TD R202: Mettez vos processus en prison avec les "Namespaces"

Jean-Marc Pouchoulon

Mai 2022

1 Pré-requis, recommandations.

Vous travaillerez individuellement et sur une machine virtuelle Linux Ubuntu [1] sur laquelle vous aurez l'accès root afin d'installer des packages si besoin est.

Vous serez peut-être amené à installer les paquets suivants :

```
apt install util-linux libcap-ng-utils firejail
```

Il n'est nul besoin d'une interface graphique pour faire fonctionner firefox sur une VM. Utilisez l'option -X lorsque vous lancerez votre session ssh. Firefox s'affichera sur votre hôte via le protocole "X" dans un tunnel SSH.

```
xhost ip_de_votre_vm # xhost + ouvre à toutes les IP
ssh -X ip_de_votre_vm
```

Pour rappel "$$" en bash représente le PID du processus dans lequel vous êtes.

2 Définition des "NameSpaces"

Les NameSpaces sont la brique essentielle des mécanismes d'isolation des processus. Ils sont utilisés pour séparer des groupes de processus et sont essentiels à la technologie des containers. Ce sont eux qui donnent l'illusion d'être sur une machine indépendante de la machine hôte. [2]

La commande suivante vous permettra d'afficher une synthèse du nombre de processus par "NameSpaces" machine virtuelle.

1. voir `http://store.iutbeziers.fr`
2. voir l'article sous licence CC `https://connect.ed-diamond.com/GNU-Linux-Magazine/glmf-239/les-namespaces-ou-l-art-de-se-demultiplier`

```
# sudo lsns|awk '{print $2}'|sort -rn|uniq -c|grep -v TYPE
8 uts
16 user
1 time
7 pid
14 net
20 mnt
11 ipc
1 cgroup
```

1. En vous aidant de l'article retrouvez la définition des différents "NameSpaces".
2. Retrouvez les identifiants des "NameSpaces de votre processus bash sous /proc/ns/.
3. Utilisez la commande lsns qui liste les "NameSpaces" dans le contexte du processus.

3 Utilisation de firejail pour isoler Firefox

firejail[3] est une "sandbox" dont le but est d'isoler les processus de Firefox afin d'améliorer la sécurité de son utilisateur. Pour ce faire il repose entre autres sur l'utilisation des "NameSpaces".

1. Lancez firefox avec la commande :

   ```
   firejail --private firefox
   ```

2. retrouvez l'identifiant de la "jail" de Firefox ;
3. avec cet identifiant rendez-vous dans la "jail" de Firefox ;
4. listez les "NameSpaces" du processus de firefox ;
5. pourquoi ne voyez-vous pas d'autres "NameSpaces" ? Comparez avec un process bash sans "jail" ;
6. montrez que vous êtes dans une jail (utilisez "ps" "lsns" "/proc"...) ;

4 Utilitaire pour les NamesSpaces

4.1 Utilisation de la commande unshare

"unshare" est une commande qui permet de créer des NamesSpaces et un processus (bash par exemple) dont les processus s'éxécutent dans les "NameSpaces".

1. Lancez la commande suivante afin de créer un processus bash appartenant à de nouveaux "NameSpaces" :

   ```
   sudo unshare -u -p -i -f -m --mount-proc /bin/sh
   ```

2. Expliquez à quoi servent les options -u et -p à l'aide de "man unshare".
3. Lancez une commande ps. Que voyez-vous ? Expliquez ?

4.2 Utilisation des commandes du packages "iproute2"

La commande "ip" issue du package "iproute2" permet de créer des "network namespaces". On se propose de créer deux "network namespaces", de leur affecter une paire de cartes virtuelles et de les lier par deux IP dans le même subnet. C'est ce principe qui peut être appliqué lors de la création de NameSpace pour les containers.

Afin de connaître les options liées à la manipulation des networks namespaces tapez :

3. https://firejail.wordpress.com/documentation-2/basic-usage/

```
ip netns help
```

1. Créez un network namespace *netns1* et network namespace *netns2*
2. Exploration du netns1 :
   a) Rattachez vous à netns1.
   b) Quels est le device créé par default ?
   c) Que vous donne comme informations la demande ethtool -k (à quoi correspond la valeur off du champ netns-local ?
   d) Le device est-il "migrable" d'un netns à l'autre ?
3. Création de cartes virtuelles réseaux.
   a) Ajoutez un device veth :

```
ip link add name vethnetns type veth peer name vethnetns-peer
```

   b) Affectez vethnetns-peer sur netns2 (ip link set ...) .
   c) Affectez via deux ip dans le même LAN et pinguez la carte de l'autre netns.