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

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

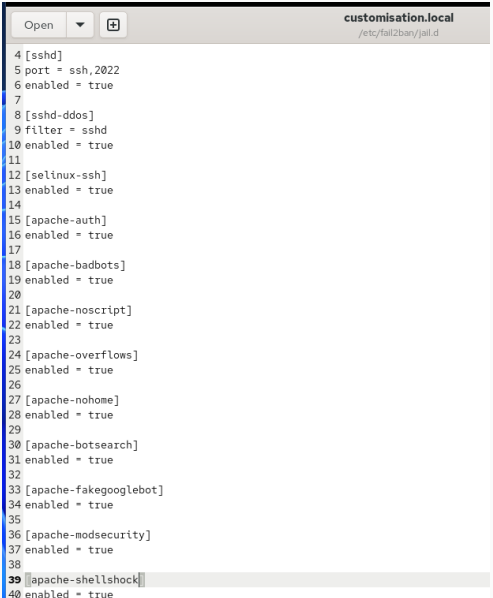
```
1 [DEFAULT]
2 bantime = 3600
3
4 [sshd]
5 port = ssh,2022
6 enabled = true
7
8 [sshd-ddos]
9 filter = sshd
10 enabled = true
11
12 [selinux-ssh]
13 enabled=true
```

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

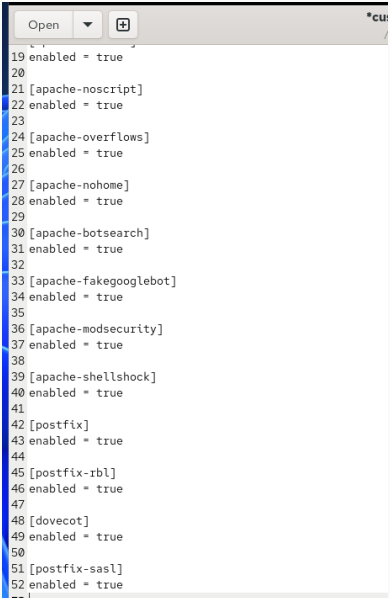
Активация Apache-тюрем



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



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 entr
ies)
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 e
ntries)
2025-11-08 10:41:47,756 fail2ban.filtersystemd  [16208]: INFO    [postfix-sasl] Jail is in operation now (process new jour
nal entries)
2025-11-08 10:41:47,756 fail2ban.filtersystemd  [16208]: INFO    [postfix-rbl] Jail is in operation now (process new journ
al entries)
2025-11-08 10:41:47,756 fail2ban.filtersystemd  [16208]: INFO    [postfix] Jail is in operation now (process new journal e
ntries)
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 ~]#
[root@server.ahmedfarg.net ~]# fail2ban-client status
Status
|- Number of jail:      16
`- Jail list:   apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity, apache-nohome, ap
ache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd, sshd-d
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 ~]#
```

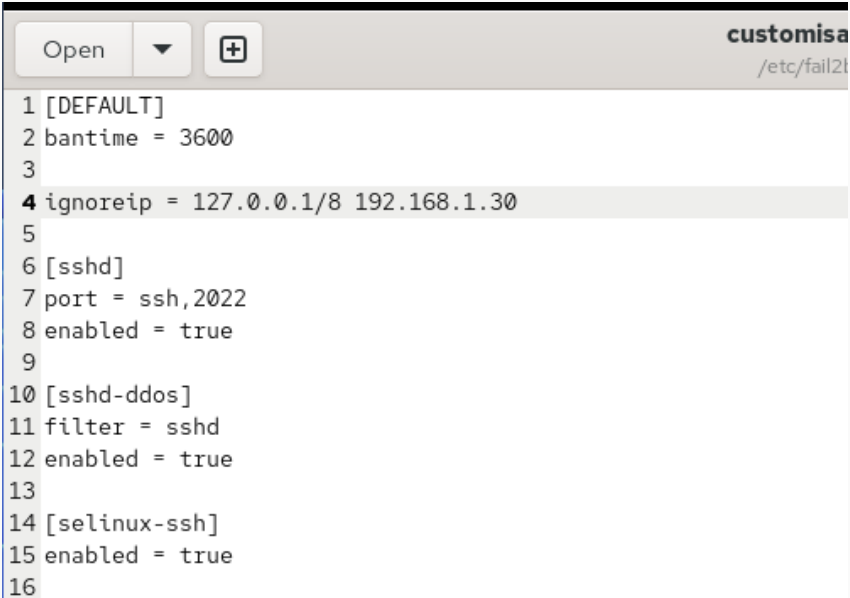

Рис. 10: Блокировка IP

Удаление адреса из бана

```
2025-11-08 10:45:26,596 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 jour
nal 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



Повторная проверка после ignoreip

```
[root@server.ahmedfarg.net ~]#
[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

Итог

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