

# Отчёт по лабораторной работе №16

Дисциплина: Администрирование сетевых подсистем

true

## Содержание

## Цель работы

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

## Задание

1. Установить и настроить Fail2ban для отслеживания работы установленных на сервере служб
2. Проверить работу Fail2ban посредством попыток несанкционированного доступа с клиента на сервер через SSH
3. Написать скрипт для Vagrant, фиксирующий действия по установке и настройке Fail2ban

## Выполнение лабораторной работы

### Защита с помощью Fail2ban

Загрузили нашу операционную систему и перешли в рабочий каталог с проектом: `cd /var/tmp/tbmanturov/vagrant` ([рис. @fig-001])

Запустили виртуальную машину `server: make server-up` ([рис. @fig-002])

Далее на виртуальной машине `server` вошли под созданным нами пользователем и открыли терминал. Перешли в режим суперпользователя: `sudo -i` ([рис. @fig-003])

На сервере установили fail2ban: `dnf -y install fail2ban` ([рис. @fig-004])

```
[root@server.tbmanturov.net ~]# dnf -y install fail2ban
Extra Packages for Enterprise Linux 8 - x86_64 [ Extra Packages for Enterprise Linux 8 - x86_64 ] --- B/s | 0 B --- ETA
[root@server.tbmanturov.net ~]#
```

Установка fail2ban

Запустили сервер fail2ban: `systemctl start fail2ban` и `systemctl enable fail2ban` ([рис. @fig-005])

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

Запуск сервера fail2ban

В дополнительном терминале запустили просмотр журнала событий fail2ban: `tail -f /var/log/fail2ban.log` ([рис. @fig-006])

```
[root@server.tbmanturov.net ~]# tail -f /var/log/fail2ban.log
2026-02-11 13:11:00,229 fail2ban.server [25744]: INFO
-----
2026-02-11 13:11:00,230 fail2ban.server [25744]: INFO Starting Fail2ban v1.1.0
2026-02-11 13:11:00,230 fail2ban.observer [25744]: INFO Observer start...
2026-02-11 13:11:00,237 fail2ban.database [25744]: INFO Connected to fail2ban persist
ent database /var/lib/fail2ban/fail2ban.sqlite3
2026-02-11 13:11:00,238 fail2ban.database [25744]: WARNING New database created. Version
4
```

Просмотр журнала событий fail2ban (1)

Создали файл с локальной конфигурацией fail2ban: touch  
/etc/fail2ban/jail.d/customisation.local ([рис. @fig-007])

В файле /etc/fail2ban/jail.d/customisation.local задали время блокирования на 1 час и  
включили защиту SSH ([рис. @fig-008]):

```
[DEFAULT]
bantime = 3600
#
# SSH servers
#
[sshd]
port = ssh,2022
enabled = true
[sshd-ddos]
filter = sshd
enabled = true
[selinux-ssh]
enabled = true
```



Редактирование файла /etc/fail2ban/jail.d/customisation.local (1)

Перезапустили fail2ban: systemctl restart fail2ban ([рис. @fig-009])

```
[root@server.tbmanturov.net ~]# systemctl restart fail2ban
[root@server.tbmanturov.net ~]#
```

Перезапуск fail2ban (1)

Посмотрели журнал событий: tail -f /var/log/fail2ban.log ([рис. @fig-010])

```
-----
2026-02-11 13:13:15,313 fail2ban.server [26338]: INFO Starting Fail2ban v1.1.0
2026-02-11 13:13:15,314 fail2ban.observer [26338]: INFO Observer start...
2026-02-11 13:13:15,319 fail2ban.database [26338]: INFO Connected to fail2ban persist
ent database /var/lib/fail2ban/fail2ban.sqlite3
```

Просмотр журнала событий fail2ban (2)

В файле /etc/fail2ban/jail.d/customisation.local включили защиту HTTP ([рис. @fig-011]):

```
#
# 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
```

```
#
# 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
```

Редактирование файла /etc/fail2ban/jail.d/customisation.local (2)

Перезапустили fail2ban: `systemctl restart fail2ban` (рис. @fig-012)

```
[root@server.tbmanturov.net ~]# systemctl restart fail2ban
[root@server.tbmanturov.net ~]#
```

Перезапуск fail2ban (2)

Посмотрели журнал событий: `tail -f /var/log/fail2ban.log` (рис. @fig-013)

```
2026-02-11 13:15:22,910 fail2ban.jail [26738]: INFO Initiated 'pyinotify' backend
2026-02-11 13:15:22,911 fail2ban.filter [26738]: INFO maxlines: 1
2026-02-11 13:15:22,912 fail2ban.filter [26738]: INFO maxRetry: 5
2026-02-11 13:15:22,912 fail2ban.filter [26738]: INFO findTime: 600
2026-02-11 13:15:22,912 fail2ban.actions [26738]: INFO banTime: 3600
2026-02-11 13:15:22,912 fail2ban.filter [26738]: INFO encoding: UTF-8
2026-02-11 13:15:22,914 fail2ban.jail [26738]: INFO Jail 'sshd' started
2026-02-11 13:15:22,916 fail2ban.jail [26738]: INFO Jail 'sshd-ssh' started
2026-02-11 13:15:22,917 fail2ban.jail [26738]: INFO Jail 'apache-auth' started
2026-02-11 13:15:22,926 fail2ban.jail [26738]: INFO Jail 'apache-badbots' started
2026-02-11 13:15:22,926 fail2ban.filtersystemd [26738]: INFO [sshd] Jail is in operation n
ow (process new journal entries)
2026-02-11 13:15:22,932 fail2ban.jail [26738]: INFO Jail 'apache-noscript' starte
d
2026-02-11 13:15:22,944 fail2ban.jail [26738]: INFO Jail 'apache-overflows' start
ed
2026-02-11 13:15:22,946 fail2ban.jail [26738]: INFO Jail 'apache-nohome' started
2026-02-11 13:15:22,947 fail2ban.jail [26738]: INFO Jail 'apache-botsearch' start
ed
2026-02-11 13:15:22,948 fail2ban.jail [26738]: INFO Jail 'apache-fakegooglebot' s
tarted
2026-02-11 13:15:22,949 fail2ban.jail [26738]: INFO Jail 'apache-modsecurity' sta
rted
2026-02-11 13:15:22,952 fail2ban.jail [26738]: INFO Jail 'apache-shellshock' star
ted
2026-02-11 13:15:22,955 fail2ban.jail [26738]: INFO Jail 'sshd-ddos' started
```

Просмотр журнала событий fail2ban (3)

В файле /etc/fail2ban/jail.d/customisation.local включили защиту почты ([рис. @fig-014]):

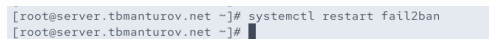
```
#
# Mail servers
#
[postfix]
enabled = true
[postfix-rbl]
enabled = true
[dovecot]
enabled = true
[postfix-sasl]
enabled = true
```



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

Редактирование файла /etc/fail2ban/jail.d/customisation.local (3)

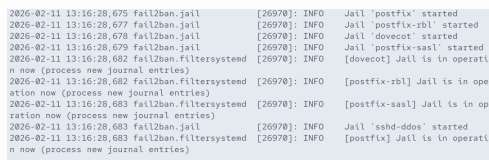
Перезапустили fail2ban: systemctl restart fail2ban ([рис. @fig-015])



```
[root@server.tbmanturov.net ~]# systemctl restart fail2ban
[root@server.tbmanturov.net ~]#
```

Перезапуск fail2ban (3)

Посмотрели журнал событий: tail -f /var/log/fail2ban.log ([рис. @fig-016])




```
2026-02-11 13:16:28,675 fail2ban.jail [26970]: INFO Jail 'postfix' started
2026-02-11 13:16:28,677 fail2ban.jail [26970]: INFO Jail 'postfix-rbl' started
2026-02-11 13:16:28,678 fail2ban.jail [26970]: INFO Jail 'dovecot' started
2026-02-11 13:16:28,679 fail2ban.jail [26970]: INFO Jail 'postfix-sasl' started
2026-02-11 13:16:28,682 fail2ban.filtersystemd [26970]: INFO [dovecot] Jail is in operatio
n now (process new journal entries)
2026-02-11 13:16:28,682 fail2ban.filtersystemd [26970]: INFO [postfix-rbl] Jail is in oper
ation now (process new journal entries)
2026-02-11 13:16:28,683 fail2ban.filtersystemd [26970]: INFO [postfix-sasl] Jail is in ope
ration now (process new journal entries)
2026-02-11 13:16:28,683 fail2ban.jail [26970]: INFO Jail 'sshd-ddos' started
2026-02-11 13:16:28,683 fail2ban.filtersystemd [26970]: INFO [postfix] Jail is in operatio
n now (process new journal entries)
```

Просмотр журнала событий fail2ban (4)

## Проверка работы Fail2ban

На сервере посмотрели статус fail2ban: fail2ban-client status ([рис. @fig-017])



```
[root@server.tbmanturov.net ~]# fail2ban-client status
Status
|- Number of jail: 16
|- Jail list: apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-mo
dsecurity, apache-nohone, apache-noscript, apache-overflow, apache-shellshock, dovecot, postf
ix, postfix-rbl, postfix-sasl, selinux-ssh, sshd, sshd-ddos
[root@server.tbmanturov.net ~]#
```

Статус fail2ban

Посмотрели статус защиты SSH в fail2ban: fail2ban-client status sshd ([рис. @fig-018])

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

#### Статус защиты SSH в fail2ban (1)

Установили максимальное количество ошибок для SSH, равное 2: `fail2ban-client set sshd maxretry 2` ([рис. @fig-019])

```
[root@server.tbmanturov.net ~]# fail2ban-client set sshd maxretry 2
2
[root@server.tbmanturov.net ~]#
```

#### установка максимального количества ошибок для SSH

С клиента попытались зайти по SSH на сервер с неправильным паролем ([рис. @fig-020]), ([рис. @fig-021])

```
[root@client.tbmanturov.net ~]# ssh -p 2222 vagrant@10.0.2.2
vagrant@10.0.2.2's password:
Permission denied, please try again.
vagrant@10.0.2.2's password:
Permission denied, please try again.
vagrant@10.0.2.2's password:
vagrant@10.0.2.2: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@client.tbmanturov.net ~]#
```

#### Попытка зайти по SSH на сервер с клиента с неправильным паролем

На сервере посмотрели статус защиты SSH и убедились что произошла блокировка адреса клиента: `fail2ban-client status sshd` ([рис. @fig-022])

```
[root@server.tbmanturov.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 6
| -- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
-- Actions
| |- Currently banned: 2
| |- Total banned: 2
-- Banned IP list: 10.0.2.15 10.0.2.2
```

#### Статус защиты SSH в fail2ban (2)

Разблокировали IP-адрес клиента: `fail2ban-client set sshd unbanip <ip-адрес клиента>` ([рис. @fig-023])

```
[root@server.tbmanturov.net ~]# fail2ban-client set sshd unbanip 10.0.2.2
1
[root@server.tbmanturov.net ~]#
```

#### Разблокировка IP-адреса клиента

Вновь посмотрели статус защиты SSH и убедились, что блокировка клиента снята: `fail2ban-client status sshd` ([рис. @fig-024])

```
[root@server.tbmanturov.net ~]# fail2ban-client set sshd unbanip 10.0.2.2
1
[root@server.tbmanturov.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 6
| -- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
-- Actions
| |- Currently banned: 1
| |- Total banned: 2
-- Banned IP list: 10.0.2.15
```

#### Статус защиты SSH в fail2ban (3)

На сервере внесли изменение в конфигурационный файл `/etc/fail2ban/jail.d/customisation.local`, добавив в раздел по умолчанию игнорирование адреса клиента ([рис. @fig-025]):

```
[DEFAULT]
bantime = 3600
ignoreip = 127.0.0.1/8 <ip-адрес клиента>
```

```
[DEFAULT]
bantime = 3600
ignoreip = 127.0.0.1/8 10.0.2.2
```

#### Редактирование файла `/etc/fail2ban/jail.d/customisation.local` (4)

Перезапустили fail2ban: `systemctl restart fail2ban` ([рис. @fig-026])

```
[root@server.tbmanturov.net ~]# systemctl restart fail2ban
[root@server.tbmanturov.net ~]#
```

#### Перезапуск fail2ban (4)

Посмотрели журнал событий: `tail -f /var/log/fail2ban.log` ([рис. @fig-027])

```
-----
2026-02-11 13:44:56,226 fail2ban.actions [27799]: NOTICE [sshd] Ban 10.0.2.2
2026-02-11 13:45:00,863 fail2ban.filter [27799]: INFO [sshd] Found 10.0.2.2 - 2026-
02-11 13:45:00
2026-02-11 13:45:45,954 fail2ban.actions [27799]: NOTICE [sshd] Unban 10.0.2.2
└─
```

#### Просмотр журнала событий fail2ban (5)

## Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине `server` перешли в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/` и создали в нём каталог `protect`, в который поместили в соответствующие подкаталоги конфигурационные файлы ([рис. @fig-030]):

```
cd /vagrant/provision/server

mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d

cp -R /etc/fail2ban/jail.d/customisation.local
/vagrant/provision/server/protect/etc/fail2ban/jail.d/
```

```
[root@server.tbanturov.net ~]# cd /vagrant/provision/server
[root@server.tbanturov.net server]# mkdir -p /vagrant/provision/server/protect/etc/fail2ban/j
ail.d
[root@server.tbanturov.net server]# cp -R /etc/fail2ban/jail.d/customisation.local /vagrant/p
rovision/server/protect/etc/fail2ban/jail.d/
[root@server.tbanturov.net server]#
```

#### Копирование конфигурационных файлов в каталог protect на сервере

В каталоге `/vagrant/provision/server` создали исполняемый файл `protect.sh` ([рис. @fig-031]):

```
cd /vagrant/provision/server

touch protect.sh

chmod +x protect.sh
```

```
[root@server.tbanturov.net server]# cd /vagrant/provision/server
[root@server.tbanturov.net server]# touch protect.sh
[root@server.tbanturov.net server]# chmod +x protect.sh
[root@server.tbanturov.net server]#
```

#### Создание исполняемого файла protect.sh на сервере

Открыв его на редактирование, прописали в нём следующий скрипт ([рис. @fig-032]):

```
#!/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
```

```
root@server:/vagrant/provision/server -- sudo -l x root@serv
GNU nano 8.1 protect.sh
#!/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
```

#### Редактирование файла protect.sh на сервере

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в соответствующем разделе конфигураций для сервера ([рис. @fig-033]):

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

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

Редактирование файла Vagrantfile

После этого можно выключать виртуальные машины server и client: make server-halt и make client-halt ([рис. @fig-034])

## Контрольные вопросы + ответы

1. Поясните принцип работы Fail2ban.

Fail2ban является инструментом для защиты от атак на серверы, основанных на анализе журналов. Он мониторит журналы системы на предмет неудачных попыток входа или других событий, а затем блокирует IP-адреса атакующих с использованием системных средств, таких как iptables. Принцип работы:

- Мониторинг журналов на предмет определенных событий
- Обнаружение повторных неудачных попыток входа или других нарушений
- Динамическое обновление правил брандмауэра для блокировки атакующих IP-адресов

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

Настройки файла jail.local имеют более высокий приоритет и перекрывают настройки из jail.conf. Таким образом, если есть конфликтующие настройки, они будут использоваться из jail.local.

3. Как настроить оповещение администратора при срабатывании Fail2ban?

В файле jail.local нужно указать параметр destemail и задать адрес электронной почты, а также параметр action с указанием определенного действия (например, action\_mw для отправки почты).

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

Пример настроек для веб-службы в файле jail.conf:

```
[apache]
enabled = true
port = http,https
filter = apache-auth
logpath = /var/log/apache/*error.log
```

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

Пример настроек для почтовой службы в файле jail.conf:

```
[postfix]
enabled = true
filter = postfix
action = iptables-multiport[name=postfix, port="submission,smtps",
protocol=tcp]
```

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, такие как блокировка IP-адреса с использованием брандмауэра, отправка уведомлений, добавление в черные списки и т.д. Описание действий можно найти в конфигурационных файлах в разделе action.

7. Как получить список действующих правил Fail2ban?

Командой `fail2ban-client status`

8. Как получить статистику заблокированных Fail2ban адресов?

Командой `fail2ban-client status <jail_name>`

9. Как разблокировать IP-адрес?

Командой `fail2ban-client set <jail_name> unbanip <ip_address>`

## Выводы

В ходе выполнения лабораторной работы №16 мы получили навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

## Список литературы

1. Лабораторная работа №16