How to install Fail2ban on ClearOS

2021-07-20: WikiSuite will now support all major Linux distros. Thus, the information below is no longer updated. It may still be valid, or not. It will be eventually removed from this site, so anything relevant should be moved to the appropriate site. For anything related to ClearOS, please search among the following: ClearOS site, code base, Developer docs, Wiki or forum.

Please contact us if you would like to help out.

This page is deprecated and will eventually be deleted, because of the New Attack Detector app from ClearOS (Fail2ban)

Please see: How to install Attack Detector (Fail2ban) on ClearOS

Make sure the clearos-epel repository is enabled

```
yum --enablerepo=clearos-centos,centos-updates-unverified install fail2ban fail2ban-systemd
```

In ClearOS 7, it is very important the sub package systemd is installed. By default, fail2ban won't do anything out of the box. You need to tell it what to do.

Edit or create a file in /etc/fail2ban/jail.d/99-fail2ban by type in CLI

```
nano /etc/fail2ban/jail.d/99-fail2ban
```

and put this content.

```
[ssh-iptables]
enabled = true
filter = sshd
action = iptables[name=SSH, port=ssh, protocol=tcp]
        sendmail-whois[name=SSH, dest=sysadmin@example.com, sender=example@example.com]
maxretry = 2
bantime = 3600
```

Edit /etc/fail2ban/jail.conf and turn on the enable flag to true. By default all is off.

```
nano /etc/fail2ban/jail.conf
```
WikiSuite: The most comprehensive and integrated Open Source enterprise solution.

In nano editor, search all (Ctrl+W+Enter for next search) enabled = false and replace false by true.

This will start blocking. This configuration will ban for 1 hour. To finish, do the following.

```
systemctl enable fail2ban
systemctl start fail2ban
```

Related links

https://tracker.clearos.com/view.php?id=7771