namespaces

Thierry Vaira
LaSalle Avignon BTS SN IR

v0.1 28/05/2020

Présentation

Les espaces de noms (***namespaces***) sont une fonctionnalité Linux qui partitionne les ressources du noyau de telle sorte

- qu'un ensemble de processus voit un ensemble de ressources tandis qu'un autre ensemble de processus voit un ensemble différent de ressources.
- qu'un ensemble de processus sont séparés de telle façon qu'ils ne puissent pas « voir » les ressources des autres groupes.

Les ressources peuvent exister dans plusieurs espaces.

Exemple de ressources

Exemples de ressources : les PID, les noms d'hôte, les UID, les noms de fichiers et certains noms associés à l'accès au réseau et la communication interprocessus (IPC).

- L'espace de nommage par identifiant de processus (***PID namespace***) fournit l'isolation pour l'allocation des PIDs, la liste des processus et de leurs détails.
- L'espace de nommage réseau (***Network namespace***) isole le contrôleur de l'interface réseau (physique ou virtuel), les règles de pare-feu **`iptables`**, les tables de routage, etc. Les espaces de nommage réseau peuvent être connectés les uns avec chacun des autres en utilisant le périphérique virtuel Ethernet « **`veth`** ».
- L'espace de nommage « UTS » (***UTS namespace***) permet le changement de nom d'hôte.
- L'espace de nommage de montage (***Mount namespace***) permet de créer différents modèles de systèmes de fichiers, ou de créer certains points de montage en lecture-seule.
- L'espace de nommage IPC (***IPC namespace***) isole le système de communication inter-processus entre les espaces de nommage.

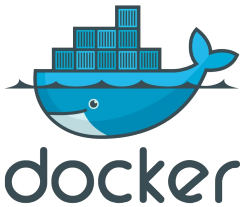
Objectif

⇒ Isolation par espace de nommage

Le rôle des **namespaces** est de créer un nouveau contexte système isolé pour le processus ciblé. On obtient une isolation pour :

- un nouvel espace de PID est initialisé et le processus prend le numéro de PID 1
- un nouvelle pile réseau est allouée au processus, donc aucun conflit possible avec les services réseaux de l'hôte
- un système de fichier indépendant permettant de monter/démonter les volumes sans incidence pour l'hôte

Utilisation



Les espaces de noms sont un aspect fondamental des **conteneurs** sous Linux.

Divers logiciels de conteneur utilisent des espaces de noms Linux (**namespaces**) en combinaison avec des groupes de contrôle (**cgroups**) pour isoler leurs processus, notamment **Docker** et LXC.

Les espaces de nom sont créés notamment avec la commande « **`unshare`** ».

Test

```
$ sudo unshare --fork --pid --mount-proc bash
# ps x
PID TTY      STAT   TIME COMMAND
1   pts/0    S      0:00 bash
9   pts/0    R+     0:00 ps x

# Côté hôte
$ ps faux
USER         PID TTY      STAT START   TIME COMMAND
tv         27251 tty1     S    12:25   0:00  \_ -bash
root       27281 tty1     S    12:26   0:00      \_ sudo unshare ...
root       27282 tty1     S    12:26   0:00          \_ unshare ...
root       27283 tty1     S+   12:26   0:00              \_ bash
```