

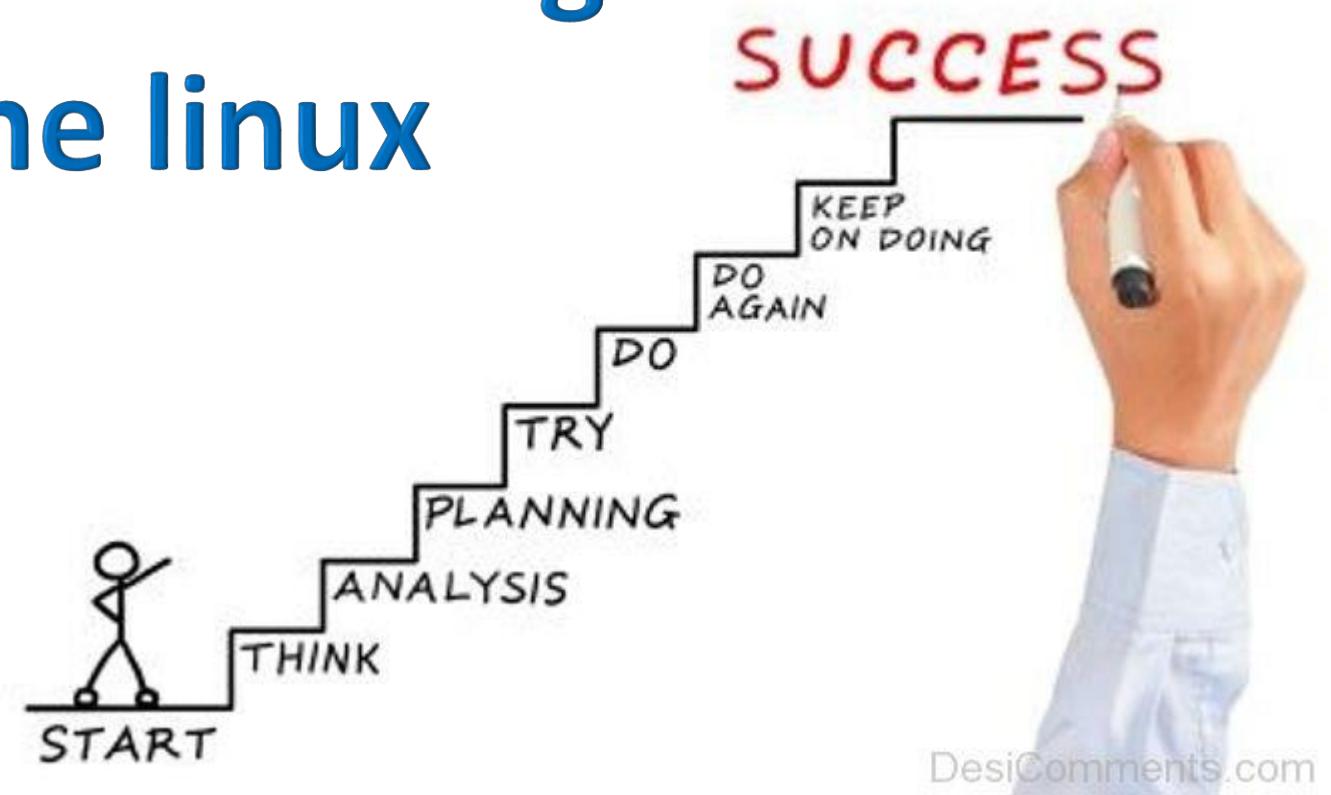
IF YOU KEEP DOING WHAT YOU BEEN DOING

YOU GONNA KEEP GETTING
WHAT YOU'VE BEEN GETTING

- STEVE HARVEY



Le processus de démarrage D'un système linux



DesiComments.com

<https://www.mageialinux-online.org/wiki/le-processus-de-demarrage-d-un-systeme-linux>

① Installation G / binx

② Processus de démarrage
et l'arrêt G / binx.

③ Gestion des processus

④ Gestion du système de fichiers ss - G / l

⑤ Users & groupes ss - G / l

⑥ Gestion et installation des logiciels
Gms G / l

⑦ Gestion des quotas sur l'utilisateur
des syst file (F.S)

⑧ Sauvegarde et
restauration des données
ss G / l

⑨ Planification des tâches
ss G / l

⑩ Gestion du réseau
ss G / l

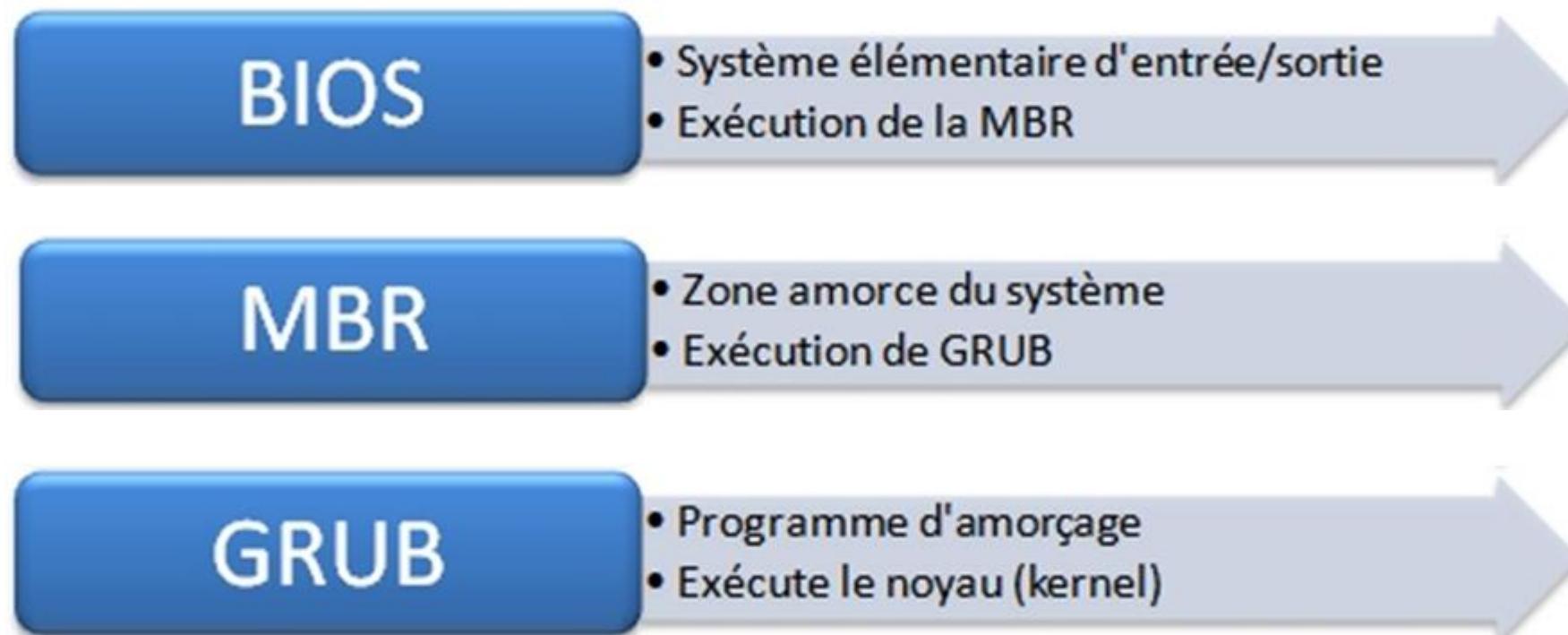
⑪ Supervision et maintenance

Le processus de démarrage d'un système Linux

Ce qu'il se passait sur un système Linux une fois que nous avons appuyé sur le bouton « Power » de notre ordinateur ?

Le démarrage d'un système Linux se fait en 6 étapes.

Càd avant que la fenêtre d'identification apparaisse, 6 processus s'exécute à tour de rôle.



BIOS

- Système élémentaire d'entrée/sortie
- Exécution de la MBR

MBR

- Zone amorce du système
- Exécution de GRUB

GRUB

- Programme d'amorçage
- Exécute le noyau (kernel)

NOYAU

- Noyau du système
- Exécute /sbin/init

INIT

- Tâches du système
- Exécute les niveaux d'exécution (runlevel)

RUNLEVEL

- Les niveaux d'exécution sont exécutés à partir du dossier /etc/rc.d/rc*.d/

1ère étape : le BIOS

1. BIOS = Basic Input/Output system : système élémentaire d'entrée/sortie. C'est un ensemble de fonctions contenu dans la mémoire morte (ROM) de la carte mère d'un ordinateur lui permettant d'effectuer des opérations élémentaires lors de sa mise sous tension.
2. Exécute des opérations de vérification de l'intégrité du système.
3. Cherche, charge et exécute le programme d'amorçage.
4. Il cherche le programme d'amorçage sur un disque dur, une disquette, un CD-Rom ou une clé USB.
5. Une fois le programme d'amorçage trouvé et chargé en mémoire, le BIOS lui donne le contrôle.
6. Simplement, le BIOS exécute la MBR.

2e étape : la MBR

1. MBR = Master Boot Record : la zone amorce.
2. C'est le premier secteur adressable d'un disque dur. Le plus souvent appelé /dev/hda ou /dev/sda.
3. La taille de cette zone est de 512 bits au maximum. Elle contient :
 - le programme d'amorçage se trouve dans les 446 premiers bits.
 - la table des partitions (les 4 partitions primaires) du disque dur sur les 64 bits suivants.
 - vérification de la validité du MBR dans les 2 derniers bits.
4. Il contient une routine d'amorçage dont le but est de charger le système d'exploitation (ou le « boot loader »/chargeur d'amorçage s'il existe - GRUB ou LiLo) présent sur la partition active.
5. Simplement, le MBR exécute le programme d'amorçage GRUB.



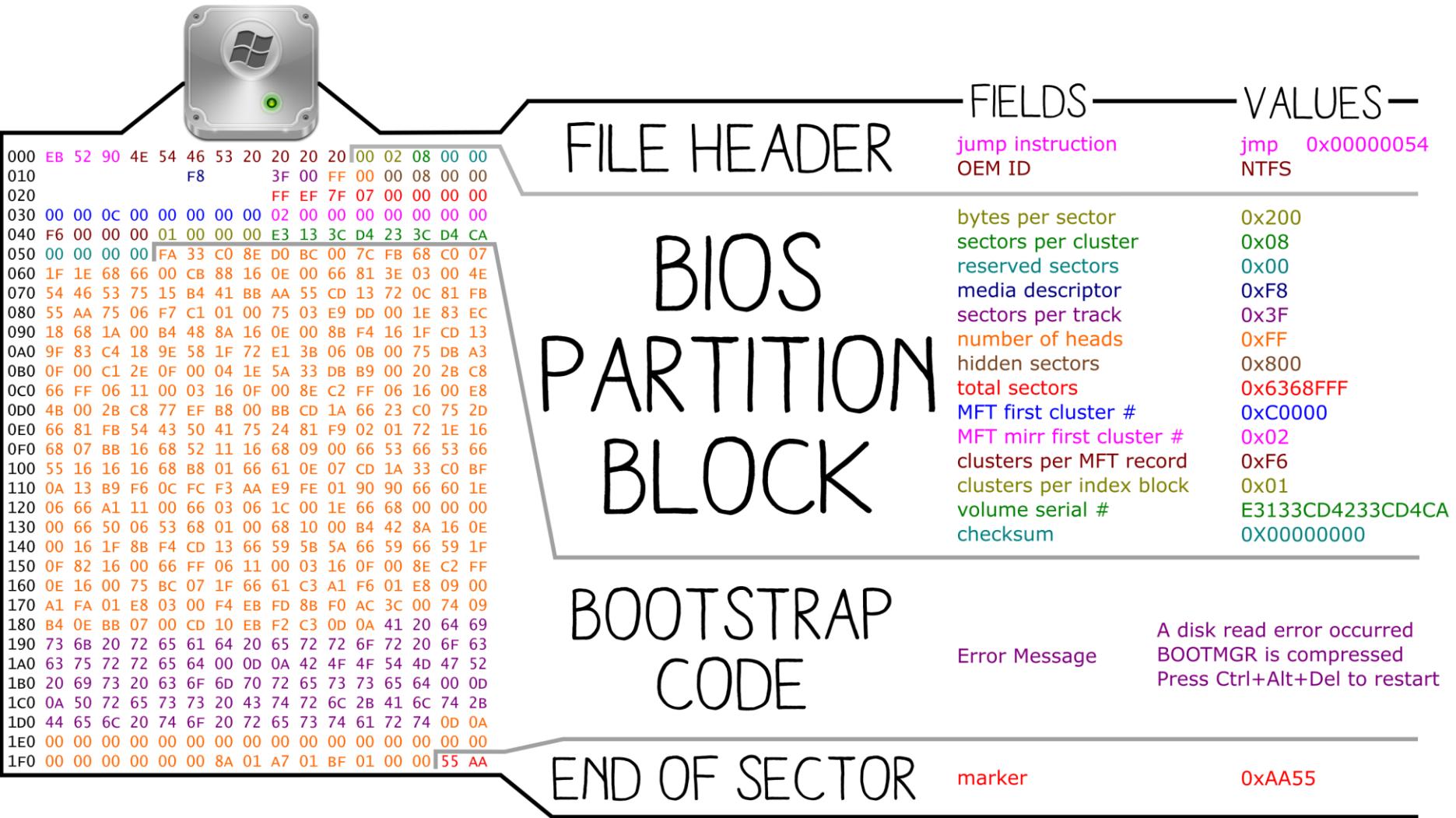
NTFS

VOLUME BOOT RECORD

Σ INVOKE-IR

BY: JARED ATKINSON

TEMPLATE BY: ANGE ALBERTIN



← Tweet



Jared Atkinson
@jaredcatkinson

NTFS Volume Boot Record Poster (first 512 bytes of the logical volume) @corkami @sansforensics

3e étape : le GRUB

1. GRUB = Grand Unified Bootloader : un programme d'amorçage de micro-ordinateur.
2. Lorsque le micro-ordinateur héberge plusieurs systèmes (on parle alors de multi-amorçage), il permet à l'utilisateur de choisir quel système démarrer.
3. Il présente une interface qui permet à l'utilisateur de choisir quel système d'exploitation démarrer.
4. Si vous avez plus d'un noyau installé sur votre système, il est possible de sélectionner celui que vous voulez exécuter.
5. Il connaît le système de fichiers (ext3, ext4, Btrfs, etc.) utilisé sur le système.
6. Simplement, GRUB charge et exécute le noyau sélectionné et l'image initrd (image d'un système minimal initialisé au démarrage du système = Initial Ram Disk).

4e étape : le noyau

1. Monte le système de fichiers racine (« root »). Donc, relie une partition ou un périphérique à un répertoire, répertoire par lequel les données présentes sur la partition ou le périphérique sont accessibles.
2. Le noyau charge et exécute le programme /sbin/init.
3. Comme le programme init est le premier programme à être exécuté par le noyau Linux, il porte le PID (ID du processus) numéro 1.
4. Le initrd permet ainsi d'avoir un système minimal pouvant ensuite charger le système de fichier principal ou bien des systèmes sans disques. Il peut être instable d'avoir "en dur" dans le kernel tous les drivers de disques. Pour éviter cela, les distributions compilent un kernel minimal avec les options de bases puis chargent les modules obligatoires nécessaires contenus dans l'archive de l'initrd.

5e étape : init

1. Il consulte le fichier /etc/inittab pour décider quel niveau d'exécution démarrer.
2. Les niveaux d'exécution sont :
 - 0 - Arrêt
 - 1 - Mode mono-utilisateur
 - 2 - Mode multi-utilisateur sans serveur applicatif
 - 3 - Mode multi-utilisateur avec serveur applicatif
 - 4 - Inutilisé ou X11 -> interface graphique selon la distribution
 - 5 - X11 -> interface graphique selon la distribution
 - 6 - Redémarrage
3. Init identifie le niveau d'exécution dans le fichier /etc/inittab et l'utilise pour charger les programmes associés au niveau.
4. En général, une distribution Linux fonctionne sur le niveau 5 ou 3.tim

6e étape : Runlevel

1. Lorsque votre système Linux démarre, vous apercevez (en appuyant sur la touche <ESC> afin de voir la version « verbeuse » du démarrage) divers services qui sont chargés. Ce sont les programmes du niveau d'exécution sur lequel votre système fonctionne qui sont chargés à partir du répertoire représentant le niveau d'exécution du système.
2. Les répertoires des niveaux d'exécution sont :
 - Run level 0 – /etc/rc.d/rc0.d/
 - Run level 1 – /etc/rc.d/rc1.d/
 - Run level 2 – /etc/rc.d/rc2.d/
 - Run level 3 – /etc/rc.d/rc3.d/
 - Run level 4 – /etc/rc.d/rc4.d/
 - Run level 5 – /etc/rc.d/rc5.d/
 - Run level 6 – /etc/rc.d/rc6.d/
3. Dans ces répertoires, on retrouve des noms de programme qui commencent par la lettre S et K.
4. Ceux qui commencent par la lettre S sont exécutés au démarrage du système (la lettre S pour « startup » = démarrage).
5. Ceux qui commencent par la lettre K sont exécutés à l'arrêt du système (la lettre K pour « kill » = arrêt).
6. De plus, dans le nom de ces programmes, il y a un chiffre après la lettre S ou K. Ce chiffre indique l'ordre d'exécution de chaque programme lors du démarrage ou de l'arrêt du système. Par exemple, S12syslog est le 12^e programme qui s'exécutera au démarrage du système.

Atelier

Réinitialisation du mot de passe root sur RHEL 9

- Objectifs pédagogiques clairs
- Explications mot par mot des commandes
- Étapes détaillées pour réinitialiser le mot de passe root
- Schéma du processus de démarrage Linux
- Notes de sécurité et bonnes pratiques
- Ressources complémentaires

Objectif pédagogique

Permettre aux étudiants d'apprendre à réinitialiser un mot de passe root oublié sur un système Red Hat Enterprise Linux 9 en utilisant l'environnement de récupération via GRUB.

Prérequis

- Connaissances de base en administration Linux
- Accès physique ou console virtuelle à une machine RHEL 9
- Compte utilisateur avec privilèges ou accès au BIOS/UEFI

Étapes de réinitialisation du mot de passe root

1. Redémarrage du système

- Redémarrer la machine RHEL 9.
- À l'écran de démarrage GRUB, appuyer sur la touche e pour éditer les paramètres de démarrage.

2. Modification des paramètres du noyau

- Repérer la ligne commençant par linux ou linux16.
- À la fin de cette ligne, ajouter :

rd.break ⇔ "ramdisk break"

- Cela permet d'interrompre le démarrage et d'entrer dans un environnement de récupération.

rd.break signifie : "Interrompre le démarrage juste après le chargement du ramdisk, pour accéder à un shell de secours."

3. Accès à l'environnement initramfs

- Appuyer sur **Ctrl + X** pour démarrer avec les nouveaux paramètres.
- Le système démarre dans un shell de secours.

4. Remontage du système en écriture

```
mount -o remount,rw /sysroot
```

5. Accès au système avec chroot

chroot /sysroot

6. Réinitialisation du mot de passe root

passwd

7. Mise à jour du contexte SELinux

touch /.autorelabel

Cela garantit que SELinux relabel les fichiers au prochain démarrage.

8. Redémarrage du système

exit

exit

Le système redémarre normalement avec le nouveau mot de passe root.