06 - Blocage, crash et dépannage d'urgence

Objectif

- Donner une vision claire du démarrage Linux et des gestes de secours quand le boot ou l'accès root est cassé.

1. Rôle de GRUB

> GRUB est le pont entre le firmware de la machine et le noyau Linux.

1. Rôle de GRUB

- Au démarrage, le firmware initialise la machine, cherche un périphérique amorçable, puis donne la main à un programme de boot.
- GRUB charge ensuite le noyau, l'initramfs et les paramètres nécessaires.
- En multi-boot, il permet aussi de choisir le système à démarrer.

2. Boot BIOS et MBR

> Historiquement, le BIOS charge les 512 premiers octets du disque : le MBR.

2. Boot BIOS et MBR

- Le MBR contient un petit code de démarrage et la table de partitions classique.
- Comme 512 octets sont très limités, GRUB utilise plusieurs étapes : une petite première étape, puis une image plus complète capable de lire `/boot/grub`.

3. GRUB Legacy

> GRUB Legacy fonctionne en étapes : stage 1, stage 1.5, stage 2.

3. GRUB Legacy

- **Stage 1** : très petit, placé dans le MBR ou le secteur de boot d'une partition.
- **Stage 1.5** : contient de quoi lire certains systèmes de fichiers.
- **Stage 2** : charge la configuration et affiche le menu.
- Cette architecture existe car le tout premier code exécuté dispose de très peu d'espace.

4. GRUB2 sur BIOS

> GRUB2 remplace les anciennes étapes par `boot.img`, `core.img` et des modules.

4. GRUB2 sur BIOS

- Sur disque MBR, `boot.img` peut être écrit dans les 440 premiers octets du MBR.
- Il charge `core.img`, souvent placé dans l'espace libre entre le MBR et la première partition.
- `core.img` charge ensuite les modules et le fichier `normal.mod`, puis lit la configuration.
- Sur disque GPT en mode BIOS, on utilise souvent une petite partition spéciale BIOS Boot d'environ 1 Mio pour stocker `core.img`.

4. GRUB2 sur BIOS — Problème classique

- Si l'index des partitions change ou si `/boot/grub` n'est plus accessible, GRUB peut tomber dans l'invite `grub rescue>` car il ne trouve plus `normal.mod`.

5. GRUB2 sur UEFI

> En UEFI, GRUB est un fichier `.efi` stocké dans la partition système EFI.

5. GRUB2 sur UEFI

- Sur une machine UEFI x64, le firmware peut lancer directement un fichier comme :

```
/efi/<distro>/grubx64.efi
```

- La partition système EFI remplace donc le démarrage par code MBR.
- Les modules GRUB et la configuration restent nécessaires, mais le point d'entrée est différent.

6. Fichiers de configuration GRUB2

> On ne modifie généralement pas `grub.cfg` directement ; on modifie les sources puis on régénère.

6. Fichiers de configuration GRUB2 — Fichiers importants

```
/etc/default/grub       paramètres généraux
/etc/grub.d/            scripts de génération du menu
/boot/grub2/grub.cfg    configuration finale Red Hat-like
/boot/grub/grub.cfg     configuration finale Debian-like
```

6. Fichiers de configuration GRUB2 — Point d'attention

- Toute modification manuelle de `grub.cfg` peut être écrasée lors d'une régénération.

7. Sauvegarder et restaurer le MBR

Le MBR est petit, mais critique.

Sauvegarder le MBR complet :

```
dd if=/dev/sda of=boot.mbr bs=512 count=1
```

Restaurer :

```
dd if=boot.mbr of=/dev/sda bs=512 count=1
```

Sauvegarder seulement le programme de boot :

```
dd if=/dev/sda of=pg.mbr bs=1 count=440
objdump -D -b binary -mi386 -Maddr16,data16 pg.mbr
```

7. Sauvegarder et restaurer le MBR — Point d'attention

- Restaurer 512 octets restaure aussi la table de partitions MBR.
- Si la table a changé, cela peut détruire l'accès aux partitions.
- Dans certains cas, on ne restaure que 440 ou 446 octets.

8. Paramètres de démarrage du noyau

> Les boot parameters servent à influencer le noyau au moment où il est chargé.

8. Paramètres de démarrage du noyau

- On les utilise pour fournir une information matérielle, forcer un comportement, démarrer en mode secours, changer la console ou remplacer temporairement le processus `init`.
- La référence complète est fournie par la documentation `bootparam` et les pages de manuel.

9. Modifier un mot de passe root perdu

> Si le bootloader n'est pas protégé, un accès physique peut souvent permettre de reprendre la main.

9. Modifier un mot de passe root perdu — Méthode avec mode recovery

1. Redémarrer.
2. Ouvrir le menu GRUB.
3. Choisir une entrée recovery.
4. Obtenir un shell root.
5. Remonter la racine en écriture.
6. Modifier le mot de passe.

```
mount -o rw,remount /
passwd root
```

9. Modifier un mot de passe root perdu — Méthode via remplacement d'init

- Si aucun mode recovery n'existe, on peut éditer temporairement l'entrée GRUB et demander au noyau de lancer un shell à la place d'init, par exemple :

```
init=/bin/bash
```

- Puis remonter la racine :

```
mount -o rw,remount /
passwd root
```

9. Modifier un mot de passe root perdu — Point d'attention

- Cette technique est une démonstration de sécurité autant qu'une technique de secours.
- Elle justifie le mot de passe GRUB, la protection firmware et le chiffrement disque.