Almely Ramos

Faill2Ban installation

Linux Admin

10/7/19

Step 1: You must be root to install this program.

Run these commands to install fail2ban

(CENTOS) “**yum install epel-release**”

Then “**yum install fail2ban-systemd**”

A screenshot of text

Description automatically generated



Step 2:

**Starting Fail2ban**

You must enable it on the system before you can use Fail2Ban

Use the command “ **systemctl enable fail2ban**”

A close up of a logo

Description automatically generated

Now you must start it, use command “**systemctl start fail2ban**”

A picture containing object

Description automatically generated

Step 3:

**Adjusting Fail2Ban**

The fail2ban config file I located at /etc/fail2ban/jail.conf . It is not recommended that you work from there, so we will copy the config file to jail.local.

Use the following statement: “**cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local**” so now we can use this file to make our changes safely.



**Configuring the Fail2ban Config file**

To configure the file, simply use a text editor (VI, VIM, OR NANO)

A close up of a logo

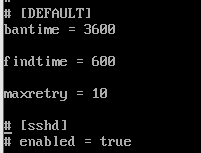
Description automatically generated

This is how it should look like:  
A screenshot of a cell phone

Description automatically generated

This is where you will add your rules.

Here are some of my rules:



Ban time – As the name says, it is a set timer for the amount of seconds someone is banned from trying to connect to the sever

Findtime- Rule to ban host if it uses up the maxretry rule during the findtime.

Maxretry- Number of retries before the person trying to connect gets banned.

Step 4:

MAKE SURE TO RESTART FAIL2BAN TO SEE CHANGES

Use command “**systemctl restart fail2ban**”