Fail2Ban for Kamailio on VoipNow 4.0.0

Applies to VoipNow 4.0.0!

Fail2Ban works by actively monitoring log files and triggering various actions based on the content of the log files.

For example, it can detect a line in your mail log file similar to the one shown below:

```
Jan  7 11:25:45 hostname sendmail[1558]: s07BPgwK001558: AUTH failure (LOGIN): authentication failure (-13) SASL
(-13): authentication failure: checkpass failed, relay=[67.216.253.197]
```

and trigger an action, such as banning the offender's IP with Firewalld.

Each monitored log is configured as a "jail" - a corresponding section in the `/etc/fail2ban/jail.local` file.

Here's a sample of jail entry that blocks SSH access:

```
[ssh]
enabled = true
port    = ssh
filter  = sshd
logpath  = /var/log/auth.log
maxretry = 6
```

The filter, which triggers the action, and the action itself are defined as separate files under `/etc/fail2ban/filter.d` and `/etc/fail2ban/action.d`.

Step-by-step guide

Requirements

- VoipNow 4.0.0 server on CentOS 7/RHEL 7 or higher
- EPEL repository to install the fail2ban rpm
- Internet access

1) Install EPEL

EPEL is a repository of additional RPM packages which can be used in RHEL, CentOS, Fedora, and other similar distributions. For more details about the project, visit the EPEL page.

If you're using CentOS, a package named epel-release is already included in the stock repository.

To install EPEL, run the following command:

```
yum install epel-release
```

and follow the on-screen instructions.

```
# yum -y install epel-release
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.ch-center.com
 * extras: mirrors.ch-center.com
 * updates: mirrors.ch-center.com
Resolving Dependencies
--> Running transaction check
---> Package epel-release.noarch 0:7-5 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=================================================================================================================
=================================================================================================================
=============
 Package
Arch                                                     Version
Repository                                                Size
=================================================================================================================
=================================================================================================================
=============
Installing:
 epel-release
noarch                                                   7-5
extras                                                    14 k

Transaction Summary
=================================================================================================================
=================================================================================================================
=============
Install  1 Package

Total download size: 14 k
Installed size: 24 k
Downloading packages:
epel-release-7-5.noarch.
rpm
|  14 kB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : epel-release-7-5.
noarch
1/1
  Verifying  : epel-release-7-5.
noarch
1/1

Installed:
  epel-release.noarch 0:7-5

Complete!
```

Next, install Fail2Ban.

2) Install Fail2Ban

```
# yum -y install fail2ban
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.ch-center.com
 * epel: mirrors.netix.net
 * extras: mirrors.ch-center.com
 * updates: mirrors.ch-center.com
```

```
Resolving Dependencies
--> Running transaction check
---> Package fail2ban.noarch 0:0.9.3-1.el7 will be installed
--> Processing Dependency: fail2ban-server = 0.9.3-1.el7 for package: fail2ban-0.9.3-1.el7.noarch
--> Processing Dependency: fail2ban-sendmail = 0.9.3-1.el7 for package: fail2ban-0.9.3-1.el7.noarch
--> Processing Dependency: fail2ban-firewalld = 0.9.3-1.el7 for package: fail2ban-0.9.3-1.el7.noarch
--> Running transaction check
---> Package fail2ban-firewalld.noarch 0:0.9.3-1.el7 will be installed
---> Package fail2ban-sendmail.noarch 0:0.9.3-1.el7 will be installed
---> Package fail2ban-server.noarch 0:0.9.3-1.el7 will be installed
--> Processing Dependency: systemd-python for package: fail2ban-server-0.9.3-1.el7.noarch
--> Processing Dependency: ipset for package: fail2ban-server-0.9.3-1.el7.noarch
--> Running transaction check
---> Package ipset.x86_64 0:6.19-4.el7 will be installed
--> Processing Dependency: ipset-libs = 6.19-4.el7 for package: ipset-6.19-4.el7.x86_64
--> Processing Dependency: libipset.so.3(LIBIPSET_3.0)(64bit) for package: ipset-6.19-4.el7.x86_64
--> Processing Dependency: libipset.so.3(LIBIPSET_2.0)(64bit) for package: ipset-6.19-4.el7.x86_64
--> Processing Dependency: libipset.so.3(LIBIPSET_1.0)(64bit) for package: ipset-6.19-4.el7.x86_64
--> Processing Dependency: libipset.so.3()(64bit) for package: ipset-6.19-4.el7.x86_64
---> Package systemd-python.x86_64 0:208-20.el7_1.6 will be installed
--> Running transaction check
---> Package ipset-libs.x86_64 0:6.19-4.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=================================================================================================================
=================================================================================================================
=============
 Package
Arch
Version
Repository                                                  Size
=================================================================================================================
=================================================================================================================
=============
Installing:
 fail2ban
noarch                                                  0.9.3-1.
el7                                                      epel                                                  9.7 k
Installing for dependencies:
 fail2ban-firewalld
noarch                                                  0.9.3-1.
el7                                                      epel                                                  9.9 k
 fail2ban-sendmail
noarch                                                  0.9.3-1.
el7                                                      epel                                                   13 k
 fail2ban-server
noarch                                                  0.9.3-1.
el7                                                      epel                                                  395 k
 ipset
x86_64                                                  6.19-4.
el7                                                        base                                                  36 k
 ipset-libs
x86_64                                                  6.19-4.
el7                                                        base                                                  46 k
 systemd-python
x86_64                                                  208-20.el7_1.
6                                                     updates                                                 91 k

Transaction Summary
=================================================================================================================
=================================================================================================================
=============
Install  1 Package (+6 Dependent packages)

Total download size: 600 k
Installed size: 1.7 M
Downloading packages:
(1/7): fail2ban-0.9.3-1.el7.noarch.
rpm
```

```
| 9.7 kB  00:00:00
(2/7): fail2ban-firewalld-0.9.3-1.el7.noarch.
rpm
| 9.9 kB  00:00:00
(3/7): fail2ban-sendmail-0.9.3-1.el7.noarch.
rpm
|  13 kB  00:00:00
(4/7): fail2ban-server-0.9.3-1.el7.noarch.
rpm
| 395 kB  00:00:00
(5/7): ipset-6.19-4.el7.x86_64.
rpm
|  36 kB  00:00:00
(6/7): systemd-python-208-20.el7_1.6.x86_64.
rpm
|  91 kB  00:00:00
(7/7): ipset-libs-6.19-4.el7.x86_64.
rpm
|  46 kB  00:00:01
------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------
-------------
Total
342 kB/s | 600 kB  00:00:01
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : systemd-python-208-20.el7_1.6.
x86_64
1/7
  Installing : ipset-libs-6.19-4.el7.
x86_64
2/7
  Installing : ipset-6.19-4.el7.
x86_64
3/7
  Installing : fail2ban-server-0.9.3-1.el7.
noarch
4/7
  Installing : fail2ban-firewalld-0.9.3-1.el7.
noarch
5/7
  Installing : fail2ban-sendmail-0.9.3-1.el7.
noarch
6/7
  Installing : fail2ban-0.9.3-1.el7.
noarch
7/7
  Verifying  : fail2ban-firewalld-0.9.3-1.el7.
noarch
1/7
  Verifying  : ipset-libs-6.19-4.el7.
x86_64
2/7
  Verifying  : ipset-6.19-4.el7.
x86_64
3/7
  Verifying  : fail2ban-0.9.3-1.el7.
noarch
4/7
  Verifying  : fail2ban-server-0.9.3-1.el7.
noarch
5/7
  Verifying  : fail2ban-sendmail-0.9.3-1.el7.
noarch
6/7
  Verifying  : systemd-python-208-20.el7_1.6.
x86_64
7/7
```

```
Installed:
  fail2ban.noarch 0:0.9.3-1.el7

Dependency Installed:
  fail2ban-firewalld.noarch 0:0.9.3-1.el7     fail2ban-sendmail.noarch 0:0.9.3-1.el7     fail2ban-server.noarch
0:0.9.3-1.el7     ipset.x86_64 0:6.19-4.el7     ipset-libs.x86_64 0:6.19-4.el7     systemd-python.x86_64 0:208-
20.el7_1.6

Complete!
```

3) Enable and start Firewalld

Firewalld is the new firewall daemon introduced in CentOS/RHEL 7 and set to replace iptables in further releases.

To enable this service, run the following command:

```
# systemctl enable firewalld
ln -s '/usr/lib/systemd/system/firewalld.service' '/etc/systemd/system/dbus-org.fedoraproject.FirewallD1.
service'
ln -s '/usr/lib/systemd/system/firewalld.service' '/etc/systemd/system/basic.target.wants/firewalld.service'
```

This command only enables the daemon, but does not start it.

To start the daemon and check its status, run the following:

```
# systemctl start firewalld

]# systemctl status firewalld
firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled)
   Active: active (running) since Tue 2015-12-08 09:57:56 UTC; 17s ago
 Main PID: 27859 (firewalld)
   CGroup: /system.slice/firewalld.service
           27859 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid
Dec 08 09:57:56 centos71 systemd[1]: Started firewalld - dynamic firewall daemon.
```

At this point, the service should appear as loaded and active.

4) Enable and start Fail2Ban

To enable and start the Fail2Ban service, run the following:

```
# systemctl enable fail2ban
ln -s '/usr/lib/systemd/system/fail2ban.service' '/etc/systemd/system/multi-user.target.wants/fail2ban.service'

# systemctl start fail2ban

# systemctl status fail2ban
fail2ban.service - Fail2Ban Service
   Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled)
   Active: active (running) since Tue 2015-12-08 09:59:21 UTC; 3s ago
     Docs: man:fail2ban(1)
  Process: 29758 ExecStart=/usr/bin/fail2ban-client -x start (code=exited, status=0/SUCCESS)
 Main PID: 29761 (fail2ban-server)
   CGroup: /system.slice/fail2ban.service
           29761 /usr/bin/python2 -s /usr/bin/fail2ban-server -s /var/run/fail2ban/fail2ban.sock -p /var/run
/fail2ban/fail2ban.pid -x -b
Dec 08 09:59:21 centos71 systemd[1]: Starting Fail2Ban Service...
Dec 08 09:59:21 centos71 fail2ban-client[29758]: 2015-12-08 09:59:21,695 fail2ban.server         [29759]:
INFO    Starting Fail2ban v0.9.3
Dec 08 09:59:21 centos71 fail2ban-client[29758]: 2015-12-08 09:59:21,695 fail2ban.server         [29759]:
INFO    Starting in daemon mode
Dec 08 09:59:21 centos71 systemd[1]: Started Fail2Ban Service.
```

5) Configure Fail2Ban to pick up the log trigger

As mentioned before, Fail2Ban monitors log files and triggers actions upon certain events being detected in these log files.

Starting with VoipNow 4.0.0, the PIKE module is used to log and throttle incoming request IP addresses.

The messages logged by Kamailio look like this:

```
1449744585: L1 Pike block from 10.150.5.113:5061
1449744585: L2 Pike block from 10.150.5.113:5061
1449744585: L3 Pike block from 10.150.5.113:5061
```

You need to create the Kamailio configuration file for Fail2Ban. This file needs must be placed in `/etc/fail2ban/filter.d/kamailio.conf` and must contain the following:

```
[Definition]
failregex = L. Pike block from <HOST>.*
```

Edit `/etc/fail2ban/jail.conf` and add:

```
[kamailio]
enabled  = true
filter   = kamailio
banaction   = firewallcmd-ipset
logpath  = /var/log/kamailio/abuse.log
maxretry = 5
bantime  = 3600
ignoreip = 127.0.0.0/8 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16
```

Define your whitelists

When setting up any type of restriction, it's a good idea to start by defining your whitelists (i.e. exceptions, for which the restrictions will not apply). For example, you can whitelist "good" IP addresses that you know very well: your own office, known customers who use static IPs, etc. Add these IPs in the **ignoreip** line.

The Kamailio jail can be tweaked using the following parameters:

- the IP will be banned after `maxretry` failed registration attempts
- the IP will be banned for `bantime` seconds

Once the configuration is done, restart Fail2Ban:

```
# systemctl reload fail2ban
```

The default Fail2Ban configuration logs messages to `/var/log/fail2ban.log`

Here you should see messages similar to:

```
2015-12-10 16:13:19,413 fail2ban.server         [12723]: INFO    Changed logging target to /var/log/fail2ban.
log for Fail2ban v0.9.3
2015-12-10 16:13:19,414 fail2ban.database       [12723]: INFO    Connected to fail2ban persistent database '/var
/lib/fail2ban/fail2ban.sqlite3'
2015-12-10 16:13:19,421 fail2ban.jail           [12723]: INFO    Creating new jail 'kamailio'
2015-12-10 16:13:19,423 fail2ban.jail           [12723]: INFO    Jail 'kamailio' uses poller
2015-12-10 16:13:19,442 fail2ban.filter         [12723]: INFO    Set jail log file encoding to UTF-8
2015-12-10 16:13:19,442 fail2ban.jail           [12723]: INFO    Initiated 'polling' backend
2015-12-10 16:13:19,456 fail2ban.filter         [12723]: INFO    Added logfile = /var/log/kamailio/abuse.log
2015-12-10 16:13:19,457 fail2ban.filter         [12723]: INFO    Set maxRetry = 5
2015-12-10 16:13:19,458 fail2ban.filter         [12723]: INFO    Set jail log file encoding to UTF-8
2015-12-10 16:13:19,459 fail2ban.actions        [12723]: INFO    Set banTime = 3600
2015-12-10 16:13:19,459 fail2ban.filter         [12723]: INFO    Set findtime = 600
2015-12-10 16:13:19,470 fail2ban.jail           [12723]: INFO    Jail 'kamailio' started
```

Once the service is started, ensure that your Fail2Ban is working.

Make sure you are not running the tests from the same IP you used to connect through SSH!

To make sure that Fail2Ban is banning the IP addresses which attempt to register with wrong passwords, try a few registrations with a wrong password yourself.

Once you've reached the number of attempts configured in the Kamailio jail, your IP should be banned and in `fail2ban.log` you will see something similar to:

```
2015-12-11 11:59:40,963 fail2ban.filter         [21060]: INFO    [kamailio] Found 10.150.8.186
2015-12-11 11:59:41,268 fail2ban.actions        [21060]: NOTICE  [kamailio] Ban 10.150.8.186
```

To ensure that the IP address was properly banned, you can use the `ipset list` command:

```
# ipset list
Name: fail2ban-default
Type: hash:ip
Revision: 1
Header: family inet hashsize 1024 maxelem 65536 timeout 600
Size in memory: 16592
References: 1
Members:
10.150.8.186 timeout 496
```

6) Use iptables instead of Firewalld

If you're not ready to switch to firewalld, you can still use iptables to manage your firewall.

Before enabling the iptables service, make sure you've disabled firewalld:

```
# systemctl stop firewalld
# systemctl mask firewalld
# yum -y install iptables-services
# touch /etc/sysconfig/iptables
# touch /etc/sysconfig/iptables6
# systemctl start iptables
# systemctl start ip6tables
# systemctl enable iptables
# systemctl enable ip6tables
```

The `/etc/fail2ban/jail.conf` should have a different `action` specified:

```
[kamailio]
enabled  = true
filter   = kamailio
action  = iptables-allports[name=kamailio, protocol=all]
logpath  = /var/log/kamailio/abuse.log
maxretry = 5
bantime  = 3600
ignoreip = 127.0.0.0/8 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16
protocol = all
```

You can check the rules using the following command:

```
iptables -L -n -v
```

7) Disable the EPEL repository

To prevent any possible VoipNow software package conflicts, you need to disable the EPEL repository by running the following command:

```
yum-config-manager --disable repository epel
```

Troubleshooting

Time problems

A common problem with fail2ban is having log entries out of sync. Make sure the system time is up to date and everything is configured to use the same time zone. For example, if the log entries are ahead in absolute time (when compared to the system local time), Fail2Ban will not report anything.

Log file scanning problems

Sometimes, you might have problems with the log file scanning. By default, Fail2ban relies on the `pyinotify` backend, which uses inotify to monitor file system events. In case this causes problems, you can switch to a polling backend by setting `backend=polling` in the Kamailio section of `jail.conf`.

If you didn't copy the example code properly, your regular expression might not be configured correctly.

To test this, use the following command:

```
# fail2ban-regex /var/log/kamailio/abuse.log /etc/fail2ban/filter.d/kamailio.conf
Running tests
=============
Use   failregex filter file : kamailio, basedir: /etc/fail2ban
Use         log file : /var/log/kamailio/abuse.log
Use         encoding : UTF-8
Results
=======
Failregex: 3 total
|-  #) [# of hits] regular expression
|   1) [3] ^.+Pike block from <HOST>:.*
`-
Ignoreregex: 0 total
Date template hits:
|- [# of hits] date format
|  [3] Epoch
`-
Lines: 3 lines, 0 ignored, 3 matched, 0 missed [processed in 0.00 sec]
```

The command output should specify how many lines were matched. In the example above, 38 matched.

Firewalld service is not started

In case the Firewalld service is not started, under /var/log/fail2ban.log you will see lines similar to the ones below:

```
2015-12-10 16:12:27,654 fail2ban.jail           [11423]: INFO    Jail 'kamailio' started
2015-12-10 16:12:27,868 fail2ban.action         [11423]: ERROR   ipset create fail2ban-default hash:ip timeout
600
firewall-cmd --direct --add-rule ipv4 filter INPUT_direct 0 -p tcp -m multiport --dports ssh -m set --match-set
fail2ban-default src -j REJECT --reject-with icmp-port-unreachable -- stdout: '\x1b[91mFirewallD is not
running\x1b[00m\n'
2015-12-10 16:12:27,868 fail2ban.action         [11423]: ERROR   ipset create fail2ban-default hash:ip timeout
600
firewall-cmd --direct --add-rule ipv4 filter INPUT_direct 0 -p tcp -m multiport --dports ssh -m set --match-set
fail2ban-default src -j REJECT --reject-with icmp-port-unreachable -- stderr: ''
2015-12-10 16:12:27,868 fail2ban.action         [11423]: ERROR   ipset create fail2ban-default hash:ip timeout
600
firewall-cmd --direct --add-rule ipv4 filter INPUT_direct 0 -p tcp -m multiport --dports ssh -m set --match-set
fail2ban-default src -j REJECT --reject-with icmp-port-unreachable -- returned 252
2015-12-10 16:12:27,868 fail2ban.actions        [11423]: ERROR   Failed to start jail 'kamailio' action
'firewallcmd-ipset': Error starting action
```

Related articles

- Fail2Ban for Kamailio on VoipNow
- Fail2Ban for Kamailio on VoipNow 4.0.0
- How to install a LetsEncrypt SSL certificate in VoipNow