

TP1- Gestion des Utilisateurs

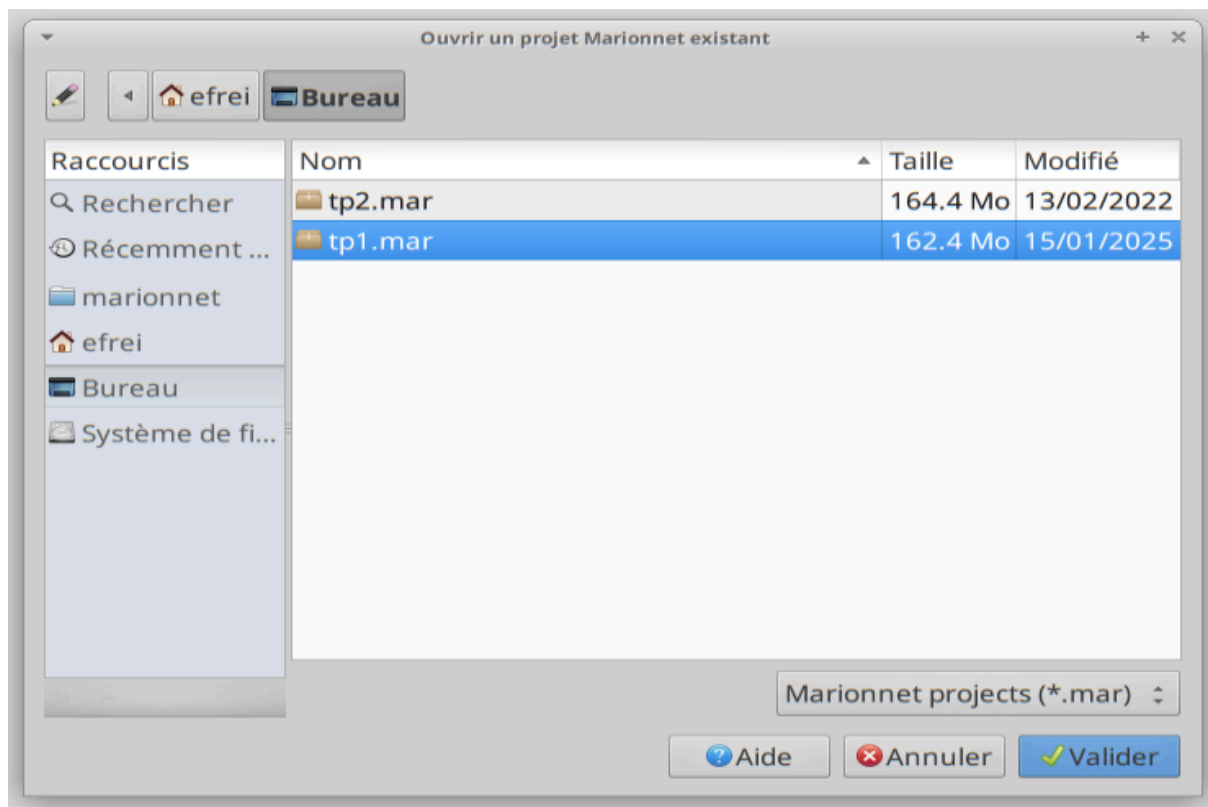
1. Préparation de l'Environnement

Avant de commencer, il faut s'assurer que Marionnet est installé sur notre machine. Marionnet est un émulateur de réseaux virtuels, souvent utilisé dans les environnements éducatifs pour simuler des réseaux Linux.

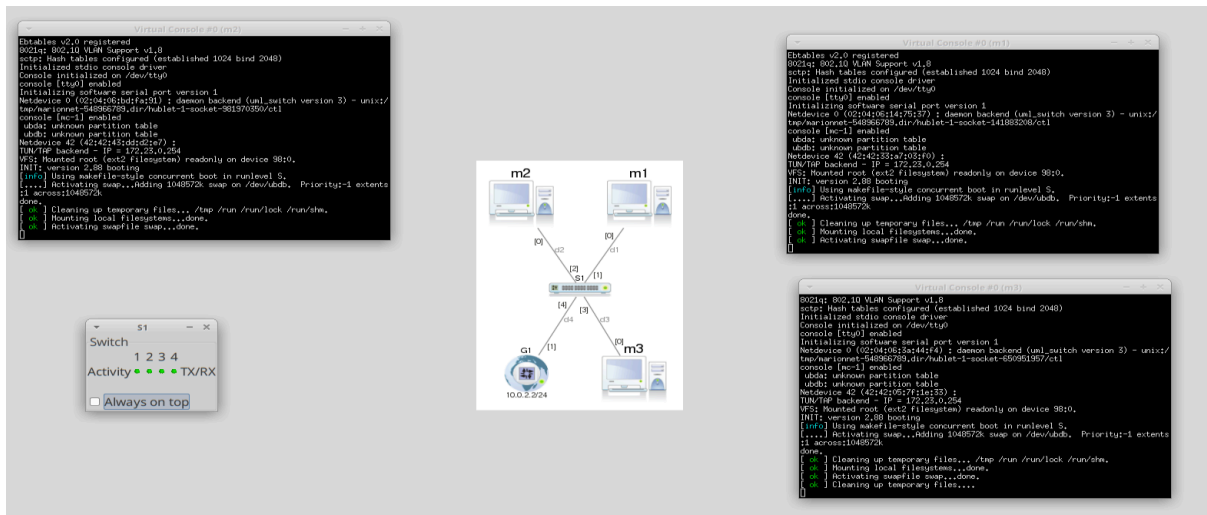
2. Mise en Place du TP

Ouvrir Marionnet et Charger le Projet :

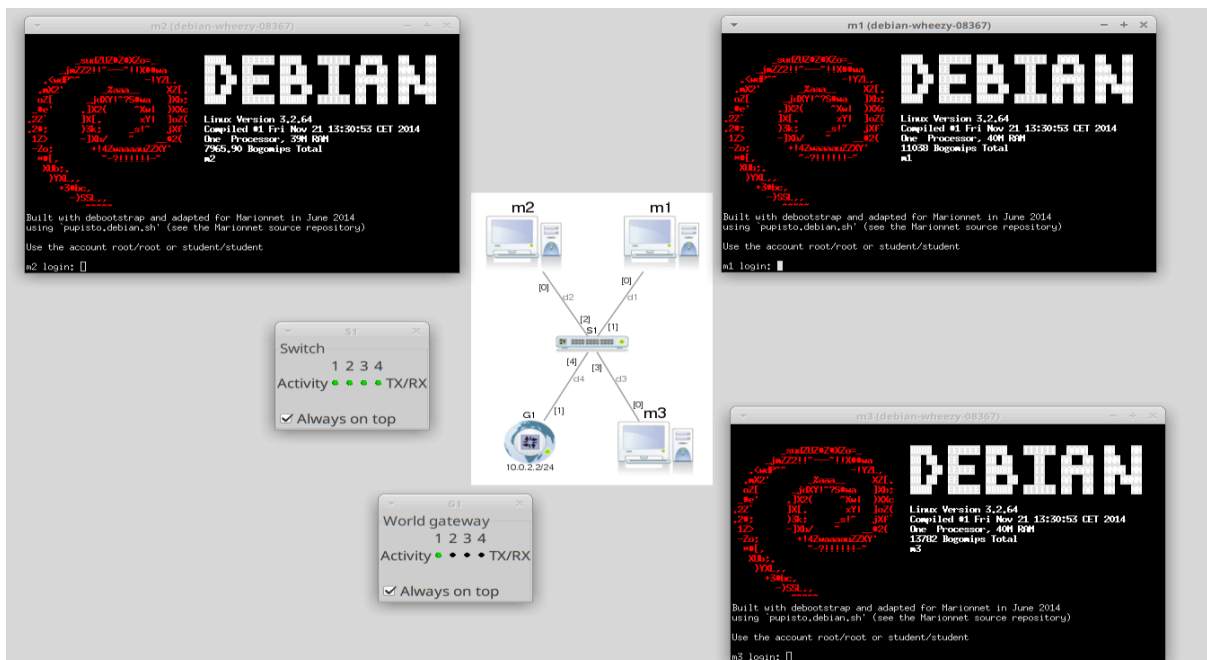
```
marionnet
```



1. Une fois Marionnet ouvert, on charge le fichier **tp1.mar** depuis le bureau.
2. **Démarrer tous les éléments du LAN** : Dans Marionnet, on sélectionne chaque équipement (m1, m2, m3) et on clique sur **Démarrer**.



On attend que toutes les machines soient ouvertes comme suit:



3. Étude de la Gestion des Utilisateurs sur l'Équipement m1

a) Lister les Utilisateurs

On va se connecter à l'équipement **m1** pour analyser les utilisateurs existants.

1. **Se connecter à m1 via Marionnet** : On double clique sur **m1** dans l'interface Marionnet pour ouvrir un terminal.

Lister les utilisateurs avec un **uid** supérieur à 999 :

```
awk -F: '$3 > 999 {print $1, $3, $4, $5, $6, $7}' /etc/passwd
```

2. Cela nous donnera :

- Le **nom de connexion** (login)
- Le **UID** (User ID)
- Le **GID** (Group ID principal)
- Le **répertoire personnel**
- L'**interpréteur de commande** (shell)

```
[0 root@m1 ~]$ awk -F: '$3 > 999 {print $1, $3, $4, $5, $6, $7}' /etc/passwd
nobody 65534 65534 nobody nobody /nonexistent /bin/sh
student 1001 1001 Student,,, Student,,, /home/student /bin/bash
tata 2001 2000 utilisateur1,b1,01 71 72 73 74,01 10 11 12 13 14, utilisateur1,b1,01 71 72 73 74,01
10 11 12 13 14, /home/utilisateurs/tata /bin/bash
tete 2002 2000 utilisateur2,b2,01 71 72 73 74,01 20 21 22 23 24, utilisateur2,b2,01 71 72 73 74,01
20 21 22 23 24, /home/utilisateurs/tete /bin/bash
titi 2003 2000 utilisateur3,b3,01 71 72 73 74,01 30 31 32 33 34, utilisateur3,b3,01 71 72 73 74,01
30 31 32 33 34, /home/utilisateurs/titi /bin/false
toto 2004 2000 utilisateur4,b4,01 71 72 73 74,01 40 41 42 43 44, utilisateur4,b4,01 71 72 73 74,01
40 41 42 43 44, /home/utilisateurs/toto /bin/bash
tutu 2005 2000 utilisateur5,b5,01 71 72 73 74,01 50 51 52 53 54, utilisateur5,b5,01 71 72 73 74,01
50 51 52 53 54, /home/utilisateurs/tutu /bin/bash
```

Résultat :

Login	tata	tete	titi	toto	tutu
UID	UID : 2001	2002	2003	2004	2005
GID	GID : 2000	2000	2000	2000	2000
Répertoire Personnel	/home/utilisat eurs/tata	/home/utilisat eurs/tete	/home/utilisat eurs/titi	/home/utilisat eurs/toto	/home/utilisat eurs/tutu
Shell	/bin/bash	/bin/bash	/bin/false (pas de session interactive)	/bin/bash	/bin/bash

b) Vérifier les Groupes Secondaires :

Pour chaque utilisateur, on peut vérifier les groupes secondaires :

```
groups <login>
```

```
[0 root@m1 ~]$ groups toto
toto : utilisateurs
[0 root@m1 ~]$ groups tutu
tutu : utilisateurs
[0 root@m1 ~]$ groups titi
titi : utilisateurs
[0 root@m1 ~]$ groups tete
tete : utilisateurs
[0 root@m1 ~]$ groups tata
tata : utilisateurs
```

On remarque que tous les utilisateurs sont dans le groupe utilisateurs.

c) Informations Complètes sur les Utilisateurs :

Les informations comme le nom complet, le numéro de bureau et le téléphone sont dans le fichier `/etc/passwd` et `/etc/gshadow`. On peut vérifier avec :

```
getent passwd <login>
chage -l <login>
```

```
[0 root@m1 ~]$ getent passwd tata
tata:x:2001:2000:utilisateur1,b1,01 71 72 73 74,01 10 11 12 13 14,:/home/utilisateurs/tata:/bin/bash
[0 root@m1 ~]$ getent passwd tete
tete:x:2002:2000:utilisateur2,b2,01 71 72 73 74,01 20 21 22 23 24,:/home/utilisateurs/tete:/bin/bash
[0 root@m1 ~]$ getent passwd titi
titi:x:2003:2000:utilisateur3,b3,01 71 72 73 74,01 30 31 32 33 34,:/home/utilisateurs/titi:/bin/false
[0 root@m1 ~]$ getent passwd toto
toto:x:2004:2000:utilisateur4,b4,01 71 72 73 74,01 40 41 42 43 44,:/home/utilisateurs/toto:/bin/bash
[0 root@m1 ~]$ getent passwd tutu
tutu:x:2005:2000:utilisateur5,b5,01 71 72 73 74,01 50 51 52 53 54,:/home/utilisateurs/tutu:/bin/bash
[0 root@m1 ~]$
```

```
[0 root@m1 ~]$ chage -l tata
Last password change           : May 12, 2011
Password expires                : never
Password inactive               : never
Account expires                 : never
Minimum number of days between password change : -1
Maximum number of days between password change : -1
Number of days of warning before password expires : -1
[0 root@m1 ~]$
```

d) Test de Connexion :

On peut simuler une connexion en utilisant :

```
su - <login>
```

```
[0 root@m1 ~]$ su - tata
tata@m1:~$
```

```
[0 root@m1 ~]$ su - tete
tete@m1:~$ exit
logout
[0 root@m1 ~]$ su - titi
[1 root@m1 ~]$ ls
total 0
[0 root@m1 ~]$ su - toto
No directory, logging in with HOME=/
toto@m1:/$ exit
logout
[0 root@m1 ~]$ su - tutu
No directory, logging in with HOME=/
tutu@m1:/$ exit
logout
```

Résultat :

- **tata** : Connexion réussie, répertoire personnel accessible, tout est normal.
- **tete** : Connexion réussie, répertoire personnel présent, aucun problème.
- **titi** : Retour immédiat sans session interactive, shell configuré sur `/bin/false`, comportement attendu.
- **toto** : Connexion avec message "No directory, logging in with HOME=/", répertoire personnel manquant ou inaccessible, nécessite correction.
- **tutu** : Même message que toto, répertoire personnel absent ou permissions incorrectes, à corriger.

4. Mise en Place de la Gestion des Utilisateurs sur m2

a) Créer les Groupes :

```
sudo groupadd -g 1600 administration
sudo groupadd -g 1700 recherche
sudo groupadd -g 1800 production
```

```
[0 root@m2 ~]$ sudo groupadd -g 1600 administration
[0 root@m2 ~]$ sudo groupadd -g 1700 recherche
[0 root@m2 ~]$ sudo groupadd -g 1800 production
```

b) Créer les Répertoires :

```
sudo mkdir -p /home/xl_networks/administration
sudo mkdir -p /home/xl_networks/recherche
sudo mkdir -p /home/xl_networks/production
sudo mkdir -p /home/users
```

```
[0 root@m2 ~]$ sudo mkdir -p /home/xl_networks/administration
[0 root@m2 ~]$ sudo mkdir -p /home/xl_networks/recherche
[0 root@m2 ~]$ sudo mkdir -p /home/xl_networks/production
[0 root@m2 ~]$ sudo mkdir -p /home/users
```

c) Ajouter les Utilisateurs :

Service Administration :

```
sudo useradd -u 1601 -g 1600 -d /home/users/zetaufrait -m -s /bin/bash -c
"ZETAUFRAIT Mélanie - Bureau 1601 - 01 69 33 61 00" mzetaufrait
echo "mzetaufrait:melanie" | sudo chpasswd
```

```
[0 root@m2 ~]$ sudo useradd -u 1601 -d /home/users/zetaufrait -m -s /bin/bash -c "ZETAUFRAIT Melanie - Bureau 1601 - 01 69 33 61 00" mzetaufrait
```

```
sudo useradd -u 1602 -g 1600 -d /home/users/terrieur -m -s /bin/bash -c "TERRIEUR Alex - Bureau 1602 - 01 69 33 61 00" aterrieur  
echo "aterrieur:alex" | sudo chpasswd  
  
sudo useradd -u 1603 -g 1600 -d /home/users/bon -m -s /bin/bash -c "BON Jean - Bureau 1603 - 01 69 33 61 00" jbon  
echo "jbon:jean" | sudo chpasswd
```

Service Recherche :

```
sudo useradd -u 1701 -g 1700 -d /home/users/assin -m -s /bin/bash -c "ASSIN Marc - Bureau 1701 - 01 69 33 61 00" massin  
echo "massin:marc" | sudo chpasswd  
  
sudo useradd -u 1702 -g 1700 -d /home/users/eparbal -m -s /bin/bash -c "EPARBAL Gilles - Bureau 1702 - 01 69 33 61 00" geparbal  
echo "geparbal:gilles" | sudo chpasswd
```

Service Production :

```
sudo useradd -u 1801 -g 1800 -d /home/users/menvussa -m -s /bin/bash -c "MENVUSSA Gérard - Bureau 1801 - 01 69 33 61 00" gmenvussa  
echo "gmenvussa:gerard" | sudo chpasswd  
  
sudo useradd -u 1802 -g 1800 -d /home/users/liguili -m -s /bin/bash -c "LIGUILI Guy - Bureau 1802 - 01 69 33 61 00" gliguili  
echo "gliguili:guy" | sudo chpasswd
```

d) Configurer les Permissions :

Pour le dossier "administration" :

```
sudo chown jbon:administration /home/xl_networks/administration  
sudo chmod 770 /home/xl_networks/administration  
sudo setfacl -m u:mzetaufrait:rx /home/xl_networks/administration  
sudo setfacl -m u:aterrieur:rx /home/xl_networks/administration
```

```
[0 root@m2 ~]$ sudo chown jbon:administration /home/xl_networks/administration  
[0 root@m2 ~]$ sudo chmod 770 /home/xl_networks/administration  
[0 root@m2 ~]$ sudo setfacl -m u:mzetaufrait:rx /home/xl_networks/administration  
[0 root@m2 ~]$ sudo setfacl -m u:aterrieur:rx /home/xl_networks/administration
```

Jean BON est devenu propriétaire du dossier **administration**.

Il a tous les droits sur ce dossier (lecture, écriture, exécution).

Mélanie ZETAUFRAIT et **Alex TERRIEUR** peuvent lire et exécuter le contenu du dossier, mais ne peuvent pas le modifier.

Tous les autres utilisateurs n'ont aucun accès à ce dossier.

Pour le dossier "production" :

```
sudo chown gmenvussa:production /home/xl_networks/production
sudo chmod 770 /home/xl_networks/production

sudo setfacl -m u:gliguili:rwX /home/xl_networks/production
sudo setfacl -m u:jbon:r /home/xl_networks/production
sudo setfacl -m u:mzetaufrait:r /home/xl_networks/production
sudo setfacl -m u:aterrieur:r /home/xl_networks/production
sudo setfacl -m u:massin:r /home/xl_networks/production
sudo setfacl -m u:geparbal:r /home/xl_networks/production
```

```
[0 root@m2 ~]$ sudo chown gmenvussa:production /home/xl_networks/production
[0 root@m2 ~]$ sudo chmod 770 /home/xl_networks/production
[0 root@m2 ~]$ sudo setfacl -m u:gliguili:rwX /home/xl_networks/production
[0 root@m2 ~]$ sudo setfacl -m u:jbon:r /home/xl_networks/production
[0 root@m2 ~]$ sudo setfacl -m u:mzetaufrait:r /home/xl_networks/production
[0 root@m2 ~]$ sudo setfacl -m u:aterrieur:r /home/xl_networks/production
[0 root@m2 ~]$ sudo setfacl -m u:massin:r /home/xl_networks/production
[0 root@m2 ~]$ sudo setfacl -m u:geparbal:r /home/xl_networks/production
```

Gérard MENVUSSA est propriétaire du dossier **production** avec tous les droits.

Guy LIGUILI a également tous les droits (lecture, écriture, exécution).

Jean BON, Mélanie ZETAUFRAIT, Alex TERRIEUR, Marc ASSIN et **Gilles EPARBAL** peuvent uniquement lire le contenu du dossier.

Tous les autres utilisateurs n'ont aucun accès à ce dossier.

Pour le dossier "recherche" :

```
sudo chown massin:recherche /home/xl_networks/recherche
sudo chmod 770 /home/xl_networks/recherche

sudo setfacl -m u:geparbal:rwX /home/xl_networks/recherche
sudo setfacl -x u:jbon /home/xl_networks/recherche
sudo setfacl -x u:mzetaufrait /home/xl_networks/recherche
sudo setfacl -x u:aterrieur /home/xl_networks/recherche
sudo setfacl -x u:gmenvussa /home/xl_networks/recherche
sudo setfacl -x u:gliguili /home/xl_networks/recherche
```

```
[0 root@m2 ~]$ sudo chown massin:recherche /home/xl_networks/recherche
[0 root@m2 ~]$ sudo chmod 770 /home/xl_networks/recherche
[0 root@m2 ~]$ sudo setfacl -m u:geparbal:rwX /home/xl_networks/recherche
[0 root@m2 ~]$ sudo setfacl -x u:jbon /home/xl_networks/recherche
[0 root@m2 ~]$ sudo setfacl -x u:mzetaufrait /home/xl_networks/recherche
[0 root@m2 ~]$ sudo setfacl -x u:aterrieur /home/xl_networks/recherche
[0 root@m2 ~]$ sudo setfacl -x u:gmenvussa /home/xl_networks/recherche
[0 root@m2 ~]$ sudo setfacl -x u:gliguili /home/xl_networks/recherche
```

Marc ASSIN est propriétaire du dossier **recherche** avec tous les droits.

Gilles EPARBAL a également **tous les droits** (lecture, écriture, exécution).

Jean BON, Mélanie ZETAUFRAIT, Alex TERRIEUR, Gérard MENVUSSA, et Guy LIGULI n'ont **aucun accès** à ce dossier.

e) Test de Connexion :

```
su - mzetaufrait
su - massin
su - gmenvussa
```

```
[0 mzetaufrait@m2 ~]$ su - mzetaufrait
Password:
[0 mzetaufrait@m2 ~]$ ^C
[130 mzetaufrait@m2 ~]$ exit
logout
```

```
[130 root@m2 ~]$ su - massin
[0 massin@m2 ~]$ ^C
[130 massin@m2 ~]$ exit
logout
[130 root@m2 ~]$ su - gmenvussa
[0 gmenvussa@m2 ~]$ exit
logout
```

e) Commandes pour la Sauvegarde :

On crée le dossier de destination si nécessaire

```
sudo mkdir -p /mnt/hostfs
```

On copie les fichiers :

```
sudo cp /etc/passwd /mnt/hostfs/
sudo cp /etc/shadow /mnt/hostfs/
sudo cp /etc/group /mnt/hostfs/
sudo cp /etc/gshadow /mnt/hostfs/
```

On vérifie la sauvegarde :

```
ls -l /mnt/hostfs/
```

On devrait voir les fichiers copiés dans ce répertoire.


```
[0 root@m2 ~]$ sudo mkdir -p /mnt/hostfs
[0 root@m2 ~]$ sudo cp /etc/passwd /mnt/hostfs
[0 root@m2 ~]$ sudo cp /etc/shadow /mnt/hostfs
[0 root@m2 ~]$ sudo cp /etc/group /mnt/hostfs
[0 root@m2 ~]$ sudo cp /etc/gshadow /mnt/hostfs
[0 root@m2 ~]$
[0 root@m2 ~]$ ls -l /mnt/hostfs/
total 28
4 -rw-r--r-- 1 1000 1000 3 Feb 2 17:12 GUESTNAME
4 -rwxrwxr-x 1 1000 1000 254 Feb 2 17:10 boot_parameters*
4 -rw-r--r-- 1 1000 1000 874 Feb 2 19:50 group
4 -rw-r----- 1 1000 1000 719 Feb 2 19:50 gshadow
4 -rw-r--r-- 1 1000 1000 26 Feb 2 17:10 marionnet-relay.rcfile
4 -rw-r--r-- 1 1000 1000 2188 Feb 2 19:49 passwd
4 -rw-r----- 1 1000 1000 2004 Feb 2 19:50 shadow
```

On vérifie sur notre machine réelle que les fichiers sont bien présents :

```
ls /tmp/marionnet-548966789.dir/tp1/hostfs/2
```

```
efrei@ubuntu1604:~$ ls /tmp/marionnet-548966789.dir/tp1/hostfs/2
boot_parameters  gshadow  marionnet-relay.rcfile  shadow
group            GUESTNAME  passwd
```

On voit bien que les fichiers sont bien présents.

5. Déploiement sur l'Équipement m3

a) Copier les Fichiers de Gestion des Utilisateurs :

```
mkdir /tmp/marionnet-548966789.dir/tp1/hostfs/4/etc

cp /tmp/marionnet-548966789.dir/tp1/hostfs/2/passwd
/tmp/marionnet-548966789.dir/tp1/hostfs/4/etc/passwd
cp /tmp/marionnet-548966789.dir/tp1/hostfs/2/group
/tmp/marionnet-548966789.dir/tp1/hostfs/4/etc/group
cp /tmp/marionnet-548966789.dir/tp1/hostfs/2/shadow
/tmp/marionnet-548966789.dir/tp1/hostfs/4/etc/shadow
cp /tmp/marionnet-548966789.dir/tp1/hostfs/2/gshadow
/tmp/marionnet-548966789.dir/tp1/hostfs/4/etc/gshadow
```

b) Tester la Connexion sur m3 :

On vérifie que les fichiers sont bien présents sur la machine m3 :

```
[0 root@m3 /mnt/hostfs]$ ls
total 16
4 GUESTNAME 4 boot_parameters* 4 etc/ 4 marionnet-relay.rcfile 0 test
[0 root@m3 /mnt/hostfs]$ cd etc/
[0 root@m3 /mnt/hostfs/etc]$ ls
total 16
4 group 4 gshadow 4 passwd 4 shadow
```

Puis on les déplace dans les répertoires systèmes sur m3:

```
sudo cp /mnt/hostfs/etc/passwd /etc/passwd
```

```
sudo cp /mnt/hostfs/etc/shadow /etc/shadow
sudo cp /mnt/hostfs/etc/group /etc/group
sudo cp /mnt/hostfs/etc/gshadow /etc/gshadow
```

```
[0 root@m3 /mnt/hostfs/etc]$ sudo cp /mnt/hostfs/etc/group /etc/group
[0 root@m3 /mnt/hostfs/etc]$ sudo cp /mnt/hostfs/etc/passwd /etc/passwd
[0 root@m3 /mnt/hostfs/etc]$ sudo cp /mnt/hostfs/etc/shadow /etc/shadow
[0 root@m3 /mnt/hostfs/etc]$ sudo cp /mnt/hostfs/etc/gshadow /etc/gshadow
```

De la même façon que pour m2, on teste les connexions utilisateurs.

```
[1 root@m3 /mnt/hostfs/etc]$ su - massin
No directory, logging in with HOME=/
massin@m3:/$ exit
logout
[0 root@m3 /mnt/hostfs/etc]$ su - gmenvussa
No directory, logging in with HOME=/
gmenvussa@m3:/$ exit
logout
[0 root@m3 /mnt/hostfs/etc]$ su - gliguili
No directory, logging in with HOME=/
gliguili@m3:/$ exit
logout
[0 root@m3 /mnt/hostfs/etc]$ su - aterrieur
No directory, logging in with HOME=/
aterrieur@m3:/$ exit
logout
[0 root@m3 /mnt/hostfs/etc]$ su - jbon
No directory, logging in with HOME=/
jbon@m3:/$ exit
logout
[0 root@m3 /mnt/hostfs/etc]$ su - geparbal
No directory, logging in with HOME=/
```

6. Correction des Erreurs sur m1 :

On va corriger les problèmes pour que tous les utilisateurs puissent se connecter correctement sur **m1**. Voici ce qu'on doit faire pour chaque utilisateur :

1. tata :

- **Connexion réussie**, répertoire personnel accessible, **aucune correction nécessaire**.

2. tete :

- **Connexion réussie**, répertoire personnel présent, **rien à corriger**.

3. titi :

- **Problème** : Retour immédiat sans session interactive.
- **Raison** : Le shell est configuré sur **/bin/false**.

Ce qu'on doit faire :

- On change le shell de **titi** pour lui permettre d'ouvrir une session interactive :

```
sudo usermod -s /bin/bash titi
```

- On s'assure que son répertoire personnel existe :

```
sudo mkdir -p /home/users/titi
sudo chown titi:2000 /home/users/titi
```

- On définit un mot de passe pour **titi** si ce n'est pas déjà fait :

```
sudo passwd titi
```

Résultat :

```
[0 root@m1 ~]$ sudo usermod -s /bin/nash titi
[0 root@m1 ~]$ sudo mkdir -p /home/users/titi
[0 root@m1 ~]$ sudo chown titi:2000 /home/users/titi
[0 root@m1 ~]$ sudo passwd titi
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
[0 root@m1 ~]$ su - titi
Cannot execute /bin/nash: No such file or directory
[127 root@m1 ~]$ sudo usermod -s /bin/bash titi
[0 root@m1 ~]$ su - titi
titi@m1:~$ exit
logout
```

4. toto :

- **Problème** : Message *"No directory, logging in with HOME=/"*.
- **Raison** : Le répertoire personnel est **manquant ou inaccessible**.

Ce qu'on doit faire :

- On crée le répertoire personnel de **toto** et on lui attribue:

```
sudo mkdir -p /home/users/toto
sudo chown toto:2000 /home/users/toto
sudo usermod -d /home/users/toto toto
```

- On vérifie que **toto** a bien un shell valide :

```
sudo usermod -s /bin/bash toto
```

- On s'assure que le mot de passe est bien défini :

```
sudo passwd toto
```

```
[0 root@m1 ~]$ su - toto
toto@m1:~$ exit
logout
```

5. tutu :

- **Problème** : Même message que **toto** ("No directory, logging in with HOME=/").
- **Raison** : Le répertoire personnel est **absent** ou **les permissions sont incorrectes**.

Ce qu'on doit faire :

- On crée le répertoire personnel de **tutu** et on le lui attribue:

```
sudo mkdir -p /home/users/tutu
sudo chown tutu:2000 /home/users/tutu
sudo usermod -d /home/users/tutu tutu
```

- On vérifie que **tutu** a bien un shell valide :

```
sudo usermod -s /bin/bash tutu
```

- On définit un mot de passe si nécessaire :

```
sudo passwd tutu
```

```
[0 root@m1 ~]$ sudo mkdir -p /home/users/tutu
[0 root@m1 ~]$ sudo chown tutu:2000 /home/users/tutu
[0 root@m1 ~]$ sudo usermod -d /home/users/tutu tutu
[0 root@m1 ~]$ sudo usermod -s /bin/bash tutu
usermod: no changes
[0 root@m1 ~]$ sudo passwd tutu
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
[0 root@m1 ~]$ su - tutu
```