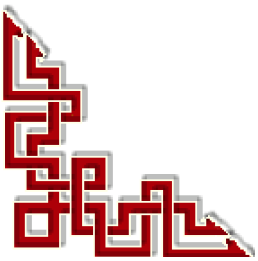
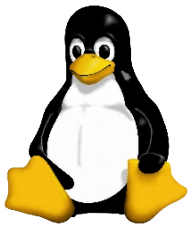
RF-232

Micronator

Serveur SME-9.x/8.x & Fail2ban





Version: 0.0.2 / mercredi 13 avril 2016 - 17:49

© RF-232, Montréal 16-2-11,
6447, avenue Jalobert, Montréal. Québec H1M 1L1

Tous droits réservés RF-232

Licence publique générale GNU

Permission vous est donnée de copier, distribuer et/ou modifier ce document selon les termes de la **Licence publique générale GNU**, version 3, 29 juin 2007, publiée par la Free Software Foundation Inc; sans section inaltérable, sans texte de première page de couverture et sans texte de dernière page de couverture. Une copie de cette licence est incluse dans la section **Licence publique générale GNU** de ce document, page**:** *27*.

AVIS DE NON-RESPONSABILITÉ

Ce document est uniquement destiné à informer. Les informations, ainsi que les contenus et fonctionnalités de ce document sont fournis sans engagement et peuvent être modifiés à tout moment. *RF-232* n'offre aucune garantie quant à l'actualité, la conformité, l'exhaustivité, la qualité et la durabilité des informations, contenus et fonctionnalités de ce document. L'accès et l'utilisation de ce document se font sous la seule responsabilité du lecteur ou de l'utilisateur.

RF-232 ne peut être tenu pour responsable de dommages de quelque nature que ce soit, y compris des dommages directs ou indirects, ainsi que des dommages consécutifs résultant de l'accès ou de l'utilisation de ce document ou de son contenu.

Chaque internaute doit prendre toutes les mesures appropriées (*mettre à jour régulièrement son logiciel antivirus, ne pas ouvrir des documents suspects de source douteuse ou non connue*) de façon à protéger le contenu de son ordinateur de la contamination d'éventuels virus circulant sur la Toile.

Avertissement

Bien que nous utilisions ici un vocabulaire issu des techniques informatiques, nous ne prétendons nullement à la précision technique de tous nos propos dans ce domaine.

Sommaire

I- Description générale....4
1. Introduction....4
2. Particularités de ce document....4
3. Commentaires et suggestions....5
4. Boutique de Micronator....5

II- Installation....6
1. Introduction....6
2. Systèmes requis....6
3. Installation....6
4. Signalisation d'une nouvelle configuration (fail2ban.conf)....9

III- Usage....10
1. Commande DB....10
2. Services....11
3. Bannissements sélectifs....12
4. Bannissements complets....12
5. Usage de Fail2ban....12
6. Script qui affiche tous les bannissements....12
7. Réintégration d'une adresse IP....14
8. Jail.conf....15
9. Désinstallation....17
10. Bogues....17
11. Toutes les commandes de Fail2ban....17
12. Le manuel original de Fail2ban....17

IV- Exemples de bannissements....18
1. Bannissement d'une adresse IP spécifique....18
2. Bannissement d'une plage d'adresses IP....19
3. Bannissement d'une semaine....19

V- Introduction à l'éditeur vi....21
1. Référence....21

Crédits....23

I- Description générale

1. Introduction

Ce document explique l'installation de la contrib **Fail2ban** sur un **Serveur SME-9.x** ou **SME-8.x**.

• Pour l'installation d'un **Serveur SME-9.1**, voir: **http://www.micronator.org/?page_id=236**.

Référence: **https://technique.arscenic.org/securite/article/fail2ban-limitation-des-tentatives**.

Fail2ban lit des fichiers journaux tels que **/var/log/auth.log** ou **/var/log/apache/error_log** et bannit les adresses **IP** qui ont obtenu un trop grand nombre d'échecs lors de l'authentification afin de limiter les tentatives de compromettre un serveur. Il met à jour les règles **iptables** pour rejeter cette adresse **IP**. Ces règles peuvent êtres définies par l'utilisateur dans un fichier de configuration. **Fail2ban** peut lire plusieurs fichiers journaux tels ceux du démon **sshd** ou du serveur **Apache**.

2. Particularités de ce document

2.1. Notes au lecteur

* Les captures d'écrans ne sont que des références.

** Les informations écrites ont préséance sur celles retrouvées dans les captures d'écrans. Veiller à se référer aux différents tableaux lorsque ceux-ci sont présents.

2.2. Conventions

Toutes les commandes à entrer à la console sont en **gras**. Les affichages à surveiller sont en **rouge**, **bleu**, **orange** ou **magenta**.

```
# ping 192.168.1.149
192.168.1.149 is alive
#
```

Les liens de référence Internet sont en **bleu** et ceux intra document en ***bleu***.


Manipulation, truc ou ruse pour se tirer d'embarras.


Une recommandation ou astuce.


Une note.


Une étape, note ou procédure à surveiller.


Paragraphe non complété ou non vérifié.


Cette icône indique que cette commande est sur une seule ligne. Le **PDF** la mettra sur deux lignes avec un [**CR**] [**LF**] entre les deux. Il faudra donc copier la commande entière dans un éditeur de texte ASCII et la mettre sur une seule ligne avant de la copier à la console.

3. Commentaires et suggestions

RF-232 apprécie énormément échanger avec ses internautes. Vos commentaires et suggestions sont indispensables à l'amélioration de la documentation et du site **micronator.org**.

N'hésitez pas à nous transmettre vos commentaires et à nous signaler tout problème d'ordre technique que vous avez rencontré ou n'arrivez pas à résoudre. Tous vos commentaires seront pris en considération et nous vous promettons une réponse dans les plus brefs délais.

Brancher les aînés,
encourager l'Informatique Libre
et la diffusion du savoir

4. Boutique de Micronator

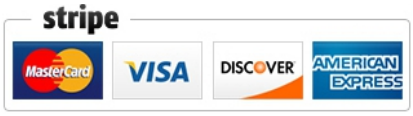
Nous sommes heureux de vous présenter notre nouvelle boutique en ligne dans laquelle vous trouverez certains de nos produits qui ne sont pas disponibles sur notre site principal. Nous vous laissons le plaisir de parcourir notre boutique **https://www.micronator.org/?post_type=product**.

Communications sécuritaires chiffrées SSL

Les communiquons avec **Stripe** et **PayPal** sont effectuées au moyen d'un **certificat SSL de 2048** bits émis par l'Autorité de Certification **Let's Encrypt**.

Faites vos achats, remplissez votre panier et réglez votre commande avec la carte bancaire de votre choix, **MasterCard**, **Visa**, **Discover**, **American Express**, etc…

Stripe



Vos données sont directement envoyées à **Stripe** qui s'occupe de tout et votre carte n'est pas conservée sur notre site. Les paiements sont sécurisés par le système **Stripe**. Cliquez ici pour voir les étapes de paiements; celles-ci sont sécurisées par le système **Stripe**.

PayPal

Il n'est pas nécessaire d'ouvrir un compte **PayPal**. Vous pouvez choisir la carte bancaire que vous désirez utiliser. Cliquez ici pour voir les étapes de paiements; celles-ci sont sécurisées par le système **PayPal**.

II- Installation

1. Introduction

Ce document est une adaptation de la contrib ci-dessous.

Référence: **https://wiki.contribs.org/Fail2ban** et **https://wiki.contribs.org/Fail2ban/fr**.

Fail2ban fonctionne en surveillant les fichiers journaux (***/var/log/pwdfail***, ***/var/log/auth.log***, *etc...*). Le plus souvent il est utilisé pour bloquer des adresses **IP** sélectionnées qui peuvent appartenir à des hôtes tentant de compromettre la sécurité du système. **Fail2ban** peut interdire une adresse **IP** d'un l'hôte qui tente trop de tentatives de connexion ou toute autre action non désirée dans un laps de temps défini par l'administrateur.

Par défaut, après l'installation de **Fail2ban**, les services de base les plus importants sont surveillés sans aucun besoin de configuration manuelle.

Fail2ban n'est pas seulement un outil contre les attaques par force brute sur **SSH**, il peut aussi être utile contre les attaques de protocole **http** ou **spam** sur votre serveur.

2. Systèmes requis

Cette contrib a été développée et vérifiée sur un **Serveur SME-9.x** et **SME-8.x**. Elle ne fonctionnera probablement pas sur un **Serveur SME-7.x**.

3. Installation

Configurez le dépôt de logiciels **Firewall-Services**.

```
[root@coquille-9 ~]# db yum_repositories set fws repository                          \
                        BaseURL http://repo.firewall-services.com/centos/\$releasever \
                        EnableGroups no GPGCheck yes                                  \
                        Name "Firewall Services"                                      \
                        GPGKey http://repo.firewall-services.com/RPM-GPG-KEY          \
                        Visible yes status disabled

[root@coquille-9 ~]#
```

3.1. Configurez le dépôt de logiciels EPEL

3.1.1. Serveur SME 9.x

```
[root@coquille-9 ~]# /sbin/e-smith/db yum_repositories set epel repository           \
     Name 'Epel - EL6'                                                               \
     BaseUrl 'http://download.fedoraproject.org/pub/epel/6/$basearch'                \
     MirrorList 'http://mirrors.fedoraproject.org/mirrorlist?repo=epel-6&arch=$basearch' \
     EnableGroups no                                                                 \
     GPGCheck yes                                                                    \
     GPGKey http://dl.fedoraproject.org/pub/epel/RPM-GPG-KEY-EPEL                    \
     Visible no                                                                      \
     status disabled

[root@coquille-9 ~]#
```

On vérifie.

```
[root@coquille-9 ~]# db yum_repositories show epel

epel=repository
    BaseUrl=http://download.fedoraproject.org/pub/epel/6/$basearch
    EnableGroups=no
    GPGCheck=yes
    GPGKey=http://dl.fedoraproject.org/pub/epel/RPM-GPG-KEY-EPEL
    MirrorList=http://mirrors.fedoraproject.org/mirrorlist?repo=epel-6&arch=$basearch
    Name=Epel - EL6
    Visible=no
    status=disabled
[root@coquille-9 ~]#
```

3.1.2. Serveur SME 8.x

```
[root@coquille-8 ~]# /sbin/e-smith/db  yum_repositories set epel repository             \
     Name 'Epel - EL5'                                                                  \
     BaseUrl 'http://download.fedoraproject.org/pub/epel/5/$basearch'                   \
     MirrorList 'http://mirrors.fedoraproject.org/mirrorlist?repo=epel-5&arch=$basearch' \
     EnableGroups no                                                                    \
     GPGCheck yes                                                                       \
     GPGKey http://dl.fedoraproject.org/pub/epel/RPM-GPG-KEY-EPEL                       \
     Visible no                                                                         \
     status disabled

[root@coquille-8 ~]#
```

3.1.3. Serveur SME 8.x

On vérifie.

```
[root@coquille-8 ~]# db yum_repositories show epel

epel=repository
    BaseUrl=http://download.fedoraproject.org/pub/epel/5/$basearch
    EnableGroups=no
    GPGCheck=yes
    GPGKey=http://dl.fedoraproject.org/pub/epel/RPM-GPG-KEY-EPEL
    MirrorList=http://mirrors.fedoraproject.org/mirrorlist?repo=epel-5&arch=$basearch
    Name=Epel - EL5
    Visible=no
    status=disabled
[root@coquille-8 ~]#
```

3.2. Signalisation de la modification de la config de yum

```
[root@coquille-9 ~]# signal-event yum-modify

[root@coquille-9 ~]#
```

3.3. Installation des RPMS

```
[root@coquille-9 ~]# yum --enablerepo=fws --enablerepo=epel install smeserver-fail2ban

Modules complémentaires chargés : fastestmirror, smeserver
Configuration du processus d'installation
Loading mirror speeds from cached hostfile
...
epel                                                      | 4.3 kB     00:00
epel/primary_db                                           | 5.8 MB     00:03
fws                                                       | 2.5 kB     00:00
fws/primary_db                                            | 199 kB     00:00
```

```
Résolution des dépendances
...
--> Résolution des dépendances terminée

Dépendances résolues

================================================================================
 Paquet                  Architecture   Version                    Dépôt      Taille
================================================================================
Installation:
 smeserver-fail2ban      noarch         9:0.1.12-1.el6.fws         fws         24 k
Installation pour dépendance:
 fail2ban                noarch         0.9.3-1.el6.1              epel       419 k
...
 python-inotify          noarch         0.9.1-1.el6                epel        50 k

Résumé de la transaction
================================================================================
Installation de     6 paquet(s)

Taille totale des téléchargements : 610 k
Taille d'installation : 1.9 M
Est-ce correct [o/N] : O
Téléchargement des paquets :
(1/6): fail2ban-0.9.3-1.el6.1.noarch.rpm                  | 419 kB     00:00
...
(6/6): smeserver-fail2ban-0.1.12-1.el6.fws.noarch.rpm     |  24 kB     00:00
--------------------------------------------------------------------------------
Total                                              321 kB/s | 610 kB     00:01
warning: rpmts_HdrFromFdno: Header V4 DSA/SHA1 Signature, key ID 7cb6de2c: NOKEY
Retrieving key from http://repo.firewall-services.com/RPM-GPG-KEY
Importing GPG key 0x7CB6DE2C:
 Userid: "Firewall Services Repo <rpms@firewall-services.com>"
 From  : http://repo.firewall-services.com/RPM-GPG-KEY
Est-ce correct [o/N] : O
Lancement de rpm_check_debug
...
  Installation  : libmnl-1.0.2-3.el6.x86_64                                 1/6
...
  Installation  : 9:smeserver-fail2ban-0.1.12-1.el6.fws.noarch              6/6
Migrating existing database accounts
...
Migrating existing database hosts
  Verifying     : fail2ban-0.9.3-1.el6.1.noarch                             1/6
...
  Verifying     : libmnl-1.0.2-3.el6.x86_64                                 6/6

Installé:
  smeserver-fail2ban.noarch 9:0.1.12-1.el6.fws

Dépendance(s) installée(s) :
  fail2ban.noarch 0:0.9.3-1.el6.1              gamin-python.x86_64 0:0.1.10-9.el6
  ipset.x86_64 0:6.11-4.el6                    libmnl.x86_64 0:1.0.2-3.el6
  python-inotify.noarch 0:0.9.1-1.el6

Terminé !

================================================================
WARNING: You now need to run BOTH of the following commands
to ensure consistent system state:

signal-event post-upgrade; signal-event reboot

You should run these commands unless you are certain that
yum made no changes to your system.
================================================================
[root@coquille-9 ~]#
```

4. Signalisation d'une nouvelle configuration (*fail2ban.conf*)

On a le choix de signaler la nouvelle configuration avec ou sans réamorçage du serveur.

À défaut d'exécuter l'un de ces blocs de commandes, l'accès au réseau sera verrouillé le temps de recharger les règles d'**iptables**.

Le démon[1] de masquage d'adresses **IP (*masq daemon*)** doit être activé pour que **Fail2ban** puisse fonctionner correctement; si on désactive ce démon, **Fail2ban** ne bannira rien.

On active le démon de masquage.

```
[root@coquille-9 ~]# db configuration setprop masq status enabled

[root@coquille-9 ~]#
```

On effectue seulement un des deux blocs ci dessous.

4.1. SANS RÉAMORÇAGE

On étend le gabarit du démon de masquage.

```
[root@coquille-9 ~]# expand-template /etc/rc.d/init.d/masq

[root@coquille-9 ~]#
```

On repart le démon de masquage.

```
[root@coquille-9 ~]# /etc/init.d/masq restart

Shutting down IP masquerade and firewall rules:         Done!

Enabling IP masquerading: done
[root@coquille-9 ~]#
```

On signale la nouvelle configuration.

```
[root@coquille-9 ~]# signal-event fail2ban-conf

[root@coquille-9 ~]#
```

4.2. AVEC RÉAMORÇAGE

```
[root@coquille-9 ~]# signal-event post-upgrade; signal-event reboot

Broadcast message from root@coquille-9
        (/dev/pts/0) at 2:23 ...

The system is going down for reboot NOW!
[root@coquille-9 ~]#
```

1 **Référence**: http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=2069962.
Un programme démon, normalement lancé au démarrage du système, est inoffensif et réside en mémoire en attente des requêtes. Il s'exécute lorsqu'une requête concerne le port sur lequel il est en veille. Parmi les fonctions dont il est chargé, on peut mentionner: le routage et la distribution du courrier électronique (***sendmail***), la gestion des connexions réseaux (***inetd***) et l'impression en tâche de fond (***lpd***). Généralement, le nom du programme démon se termine par **d** ou **.d**.
Chaque serveur Web a un démon **httpd** (***H**yper**T**ext **T**ransfer **P**rotocol **D**aemon*) qui attend continuellement les requêtes provenant des clients Web et de leurs utilisateurs.

III- Usage

1. Commande DB

Il n'existe pas de panneau de configuration pour **Fail2ban** dans le gestionnaire **Server Manager**. Toutefois, on peut gérer cette contrib avec **db configuration**.

On affiche la configuration de **Fail2ban**.

```
[root@coquille-9 ~]# config show fail2ban

fail2ban=service
    Mail=enabled
    status=enabled
[root@coquille-9 ~]#
```

1.1. Options disponibles

- **IgnoreIP**: listes d'adresses **IP** ou de sous-réseaux, en notation **CIDR**, qui ne seront jamais bloquées par **Fail2ban**. Une virgule sépare les adresses. Exemple: **12.15.22.4**,**17.20.0.0/16**. Tous vos réseaux locaux et les réseaux autorisés à accéder au gestionnaire du serveur (***Server Manager*** | ***Accès à distance*** | ***Gestion à distance***) sont toujours automatiquement mis sur la liste blanche.
- **FilterLocalNetworks**: peut être activé ou désactivé (*désactivé par défaut*). Si activé, les réseaux locaux ne seront pas mis sur la liste blanche et **Fail2ban** pourra ainsi bannir des hôtes du réseau interne. Les réseaux autorisés à accéder au gestionnaire du serveur ne seront pas affectés (*ils ne seront jamais bloqués*).
- **BanTime**: durée (*en secondes*) d'un bannissement. Par défaut: **1800**.
- **FindTime**: fenêtre de vérification de **Fail2ban**, en secondes. Par défaut: **900**. Signifie que **Fail2ban** vérifiera seulement le nombre de connexions échouées ou tentées durant les **15** dernières minutes (*900 secondes*).
- **MaxRetry**: nombre de tentatives échouées dans les dernières **FindTime** secondes pour déclencher un bannissement. Par défaut: **3**.
- **Mail**: peut être activé ou désactivé (*activé par défaut*). S'il est activé, chaque bannissement sera notifié par courriel.
- **MailRecipient**: si **Mail** est activé, l'adresse du courriel qui recevra les notifications de bannissement. Par défaut: **root** (*le compte **"admin"** recevra les courriels*).

Après avoir changé l'un de ces paramètres, vous devez le signaler à l'aide de la commande suivante:

```
signal-event fail2ban-conf
```

1.1.1. Exemple

Si on veut mettre une adresse **IP** particulière ainsi qu'un sous-réseau sur la liste blanche, on lance la commande:

```
config setprop fail2ban IgnoreIP 12.15.22.4,17.20.0.0/16
```

Il faut signaler la modification.

```
signal-event fail2ban-conf
```

La commande **signal-event fail2ban-conf** redémarre effectivement le service et efface les bannissements existants. Un changement de **findtime** résulte en un rebalayage des fichiers journaux pour refaire le bannissement; ce rebalayage peut être assez long et prendre beaucoup de temps processeur.

2. Services

Les services suivants sont surveillés et **Fail2ban** interdira les adresses **IP** pour la durée **BanTime** si plus de **MaxRetry** d'échecs d'authentification se produisent en moins de **FindTime**.

- **ssh**
- **dovecot**: (*seulement avec **SME-9** ou si on utilise* **smeserver-dovecot**)
- **qpsmtpd**: si un serveur externe vous envoie trop de courriels que rejette **Fail2ban**, c'est que c'est probablement un polluposteur et **Fail2ban** va le mettre sur la liste noire. **MaxRetry** est de **x3** pour ce service; ainsi avec la configuration par défaut, un serveur externe va être mis sur la liste noire si **9** courriels sont rejetés en deça de **15** minutes.
- **httpd-e-smith**: le serveur standard de **http**. Trois différents filtres vérifient les journaux du serveur **Apache**.

  noscripts: vérifie le client qui demande de rouler des scripts qui ne sont pas disponibles sur le serveur. Habituellement, c'est un pirate adolescent (*script-kiddy*) qui essaie d'exploiter des failles de vulnérabilité.

  scan: un autre jeu de filtre pour les balayages populaires (*phpMyAdmin, wp-login, zone admin, etc...*).

  auth: va vérifier les défaillances d'authentification standards.
- **pam**: va vérifier les défaillances d'authentification génériques. Tout ce qui utilise **pam** devrait fonctionner.
- **SOGo**: vérifie les journaux de **SOGo** pour des défaillances d'authentification.
- **LemonLDAP-NG**: vérifie les journaux système pour les défaillances d'authentification au portail **LemonLDAP::NG**.
- **ftp**: vérifie les défaillances d'authentification au démon **FTP**.
- **Ejabberd**: vérifie les défaillances d'authentification à **ejabberd**.

Chaque filtre se désactive automatiquement si le service correspondant est désactivé.

2.1. Filtre spécifique

Vous pouvez également désactiver un filtre spécifique.

Exemple, si vous souhaitez désactiver les filtres **Apache**.

```
db configuration setprop httpd-e-smith Fail2Ban disabled
```

Puis, il faut signaler le changement de la configuration.

```
signal-event fail2ban-conf
```

3. Bannissements sélectifs

Fail2ban fera de son mieux pour effectuer une interdiction sélective.

3.1. Exemple

Si 3 échecs d'authentification **SSH** sont détectés, seul le port **TCP 22** (*ou tout autre port vous avez choisi pour **SSH***) sera bloqué pour l'adresse **IP** fautive. Idem pour **httpd-e-smith**, **SOGo**, **LemonLDAP::NG** bloquera les ports **TCP 80** et **443**, **qpsmtpd** bloquera les ports **TCP 25** et **465**, **dovecot** bloquera **143** et **993**, etc...

4. Bannissements complets

Il existe seulement deux façons de bannir complètement tous les ports/protocoles pour une adresse **IP** fautive:

- **pam** Comme il s'agit d'un fichier générique, il n'est pas possible de vérifier où le service a été utilisé lors d'un échec d'authentification, donc l'ensemble de l'**IP** du client sera mis en liste noire.
- **recidive** Il s'agit d'un filtre spécial. Il surveille les journaux **Fail2Ban** et met sur la liste noire l'adresse **IP** du client qui se fait verrouillée plusieurs fois. Si un client est bloqué **5** fois en **24** heures, il sera mis sur la liste noire pour une semaine complète.

5. Usage de Fail2ban

5.1. Affichage de toutes les prisons

```
[root@coquille-9 ~]# fail2ban-client status

Status
|- Number of jail:      13
`- Jail list:   http-auth, http-badbots, http-fakegooglebot, http-noscript, http-overflows,
http-scan, http-shellshock, imap, pam-generic, qpsmtpd, recidive, ssh, ssh-ddos
[root@coquille-9 ~]#
```

5.2. Affichage des adresses IP bannies d'une prison spécifique

```
[root@coquille-9 ~]# fail2ban-client status ssh

Status for the jail: ssh
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:        /var/log/sshd/current
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[root@coquille-9 ~]#
```

6. Script qui affiche tous les bannissements

Le script ci dessous affichera le nombre total de tous les bannissements de toutes les prisons

On crée le fichier dans le répertoire **/root**.

On se rend donc dans le répertoire de l'usager **root**.

```
[root@coquille-9 ~]# cd

[root@coquille-9 ~]#
```

On vérifie.

```
[root@coquille-9 ~]# pwd

/root
[root@coquille-9 ~]#
```

On crée le fichier.

```
[root@coquille-9 ~]# touch checklist_ban.sh

[root@coquille-9 ~]#
```

On ajuste les droits.

```
[root@coquille-9 ~]# chmod 700 checklist_ban.sh

[root@coquille-9 ~]#
```

On vérifie.

```
[root@coquille-9 ~]# ls -alsd checklist_ban.sh

0 -rwx------ 1 root root 0 11 févr. 07:22 checklist_ban.sh
[root@coquille-9 ~]#
[root@coquille-9 ~]#
```

On édite avec l'éditeur **vi**.

```
 vi checklist_ban.sh
```

On entre ce qui suit dans le fichier qu'on vient d'ouvrir.

```
#!/bin/bash
#lancer le script en sudo
JAILS=$(fail2ban-client status | grep " Jail list:" | sed 's/`- Jail list://g' | sed
's/,//g')
for j in $JAILS
do
echo "$j $(fail2ban-client status $j | grep " Currently banned:" | sed 's/   |- Currently
banned:\t//g')"
done
```

On ferme le fichier. On appuie sur la touche [**ESC**] pour entrer en mode commande, puis on entre ce qui suit.

```
:wq
```

On vérifie.

```
[root@coquille-9 ~]# cat checklist_ban.sh

#!/bin/bash
#lancer le script en sudo
JAILS=$(fail2ban-client status | grep " Jail list:" | sed 's/`- Jail list://g' | sed
's/,//g')
for j in $JAILS
do
echo "$j $(fail2ban-client status $j | grep " Currently banned:" | sed 's/   |- Currently
banned:\t//g')"
done
[root@coquille-9 ~]#
```

On lance le script pour vérifier son fonctionnement.

```
[root@coquille-9 ~]# ./checklist_ban.sh

http-auth 0
http-badbots 0
http-fakegooglebot 0
http-noscript 0
http-overflows 0
http-scan 0
http-shellshock 0
imap 0
pam-generic 0
qpsmtpd 1
recidive 0
ssh 0
ssh-ddos 0
[root@coquille-9 ~]#
```

Le script fonctionne parfaitement.

7. Réintégration d'une adresse IP

Dans certains cas, vous pouvez réintégrer une adresse **IP** immédiatement si vous ne voulez pas attendre le processus automatique de réintégration de **Fail2ban**.

- Vous devez trouver la prison spécifique qui a bloqué l'adresse **IP**. Pour ce faire, vous pouvez vous référer au courriel reçu par l'utilisateur **admin**.
- Ou vous pouvez afficher une prison spécifique.

```
[root@coquille-9 ~]# fail2ban-client status qpsmtpd

Status for the jail: qpsmtpd
|- Filter
|  |- Currently failed: 4
|  |- Total failed:     99
|  `- File list:        /var/log/sqpsmtpd/current /var/log/qpsmtpd/current
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   123.123.123.123
[root@coquille-9 ~]#
```

On utilise la commande suivante pour réintégrer l'adresse **IP**.

```
[root@coquille-9 ~]# fail2ban-client set qpsmtpd unbanip 123.123.123.123

[root@coquille-9 ~]#
```

La commande générique est la suivante.

```
fail2ban-client set PRISON unbanip ADRESSE_IP
```

Si on veut connaître toutes les prisons actives.

```
[root@coquille-9 ~]# fail2ban-client status

Status
|- Number of jail:      13
`- Jail list:   http-auth, http-badbots, http-fakegooglebot, http-noscript, http-overflows,
http-scan, http-shellshock, imap, pam-generic, qpsmtpd, recidive, ssh, ssh-ddos
[root@coquille-9 ~]#
```

8. Jail.conf

À faire seulement si on veut configurer d'une manière spéciale et très spécifique avec un gabarit personnalisé.

Le fichier de configuration **jail.conf** est basé sur le gabarit **/etc/e-smith/templates/etc/fail2ban/jail.conf** et le fichier par défaut contient la configuration comme ci-dessous. Vous pouvez ajouter votre propre gabarit **template-custom** pour **jail.conf** dans le répertoire des gabarits personnalisés **/etc/e-smith/templates-custom/etc/** en y créant le répertoire **fail2ban/jail.conf**.

Le chemin complet de votre gabarit personnalisé sera: **/etc/e-smith/templates-custom/etc/ fail2ban/jail.conf/**.

Si c'est la première fois, on doit créer le dossier du gabarit personnalisé.

```
[root@coquille-9 ~]# mkdir -p  /etc/e-smith/templates-custom/etc/fail2ban/jail.conf

[root@coquille-9 ~]#
```

On vérifie.

```
[root@coquille-9 ~]# ls -alsd /etc/e-smith/templates-custom/etc/fail2ban/jail.conf

4 drwxr-xr-x 2 root root 4096 11 févr. 08:03 /etc/e-smith/templates-custom/etc/fail2ban/jail.conf
[root@coquille-9 ~]#
```

On déploie le gabarit.

```
[root@coquille-9 ~]# expand-template /etc/rc.d/init.d/masq

[root@coquille-9 ~]#
```

On repart le démon **masq**.

```
[root@coquille-9 ~]# /etc/init.d/masq restart


Shutting down IP masquerade and firewall rules:         Done!

Enabling IP masquerading: done
[root@coquille-9 ~]#
```

On signale la modification de la configuration. (*Peut prendre quelques secondes.*)

```
[root@coquille-9 ~]# signal-event fail2ban-conf

[root@coquille-9 ~]#
```

8.1. Le fichier *jail.conf* par défaut

On peut toujours se référer aux fichiers du gabarit standard de **Fail2ban** dans les contenus des sous-répertoires: **/etc/e-smith/templates/etc/fail2ban/fail2ban.conf**.

Les fichiers actifs, lorsque le gabarit standard de **Fail2ban** est lu lors de l'amorçage du serveur, sont dans le répertoire: **/etc/fail2ban**.

Le fichier **jail.conf** sera situé dans le répertoire de votre gabarit i.e. **fail2ban/jail.conf/jail.conf**. Il commence toujours par le paragraphe **[DEFAULT]** suivi d'un paragraphe pour chacun des services surveillés par **Fail2-ban**.

Votre **réseau** et votre **serveur** sont dans la liste des adresses **IP** ignorées par **Fail2ban** (*voir **IgnoreIP** au paragraphe **Options disponibles** à la page **10***).

```
[DEFAULT]
ignoreip = 127.0.0.0/8,192.168.1.1,192.168.1.0/24
bantime  = 1800
findtime  = 900
maxretry = 3
usedns = yes
backend = auto
```

Les différents services qu'on peut ajouter au fichier **jail.conf**. Un paragraphe par service.

```
[ssh]
enabled  = true
filter   = sshd
logpath  = /var/log/sshd/current
action   = smeserver-iptables[port="22",protocol=tcp,bantime=1800]
           smeserver-sendmail[name="SSH",dest=root]
```

```
[ssh-ddos]
enabled  = true
filter   = sshd-ddos
logpath  = /var/log/sshd/current
action   = smeserver-iptables[port="22",protocol=tcp,bantime=1800]
           smeserver-sendmail[name="SSH",dest=root]
```

```
[qpsmtpd]
enabled  = true
filter   = qpsmtpd
logpath  = /var/log/*qpsmtpd/current
maxretry = 9
action   = smeserver-iptables[port="25,465",protocol=tcp,bantime=1800]
           smeserver-sendmail[name="Qpsmtpd",dest=root]
```

```
[http-overflows]
enabled  = true
filter   = apache-overflows
logpath  = /var/log/httpd/error_log
action   = smeserver-iptables[port="80,443",protocol=tcp,bantime=1800]
           smeserver-sendmail[name="Apache (overflows)",dest=root]
```

```
[http-noscript]
enabled  = true
filter   = apache-noscript
logpath  = /var/log/httpd/error_log
action   = smeserver-iptables[port="80,443",protocol=tcp,bantime=1800]
           smeserver-sendmail[name="Apache (noscript)",dest=root]
```

```
[http-scan]
enabled  = true
filter   = apache-scan
logpath  = /var/log/httpd/error_log
action   = smeserver-iptables[port="80,443",protocol=tcp,bantime=1800]
           smeserver-sendmail[name="Apache (scan)",dest=root]
```

```
[http-auth]
enabled  = true
filter   = apache-auth
logpath  = /var/log/httpd/error_log
action   = smeserver-iptables[port="80,443",protocol=tcp,bantime=1800]
           smeserver-sendmail[name="Apache (auth)",dest=root]
```

```
[pam-generic]
enabled  = true
filter   = pam-generic
logpath  = /var/log/secure
maxretry = 6
action   = smeserver-iptables[bantime=1800]
           smeserver-sendmail[name="PAM generic",dest=root]
```

```
[recidive]
enabled  = true
filter   = recidive
logpath  = /var/log/fail2ban/daemon.log
bantime  = 604800
findtime = 86400
maxretry = 5
backend  = polling
action   = smeserver-iptables[bantime=604800]
           smeserver-sendmail[name="Recidive",dest=root]
```

9. Désinstallation

Il suffit de lancer la commande suivante pour désinstaller **Fail2ban**.

```
yum remove smeserver-fail2ban fail2ban
```

10. Bogues

S'il vous plaît, rapportez les bogues dans la section **SME-Contribs** de **bugzilla** et sélectionnez le composant **smeserver-fail2ban** ou utilisez **ce lien**.

Aperçu ci-dessous des problèmes actuels de cette contrib.

ID	Product	Version	Status	Summary (2 tasks
8763	SME Contribs	9.0	CONFIRMED	WARNING 'ignoreregex' not defined in 'Definition'. Using default one.
8645	SME Contribs	8.1	UNCONFIRMED	AuthExtern pwauth failures not been logged by fail2ban jail http-auth

11. Toutes les commandes de Fail2ban

Voir: **http://www.fail2ban.org/wiki/index.php/Commands**.

12. Le manuel original de Fail2ban

Voir: **http://www.fail2ban.org/wiki/index.php/MANUAL_0_8**.

IV- Exemples de bannissements

1. Bannissement d'une adresse IP spécifique

Quelquefois, il est préférable de bannir une adresse spécifique pour arrêter de recevoir des courriels d'un pollu-posteur.

Dans **Thunderbird**, on sélectionne le courriel | **Affichage** | **Code source du message**.

```
X-Spam-Level: ******
X-Spam-Status: Yes, hits=6.9 required=5.0

tests=AXB_JT_FOLNO0,HTML_MESSAGE,MIME_QP_LONG_LINE,RAZOR2_CF_RANGE_51_100,RAZOR2_CF_RANGE_E8
_51_100,RAZOR2_CHECK,RCVD_IN_DNSWL_LOW
X-Spam-Flag: YES
X-Spam-Check-By: micronator.org
Received: from smtp13.macau.ctm.net (HELO zimbramta07.macau.ctm.net) (125.31.5.33)
    by micronator.org (qpsmtpd/0.84) with (AES256-GCM-SHA384 encrypted) ESMTPS; Mon, 08 Feb
2016 03:38:39 -0500
```

Comme on le voit ci-dessus, **SpamAssassin** a donné un statut de **6.9** à ce courriel.

1.1. Bannissement

On bloque cette adresse dans la prison **qpsmtpd**.

```
[root@coquille-9 ~]# fail2ban-client set qpsmtpd banip 125.31.5.33

125.31.5.33
[root@coquille-9 ~]#
```

On vérifie.

```
[root@coquille-9 ~]# fail2ban-client status qpsmtpd

Status for the jail: qpsmtpd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     12
|  `- File list:        /var/log/sqpsmtpd/current /var/log/qpsmtpd/current
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   125.31.5.33
[root@coquille-9 ~]#
```

2. Bannissement d'une plage d'adresses IP

On fait une recherche de l'adresse **125.31.5.33** sur **http://www.monwhois.fr/**.

```
...
Lookup results for 125.31.5.33 from whois.lacnic.net server:

inetnum:        125.31.0.0 - 125.31.63.255
...
address:        Rua da Lagos, Telecentro
address:        P.O. Box 868
address:        Taipa
address:        Macau
e-mail:         noc@macau.ctm.net
...
route:          125.31.5.0/24
...
```

Route spécifie **125.31.5.0/24**

2.1. Bannissement

On ne connaît personne à Macau. Nous allons donc bannir toute cette plage d'adresses pour les courriels (*prison **qpsmtpd***).

```
[root@coquille-9 ~]# fail2ban-client set qpsmtpd banip 125.31.5.33/24

125.31.5.33/24
[root@coquille-9 ~]#
```

On vérifie.

```
[root@coquille-9 ~]# fail2ban-client status qpsmtpd

Status for the jail: qpsmtpd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     24
|  `- File list:        /var/log/sqpsmtpd/current /var/log/qpsmtpd/current
`- Actions
   |- Currently banned: 1
   |- Total banned:     2
   `- Banned IP list:   125.31.5.33/24
[root@coquille-9 ~]#
```

3. Bannissement d'une semaine

Si on veut bannir pour un peu plus longtemps, une semaine, on peut utiliser la prison **recidive**; voir le paragraphe ***Bannissements complets*** à la page ***12***.

On vérifie que la prison **recidive** est active,

```
[root@coquille-9 ~]# fail2ban-client status

Status
|- Number of jail:      13
`- Jail list:   http-auth, http-badbots, http-fakegooglebot, http-noscript, http-overflows,
http-scan, http-shellshock, imap, pam-generic, qpsmtpd, recidive, ssh, ssh-ddos
[root@coquille-9 ~]#
```

3.1. Bannissement

On bannit la plage d'adresses **IP** du paragraphe précédent pour une semaine dans la prison **recidive**.

```
[root@coquille-9 ~]# fail2ban-client set recidive banip 125.31.5.33/24

125.31.5.33/24
[root@coquille-9 ~]#
```

On vérifie.

```
[root@coquille-9 ~]# fail2ban-client status recidive

Status for the jail: recidive
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     39
|  `- File list:        /var/log/fail2ban/daemon.log
`- Actions
   |- Currently banned: 3
   |- Total banned:     3
   `- Banned IP list:   162.213.152.92 66.131.226.189 125.31.5.33/24
[root@coquille-9 ~]#
```

3.2. Affichage de toutes le prisons

```
[root@coquille-9 ~]# ./checklist_ban.sh

ftp 0
http-auth 0
http-badbots 0
http-fakegooglebot 0
http-noscript 0
http-overflows 0
http-scan 0
http-shellshock 0
imap 0
pam-generic 0
qpsmtpd 1
recidive 3
ssh 0
ssh-ddos 0
[root@coquille-9#
```

V- Introduction à l'éditeur vi

1. Référence

http://www.iro.umontreal.ca/~dift3830/vi.html.

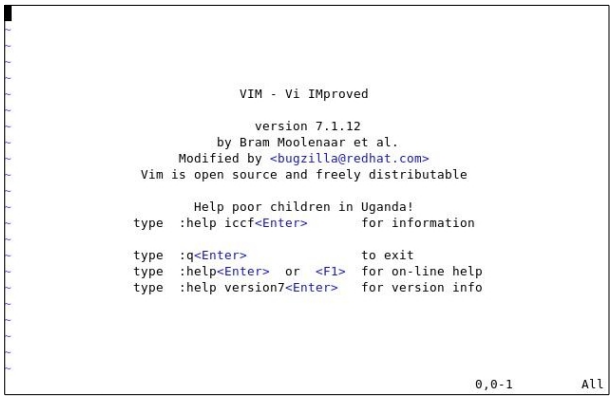
vi est un éditeur de texte très puissant. Sa convivialité par contre lui fait défaut. Ceci dit, il est toujours utile d'en connaître les rudiments, car son omniprésence est presque garantie sur les systèmes modernes.

La documentation de **vi** étant très abondante, on se limitera pour cette démo aux commandes les plus usuelles.

Tout d'abord l'invocation. On peut invoquer **vi** à partir du shell de plusieurs façons dont voici quelques unes:

- **vi**: ouvre **vi** avec un contenu vide.
- **vi nom_de_fichier**: ouvre un fichier et l'affiche à l'écran.
- **vi +nom_de_fichier**: ouvre un fichier et positionne le curseur à la fin de celui-ci.

Dès son invocation, **vi** se met en **mode commande**. Dans ce mode, il est possible d'entrer les commandes qui seront vues plus bas. Si on tape une commande susceptible de modifier un texte (*insertion d'un caractère par exemple*), **vi** bascule en **mode édition**; dans ce mode tous caractère tapé sera considéré comme faisant partie du texte, tandis que les caractères saisis en **mode commande**, seront eux interprétés comme étant des commandes et ne seront jamais rajoutés au texte.



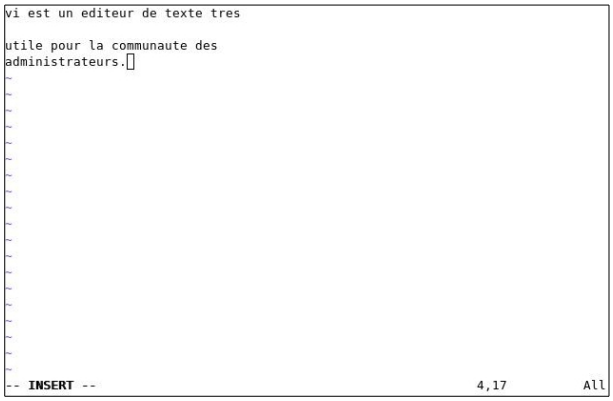
Afin de basculer du **mode édition** au **mode commande** il suffit de presser la touche [**Esc**].

Nous allons commencer par invoquer **vi** à partir du **shell** en tapant:

vi

Ce qui devrait donner l'affichage ci-contre:

vi est déjà en **mode commande**, pour le faire passer en **mode édition**, on tapera la commande **i** (*insert*) qui nous permettra d'**i**nsérer du texte.



Après avoir tapé le texte suivant:

```
"vi est un éditeur de texte très

utile pour la communauté des
administrateurs."
```

On obtiendra l'affichage ci-contre.

En **mode insertion**, on peut passer en **mode commande** par simple pression sur la touche [**Esc**].

Une fois en **mode commande** on voudrait par exemple, éliminer la ligne blanche qui se trouve juste après la première. On positionne alors le curseur à la hauteur de la 2e ligne et on tape **dd**.

Ceci aura pour effet de supprimer la ligne.

Les commandes abondent dans **vi**; c'est pourquoi on n'en citera que quelques unes.

Si on est satisfait il ne nous reste plus qu'à sauvegarder le document sous le nom **texte1.txt** à l'aide de la commande suivante:

```
:w texte1.txt
```

(*Pour les sauvegardes ultérieures, il n'est pas nécessaire d'ajouter le nom de fichier*).

Afin de quitter **vi** il suffit de taper la commande:

```
:q texte1.txt
```

Commande	**Effets**
i (insert)	Insère un texte sur le curseur.
I	Insère au début de la ligne.
a (append)	Insère après le curseur.
A	Insère à la fin de la ligne.
Les flèches	pour les déplacements.
Ctrl-F (forward)	Défiler d'un écran vers le bas.
Ctrl-B (backward)	Défiler d'un écran vers le haut.
nG (goto)	va à la nième ligne dans le texte.
G	Va à la fin du texte.
x	Effacer le caractère courant.
dd	Effacer la ligne courante.
D	Effacer depuis la position du curseur jusqu'à la fin de la ligne.
db(DeleteBegining)	Effacer depuis la position courante jusqu'au début de la ligne.
/chaîne	rechercher la chaîne 'chaîne' dans le texte, on peut taper 'n' pour voir les autres occurrences.
:w fichier	copie le texte courant sur le disque sous le nom fichier.
:wq (write & quit)	écrit le fichier sur le disque et quitte vi.
:q!	Quitter sans sauvegarder.
:set nu	Affiche le numérotage des lignes.

Victoire totale, hissons la bannière de la victoire.

Crédits

© 2016 RF-232

Auteur: **Michel-André Robillard CLP**

Remerciement: **Tous les contributeurs GNU/GPL**.

Intégré par: **Michel-André Robillard CLP**

Contact: **michelandre at micronator.org**

Répertoire de ce document: E:\000_DocPourRF232_general\RF-232_SME-9.1_fail2ban\RF-232_SME-9.1_fail2ban_2016-04-13_17h49.odt

Historique des modifications**:**

Version	*Date*	*Commentaire*	*Auteur*
0.0.1	2016-02-10	Début.	M.-A. Robillard
0.0.2	2016-02-12	Ajout d'exemples de bannissements et d'une mise en garde pour une configuration personnalisée de jail.conf. Mise à jour.	M.-A. Robillard

Index

1

125.31.5.0/24.....19
125.31.5.33.....18
127.0.0.0/8.....16
143.....12
15 minutes.....11
1800.....10
192.168.1.0/24.....16
192.168.1.1.....16

2

2048 bits.....5

4

443.....12
465.....12

5

5 fois en 24 heures.....12

9

9 courriels sont rejetés.....11
900.....10
993.....12

A

Accès à distance.....10
admin.....10
adresses IP bannies.....12
Affichage.....18
American Express.....5
Apache.....4, 11
ASCII.....4
astuce.....4
auth.....11
AuthExtern.....17
Autorité de Certification Let's Encrypt.....5
AVEC RÉAMORÇAGE.....9
Avertissement.....2

B

backend = auto.....16
Banned IP list.....12
Banned IP list: 125.31.5.33.....18
Banned IP list: 125.31.5.33/24.....19
Bannissement d'une adresse.....18
Bannissement d'une plage.....19
Bannissement d'une semaine.....19
Bannissements complets.....12
Bannissements sélectifs.....12
BanTime.....10
bantime = 1800.....16
BaseURL.....6
bleu.....4
Bogues.....17
Boutique de Micronator.....5
Brancher les aînés.....5

C

certificat SSL.....5
checklist_ban.sh.....13
chmod 700.....13
CIDR.....10
Code source du message.....18
Commande DB.....10
commande signal-event fail2ban-conf.....11
Commentaire.....23
Commentaires et suggestions.....5
config de yum.....7
config setprop fail2ban.....10
config show fail2ban.....10
contrib.....6
Conventions.....4
CR.....4
Crédits.....23
Ctrl-B.....22
Ctrl-F.....22
Currently banned.....12
Currently failed.....12

D

db configuration.....10
dd.....22
dépôt de logiciels EPEL.....6
Description générale.....4
Discover.....5
disponibles.....10
dovecot.....11

E

éditeur vi.....13, 21
Ejabberd.....11
EnableGroups.....6
EPEL.....6
Epel - EL5.....7
Epel - EL6.....6
epel repository.....7
epel/5.....7
epel/6.....6
étape.....4

F

Fail2ban.....4
fail2ban-client status.....12, 14, 19
fail2ban.conf.....9
fail2ban.noarch.....8
fail2ban/jail.conf.....15
fastestmirror.....7
File list.....12
FilterLocalNetworks.....10
Filtre spécifique.....11
findtime.....11
FindTime.....10
findtime = 900.....16
Firewall Services Repo.....8
Firewall-Services.....6
ftp.....11

G

gamin-python.....8
Gestion à distance.....10
GPGKey.....6

H

hits=6.9.....18
http.....11
http-auth.....14
http-badbots.....14
http-fakegooglebot.....14
http-noscript.....14
http-overflows.....14
http-scan.....14
http-shellshock.....14
httpd.....9
httpd-e-smith.....11

HyperText Transfer Protocol Daemon....9

I

i (insert)....22
IgnoreIP....10, 16
ignoreregex....17
imap....14
inetd....9
Installation....6
Installation des RPMS....7
Ipd....9
ipset.x86_64....8
iptables....4, 9

J

Jail.conf....15
jail.conf par défaut....15

L

LemonLDAP-NG....11
LemonLDAP::NG....11
LF....4
libmnl.x86_64....8
ls -alsd....13

M

magenta....4
Mail....10
MailRecipient....10
Manipulation....4
manuel original....17
masq daemon....9
masq restart....9, 15
MasterCard....5
MaxRetry....10
maxretry = 3....16
micronator.org....5
mode commande....21
mode édition....21

N

NOKEY....8
non vérifié....4
NON-RESPONSABILITÉ....2
noscripts....11
note....4
Notes au lecteur....4
numérotage des lignes....22

O

orange....4

P

pam....11, 12
pam-generic....14
Particularités de ce document....4
PayPal....5
PDF....4
prison recidive....19
prison spécifique....12
procédure....4
pwauth....17
python-inotify.noarch....8

Q

qpsmtpd....11, 12

R

recidive....12, 14
recommandation....4
référence Internet....4
Réintégration....14
Résolution des dépendances....8
RF-232....5
root....10
rouge....4
Route....19

S

SANS RÉAMORÇAGE....9
scan....11
sed....13
sendmail....9
Server Manager....10
Serveur SME-7.x....6
Services....11
set qpsmtpd banip....18
set recidive banip....20
setprop masq status enabled....9
signal-event fail2ban-conf....9
signal-event post-upgrade....8
signal-event reboot....8
signal-event yum-modify....7
Signalisation de la modification....7
SME-8.x....6
SME-9....11
SME-9.x....6
smeserver-fail2ban.noarch....8
SOGo....11
spam....6
SpamAssassin....18
ssh....11
SSH....6
ssh-ddos....14
sshd....4
SSL....5
Status for the jail....12
status qpsmtpd....14, 18
status recidive....20
status ssh....12
Stripe....5
sudo....13
Systèmes requis....6

T

TCP 22....12
TCP 25....12
TCP 80....12
Thunderbird....18
Total banned....12
Total failed....12
touch....13
tous les bannissements....12
Toutes les commandes....17

U

unbanip....14
Usage....10
Usage de Fail2ban....12
usager root....12
usedns = yes....16
utilisateur admin....14

V

vi checklist_ban.sh....13
Victoire....22
Visa....5

X

X-Spam-Flag: YES....18
X-Spam-Level....18
x3....11

Y

yum remove....17
yum_repositories....6

-

--enablerepo=epel.....7
--enablerepo=fws.....7

:

:q.....22
:q!.....22
:set nu.....22
:w.....22
:wq.....13

.

.d.....9

[

[DEFAULT].....15
[Esc].....21
[ESC].....13

/

/etc/e-smith/templates-custom.....15
/etc/e-smith/templates/.....15
/etc/fail2ban.....15
/etc/fail2ban/jail.conf.....15
/root.....12
/var/log/auth.log.....4, 6
/var/log/pwdfail.....6
/var/log/sshd/current.....12

#

#!/bin/bash.....13

©

© RF-232.....2

LICENCE PUBLIQUE GÉNÉRALE GNU

Version 3, du 29 juin 2007.
Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Chacun est autorisé à copier et distribuer des copies conformes de ce document de licence, mais toute modification en est proscrite.

- -

Traduction française par Philippe Verdy <verdy_p (à) wanadoo (point) fr>, le 30 juin 2007 (dernière correction du 4 janvier 2011).

Avertissement important au sujet de cette traduction française.

Ceci est une traduction en français de la licence “GNU General Public License” (GPL). Cette traduction est fournie ici dans l’espoir qu’elle facilitera sa compréhension, mais elle ne constitue pas une traduction officielle ou approuvée d’un point de vue juridique.

La Free Software Foundation (FSF) ne publie pas cette traduction et ne l’a pas approuvée en tant que substitut valide au plan légal pour la licence authentique “GNU General Public Licence”. Cette traduction n’a pas encore été passée en revue attentivement par un juriste et donc le traducteur ne peut garantir avec certitude qu’elle représente avec exactitude la signification légale des termes de la licence authentique “GNU General Public License” publiée en anglais. Cette traduction n’établit donc légalement aucun des termes et conditions d’utilisation d’un logiciel sous licence GNU GPL — seul le texte original en anglais le fait. Si vous souhaitez être sûr que les activités que vous projetez seront autorisées par la GNU General Public License, veuillez vous référer à sa seule version anglaise authentique.

La FSF vous recommande fermement de ne pas utiliser cette traduction en tant que termes officiels pour vos propres programmes; veuillez plutôt utiliser la version anglaise authentique telle que publiée par la FSF. Si vous choisissez d’acheminer cette traduction en même temps qu’un Programme sous licence GNU GPL, cela ne vous dispense pas de l’obligation d’acheminer en même temps une copie de la licence authentique en anglais, et de conserver dans la traduction cet avertissement important en français et son équivalent en anglais ci-dessous.

Important Warning About This French Translation.

This is a translation of the GNU General Public License (GPL) into French. This translation is distributed in the hope that it will facilitate understanding, but it is not an official or legally approved translation.

The Free Software Foundation (FSF) is not the publisher of this translation and has not approved it as a legal substitute for the authentic GNU General Public License. The translation has not been reviewed carefully by lawyers, and therefore the translator cannot be sure that it exactly represents the legal meaning of the authentic GNU General Public License published in English. This translation does not legally state the terms and conditions of use of any Program licenced under GNU GPL — only the original English text of the GNU LGPL does that. If you wish to be sure whether your planned activities are permitted by the GNU General Public License, please refer to its sole authentic English version.

The FSF strongly urges you not to use this translation as the official distribution terms for your programs; instead, please use the authentic English version published by the FSF. If you choose to convey this translation along with a Program covered by the GPL Licence, this does not remove your obligation to convey at the same time a copy of the authentic GNU GPL License in English, and you must keep in this translation this important warning in English and its equivalent in French above.

- -

Préambule

La Licence Publique Générale GNU (**“GNU General Public License”**) est une licence libre, en **“copyleft”**, destinée aux œuvres logicielles et d’autres types d’œuvres.

Les licences de la plupart des œuvres logicielles et autres œuvres de la pratique sont conçues pour vous ôter votre liberté de partager et modifier ces œuvres. À l’inverse, la Licence Publique Générale GNU a pour but de garantir votre liberté de partager et changer toutes les versions d’un programme — afin d’assurer qu’il restera libre pour tous les utilisateurs. Nous, la **Free Software Foundation**, utilisons la Licence Publique Générale GNU pour la plupart de nos logiciels; cela s’applique aussi à toute autre œuvre éditée de cette façon par ses auteurs. Vous pouvez, vous aussi, l’appliquer à vos propres programmes.

Quand nous parlons de logiciel libre (**“free”**), nous nous référons à la liberté (**“freedom”**), pas au prix. Nos Licences Publiques Générales sont conçues pour assurer que vous ayez la liberté de distribuer des copies de logiciel libre (et le facturer si vous le souhaitez), que vous receviez le code source ou pouviez l’obtenir si vous le voulez, que vous pouviez modifier le logiciel ou en utiliser toute partie dans de nouveaux logiciels libres, et que vous sachiez que vous avez le droit de faire tout ceci.

Pour protéger vos droits, nous avons besoin d’empêcher que d’autres vous restreignent ces droits ou vous demande de leur abandonner ces droits. En conséquence, vous avez certaines responsabilités si vous distribuez des copies d’un tel programme ou si vous le modifiez : les responsabilités de respecter la liberté des autres.

Par exemple, si vous distribuez des copies d’un tel programme, que ce soit gratuit ou contre un paiement, vous devez accorder aux Destinataires les mêmes libertés que vous avez reçues. Vous devez aussi vous assurer qu’eux aussi reçoivent ou peuvent recevoir son code source. Et vous devez leur montrer les termes de cette licence afin qu’ils connaissent leurs droits.

Les développeurs qui utilisent la GPL GNU protègent vos droits en deux étapes : (1) ils affirment leur droits d’auteur (**“**copyright**”**) sur le logiciel, et (2) vous accordent cette Licence qui vous donne la permission légale de le copier, le distribuer et/ou le modifier.

Pour la protection des développeurs et auteurs, la GPL stipule clairement qu’il n’y a pas de garantie pour ce logiciel libre. Aux fins à la fois des utilisateurs et auteurs, la GPL requière que les versions modifiées soient marquées comme changées, afin que leurs problèmes ne soient pas attribués de façon erronée aux auteurs des versions précédentes.

Certains dispositifs sont conçus pour empêcher l’accès des utilisateurs à l’installation ou l’exécution de versions modifiées du logiciel à l’intérieur de ces dispositifs, alors que les fabricants le peuvent. Ceci est fondamentalement incompatible avec le but de protéger la liberté des utilisateurs de modifier le logiciel. L’aspect systématique de tels abus se produit dans le secteur des produits destinés aux utilisateurs individuels, ce qui est précisément ce qui est le plus inacceptable. Aussi, nous avons conçu cette version de la GPL pour prohiber cette pratique pour ces produits. Si de tels problèmes surviennent dans d’autres domaines, nous nous tenons prêt à étendre cette restriction à ces domaines dans de futures versions de la GPL, autant qu’il sera nécessaire pour protéger la liberté des utilisateurs.

Finalement, chaque programme est constamment menacé par les brevets logiciels. Les États ne devraient pas autoriser de tels brevets à restreindre le développement et l’utilisation de logiciels libres sur des ordinateurs d’usage général; mais dans ceux qui le font, nous voulons spécialement éviter le danger que les brevets appliqués à un programme libre puisse le rendre effectivement propriétaire. Pour empêcher ceci, la GPL assure que les brevets ne peuvent être utilisés pour rendre le programme non-libre.

Les termes précis et conditions concernant la copie, la distribution et la modification suivent.

TERMES ET CONDITIONS

Article 0. Définitions.

"Cette Licence" se réfère à la version 3 de la **“**GNU General Public License**”** (le texte original en anglais).

"Droit d’Auteur" signifie aussi les droits du “copyright” ou voisins qui s’appliquent à d’autres types d’œuvres, tels que celles sur les masques de semi-conducteurs.

"Le Programme" se réfère à toute œuvre qui peut être sujette au Droit d’Auteur (“copyright”) et dont les droits d’utilisation sont concédés en vertu de cette Licence. Chacun des Licenciés, à qui cette Licence est concédée, est désigné par "vous." Les "Licenciés" et les "Destinataires" peuvent être des personnes physiques ou morales (individus ou organisations).

"Modifier" une œuvre signifie en obtenir une copie et adapter tout ou partie de l’œuvre d’une façon qui nécessite une autorisation d’un titulaire de Droit d’Auteur, autre que celle permettant d’en produire une copie conforme. L’œuvre résultante est appelée une "version modifiée" de la précédente œuvre, ou une œuvre "basée sur" la précédente œuvre.

Une "Œuvre Couverte" signifie soit le Programme non modifié soit une œuvre basée sur le Programme.

"Propager" une œuvre signifie faire quoi que ce soit avec elle qui, sans permission, vous rendrait directement ou indirectement responsable d’un délit de contrefaçon suivant les lois relatives au Droit d’Auteur, à l’exception de son exécution sur un ordinateur ou de la modification d’une copie privée. La propagation inclue la copie, la distribution (avec ou sans modification), la mise à disposition envers le public, et aussi d'autres activités dans certains pays.

"Acheminer" une œuvre signifie tout moyen de propagation de celle-ci qui permet à d’autres parties d’en réaliser ou recevoir des copies. La simple interaction d’un utilisateur à travers un réseau informatique, sans transfert effectif d’une copie, ne constitue pas un acheminement.

Une interface utilisateur interactive affiche des "Notices Légales Appropriées" quand elle comprend un dispositif convenable, bien visible et évident qui (1) affiche une notice appropriée sur les droits d’auteur et (2) informe l’utilisateur qu’il n’y a pas de garantie pour l’œuvre (sauf si des garanties ont été fournies hors du cadre de cette Licence), que les licenciés peuvent acheminer l’œuvre sous cette Licence, et comment consulter une copie de cette Licence. Si l’interface présente une liste de commandes utilisateur ou d’options, tel qu’un menu, un élément évident dans la liste présentée remplit ce critère.

Article 1. Code source.

Le "code source" d’une œuvre signifie la forme préférée de l’œuvre qui permet ou facilite les modifications de celle-ci. Le "code objet" d’une œuvre signifie toute forme de l’œuvre qui n’en est pas le code source.

Une "Interface Standard" signifie une interface qui est soit celle d’une norme officielle définie par un organisme de normalisation reconnu ou, dans le cas des interfaces spécifiées pour un langage de programmation particulier, une interface largement utilisée parmi les développeurs qui travaillent dans ce langage.

Les "Bibliothèques Système" d’une œuvre exécutable incluent tout ce qui, en dehors de l’œuvre dans son ensemble, (a) est inclus dans la forme usuelle de paquetage d’un Composant Majeur mais ne fait pas partie de ce Composant Majeur et (b) sert seulement à permettre l’utilisation de l’œuvre avec ce Composant Majeur ou à mettre en œuvre une Interface Standard pour laquelle une mise en œuvre est disponible au public sous forme de code source; un "Composant Majeur" signifie, dans ce contexte, un composant majeur essentiel (noyau, système de fenêtrage, etc.) du système d’exploitation (le cas échéant) d’un système sur lequel l’œuvre exécutable fonctionne, ou bien un compilateur utilisé pour produire le code objet de l’œuvre, ou un interprète de code objet utilisé pour exécuter celui-ci.

Le "Source Correspondant" d’une œuvre sous forme de code objet signifie l’ensemble des codes sources nécessaires pour générer, installer et (dans le cas d’une œuvre exécutable) exécuter le code objet et modifier l’œuvre, y compris les scripts pour contrôler ces activités. Cependant, cela n’inclue pas les Bibliothèques Système de l’œuvre, ni les outils d’usage général ou les programmes libres généralement disponibles qui peuvent être utilisés sans modification pour achever ces activités mais ne sont pas partie de cette œuvre. Par exemple le Source Correspondant inclut les fichiers de définition d’interfaces associés aux fichiers sources de l’œuvre, et le code source des bibliothèques partagées et des sous-routines liées dynamiquement, pour lesquelles l’œuvre est spécifiquement conçue pour les requérir via, par exemple, des communications de données ou contrôles de flux internes entre ces sous-programmes et d’autres parties de l’œuvre.

Le Source Correspondant n’a pas besoin d’inclure tout ce que les utilisateurs peuvent régénérer automatiquement à partir d’autres parties du Source Correspondant.

Le Source Correspondant pour une œuvre sous forme de code source est cette même œuvre.

Article 2. Permissions de base.

Tous les droits accordés suivant cette Licence le sont jusqu’au terme des Droits d’Auteur (“copyright”) sur le Programme, et sont irrévocables pourvu que les conditions établies soient remplies. Cette Licence affirme explicitement votre permission illimitée d’exécuter le Programme non modifié. La sortie produite par l’exécution d’une Œuvre Couverte n’est couverte par cette Licence que si cette sortie, étant donné leur contenu, constitue une Œuvre Couverte. Cette Licence reconnaît vos propres droits d’usage raisonnable (“fair use” en législation des États-Unis d’Amérique) ou autres équivalents, tels qu’ils sont pourvus par la loi applicable sur le Droit d’Auteur (“copyright”).

Vous pouvez créer, exécuter et propager sans condition des Œuvres Couvertes que vous n’acheminez pas, aussi longtemps que votre licence demeure en vigueur. Vous pouvez acheminer des Œuvres Couvertes à d’autres personnes dans le seul but de leur faire réaliser des modifications à votre usage exclusif, ou pour qu’ils vous fournissent des facilités vous permettant d’exécuter ces œuvres, pourvu que vous vous conformiez aux termes de cette Licence lors de l’acheminement de tout matériel dont vous ne contrôlez pas le Droit d’Auteur (“copyright”). Ceux qui, dès lors, réalisent ou exécutent pour vous les Œuvres Couvertes ne doivent alors le faire qu’exclusivement pour votre propre compte, sous votre direction et votre contrôle, suivant des termes qui leur interdisent de réaliser, en dehors de leurs relations avec vous, toute copie de votre matériel soumis au Droit d’Auteur.

L’acheminement dans toutes les autres circonstances n’est permis que selon les conditions établies ci-dessous. La concession de sous-licences n’est pas autorisé; l’article 10 rend cet usage non nécessaire.

Article 3. Protection des droits légaux des utilisateurs envers les lois anti-contournement.

Aucune Œuvre Couverte ne doit être vue comme faisant partie d’une mesure technologique effective selon toute loi applicable remplissant les obligations prévues à l’article 11 du traité international sur le droit d’auteur adopté à l’OMPI le 20 décembre 1996, ou toutes lois similaires qui prohibent ou restreignent le contournement de telles mesures.

Si vous acheminez une Œuvre Couverte, vous renoncez à tout pouvoir légal d’interdire le contournement des mesures technologiques dans tous les cas où un tel contournement serait effectué en exerçant les droits prévus dans cette Licence pour cette Œuvre Couverte, et vous déclarez rejeter toute intention de limiter l’opération ou la modification de l’Œuvre, en tant que moyens pour renforcer, à l’encontre des utilisateurs de cette Œuvre, vos droits légaux ou ceux de tierces parties d’interdire le contournement desdites mesures technologiques.

Article 4. Acheminement des copies conformes.

Vous pouvez acheminer des copies conformes du code source du Programme tel que vous l’avez reçu, sur n’importe quel support, pourvu que vous publiiez scrupuleusement et de façon appropriée sur chaque copie une notice de Droit d’Auteur appropriée; gardez intactes toutes les notices établissant que cette Licence et tous les termes additionnels non permissifs ajoutés en accord avec l’article 7 s’appliquent à ce code; et donnez à chacun des Destinataires une copie de cette Licence en même temps que le Programme.

Vous pouvez facturer un prix quelconque, y compris gratuit, pour chacune des copies que vous acheminez, et vous pouvez offrir une protection additionnelle de support ou de garantie en échange d’un paiement.

Article 5. Acheminement des versions sources modifiées.

Vous pouvez acheminer une œuvre basée sur le Programme, ou bien les modifications pour le produire à partir du Programme, sous la forme de code source suivant les termes de l’article 4, pourvu que vous satisfassiez aussi à chacune des conditions requises suivantes :

- a) L’œuvre doit comporter des notices évidentes établissant que vous l’avez modifiée et donnant la date correspondante.
- b) L’œuvre doit comporter des notices évidentes établissant qu’elle est éditée selon cette Licence et les conditions ajoutées d’après l’article 7. Cette obligation vient modifier l’obligation de l’article 4 de "garder intactes toutes les notices."
- c) Vous devez licencier l’œuvre entière, comme un tout, suivant cette Licence à quiconque entre en possession d’une copie. Cette Licence s’appliquera en conséquence, avec les termes additionnels applicables prévus par l’article 7, à la totalité de l’œuvre et chacune de ses parties, indépendamment de la façon dont elles sont empaquetées. Cette licence ne donne aucune permission de licencier l’œuvre d’une autre façon, mais elle n’invalide pas une telle permission que vous auriez reçue séparément.
- d) Si l’œuvre a des interfaces utilisateurs interactives, chacune doit afficher les Notices Légales Appropriées; cependant si le Programme a des interfaces qui n’affichent pas les Notices Légales Appropriées, votre œuvre n’a pas à les modifier pour qu’elles les affichent.

Une compilation d’une Œuvre Couverte avec d’autres œuvres séparées et indépendantes, qui ne sont pas par leur nature des extensions de l’Œuvre Couverte, et qui ne sont pas combinés avec elle de façon à former un programme plus large, dans ou sur un volume de stockage ou un support de distribution, est appelé un "agrégat" si la compilation et son Droit d’Auteur résultant ne sont pas utilisés pour limiter l’accès ou les droits légaux des utilisateurs de la compilation en deçà de ce que permettent les œuvres individuelles. L’inclusion d’une Œuvre Couverte dans un agrégat ne cause pas l’application de cette Licence aux autres parties de l’agrégat.

Article 6. Acheminement des formes non sources.

Vous pouvez acheminer sous forme de code objet une Œuvre Couverte suivant les termes des articles 4 et 5, pourvu que vous acheminiez également suivant les termes de cette Licence le Source Correspondant lisible par une machine, d’une des façons suivantes :

- a) Acheminer le code objet sur, ou inclus dans, un produit physique (y compris un support de distribution physique), accompagné par le Source Correspondant fixé sur un support physique durable habituellement utilisé pour les échanges de logiciels.
- b) Acheminer le code objet sur, ou inclus dans, un produit physique (y compris un support de distribution physique), accompagné d’une offre écrite, valide pour au moins trois années et valide pour aussi longtemps que vous fournissez des pièces de rechange ou un support client pour ce modèle de produit, afin de donner à quiconque possède le code objet soit (1) une copie du Source Correspondant à tout logiciel dans ce produit qui est couvert par cette Licence, sur un support physique durable habituellement utilisé pour les échanges de logiciels, pour un prix non supérieur au coût raisonnable de la réalisation physique de l’acheminement de la source, ou soit (2) un accès permettant de copier le Source Correspondant depuis un serveur réseau sans frais.
- c) Acheminer des copies individuelles du code objet avec une copie de l’offre écrite de fournir le Source Correspondant. Cette alternative est permise seulement occasionnellement et non-commercialement, et seulement si vous avez reçu le code objet avec une telle offre, en accord avec l’article 6 alinéa b.
- d) Acheminer le code objet en offrant un accès depuis un emplacement désigné (gratuit ou contre facturation) et offrir un accès équivalent au Source Correspondant de la même façon via le même emplacement et sans facturation supplémentaire. Vous n’avez pas besoin d’obliger les Destinataires à copier le Source Correspondant en même temps que le code objet. Si l’emplacement pour copier le code objet est un serveur réseau, le Source Correspondant peut être sur un serveur différent (opéré par vous ou par un tiers) qui supporte des facilités équivalentes de copie, pourvu que vous mainteniez des directions claires à proximité du code objet indiquant où trouver le Source Correspondant. Indépendamment de quel serveur héberge le Source Correspondant, vous res-

tez obligé de vous assurer qu'il reste disponible aussi longtemps que nécessaire pour satisfaire à ces obligations.

- e) Acheminer le code objet en utilisant une transmission d'égal-à-égal, pourvu que vous informiez les autres participants sur l'endroit où le code objet et le Source Correspondant de l'œuvre sont offerts sans frais au public général suivant l'article 6 alinéa d.

Une portion séparable du code objet, dont le code source est exclu du Source Correspondant en tant que Bibliothèque Système, n'a pas besoin d'être incluse dans l'acheminement de l'œuvre sous forme de code objet.

Un "Produit Utilisateur" est soit (1) un "Produit de Consommation," ce qui signifie toute propriété personnelle tangible normalement utilisée à des fins personnelles, familiales ou relatives au foyer, soit (2) toute chose conçue ou vendue pour l'incorporation dans un lieu d'habitation. Pour déterminer si un produit constitue un Produit de Consommation, les cas ambigus sont résolus en fonction de la couverture. Pour un produit particulier reçu par un utilisateur particulier, l'expression "normalement utilisée" ci-avant se réfère à une utilisation typique ou l'usage commun de produits de même catégorie, indépendamment du statut de cet utilisateur particulier ou de la façon spécifique dont cet utilisateur particulier utilise effectivement ou s'attend lui-même ou est attendu à utiliser ce produit. Un produit est un Produit de Consommation indépendamment du fait que ce produit a ou n'a pas d'utilisations substantielles commerciales, industrielles ou hors Consommation, à moins que de telles utilisations représentent le seul mode significatif d'utilisation du produit.

Les "Informations d'Installation" d'un Produit Utilisateur signifient toutes les méthodes, procédures, clés d'autorisation ou autres informations requises pour installer et exécuter des versions modifiées d'une Œuvre Couverte dans ce Produit Utilisateur à partir d'une version modifiée de son Source Correspondant. Les informations qui suffisent à assurer la continuité de fonctionnement du code objet modifié ne doivent en aucun cas être empêchées ou interférées du seul fait qu'une modification a été effectuée.

Si vous acheminez le code objet d'une Œuvre Couverte dans, ou avec, ou spécifiquement pour l'utilisation dans, un Produit Utilisateur et si l'acheminement se produit en tant qu'élément d'une transaction dans laquelle le droit de possession et d'utilisation du Produit Utilisateur est transféré au Destinataire définitivement ou pour un terme fixé (indépendamment de la façon dont la transaction est caractérisée), le Source Correspondant acheminé selon cet article-ci doit être accompagné des Informations d'Installation. Mais cette obligation ne s'applique pas si ni vous ni aucune tierce partie ne détient la possibilité d'installer un code objet modifié sur le Produit Utilisateur (par exemple, l'œuvre a été installée en mémoire morte).

L'obligation de fournir les Informations d'Installation n'inclue pas celle de continuer à fournir un service de support, une garantie ou des mises à jour pour une œuvre qui a été modifiée ou installée par le Destinataire, ou pour le Produit Utilisateur dans lequel elle a été modifiée ou installée. L'accès à un réseau peut être rejeté quand la modification elle-même affecte matériellement et défavorablement les opérations du réseau ou viole les règles et protocoles de communication au travers du réseau.

Le Source Correspondant acheminé et les Informations d'Installation fournies, en accord avec cet article, doivent être dans un format publiquement documenté (et dont une implémentation est disponible auprès du public sous forme de code source) et ne doit nécessiter aucune clé ou mot de passe spécial pour le dépaquetage, la lecture ou la copie.

Article 7. Termes additionnels.

Les « permissions additionnelles » désignent les termes qui supplémentent ceux de cette Licence en émettant des exceptions à l'une ou plusieurs de ses conditions. Les permissions additionnelles qui sont applicables au Programme entier doivent être traitées comme si elles étaient incluent dans cette Licence, dans les limites de leur validité suivant la loi applicable. Si des permissions additionnelles s'appliquent seulement à une partie du Programme, cette partie peut être utilisée séparément suivant ces permissions, mais le Programme tout entier reste gouverné par cette Licence sans regard aux permissions additionnelles.

Quand vous acheminez une copie d'une Œuvre Couverte, vous pouvez à votre convenance ôter toute permission additionnelle de cette copie, ou de n'importe quelle partie de celui-ci. (Des permissions additionnelles peuvent être rédigées de façon à requérir leur propre suppression dans certains cas où vous modifiez l'œuvre.) Vous pouvez placer les permissions additionnelles sur le matériel acheminé, ajoutées par vous à une Œuvre Couverte pour laquelle vous avez ou pouvez donner les permissions de Droit d'Auteur ("copyright") appropriées.

Nonobstant toute autre clause de cette Licence, pour tout constituant que vous ajoutez à une Œuvre Couverte, vous pouvez (si autorisé par les titulaires de Droit d'Auteur pour ce constituant) supplémenter les termes de cette Licence avec des termes :

- a) qui rejettent la garantie ou limitent la responsabilité de façon différente des termes des articles 15 et 16 de cette Licence; ou
- b) qui requièrent la préservation de notices légales raisonnables spécifiées ou les attributions d'auteur dans ce constituant ou dans les Notices Légales Appropriées affichées par les œuvres qui le contiennent; ou
- c) qui prohibent la représentation incorrecte de l'origine de ce constituant, ou qui requièrent que les versions modifiées d'un tel constituant soient marquées par des moyens raisonnables comme différentes de la version originale; ou
- d) qui limitent l'usage à but publicitaire des noms des concédants de licence et des auteurs du constituant; ou
- e) qui refusent à accorder des droits selon la législation relative aux marques commerciales, pour l'utilisation dans des noms commerciaux, marques commerciales ou marques de services; ou
- f) qui requièrent l'indemnisation des concédants de licences et auteurs du constituant par quiconque achemine ce constituant (ou des versions modifiées de celui-ci) en assumant contractuellement la responsabilité envers le Destinataire, pour toute responsabilité que ces engagements contractuels imposent directement à ces octroyants de licences et auteurs.

Tous les autres termes additionnels non permissifs sont considérés comme des « restrictions avancées » dans le sens de l'article 10. Si le Programme tel que vous l'avez reçu, ou toute partie de celui-ci, contient une notice établissant qu'il est gouverné par cette Licence en même temps qu'un terme qui est une restriction avancée, vous pouvez ôter ce terme. Si un document de licence contient une restriction avancée mais permet la reconcession de licence ou l'acheminement suivant cette Licence, vous pouvez ajouter une Œuvre Couverte constituante gouvernée par les termes de ce document de licence, pourvu que la restriction avancée ne survit pas à une telle cession de licence ou un tel acheminement.

Si vous ajoutez des termes à une Œuvre Couverte en accord avec cet article, vous devez placer, dans les fichiers sources appropriés, une déclaration des termes additionnels qui s'appliquent à ces fichiers, ou une notice indiquant où trouver les termes applicables.

Les termes additionnels, qu'ils soient permissifs ou non permissifs, peuvent être établis sous la forme d'une licence écrite séparément, ou établis comme des exceptions; les obligations ci-dessus s'appliquent dans chacun de ces cas.

Article 8. Terminaison.

Vous ne pouvez ni propager ni modifier une Œuvre Couverte autrement que suivant les termes de cette Licence. Toute autre tentative de le propager ou le modifier est nulle et terminera automatiquement vos droits selon cette Licence (y compris toute licence de brevet accordée selon le troisième paragraphe de l'article 11).

Cependant, si vous cessez toute violation de cette Licence, alors votre licence depuis un titulaire de Droit d'Auteur ("copyright") est réinstaurée (a) à titre provisoire à moins que et jusqu'à ce que le titulaire de Droit d'Auteur termine finalement et explicitement votre licence, et (b) de façon permanente si le titulaire de Droit d'Auteur ne parvient pas à vous notifier de la violation par quelque moyen raisonnable dans les soixante (60) jours après la cessation.

De plus, votre licence depuis un titulaire particulier de Droit d'Auteur est réinstaurée de façon permanente si ce titulaire vous a notifié de la violation par quelque moyen raisonnable, et si c'est la première fois que vous avez reçu une notification de violation de cette Licence (pour une œuvre quelconque) depuis ce titulaire de Droit d'Auteur, et si vous résolvez la violation dans les trente (30) jours qui suivent votre réception de la notification.

La terminaison de vos droits suivant cette section ne terminera pas les licences des parties qui ont reçu des copies ou droits de votre part suivant cette Licence. Si vos droits ont été terminés et non réinstaurés de façon permanente, vous n'êtes plus qualifié à recevoir de nouvelles licences pour les mêmes constituants selon l'article 10.

Article 9. Acceptation non requise pour obtenir des copies.

Vous n'êtes pas obligé d'accepter cette licence afin de recevoir ou exécuter une copie du Programme. La propagation asservie d'une Œuvre Couverte qui se produit simplement en conséquence d'une transmission d'égal-à-égal pour recevoir une copie ne nécessite pas l'acceptation. Cependant, rien d'autre que cette Licence ne vous accorde la permission de propager ou modifier une quelconque Œuvre Couverte. Ces actions enfreignent le Droit d'Auteur si vous n'acceptez pas cette Licence. Par conséquent, en modifiant ou propageant une Œuvre Couverte, vous indiquez votre acceptation de cette Licence pour agir ainsi.

Article 10. Cession automatique de Licence aux Destinataires et intermédiaires.

Chaque fois que vous acheminez une Œuvre Couverte, le Destinataire reçoit automatiquement une licence de la part des concédants originaux, pour exécuter, modifier et propager cette œuvre, suivant les termes de cette Licence. Vous n'êtes pas responsable du renforcement de la conformation des tierces parties aux termes de cette Licence.

Une "transaction d'entité" désigne une transaction qui transfère le contrôle d'une organisation, ou de substantiellement tous ses actifs, ou la subdivision d'une organisation, ou la fusion de plusieurs organisations. Si la propagation d'une Œuvre Couverte résulte d'une transaction d'entité, chaque partie à cette transaction qui reçoit une copie de l'œuvre reçoit aussi les licences pour l'œuvre que le prédécesseur intéressé à cette partie avait ou pourrait donner selon le paragraphe précédent, plus un droit de possession du Source Correspondant de cette œuvre depuis le prédécesseur intéressé si ce prédécesseur en dispose ou peut l'obtenir par des efforts raisonnables.

Vous ne pouvez imposer aucune restriction avancée dans l'exercice des droits accordés ou affirmés selon cette Licence. Par exemple, vous ne pouvez imposer aucun paiement pour la licence, aucune royaltie, ni aucune autre charge pour l'exercice des droits accordés selon cette Licence; et vous ne pouvez amorcer aucun litige judiciaire (y compris une réclamation croisée ou contre-réclamation dans un procès) sur l'allégation qu'une revendication de brevet est enfreinte par la réalisation, l'utilisation, la vente, l'offre de vente, ou l'importation du Programme ou d'une quelconque portion de celui-ci.

Article 11. Brevets.

Un « contributeur » est un titulaire de Droit d'Auteur (**"copyright"**) qui autorise l'utilisation selon cette Licence du Programme ou de l'œuvre sur laquelle le Programme est basé. L'œuvre ainsi soumise à licence est appelée la "version contributive" de ce contributeur.

Les "revendications de brevet essentielles" sont toutes les revendications de brevets détenues ou contrôlées par le contributeur, qu'elles soient déjà acquises par lui ou acquises subséquemment, qui pourraient être enfreintes de quelque manière, permises par cette Licence, sur la réalisation, l'utilisation ou la vente de la version contributive de celui-ci. Aux fins de cette définition, le "contrôle" inclue le droit de concéder des sous-licences de brevets d'une manière consistante, nécessaire et suffisante, avec les obligations de cette Licence.

Chaque contributeur vous accorde une licence de brevet non exclusive, mondiale et libre de toute royaltie, selon les revendications de brevet essentielles, pour réaliser, utiliser, vendre, offrir à la vente, importer et autrement exécuter, modifier et propager les contenus de sa version contributive.

Dans les trois paragraphes suivants, une "licence de brevet" désigne tous les accords ou engagements exprimés, quel que soit le nom que vous lui donnez, de ne pas mettre en vigueur un brevet (telle qu'une permission explicite pour mettre en pratique un brevet, ou un accord pour ne pas poursuivre un Destinataire pour cause de violation de brevet). "Accorder" une telle licence de brevet à une partie signifie conclure un tel accord ou engagement à ne pas faire appliquer le brevet à cette partie.

Si vous acheminez une Œuvre Couverte, dépendant en connaissance d'une licence de brevet, et si le Source Correspondant de l'œuvre n'est pas disponible à quiconque copie, sans frais et suivant les termes de cette Licence, à travers un serveur réseau publiquement accessible ou tout autre moyen immédiatement accessible, alors vous devez soit (1) rendre la Source Correspondante ainsi disponible, soit (2) vous engager à vous priver pour vous-même du bénéfice de la licence de brevet pour cette œuvre particulière, soit (3) vous engager, d'une façon consistante avec les obligations de cette Licence, à étendre la licence de brevet aux Destinataires de cette œuvre. "Dépendant en connaissance" signifie que vous avez effectivement connaissance que, selon la licence de brevet, votre acheminement de l'Œuvre Couverte dans un pays, ou l'utilisation de l'Œuvre Couverte par votre Destinataire dans un pays, enfreindrait un ou plusieurs brevets identifiables dans ce pays où vous avez des raisons de penser qu'ils sont valides.

Si, conformément à ou en liaison avec une même transaction ou un même arrangement, vous acheminez, ou propagez en procurant un acheminement de, une Œuvre Couverte et si accordez une licence de brevet à l'une des parties recevant l'Œuvre Couverte pour lui permettre d'utiliser, propager, modifier ou acheminer une copie spécifique de l'Œuvre Couverte, alors votre accord est automatiquement étendu à tous les Destinataires de l'Œuvre Couverte et des œuvres basées sur celle-ci.

Une licence de brevet est "discriminatoire" si, dans le champ de sa couverture, elle n'inclut pas un ou plusieurs des droits qui sont spécifiquement accordés selon cette Licence, ou en prohibe l'exercice, ou est conditionnée par le non-exercice d'un ou plusieurs de ces droits. Vous ne pouvez pas acheminer une Œuvre Couverte si vous êtes partie à un arrangement, selon lequel une partie tierce exerçant son activité dans la distribution de logiciels et à laquelle vous effectuez un paiement fondé sur l'étendue de votre activité d'acheminement de l'œuvre, et selon lequel la partie tierce accorde, à une quelconque partie qui recevrait depuis vous l'Œuvre Couverte, une licence de brevet discriminatoire (a) en relation avec les copies de l'Œuvre Couverte acheminées par vous (ou les copies réalisées à partir de ces copies), ou (b) avant tout destinée à et en relation avec des produits spécifiques ou compilations contenant l'Œuvre Couverte, à moins que vous ayez conclu cet arrangement ou que la licence de brevet ait été accordée avant le 28 mars 2007.

Rien dans cette Licence ne devrait être interprété comme devant exclure ou limiter toute licence implicite ou d'autres moyens de défense à une infraction qui vous seraient autrement disponible selon la loi applicable relative aux brevets.

Article 12. Non abandon de la liberté des autres.

Si des conditions vous sont imposées (que ce soit par décision judiciaire, par un accord ou autrement) qui contredisent les conditions de cette Licence, elles ne vous excusent pas des conditions de cette Licence. Si vous ne pouvez pas acheminer une Œuvre Couverte de façon à satisfaire simultanément vos obligations suivant cette Licence et toutes autres obligations pertinentes, alors en conséquence vous ne pouvez pas du tout l'acheminer. Par exemple, si vous avez un accord sur des termes qui vous obligent à collecter pour le réacheminement des royalties depuis ceux à qui vous acheminez le Programme, la seule façon qui puisse vous permettre de satisfaire à la fois à ces termes et ceux de cette Licence sera de vous abstenir entièrement d'acheminer le Programme.

Article 13. Utilisation avec la Licence Générale Publique Affero GNU.

Nonobstant toute autre clause de cette Licence, vous avez la permission de lier ou combiner toute Œuvre Couverte avec une œuvre placée sous la version 3 de la Licence Générale Publique GNU Affero ("GNU Affero General Public License") en une seule œuvre combinée, et d'acheminer l'œuvre résultante. Les termes de cette Licence continueront à s'appliquer à la partie formant une Œuvre Couverte, mais les obligations spéciales de la Licence Générale Publique GNU Affero, article 13, concernant l'interaction à travers un réseau, s'appliqueront à la combinaison en tant que telle.

Article 14. Versions révisées de cette Licence.

La Free Software Foundation peut publier des versions révisées et/ou nouvelles de la Licence Publique Générale GNU ("GNU General Public License") de temps en temps. De telles version nouvelles resteront similaires dans l'esprit avec la présente version, mais peuvent différer dans le détail afin de traiter de nouveaux problèmes ou préoccupations.

Chaque version reçoit un numéro de version distinctif. Si le Programme indique qu'une version spécifique de la Licence Publique Générale GNU "ou toute version ultérieure" ("or any later version") s'applique à celui-ci, vous avez le choix de suivre soit les termes et conditions de cette version numérotée, soit ceux de n'importe quelle version publiée ultérieurement par la Free Software Foundation. Si le Programme n'indique pas une version spécifique de la Licence Publique Générale GNU, vous pouvez choisir l'une quelconque des versions qui ont été publiées par la Free Software Foundation.

Si le Programme spécifie qu'un intermédiaire peut décider quelles versions futures de la Licence Générale Publique GNU peut être utilisée, la déclaration publique d'acceptation d'une version par cet intermédiaire vous autorise à choisir cette version pour le Programme.

Des versions ultérieures de la licence peuvent vous donner des permissions additionnelles ou différentes. Cependant aucune obligation additionnelle n'est imposée à l'un des auteurs ou titulaires de Droit d'Auteur du fait de votre choix de suivre une version ultérieure.

Article 15. Déclaration d'absence de garantie.

Il n'y a aucune garantie pour le programme, dans les limites permises par la loi applicable. À moins que cela ne soit établi différemment par écrit, les propriétaires de droits et/ou les autres parties fournissent le programme "en l'état" sans garantie d'aucune sorte, qu'elle soit exprimée ou implicite, ceci comprenant, sans se limiter à celles-ci, les garanties implicites de commercialisabilité et d'adéquation à un objectif particulier. Vous assumez le risque entier concernant la qualité et les performances du programme. Dans l'éventualité où le programme s'avérerait défectueux, vous assumez les coûts de tous les services, réparations ou corrections nécessaires.

Article 16. Limitation de responsabilité.

En aucune autre circonstance que celles requises par la loi applicable ou accordées par écrit, un titulaire de droits sur le programme, ou tout autre partie qui modifie ou achemine le programme comme permis ci-dessus, ne peut être tenu pour responsable envers vous pour les dommages, incluant tout dommage général, spécial, accidentel ou induit survenant par suite de l'utilisation ou de l'incapacité d'utiliser le programme (y compris, sans se limiter à celles-ci, la perte de données ou l'inexactitude des données retournées ou les pertes subies par vous ou des parties tierces ou l'incapacité du programme à fonctionner avec tout autre programme), même si un tel titulaire ou toute autre partie a été avisé de la possibilité de tels dommages.

Article 17. Interprétation des sections 15 et 16.

Si la déclaration d'absence de garantie et la limitation de responsabilité fournies ci-dessus ne peuvent prendre effet localement selon leurs termes, les cours de justice qui les examinent doivent appliquer la législation locale qui approche au plus près possible une levée absolue de toute responsabilité civile liée au Programme, à moins qu'une garantie ou assumation de responsabilité accompagne une copie du Programme en échange d'un paiement.