Install Fail2Ban on Debian

Installation

Download: https://www.fail2ban.org/wiki/index.php/Downloads

```
# Debian 7.x
tar xzf 0.9.2.tar.gz
cd fail2ban-0.9.2/
python setup.py install
```

Verify

```
fail2ban-client -h
```

Configuration for Asterisk

On Asterisk)

/etc/asterisk/logger.conf:

```
...
[logfiles]
...
fail2ban => notice,warning,security
```

Restart the logger on Asterisk

```
asterisk -rx "logger reload"
asterisk -rx "logger show channels"
```

On Fail2Ban)

/etc/fail2ban/jail.d/asterisk.conf

```
[asterisk]
enabled = true
```

```
logpath = /var/log/asterisk/fail2ban
maxretry = 5
bantime = 259200
```

Configuration for SSH

/etc/fail2ban/jail.d/sshd.conf

```
[sshd]
enabled = true
bantime = 7200
findtime = 900
maxretry = 4
```

Auto startup

```
cd fail2ban-0.9.2/
cp files/debian-initd /etc/init.d/fail2ban
chmod 0755 /etc/init.d/fail2ban
update-rc.d fail2ban defaults
```

Service start

```
service fail2ban start
```

Setup Logrotate

/etc/logrotate.d/fail2ban

```
/var/log/fail2ban.log {
    missingok
    notifempty
    size 30k
    create 0600 root root
    postrotate
        /usr/bin/fail2ban-client set logtarget /var/log/fail2ban.log 1>/dev/null || true
        #/usr/bin/fail2ban-client reload 2> /dev/null || true
    endscript
}
```

FAQ

Q:?? Call Log ??????

> Call from '' (195.154.134.116:5071) to extension '8011441295298642' rejected because extension not found in context 'public'.

Ans??? Asterisk ? allowguest=no

?? sip.conf

```
allowguest=no
```

Apply the changes

```
#> asterisk -rx "sip reload"
#> asterisk -rx "sip show settings" | grep -i "Allow unknown access"
  Allow unknown access:   No
```

Revision #2
Created 9 April 2021 03:34:42 by Admin
Updated 11 November 2021 13:08:38 by Admin