

Crowdsec

Installation de Crowdsec

```
curl -s  
https://packagecloud.io/install/repositories/crowdsec/crowdsec/script.deb.sh  
| bash  
apt-get install crowdsec  
systemctl restart crowdsec
```

Installation d'un bouncer Crowdsec

Un bouncer est une application qui prend action sur base des détections de Crowdsec. Il en existe pour plusieurs applications (wordpress, nginx, ...) mais ici je propose de bloquer l'attaquant par règles firewall.

```
apt install crowdsec-firewall-bouncer-iptables
```

Après il est possible de voir les règles de blocage en application:

```
ipset list crowdsec-blacklists
```

Quelques commandes

```
# Liste les collections  
cscli collections list  
# Liste les décisions locales  
cscli decision list  
# Liste les décisions venant du serveur central de Crowdsec (ou un serveur  
central intermédiaire si configuré)  
cscli decisions list --origin CAPI  
# Liste toutes les décisions  
cscli decisions list --all  
# Liste les alertes  
cscli alerts list  
# Liste les bouncers enregistrés  
cscli bouncers list  
# Supprimer une décision s'appliquant à une ip spécifique  
cscli decisions delete -i 1.2.3.4
```

From:

<https://wiki.makeitsimple.be/> - makeITsimple wiki

Permanent link:

<https://wiki.makeitsimple.be/doku.php?id=linux:crowdsec>

Last update: **2023/12/26 09:02**

