

## Administration Unix

### 4IIR

#### TP n° 2 : Configuration des paramètres du Boot Loader GRUB2

##### Objectif :

- Comprendre comment fonctionne Grub2, analyser le contenu du fichier de configuration grub.cfg, et comment il est généré.
- Manipuler les commandes les plus utiles de Grub2.

##### Configuration initiale :

- Ce TP est à réaliser avec une station sous Redhat Entreprise Linux 8

#### A. Présentation :

**GRUB 2** est la dernière version du GNU GRUB (GRand Unified Bootloader). C'est un chargeur de démarrage universel qui est responsable du chargement et du transfert du contrôle au noyau du système. Il vous permet aussi de démarrer sur le système d'exploitation que vous souhaitez.

Comme toute application Linux, il possède des fichiers de configuration qui se trouvent dans **/boot** et **/etc** avec notamment **/etc/default/grub**. Il fournit aussi des commandes comme **grub2-mkinstall** et **grub2-mkconfig** pour notamment installer ou configurer GRUB.

#### B. Dossier /boot avec les fichiers de configuration GRUB

Le dossier **/boot** contient les fichiers de configuration du démarrage (boot), noyaux et d'autres fichiers indispensables au moment du démarrage, y compris le dossier de configuration de GRUB. Afficher le contenu de ce dossier :

```
root@hostname# ls /boot
```

Le tableau ci-dessous, donne les principaux dossiers et fichiers de configuration de Grub2 :

Emplacement	Description
<b>/boot/grub2/grub.cfg</b>	C'est le fichier de configuration principal qui doit être généré automatiquement.
<b>/etc/grub.d/</b>	Ce dossier stocke les scripts GRUB. Ces scripts sont des blocs de construction à partir desquels le fichier <b>grub.cfg</b> est construit. Lorsque la commande GRUB appropriée est exécutée, les scripts sont lus dans une certaine séquence et <b>grub.cfg</b> est créé.
<b>/etc/default/grub</b>	Contient les paramètres du menu GRUB qui sont lus par les scripts GRUB et écrits dans <b>grub.cfg</b> . C'est la partie de personnalisation du GRUB.

Ainsi :

- **/etc/default/grub** contient la personnalisation.

- Les scripts **/etc/grub.d/** contiennent des informations de menu GRUB et des scripts de démarrage du système d'exploitation.

Lorsque la commande **grub2-mkconfig** est exécutée, elle lit le contenu du fichier **/etc/default/grub** et des scripts **grub.d** et crée le fichier **grub.cfg**.

### 1. Le dossier **/etc/grub.d**

Les scripts sont numérotés pour respecter un ordre d'exécution lors de la construction du fichier. Vous pouvez lister le contenu de **/etc/grub.d** :

```
root@hostname# ls -l /etc/grub.d
```

Voici quelques exemples de scripts. Ils ne sont pas forcément présents chez vous, cela dépend de la distribution Linux :

- **00\_header**: script permettant la génération de l'en-tête du fichier **grub.cfg**. Cet en-tête est généré principalement à l'aide des informations paramétrées dans le fichier **/etc/default/grub**
- **01\_users** : qui n'est créé que lorsqu'un mot de passe du chargeur de démarrage est attribué.
- **20\_linux\_xen**: script pour Xen Linux et Xen Hypervisor
- **30\_os-prober** : script permettant de détecter les autres systèmes installés et générer les entrées correspondantes.
- **40\_custom**: script permettant de générer des entrées introduites manuellement dans ce fichier
- **10\_linux**: script permettant de générer les entrées correspondant au système GNU/Linux hôte

### 2. Le fichier **/etc/default/grub**

Le fichier de configuration par défaut pour GRUB2 est **/boot/grub2/grub.cfg**. Vous ne devez pas éditer ou modifier ce fichier, sauf si vous êtes bien familiarisé avec GRUB2. C'est le fichier principal pour démarrer dans le système d'exploitation Linux. Si vous faites une mauvaise configuration, vous vous retrouverez sûrement avec un système défectueux. Alors, ne touchez pas à ce fichier !

Le fichier **/boot/grub/grub.cfg** est automatiquement généré par **grub2-mkconfig** en utilisant les scripts de **/etc/grub.d** et les paramètres de **/etc/default/grub**. Toutes les modifications que vous avez apportées dans le fichier **/etc/default/grub** seront répercutées sur le GRUB2.

Pour voir le contenu du fichier **/etc/default/grub**:

```
root@hostname# cat /etc/default/grub
```

Les premières clés et valeurs de configuration /etc/default/grub :

Clés	Description
GRUB_TIMEOUT	Le temps en secondes après l'affichage du menu pour démarrer l'entrée par défaut, sauf si une touche est enfoncée. La valeur par défaut est 5. Définissez sur 0 pour démarrer immédiatement sans afficher le menu, ou sur -1 pour attendre indéfiniment
GRUB_DISTRIBUTOR	Défini par les distributeurs de GRUB et utilisé pour générer des titres d'entrée de menu plus informatifs. Par exemple : GRUB_DISTRIBUTOR=`echo -n TITRE PERSONNALISÉ`#donne : TITRE PERSONNALISÉ GNU/Linux
GRUB_DEFAULT	L'entrée de menu par défaut pour démarrer : <ul style="list-style-type: none"> <li>– Une valeur de 0 démarre la première entrée de menu.</li> <li>– Une valeur de 1 démarre la deuxième entrée de menu.</li> <li>– Une valeur de saved indique à GRUB 2 de charger le dernier système d'exploitation chargé avec succès</li> </ul>
GRUB_DISABLE_SUBMENU	Si on souhaite voir directement une entrée de menu par noyau linux disponible (On peut supprimer les noyaux les plus anciens)
GRUB_TERMINAL_OUTPUT	Sélectionne le périphérique de sortie du terminal. Vous pouvez sélectionner plusieurs périphériques ici, séparés par des espaces. Les noms de terminaux valides peuvent inclure 'console' (console native de la plate-forme), 'serial' (terminal série), 'serial_<port>' (terminal série avec sélection explicite du port), 'gfxterm' (sortie en mode graphique), etc.
GRUB_CMDLINE_LINUX	Paramètres de démarrage du noyau.
GRUB_TIMEOUT_STYLE	Pour afficher ou non le menu Grub : <ul style="list-style-type: none"> <li>– Une valeur "hidden" veut dire que le menu n'apparaît pas au démarrage</li> <li>– Une valeur "menu" forcera l'affichage du menu Grub au démarrage (on peut aussi commenter la ligne GRUB_TIMEOUT_STYLE=hidden)</li> </ul>

Chaque fois que vous avez apporté des modifications à ce fichier, vous devez exécuter la commande suivante pour appliquer les modifications au GRUB :

```
root@hostname# grub2-mkconfig -o /boot/grub2/grub.cfg
```

NB !!!!! Noter que si votre système utilise UEFI, l'emplacement de la configuration de GRUB sera : /boot/efi/EFI/redhat/grub.cfg

```
root@hostname# grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

### C. Atelier 1 : Configuration du chargeur de démarrage Grub

1. Se connecter en tant que root
2. Sauvegarder le fichier original **/etc/default/grub** avant d'apporter des modifications.
3. Visualiser le fichier de configuration de grub **/etc/default/grub**, interpréter le contenu de ce fichier
4. Modifier le fichier de configuration de grub afin de :

#### a) Sélectionner le système par défaut

Ouvrez le fichier **/etc/default/grub** à l'aide de n'importe quel éditeur de texte, et trouvez la ligne **"GRUB\_DEFAULT"**. Nous pouvons sélectionner le système d'exploitation par défaut pour démarrer en utilisant cette option. Si vous définissez la valeur sur **"0"**, le premier système d'exploitation dans l'entrée du menu de démarrage GRUB démarrera. Si vous le définissez sur **"1"**, le deuxième système d'exploitation démarrera, et ainsi de suite.

De plus, si vous avez plusieurs OS dans votre système, vous pouvez démarrer le dernier système d'exploitation en utilisant la valeur **GRUB\_DEFAULT = saved**. Chaque fois que vous redémarrez le système, le dernier système d'exploitation démarre. Veuillez noter que vous devez ajouter une ligne **GRUB\_SAVEDEFAULT = true** pour que cette astuce fonctionne.

Exécutez la commande suivante pour recréer le fichier de configuration GRUB.

```
root@hostname # grub2-mkconfig -o /boot/grub2/grub.cfg
```

#### b) Définir le temps d'attente avant le démarrage du système par défaut

Par défaut, l'entrée sélectionnée dans le menu de démarrage commencera à démarrer dans 5 secondes. Vous pouvez augmenter ou diminuer ce paramètre de délai **GRUB\_TIMEOUT**. Si la valeur est **"0"**, le système d'exploitation par défaut commencera immédiatement à démarrer. Si la valeur est **"5"**, le menu de démarrage apparaîtra pendant 5 secondes, afin que vous puissiez sélectionner le système d'exploitation que vous souhaitez charger au démarrage du système. Si la valeur est **"-1"** le menu de grub va rester affiché indéfiniment.

Modifiez cette valeur afin de pouvoir attendre 10 secondes avant le démarrage de l'entrée sélectionnée.

Exécutez la commande suivante pour recréer le fichier de configuration GRUB.

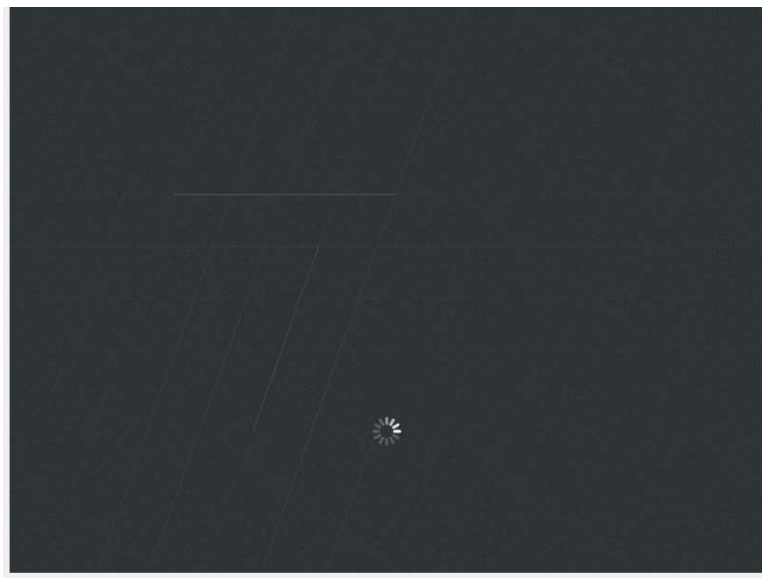
```
root@hostname # grub2-mkconfig -o /boot/grub2/grub.cfg
```

#### c) Changer les paramètres à passer au noyau

Le noyau Linux peut recevoir divers paramètres au moment du démarrage ou de l'exécution. Ces paramètres personnalisent le comportement par défaut du noyau (par exemple, le redémarrage automatique en cas de panique du noyau), ou informent le noyau sur la configuration matérielle. Les paramètres du noyau peuvent être modifiés au moment de l'exécution, tandis que certains paramètres du noyau doivent être transmis au noyau au moment du démarrage en modifiant la ligne **GRUB\_CMDLINE\_LINUX** dans le fichier de configuration de grub.

Par défaut cette ligne contient ces deux options : **rhgb** et **quiet**.

- **Rhgb** (Red Hat Graphical Boot): Spécifie que l'affichage graphique de démarrage doit être utilisé pour indiquer la progression du démarrage.
- **Quiet** : Réduit la sortie de débogage.



Supprimez ces deux options et vous allez remarquer qu'au prochain redémarrage tous les messages d'initialisation vont s'afficher en mode console au lieu du mode graphique présenté dans la figure ci-après.

Exécutez la commande suivante pour recréer le fichier de configuration GRUB.

```
root@hostname # grub2-mkconfig -o /boot/grub2/grub.cfg
```

#### **d) Changer le mode de démarrage par défaut de Linux**

Par défaut votre système RedHat démarre sur le mode graphique, si vous voulez que votre système démarre par défaut sur le mode Console, modifiez ou ajoutez la ligne suivante dans le fichier de configuration de grub:

```
GRUB_CMDLINE_LINUX_DEFAULT="3"
```

**3:** c'est le numéro représentant le mode multi-utilisateurs complet: Tous les services nécessaires sont démarrés et plusieurs utilisateurs peuvent se connecter en mode texte.

Exécutez la commande suivante pour recréer le fichier de configuration GRUB.

```
root@hostname # grub2-mkconfig -o /boot/grub2/grub.cfg
```

#### **e) Ajouter des entrées pour redémarrer et arrêter le système**

Vous pouvez ajouter des entrées personnalisées dans le fichier "**40\_custom**" se trouvant dans **/etc/grub.d/** pour inclure des options spécifiques telles que "Redémarrer" et "Arrêter le système" dans le menu GRUB.

Ouvrez le fichier **/etc/grub.d/40\_custom** à l'aide de n'importe quel éditeur de texte, Ajoutez les entrées personnalisées pour "Redémarrer" et "Arrêter le système" dans ce fichier.

```
menuentry "Redemarrer" {  
    echo "Redemarrer le systeme..."  
    reboot  
}
```

```
}  
  
menuentry "Arreter le systeme" {  
    echo "Arret du systeme..."  
    halt  
}
```

Enregistrez et fermez le fichier.

Exécutez la commande suivante pour recréer le fichier de configuration GRUB.

```
root@hostname # grub2-mkconfig -o /boot/grub2/grub.cfg
```

Redémarrez votre machine et vérifiez si les modifications que vous avez apportées ont été faites.

#### D. Atelier 2 : Réinitialisation du mot de passe root

GRUB peut nous aider également à dépanner les systèmes d'exploitation. Il dispose d'une interface en ligne de commande, ayant pour invite (prompt) "**grub >**".

1. Pour accéder à cette interface Redémarrer votre système, au niveau du GRUB, sélectionner le système sur lequel vous souhaitez bouter et appuyer sur la touche « **e** ».

À partir de cette interface, vous pouvez réinitialiser le mot de passe oublié de l'utilisateur root en vous connectant au système d'exploitation en mode mono-utilisateur.

2. Chercher la commande linux permettant de charger le noyau, puis passez le paramètre **rd.break** au noyau. Le paramètre **rd.break** a pour effet d'interrompre le processus de démarrage avant que initramfs ne passe le contrôle à systemd.
3. Appuyez sur les touches **Ctrl+x** pour booter le noyau avec la configuration modifiée.
4. Une fois le Shell root est lancé, remontez le système de fichier **/sysroot** en lecture/écriture, puis faite un chroot de **/sysroot**.

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

5. Modifier le mot de passe root

```
#passwd
```

6. Configurez le système pour effectuer automatiquement un re-labellisation SELINUX après le démarrage, ceci est nécessaire car la commande passwd recrée **/etc/shadow** sans contexte SELinux.

```
#touch /.autorelabel
```

7. Quittez le Shell root, puis vérifiez la réinitialisation du mot de passe en ouvrant une session root.

### E. Atelier 3 : Protection de l'interface grub par mot de passe

Nous avons vu qu'à partir de l'interface de la ligne de commande de Grub, vous pouvez réinitialiser le mot de passe oublié de l'utilisateur root en vous connectant au système d'exploitation en mode mono-utilisateur. Vous pouvez aussi configurer le noyau d'un système d'exploitation particulier en fonction de vos besoins.

Donc il faut protéger le chargeur de démarrage avec un mot de passe pour les raisons suivantes :

- Prévenir les accès au mode utilisateur Single – Si un attaquant peut démarrer en mode single user, il devient l'utilisateur root.
- Prévenir les accès à la console GRUB – Si un attaquant parvient à utiliser la console GRUB, il peut changer sa configuration ou collecter des informations sur le système en utilisant la commande cat.
- Prévenir les accès à des systèmes d'exploitation non sécurisés. S'il y a un double boot sur le système, un attaquant peut sélectionner au démarrage un système d'exploitation comme DOS qui ignore les contrôles d'accès et les permissions des fichiers.

Exécutez la commande suivante pour générer le mot de passe GRUB pour l'utilisateur root :

```
root@hostname# grub2-setpassword  
Enter password:  
Confirm password:
```

Cette commande génère un mot de passe haché qui est stocké dans le fichier */boot/grub2/user.cfg*.

**Remarque :** par défaut, le fichier *user.cfg* n'existe pas. Si vous avez précédemment généré un mot de passe à l'aide de la commande `grub2-setpassword`, ce fichier existera, sinon cette commande générera un nouveau fichier.

```
root@hostname # cd /boot/grub2/  
root@hostname # ls  
device.map  fonts  grub.cfg  grubenv  i386-pc  user.cfg
```

Vous pouvez afficher le mot de passe généré à l'aide de la commande cat.

```
root@hostname# cat user.cfg  
GRUB2_PASSWORD=grub.pbkdf2.sha512.10000.9673E78A74C300135E39EB9CF4093448522  
D02E6CA8F72B92B9F46FB32C26FF78C6A5B299CB0156CF9F7EAA7AE20CDF374551424CFC896  
3E929962BD02098076.C14F44BDE163038AD59C7E93296112A777B4DBB1A55606142AB04B67  
C7AA255DF003E9316163687A4A7533EE4759E9237CB2EEE984A03F85A98A9144FAEE3172
```

Comme nous avons implémenté une nouvelle configuration, nous devons recréer le fichier de configuration GRUB.

Exécutez la commande suivante pour recréer le fichier de configuration GRUB.

```
root@hostname # grub2-mkconfig -o /boot/grub2/grub.cfg
```

Nous avons réussi à définir le mot de passe de grub2. Maintenant, nous devons redémarrer le système pour vérifier si le mot de passe est correctement défini.

Exécutez donc la commande suivante pour redémarrer le système.

```
root@hostname # reboot
```

Au niveau du GRUB, sélectionner le système sur lequel vous souhaitez booter et appuyer sur la touche « e ». Le login et le mot de passe grub vous seront alors demandés. Après avoir entré le nom d'utilisateur et le mot de passe corrects, vous pouvez éditer GRUB.

La suppression de la protection par mot de passe de GRUB est facile. Supprimez le fichier user.cfg en utilisant la commande suivante. C'est tout.

```
root@hostname # rm /boot/grub2/user.cfg  
rm: remove regular file '/boot/grub2/user.cfg'? y
```