Utiliser Podman sur une base ArchLinux/Manjaro

Afin d'utiliser Podman et/ou Buildah pour construire des containers "unprivileged" sur un système ArchLinux ou Manjaro, il est nécessaire de suivre plusieurs étapes d'installation supplémentaires.

Tout d'abord, il faut un noyau qui prend en charge les "user namespaces". Tous les noyaux Arch Linux prennent en charge cette fonctionnalité de base, cependant, le noyau Arch par défaut est livré avec les "user namespaces" activés uniquement pour l'utilisateur root...

- Tout d'abord, il faut créer deux fichiers qui vont être utilisés par Podman pour créer des containers "unprivileged" :

```
$ sudo /etc/subgid
votreuser:10000:65536

$ sudo /etc/subuid
votreuser:10000:65536
```

Explication : l'user root (UID 0) du container va être mappé sur le système avec un UID compris entre 10000 et 75536 (+ 65536), et donc ses privilèges seront minimes.

- Enfin, il convient de créer un fichier de configuration sysctl afin d'activer le mécanisme d'user namespaces pour les utilisateurs non-root. Pour cela, créer un fichier `/etc/sysctl.d/00-local-userns.conf` et ajouter le contenu suivant :

```
# vi /etc/sysctl.d/00-local-userns.conf
kernel.unprivileged_userns_clone=1
```

- Reboot le système !

Revision #1
Created 31 October 2019 11:36:12 by Cécile
Updated 31 October 2019 11:36:31 by Cécile