

Principes d'admin et sécurité

Bonjour .. je voudrais valider les bonnes pratiques en matière d'administration de serveur hébergé (vps ou baremetal) - Si on est 2 admins - Doit-t-on proscrire l'accès en root, même par clé rsa ?- si oui, doit-t-on avoir un compte par admin pour les logs et la traçabilité ?- dans ce cas, il y a juste sudoers, pas root .. Est-ce correcte ?

Voici les bonnes pratiques en matière d'administration de serveurs (VPS ou bare metal), surtout quand vous êtes plusieurs administrateurs :

1. Accès en root

À proscrire absolument, même par clé RSA.

- **Pourquoi ?** Même avec une clé RSA, un accès direct en root expose le serveur à des risques majeurs (erreur humaine, fuite de clé, attaque ciblée).
- **Alternative :** Utilisez toujours un compte utilisateur standard, puis `sudo` pour les commandes nécessitant des privilèges élevés.

2. Un compte par admin pour la traçabilité

Oui, chaque admin doit avoir son propre compte.

- **Pourquoi ?**
 - **Traçabilité :** Chaque action est liée à un utilisateur spécifique, ce qui facilite l'audit et la responsabilité.
 - **Sécurité :** Limite l'impact d'une compromission (une clé ou un mot de passe volé ne donne accès qu'à un seul compte).
- **Configuration :**
 - Chaque compte doit être ajouté au groupe `sudo` (ou `wheel` selon la distribution) pour pouvoir utiliser `sudo`.
 - Exemple de commande pour ajouter un utilisateur au groupe sudo :

bash

```
usermod -aG sudo nom_utilisateur
```

3. Configuration des droits sudo

Oui, les admins doivent être sudoers, pas root.

- **Fichier de configuration :** `/etc/sudoers` (à éditer avec `visudo`).
- **Exemple de ligne pour un admin :**

plaintext

```
nom_utilisateur ALL=(ALL:ALL) ALL
```

- **Bonnes pratiques :**
 - Limitez les commandes sudo si possible (principe du moindre privilège).
 - Activez les logs des commandes sudo (`/var/log/auth.log` ou `/var/log/secure` selon la distribution).

4. Autres recommandations

- **Clés SSH uniquement :** Désactivez l'authentification par mot de passe (`PasswordAuthentication no` dans `/etc/ssh/sshd_config`).
- **Mots de passe forts :** Même pour les comptes sudoers, utilisez des mots de passe robustes ou des clés SSH.
- **Mises à jour :** Maintenez le système et les outils (OpenSSH, sudo) à jour.
- **Sauvegardes :** Sauvegardez régulièrement les fichiers de configuration critiques (`/etc/sudoers`, `/etc/ssh/sshd_config`).

Résumé de votre cas

- **Accès root direct :** Non, même avec clé RSA.
- **Un compte par admin :** Oui, pour la traçabilité.
- **Sudoers uniquement :** Oui, avec configuration dans `/etc/sudoers`.

Revision #1

Created 2026-04-19 13:54:58 UTC by Nicolas Farrie

Updated 2026-04-19 13:59:21 UTC by Nicolas Farrie