Настройка fail2ban (защита от брутфорса)

Fail2ban ?????? ? Linux ??????? ?? log–?????? ?????????? ????? ?????????? ????????????? ? ????????????? ??? IP ?????. ????????? ????? ???????? ? ?????????? ??????? ?? ??? ?????????? *NIX–???????, ????? ??? Apache, Nginx, Guacamole, sshd, Exim, Postfix ? ??????. ? ?????? ?????? ?? ????? ???????? ?????? SSH.

?????????:

```
apt-get -y install fail2ban
```

???????? ?????????? ? ?????????:

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

?????? ?????? ????:

```
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
vi /etc/fail2ban/jail.local
```

?????????? ????? jail.local:

```
[DEFAULT]
bantime  = 1d
findtime  = 4h
maxretry = 2

[sshd]
enabled = true
mode = aggressive
port = 2222
# incremental banning:
bantime.increment = true
# default factor (causes increment - 1h -> 1d 2d 4d 8d 16d 32d ...):
bantime.factor = 24
# max banning time = 6 week:
bantime.maxtime = 6w
logpath = %(sshd_log)s
backend = %(sshd_backend)s
```

? ??????? ???? fail2ban ??????? ???? 2222 ?????? ssh, ????? ?????????? ?? 1 ???? ????????? ??????????? ? ?????? 2 ???????? ??????? ????? ? ??????? 4 ?????, ?????????? ???????????????, ? ?????? ???? ???? ?? ???????? ???????? ???????? ???????? - ???? ?? 2 ??? ? ??? ?? ????????????? ????? ?????????? ?? 6 ??????.

?????????? ?????? ??? ?????????? ????? ????????????:

```
systemctl restart fail2ban
```

???????? ??????? fail2ban:

```
less /var/log/fail2ban.log
```

??????? ?????????? ??????????? ?? ???????:

```
cat /var/log/fail2ban.log | grep "\[sshd\] Ban" | wc -l
```

???????? ?????????????? IP-???????:

```
fail2ban-client status | grep "Jail list" | sed -E 's/^[^:]+:[ \t]+//' | sed 's/,//g'
```

????????????? ??????:

```
fail2ban-client set YOURJAILNAMEHERE unbanip IPADDRESSHERE
```

Revision #3
Created 2024-04-01 12:19:43 UTC by Boris Rzr
Updated 2024-04-01 13:08:04 UTC by Boris Rzr