sudo

La commande “sudo” est une commande sous Linux qui permet à un utilisateur d'exécuter des commandes avec les privilèges d'un autre utilisateur, généralement l'utilisateur **superutilisateur** (`root`).

La commande `sudo` est souvent utilisée pour exécuter des commandes en tant qu'administrateur sans avoir à se connecter en tant que **superutilisateur**, ce qui permet une meilleure sécurité et une meilleure traçabilité des actions effectuées.

Lorsque vous utilisez la commande `sudo`, vous devez spécifier le nom de l'utilisateur dont les privilèges vous souhaitez utiliser, suivi de la commande à exécuter. Par exemple, si vous souhaitez mettre à jour votre système en tant qu'administrateur, vous pouvez taper :

```
sudo apt update
```

Ensuite, vous devrez entrer le mot de passe de votre utilisateur pour confirmer que vous êtes autorisé à exécuter la commande avec les privilèges de l'utilisateur spécifié. Si vous avez les autorisations nécessaires, la commande sera exécutée.

Il est recommandé d'utiliser `sudo` plutôt que de `su` pour exécuter des commandes en tant qu'administrateur car elle permet de limiter les risques d'erreurs et de sécurité. En effet, les commandes exécutées avec `sudo` sont enregistrées dans les journaux système, ce qui facilite la détection des actions suspectes ou malveillantes.

La commande `sudo` est généralement déjà installée sur la plupart des distributions Linux. Cependant, si elle n'est pas installée sur votre système, vous pouvez l'installer en utilisant le gestionnaire de paquets de votre distribution en adminstrateur :

```
su -
```

Puis selon votre distribution :

Debian, Ubuntu et dérivés :

```
apt update
apt install sudo
```

Red Hat, CentOS et dérivés :

```
yum install sudo
```

Fedora :

```
dnf install sudo
```

Pour pouvoir utiliser la commande `sudo`, l'utilisateur courant doit être autorisé à le faire. Je vous le détaille ci-dessous.

Préconfiguration du groupe sudo

Pour voir la préconfiguration du groupe `sudo`, vous pouvez afficher le contenu du fichier `/etc/sudoers`. Ce fichier contient la configuration globale de sudo et spécifie les utilisateurs, les groupes et les commandes qui sont autorisés à utiliser `sudo`.

Voici comment afficher le contenu du fichier `/etc/sudoers` :

– Ouvrez un terminal sur votre système Linux.

– Tapez la commande suivante et appuyez sur Entrée :

```
sudo cat /etc/sudoers
```

– Entrez le mot de passe de votre utilisateur si vous y êtes invité.

Cette commande affiche le contenu du fichier `/etc/sudoers` dans le terminal. Vous pouvez y rechercher les sections qui concernent le groupe `sudo` pour voir les autorisations de ce groupe.

Par exemple, la section suivante du fichier `/etc/sudoers` accorde des autorisations au groupe `sudo` :

```
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

Cette section spécifie que les membres du groupe `sudo` sont autorisés à exécuter toutes les commandes avec les privilèges de tous les utilisateurs et groupes. Vous pouvez également trouver d'autres sections qui spécifient des autorisations pour des utilisateurs ou des commandes spécifiques.

Le fichier `/etc/sudoers` est un fichier de configuration critique, et toute modification incorrecte peut entraîner des problèmes de sécurité ou des erreurs système. Par conséquent, il est recommandé de faire une copie de sauvegarde du fichier avant de le modifier et de suivre les bonnes pratiques de sécurité recommandées pour la gestion des utilisateurs et des permissions sur votre système.

Ajouter un utilisateur au groupe sudo pour autoriser l'utilisation de sudo

Pour autoriser un utilisateur à utiliser la commande `sudo`, vous pouvez suivre les étapes suivantes :

1. Ouvrez un terminal sur votre système Linux.

2. Utilisez la commande usermod pour ajouter l'utilisateur `alice` au groupe `sudo` :

```
sudo usermod -aG sudo alice
```

Cette ligne de commande ajoute l'utilisateur `alice` au groupe `sudo` en utilisant `usermod`. Le paramètre `-aG` signifie “ajouter à un groupe”.

Assurez-vous d'avoir les privilèges d'administrateur sur votre système pour exécuter ces commandes avec `sudo`.

Si vous avez le message `usermod : le groupe 'sudo' n'existe pas` passez à la méthode “Ajouter des droits sudoers pour un utilisateur”.

Ajouter des droits sudoers pour un utilisateur

Il s'agit de permettre à l'utilisateur courant d'utiliser la commande `sudo` en modifiant les droits d'accès dans le fichier **sudoers**.

Vous pouvez suivre également une approche qui consiste à ajouter des autorisations personnalisées dans des fichiers situés dans le répertoire `/etc/sudoers.d/` plutôt que de modifier directement le fichier principal `/etc/sudoers`, ceci afin de suivre les meilleures pratiques. Voici comment ajouter l'utilisateur `alice` à la liste des utilisateurs autorisés à utiliser `sudo` en suivant cette approche :

1. Ouvrez un terminal sur votre système Linux.

2. Créez un fichier dans le répertoire `/etc/sudoers.d/` pour l'utilisateur `alice`. Vous pouvez utiliser la commande `sudo visudo` pour éditer ce fichier spécifique avec `visudo` :

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

Si le fichier `alice` n'existe pas, il sera créé.

3. À l'intérieur de l'éditeur de texte `visudo`, ajoutez la ligne suivante au fichier `/etc/sudoers.d/alice` :

```
alice  ALL=(ALL:ALL) ALL
```

Cette ligne spécifie que l'utilisateur `alice` est autorisé à utiliser `sudo` pour toutes les commandes, avec les privilèges de tous les utilisateurs et groupes.

4. Après avoir ajouté la ligne, sauvegardez les modifications et quittez l'éditeur de texte. La commande `visudo` vérifiera la syntaxe du fichier pour s'assurer qu'il n'y a pas d'erreurs.

5. Assurez-vous que les fichiers dans `/etc/sudoers.d/` ont les bonnes autorisations. Ils doivent appartenir à `root` et avoir des permissions `440` :

```
chmod 440 /etc/sudoers.d/alice
chown root:root /etc/sudoers.d/alice
```

Ne pas demander le mot de passe

Pour permettre à un utilisateur d'exécuter des commandes `sudo` sans être invité systématiquement à entrer son mot de passe, vous pouvez configurer des règles de sudoers spécifiques pour cet utilisateur.

Il est essentiel de comprendre que cela peut introduire des problèmes de sécurité et doit être fait avec précaution. Ne désactivez pas systématiquement le mot de passe pour `sudo` sans une bonne raison, car cela peut compromettre la sécurité de votre système.

1. Ouvrez un terminal sur votre système Linux.

2. Exécutez la commande suivante pour ouvrir le fichier `/etc/sudoers` avec `visudo` (en tant qu'administrateur) :

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

Cette commande ouvre le fichier `sudoers` en mode édition sécurisé.

3. À l'intérieur de l'éditeur de texte `visudo`, ajoutez la ligne suivante en remplaçant `alice` par le nom de l'utilisateur pour lequel vous souhaitez désactiver le mot de passe pour `sudo` :

```
alice ALL=(ALL:ALL) NOPASSWD:ALL
```

Cette ligne indique que l'utilisateur `alice` peut exécuter toutes les commandes avec `sudo` sans être invité à entrer son mot de passe.

4. Après avoir ajouté la ligne, sauvegardez les modifications et quittez l'éditeur de texte. La commande `visudo` vérifiera la syntaxe du fichier pour s'assurer qu'il n'y a pas d'erreurs.

5. Pour que les modifications prennent effet, l'utilisateur `alice` devra exécuter des commandes `sudo`

sans être invité à entrer son mot de passe lors de la prochaine session.

Il est important de noter que la désactivation systématique du mot de passe pour `sudo` présente un risque de sécurité important, car cela permet à l'utilisateur de lancer des commandes avec des privilèges élevés sans vérification d'identité. Cette méthode doit être utilisée avec précaution et uniquement pour des cas spécifiques où elle est nécessaire, comme l'automatisation de certaines tâches système. Assurez-vous de comprendre les implications de cette configuration avant de l'appliquer et ne l'utilisez que lorsque c'est absolument nécessaire.