Mettre en place fail2ban sur Debian

fr:Mettre en place fail2ban sur Debian ro:Implementa fail2ban pe Debian pl:Fail2ban wdrożenia na Debianie he:יישם את fail2ban על דביאן ru:Реализовать fail2ban на Debian ja:Debian の fail2ban を実装します。 ar:تنفيذ fail2ban على ديبيان zh:在 Debian 上实现 fail2ban de:Fail2ban auf Debian zu implementieren nl:Implementeren fail2ban op Debian it:Implementare fail2ban su Debian pt:Implementar o fail2ban no Debian es:Implementar fail2ban en Debian en:Implement fail2ban on Debian

Introduction

Une machine connectée en permanence constitue une cible de choix pour les attaques extérieures. Bien que l'utilisation d'un pare-feu réduise grandement les risques, il est nécessaire de contrôler les accès protégés par mot de passe d'un trop grand nombre de demandes de connexion échouées, dans le cas par exemple des attaques par *force brute* ou *bruteforce*

L'outil **fail2ban** permet de surveiller l'activité des logs de certains services, tel que SSH ou Apache. Lors d'un trop grand nombre d'authentifications ratées **fail2ban** va générer une règle IPTables, cette règle aura pour but d'interdire pendant une durée déterminée les connexions depuis l'adresse IP susceptible d'être un attaquant.
Cet article a pour but d'introduire le service fail2ban et sa configuration. Cet article n'est pas exhaustif sur les paramètres de configuration du service, il vous appartient de vérifier la cohérence de la configuration avec votre système.

Pré-requis

L'un des pré-requis essentiel est de conserver son système le plus à jour possible.

```
apt-get update
apt-get upgrade
```

Afin de conserver votre système Debian [1] à jour, assurez-vous de posséder une liste des dépôts officiels. Vous pourrez trouver une liste des dépôts disponibles chez Ikoula et les instructions d'installation à cette adresse.

Avertissement: Avant toute modification de votre système prévoyez toujours une sauvegarde [2] de vos fichiers en cas de mauvaise manipulation.
Sur un serveur [3] de production, pensez à effectuer ces opérations pendant les heures creuses afin de minimiser l'impact de vos actions.

Mise en place

Installation de fail2ban

Installer fail2ban, qui est normalement présent dans les paquets officiels Debian

```
apt-get install fail2ban
```

Le service **fail2ban** est maintenant installé et démarré.

Fichier de configuration

La configuration de **fail2ban** est conservée dans le dossier */etc/fail2ban*. La configuration par défaut est définie dans le fichier **jail.conf**, ce fichier est automatiquement modifié lors des mises à jour du service, il est donc recommandé d'effectuer la configuration du service **fail2ban** dans un fichier de paramètres local **jail.local**, par exemple.

Copier le fichier jail.conf vers jail.local

```
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

Nous pouvons à présent éditer la configuration de **fail2ban** afin de personnaliser son comportement.

Configuration

Afin de modifier la configuration, il nous faut éditer le fichier **jail.local**.

Editer le fichier jail.conf

```
vi /etc/fail2ban/jail.local
```

Le fichier de configuration s'organise autour de différentes sections

Section DEFAULT

La partie *DEFAULT* qui permet de personnaliser le comportement général du service tel que les adresse IP ignorées, le temps d'un ban, le nombre maximum d'essais autorisés. Cette section est le plus souvent correctement configurée pour votre usage, vous pouvez cependant la modifier afin d'ajuster son comportement à la configuration de votre système.
Parmi les paramètres de la section *DEFAULT* voici les plus importants :

- **Ignoreip**: Ce paramètre sert à exclure une ou plusieurs adresses IP de fail2ban, ce paramètre est utile afin d'éviter de vous bannir vous-même ou un de vos utilisateurs si il vous arrivait d'oublier votre mot de passe un trop grand nombre de fois.
- **Bantime**: Ce paramètre sert à définir le temps en secondes d'un bannissement. Par défaut le bannissement dure 10 minutes.
- **Maxretry**: Ce paramètre sert à définir un nombre maximal d'essais ratés avant d'entreprendre un bannissement de l'utilisateur.

Section ACTION

La partie *ACTION* définie la réaction de **fail2ban** lorsque le nombre d'essai maximum a été atteint. Nous pouvons par exemple définir le destinataire du mail d'alerte, le service mail utilisé, le protocole par défaut de la surveillance, ainsi que l'action entreprise par **fail2ban** qui peut aller du simple ban au relevé d'informations complet sur l'origine de l'attaque et du *reporting* vers un service de blacklist choisi (Cloudfare, Badips.com, Blocklist.de, ...)
La section *ACTION* permet de définir le comportement de **fail2ban** lors d'un bannissement.

- **Banaction**: Ce paramètre sert à définir le fichier appelé lors d'un bannissement. Par défaut c'est l'appel à IPTables qui est effectué afin de bannir l'adresse IP sur tous les ports
- **Action**: Ce paramètre sert à définir l'action exécutée lors d'un bannissement. Plusieurs raccourcis sont disponibles comme par exemple l'établissement d'une règle IPTables ou l'envoi d'un mail d'alerte.

Section JAILS

La section *JAILS* permet de définir un comportement personnalisé pour les différents services surveillés tels que ssh, apache, etc...
La syntaxe générale d'une section *JAIL* est la suivante:

```
# nom de l'application ou du service
[sshd]
# le port sur lequel la surveillance doit être effectuée, ce peut être un chiffre (22) ou un mot-clé de protocole (ssh)
port = ssh
# le chemin du fichier de log sur lequel fail2ban doit aller vérifier
```

```
logpath = %(sshd_log)s


# Nous pouvons également "override" les paramètres par défauts, par exemple le nombre d'essais max
maxretry = 3 ; Abaisser le nombre d'erreurs à 3 pour le ssh
# Egalement le temps d'un bannissement
bantime = 1200 ; Doubler le temps de bannissement pour le ssh
```

Le fichier de configuration par défaut de **fail2ban** contient déjà un certain nombre de services. Il est donc recommandé d'effectuer d'abord une recherche sur les services présents avant d'en ajouter un nouveau.

Redémarrage

Lorsque toutes les modifications sont terminées, il vous suffit de redémarrer le service **fail2ban** pour que la nouvelle configuration soit prise en compte.

Redémarrer le service

```
service fail2ban restart
```

Options

Le service **fail2ban** possède de nombreux autres configurations possibles. Parmi lesquelles la configuration de l'envoi de mail, la possibilité de grouper l'envoi d'un mail après un nombre défini de bannissements.
Afin de configurer les différentes options nous vous invitons à vous reporter au site officiel **fail2ban**.

"Interagir avec le service Fail2ban/Liste des commandes"

Lister tout les commandes du Client fail2ban.

```
fail2ban-client -h
```

Obtenir l'état actuel du serveur :

```
sudo fail2ban-client status
```

Vérifiez le statut de la prison (SSHD):

```
sudo fail2ban-client status sshd
```

Débannir une IP :

```
sudo fail2ban-client set sshd unbanip 11.22.33.44
```

Bannir une IP :

```
sudo fail2ban-client set sshd banip 11.22.33.44
```

Vérification en temps réel logs d'authentification du Serveur.

```
tail -f /var/log/auth.log
```

Références

[1] https://www.ikoula.com/fr/serveur-dedie/linux/debian
[2] https://express.ikoula.com/fr/sauvegarde-et-restauration
[3] https://express.ikoula.com/fr/serveur-dedie

Sources et contributeurs de l'article

Mettre en place fail2ban sur Debian *Source*: https://fr-wiki.ikoula.com/index.php?oldid=31584 *Contributeurs*: Blejeune06c94, Cbrochot1072d, Ccunha64415, Tallartazzola50781, Woussen.alexis59c630e