

# **Отчёт по лабораторной работе №16**

**Дисциплина: Администрирование сетевых подсистем**

Ибрахим Мохсейн Алькамаль

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
2.1	Защита с помощью Fail2ban . . . . .	6
2.2	Проверка работы Fail2ban . . . . .	13
2.3	Внесение изменений в настройки внутреннего . . . . .	19
<b>3</b>	<b>Выводы</b>	<b>21</b>
<b>4</b>	<b>Контрольные вопросы</b>	<b>22</b>

## Список иллюстраций

2.1	Установка пакета fail2ban и зависимостей через dnf . . . . .	6
2.2	Запуск службы fail2ban и включение автозагрузки . . . . .	7
2.3	Просмотр журнала fail2ban.log в реальном времени . . . . .	7
2.4	Создание и перезапуск службы после настройки . . . . .	8
2.5	Конфигурация customisation.local с параметрами bantime и SSH . . . .	8
2.6	Создание и перезапуск службы после настройки . . . . .	9
2.7	Журнал запуска jail-модулей SSH в fail2ban . . . . .	9
2.8	Конфигурация HTTP jail-модулей в customisation.local . . . . .	10
2.9	Журнал запуска HTTP jail-модулей . . . . .	10
2.10	Подтверждение запуска HTTP jail-модулей в журнале . . . . .	11
2.11	Конфигурация jail-модулей для почтовых сервисов . . . . .	12
2.12	Журнал запуска jail-модулей почтовых сервисов . . . . .	12
2.13	Подтверждение работы jail-модулей почтовых сервисов . . . . .	13
2.14	Общий статус fail2ban-client . . . . .	13
2.15	Статус jail-модуля sshd до проверки . . . . .	14
2.16	Установка параметра maxretry для sshd . . . . .	15
2.17	Попытки входа по SSH с неверным паролем . . . . .	15
2.18	Блокировка IP-адреса клиента в sshd . . . . .	16
2.19	Команда разблокировки IP-адреса клиента . . . . .	16
2.20	Статус sshd после снятия блокировки . . . . .	16
2.21	Добавление параметра ignoreip в customisation.local . . . . .	17
2.22	Попытка входа с клиента после изменения конфигурации . . . . .	17
2.23	Сообщения журнала о игнорировании IP-адреса . . . . .	18
2.24	Статус sshd после включения ignoreip . . . . .	18
2.25	Создание каталога protect и копирование customisation.local . . . . .	19
2.26	Содержимое скрипта protect.sh . . . . .	20
2.27	Добавление блока provision в Vagrantfile . . . . .	20

## **Список таблиц**

# 1 Цель работы

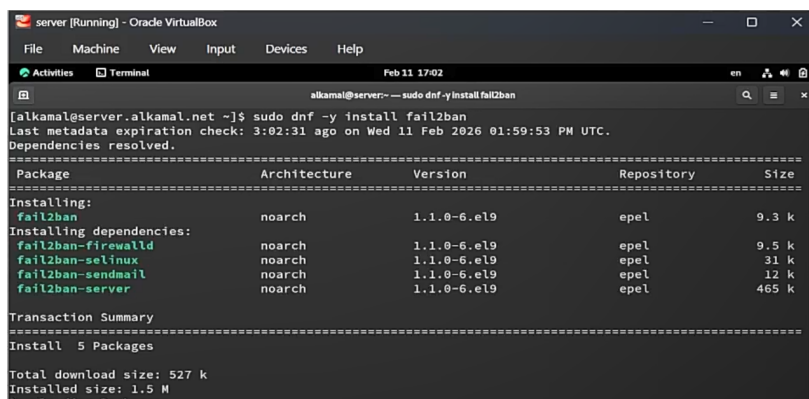
Получить навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

## 2 Выполнение лабораторной работы

### 2.1 Защита с помощью Fail2ban

#### 2.1.1 Установка Fail2ban

На сервере выполнена установка пакета `fail2ban` с использованием менеджера пакетов `dnf`. В процессе установки также автоматически установлены зависимости: `fail2ban-firewalld`, `fail2ban-selinux`, `fail2ban-sendmail`, `fail2ban-server`. Установка выполнена из репозитория `epel` (рис. 2.1).



```
server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Feb 11 17:02
alkamal@server:~$ sudo dnf -y install fail2ban
[alkamal@server.alkamal.net ~]$ sudo dnf -y install fail2ban
Last metadata expiration check: 3:02:31 ago on Wed 11 Feb 2026 01:59:53 PM UTC.
Dependencies resolved.
=====
Package                        Architecture Version      Repository Size
=====
Installing:
fail2ban                       noarch       1.1.0-6.el9  epel       9.3 k
Installing dependencies:
fail2ban-firewalld             noarch       1.1.0-6.el9  epel       9.5 k
fail2ban-selinux               noarch       1.1.0-6.el9  epel       31 k
fail2ban-sendmail              noarch       1.1.0-6.el9  epel       12 k
fail2ban-server                noarch       1.1.0-6.el9  epel      465 k
=====
Transaction Summary
=====
Install 5 Packages
Total download size: 527 k
Installed size: 1.5 M
Downloading Packages:
```

Рисунок 2.1: Установка пакета `fail2ban` и зависимостей через `dnf`

## 2.1.2 Запуск и добавление службы в автозагрузку

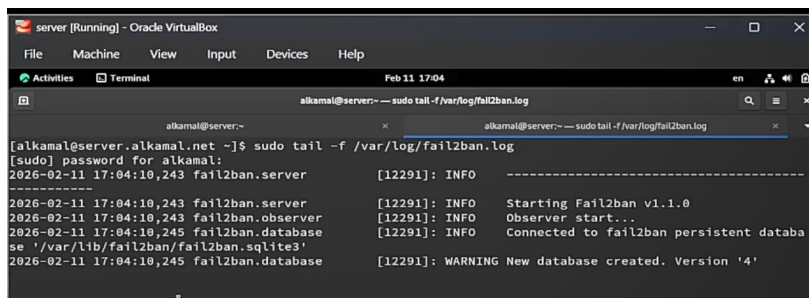
После установки выполнен запуск службы `fail2ban` командой `systemctl start fail2ban`, затем служба добавлена в автозагрузку командой `systemctl enable fail2ban`. Создана символическая ссылка в каталоге `multi-user.target.wants`, что подтверждает корректную регистрацию службы в системе (рис. 2.2).

```
[alkamal@server.alkamal.net ~]$ sudo systemctl start fail2ban
[alkamal@server.alkamal.net ~]$ sudo systemctl enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/systemd/system/fail2ban.service.
[alkamal@server.alkamal.net ~]$
```

Рисунок 2.2: Запуск службы `fail2ban` и включение автозагрузки

## 2.1.3 Контроль журнала событий Fail2ban

В дополнительном терминале выполнен мониторинг журнала `/var/log/fail2ban.log` с помощью команды `tail -f`. В журнале зафиксирован запуск сервера `Fail2ban` версии 1.1.0, инициализация `observer` и создание новой базы данных `fail2ban.sqlite3` (рис. 2.3).



```
server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Feb 11 17:04
alkamal@server:~$ sudo tail -f /var/log/fail2ban.log
alkamal@server:~$ sudo tail -f /var/log/fail2ban.log
[alkamal@server.alkamal.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for alkamal:
2026-02-11 17:04:10,243 fail2ban.server [12291]: INFO -----
2026-02-11 17:04:10,243 fail2ban.server [12291]: INFO Starting Fail2ban v1.1.0
2026-02-11 17:04:10,243 fail2ban.observer [12291]: INFO Observer start...
2026-02-11 17:04:10,245 fail2ban.database [12291]: INFO Connected to fail2ban persistent databa
se '/var/lib/fail2ban/fail2ban.sqlite3'
2026-02-11 17:04:10,245 fail2ban.database [12291]: WARNING New database created. Version '4'
```

Рисунок 2.3: Просмотр журнала `fail2ban.log` в реальном времени

## 2.1.4 Создание файла локальной конфигурации

Создан файл локальной конфигурации `/etc/fail2ban/jail.d/customisation.local` с использованием команды `touch`, после чего выполнено его редактирование в текстовом редакторе `nano` (рис. 2.6).

```

[alkamal@server.alkamal.net ~]$ sudo touch /etc/fail2ban/jail.d/customisation.local
[alkamal@server.alkamal.net ~]$ sudo nano /etc/fail2ban/jail.d/customisation.local
[alkamal@server.alkamal.net ~]$ sudo systemctl restart fail2ban
[alkamal@server.alkamal.net ~]$

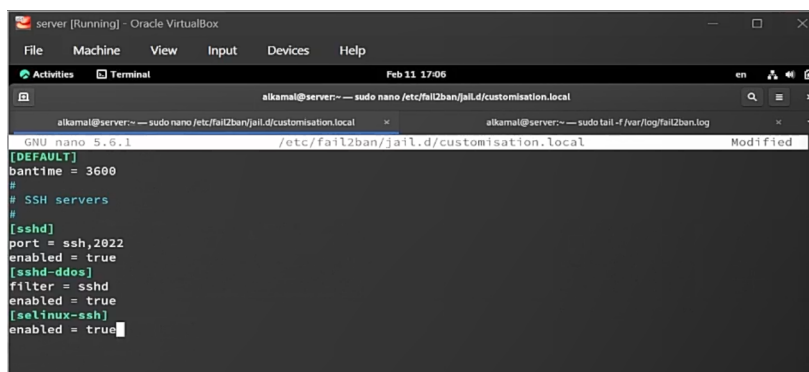
```

Рисунок 2.4: Создание и перезапуск службы после настройки

## 2.1.5 Настройка параметров блокирования и защиты SSH

В файле `/etc/fail2ban/jail.d/customisation.local` заданы параметры:

- В секции `[DEFAULT]` установлено время блокировки `bantime = 3600` секунд (1 час).
- Включена защита SSH в секциях `[sshd]`, `[sshd-ddos]`, `[selinux-ssh]`.
- Для `sshd` указан порт `ssh, 2022`.
- Для всех перечисленных служб установлен параметр `enabled = true` (рис. 2.5).



```

GNU nano 5.6.1 /etc/fail2ban/jail.d/customisation.local Modified
[DEFAULT]
bantime = 3600
#
# SSH servers
#
[sshd]
port = ssh,2022
enabled = true
[sshd-ddos]
filter = sshd
enabled = true
[selinux-ssh]
enabled = true

```

Рисунок 2.5: Конфигурация customisation.local с параметрами bantime и SSH

## 2.1.6 Перезапуск службы Fail2ban

После внесения изменений выполнен перезапуск службы командой `systemctl restart fail2ban`, что обеспечивает применение новой конфигурации (рис. 2.6).



```

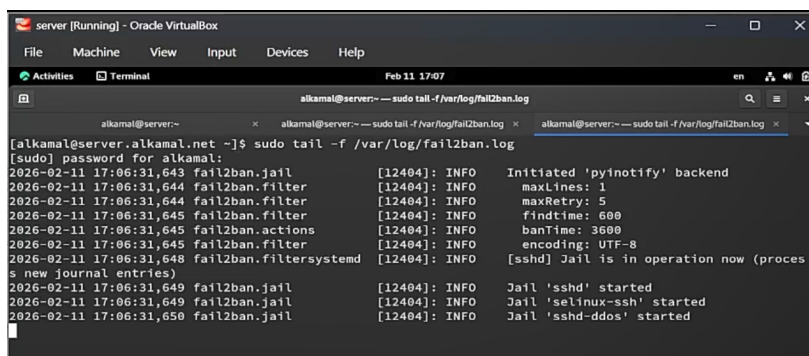
[alkamal@server.alkamal.net ~]$ sudo touch /etc/fail2ban/jail.d/customisation.local
[alkamal@server.alkamal.net ~]$ sudo nano /etc/fail2ban/jail.d/customisation.local
[alkamal@server.alkamal.net ~]$ sudo systemctl restart fail2ban
[alkamal@server.alkamal.net ~]$

```

Рисунок 2.6: Создание и перезапуск службы после настройки

## 2.1.7 Просмотр журнала событий Fail2ban

После перезапуска службы выполнен мониторинг журнала `/var/log/fail2ban.log`. В журнале зафиксирована инициализация backend `pyinotify`, параметры `maxLines`, `maxRetry`, `findtime`, `banTime` = 3600, а также запуск jail-модулей `sshd`, `selinux-ssh`, `sshd-ddos` (рис. 2.7).



```

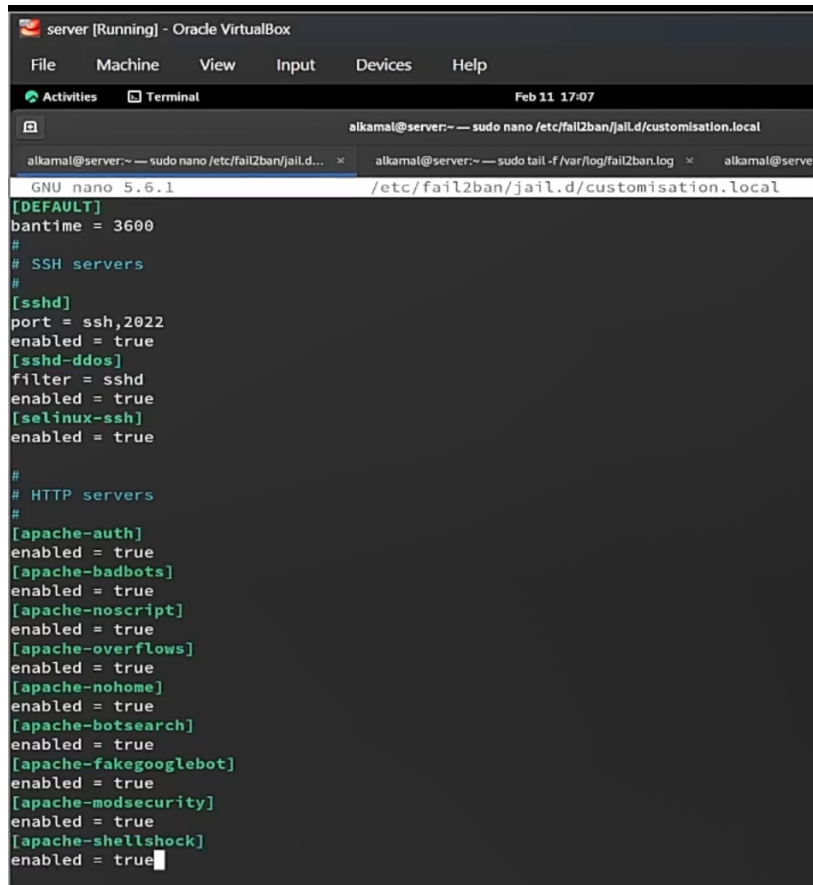
[alkamal@server.alkamal.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for alkamal:
2026-02-11 17:06:31,643 fail2ban.jail [12404]: INFO Initiated 'pyinotify' backend
2026-02-11 17:06:31,644 fail2ban.filter [12404]: INFO maxLines: 1
2026-02-11 17:06:31,644 fail2ban.filter [12404]: INFO maxRetry: 5
2026-02-11 17:06:31,645 fail2ban.filter [12404]: INFO findtime: 600
2026-02-11 17:06:31,645 fail2ban.actions [12404]: INFO banTime: 3600
2026-02-11 17:06:31,645 fail2ban.filter [12404]: INFO encoding: UTF-8
2026-02-11 17:06:31,648 fail2ban.filtersystemd [12404]: INFO [sshd] Jail is in operation now (proces
5 new journal entries)
2026-02-11 17:06:31,649 fail2ban.jail [12404]: INFO Jail 'sshd' started
2026-02-11 17:06:31,649 fail2ban.jail [12404]: INFO Jail 'selinux-ssh' started
2026-02-11 17:06:31,650 fail2ban.jail [12404]: INFO Jail 'sshd-ddos' started

```

Рисунок 2.7: Журнал запуска jail-модулей SSH в fail2ban

## 2.1.8 Включение защиты HTTP

В файле `/etc/fail2ban/jail.d/customisation.local` активированы jail-модули для HTTP-сервера Apache: `apache-auth`, `apache-badbots`, `apache-noscript`, `apache-overflows`, `apache-nohome`, `apache-botsearch`, `apache-fakegooglebot`, `apache-modsecurity`, `apache-shellshock`. Для каждого модуля установлен параметр `enabled = true` (рис. 2.8).

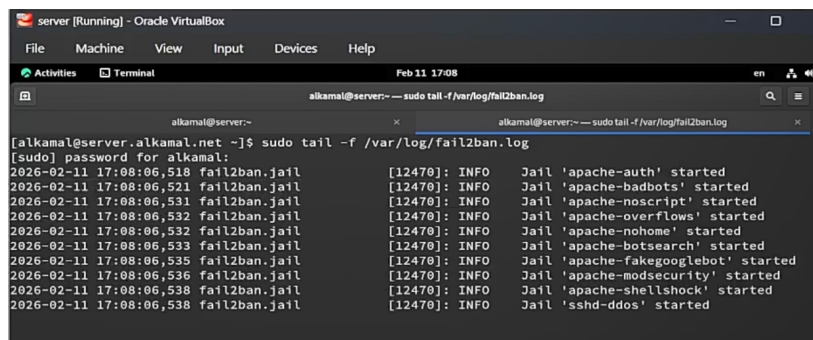


```
server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 11 17:07
alkamal@server:~ — sudo nano /etc/fail2ban/jail.d/customisation.local
GNU nano 5.6.1 /etc/fail2ban/jail.d/customisation.local
[DEFAULT]
bantime = 3600
#
# SSH servers
#
[sshd]
port = ssh,2022
enabled = true
[sshd-ddos]
filter = sshd
enabled = true
[selinux-ssh]
enabled = true
#
# HTTP servers
#
[apache-auth]
enabled = true
[apache-badbots]
enabled = true
[apache-noscript]
enabled = true
[apache-overflows]
enabled = true
[apache-nohome]
enabled = true
[apache-botsearch]
enabled = true
[apache-fakegooglebot]
enabled = true
[apache-modsecurity]
enabled = true
[apache-shellshock]
enabled = true
```

Рисунок 2.8: Конфигурация HTTP jail-модулей в customisation.local

## 2.1.9 Перезапуск Fail2ban после настройки HTTP

После внесения изменений выполнен перезапуск службы `systemctl restart fail2ban`, что обеспечило загрузку новых jail-настроек (рис. 2.10).

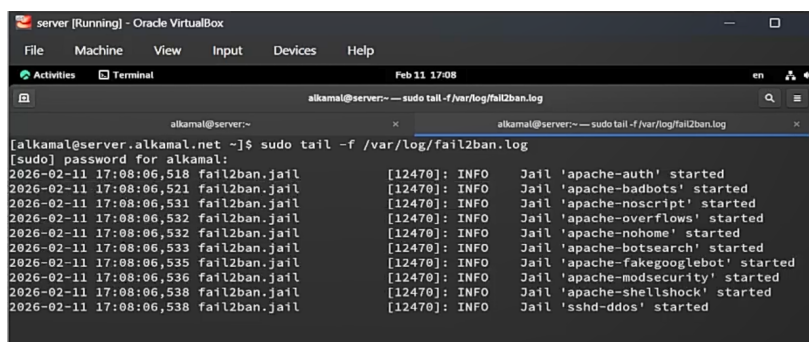


```
server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 11 17:08
alkamal@server:~ — sudo tail -f /var/log/fail2ban.log
alkamal@server:~ — sudo tail -f /var/log/fail2ban.log
[alkamal@server.alkamal.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for alkamal:
2026-02-11 17:08:06,518 fail2ban.jail [12470]: INFO Jail 'apache-auth' started
2026-02-11 17:08:06,521 fail2ban.jail [12470]: INFO Jail 'apache-badbots' started
2026-02-11 17:08:06,531 fail2ban.jail [12470]: INFO Jail 'apache-noscript' started
2026-02-11 17:08:06,532 fail2ban.jail [12470]: INFO Jail 'apache-overflows' started
2026-02-11 17:08:06,533 fail2ban.jail [12470]: INFO Jail 'apache-nohome' started
2026-02-11 17:08:06,533 fail2ban.jail [12470]: INFO Jail 'apache-botsearch' started
2026-02-11 17:08:06,535 fail2ban.jail [12470]: INFO Jail 'apache-fakegooglebot' started
2026-02-11 17:08:06,536 fail2ban.jail [12470]: INFO Jail 'apache-modsecurity' started
2026-02-11 17:08:06,538 fail2ban.jail [12470]: INFO Jail 'apache-shellshock' started
2026-02-11 17:08:06,538 fail2ban.jail [12470]: INFO Jail 'sshd-ddos' started
```

Рисунок 2.9: Журнал запуска HTTP jail-модулей

## 2.1.10 Контроль журнала после включения HTTP-защиты

В журнале `/var/log/fail2ban.log` зафиксирован запуск jail-модулей `apache-auth`, `apache-badbots`, `apache-noscript`, `apache-overflows`, `apache-nohome`, `apache-botsearch`, `apache-fakegooglebot`, `apache-modsecurity`, `apache-shellshock`, а также повторная активация `sshd-ddos` (рис. 2.10).



```
server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Feb 11 17:08
alkamal@server:~$ sudo tail -f /var/log/fail2ban.log
alkamal@server:~$ sudo tail -f /var/log/fail2ban.log
[alkamal@server.alkamal.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for alkamal:
2026-02-11 17:08:06,518 fail2ban.jail [12470]: INFO Jail 'apache-auth' started
2026-02-11 17:08:06,521 fail2ban.jail [12470]: INFO Jail 'apache-badbots' started
2026-02-11 17:08:06,531 fail2ban.jail [12470]: INFO Jail 'apache-noscript' started
2026-02-11 17:08:06,532 fail2ban.jail [12470]: INFO Jail 'apache-overflows' started
2026-02-11 17:08:06,532 fail2ban.jail [12470]: INFO Jail 'apache-nohome' started
2026-02-11 17:08:06,533 fail2ban.jail [12470]: INFO Jail 'apache-botsearch' started
2026-02-11 17:08:06,535 fail2ban.jail [12470]: INFO Jail 'apache-fakegooglebot' started
2026-02-11 17:08:06,536 fail2ban.jail [12470]: INFO Jail 'apache-modsecurity' started
2026-02-11 17:08:06,538 fail2ban.jail [12470]: INFO Jail 'apache-shellshock' started
2026-02-11 17:08:06,538 fail2ban.jail [12470]: INFO Jail 'sshd-ddos' started
```

Рисунок 2.10: Подтверждение запуска HTTP jail-модулей в журнале

## 2.1.11 Включение защиты почтовых сервисов

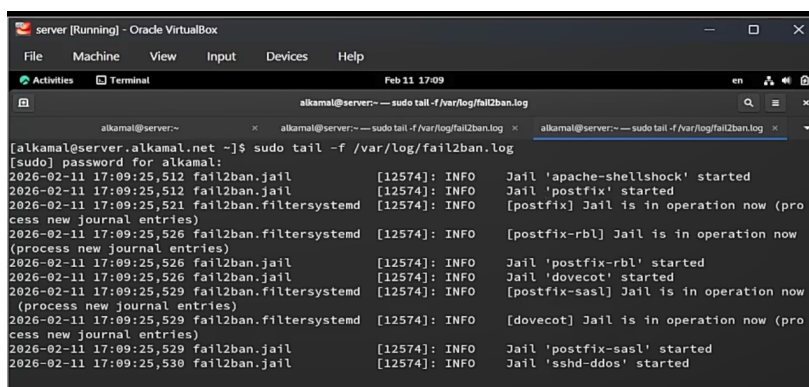
В файле `/etc/fail2ban/jail.d/customisation.local` активированы jail-модули для почтовых сервисов: `postfix`, `postfix-rbl`, `dovecot`, `postfix-sasl`. Для каждого модуля установлен параметр `enabled = true` (рис. 2.11).

```
#
# Mail servers
#
[postfix]
enabled = true
[postfix-rbl]
enabled = true
[dovecot]
enabled = true
[postfix-sasl]
enabled = true
```

Рисунок 2.11: Конфигурация jail-модулей для почтовых сервисов

### 2.1.12 Перезапуск Fail2ban после настройки почтовых служб

После добавления конфигурации выполнен перезапуск службы fail2ban для применения изменений (рис. 2.13).



```
server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Feb 11 17:09
alkamal@server:~$ sudo tail -f /var/log/fail2ban.log
[alkamal@server alkamal.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for alkamal:
2026-02-11 17:09:25,512 fail2ban.jail [12574]: INFO Jail 'apache-shellshock' started
2026-02-11 17:09:25,512 fail2ban.jail [12574]: INFO Jail 'postfix' started
2026-02-11 17:09:25,521 fail2ban.filtersystemd [12574]: INFO [postfix] Jail is in operation now (pro
cess new journal entries)
2026-02-11 17:09:25,526 fail2ban.filtersystemd [12574]: INFO [postfix-rbl] Jail is in operation now
(process new journal entries)
2026-02-11 17:09:25,526 fail2ban.jail [12574]: INFO Jail 'postfix-rbl' started
2026-02-11 17:09:25,526 fail2ban.jail [12574]: INFO Jail 'dovecot' started
2026-02-11 17:09:25,529 fail2ban.filtersystemd [12574]: INFO [postfix-sasl] Jail is in operation now
(process new journal entries)
2026-02-11 17:09:25,529 fail2ban.filtersystemd [12574]: INFO [dovecot] Jail is in operation now (pro
cess new journal entries)
2026-02-11 17:09:25,529 fail2ban.jail [12574]: INFO Jail 'postfix-sasl' started
2026-02-11 17:09:25,530 fail2ban.jail [12574]: INFO Jail 'sshd-ddos' started
```

Рисунок 2.12: Журнал запуска jail-модулей почтовых сервисов

### 2.1.13 Контроль журнала после включения почтовой защиты

В журнале событий зафиксирован запуск jail-модулей postfix, postfix-rbl, dovecot, postfix-sasl. Для каждого модуля отображается сообщение Jail is in operation now, что подтверждает успешную активацию защиты почтовых сервисов (рис. 2.13).

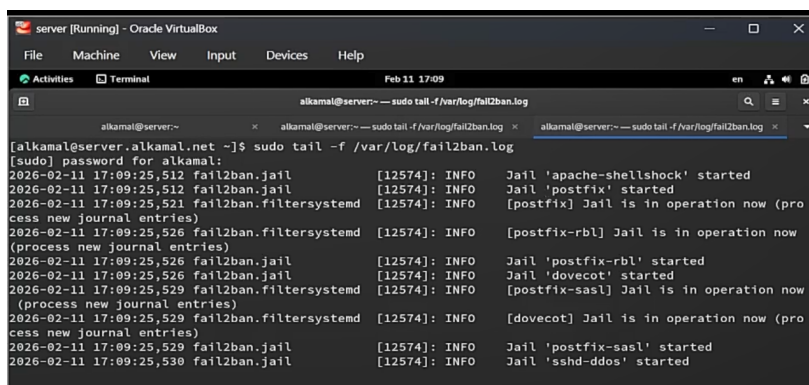


Рисунок 2.13: Подтверждение работы jail-модулей почтовых сервисов

## 2.2 Проверка работы Fail2ban

### 2.2.1 Просмотр общего статуса Fail2ban

На сервере выполнена команда `fail2ban-client status`. В выводе отображено общее количество jail-модулей (16) и их список, включая `apache-*`, `dovecot`, `postfix`, `sshd`, `sshd-ddos`, `selinux-ssh` и другие. Это подтверждает активную работу всех ранее настроенных модулей (рис. 2.16).

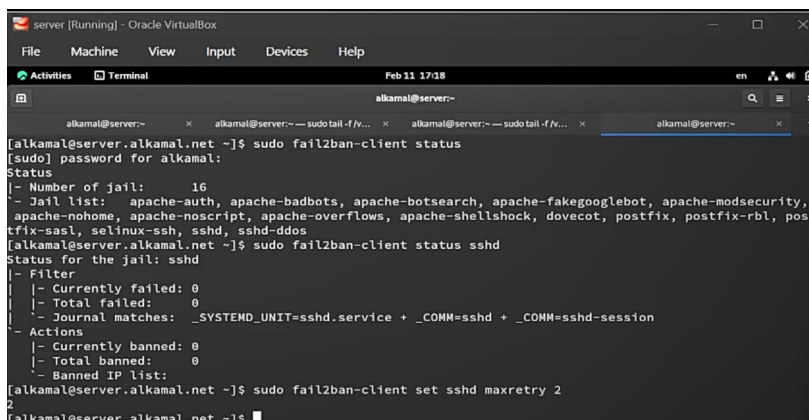
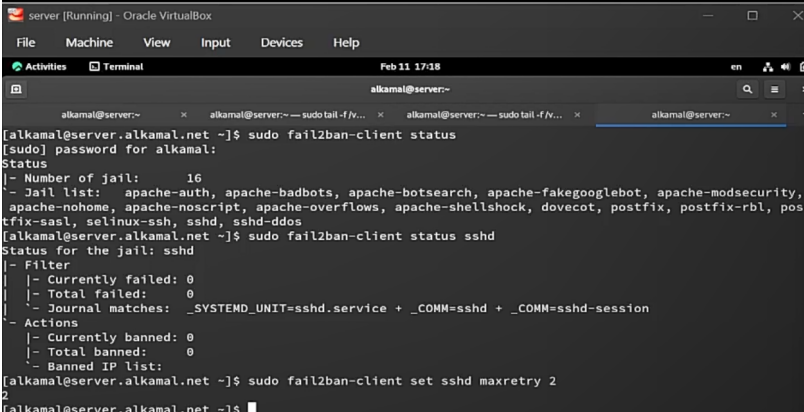


Рисунок 2.14: Общий статус fail2ban-client

## 2.2.2 Просмотр статуса защиты SSH

Выполнена команда `fail2ban-client status sshd`. В разделе `Filter` указаны значения `Currently failed: 0`, `Total failed: 0`. В разделе `Actions` значения `Currently banned: 0`, `Total banned: 0`, список заблокированных IP-адресов отсутствует. Это подтверждает отсутствие попыток неуспешной аутентификации на момент проверки (рис. 2.16).



```
server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Feb 11 17:18
alkamal@server:~
[alkamal@server.alkamal.net ~]$ sudo fail2ban-client status
[sudo] password for alkamal:
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-ddos
[alkamal@server.alkamal.net ~]$ sudo 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:
[alkamal@server.alkamal.net ~]$ sudo fail2ban-client set sshd maxretry 2
2
[alkamal@server.alkamal.net ~]$
```

Рисунок 2.15: Статус jail-модуля sshd до проверки

## 2.2.3 Установка максимального количества ошибок

Выполнена команда `fail2ban-client set sshd maxretry 2`, устанавливающая параметр `maxretry = 2` для jail-модуля `sshd`. После двух неудачных попыток входа IP-адрес клиента должен быть заблокирован (рис. 2.16).

```
server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Feb 11 17:18
alkamal@server:~$ sudo fail2ban-client status
[sudo] password for alkamal:
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-ddos
[alkamal@server.alkamal.net ~]$ sudo 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:
[alkamal@server.alkamal.net ~]$ sudo fail2ban-client set sshd maxretry 2
2
[alkamal@server.alkamal.net ~]$
```

Рисунок 2.16: Установка параметра maxretry для sshd

## 2.2.4 Попытка входа по SSH с неправильным паролем

С клиента выполнена попытка подключения к серверу по SSH с использованием неверного пароля. После нескольких попыток аутентификации сервер возвращает сообщение `Permission denied`, что фиксируется Fail2ban как ошибки входа (рис. 2.17).

```
client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Feb 11 17:19
alkamal@client:~$ ssh -o PreferredAuthentications=password -o PubkeyAuthentication=no alkamal@server.alkamal.net
alkamal@server.alkamal.net's password:
Permission denied, please try again.
alkamal@server.alkamal.net's password:
Permission denied, please try again.
alkamal@server.alkamal.net's password:
alkamal@server.alkamal.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[alkamal@client.alkamal.net ~]$
```

Рисунок 2.17: Попытки входа по SSH с неверным паролем

## 2.2.5 Проверка блокировки IP-адреса

На сервере повторно выполнена команда `fail2ban-client status sshd`. В разделе `Actions` указано `Currently banned: 1`, `Total banned: 1`, а в списке `Banned IP list` отображён адрес клиента `192.168.1.30`. Это подтверждает успешную блокировку IP-адреса после превышения установленного порога ошибок (рис. 2.18).

```
[alkamal@server.alkamal.net ~]$ sudo fail2ban-client status sshd
[sudo] password for alkamal:
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
[alkamal@server.alkamal.net ~]$
```

Рисунок 2.18: Блокировка IP-адреса клиента в sshd

## 2.2.6 Разблокировка IP-адреса клиента

Выполнена команда `fail2ban-client set sshd unbanip 192.168.1.30`, снимающая блокировку с IP-адреса клиента (рис. 2.19).

```
[alkamal@server.alkamal.net ~]$ sudo fail2ban-client set sshd unbanip 192.168.1.30
1
[alkamal@server.alkamal.net ~]$
```

Рисунок 2.19: Команда разблокировки IP-адреса клиента

## 2.2.7 Проверка снятия блокировки

Повторно выполнена команда `fail2ban-client status sshd`. В разделе **Actions** указано `Currently banned: 0`, список заблокированных IP-адресов пуст. Это подтверждает успешное снятие блокировки клиента (рис. 2.20).

```
[alkamal@server.alkamal.net ~]$ sudo 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:
[alkamal@server.alkamal.net ~]$
```

Рисунок 2.20: Статус sshd после снятия блокировки



## 2.2.8 Добавление игнорирования IP-адреса клиента

В файл `/etc/fail2ban/jail.d/customisation.local` в секции `[DEFAULT]` добавлен параметр `ignoreip = 127.0.0.1/8 192.168.1.30`, где `192.168.1.30` — IP-адрес клиента. Параметр `ignoreip` исключает указанный адрес из процедуры блокировки независимо от количества ошибок аутентификации (рис. 2.21).

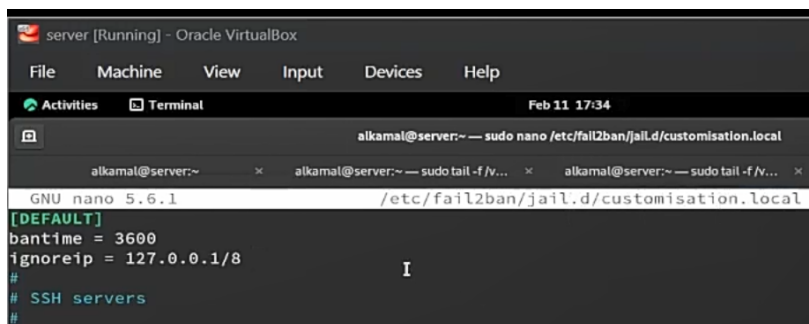


Рисунок 2.21: Добавление параметра `ignoreip` в `customisation.local`

## 2.2.9 Перезапуск службы Fail2ban

После изменения конфигурации выполнен перезапуск службы командой `systemctl restart fail2ban` для применения параметра `ignoreip` (рис. 2.22).

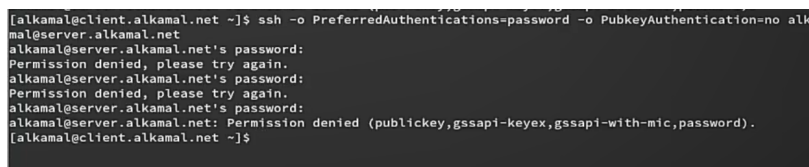


Рисунок 2.22: Попытка входа с клиента после изменения конфигурации

## 2.2.10 Просмотр журнала событий

В журнале `/var/log/fail2ban.log` отображаются сообщения вида `[sshd] Ignore 192.168.1.30 by ip` и `[selinux-ssh] Ignore`

192.168.1.30 by ip, что подтверждает корректную обработку параметра ignoreip и исключение клиента из механизма блокировки (рис. 2.23).

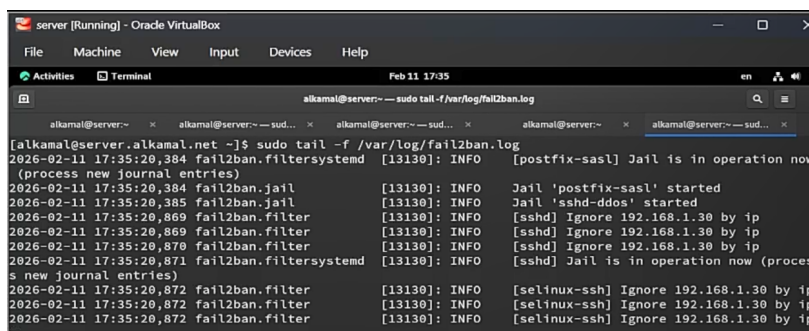


Рисунок 2.23: Сообщения журнала о игнорировании IP-адреса

## 2.2.11 Повторная попытка входа и проверка статуса SSH

С клиента выполнены повторные попытки входа по SSH с неправильным паролем. Несмотря на ошибки аутентификации, IP-адрес не блокируется.

При проверке статуса jail-модуля sshd (fail2ban-client status sshd) указано: Currently banned: 0, Total banned: 0, список Banned IP list пуст, что подтверждает отсутствие блокировки благодаря параметру ignoreip (рис. 2.24).

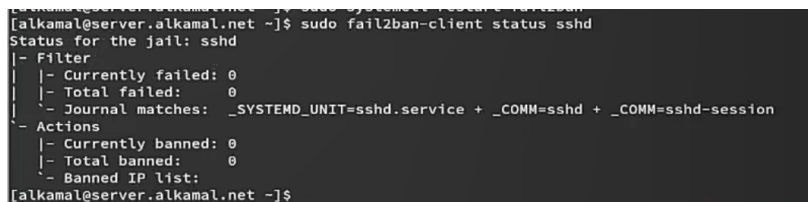


Рисунок 2.24: Статус sshd после включения ignoreip

## 2.3 Внесение изменений в настройки внутреннего

### 2.3.1 Подготовка каталога и копирование конфигурации

#### Fail2ban

На виртуальной машине `server` выполнен переход в каталог `/vagrant/provision/server`. Создан каталог `protect/etc/fail2ban/jail.d`, после чего файл `customisation.local` скопирован из системного каталога `/etc/fail2ban/jail.d/` во внутреннюю структуру `provision`. Это обеспечивает перенос текущей конфигурации Fail2ban в среду автоматической настройки Vagrant (рис. 2.25).

```
[alkamal@server.alkamal.net ~]$ cd /vagrant/provision/server
[alkamal@server.alkamal.net server]$ mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d
[alkamal@server.alkamal.net server]$ sudo cp -R /etc/fail2ban/jail.d/customisation.local /vagrant/provis
ion/server/protect/etc/fail2ban/jail.d/
[alkamal@server.alkamal.net server]$ cd /vagrant/provision/server
[alkamal@server.alkamal.net server]$ touch protect.sh
[alkamal@server.alkamal.net server]$ chmod +x protect.sh
[alkamal@server.alkamal.net server]$ nano protect.sh
```

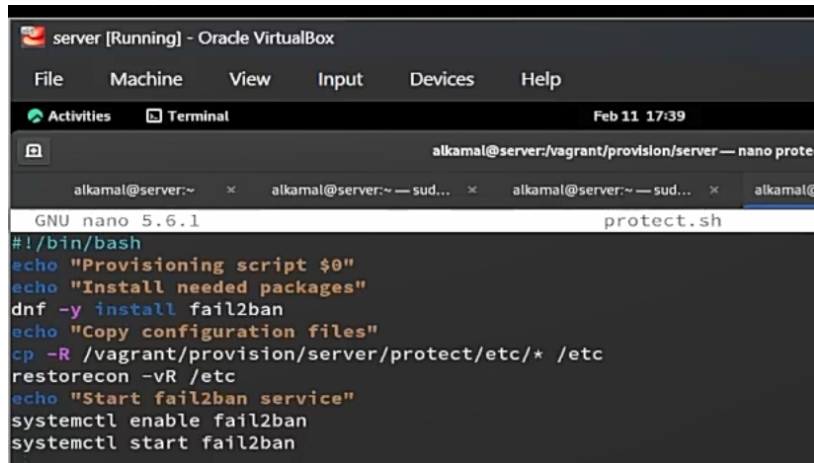
Рисунок 2.25: Создание каталога `protect` и копирование `customisation.local`

### 2.3.2 Создание и настройка скрипта `protect.sh`

В каталоге `/vagrant/provision/server` создан исполняемый файл `protect.sh` и открыт для редактирования. В скрипте реализованы следующие действия:

- установка пакета `fail2ban`;
- копирование конфигурационных файлов из `/vagrant/provision/server/protect` в `/etc`;
- восстановление контекстов SELinux командой `restorecon -vR /etc`;
- включение и запуск службы `fail2ban`.

Скрипт предназначен для автоматической настройки защиты при развертывании виртуальной машины (рис. 2.26).

The image shows a terminal window titled 'server [Running] - Oracle VirtualBox'. The terminal is running the GNU nano 5.6.1 editor, editing a file named 'protect.sh'. The script content is as follows:

```
#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
dnf -y install fail2ban
echo "Copy configuration files"
cp -R /vagrant/provision/server/protect/etc/* /etc
restorecon -vR /etc
echo "Start fail2ban service"
systemctl enable fail2ban
systemctl start fail2ban
```

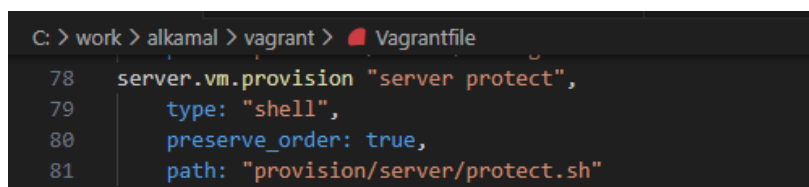
Рисунок 2.26: Содержимое скрипта protect.sh

### 2.3.3 Добавление provision-конфигурации в Vagrantfile

В файле Vagrantfile в разделе конфигурации виртуальной машины server добавлен блок:

```
server.vm.provision "server protect",
  type: "shell",
  preserve_order: true,
  path: "provision/server/protect.sh"
```

Данная конфигурация обеспечивает выполнение скрипта protect.sh при запуске или пересоздании виртуальной машины server, тем самым автоматизируя применение настроек Fail2ban (рис. 2.27).

The image shows a terminal window with the command prompt 'C: > work > alkamal > vagrant >'. The file 'Vagrantfile' is open in the editor, showing the following configuration:

```
78 server.vm.provision "server protect",
79   type: "shell",
80   preserve_order: true,
81   path: "provision/server/protect.sh"
```

Рисунок 2.27: Добавление блока provision в Vagrantfile

## 3 Выводы

В ходе работы выполнена установка и базовая настройка системы предотвращения вторжений Fail2ban на сервере. Реализована защита сервисов SSH, HTTP (Apache) и почтовых служб (Postfix, Dovecot) с заданием времени блокировки и порога ошибок аутентификации.

Экспериментально подтверждена корректность механизма блокировки IP-адреса клиента при превышении значения `maxretry`, а также возможность снятия блокировки вручную. Дополнительно проверена работа параметра `ignoreip`, обеспечивающего исключение заданного адреса из процесса блокировки.

Настройки Fail2ban вынесены в систему автоматического развёртывания Vagrant посредством создания скрипта `protect.sh` и добавления соответствующего блока `provision` в `Vagrantfile`. Это обеспечивает воспроизводимость конфигурации и автоматическую активацию механизмов защиты при запуске виртуальной машины.

## 4 Контрольные вопросы

1. Поясните принцип работы Fail2ban.

Fail2ban - это программное обеспечение, которое предотвращает атаки на сервер, анализируя лог-файлы и блокируя IP-адреса, с которых идут подозрительные или злонамеренные действия. Он работает следующим образом:

- Мониторит указанные лог-файлы на наличие заданных событий (например, неудачных попыток входа).
- Когда число попыток превышает определенный порог, Fail2ban временно блокирует IP-адрес, добавляя правила в фаервол.
- Заблокированный IP-адрес может быть разблокирован автоматически после определенного периода времени

2. Настройки какого файла более приоритетны: `jail.conf` или `jail.local`?

Настройки файла `jail.local` более приоритетны, чем настройки файла `jail.conf`.

3. Как настроить оповещение администратора при срабатывании Fail2ban?

Чтобы настроить оповещение администратора при срабатывании Fail2ban, необходимо настроить отправку уведомлений по электронной почте или другим способом. Это можно сделать, изменяя настройки в файле `jail.local`, добавляя адрес электронной почты администратора и настройки SMTP-сервера.

4. Поясните построчно настройки по умолчанию в конфигурационном файле `/etc/fail2ban/jail.conf`, относящиеся к веб-службе.

Примеры настроек по умолчанию в конфигурационном файле `/etc/fail2ban/jail.conf` относящиеся к веб-службе:

- `[apache]` - секция, относящаяся к веб-серверу Apache.
- `enabled = true` - включение проверки лог-файлов Apache.
- `port = http,https` - указание портов для мониторинга.
- `filter = apache-auth` - указание фильтра для обработки лог-файлов.
- `logpath = /var/log/apache/*error.log` - путь к лог-файлам Apache.
- `maxretry = 5` - максимальное количество попыток до блокировки адреса.
- `bantime = 600` - продолжительность блокировки в секундах.

5. Поясните построчно настройки по умолчанию в конфигурационном файле `/etc/fail2ban/jail.conf`, относящиеся к почтовой службе.

Примеры настроек по умолчанию в конфигурационном файле `/etc/fail2ban/jail.conf` относящиеся к почтовой службе:

- `[postfix]` - секция, относящаяся к почтовому серверу Postfix.
- `enabled = true` - включение проверки лог-файлов Postfix.
- `port = smtp,ssmtp` - указание портов для мониторинга.
- `filter = postfix` - указание фильтра для обработки лог-файлов.
- `logpath = /var/log/mail.log` - путь к лог-файлам Postfix.
- `maxretry = 3` - максимальное количество попыток до блокировки адреса.
- `bantime = 3600` - продолжительность блокировки в секундах

6. Какие действия может выполнять Fail2ban при обнаружении атакующего IP-адреса? Где можно посмотреть описание действий для последующего использования в настройках Fail2ban?

Fail2ban может выполнять различные действия при обнаружении атакующего IP-адреса, такие как блокировка адреса через фаервол, добавление правил в IP-таблицы, отправка уведомлений администратору и другие. Описание доступных действий можно найти в документации или руководстве Fail2ban.

7. Как получить список действующих правил Fail2ban?

Можно использовать команду: `fail2ban-client status`.

8. Как получить статистику заблокированных Fail2ban адресов?

Можно использовать команду `fail2ban-client status <jail-name>`, где `<jail-name>` - имя конкретного jail, например, «ssh» или «apache».

9. Как разблокировать IP-адрес?

`fail2ban-client set sshd unbanip <ip-адрес>`