

Администрирование сетевых подсистем

Fail2ban – базовая защита от brute-force атак

Метвалли Ахмед Фарг Набеех

2025

Российский университет дружбы народов, Москва, Россия

Цели работы

Основная цель

Получить навыки установки, настройки и проверки работы Fail2ban для защиты сервисов от атак типа «brute force».

Выполнение

Установка и запуск

```
running scripts...
```

Installed:

```
fail2ban-1.1.0-6.el10_0.noarch      fail2ban-firewalld-1.1.0-6.el10_0.noarch fail2ban-selinux-1.1.0-6.el10_0.noarch
fail2ban-sendmail-1.1.0-6.el10_0.noarch fail2ban-server-1.1.0-6.el10_0.noarch
```

Complete!

```
[root@server.ahmedfarg.net ~]# systemctl start fail2
Failed to start fail2.service: Unit fail2.service not found.
[root@server.ahmedfarg.net ~]# systemctl start fail2ban.service
[root@server.ahmedfarg.net ~]# systemctl enable fail2ban.service
Created symlink '/etc/systemd/system/multi-user.target.wants/fail2ban.service' → '/usr/lib/systemd/system/fail2ban.service'.
[root@server.ahmedfarg.net ~]#
```

Рис. 1: Установка и запуск Fail2ban

Анализ логов

```
[ahmedfarg@server.ahmedfarg.net ~]$  
[ahmedfarg@server.ahmedfarg.net ~]$ tail -f /var/log/fail2ban.log  
tail: cannot open '/var/log/fail2ban.log' for reading: Permission denied  
tail: no files remaining  
[ahmedfarg@server.ahmedfarg.net ~]$ sudo tail -f /var/log/fail2ban.log  
[sudo] password for ahmedfarg:  
2025-11-08 10:32:57,391 fail2ban.server      [14445]: INFO  -----  
2025-11-08 10:32:57,391 fail2ban.server      [14445]: INFO  Starting Fail2ban v1.1.0  
2025-11-08 10:32:57,391 fail2ban.observer    [14445]: INFO  Observer start...  
2025-11-08 10:32:57,395 fail2ban.database    [14445]: INFO  Connected to fail2ban persistent database '/var/lib/fail2  
ban/fail2ban.sqlite3'  
2025-11-08 10:32:57,396 fail2ban.database    [14445]: WARNING New database created. Version '4'
```

Рис. 2: Первичный журнал Fail2ban

Локальный конфигурационный файл

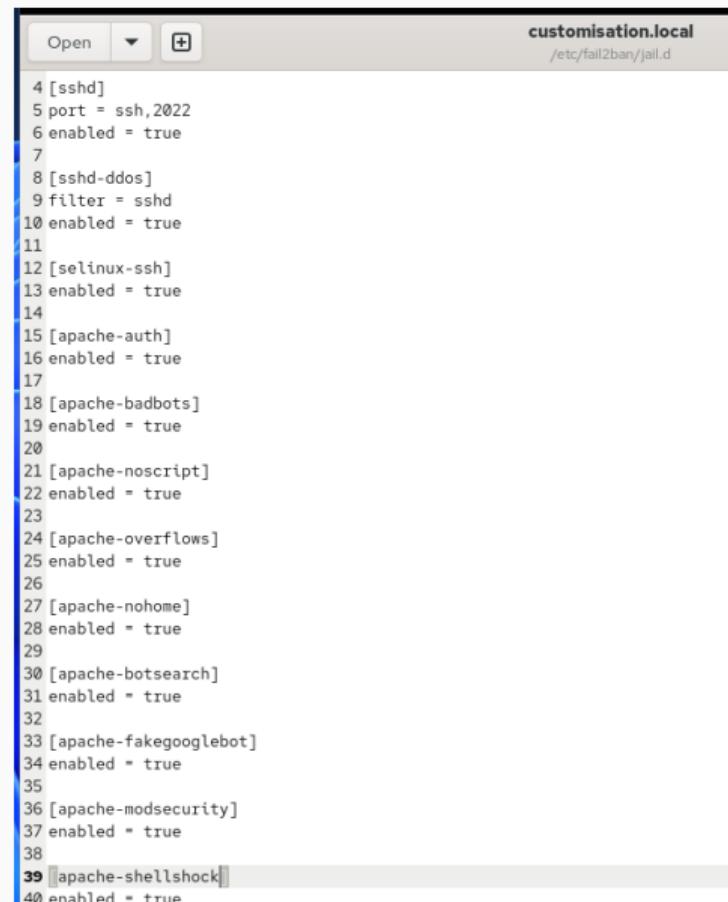
```
1 [DEFAULT]
2 bantime = 3600
3
4 [sshd]
5 port = ssh,2022
6 enabled = true
7
8 [sshd-ddos]
9 filter = sshd
10 enabled = true
11
12 [selinux-ssh]
13 enabled=true
```

Создание и запуск тюрем (jails)

```
ce + _COMM=sshd + _COMM=sshd-session'
2025-11-08 10:37:43,796 fail2ban.filter      [15364]: INFO    maxRetry: 5
2025-11-08 10:37:43,796 fail2ban.filter      [15364]: INFO    findtime: 600
2025-11-08 10:37:43,796 fail2ban.actions    [15364]: INFO    banTime: 3600
2025-11-08 10:37:43,796 fail2ban.filter      [15364]: INFO    encoding: UTF-8
2025-11-08 10:37:43,796 fail2ban.jail       [15364]: INFO    Creating new jail 'selinux-ssh'
2025-11-08 10:37:43,798 fail2ban.jail       [15364]: INFO    Jail 'selinux-ssh' uses pyinotify {}
2025-11-08 10:37:43,799 fail2ban.jail       [15364]: INFO    Initiated 'pyinotify' backend
2025-11-08 10:37:43,799 fail2ban.datedetector [15364]: INFO    date pattern `--: `Epoch`'
2025-11-08 10:37:43,799 fail2ban.filter      [15364]: INFO    maxRetry: 5
2025-11-08 10:37:43,800 fail2ban.filter      [15364]: INFO    findtime: 600
2025-11-08 10:37:43,800 fail2ban.actions    [15364]: INFO    banTime: 3600
2025-11-08 10:37:43,800 fail2ban.filter      [15364]: INFO    encoding: UTF-8
2025-11-08 10:37:43,801 fail2ban.filter      [15364]: INFO    Added logfile: '/var/log/audit/audit.log' (pos = 0, hash
= 9d8609ce4a4cf22353ac8d8ce1b750cd2dd5ec6e)
2025-11-08 10:37:43,801 fail2ban.jail       [15364]: INFO    Creating new jail 'sshd-ddos'
2025-11-08 10:37:43,802 fail2ban.jail       [15364]: INFO    Jail 'sshd-ddos' uses pyinotify {}
2025-11-08 10:37:43,802 fail2ban.jail       [15364]: INFO    Initiated 'pyinotify' backend
2025-11-08 10:37:43,803 fail2ban.filter      [15364]: INFO    maxLines: 1
2025-11-08 10:37:43,803 fail2ban.filter      [15364]: INFO    maxRetry: 5
2025-11-08 10:37:43,803 fail2ban.filter      [15364]: INFO    findtime: 600
2025-11-08 10:37:43,803 fail2ban.actions    [15364]: INFO    banTime: 3600
2025-11-08 10:37:43,803 fail2ban.filter      [15364]: INFO    encoding: UTF-8
2025-11-08 10:37:43,803 fail2ban.jail       [15364]: INFO    Jail 'sshd' started
2025-11-08 10:37:43,804 fail2ban.jail       [15364]: INFO    Jail 'selinux-ssh' started
2025-11-08 10:37:43,805 fail2ban.jail       [15364]: INFO    Jail 'sshd-ddos' started
```

Рис. 4: Запуск SSH-тюрем

Активация Apache-тюрем



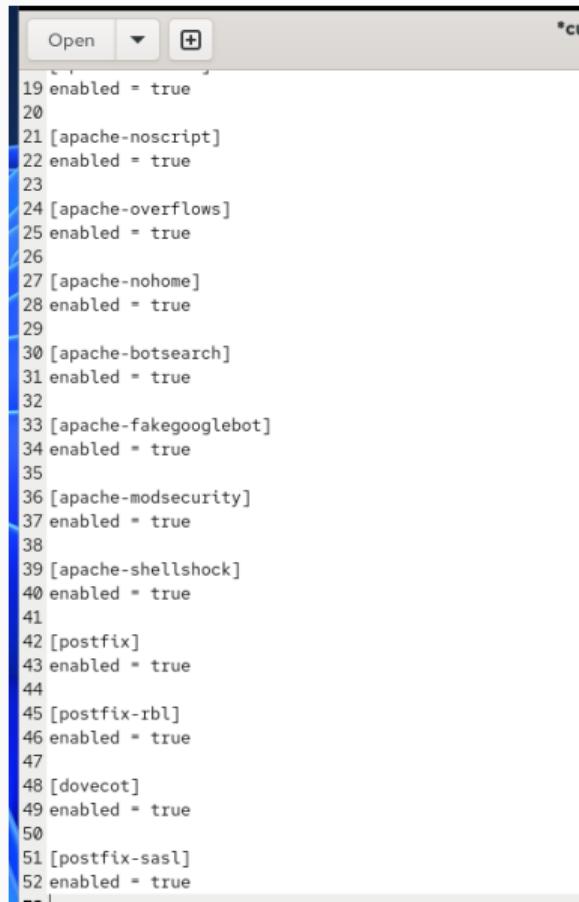
The screenshot shows a text editor window with the title bar "customisation.local" and the path "/etc/fail2ban/jail.local". The content of the file is a configuration for fail2ban, specifically for Apache-related services. The file contains 40 numbered lines, each starting with a section name in brackets and followed by an "enabled = true" directive. The sections include sshd, sshd-ddos, selinux-ssh, apache-auth, apache-badbots, apache-noscript, apache-overflows, apache-nohome, apache-botsearch, apache-fakegooglebot, apache-modsecurity, and apache-shellshock. Line 39 contains a comment "apache-shellshock" preceded by three underscores.

```
4 [sshd]
5 port = ssh,2022
6 enabled = true
7
8 [sshd-ddos]
9 filter = sshd
10 enabled = true
11
12 [selinux-ssh]
13 enabled = true
14
15 [apache-auth]
16 enabled = true
17
18 [apache-badbots]
19 enabled = true
20
21 [apache-noscript]
22 enabled = true
23
24 [apache-overflows]
25 enabled = true
26
27 [apache-nohome]
28 enabled = true
29
30 [apache-botsearch]
31 enabled = true
32
33 [apache-fakegooglebot]
34 enabled = true
35
36 [apache-modsecurity]
37 enabled = true
38
39 apache-shellshock
40 enabled = true
```

Проверка логов

```
2025-11-08 10:40:02,565 fail2ban.jail          [15924]: INFO  Initiated 'pyinotify' backend
2025-11-08 10:40:02,566 fail2ban.filter        [15924]: INFO  maxRetry: 1
2025-11-08 10:40:02,566 fail2ban.filter        [15924]: INFO  findtime: 600
2025-11-08 10:40:02,566 fail2ban.actions       [15924]: INFO  banTime: 3600
2025-11-08 10:40:02,566 fail2ban.filter        [15924]: INFO  encoding: UTF-8
2025-11-08 10:40:02,566 fail2ban.filter        [15924]: INFO  Added logfile: '/var/log/httpd/server.ahmedfarg.net-error
_log' (pos = 0, hash = )
2025-11-08 10:40:02,566 fail2ban.filter        [15924]: INFO  Added logfile: '/var/log/httpd/error_log' (pos = 0, hash
= 64a57b6db0a2d4ba8687eed09cf796192789ee08)
2025-11-08 10:40:02,566 fail2ban.filter        [15924]: INFO  Added logfile: '/var/log/httpd/ssl_error_log' (pos = 0, h
ash = 365eda5704041c91978b6e33f696f017ee7670f1)
2025-11-08 10:40:02,566 fail2ban.filter        [15924]: INFO  Added logfile: '/var/log/httpd/www.ahmedfarg.net-error_lo
g' (pos = 0, hash = 201863b251e865fb5e5bad9ba4eb416b7761df1b)
2025-11-08 10:40:02,566 fail2ban.jail          [15924]: INFO  Creating new jail 'sshd-ddos'
2025-11-08 10:40:02,566 fail2ban.jail          [15924]: INFO  Jail 'sshd-ddos' uses pyinotify {}
2025-11-08 10:40:02,567 fail2ban.jail          [15924]: INFO  Initiated 'pyinotify' backend
2025-11-08 10:40:02,567 fail2ban.filter        [15924]: INFO  maxLines: 1
2025-11-08 10:40:02,568 fail2ban.filter        [15924]: INFO  maxRetry: 5
2025-11-08 10:40:02,568 fail2ban.filter        [15924]: INFO  findtime: 600
2025-11-08 10:40:02,568 fail2ban.actions       [15924]: INFO  banTime: 3600
2025-11-08 10:40:02,568 fail2ban.filter        [15924]: INFO  encoding: UTF-8
2025-11-08 10:40:02,568 fail2ban.filtersystemd [15924]: INFO  [sshd] Jail is in operation now (process new journal entr
ies)
2025-11-08 10:40:02,568 fail2ban.jail          [15924]: INFO  Jail 'sshd' started
2025-11-08 10:40:02,569 fail2ban.jail          [15924]: INFO  Jail 'selinux-ssh' started
2025-11-08 10:40:02,570 fail2ban.jail          [15924]: INFO  Jail 'apache-auth' started
2025-11-08 10:40:02,570 fail2ban.jail          [15924]: INFO  Jail 'apache-badbots' started
2025-11-08 10:40:02,570 fail2ban.jail          [15924]: INFO  Jail 'apache-noscript' started
2025-11-08 10:40:02,571 fail2ban.jail          [15924]: INFO  Jail 'apache-overflows' started
2025-11-08 10:40:02,572 fail2ban.jail          [15924]: INFO  Jail 'apache-nohome' started
2025-11-08 10:40:02,572 fail2ban.jail          [15924]: INFO  Jail 'apache-botsearch' started
2025-11-08 10:40:02,573 fail2ban.jail          [15924]: INFO  Jail 'apache-fakegooglebot' started
2025-11-08 10:40:02,573 fail2ban.jail          [15924]: INFO  Jail 'apache-modsecurity' started
2025-11-08 10:40:02,574 fail2ban.jail          [15924]: INFO  Jail 'apache-shellshock' started
2025-11-08 10:40:02,574 fail2ban.jail          [15924]: INFO  Jail 'sshd-ddos' started
```

Активация тюрем



The screenshot shows a file editor window with a toolbar at the top containing 'Open' and a '+' button. The main area displays a configuration file with the following content:

```
19 enabled = true
20
21 [apache-noscript]
22 enabled = true
23
24 [apache-overflows]
25 enabled = true
26
27 [apache-nohome]
28 enabled = true
29
30 [apache-botsearch]
31 enabled = true
32
33 [apache-fakegooglebot]
34 enabled = true
35
36 [apache-modsecurity]
37 enabled = true
38
39 [apache-shellshock]
40 enabled = true
41
42 [postfix]
43 enabled = true
44
45 [postfix-rbl]
46 enabled = true
47
48 [dovecot]
49 enabled = true
50
51 [postfix-sasl]
52 enabled = true
--|
```

Проверка запуска почтовых тюрем

```
2025-11-08 10:41:47,746 fail2ban.filter [16208]: INFO findtime: 600
2025-11-08 10:41:47,746 fail2ban.actions [16208]: INFO banTime: 3600
2025-11-08 10:41:47,746 fail2ban.filter [16208]: INFO encoding: UTF-8
2025-11-08 10:41:47,746 fail2ban.filtersystemd [16208]: INFO [sshd] Jail is in operation now (process new journal entries)
2025-11-08 10:41:47,747 fail2ban.jail [16208]: INFO Jail 'sshd' started
2025-11-08 10:41:47,748 fail2ban.jail [16208]: INFO Jail 'selinux-ssh' started
2025-11-08 10:41:47,750 fail2ban.jail [16208]: INFO Jail 'apache-auth' started
2025-11-08 10:41:47,751 fail2ban.jail [16208]: INFO Jail 'apache-badbots' started
2025-11-08 10:41:47,752 fail2ban.jail [16208]: INFO Jail 'apache-noscript' started
2025-11-08 10:41:47,752 fail2ban.jail [16208]: INFO Jail 'apache-overflows' started
2025-11-08 10:41:47,753 fail2ban.jail [16208]: INFO Jail 'apache-nohome' started
2025-11-08 10:41:47,753 fail2ban.jail [16208]: INFO Jail 'apache-botsearch' started
2025-11-08 10:41:47,753 fail2ban.jail [16208]: INFO Jail 'apache-fakegooglebot' started
2025-11-08 10:41:47,753 fail2ban.jail [16208]: INFO Jail 'apache-modsecurity' started
2025-11-08 10:41:47,754 fail2ban.jail [16208]: INFO Jail 'apache-shellshock' started
2025-11-08 10:41:47,754 fail2ban.jail [16208]: INFO Jail 'postfix' started
2025-11-08 10:41:47,754 fail2ban.jail [16208]: INFO Jail 'postfix-rbl' started
2025-11-08 10:41:47,755 fail2ban.jail [16208]: INFO Jail 'dovecot' started
2025-11-08 10:41:47,756 fail2ban.filtersystemd [16208]: INFO [dovecot] Jail is in operation now (process new journal entries)
2025-11-08 10:41:47,756 fail2ban.filtersystemd [16208]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)
2025-11-08 10:41:47,756 fail2ban.filtersystemd [16208]: INFO [postfix-rbl] Jail is in operation now (process new journal entries)
2025-11-08 10:41:47,756 fail2ban.filtersystemd [16208]: INFO [postfix] Jail is in operation now (process new journal entries)
2025-11-08 10:41:47,756 fail2ban.jail [16208]: INFO Jail 'postfix-sasl' started
2025-11-08 10:41:47,757 fail2ban.jail [16208]: INFO Jail 'sshd-ddos' started
```

Рис. 8: Работа тюрем почтовых сервисов

Список активных тюрем

```
[root@server.ahmedfarg.net ~]# fail2ban-client status
[root@server.ahmedfarg.net ~]# fail2ban-client status sshd
Status
|- Number of jail:      16
`- Jail list: apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity, apache-nohome, apache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd, sshd-dos
[root@server.ahmedfarg.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:     0
| `- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[root@server.ahmedfarg.net ~]# fail2ban-client set sshd maxretry 2
2
```

Рис. 9: Статус SSH-тюрьмы

Умышленный ввод неправильного пароля

```
[root@server.ahmedfarg.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 3
|   '- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
  |- Currently banned: 1
  |- Total banned: 1
    '- Banned IP list: 192.168.1.30
[root@server.ahmedfarg.net ~]#
[root@server.ahmedfarg.net ~]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.ahmedfarg.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 3
|   '- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
  |- Currently banned: 0
  |- Total banned: 1
    '- Banned IP list:
[root@server.ahmedfarg.net ~]#
```

Рис. 10: Блокировка IP

Удаление адреса из бана

```
2025-11-08 10:45:20,590 fail2ban.jail      [16762]: INFO    Jail 'dovecot' started
2025-11-08 10:45:26,596 fail2ban.jail      [16762]: INFO    Jail 'postfix-sasl' started
2025-11-08 10:45:26,596 fail2ban.filtersystemd [16762]: INFO    [postfix-sasl] Jail is in operation now (process new journal entries)
2025-11-08 10:45:26,596 fail2ban.jail      [16762]: INFO    Jail 'sshd-ddos' started
2025-11-08 10:45:39,820 fail2ban.filter   [16762]: INFO    [sshd] Ignore 192.168.1.30 by ip
2025-11-08 10:45:43,293 fail2ban.filter   [16762]: INFO    [sshd] Ignore 192.168.1.30 by ip
2025-11-08 10:45:46,561 fail2ban.filter   [16762]: INFO    [sshd] Ignore 192.168.1.30 by ip
```

Рис. 11: Разблокировка IP

Исключение клиента из блокировки

The screenshot shows a configuration editor window with a toolbar at the top containing 'Open', a dropdown arrow, and a '+' button. To the right of the toolbar, the text 'customisa' and '/etc/fail2b...' is visible. The main area displays a configuration file with the following content:

```
1 [DEFAULT]
2 bantime = 3600
3
4 ignoreip = 127.0.0.1/8 192.168.1.30
5
6 [sshd]
7 port = ssh,2022
8 enabled = true
9
10 [sshd-ddos]
11 filter = sshd
12 enabled = true
13
14 [selinux-ssh]
15 enabled = true
16
```

The line '4 ignoreip = 127.0.0.1/8 192.168.1.30' is highlighted with a light gray background.

Повторная проверка после ignoreip

```
[root@server.ahmedfarg.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:      0
| `-. Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM:sshd + _COMM:sshd-session
`- Actions
  |- Currently banned: 0
  |- Total banned:     0
  `-. Banned IP list:
[root@server.ahmedfarg.net ~]# █
```

Рис. 13: Нет блокировок

Выводы

- Fail2ban установлен и настроен.
- Защита настроена для SSH, HTTP и почтовых сервисов.
- Реализована проверка блокировок и их снятие.
- Конфигурация автоматизирована с помощью Vagrant.