Installer CrowdSec pour Apache sur Debian 11

Dans cette procédure, je vais vous montrer comment installer CrowdSec sur Debian 11 pour protéger son site Web Apache. CrowdSec est un outil qui va permettre de bloquer les attaques qu'il détecte sur le serveur, nous allons utilisé un serveur Debian 11 dans notre démonstration. CrowdSec fonctionne avec des modules appelés des Bouncers. Les bouncers permettent de bloqué les trafics réseau qui ne sont pas détecter comme « normaux ». Ils peuvent soit bloqué complètement la requête ou afficher à Captcha dans le but de vérifier qu'il ne s'agit pas d'un robot.

Prérequis :

- Une machine Debian avec Apache2 d'installé.
- Avoir Composer d'installer
- Avoir les permissions root ou avoir sudo

Installer CrowdSec pour Apache 2 sur Debian 11 :

Avant de commencer l'installation de CrowdSec, commencer par mettre à jour la liste des paquets votre machine Debian 11

```
sudo apt update
```

Ensuite télécharger le CrowdSec sur votre machine Debian :

```
sudo apt install -y crowdsec
```

Après avoir installer CrowdSec sur votre machine, la CLI de CrowdSec (CSCLI) vous permet de voir les services pouvant être protéger par CrowdSec présents sur votre machine.

```
cscli collections list
```

```
root@localhost:~# cscli collections list
--------------------------------------------------------------------------------------------------------------
 NAME                                  STATUS    VERSION  LOCAL PATH
--------------------------------------------------------------------------------------------------------------
 crowdsecurity/modsecurity             ✔ enabled  0.1      /etc/crowdsec/collections/modsecurity.yaml
 crowdsecurity/vsftpd                  ✔ enabled  0.1      /etc/crowdsec/collections/vsftpd.yaml
 crowdsecurity/sshd                    ✔ enabled  0.1      /etc/crowdsec/collections/sshd.yaml
 crowdsecurity/base-http-scenarios     ✔ enabled  0.4      /etc/crowdsec/collections/base-http-scenarios.yaml
 crowdsecurity/mysql                   ✔ enabled  0.1      /etc/crowdsec/collections/mysql.yaml
 crowdsecurity/linux                   ✔ enabled  0.2      /etc/crowdsec/collections/linux.yaml
 crowdsecurity/postfix                 ✔ enabled  0.2      /etc/crowdsec/collections/postfix.yaml
 crowdsecurity/whitelist-good-actors   ✔ enabled  0.1      /etc/crowdsec/collections/whitelist-good-actors.yaml
 crowdsecurity/apache2                 ✔ enabled  0.1      /etc/crowdsec/collections/apache2.yaml
 crowdsecurity/dovecot                 ✔ enabled  0.1      /etc/crowdsec/collections/dovecot.yaml
 crowdsecurity/nginx                   ✔ enabled  0.1      /etc/crowdsec/collections/nginx.yaml
 crowdsecurity/wordpress               ✔ enabled  0.1      /etc/crowdsec/collections/wordpress.yaml
 crowdsecurity/iptables                ✔ enabled  0.1      /etc/crowdsec/collections/iptables.yaml
 crowdsecurity/naxsi                   ✔ enabled  0.1      /etc/crowdsec/collections/naxsi.yaml
--------------------------------------------------------------------------------------------------------------
```

Vous pouvez également lister les bouncers installés et disponibles sur votre machine :

```
cscli bouncers list
```

Si vous exécutez cette commande, vous allez voir un tableau vide. C’est normal car nous n’avons pas encore installer de bouncer.

Installation du Bouncer Apache 2 sur CrowdSec (Debian 11) :

Avant de commencer l’installation du Bouncer, assurez-vous d’avoir composer d’installé. Si vous ne l’avez pas installer, voici une procédure pour l’installer :

Installer Composer sur Debian 11

Nous allons installer git sur la machine pour pouvoir cloner le Repo du bouncer :

```
sudo apt install git -y
```

Puis nous clonons le Repo GitHub :

```
git clone https://github.com/crowdsecurity/cs-php-bouncer.git
```

On se rend dans le dossier du projet :

```
cd cs-php-bouncer/
```

Enfin on lance l'installation avec un compte utilisateur (pas avec le compte root ni avec sudo mais le compte utilisateur doit être dans le groupe 'sudo')

```
./install.sh --apache
```

Puis on donne les droit en tant que propriétaire www-data (apache) sur le répertoire de CrowdSec

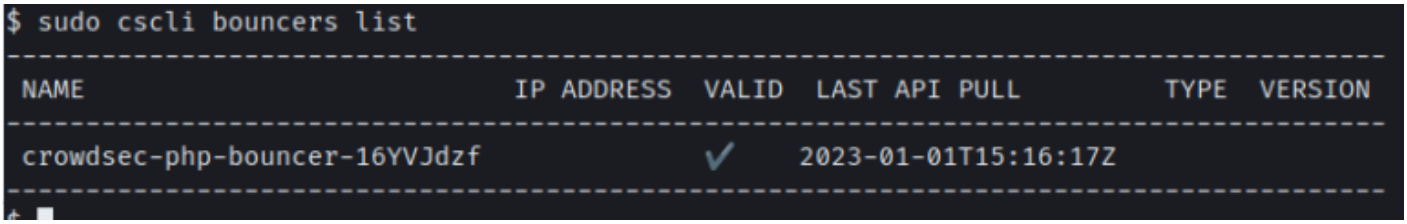
```
sudo chown www-data /usr/local/php/crowdsec/
```

Puis on redémarre le service de Apache

```
sudo systemctl reload apache2
```

Enfin le Bouncer de Apache va apparaître dans la liste des bouncers :

```
sudo cscli bouncers list
```



Ensuite on va afficher un Captcha pour les utilisateurs qui consulterons notre site web avec un mauvais User-agent (Généralement les outils de pentest utilisent des User-Agent différent des navigateurs Web) et les crawler non static.

On va modifier le fichier de configuration :

```
sudo nano /etc/crowdsec/profiles.yaml
```

```
# Mauvais User-Agent + Crawler
name: crawler_captcha_remediation
filters:
 - Alert.Remediation == true && Alert.GetScenario() in ["crowdsecurity/http-crawl-non_statics",
decisions:
 - type: captcha
   duration: 4h
on_success: break
---
name: default_ip_remediation
filters:
 - Alert.Remediation == true && Alert.GetScope() == "Ip"
decisions:
```

```
 - type: ban
   duration: 4h
on_success: break
---
```

Puis on redémarre CrowdSec pour qu'il utilise la nouvelle configuration :

```
sudo systemctl restart crowdsec
```

Il est possible d'afficher toutes les actions que CrowdSec aura pris avec cette commande :

```
sudo cscli decisions list
```

C'est également possible de débanir une adresse IP :

```
sudo cscli decisions delete --ip adresse-ip-a-deban
```

La CLI de CrowdSec est pratique mais CrowSec propose également une interface graphique Web avec Docker.

> Sources :
>
> *https://doc.crowdsec.net/*

Created 2025-01-30 17:08:54 UTC by Nicolas
Updated 2025-01-30 17:09:28 UTC by Nicolas