Xenial | administration | sécurité | sudoers

Configuration avancée de l'utilitaire sudo

L'utilitaire « sudo », par le jeu de paramètres dont il dispose, peut autoriser ou refuser à un utilisateur ou à un groupe d'utilisateur l'exécution de tâches privilégiées avec ou sans saisie d'un mot de passe. Cette gestion des droits accordés aux utilisateurs est consignée dans le fichier */etc/**sudoers***. Le présent document n'est cependant pas le manuel d'utilisation de ce fichier. Son objectif est d'indiquer comment le modifier dans le contexte des distributions Ubuntu, et de donner quelques exemples de configuration adaptés à un environnement domestique ou à une PME/PMI.

D'autres paramètres, destinés aux administrateurs de systèmes, concernent également la durée de validité de l'authentification des utilisateurs, la localisation du journal des événements et le niveau de courtoisie de `sudo` .

1. Modification du fichier /etc/sudoers

1.1 /etc/sudoers.d/

Confer le fichier */etc/sudoers.d/**README***
La gestion de `sudo` est améliorée dans les dernières versions (Debian version 1.7.2). C'est à dire pour toutes les versions d'Ubuntu supportées.

Tous les fichiers du répertoire **/etc/sudoers.d/** ne finissant pas par `~` ou ne contenant pas un `.` sont lus et analysés lorsque l'on utilise la commande `sudo` .

Pour modifier le fonctionnement de la commande `sudo` , l'administrateur du système ne modifie plus le fichier */etc/**sudoers*** mais positionne des fichiers de personnalisation dans le répertoire */etc/**sudoers.d***.

1.1.1 avantages

vous pouvez définir autant de fichiers que de modifications (voir le §2). Le nom est libre et peut donc faire référence à l'élément personnalisé. Exemples : **monfichier** , **10-sysctl** , **20-userX** , **30-apt**.

1. Vous disposez d'un aperçu des modifications en listant simplement le contenu du répertoire */etc/**sudoers.d***.
2. l'administrateur peut annuler à tout moment une autorisation particulière de la commande `sudo` en supprimant le fichier de personnalisation correspondant.
3. En supprimant tous les fichiers de personnalisation, vous êtes certain de revenir à la configuration par défaut de `sudo` qui sera restée d'origine.
4. Cette configuration peut se mettre à jour sans perdre vos modifications locales.

pour ce faire

```
sudo visudo -f /etc/sudoers.d/monfichier
```

1.2 /etc/sudoers

Si il est toujours préférable de privilégier d'écrire ses modifications locales dans /etc/sudoers.d il est toujours possible de surcharger directement le fichier /etc/sudoers.

La configuration de `sudo` est enregistrée dans le fichier de configuration */etc/**sudoers***.

La modification de ce fichier s'effectue à travers un utilitaire de vérification appelé **visudo**.

```
sudo visudo
```

Il effectue une vérification de l'intégrité du fichier après modification avant de l'enregistrer. En cas d'erreur lors de la modification, le nouveau fichier n'est pas enregistré, ce qui vous évite de vous retrouver dans l'impossibilité de corriger votre erreur. Enfin, il s'assure que ce fichier conserve ses droits Unix originaux, ce qui garantit le bon fonctionnement de `sudo` .
À la fermeture du fichier */etc/sudoers* ouvert par son outil d'édition **visudo**, la nouvelle configuration est automatiquement chargée.

1.3 Choisir l'éditeur utilisé par visudo

1.3.1 A chaque fois

Pour forcer l'utilisation d'un éditeur lors de l'ouverture du fichier */etc/**sudoers*** par **visudo** , exécutez dans une fenêtre de terminal l'une des commandes suivantes :

- **Dans Ubuntu :** `sudo VISUAL=/usr/bin/gedit visudo`
- **Dans Kubuntu :** `sudo VISUAL=/usr/bin/kate visudo`
- **Dans Xubuntu :** `sudo VISUAL=/usr/bin/mousepad visudo`
- **Dans Lubuntu :** `sudo VISUAL=/usr/bin/leafpad visudo`
- **En mode console :** `sudo EDITOR=/usr/bin/nano visudo` **ou** `sudo EDITOR=/usr/bin/vim visudo`

1.3.2 configurer l'éditeur par défaut

pour changer l'éditeur en ligne de commande, par défaut, il suffit de lancer :

```
sudo update-alternatives --config editor
```

et de sélectionner l'éditeur de votre choix, dans la liste des éditeurs de texte déjà installés.

---

2. Ajout ou retrait de privilèges à un compte d'utilisateur ou un groupe d'utilisateurs

À **la fin du fichier**, ajoutez une ligne d'instruction…

En cas de litige entre ligne, ce sera la dernière dans le fichier sudoers qui sera comptée ! Si par exemple , *jérome* fait partie du groupe *paris* et que vous mettez que *jérome* peut executer la commande *ls*, puis que plus loin vous mettez que le groupe *paris* ne peut pas executer la commande *ls*, *jérome* ne pourra pas executer la commande *ls* (du moins pas avec sudo) car la dernière ligne qui le concerne refuse l'execution de ls ! D'où l'importance de **bien situer la ligne que vous souhaitez inclure**, notamment **par rapport aux lignes déjà pré-définies pour les groupes admin et sudo** !

…telle que la suivante :

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

- `identifiant` représente un identifiant utilisateur du système Ubuntu. Un seul identifiant doit être précisé par ligne ;
- `%groupe` désigne un groupe d'utilisateurs du système Ubuntu. Le nom du groupe doit donc être précédé d'un symbole de pourcentage (`%`). Un seul groupe doit être précisé par ligne ;
- `ALL` désigne la ou les machines dans lesquelles les commandes suivantes sont autorisées ou refusées pour cet utilisateur ou ce groupe d'utilisateurs. Le mot-clé `ALL` désigne l'ensemble des machines de votre parc informatique. Dans le cadre d'une utilisation à domicile, laisser `ALL` n'est pas un inconvénient. Dans un grand parc d'entreprise, de meilleures stratégies sont à prévoir ;
- `user` (entre parenthèses) désigne l'utilisateur dont on prend les droits (peut valoir ALL pour tous)
- `commande` et `autrecommande` 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. Pour cette raison, préférez saisir des chemins absolus vers des commandes plutôt que des chemins relatifs (par exemple, `/usr/sbin/update-manager` plutôt que `update-manager`). Pour connaître le chemin absolu d'une commande ou d'un utilitaire, saisissez dans un terminal `which` *`commande`* [1], ou `whereis` *`commande`* [2] en remplaçant *`commande`* par la commande en question.

2.1 Exécuter des tâches d'administration sans mot de passe

À la fin du fichier, ajoutez une ligne d'instruction telle que la suivante :

```
identifiant     ALL = (ALL) /chemin/complet/commande, NOPASSWD: /chemin/complet/autrec
%groupe ALL = (ALL) NOPASSWD: /chemin/complet/commande,/chemin/complet/autrecommande
```

Toutes les commandes situées à la droite du mot-clé `NOPASSWD:` peuvent être exécutées par l'utilisateur ou le groupe d'utilisateurs précisé en début d'instruction. Celles restées à sa gauche sont toujours soumises à l'authentification par mot de passe.

Dans cet exemple, *identifiant* doit fournir son mot de passe pour exécuter `commande`, mais n'a pas à le saisir pour exécuter `autrecommande`. Quand aux membres du groupe *groupe*, ils n'ont pas à saisir leur mot de passe pour exécuter `commande` ou `autrecommande`.

Attention : il ne faut pas mettre juste la commande, mais tout le chemin vers le fichier. Par exemple il ne faut pas mettre "ls" mais "/bin/ls".

Attention aux brèches de sécurité !
Faites *extrêmement* attention lorsque vous autorisez un utilisateur ou un groupe à exécuter une commande sans mot de passe. Ceci pourrait causer des brèches de sécurité si les commandes autorisées sont potentiellement dangereuses.

Pensez à utiliser newgrp pour basculer votre groupe actif avant de faire appel à la commande autorisée par le sudo.
Voici un petit exemple, changer un code clavier.
Après avoir créé le groupe codeclavier, pensez à utiliser un numéro spécial pour éviter les conflits avec les groupes utilisateurs, vous ajoutez cette ligne dans le fichier /etc/sudoers.

```
%codeclavier    ALL = (ALL) NOPASSWD: /bin/changecode
```

et maintenant le petit script évidemment mis dans /bin/code.clavier.sh

```
sudo /bin/changecode
```

et enfin /bin/changecode

```
#!/bin/sh
setkeycodes 0x2b 86
```

Et miracle, il marche. Si vous ajoutez un lien dans /etc/profile.d/, il sera exécuté à votre connexion en toute transparence!!!

2.2 Exécuter un programme en tant qu'un autre 'user'

La commande sudo permet d'exécuter un programme en tant qu'un autre utilisateur. Par exemple, la ligne :

```
foo      ALL=(bar) NOPASSWD: /chemin/complet/program
```

permet à foo d'utiliser program en tant que bar sans qu'on ne lui demande son mot de passe.

Note : Après il faut quand même utiliser **sudo** pour le lancement de **program**. Comme ceci :

```
sudo program
```

---

3. Changement d'options

3.1 Augmenter ou réduire le temps de grâce avant que la saisie du mot de passe soit de nouveau demandée

Ajoutez l'option `timestamp_timeout=X` à la fin de la ligne débutant par `Defaults` . La valeur `X` doit être remplacée par la durée, en minutes, durant laquelle le mot de passe n'a pas à être fourni pour effectuer des actions d'administration dans le terminal ou pseudo-terminal courant. La valeur `0` désactive ce temps de grâce : un mot de passe doit être fourni à chaque action d'administration.

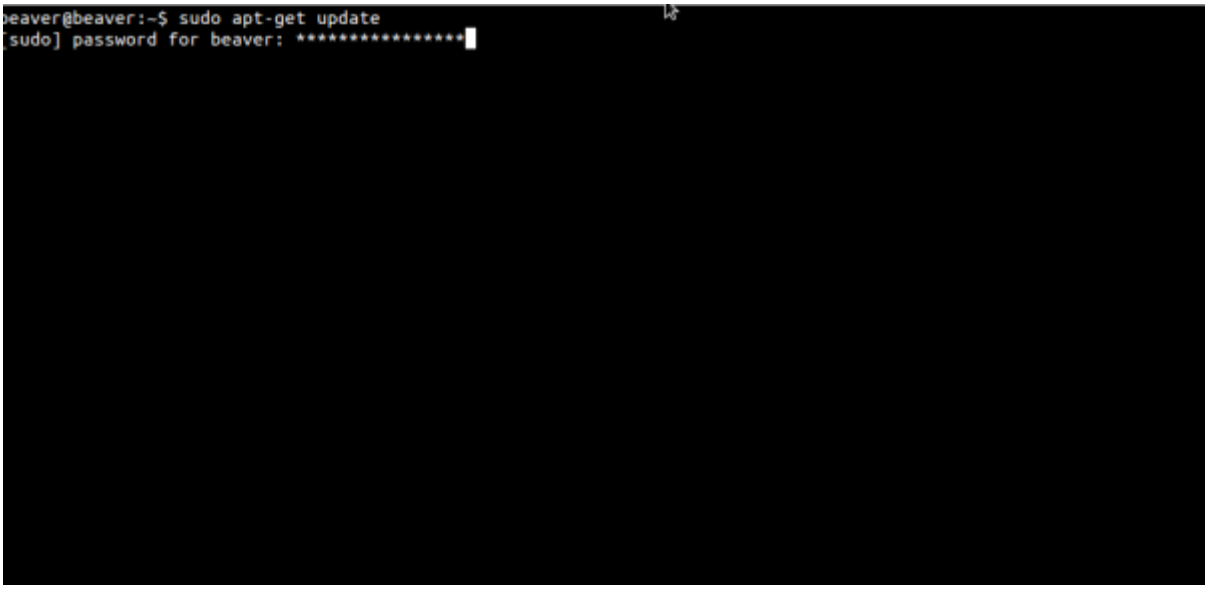
```
Defaults        env_reset
```

devient

```
Defaults        env_reset,timestamp_timeout=X
```

Si cette option n'est pas précisée, le temps de grâce par défaut est 15 minutes.

3.2 Afficher des astérisques lors de la saisie du mot de passe

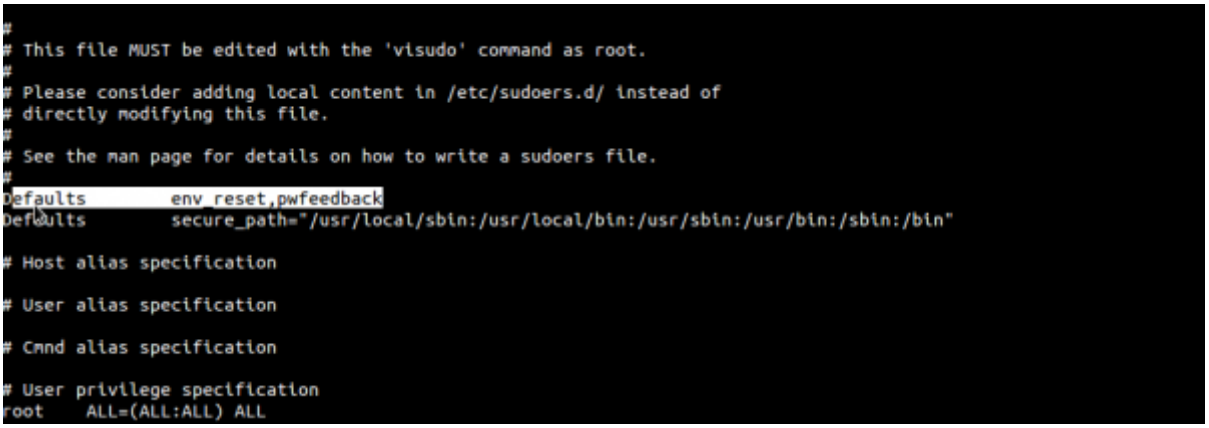


Ajoutez l'option `pwfeedback` à la fin de la ligne débutant par `Defaults` .

```
Defaults        env_reset
```

devient

```
Defaults        env_reset,pwfeedback
```



3.3 Changer le message d'erreur de mauvais mot de passe

Ajoutez l'option badpass_message="texte à afficher" à la fin de la ligne débutant par "Defaults".

```
Defaults        env_reset
```

devient

```
Defaults        env_reset,badpass_message="texte à afficher"
```

3.4 Des insultes en cas d'erreur de mot de passe

Ajoutez l'option `insults` à la fin de la ligne débutant par `Defaults` .

```
Defaults        env_reset
```

devient

```
Defaults        env_reset,insults
```

---

4. Réparer un fichier erroné

Si, en tentant d'exécuter une commande sudo, vous obtenez une erreur comme ci-dessous, c'est que votre fichier sudoers est corrompu. Comme il est corrompu, vous ne pouvez plus exécuter sudo, et donc plus modifier le fichier … cercle vicieux

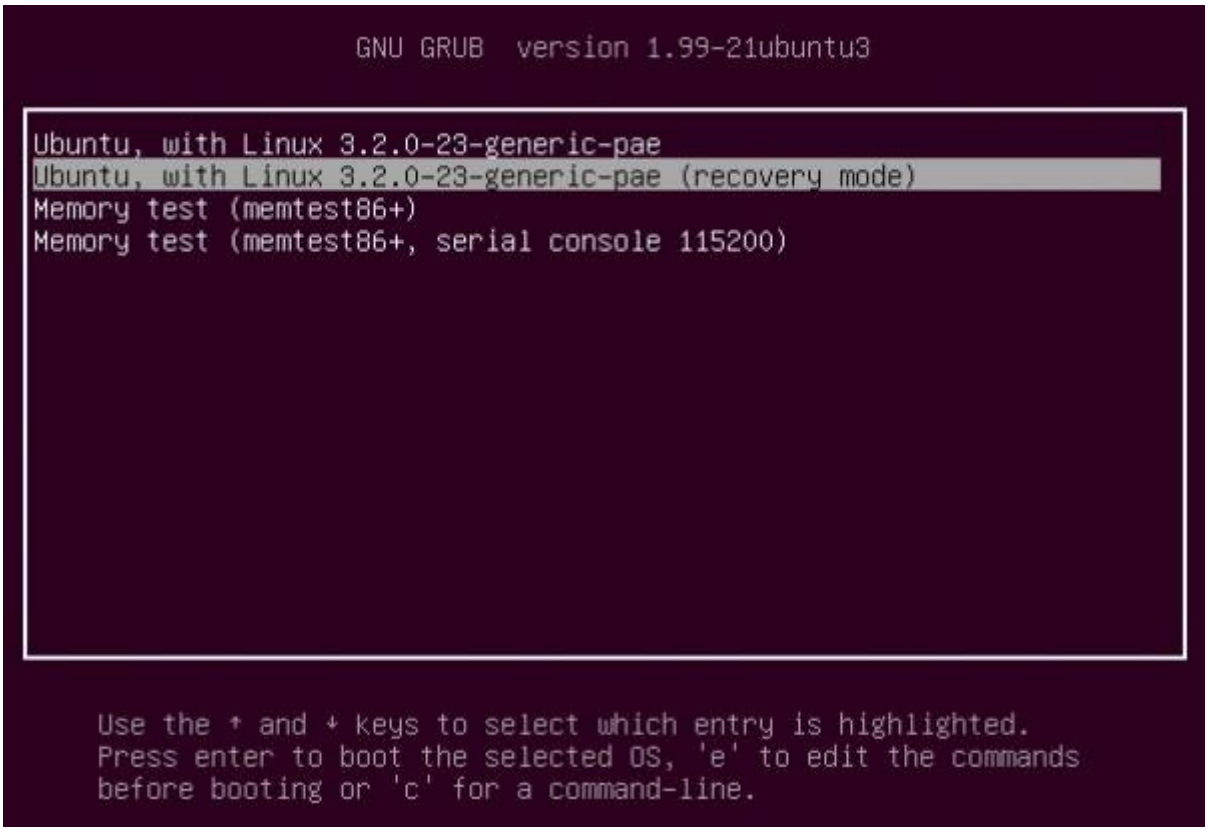
```
toto@fixe:~$ sudo
>>> sudoers file: syntax error, line 0 <<<
```

Une solution à tenter est de lancer la commande :

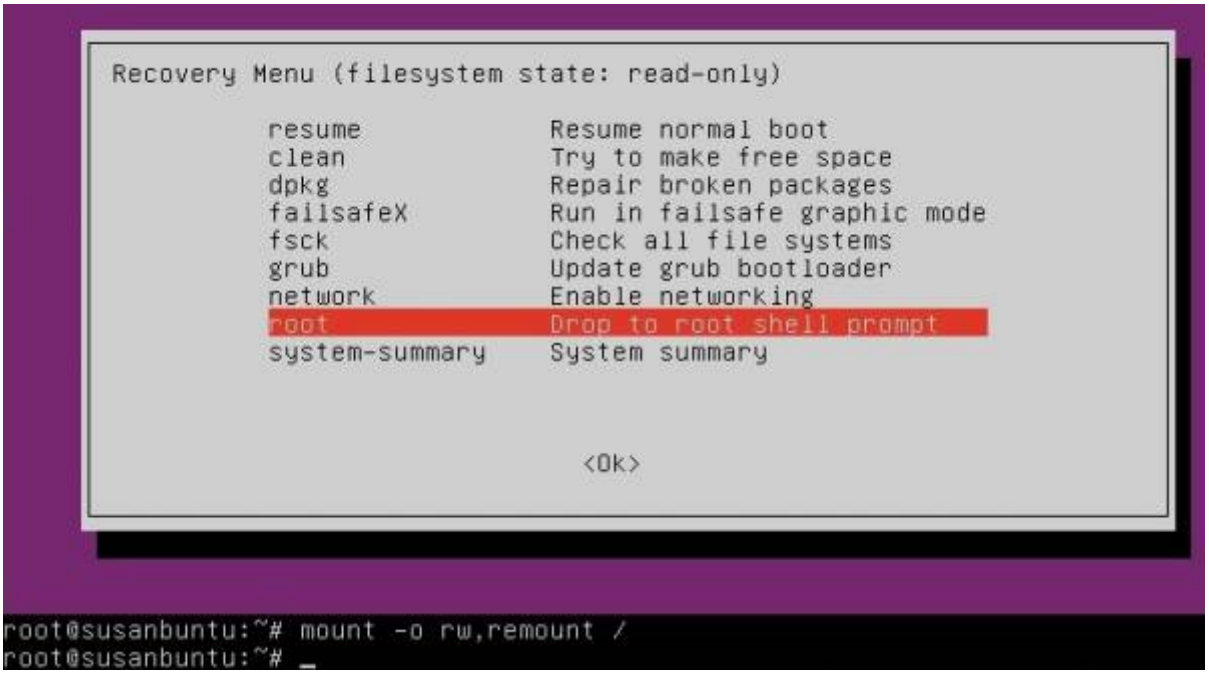
```
pkexec visudo
```

Ou bien d'utiliser la solution suivante (https://www.psychocats.net/ubuntu/fixsudo)[3].

4.1 Redémarrer en mode recovery



4.2 Choisir l'option "root"



4.3 Remonter les disques en écriture

```
mount -o remount,rw /
```

4.4 Editer / corriger le fichier 'sudoers'

Faire les opérations souhaitées comme éditer le fichier à la main :

```
    cp /etc/sudoers /etc/sudoers.backup
    nano /etc/sudoers
```

Voir ici (https://www.psychocats.net/ubuntu/fixsudo) pour d'autres possibilités.

5. Aller plus loin...

Consultez la page de manuel officiel du fichier */etc/**sudoers*** :

- En ligne : Sudoers Manual (http://www.sudo.ws/sudo/sudoers.man.html) ;
- Copie locale : `man sudoers` Ce document regorge d'options supplémentaires et d'exemples pour personnaliser grandement le comportement de `sudo` .
- **(fr)** Comment donner certains droits root à un utilisateur (Sudo) (http://guide.andesi.org/html/ksudo.html)

———

[1] which (http://manpages.ubuntu.com/which)
[2] whereis (http://manpages.ubuntu.com/whereis)
[3] source http://askubuntu.com/questions/73864/how-to-modify-a-invalid-etc-sudoers-file-it-throws-out-an-error-and-not-allowi (http://askubuntu.com/questions/73864/how-to-modify-a-invalid-etc-sudoers-file-it-throws-out-an-error-and-not-allowi)