Sub user do

sudo (abréviation de ***substitute user do***) est une commande de type Linux.

Cette commande permet à l'administrateur système d'**accorder** **à certains utilisateurs** (ou **groupes d'utilisateurs**) la possibilité de **lancer une commande en tant qu'administrateur**, ou **comme autre utilisateur**, tout en **conservant une** **trace des commandes saisies et des arguments**.

La commande sudo (*Super User DO*) sous Linux est généralement utilisée comme préfixe d'une commande que seul le super-utilisateur est autorisé à exécuter.

En préfixant sudo avec n'importe quelle commande, il exécute cette commande avec des privilèges élevés ou, en d'autres termes, permet à un utilisateur disposant des autorisations appropriées d'exécuter une commande en tant qu'autre utilisateur, tel que le super-utilisateur.

La philosophie qui sous-tend cela est de **donner aussi peu que possible de droits**, mais de permettre quand même aux utilisateurs de faire leur travail.

sudo est aussi un **moyen efficace d'enregistrer** …

* **qui a exécuté** ;
* **quelle commande**
* et **quand**.

# Installation

Sur certaines distributions, l’utilitaire sudo n’est pas installé.  
Pour installer l’utilitaire …  
**>> su -  
>> apt install sudo  
>> exit**

Pour vérifier la version de sudo …  
**>> sudo --version**ou **>> sudo -V  
Sudo version 1.9.5p2  
La version du greffon de politique de sudoers est 1.9.5p2  
La version de la grammaire du fichier sudoers est 48  
Sudoers I/O plugin version 1.9.5p2  
Sudoers audit plugin version 1.9.5p2**

# Utilité de sudo

Utiliser sudo est **plus sécuritaire que d'ouvrir une session en tant que super-utilisateur** pour un certain nombre de raisons dont …

* **Personne n'a à connaître le mot de passe du super-utilisateur**   
  (sudo demande le mot de passe de l'utilisateur courant) ;
* Des **droits supplémentaires peuvent être accordés temporairement** à des utilisateurs puis retirés sans qu'il aient besoin de la modification de mot de passe ;
* Il est **facile de n'exécuter que les commandes qui nécessitent des droits spéciaux** avec sudo et le reste du temps, on travaille en tant qu'utilisateur non-privilégié, ce qui réduit les dommages que l'on peut commettre par erreur ;
* **Contrôler et enregistrer** …  
  Lorsqu’une commande sudo est exécutée, le **nom de l'utilisateur et la commande sont enregistrés dans un fichier de journalisation**.

# Ajout d’un utilisateur au groupe sudo

Les utilisateurs qui peuvent utiliser la commande sudo doivent avoir une entrée dans le fichier /etc/sudoers.

Par défaut, sudo exige que les utilisateurs s'authentifient avec un mot de passe qui est le mot de passe de l'utilisateur, et non le mot de passe root lui-même.

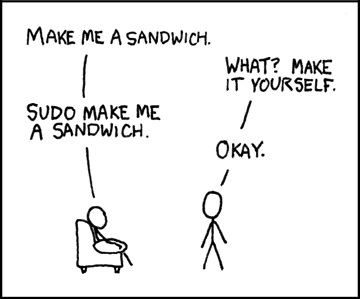
Pour ajouter l'utilisateur tux au groupe sudo …  
**>> sudo usermod --append --groups sudo tux  
>> sudo usermod -aG sudo tux**

On peut ensuite vérifier le résultat avec la commande …  
**>> sudo cat /etc/group | grep sudo  
sudo:x:27:tux**

Une fois que l'utilisateur a été ajouté au nouveau groupe, il **doit se déconnecter puis se reconnecter** afin que l'appartenance au nouveau groupe soit effective.   
En effet, **l'appartenance à un groupe est accordée à un utilisateur au moment de sa connexion**.

Une des erreurs les plus communes est que les utilisateurs se rajoutent à un groupe mais oublient de se déconnecter puis de se reconnecter : ils rencontrent alors des problèmes parce que leur appartenance n'est pas effective.   
On peut vérifier les groupes auxquels on appartient avec la commande id.

**Remarque** …  
Pour la **distribution RHEL/CentOS**, le **groupe wheel** contrôle les utilisateurs sudo.  
On ajoute un utilisateur au groupe wheel avec la commande suivante …  
**>> sudo usermod -aG wheel <Nom d’utilisateur>**



# Fichier /etc/sudoers

Pour modifier ou afficher le fichier sudoers, on doit utiliser la commande sudo ou encore devenir root.   
Pour éditer le fichier sudoers, il est recommandé d'utiliser la commande visudo.

Il est possible d’autoriser certains utilisateurs à exécuter certains programmes.  
Voici un exemple …

**# /etc/sudoers**

**#**

**# This file MUST be edited with the 'visudo' command as root.**

**#**

**# See the man page for details on how to write a sudoers file.**

**# Defaults env\_reset**

**Defaults secure\_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"**

**# Host alias specification**

**# User alias specification  
User\_Alias ADMINS = tux, squiddly, grangallo, atomas**

**# Cmnd alias specification**

**Cmnd\_Alias SHUTDOWN = /sbin/reboot, /sbin/poweroff, /usr/sbin/shutdown**

**Cmnd\_Alias PKGMGMT = /usr/bin/dpkg, /usr/bin/apt, /usr/bin/aptitude**

**Cmnd\_Alias GESTION\_UTILISATEURS = /usr/sbin/useradd, /usr/sbin/usermod, /usr/sbin/userdel**

**# User privilege specification  
# Users listed above (ADMINS) can run package managers and reboot the system.**

**ADMINS ALL = PKGMGMT, SHUTDOWN, GESTION\_UTILISATEURS**

**# Allow members of group sudo to execute any command**

**%sudo ALL=(ALL:ALL) ALL**

**#Default rule for root.**

**root ALL=(ALL) ALL**

**tux localhost = /usr/bin/wireshark**

**squiddly localhost = (ansible) /usr/bin/pkill, /usr/bin/kill**

**#includedir /etc/sudoers.d**

**Privilèges**

Voici, en quelques mots, comment il est possible de spécifier des privilèges (habituellement en fin de fichier).

Elles se présentent ainsi …  
**utilisateur hôte=() commandes**

Par exemple …

* **tux DebianBullseye = /usr/bin/wireshark**Autorise l'utilisateur tu à exécuter *wireshark* en tant que *root* sur son propre système ;
* **squiddly DebianBullseye = (ansible) /usr/bin/pkill, /usr/bin/kill**Autorise l'utilisateur squiddly à exécuter les commandes *pkill* et *kill* en tant qu'utilisateur *ansible*   
  (par exemple, grâce à cette commande … **sudo -u ansible kill ansible** ou **sudo -u ansible pkill ansible**) ;
* **%admin ALL=(ALL) ALL**Autorise les membres du groupe admin d’exécuter toutes les commandes sous n'importe quel compte (=(ALL)), à partir de n'importe quel hôte ;
* **%sudo ALL=NOPASSWD:ALL**Autoriserait (s'il n'était pas commenté) les utilisateurs du groupe *sudo* à exécuter n'importe quelle commande à partir de n'importe quel hôte en tant que n'importe quel utilisateur sans saisir un mot de passe.

**Attention** …  
Il est prudent de ne pas accorder des droits *root* aux utilisateurs leur permettant de modifier leurs propres droits.   
Par exemple, si on accorde les droits *root* pour l'exécution de *nano* ou *gedit*, rien ne les empêcherait de modifier le fichier /*etc/group* pour s'ajouter dans le groupe *admin*.

# sudoers est en lecture seule

Le **fichier /etc/sudoers** est **intentionnellement en lecture seule**, même pour le super-utilisateur 9root).  
Seuls les administrateurs peuvent **modifier ce fichier et cela seulement avec la commande visudo**.

Le fichier /**etc/sudoers peut être modifié à l’aide d’un éditeur de texte comme nano** mais visudo est plus utile car il possède une **fonction de vérification syntaxique**. Cela permet de **préserver l’intégrité du fichier**.

Si le fichier /etc/sudoers est endommagé, la **réparation est simple avec la commande su -c visudo**.

# Alias

Pour éviter d’alourdir le fichier /ect/sudoers (trop nombreuses lignes), il est possible d’utiliser des alias.

Voici quelques exemples …

* **User\_Alias GROUPENGINX = tux, squiddly**
* **Host\_Alias GRAPHISME = 192.168.1.2, 192.168.1.3, 192.168.1.4**
* **Cmnd\_Alias STOP = /usr/bin/pkill, /usr/bin/kill**

Ainsi, il est possible de les utiliser pour rédiger des éléments plus simples …  
**GROUPENGINX GRAPHISME=(nginx) STOP**

Autres exemples …

* **User\_Alias ADMINS = grangallo alcibiade**
* **Cmnd\_Alias SHUTDOWN = /sbin/reboot, /sbin/poweroff**
* **Cmnd\_Alias PKGMGMT = /usr/bin/dpkg, /usr/bin/apt, /usr/bin/aptitude**
* **ADMINS ALL = PKGMGMT, SHUTDOWN**

# Commandes Defaults

Quelques commandes supplémentaires sont disponibles afin de paramétrer la commande sudo.   
Elles sont à ajouter à la ligne Defaults.

Voici quelques exemples …

**Insults**  
Affiche des drôles de messages lorsque l’on se trompe de mot de passe pour sudo   
Exemple …  
**insult= ‘je connais des manchots qui sont meilleur que toi à la saisie’**

**timestamp\_timeout**Modifie le temps nécessaire avant de devoir saisir à nouveau le mot de passe (par défaut de **5 minutes**)  
Exemple …  
**timestamp\_timeout=0 … ne conserve pas en mémoire le mot de passe**

**passwd\_tries**  
Modifie le nombre de mots de passe incorrects acceptés (par défaut 3 tentatives)  
Exemple …  
**passwd\_tries:2 n'autorise que 2 tentatives avant que la commande échoue**

Enfin, il existe deux façons d'ajouter ces options …

* en les ajoutant pour tout le monde …  
  **Defaults insults,logfile=/var/log/sudo**
* en les ajoutant pour une personne en particulier …  
  **Defaults:tux insults,logfile=/var/log/sudo,passwd\_tries:2**

# Directive include

Le fichier /etc/sudoers standard, dans les dernières versions de Debian se termine, avec la ligne …  
**# @includedir /etc/sudoers.d**

Cela permet à d'autres paquets de fournir des bouts de code dans le **répertoire /etc/sudoers.d/<Nom de paquet>** qui modifient la configuration de sudo.

On peut modifier la ligne en retirant le caractère # initial (le dièse) afin d,activer cette fonctionnalité.

## Journalisation

Les messages de journalisation de sudo se trouvent dans les journaux d’authentification.  
On peut les consulter à l’aide de la commande …  
**>> sudo less /var/log/auth.log**

Voici une ligne de ce fichier …  
**Mar 22 14:07:45 : squiddly : TTY=pts/0 ; PWD=/home/squiddly ; USER=root ; COMMAND=/bin/nano /etc/systemd/system/mnt-data.mount**On constate que le mardi 22 à 14h07, l'utilisateur squiddly (se trouvant dans le dossier /home/squiddly) a exécuté (au nom de root) la commande nano /etc/systemd/system/mnt-data.mount

Le fichier journal contiendra une bonne quantité d’entrées qui ne sont probablement pas intéressantes (pour les messages sudo) …  
**>> sudo grep sudo /var/log/auth.log**

Si on préfére les avoir au format fichier, on ajoute une telle redirection après la commande …  
**>> sudo grep sudo /var/log/auth.log | sudo tee sudolist.txt**

**logfile**  
La directive Defaults logfile définie le fichier de journalisation de sudo.  
Elle peut s’avérer utile pour regrouper au sein d’un même journal toutes les messages relatifs à sudo …  
**>> sudo visudo  
Defaults logfile=/var/log/sudo**

# Problèmes et conseils

## Chemin d’accès (PATH) non configuré

Voici une erreur classique qui survient avec l'utilisation de sudo pour installer un paquet …  
**dpkg: warning: 'ldconfig' not found in PATH or not executable.  
dpkg: warning: 'start-stop-daemon' not found in PATH or not executable.  
dpkg: error: 2 expected programs not found in PATH or not executable.  
Note: root's PATH should usually contain /usr/local/sbin, /usr/sbin and /sbin.**

Le fichier /etc/sudoers fourni par le paquet contient cette ligne …  
**Defaults secure\_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"**

## Redirection d’un flux avec sudo

sudo pose a priori des problèmes pour la redirection de flux dans une console.

Par exemple, la redirection suivante ne fonctionnera pas …   
**>> sudo echo 2 > /dev/null**

La raison de cet échec est que sudo n'exécute que la première tâche (echo 2) avec l'identité empruntée ;   
la redirection, quant à elle, est effectuée en mode utilisateur uniquement.

La solution, pour contourner cette limitation, est d'appeler un nouvel interpréteur de commandes et de lui faire exécuter votre redirection de flux.   
Par exemple …  
**>> sudo sh -c 'echo 2 > /dev/null'**

De cette manière, c'est tout l'interpréteur sh et la commande passée en argument qui est exécutée avec l'identité empruntée

**Remarque** …  
La configuration de sudo est parfois un peu laborieuse, mais c’est le prix à payer pour une administration saine d’un système.   
Il faut faire aussi attention à ne pas se laisser tenter par une délégation de droits trop simpliste comme …   
**admin ALL = (ALL) NOPASSWD: ALL**

La page de man de sudo et sudoers (man sudoers – man sudo) comporte de nombreux exemples d’utilisation avancée de sudo.

## Commande sudo

**sudo – Exécution d’une commande en tant qu'un autre utilisateur**

Voici quelques commutateurs pratiques …

|  |  |  |
| --- | --- | --- |
| Forme  courte | Forme  longue | Description du commutateur |
| -b | **--background** | Exécution de la commande en arrière-plan |
| -h | **--help** | Affichage du message d'aide et terminer |
| -i | **--login** | Exécution de l’interpréteur de commandes (*shell*) d’ouverture de session (*login*) de l'utilisateur ciblé Une commande peut aussi être spécifiée |
| -l | **--list** | Affichage des privilèges de l'utilisateur ou vérification d’une commande spécifique  Utiliser deux fois affiche une forme plus longue (--list –list) |
| -s | **--shell** | Exécution de l’interpréteur de commandes (shell) en tant que l'utilisateur ciblé Une commande peut aussi être spécifiée |
| -U | **--other-user=user** | En mode liste, affichage des privilèges de l'utilisateur ciblé |
| -u | **--user=user** | Exécution de la commande (ou édition de fichier) sous le nom d'utilisateur  ou le ID spécifié |
| -V | **--version** | Affichage des informations de version |

**Astuce** …  
Lors de la saisie d’une commande nécessitant les droits d’administratration sans sudo, il est possible de saisir la commande **sudo !!** qui reprendra automatiquement la dernière commande en ajoutant sudo

Exécution d’une commande en tant qu'utilisateur différent

Pour exécuter une commande au nom d’un utilisateur différent …  
**>> sudo -u <Nom de l’utilisateur> ,Commande>  
>> sudo -u root whoami**

## Basculement vers root

## Il est possible de basculer rapidement l’invite de commande vers le shell BASH en tant qu'utilisateur root … >> sudo bash

## Éditeur de texte par défaut

En fonction de la distribution, vim ou nano sont les éditeurs de texte par défaut pour la commande visudo.

Pour modifier l’éditeur de texte …  
**>> sudo update-alternatives --config editor**   
**Il existe 3 choix pour l'alternative editor (qui fournit /usr/bin/editor).  
 Sélection Chemin Priorité État  
------------------------------------------------------------  
\* 0 /bin/nano 40 mode automatique  
 1 /bin/nano 40 mode manuel  
 2 /usr/bin/mcedit 25 mode manuel  
 3 /usr/bin/vim.tiny 15 mode manuel  
Appuyez sur <Entrée> pour conserver la valeur par défaut[\*] ou choisissez le numéro sélectionné :**

## Variables d'environnement

Ces variables d'environnement sont utilisées par sudo …

|  |  |
| --- | --- |
| Variable | Description |
| EDITOR | Éditeur par défaut à utiliser en mode -e (sudoedit) si la variable VISUAL n'est pas définie |
| HOME | En mode -s ou -H (ou si sudo a été configuré avec l'option --enable-shell-sets-home),  définie sur homedir de l'utilisateur cible |
| PATH | Définie sur une valeur saine si l'option secure\_path sudoers est définie |
| SHELL | Utilisée pour déterminer le shell à exécuter avec l'option -s |
| SUDO\_PROMPT | Utilisée comme invite de mot de passe par défaut |
| SUDO\_COMMAND | Définie sur la commande exécutée par sudo |
| SUDO\_USER | Définie sur le login de l'utilisateur qui a appelé sudo |
| SUDO\_UID | Définie sur l'UID de l'utilisateur qui a appelé sudo |
| SUDO\_GID | Définie sur le GID de l'utilisateur qui a invoqué sudo |
| SUDO\_PS1 | Si définie, la variable PS1 sera définie sur cette valeur |
| USER | Définie sur l'utilisateur cible (root sauf si l'option -u est spécifiée) |
| VISUAL | Éditeur par défaut à utiliser en mode -e (sudoedit) |