

Администрирование системных подсистем

Fail2ban: базовая защита от brute-force атак

Сейдалиев Тагьетдин Ровшенович

11 декабря 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

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

Установка Fail2ban

- Установка пакета Fail2ban
- Включение автозапуска сервиса
- Проверка логов запуска

```
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.trseidaliev.net server]# systemctl start fail2ban.service
[root@server.trseidaliev.net server]# systemctl enable fail2ban.service
Created symlink '/etc/systemd/system/multi-user.target.wants/fail2ban.service' → '/usr/lib/systemd/system/fail2ban.service'.
[root@server.trseidaliev.net server]# █
```

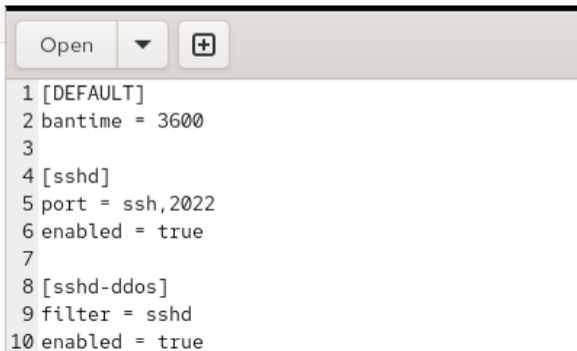
Рис. 1: Установка Fail2ban

```
[trseidaliev@server.trseidaliev.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for trseidaliev:
2025-12-11 11:02:41,375 fail2ban.server [16733]: INFO -----
2025-12-11 11:02:41,375 fail2ban.server [16733]: INFO Starting Fail2ban v1.1.0
2025-12-11 11:02:41,376 fail2ban.observer [16733]: INFO Observer start...
2025-12-11 11:02:41,380 fail2ban.database [16733]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2025-12-11 11:02:41,381 fail2ban.database [16733]: WARNING New database created. Version '4'
```

Рис. 2: Логи Fail2ban

Настройка Fail2ban

- Создание файла *customisation.local*
- Настройка:
 - bantime = 3600
 - защита SSH
 - защита SSH DDoS
 - включение selinux-ssh



The screenshot shows a file editor window with a toolbar at the top containing an 'Open' button, a dropdown arrow, and a '+' icon. The main area displays the content of the *customisation.local* file, which is a configuration file for SSH. The file contains the following lines:

```
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
```

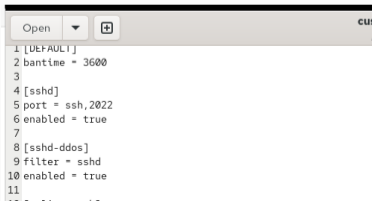
Активированные jails SSH

```
2025-12-11 11:06:25,815 fail2ban.server [17434]: INFO -----
2025-12-11 11:06:25,815 fail2ban.server [17434]: INFO Starting Fail2ban v1.1.0
2025-12-11 11:06:25,815 fail2ban.observer [17434]: INFO Observer start...
2025-12-11 11:06:25,821 fail2ban.database [17434]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ba
n.sqlite3'
2025-12-11 11:06:25,822 fail2ban.jail [17434]: INFO Creating new jail 'sshd'
2025-12-11 11:06:25,824 fail2ban.jail [17434]: INFO Jail 'sshd' uses systemd {}
2025-12-11 11:06:25,826 fail2ban.jail [17434]: INFO Initiated 'systemd' backend
2025-12-11 11:06:25,826 fail2ban.filter [17434]: INFO maxLines: 1
2025-12-11 11:06:25,831 fail2ban.filtersystemd [17434]: INFO [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.service + _COMM=
sshd + _COMM=sshd-session'
2025-12-11 11:06:25,831 fail2ban.filter [17434]: INFO maxRetry: 5
2025-12-11 11:06:25,831 fail2ban.filter [17434]: INFO findtime: 600
2025-12-11 11:06:25,831 fail2ban.actions [17434]: INFO banTime: 3600
2025-12-11 11:06:25,831 fail2ban.filter [17434]: INFO encoding: UTF-8
2025-12-11 11:06:25,831 fail2ban.jail [17434]: INFO Creating new jail 'selinux-ssh'
2025-12-11 11:06:25,833 fail2ban.jail [17434]: INFO Jail 'selinux-ssh' uses pyinotify {}
2025-12-11 11:06:25,834 fail2ban.jail [17434]: INFO Initiated 'pyinotify' backend
2025-12-11 11:06:25,835 fail2ban.datedetector [17434]: INFO date pattern '': 'Epoch'
2025-12-11 11:06:25,835 fail2ban.filter [17434]: INFO maxRetry: 5
2025-12-11 11:06:25,835 fail2ban.filter [17434]: INFO findtime: 600
2025-12-11 11:06:25,835 fail2ban.actions [17434]: INFO banTime: 3600
2025-12-11 11:06:25,835 fail2ban.filter [17434]: INFO encoding: UTF-8
2025-12-11 11:06:25,835 fail2ban.filter [17434]: INFO Added logfile: '/var/log/audit/audit.log' (pos = 0, hash = 943773af9
0a21e5e54a84e7f08f9cf468fe6551e)
2025-12-11 11:06:25,836 fail2ban.jail [17434]: INFO Creating new jail 'sshd-ddos'
2025-12-11 11:06:25,836 fail2ban.jail [17434]: INFO Jail 'sshd-ddos' uses pyinotify {}
2025-12-11 11:06:25,836 fail2ban.jail [17434]: INFO Initiated 'pyinotify' backend
2025-12-11 11:06:25,837 fail2ban.filter [17434]: INFO maxLines: 1
2025-12-11 11:06:25,837 fail2ban.filter [17434]: INFO maxRetry: 5
2025-12-11 11:06:25,837 fail2ban.filter [17434]: INFO findtime: 600
2025-12-11 11:06:25,837 fail2ban.actions [17434]: INFO banTime: 3600
2025-12-11 11:06:25,837 fail2ban.filter [17434]: INFO encoding: UTF-8
2025-12-11 11:06:25,837 fail2ban.jail [17434]: INFO Jail 'sshd' started
2025-12-11 11:06:25,838 fail2ban.jail [17434]: INFO Jail 'selinux-ssh' started
2025-12-11 11:06:25,838 fail2ban.jail [17434]: INFO Jail 'sshd-ddos' started
2025-12-11 11:06:25,839 fail2ban.filtersystemd [17434]: INFO [sshd] Jail is in operation now (process new journal entries)
```

Защита HTTP

Включённые jails Apache

- apache-auth
- apache-badbots
- apache-noscript
- apache-overflows
- apache-nohome
- apache-botsearch
- apache-fakegooglebot
- apache-modsecurity
- apache-shellshock



A screenshot of a terminal window with a title bar containing 'Open', a dropdown arrow, and a '+' icon. The terminal text shows the configuration for a jail named 'cus'. The configuration includes a default section with 'bantime = 3600', an 'sshd' section with 'port = ssh,2022' and 'enabled = true', and an 'sshd-ddos' section with 'filter = sshd' and 'enabled = true'. Line numbers 1 through 11 are visible on the left side of the terminal output.

```
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
```

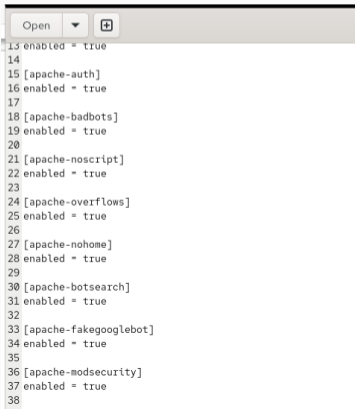
Логи запуска HTTP-защиты

```
2025-12-11 11:09:05,881 fail2ban.jail [17802]: INFO Creating new jail 'apache-shellshock'
2025-12-11 11:09:05,881 fail2ban.jail [17802]: INFO Jail 'apache-shellshock' uses pyinotify {}
2025-12-11 11:09:05,882 fail2ban.jail [17802]: INFO Initiated 'pyinotify' backend
2025-12-11 11:09:05,882 fail2ban.filter [17802]: INFO maxRetry: 1
2025-12-11 11:09:05,882 fail2ban.filter [17802]: INFO findtime: 600
2025-12-11 11:09:05,882 fail2ban.actions [17802]: INFO banTime: 3600
2025-12-11 11:09:05,882 fail2ban.filter [17802]: INFO encoding: UTF-8
2025-12-11 11:09:05,882 fail2ban.filter [17802]: INFO Added logfile: '/var/log/httpd/server.trseidaliev.net-error_log' (po
s = 0, hash = )
2025-12-11 11:09:05,882 fail2ban.filter [17802]: INFO Added logfile: '/var/log/httpd/error_log' (pos = 0, hash = c3f7d2f2b
31c82c8e57529a05ff2330425da3e45)
2025-12-11 11:09:05,882 fail2ban.filter [17802]: INFO Added logfile: '/var/log/httpd/ssl_error_log' (pos = 0, hash = 834dc
9d03de26a7046271efadca06ebc418c4b23)
2025-12-11 11:09:05,882 fail2ban.filter [17802]: INFO Added logfile: '/var/log/httpd/www.trseidaliev.net-error_log' (pos =
0, hash = 98d06fc6cfc8091598a78988025c306ce0346456)
2025-12-11 11:09:05,883 fail2ban.jail [17802]: INFO Creating new jail 'sshd-ddos'
2025-12-11 11:09:05,883 fail2ban.jail [17802]: INFO Jail 'sshd-ddos' uses pyinotify {}
2025-12-11 11:09:05,883 fail2ban.jail [17802]: INFO Initiated 'pyinotify' backend
2025-12-11 11:09:05,884 fail2ban.filter [17802]: INFO maxLines: 1
2025-12-11 11:09:05,884 fail2ban.filter [17802]: INFO maxRetry: 5
2025-12-11 11:09:05,884 fail2ban.filter [17802]: INFO findtime: 600
2025-12-11 11:09:05,884 fail2ban.actions [17802]: INFO banTime: 3600
2025-12-11 11:09:05,884 fail2ban.filter [17802]: INFO encoding: UTF-8
2025-12-11 11:09:05,884 fail2ban.filterssystemd [17802]: INFO [sshd] Jail is in operation now (process new journal entries)
2025-12-11 11:09:05,884 fail2ban.jail [17802]: INFO Jail 'sshd' started
2025-12-11 11:09:05,885 fail2ban.jail [17802]: INFO Jail 'selinux-ssh' started
2025-12-11 11:09:05,886 fail2ban.jail [17802]: INFO Jail 'apache-auth' started
2025-12-11 11:09:05,886 fail2ban.jail [17802]: INFO Jail 'apache-badbots' started
2025-12-11 11:09:05,887 fail2ban.jail [17802]: INFO Jail 'apache-noscript' started
2025-12-11 11:09:05,888 fail2ban.jail [17802]: INFO Jail 'apache-overflows' started
2025-12-11 11:09:05,888 fail2ban.jail [17802]: INFO Jail 'apache-nohome' started
2025-12-11 11:09:05,888 fail2ban.jail [17802]: INFO Jail 'apache-botsearch' started
2025-12-11 11:09:05,889 fail2ban.jail [17802]: INFO Jail 'apache-fakegooglebot' started
2025-12-11 11:09:05,890 fail2ban.jail [17802]: INFO Jail 'apache-modsecurity' started
2025-12-11 11:09:05,890 fail2ban.jail [17802]: INFO Jail 'apache-shellshock' started
2025-12-11 11:09:05,890 fail2ban.jail [17802]: INFO Jail 'sshd-ddos' started
```

Защита почтовых служб

Включённые почтовые jails

- postfix
- postfix-rbl
- dovecot
- postfix-sasl



```
Open ▼ +
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
```

Активация почтовых jails

```
2025-12-11 11:10:48,768 fail2ban.jail [18093]: INFO Initiated 'systemd' backend
2025-12-11 11:10:48,768 fail2ban.filtersystemd [18093]: INFO [postfix-sasl] Added journal match for: '_SYSTEMD_UNIT=postfix.servi
ce _SYSTEMD_UNIT=postfix@-.service'
2025-12-11 11:10:48,768 fail2ban.filter [18093]: INFO maxRetry: 5
2025-12-11 11:10:48,768 fail2ban.filter [18093]: INFO findtime: 600
2025-12-11 11:10:48,768 fail2ban.actions [18093]: INFO banTime: 3600
2025-12-11 11:10:48,768 fail2ban.filter [18093]: INFO encoding: UTF-8
2025-12-11 11:10:48,768 fail2ban.jail [18093]: INFO Creating new jail 'sshd-ddos'
2025-12-11 11:10:48,768 fail2ban.jail [18093]: INFO Jail 'sshd-ddos' uses pyinotify {}
2025-12-11 11:10:48,769 fail2ban.jail [18093]: INFO Initiated 'pyinotify' backend
2025-12-11 11:10:48,769 fail2ban.filter [18093]: INFO maxLines: 1
2025-12-11 11:10:48,770 fail2ban.filter [18093]: INFO maxRetry: 5
2025-12-11 11:10:48,770 fail2ban.filter [18093]: INFO findtime: 600
2025-12-11 11:10:48,770 fail2ban.filter [18093]: INFO banTime: 3600
2025-12-11 11:10:48,770 fail2ban.actions [18093]: INFO encoding: UTF-8
2025-12-11 11:10:48,770 fail2ban.filter [18093]: INFO Jail 'sshd' started
2025-12-11 11:10:48,770 fail2ban.filtersystemd [18093]: INFO [sshd] Jail is in operation now (process new journal entries)
2025-12-11 11:10:48,771 fail2ban.jail [18093]: INFO Jail 'selinux-ssh' started
2025-12-11 11:10:48,771 fail2ban.jail [18093]: INFO Jail 'apache-auth' started
2025-12-11 11:10:48,772 fail2ban.jail [18093]: INFO Jail 'apache-badbots' started
2025-12-11 11:10:48,772 fail2ban.jail [18093]: INFO Jail 'apache-noscript' started
2025-12-11 11:10:48,772 fail2ban.jail [18093]: INFO Jail 'apache-overflows' started
2025-12-11 11:10:48,773 fail2ban.jail [18093]: INFO Jail 'apache-nohome' started
2025-12-11 11:10:48,773 fail2ban.jail [18093]: INFO Jail 'apache-botsearch' started
2025-12-11 11:10:48,773 fail2ban.jail [18093]: INFO Jail 'apache-fakegooglebot' started
2025-12-11 11:10:48,774 fail2ban.jail [18093]: INFO Jail 'apache-modsecurity' started
2025-12-11 11:10:48,774 fail2ban.jail [18093]: INFO Jail 'apache-shellshock' started
2025-12-11 11:10:48,774 fail2ban.jail [18093]: INFO Jail 'postfix' started
2025-12-11 11:10:48,774 fail2ban.jail [18093]: INFO Jail 'postfix-rbl' started
2025-12-11 11:10:48,775 fail2ban.jail [18093]: INFO Jail 'dovecot' started
2025-12-11 11:10:48,776 fail2ban.filtersystemd [18093]: INFO [postfix-sasl] Jail is in operation now (process new journal entries
)
2025-12-11 11:10:48,776 fail2ban.filtersystemd [18093]: INFO [postfix] Jail is in operation now (process new journal entries)
2025-12-11 11:10:48,776 fail2ban.filtersystemd [18093]: INFO [postfix-rbl] Jail is in operation now (process new journal entries)
2025-12-11 11:10:48,776 fail2ban.jail [18093]: INFO Jail 'postfix-sasl' started
2025-12-11 11:10:48,776 fail2ban.filtersystemd [18093]: INFO [dovecot] Jail is in operation now (process new journal entries)
2025-12-11 11:10:48,776 fail2ban.jail [18093]: INFO Jail 'sshd-ddos' started
```

Проверка работы Fail2ban

```
[root@client.trseidaliev.net client]#  
[root@client.trseidaliev.net client]# ssh trseidaliev@server.trseidaliev.net  
The authenticity of host 'server.trseidaliev.net (192.168.1.1)' can't be established.  
ED25519 key fingerprint is SHA256:n0w0vphoobfpKiXoFhmCpcTAKAVt01RYFK5Kxnw0XTU.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'server.trseidaliev.net' (ED25519) to the list of known hosts.  
trseidaliev@server.trseidaliev.net's password:  
Permission denied, please try again.  
trseidaliev@server.trseidaliev.net's password:  
Permission denied, please try again.  
trseidaliev@server.trseidaliev.net's password:  
trseidaliev@server.trseidaliev.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).  
[root@client.trseidaliev.net client]#
```

Рис. 9: Общий статус Fail2ban

```
[root@client.trseidaliyev.net client]#  
[root@client.trseidaliyev.net client]# ssh trseidaliyev@server.trseidaliyev.net  
The authenticity of host 'server.trseidaliyev.net (192.168.1.1)' can't be established.  
ED25519 key fingerprint is SHA256:n0w0vphoobfpKiXoFhmCpcTAKAVt01RYFK5Kxnw0XTU.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'server.trseidaliyev.net' (ED25519) to the list of known hosts.  
trseidaliyev@server.trseidaliyev.net's password:  
Permission denied, please try again.  
trseidaliyev@server.trseidaliyev.net's password:  
Permission denied, please try again.  
trseidaliyev@server.trseidaliyev.net's password:  
trseidaliyev@server.trseidaliyev.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).  
[root@client.trseidaliyev.net client]#
```

Рис. 10: Попытки входа SSH

Блокировка клиента

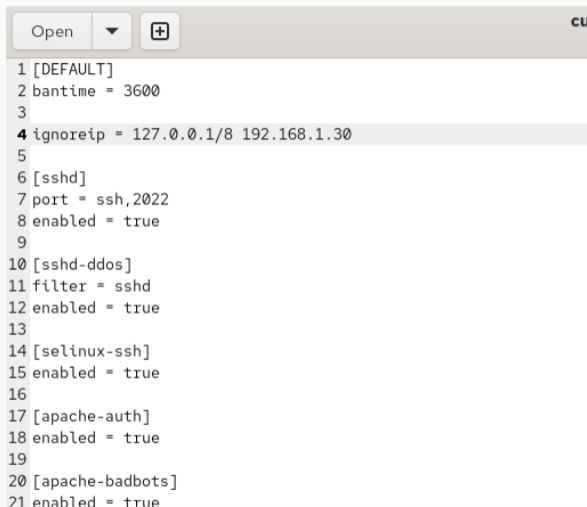
```
[root@server.trseidaliev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 3
| `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 1
   |- Total banned: 1
   `-- Banned IP list: 192.168.1.30
[root@server.trseidaliev.net server]# fail2ban-client set unbanip 192.168.1.30
2025-12-11 11:14:30,306 fail2ban [18598]: ERROR NOK: ('Invalid command '192.168.1.30' (no set action or not yet implemented)',)
Invalid command '192.168.1.30' (no set action or not yet implemented)
[root@server.trseidaliev.net server]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.trseidaliev.net server]# 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.trseidaliev.net server]#
```

Рис. 11: Заблокированный IP

```
[root@server.trseidaliev.net server]# 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.trseidaliev.net server]# fail2ban-client set unbanip 192.168.1.30
2025-12-11 11:14:30,306 fail2ban [18598]: ERROR NOK: ('Invalid command '192.168.1.30' (no set action or not yet implemented)',)
Invalid command '192.168.1.30' (no set action or not yet implemented)
[root@server.trseidaliev.net server]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.trseidaliev.net server]# 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.trseidaliev.net server]#
```

Рис. 12: Разблокировка

Исключение IP из блокировки



The image shows a configuration file editor window with a title bar containing 'Open', a dropdown arrow, and a '+' icon. The file content is as follows:

```
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
17 [apache-auth]
18 enabled = true
19
20 [apache-badbots]
21 enabled = true
```

Рис. 13: ignoreip

```
2025-12-11 11:16:09,574 fail2ban.filtersystemd [18868]: INFO [postfix-sasl] Jail is in operation now (process new journal en
2025-12-11 11:16:09,574 fail2ban.jail [18868]: INFO Jail 'postfix-sasl' started
2025-12-11 11:16:09,574 fail2ban.jail [18868]: INFO Jail 'sshd-ddos' started

2025-12-11 11:16:19,551 fail2ban.filter [18868]: INFO [sshd] Ignore 192.168.1.30 by ip
2025-12-11 11:16:23,789 fail2ban.filter [18868]: INFO [sshd] Ignore 192.168.1.30 by ip
2025-12-11 11:16:27,691 fail2ban.filter [18868]: INFO [sshd] Ignore 192.168.1.30 by ip
```

Рис. 14: Ignore log

Итоги работы

- Установлен и настроен Fail2ban
- Активирована защита SSH, HTTP и почтовых служб
- Проверена блокировка и разблокировка IP
- Добавлен игнорируемый IP клиента
- Проанализированы логи и работа jails
- Настроена автоматизация конфигурации Fail2ban
- Подготовлен скрипт для провижининга