

fail2ban opvolgen



context

dit document beschrijft hoe je de werking van [fail2ban](#) opvolgt.

stappenplan

- meld aan op het Linux systeem en voer uit: `fail2ban-client status sshd`
- dit geeft de activiteit op je systeem weer:

```
Status for the jail: sshd
|- Filter
| |- Currently failed: 10
| |- Total failed:      1661
| `-- File list:        /var/log/auth.log
`- Actions
  |- Currently banned: 6
  |- Total banned:     358
  `-- Banned IP list:  65.108.213.31 103.250.10.186 137.184.41.13
24.69.190.84 208.109.13.144 94.101.178.121
```

- analyseer de ingelijke activiteit (`view /var/log/fail2ban.log`)
 - worden hosts geband na het aangegeven aantal aanmeldpogingen (`maxretry =`) binnen aangeduide tijd (`findtime =`) voor de aangeduide duur (`bantime =`)?
 - kijk de 10 meest voorkomende IP meerdere na die geband worden: `grep Ban /var/log/fail2ban.log |awk '{print $8}'|sort|uniq -d -c|sort -k1 -n -r|head -10`
 - kijk de 10 meest voorkomende gebruikers na waarmee wordt aangemeld: `grep invalid /var/log/auth.log|awk '{print $10}'|sort|uniq -d -c|sort -k1 -n -r|head -10`
 - blokkeer IP's die meermaals worden geband: `ufw deny from <ip> to any`
- Om Bans online te volgen:

```
tail -f /var/log/fail2ban.log|grep Ban
```

```
2022-12-28 11:03:13,398 fail2ban.actions [908]: NOTICE [sshd] Ban 179.60.147.157
2022-12-28 11:19:09,067 fail2ban.actions [908]: NOTICE [sshd] Ban 179.60.147.157
2022-12-28 11:39:36,235 fail2ban.actions [908]: NOTICE [sshd] Ban 179.60.147.157
2022-12-28 11:45:27,851 fail2ban.actions [908]: NOTICE [sshd] Ban 42.200.64.243
2022-12-28 11:46:46,559 fail2ban.actions [908]: NOTICE [sshd] Ban 143.198.186.69
2022-12-28 11:47:19,814 fail2ban.actions [908]: NOTICE [sshd] Ban 104.131.91.148
2022-12-28 11:47:46,461 fail2ban.actions [908]: NOTICE [sshd] Ban 51.250.88.81
2022-12-28 11:48:05,700 fail2ban.actions [908]: NOTICE [sshd] Ban 43.157.10.210
2022-12-28 11:48:50,368 fail2ban.actions [908]: NOTICE [sshd] Ban 128.199.105.111
2022-12-28 11:48:56,392 fail2ban.actions [908]: NOTICE [sshd] Ban 117.220.10.3
2022-12-28 11:49:55,695 fail2ban.actions [908]: NOTICE [sshd] Ban 13.77.174.169
2022-12-28 11:50:11,730 fail2ban.actions [908]: NOTICE [sshd] Ban 43.156.90.36
2022-12-28 11:50:53,756 fail2ban.actions [908]: NOTICE [sshd] Ban 157.245.218.29
```

meer info

- [fail2ban](#)
- [using fail2ban](#)

[Linux](#)

From:

<https://www.louslab.be/> - Lou's lab

Permanent link:

https://www.louslab.be/doku.php?id=linux:fail2ban_opvolgen

Last update: **2024/11/16 18:14**

