Ruben Battocchio
22/01/2026

---

# TP: Scénario

---



## I. Introduction

L'entreprise Xacorp, leader dans l'innovation technologique, déploie un nouveau serveur de gestion pour son département "Recherche & Développement". Dans le cadre du projet TP21 Linux, vous jouez le rôle de l'administrateur système chargé de configurer cet environnement de zéro. L'objectif est de structurer les accès pour l'équipe technique tout en garantissant la confidentialité des données sensibles.

## II. Prise de controle et initialisation

La mission commence par une élévation de privilèges. Conformément aux consignes de sécurité de Xacorp, l'administrateur doit passer en mode super-utilisateur avec la commande `su` en utilisant le mot de passe "btssio". Pour s'assurer qu'aucune erreur d'identité ne compromette la suite des opérations, la commande `whoami` est lancée pour confirmer le statut "root". Une fois cette vérification faite, l'administrateur se déplace dans le répertoire `/home` pour préparer l'arborescence de travail.

```
user@linux-vm:~$ su -
Mot de passe : btssio
root@linux-vm:~# whoami
root
root@linux-vm:~# cd /home
```

# III. Gestion de l'arborescence

Le cœur de l'infrastructure Xacorp repose sur un dossier central nommé `xacorp`, créé via la commande `mkdir`. Après avoir vérifié sa création avec `ls`, l'administrateur pénètre dans ce dossier pour y générer le fichier de configuration stratégique : `plans_secrets`. Ce fichier est édité avec l'outil `vi` pour y inscrire les directives du projet. Pour confirmer l'intégrité des données saisies, le contenu est relu immédiatement grâce à la commande `cat`. Enfin, une commande `pwd` permet de valider le chemin absolu avant de passer à la gestion des utilisateurs.

```
root@linux-vm:/home# mkdir xacorp
root@linux-vm:/home# ls
alice  bob  user  xacorp
root@linux-vm:/home# cd xacorp
root@linux-vm:/home/xacorp# pwd
/home/xacorp
root@linux-vm:/home/xacorp# vi plans_secrets
# [Dans vi : Appuyer sur 'i', taper "CONFIDENTIEL : Moteur X1", puis ':wq']
root@linux-vm:/home/xacorp# cat plans_secrets
CONFIDENTIEL : Moteur X1
```

# IV. Administration des utilisateurs et des groupes

La sécurité de Xacorp repose sur une séparation stricte des rôles. Deux comptes sont créés pour les ingénieurs principaux, `Alice` et `Bob`, via la commande `useradd`. Leurs identités sont immédiatement vérifiées dans les fichiers systèmes `shadow` ou `passwd` à l'aide de filtres `grep`. Pour permettre une collaboration efficace, un groupe de travail nommé `ingenieurs` est généré avec `groupadd`. Alice et Bob y sont ensuite rattachés par la commande `usermod`. Chaque utilisateur se voit attribuer un mot de passe sécurisé avec `passwd` pour finaliser la création de leurs sessions respectives.

```
root@linux-vm:/home/xacorp# useradd Alice
root@linux-vm:/home/xacorp# useradd Bob
root@linux-vm:/home/xacorp# passwd Alice
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: le mot de passe a été mis à jour avec succès
root@linux-vm:/home/xacorp# grep Alice /etc/passwd
Alice:x:1001:1001::/home/Alice:/bin/bash
root@linux-vm:/home/xacorp# groupadd ingenieurs
root@linux-vm:/home/xacorp# usermod -g ingenieurs Alice
root@linux-vm:/home/xacorp# usermod -g ingenieurs Bob
```

# V. Sécurisation et test des accés

La dernière étape cruciale consiste à verrouiller l'accès aux plans de Xacorp. L'administrateur modifie le groupe propriétaire du fichier `plans_secrets` pour l'attribuer aux `ingenieurs` avec la commande `chgrp`. Les permissions sont ensuite finement réglées avec `chmod 771` : cela permet au propriétaire (root) et aux membres du groupe (Alice et Bob) de lire, écrire et exécuter le fichier, tandis que les autres utilisateurs n'ont qu'un droit d'exécution très limité. Une vérification finale via `ls -l` confirme que les bits de protection sont correctement appliqués. Le scénario s'achève par un test de session réelle : l'administrateur simule une connexion en tant qu'Alice (`su Alice`) pour vérifier qu'elle peut effectivement travailler sur les fichiers de Xacorp.

```
root@linux-vm:/home/xacorp# chgrp ingenieurs plans_secrets
root@linux-vm:/home/xacorp# chmod 771 plans_secrets
root@linux-vm:/home/xacorp# ls -l plans_secrets
-rwxrwx--x 1 root ingenieurs 24 Jan 29 14:30 plans_secrets
root@linux-vm:/home/xacorp# su Alice
Alice@linux-vm:/home/xacorp$ whoami
Alice
Alice@linux-vm:/home/xacorp$ cat plans_secrets
CONFIDENTIEL : Moteur X1
```

```
/home/
├── Alice/
├── Bob/
└── xacorp/
    └── plans_secrets
```