

Partie 5 : Gestion des utilisateurs

A/ Configuration et utilisation de la commande sudo

Avant d'aborder la gestion des utilisateurs sous Linux, il est important de rappeler pourquoi il est **fortement déconseillé de se connecter directement avec le compte administrateur root**.

En ligne de commande, une simple erreur de frappe peut avoir des conséquences importantes, voire irréversibles, sur le système.

Linux met donc à disposition un mécanisme permettant d'exécuter ponctuellement des commandes avec des priviléges élevés **sans se connecter en tant que root**. Ce mécanisme repose sur la commande sudo.

La commande sudo autorise un utilisateur, sous réserve qu'il soit déclaré dans le fichier de configuration /etc/sudoers, à exécuter certaines commandes avec des priviléges administrateur. Chaque utilisation de sudo nécessite une **authentification par mot de passe**, garantissant ainsi une traçabilité et un meilleur contrôle des actions effectuées.

Sous Ubuntu, l'utilisateur créé lors de l'installation du système est automatiquement ajouté à un groupe disposant de priviléges élevés, ce qui lui permet d'utiliser la commande sudo par défaut.

La configuration des droits associés à sudo est définie dans le fichier /etc/sudoers.

Travail à réaliser

1. Affichez le contenu du fichier /etc/sudoers.

- o La commande sudo est-elle nécessaire pour accéder à ce fichier ?

La commande sudo sert à éléver les privilèges sur le système d'exploitation.

```
kawai@kawai-VirtualBox:~$ cat /etc/sudoers
cat: /etc/sudoers: Permission non accordée
kawai@kawai-VirtualBox:~$ █
```

- o Justifiez votre réponse.

Sans la commande sudo , l'accès est non accessible (permission non accordée)

Remarque

Si vous ne parvenez pas à afficher le contenu du fichier, cela signifie que vous ne disposez pas des droits nécessaires et qu'il faut utiliser la commande sudo.

2. Repérez dans le fichier /etc/sudoers les lignes suivantes :

Allow members of group sudo to execute any command

%sudo ALL=(ALL:ALL) ALL

3. À l'aide de recherche en ligne, expliquez la signification de ces lignes.

Allow members of group sudo to execute any command = commentaire avec le hashtag , cela indique les membres du groupe avec une élévation de privilèges.

%sudo ALL=(ALL:ALL) ALL = Tous les utilisateurs que vous ajoutez au groupe 'sudo' ont le droit d'exécuter n'importe quelle commande sur cette machine, tant qu'ils connaissent leur propre mot de passe

4. On pourra notamment retenir que :

- o les membres du groupe **sudo** disposent de **tous les privilèges** sur le système.

La question qui se pose alors est :

Êtes-vous membre du groupe sudo ? Oui je suis dans le groupe sudo

```
kawai@kawai-VirtualBox:~$ grep "sudo" /etc/group
sudo:x:27:kawai
kawai@kawai-VirtualBox:~$
```

Sous Linux, les groupes d'utilisateurs sont définis dans le fichier /etc/group.

Chaque ligne de ce fichier contient :

- le nom du groupe,
- son identifiant numérique (GID),
- et éventuellement la liste des utilisateurs appartenant à ce groupe en tant que groupe secondaire.

(Un utilisateur possède toujours un groupe principal et peut appartenir à plusieurs groupes secondaires.)

5. Recherchez votre identifiant de connexion (*login*) dans le fichier /etc/group et vérifiez qu'il appartient bien au groupe sudo.

```
kawai@kawai-VirtualBox:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,kawai
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:kawai
floppy:x:25:
tape:x:26:
sudo:x:27:kawai
```

77

- Est-il nécessaire d'utiliser la commande sudo pour afficher le contenu de ce fichier ?

Non car :

- Expliquez votre réponse.

Non, l'utilisation de sudo n'est pas nécessaire pour afficher le contenu de /etc/group , en tapant la commande : cat /etc/group on peut aussi voir le contenu.

Contrairement au fichier /etc/sudoers (vu précédemment), le fichier /etc/group est lisible par tout le monde (World Readable).

5. En vous appuyant sur votre justification à la question précédente, indiquez si l'utilisation de la commande sudo est nécessaire pour afficher le contenu du fichier : /var/log/syslog

Justifiez votre réponse.

La commande cat/var/log/syslog, doit être exécuté avec le sudo sinon ca affiche accès refusé, les privilèges sont restreint.

6. Même question pour le fichier suivant : /etc/shadow

Justifiez votre réponse.

La commande cat /etc/shadow doit être exécuter avec les privilèges (sudo)

```
kawai@kawai-VirtualBox:~$ cat /etc/shadow
cat: /etc/shadow: Permission non accordée
kawai@kawai-VirtualBox:~$ █
```

B/ Gestion des utilisateurs

Chaque utilisateur du système Linux est identifié par un **identifiant numérique unique**, appelé **UID** (*User ID*).

Par convention, l'utilisateur root possède l'UID **0**.

La création d'un compte utilisateur consiste donc à :

- déclarer un nouvel UID ;
- l'associer à un **nom d'utilisateur** (*login*), sous forme de chaîne de caractères.

Chaque utilisateur appartient obligatoirement à un **groupe primaire**, lui aussi identifié par un identifiant numérique appelé **GID** (*Group ID*).

De la même manière, la création d'un groupe correspond à la déclaration d'un nouveau GID associé à un nom de groupe.

Remarque importante

Les informations relatives aux utilisateurs et aux groupes sont stockées dans les fichiers suivants :

- /etc/passwd : informations générales sur les utilisateurs (login, UID, groupe principal, répertoire personnel, shell...);
- /etc/shadow : mots de passe chiffrés des utilisateurs (fichier protégé) ;
- /etc/group : informations concernant les groupes.

Dans le cas d'ordinateurs gérés par un serveur (annuaire, domaine...), ces informations peuvent être centralisées sur ce dernier.

Si un ordinateur personnel est destiné à être utilisé par plusieurs personnes, il est nécessaire de créer **un compte utilisateur distinct pour chaque personne**.

Travail à réaliser

- Quel est votre **UID** ? **UID = 1000**

```
kawai:x:1000:1000:Kawai:/home/kawai:/bin/bash
kawai@kawai-VirtualBox:~$
```

- Vérifiez vos informations avec la commande **id**. Correspond-elle à ce que vous avez trouvé dans le fichier /etc/passwd ?"

```
kawai@kawai-VirtualBox:~$ id
uid=1000(kawai) gid=1000(kawai) groupes=1000(kawai),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),100(users),
114(lpadmin)
kawai@kawai-VirtualBox:~$
```

La commande id ne "devine" pas ces informations. Elle va justement lire le fichier /etc/passwd (et /etc/group) pour afficher ces données de manière lisible à l'écran. C'est donc normal que les deux soient identiques.

- Quel est votre **groupe principal** ?

Mon groupe principal est le gid = 1000 (kawai)

Chaque nouvel utilisateur est créé à partir de paramètres par défaut définis dans le fichier /etc/adduser.conf.

- En vous appuyant sur votre UID actuel et sur les informations contenues dans /etc/adduser.conf, quel sera l'UID attribué par défaut au **prochain utilisateur créé** ?

```
# Default: FIRST_UID=1000, LAST_UID=59999
#FIRST_UID=1000
#LAST_UID=59999
```

Le prochain utilisateur crée sera uid = 1001

- À l'aide de la commande addgroup, créez un groupe nommé **invite**.

```
kawai@kawai-VirtualBox:~$ sudo addgroup invite
info: Choix d'un GID dans la plage 1000 à 59999 ...
info: Ajout du groupe « invite » (GID 1001)...
kawai@kawai-VirtualBox:~$
```

- Consultez le manuel de la commande adduser. (Notez la commande)

man adduser

- Créez un nouvel utilisateur nommé **user1** avec les caractéristiques suivantes :

- UID attribué par défaut ;
- groupe primaire : **invite** ;
- répertoire personnel : /home/user1 ;
- mot de passe défini sur **user1**.

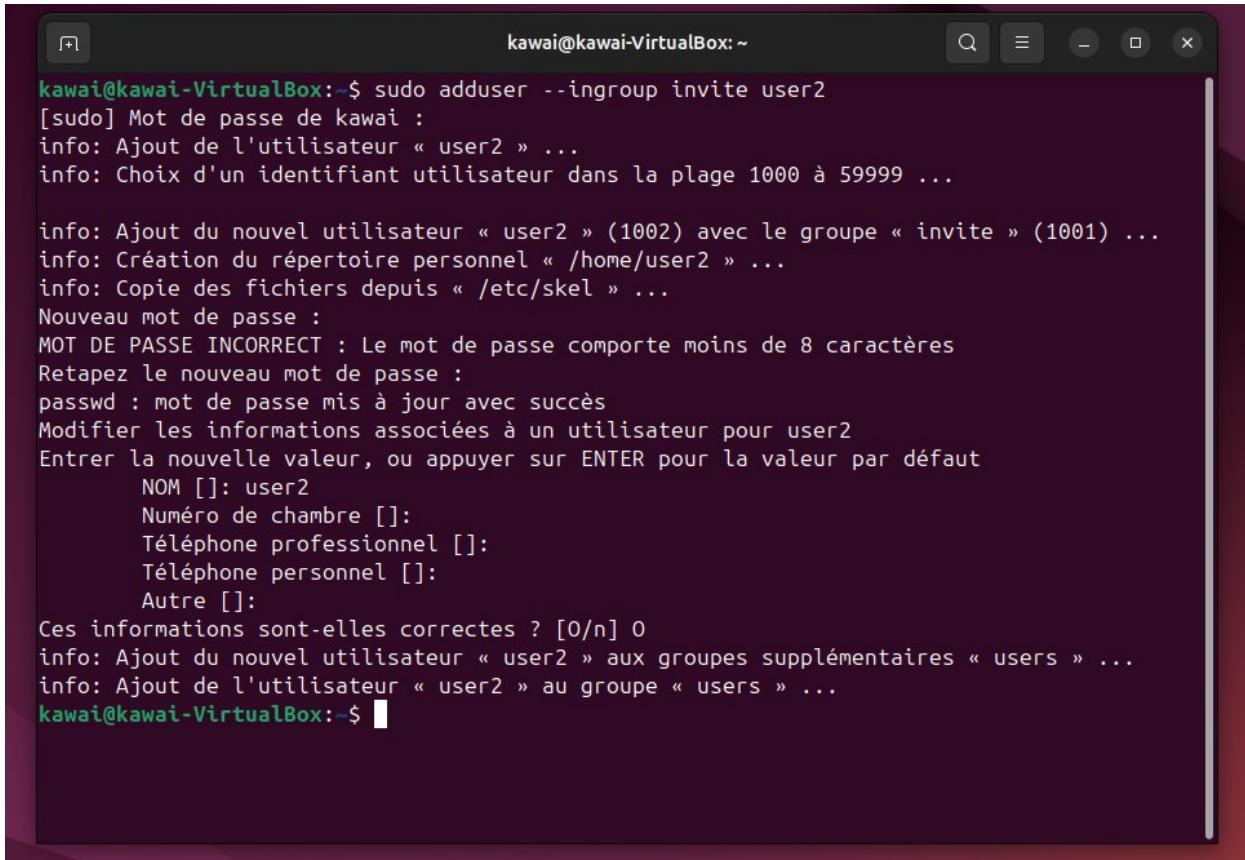
```
kawai@kawai-VirtualBox:~$ sudo adduser user1
info: Ajout de l'utilisateur « user1 » ...
info: Choix d'un UID/GID dans la plage 1000 à 59999 ...
info: Ajout du nouveau groupe « user1 » (1002) ...
info: Ajout du nouvel utilisateur « user1 » (1002) avec le groupe « user1 » (1002) ...
info: Création du répertoire personnel « /home/user1 » ...
info: Copie des fichiers depuis « /etc/skel » ...
Nouveau mot de passe :
MOT DE PASSE INCORRECT : Le mot de passe comporte moins de 8 caractères
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour user1
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
    NOM []: user1
    Numéro de chambre []:
    Téléphone professionnel []:
    Téléphone personnel []:
    Autre []:
Ces informations sont-elles correctes ? [0/n] 0
info: Ajout du nouvel utilisateur « user1 » aux groupes supplémentaires « users » ...
info: Ajout de l'utilisateur « user1 » au groupe « users » ...
kawai@kawai-VirtualBox:~$
```

```
kawai@kawai-VirtualBox:~$ sudo adduser --ingroup invite user1
info: Ajout de l'utilisateur « user1 » ...
info: Choix d'un identifiant utilisateur dans la plage 1000 à 59999 ...

info: Ajout du nouvel utilisateur « user1 » (1001) avec le groupe « invite » (1001) ...
warn: Le répertoire personnel « /home/user1 » existe déjà. Pas de modification de ce répertoire.
warn: Attention : le répertoire personnel « /home/user1 » n'appartient pas à l'utilisateur que vous êtes en train de créer.
Nouveau mot de passe :
MOT DE PASSE INCORRECT : Le mot de passe comporte moins de 8 caractères
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour user1
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
    NOM []: user1
    Numéro de chambre []:
    Téléphone professionnel []:
    Téléphone personnel []:
    Autre []:
Ces informations sont-elles correctes ? [0/n] 0
info: Ajout du nouvel utilisateur « user1 » aux groupes supplémentaires « users » ...
info: Ajout de l'utilisateur « user1 » au groupe « users » ...
kawai@kawai-VirtualBox:~$
```

8. Créez un nouvel utilisateur nommé **user2** avec les caractéristiques suivantes :

- UID attribué par défaut ;
- groupe primaire : **invite** ;
- répertoire personnel : /home/user2 ;
- mot de passe défini sur **user2**.



```
kawai@kawai-VirtualBox:~$ sudo adduser --ingroup invite user2
[sudo] Mot de passe de kawai :
info: Ajout de l'utilisateur « user2 » ...
info: Choix d'un identifiant utilisateur dans la plage 1000 à 59999 ...

info: Ajout du nouvel utilisateur « user2 » (1002) avec le groupe « invite » (1001) ...
info: Création du répertoire personnel « /home/user2 » ...
info: Copie des fichiers depuis « /etc/skel » ...

Nouveau mot de passe :
MOT DE PASSE INCORRECT : Le mot de passe comporte moins de 8 caractères
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour user2
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
    NOM []: user2
    Numéro de chambre []:
    Téléphone professionnel []:
    Téléphone personnel []:
    Autre []

Ces informations sont-elles correctes ? [0/n] 0
info: Ajout du nouvel utilisateur « user2 » aux groupes supplémentaires « users » ...
info: Ajout de l'utilisateur « user2 » au groupe « users » ...
kawai@kawai-VirtualBox:~$
```

C/ Consoles en mode texte et console graphique

En plus de la session graphique utilisée habituellement, Linux démarre par défaut **plusieurs consoles en mode texte** (généralement 6).

Ces consoles permettent de se connecter au système sans interface graphique, ce qui est particulièrement utile pour l'administration de serveurs.

Les combinaisons suivantes permettent de changer de console :

- **CTRL + ALT + F1 ou F2 : console graphique.**
- **CTRL + ALT + F3 à CTRL + ALT + F6 : consoles texte :**

Lorsqu'un utilisateur se connecte sur une console texte puis bascule vers une autre console ou vers l'interface graphique, la session reste **ouverte en arrière-plan**.

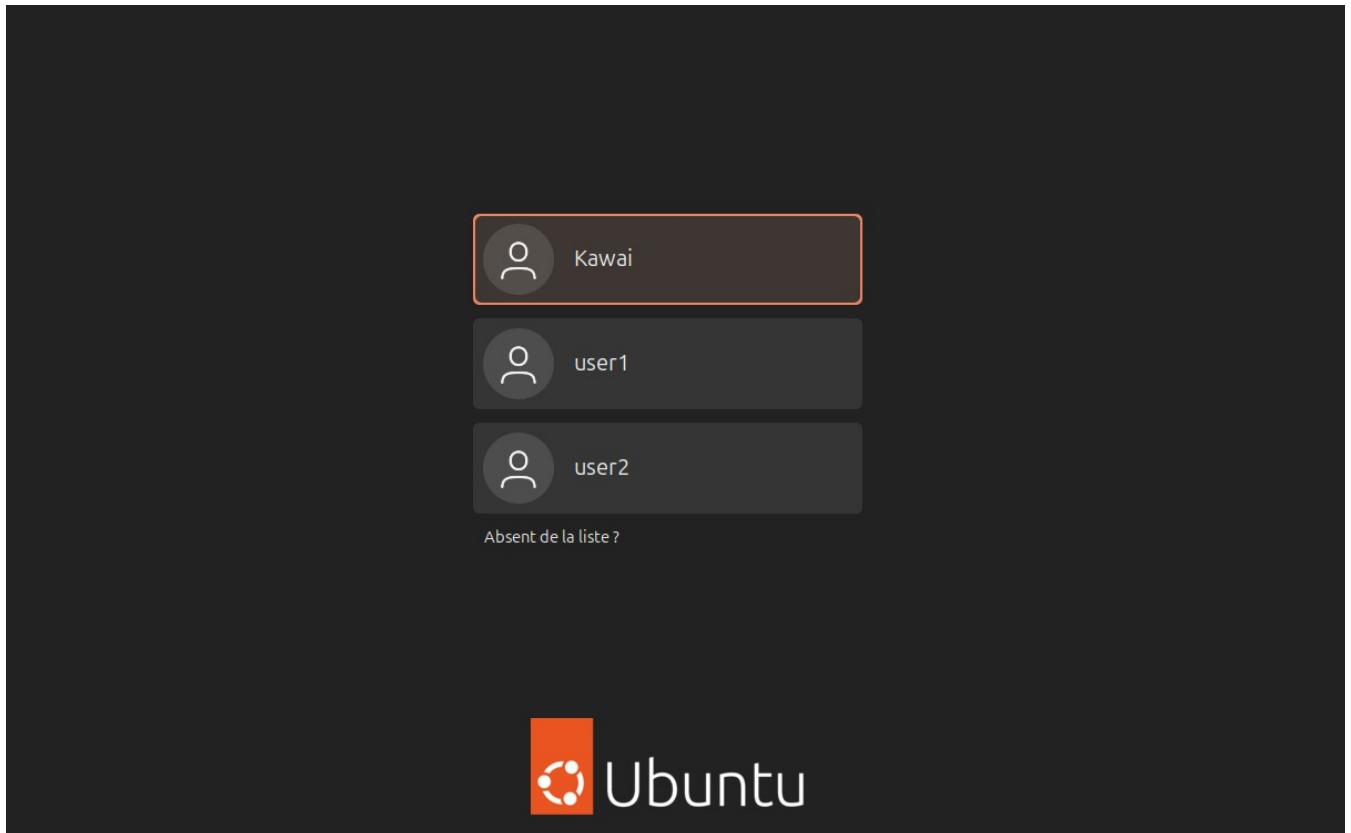
Il est donc important de penser à se déconnecter afin d'éviter de laisser une session active.

Pour se déconnecter :

- taper exit
- ou utiliser CTRL + D.

Travail à réaliser

1. Accédez à une console de connexion en mode texte en appuyant sur CTRL + ALT + F1.



2. Connectez-vous avec le login et le mot de passe de **user1**, puis vérifiez que son répertoire personnel est bien :
3. /home/user1

A screenshot of a terminal window titled "Terminal". The window is dark-themed. The terminal output shows the user "user1" attempting to access their home directory. The first command, "bash: /home/user1/.bashrc: Permission non accordée", indicates a permission denied error for the .bashrc file. The subsequent commands, "getent passwd user1" and "ls -la ~", show the user information and the contents of the user's home directory, which is empty. The terminal window has a standard title bar with icons for minimize, maximize, and close.

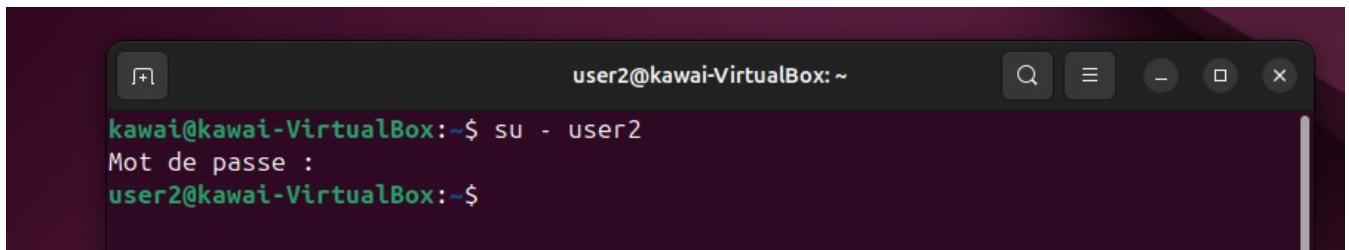
- Déconnectez-vous (exit ou CTRL + D) avant de revenir à la console graphique (CTRL + ALT + F7).

D/ Changement d'utilisateur avec la commande su

La commande su permet à un utilisateur de se connecter, dans un terminal, sous l'identité d'un autre utilisateur afin d'exécuter des commandes shell.

Dans un terminal, tapez la commande suivante :

su - user2



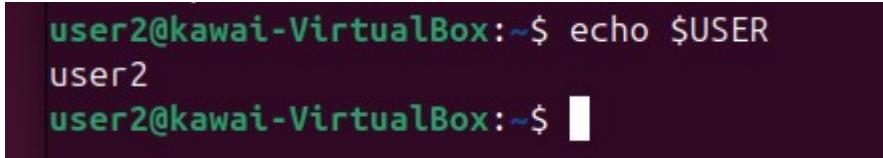
A screenshot of a terminal window titled "user2@kawai-VirtualBox: ~". The window shows the command "su - user2" being entered, followed by a password prompt "Mot de passe :". The prompt ends with a dollar sign, indicating successful login as user2.

```
user2@kawai-VirtualBox:~$ su - user2
Mot de passe :
user2@kawai-VirtualBox:~$
```

Observez le changement du prompt indiquant que l'utilisateur **user2** est maintenant connecté.

Vérifiez également l'utilisateur courant avec la commande :

echo \$USER



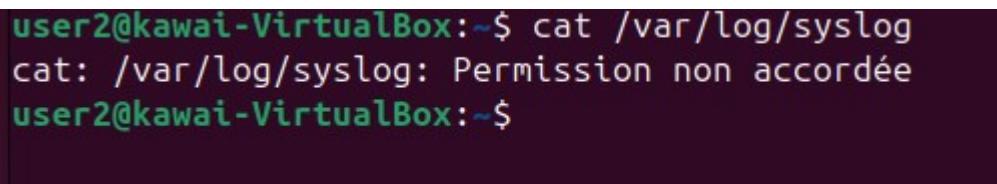
A screenshot of a terminal window showing the command "echo \$USER" being run. The output is "user2", indicating the current user is user2.

```
user2@kawai-VirtualBox:~$ echo $USER
user2
user2@kawai-VirtualBox:~$
```

Travail à réaliser

- Tentez d'afficher le contenu du fichier /var/log/syslog **avec et sans** la commande sudo.
Que constatez-vous ?

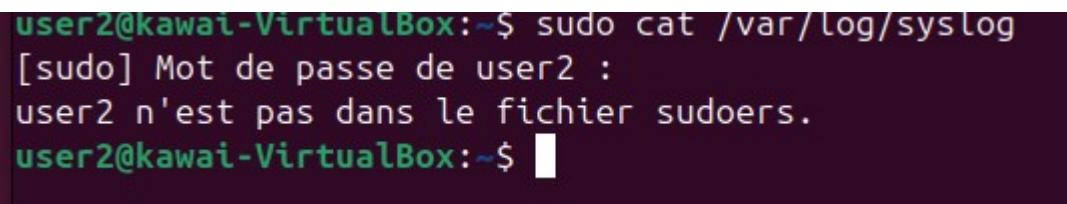
SANS SUDO



A screenshot of a terminal window showing the command "cat /var/log/syslog" being run. The output is "cat: /var/log/syslog: Permission non accordée", indicating permission was denied.

```
user2@kawai-VirtualBox:~$ cat /var/log/syslog
cat: /var/log/syslog: Permission non accordée
user2@kawai-VirtualBox:~$
```

AVEC SUDO



A screenshot of a terminal window showing the command "sudo cat /var/log/syslog" being run. It prompts for a password for user2, then displays the message "user2 n'est pas dans le fichier sudoers.", indicating user2 is not listed in the sudoers file.

```
user2@kawai-VirtualBox:~$ sudo cat /var/log/syslog
[sudo] Mot de passe de user2 :
user2 n'est pas dans le fichier sudoers.
user2@kawai-VirtualBox:~$
```

Afin d'augmenter les priviléges de l'utilisateur **user2**, nous allons l'ajouter à un groupe secondaire.

- Déconnectez-vous de l'utilisateur user2, puis exécutez la commande suivante :

sudo adduser user2 adm

```
kawai@kawai-VirtualBox:~$ sudo adduser user2 adm
[sudo] Mot de passe de kawai :
info: Ajout de l'utilisateur « user2 » au groupe « adm » ...
kawai@kawai-VirtualBox:~$ su - user2
Mot de passe :
user2@kawai-VirtualBox:~$ id
uid=1002(user2) gid=1001(invite) groupes=1001(invite),4(adm),100(users)
user2@kawai-VirtualBox:~$
```

3. Reconnectez-vous avec l'utilisateur user2 à l'aide de la commande su, puis tentez à nouveau d'afficher le contenu du fichier /var/log/syslog **avec** et **sans** sudo.

Commentez les résultats observés.

SANS SUDO

```
user2@kawai-VirtualBox:~$ cat /var/log/syslog
```

```
emoting known real-time threads.
2026-02-02T14:47:05.917612+01:00 kawai-VirtualBox rtkit-daemon[1220]: S
uccessfully demoted thread 1977 of process 1950.
2026-02-02T14:47:05.917715+01:00 kawai-VirtualBox rtkit-daemon[1220]: S
uccessfully demoted thread 1743 of process 1715.
2026-02-02T14:47:05.917782+01:00 kawai-VirtualBox rtkit-daemon[1220]: S
uccessfully demoted thread 1759 of process 1724.
2026-02-02T14:47:05.917849+01:00 kawai-VirtualBox rtkit-daemon[1220]: S
uccessfully demoted thread 1724 of process 1724.
2026-02-02T14:47:05.917915+01:00 kawai-VirtualBox rtkit-daemon[1220]: S
uccessfully demoted thread 1747 of process 1707.
2026-02-02T14:47:05.917980+01:00 kawai-VirtualBox rtkit-daemon[1220]: S
uccessfully demoted thread 1707 of process 1707.
2026-02-02T14:47:05.918163+01:00 kawai-VirtualBox rtkit-daemon[1220]: S
uccessfully demoted thread 1736 of process 1723.
2026-02-02T14:47:05.918717+01:00 kawai-VirtualBox rtkit-daemon[1220]: S
uccessfully demoted thread 1723 of process 1723.
2026-02-02T14:47:05.918783+01:00 kawai-VirtualBox rtkit-daemon[1220]: D
emoted 8 threads.
2026-02-02T14:48:38.668979+01:00 kawai-VirtualBox PackageKit: daemon qu
it
2026-02-02T14:48:38.678739+01:00 kawai-VirtualBox systemd[1]: packageki
```

Réponse : Le contenu du fichier /var/log/syslog s'affiche sans erreur.

AVEC SUDO :

```
user2@kawai-VirtualBox:~$ sudo cat /var/log/syslog
[sudo] Mot de passe de user2 :
user2 n'est pas dans le fichier sudoers.
user2@kawai-VirtualBox:~$
```

Avec le sudo le résultat affiche : user2 n'est pas dans le fichier sudoers. La commande ne marche pas.

4. Proposez une solution sans la mettre en exécution.

Afin que l'utilisateur 2 possède les permissions maximales , il faudrait ajouter l'utilisateur 2 dans le groupe sudo.

La commande serait : add user2 --ingroup sudo

5. Déconnectez-vous de l'utilisateur user2.

```
user2@kawai-VirtualBox:~$ exit  
déconnexion  
kawai@kawai-VirtualBox:~$ █
```

E/ Synthèse et rédaction du rapport (Bilan)

Pour conclure ce TP, vous devez rédiger un compte-rendu structuré résumant vos manipulations et vos observations. Votre rapport devra impérativement répondre aux points suivants en utilisant un vocabulaire technique précis :

1. La sécurité des privilèges

- Expliquez la différence fondamentale entre l'utilisateur **root** et l'usage de la commande **sudo**.

Root contre Sudo : La différence fondamentale réside dans la portée des droits. L'utilisateur root est le super-utilisateur : il a un accès total et permanent au système. À l'inverse, la commande sudo permet à un utilisateur standard d'obtenir une élévation de privilèges temporaire, uniquement pour l'exécution d'une commande précise, avant de redevenir un utilisateur normal.

- Pourquoi est-il plus sûr d'utiliser sudo plutôt que de rester connecté en permanence en tant que root ? (Pensez à la notion de "traçabilité" et de "limitation des erreurs").

La traçabilité : Contrairement à une connexion directe en root (où l'on ne sait pas qui agit si le mot de passe est partagé), chaque commande lancée via sudo est enregistrée dans les journaux (logs). On sait donc quel utilisateur a lancé quelle commande.

La limitation des erreurs : Rester connecté en root augmente le risque de supprimer des fichiers système par erreur. Avec sudo, l'utilisateur doit réfléchir et taper son mot de passe pour valider une action administrative, ce qui limite les "fausses manipulations". Comme par exemple : avec la commande rm sans l'élévation (sudo) des privilèges , on évite de supprimer des fichiers systèmes sans faire exprès ou sans la connaissance de la commande.

2. L'organisation du système

- Dressez un schéma ou un tableau récapitulant les 3 fichiers de configuration principaux que vous avez étudiés (/etc/passwd, /etc/shadow, /etc/group).
- Pour chaque fichier, précisez son rôle et indiquez s'il est accessible en lecture à un utilisateur "standard".

Fichiers	Leur Rôle	Accessible en lecture (utilisateur standard) ?
/etc/passwd	Contient la liste des utilisateurs, leur UID, GID, répertoire personnel et shell.	OUI
/etc/shadow	Contient les mots de passe chiffrés et les infos d'expiration des comptes.	NON (Réservé à root)
/etc/group	Définit les groupes présents sur le système et leurs membres.	OUI

3. Gestion des droits : le cas pratique

- Reprenez l'exemple de l'utilisateur user2 et du fichier /var/log/syslog.
- Expliquez pourquoi, au début, user2 ne pouvait pas lire ce fichier, et comment l'ajout au groupe adm a résolu le problème sans pour autant donner les pleins pouvoirs (droits sudo) à l'utilisateur.

1-Le fichier **/var/log/syslog** appartient au groupe **adm**. Les permissions sont réglées pour que seuls le propriétaire et le groupe puissent le lire. Comme **user2** n'était pas membre du groupe **adm**, l'accès lui était refusé.

2-J'ai ajouté **user2** au groupe **adm**. Cela a suffit pour lui donner l'accès en lecture au fichier. C'est plus sécurisé que de lui donner les droits **sudo**, car cela lui permet de consulter les logs sans pour autant devenir administrateur de toute la machine.

- Ajoutez une capture d'écran de la commande id user2

```
kawai@kawai-VirtualBox:~$ id user2
uid=1002(user2) gid=1001(invite) groupes=1001(invite),100(users)
kawai@kawai-VirtualBox:~$
```

4. Conclusion personnelle

- Quelle est, selon vous, la règle d'or à retenir lors de la création d'un nouvel utilisateur sur un serveur en production ?

Pour conclure, la règle d'or à retenir en entreprise ou en production est le principe du moindre privilège. Lorsqu'on crée un compte, on ne doit jamais donner les droits d'administration par défaut. Il faut accorder à l'utilisateur uniquement les permissions strictement nécessaires à son travail (via des groupes spécifiques) pour limiter la surface d'attaque et protéger l'intégrité du serveur.

