chroot

Thierry Vaira
LaSalle Avignon BTS SN IR

v0.1 28/05/2020

Présentation

`chroot` (*ch*ange *root*) est un appel système et une commande des systèmes d'exploitation Unix permettant de changer le répertoire racine d'un processus de la machine hôte.

Les systèmes BSD ont étendu le concept en fournissant la commande **`jail`**.

En 2003, l'utilisation plus répandue du `chroot` *shell* Linux donne naissance aux plateformes Internet de microservices applicatifs SaaS et PaaS avec une consommation facturée à l'usage des ressources du *jail*, prémices du *cloud*, de la virtualisation système des serveurs, ainsi que des technologies renommées plus tard containers (tel que **Docker**).

Objectif

La commande **`chroot`** permet d'isoler l'exécution d'un processus et d'éviter ainsi la compromission complète d'un système lors de l'exploitation d'une faille.

Si le processus se retrouve “compromis”, il n'aura accès qu'à l'environnement isolé et non pas à l'ensemble du système d'exploitation. Cet environnement est appelé un chroot jail (une “prison”).

Il permet également de faire tourner plusieurs instances d'un même ensemble de services ou démons sur la même machine hôte.

Test : la commande chroot

```
$ man chroot

$ which chroot
/usr/sbin/chroot

$ sudo chmod +s /usr/sbin/chroot
$ ls -l /usr/sbin/chroot
-rwsr-sr-x 1 root root 39096 janv. 18  2018 /usr/sbin/chroot
```

Test : script de connexion

```
$ which bash
/bin/bash

$ sudo vim /bin/chlogin
#!/bin/bash
exec -c /usr/sbin/chroot /home/$USER /bin/bash

$ sudo chmod +x /bin/chlogin
$ ls -l /bin/chlogin
-rwxr-xr-x 1 root root 59 mai   28 06:07 /bin/chlogin
```

Test : création de l'utilisateur test

```
$ sudo useradd --home-dir /home/test --create-home --shell /bin/chlogin test
$ cat /etc/passwd
...
tv:x:1000:1000:Thierry Vaira:/home/tv:/bin/bash
test:x:1003:1004::/home/test:/bin/chlogin

$ sudo passwd test
...
passwd: password updated successfully

$ sudo cat /etc/shadow
...
test:$6$4y8xAwX.$mSIEXeBrLL1UYME3nxmSF.RuKpNgMZ7PhrrwIlyTxuzxLS0ZN2duTldUwQPdv
J6SEAmnBke7mM7Cu65u1Ow15/:18410:0:99999:7:::
```

Test : création de l'environnement

```
$ sudo mkdir /home/test/bin ; sudo mkdir /home/test/lib
$ sudo cp /bin/bash /home/test/bin/
$ ldd /bin/bash
    libtinfo.so.5 => /lib/x86_64-linux-gnu/libtinfo.so.5 (0x00007f89f12bb000)
    libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2 (0x00007f89f10b7000)
    libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f89f0cc6000)
    /lib64/ld-linux-x86-64.so.2 (0x00007f89f17ff000)

$ sudo mkdir /home/test/lib/x86_64-linux-gnu
$ ldd /bin/bash | awk '{ print "sudo cp " $3 " /home/test" $3}' | /bin/bash
$ sudo mkdir /home/test/lib64
$ sudo cp /lib64/ld-linux-x86-64.so.2 /home/test/lib64/ld-linux-x86-64.so.2
```

Test : l'environnement

```
$ tree /home/test/
/home/test/
├── bin
│   └── bash
├── lib
│   └── x86_64-linux-gnu
│       ├── libc.so.6
│       ├── libdl.so.2
│       └── libtinfo.so.5
└── lib64
    └── ld-linux-x86-64.so.2
```

Test : login test

```
serveur login: test
Password:
Last login: Thu May 28 06:31:50 UTC 2020 on tty1
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-76-generic x86_64)

bash-4.4$ pwd
/
bash-4.4$ ls
bash: ls: command not found
bash-4.4$
bash-4.4$
bash-4.4$
```

Test : modification de l'environnement

```
$ sudo cp /bin/ls /home/test/bin/
$ ldd /bin/ls | awk '{ print "sudo cp " $3 " /home/test" $3}' | /bin/bash
```