on souhaite prendre le contrôle d'une machine, on vise bien souvent les droits *root*, mais pas nécessairement. Qui plus est, il est en général nécessaire de d'abord obtenir un shell utilisateur en guise d'étape intermédiaire.

Si l'on utilise sudo, un attaquant ayant obtenu le mot de passe utilisateur pourra immédiatement devenir root.

Si l'on n'utilise pas sudo, un attaquant ayant obtenu le mot de passe utilisateur devra encore obtenir le mot de passe root, ou trouver un moyen de leurrer l'utilisateur pour l'obtenir. Inversement, si l'attaquant a un accès physique à la machine, il lui suffira d'obtenir le pass root directement, sans avoir à trouver le pass utilisateur.

Reste qu'en fait, la différence n'est pas si importante que ça. En effet, une fois le mot de passe utilisateur obtenu, il est aisé d'effacer tous ses fichiers, ou de les chiffrer, ou de les récupérer, ou de

rajouter des « pièges » pour récupérer ce que l'utilisateur écrit au clavier.

Donc, la morale de l'histoire, c'est qu'il n'y a pas de grosses grosses différences de sécurité entre les deux (pas de sudo restant *un peu plus sûr* pour une utilisation simple de la machine.) En matière de sécurité, le plus gros risque est que l'attaquant réussisse à se connecter à votre compte utilisateur (sans pour autant connaître votre mot de passe), reste à voir comment réduire les possibilités de cela et les implications de sécurité dans ce cas là, mais ceci est une autre histoire.

Conclusion

N'utilisez pas `su` ou `su -c`.

Pour le reste:

Version shell	version one-line	path	pwd
`su -l`	`su -l -c "…"`	root	`/root`
`sudo -s`	`sudo …`	root	inchangé
`sudo -i`	`sudo -i …`	root	`/root`

`su -` est identique à `su -l`, mais cette dernière forme est recommandée par `man su`.