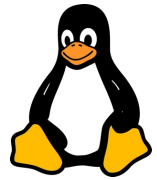
SUDO



Introduction :

Dans les systèmes Unix et Linux, les droits de superutilisateur (root) sont nécessaires pour exécuter des commandes qui modifient des aspects cruciaux du système. Cependant, il est dangereux de travailler constamment avec les privilèges de superutilisateur en raison des risques de sécurité et de la possibilité de commettre des erreurs avec des conséquences systèmes importantes. Pour résoudre ce problème, les systèmes Linux offrent une solution appelée sudo.

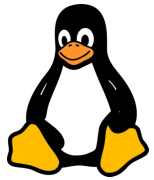
Qu'est-ce que Sudo?

sudo est un programme pour Unix et Linux qui permet à un utilisateur de lancer des commandes avec les privilèges de sécurité d'un autre utilisateur, par défaut le superutilisateur root. Le nom sudo est dérivé de "superuser do" ou "substitute user do".

Le Groupe Sudo :

Sous Linux, les utilisateurs autorisés à utiliser la commande sudo sont membres d'un groupe spécial appelé sudo. L'appartenance à ce groupe est contrôlée par le fichier de configuration /etc/sudoers.

SUDO



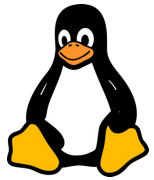
Comment Utiliser Sudo ?

- Pour utiliser sudo, préfixez simplement une commande avec sudo et entrez votre mot de passe lorsque vous y êtes invité.
- Par exemple, pour exécuter apt-get update avec des privilèges root, vous écririez sudo apt-get update.
- Si votre utilisateur est dans le groupe sudo, le système vous demandera votre mot de passe, puis exécutera la commande avec des privilèges élevés.

Ajouter un Utilisateur au Groupe Sudo :

- Pour ajouter un utilisateur au groupe sudo, un superutilisateur doit exécuter la commande: usermod -aG sudo username.
- Vous pouvez également ajouter un utilisateur au groupe sudo en le modifiant directement dans le fichier /etc/sudoers.

SUDO



Fichier /etc/sudoers :

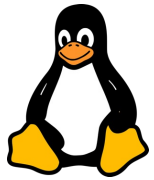
- C'est un fichier de configuration qui détermine qui peut utiliser sudo et quelles commandes ils peuvent exécuter.
- Il est édité avec la commande visudo, qui vérifie la syntaxe avant de sauvegarder les modifications pour éviter les erreurs de configuration.
- Les lignes dans /etc/sudoers ressemblent à ceci : username ALL=(ALL:ALL) ALL, ce qui signifie que l'utilisateur username peut exécuter toutes les commandes en tant que tous les utilisateurs sur toutes les machines.

La syntaxe complète est :

```
utilisateur hôte=(utilisateur_cible) commandes
```

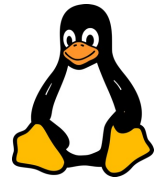
- Utilisateur : l'utilisateur qui a les permissions.
- Hôte : les machines sur lesquelles les permissions s'appliquent.
- Utilisateur_cible : les utilisateurs sous lesquels les commandes peuvent être exécutées. (ALL) signifie n'importe quel utilisateur.
- Commandes : les commandes que l'utilisateur est autorisé à exécuter.

SUDO



```
  GNU nano 5.4                        /etc/sudoers.tmp *
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:>
Defaults        timestamp_timeout=1
# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d



^G Aide      ^O Écrire    ^W Chercher  ^K Couper     ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^\ Remplacer ^U Coller     ^J Justifier ^_ Aller ligne
```

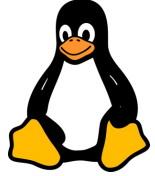
SUDO



```
  GNU nano 5.4                        /etc/sudoers.tmp *
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:>
Defaults        timestamp_timeout=1
# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
bob     ALL=(ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d


^G Aide       ^O Écrire     ^W Chercher  ^K Couper     ^T Exécuter  ^C Emplacement
^X Quitter    ^R Lire fich. ^\ Remplacer ^U Coller     ^J Justifier ^_ Aller ligne
```

Ici, on ajoute l'utilisateur bob et on lui donne tous les droits. C'est l'équivalent de l'ajout de l'utilisateur au groupe sudo.

SUDO



john ALL=(ALL) ALL

Cette ligne permet à l'utilisateur john d'exécuter n'importe quelle commande en tant que n'importe quel utilisateur sur toutes les machines.

%admin ALL=(ALL) ALL

Tout membre du groupe admin peut exécuter toutes les commandes sur toutes les machines.

bob ALL=(ALL) NOPASSWD: ALL

L'utilisateur bob peut exécuter toutes les commandes sans avoir à entrer son mot de passe.

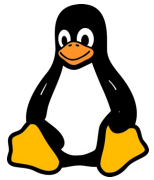
dave ALL=(www-data) ALL

L'utilisateur dave peut exécuter n'importe quelle commande mais seulement en tant que l'utilisateur www-data.

alice ALL=(ALL) /bin/ls, /bin/cat, /usr/bin/top

Cela signifie que l'utilisateur alice peut exécuter les commandes /bin/ls, /bin/cat, et /usr/bin/top sur toutes les machines en tant que n'importe quel utilisateur.

SUDO



Pratiques Recommandées :

- Utilisez sudo au lieu de se connecter en tant que root.
- Limitez l'accès sudo aux utilisateurs qui en ont besoin.
- Utilisez sudo pour exécuter des commandes spécifiques avec des privilèges élevés plutôt que de travailler avec un shell root ouvert.

Sécurité :

- L'utilisation de sudo offre une trace d'audit des commandes exécutées avec des privilèges élevés, car chaque commande sudo est enregistrée dans /var/log/auth.log.
- Le mot de passe de l'utilisateur est requis pour utiliser sudo, ce qui signifie qu'une personne doit authentifier chaque session de privilèges élevés.