Durcissement post-installation

virtualisation, VM, Debian, post-install, durcissement

Une fois l'installation d'un OS “de base” (voir cette page), et la configuration post-install (voir cette page) effectuées, nous allons appliquer le durcissement de l'OS.

Hooks APT

Afin de pouvoir repasser les partitions /boot et /usr en read / write, et la partion /tmp en exec lors de l'installation de nouveaux paquets ou lors de l'upgrade de l'OS, nous ajoutons des hooks pour APT.

Nous créons le fichier 00apt

```
# vi /etc/apt/apt.conf.d/00apt
```

Nous y ajoutons ceci

```
DPkg::Pre-Invoke {
        "mount -o remount,rw /boot";
        "mount -o remount,rw /usr";
        "mount -o remount,exec /tmp";
};
DPkg::Post-Invoke {
        "mount -o remount,ro /boot";
        "mount -o remount,ro /usr";
        "mount -o remount,noexec /tmp";
};
```

Fstab

Nous éditons le fichier fstab

```
# vi /etc/fstab
```

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system>                           <mount point>   <type>  <options>
<dump>  <pass>
/dev/mapper/vg_sys-lv_root                /               btrfs   defaults
0       0
# /boot was on /dev/sda1 during installation
```

```
UUID=8077782c-de8c-4850-88ca-d93a1b706979 /boot           ext4
ro,nodev,nosuid,noexec        0       2
/dev/mapper/vg_sys-lv_tmp                 /tmp            btrfs
relatime,nodev,nosuid,noexec  0       0
/dev/mapper/vg_sys-lv_usr                 /usr            btrfs   ro,nodev
0       0
/dev/mapper/vg_sys-lv_log                 /var/log        btrfs
nodev,nosuid,noexec           0       0
/dev/mapper/vg_sys-lv_audit               /var/log/audit  btrfs
nodev,nosuid,noexec           0       0
/tmp                                      /var/tmp        none
rw,noexec,nosuid,nodev,bind   0       0
/dev/mapper/vg_sys-lv_swap                none            swap    sw
0       0
```