TP1 : Construction d'un conteneur à partir de zéro

Ifrim Vasile-Alexandru
M2 SSI

1. Dans le répertoire TP1 créez une sous-répertoire container pour le conteneur.

```
$ mkdir -p ~/TP1/container
```

2. Installez debootstrap pour initialiser un système de fichiers minimal.

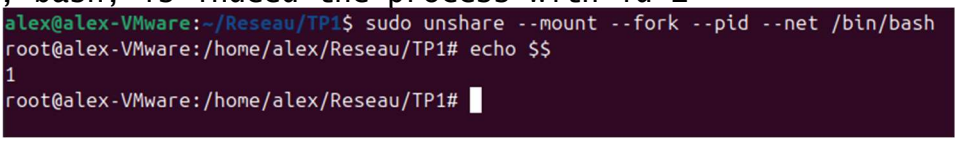
```
$ sudo apt-get update
$ sudo apt-get install debootstrap
```

3. Initialisez un système de fichiers minimal Debian minimal dans le répertoire container.

```
$ # in my case i had to desactivate checking for the keyring file
$ sudo debootstrap --no-check-gpg stable TP1/container
http://deb.debian.org/debian/
```

4. Utilisez unshare pour créer un nouveau namespace. qui isolera le réseau, les processus, et le système de fichiers ...

```
$ sudo unshare --net --pid --mount --fork /bin/bash
$ # --net = unshare network namesapce
$ # --pid = unshare pid namespace
$ # --fork = fork before executing a program (ex. '/bin/bash')
# # this way we launch a bash process in our shell, belonging to the
newly created namespace.
# # we can check by doing 'echo $$' and seeing that the current
process, bash, is indeed the process with id 1
```



5. Utiliser OverlayFS pour simuler un système de fichiers en couches. Utiliser les noms de répertoires (container (lower), upper, work et merged).

```
# mkdir {upper,work,merged}
```

6. Montez le système de fichiers OverlayFS. La couche basse est celle qui contient le système de fichiers minimal : le répertoire container.

```
# sudo mount -t overlay container_fs -o
lowerdir=./container,upperdir=./upper,workdir=./work ./merged
# # lowerdir - readonly
# # upperdir – any modifications to the merged directory will be
reflected here
# # work – used by overlayfs to manage copy-on-write changes, a
technique to manage shared data
```

7. Expliquez en quoi la commande pivot_root est essentielle lors de la création d'un conteneur. En quoi diffère-t-elle de chroot, et pourquoi pivot_root est-il souvent préféré pour l'isolement des conteneurs ?

The `pivot_root` command is crucial essential because it changes the current process's root filesystem to a new one, allowing the original to be unmounted. On the other hand, `chroot` only changes the root directory. This means that `pivot_root` offers better isolation.

8. Créez un répertoire temporaire pour pouvoir exécuter la commande pivot_root.

```
# mkdir -p merged/tmp/pivot_tmp
# # check pivot_root man pages; an important observation is that the
temp directory for the old root fs must be a subdirectory of the new
root fs
```

9. Utilisez pivot_root pour déplacer la racine de merged à old_root.

```
root@alex-VMware:/home/alex/Reseau/TP1# mount -t overlay container_fs -o lowerdir=./container,upperdir=./upper,workdir=./work ./merged
root@alex-VMware:/home/alex/Reseau/TP1# pivot_root merged merged/tmp/pivot_temp
root@alex-VMware:/home/alex/Reseau/TP1# cd /
root@alex-VMware:/# ls /home/
testf
root@alex-VMware:/# uname
Linux
root@alex-VMware:/# uname -r
6.8.0-47-generic
root@alex-VMware:/# cat /etc/os-release
PRETTY_NAME="Debian GNU/Linux 12 (bookworm)"
NAME="Debian GNU/Linux"
VERSION_ID="12"
VERSION="12 (bookworm)"
VERSION_CODENAME=bookworm
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
root@alex-VMware:/#
```

10. Monter les systèmes de fichiers nécessaires : proc, sys, tmp.

```
root@alex-VMware:/# ps
Error, do this: mount -t proc proc /proc
root@alex-VMware:/# mount -t proc proc /proc
root@alex-VMware:/# ps
    PID TTY          TIME CMD
      1 ?        00:00:00 bash
     16 ?        00:00:00 ps
root@alex-VMware:/#
```

TTY = ? indicates that the process is not attached to a controlling terminal; this is because we didn't inherit the namespace for it

```
# mount -t proc proc /proc
# #process and system information
# mount -t sys sys /sys
# mount -t tmp tmp /tmp
```

11. Recouvrer le shell courant par un bash.

```
# exec /bin/bash
```

12. Ecrire un script shell permettant la création d'un conteneur à partir de zéro.

```
#!/bin/bash
mkdir -p TP1/{container,upper,work,merged}
cd TP1
sudo debootstrap --no-check-gpg stable ./container
http://deb.debian.org/debian/
sudo unshare --fork --pid --mount --net /bin/bash
mount -t overlay overlay -o
lowerdir=./container,upperdir=./upper,workdir=./work ./merged
mkdir -p ./merged/tmp/old_root
pivot_root ./merged ./merged/tmp/old_root
mount -t proc proc /proc
mount -t sysfs sys /sys
mount -t tmpfs tmp /tmp
exec /bin/bash
```