Installation et utilisation de Fail2Ban

Fail2ban est un outil utile pour sécuriser votre serveur Ubuntu en bloquant les adresses IP qui montrent des signes de comportement malveillant, comme des tentatives répétées de connexion échouées. Voici les étapes pour installer et configurer Fail2ban sur un serveur Ubuntu :

Étape 1: Mise à jour des paquets

Avant d'installer de nouveaux logiciels, il est toujours conseillé de mettre à jour la liste des paquets et d'installer les mises à jour disponibles.

```
sudo apt update
sudo apt upgrade
```

Étape 2: Installation de Fail2ban

Installez Fail2ban à l'aide de la commande `apt`.

```
sudo apt install fail2ban
```

Étape 3: Configuration de Fail2ban

1. **Copier le fichier de configuration par défaut :**

   Pour éviter que vos modifications soient écrasées lors des mises à jour de Fail2ban, copiez le fichier de configuration par défaut.

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

2. **Éditer le fichier `jail.local` :**

   Ouvrez le fichier `jail.local` pour le modifier.

```
sudo nano /etc/fail2ban/jail.local
```

Dans ce fichier, vous pouvez configurer les options globales et spécifiques aux services. Les options courantes à configurer sont :

- **ignoreip** : Liste des adresses IP à ne jamais bannir.
- **bantime** : Durée du bannissement d'une IP (par défaut 10 minutes).
- **findtime** : Période pendant laquelle les tentatives de connexion échouées sont comptabilisées.
- **maxretry** : Nombre de tentatives échouées avant le bannissement. Par exemple, pour définir des valeurs spécifiques :

```
[DEFAULT]
ignoreip = 127.0.0.1/8 ::1
bantime  = 3600
findtime = 600
maxretry = 5
```

3. **Activer des jails spécifiques :**

   Fail2ban utilise des "jails" pour surveiller les services. Vous pouvez activer et configurer des jails spécifiques pour des services comme SSH, Apache, etc. Par exemple, pour activer et configurer le jail pour SSH :

```
[sshd]
enabled = true
port    = ssh
logpath = /var/log/auth.log
maxretry = 5
```

Étape 4: Redémarrer Fail2ban

Après avoir modifié la configuration, redémarrez Fail2ban pour appliquer les changements.

```
sudo systemctl restart fail2ban
```

Étape 5: Vérifier le statut de Fail2ban

Vérifiez que Fail2ban fonctionne correctement et surveille les jails activés.

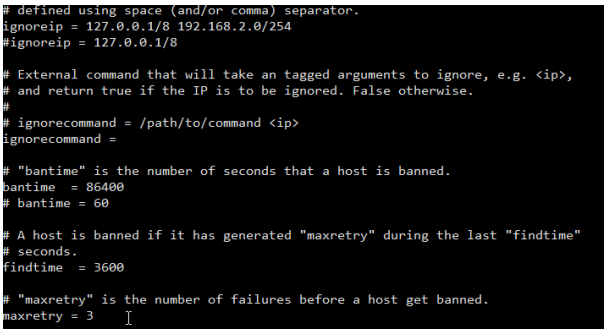
```
sudo systemctl status fail2ban
```

Étape 6: Surveiller Fail2ban

Vous pouvez vérifier les logs de Fail2ban pour voir quelles actions il a prises.

```
sudo tail -f /var/log/fail2ban.log
```

Commandes Utiles



- **Lister les jails actifs :**

  ```
  sudo fail2ban-client status
  ```

- **Vérifier le statut d'un jail spécifique :**

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

- **Débannir une IP spécifique :**

  ```
  sudo fail2ban-client set sshd unbanip <IP_ADDRESS>
  ```

Conclusion

En suivant ces étapes, vous aurez installé et configuré Fail2ban sur votre serveur Ubuntu pour renforcer sa sécurité contre les tentatives de connexion non autorisées.