РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

ОТЧЕТ

по лабораторной работе № 16

**«Базовая защита от атак типа «brute force»»**

Дисциплина: Администрирование сетевых подсистем

Студент: Карташова А.С.

Группа: НФИбд-03-18

**МОСКВА**

2020 г.

**Оглавление**

[Цель работы 2](#_Toc61105089)

[Задачи 2](#_Toc61105090)

[Ход работы 2](#_Toc61105091)

[Защита с помощью Fail2ban 2](#_Toc61105092)

[Проверка работы Fail2ban 6](#_Toc61105093)

[Внесение изменений в настройки внутреннего окружения виртуальных машин 9](#_Toc61105094)

[Заключение 10](#_Toc61105095)

[Контрольные вопросы 11](#_Toc61105096)

# Цель работы

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

# Задачи

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

# Ход работы

## Защита с помощью Fail2ban

На сервере установим fail2ban:

**Команда:** dnf -y install fail2ban

Запустим сервер fail2ban:

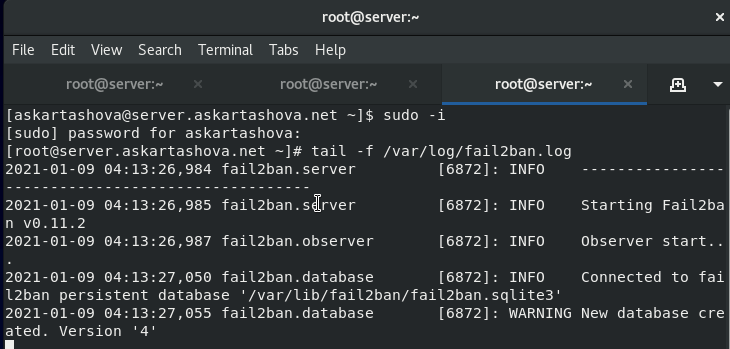
**Команда:** systemctl start fail2ban

systemctl enable fail2ban



В дополнительном терминале запустим просмотр журнала событий fail2ban:

**Команда:** tail -f /var/log/fail2ban.log

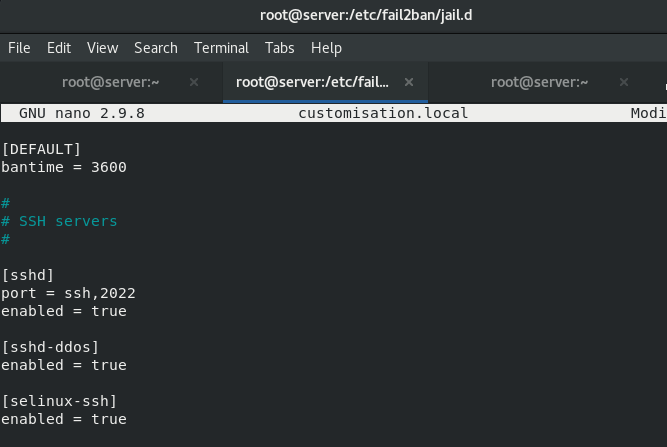


Создадим файл с локальной конфигурацией fail2ban:

**Команда:** touch /etc/fail2ban/jail.d/customisation.local

В файле /etc/fail2ban/jail.d/customisation.local:

1. задайте время блокирования на 1 час (время задаётся в секундах):
2. включим защиту SSH:

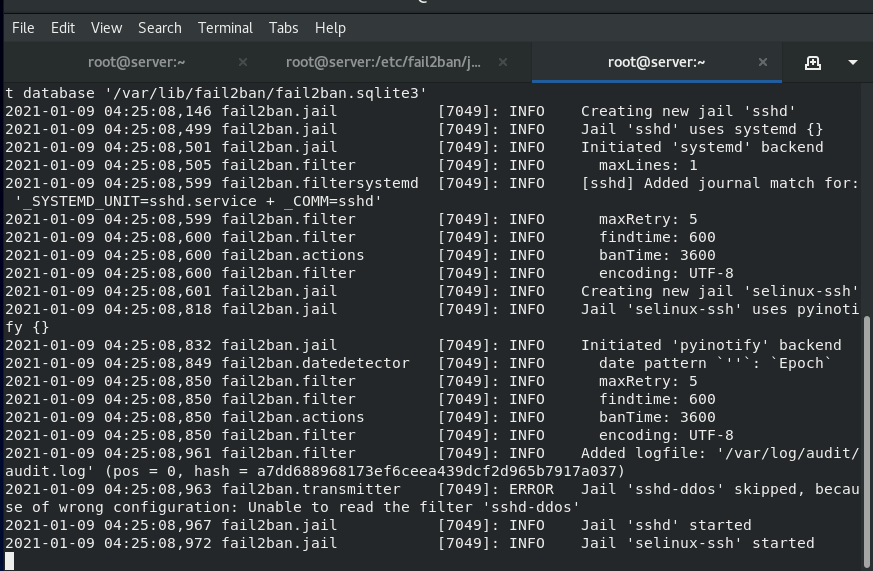


Перезапустим fail2ban

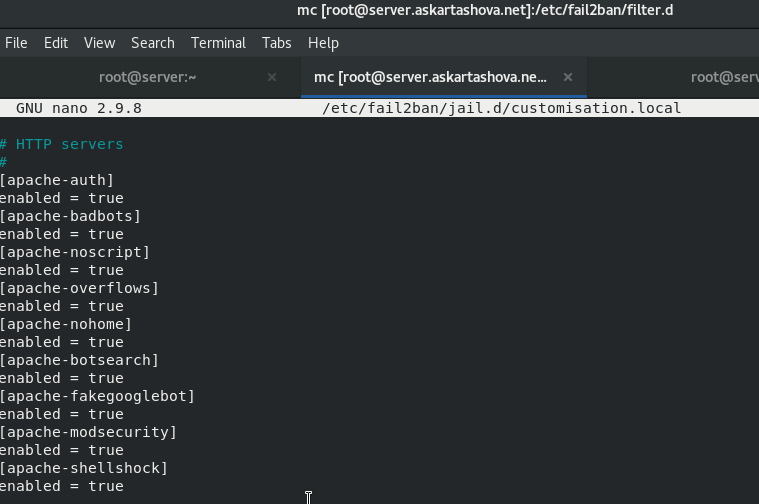
**Команда:** systemctl restart fail2ban

Посмотрим журнал событий:

**Команда:** tail -f /var/log/fail2ban.log



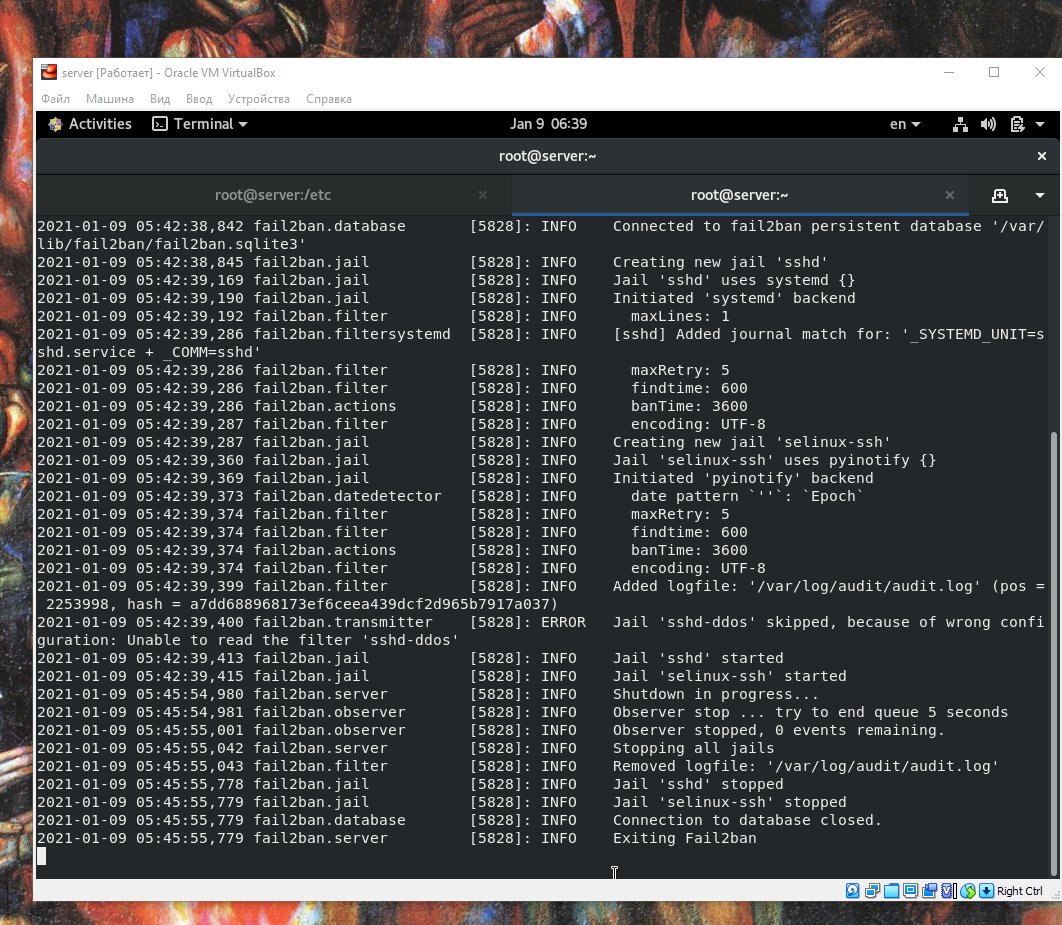
Мы видим, что запустились службы sshd и selinux-ssh

В файле /etc/fail2ban/jail.d/customisation.local включим защиту HTTP

Перезапустим fail2ban

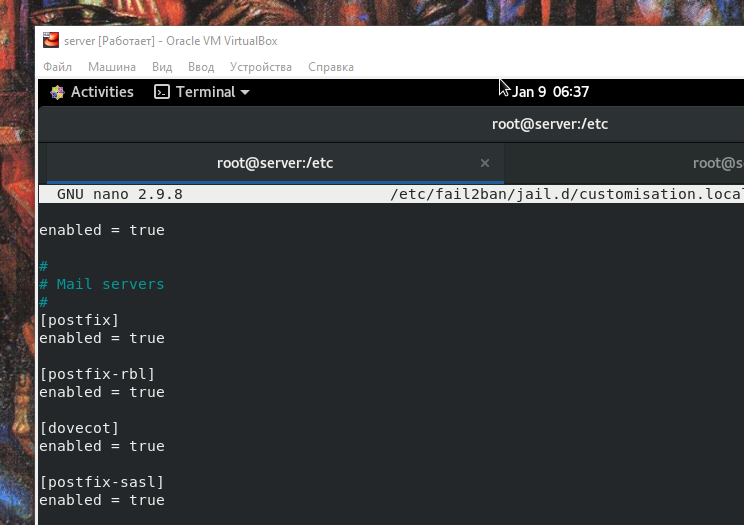
**Команда:** systemctl restart fail2ban

Посмотрим журнал событий:



**Команда:** tail -f /var/log/fail2ban.log

В файле /etc/fail2ban/jail.d/customisation.local включим защиту почты:

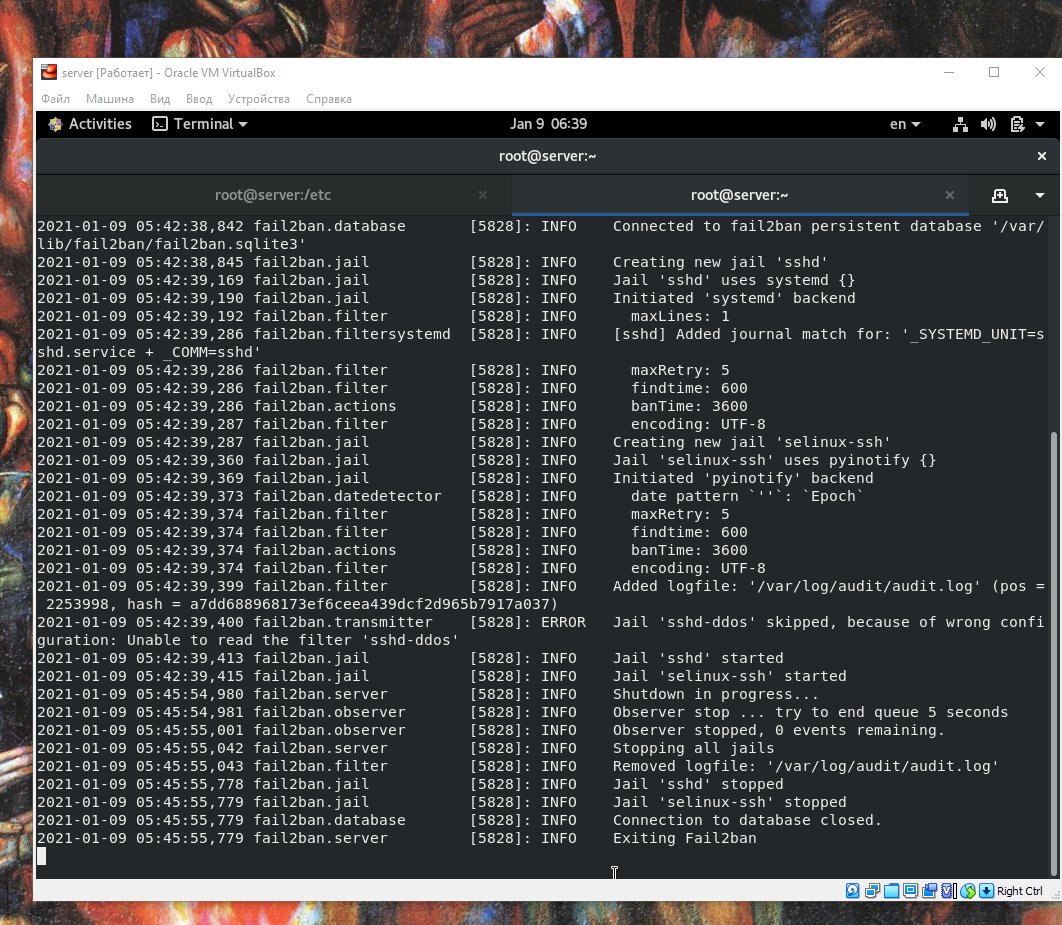


Перезапустим fail2ban:

**Команда:** systemctl restart fail2ban

Посмотрим журнал событий:

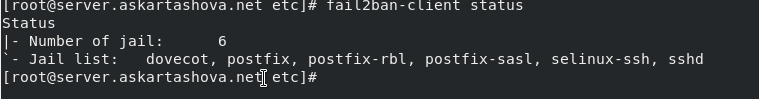
**Команда:** tail -f /var/log/fail2ban.log



## Проверка работы Fail2ban

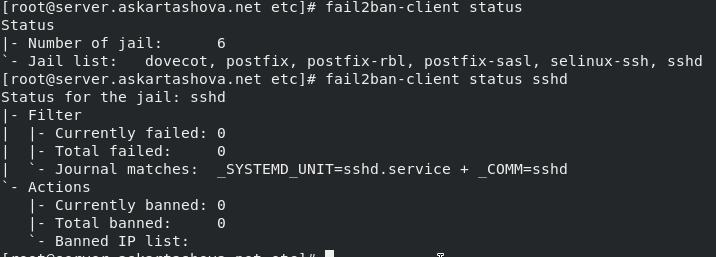
На сервере посмотрим статус fail2ban:

**Команда:** fail2ban-client status



Посмотрим статус защиты SSH в fail2ban:

**Команда:** fail2ban-client status sshd

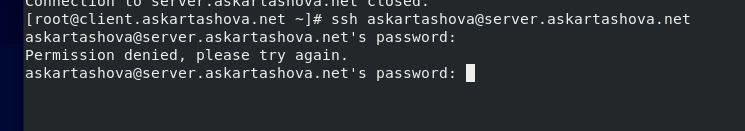


Установим максимальное количество ошибок для SSH, равное 2:

**Команда:** fail2ban-client set sshd maxretry 2

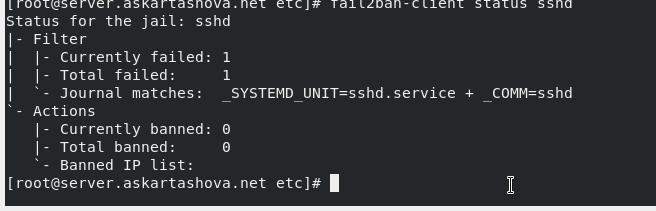


С клиента попытаемся зайти по SSH на сервер с неправильным паролем.



На сервере посмотрим статус защиты SSH:

**Команда:** fail2ban-client status sshd



Убедимся, что произошла блокировка адреса клиента.

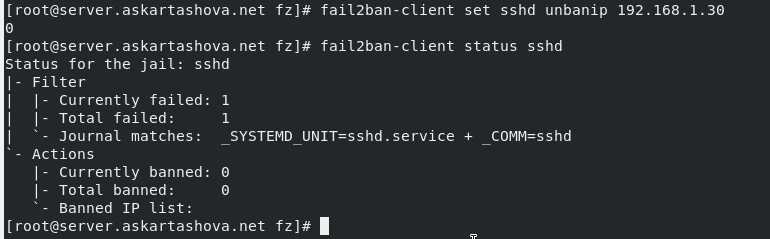
Разблокируем IP-адрес клиента:

**Команда:** fail2ban-client set sshd unbanip 192.168.1.30

Вновь посмотрим статус защиты SSH:

**Команда:** fail2ban-client status sshd

Убедимся, что блокировка клиента снята

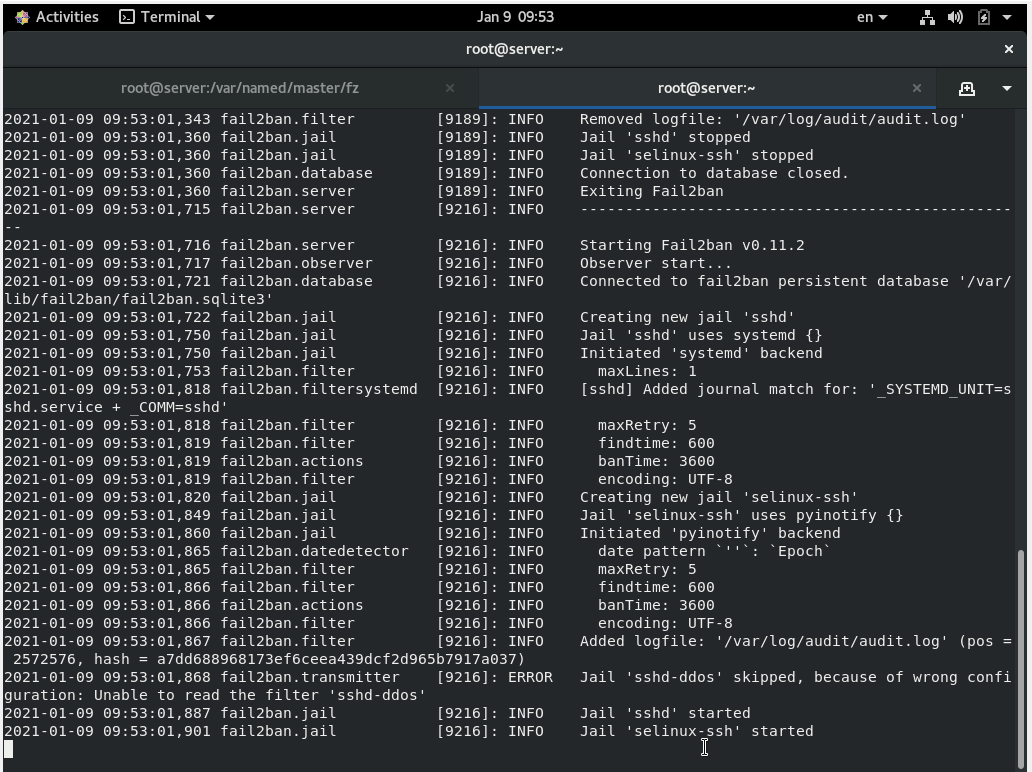


На сервере внесем изменение в конфигурационный файл /etc/fail2ban/jail.d/customisation.local, добавив в раздел по умолчанию игнорирование адреса клиента

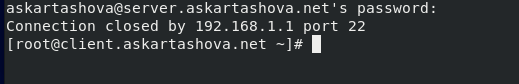
Перезапустим fail2ban.

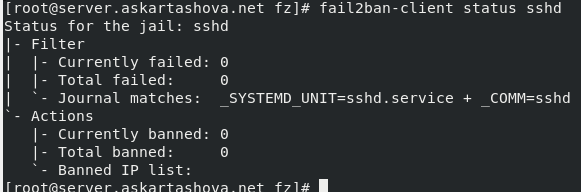


Посмотрим журнал событий:

**Команда:** tail -f /var/log/fail2ban.log

Вновь попытамся войти с клиента на сервер с неправильным паролем и посмотрит статус защиты SSH.



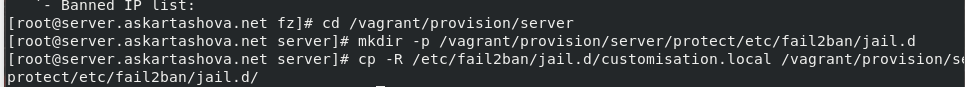


## Внесение изменений в настройки внутреннего окружения виртуальных машин

На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём

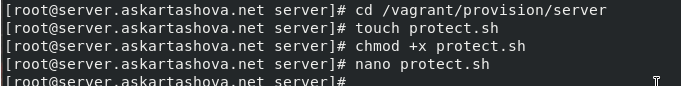
каталог protect, в который поместим в соответствующие подкаталоги конфигу-

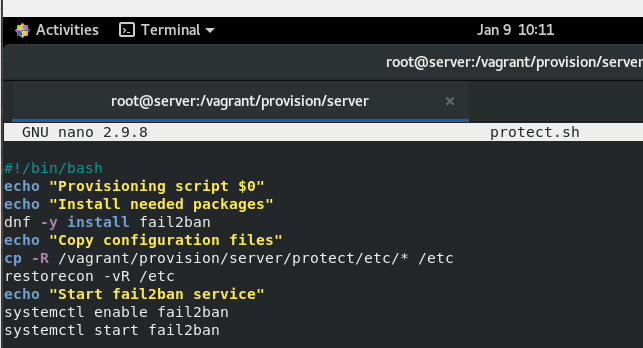
рационные файлы.



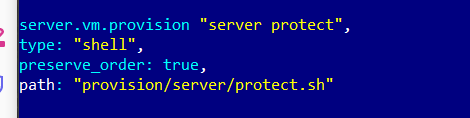
В каталоге /vagrant/provision/server создайте исполняемый файл protect.sh:

Открыв его на редактирование, пропишем в нём скрипт,  
повторяющий наши действия.





Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в соответствующем разделе конфигураций для сервера



# Заключение

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

# Контрольные вопросы

1. Поясните принцип работы Fail2ban.

Fail2ban отслеживает сетевую активность на портах узла путём сканирования текстовых лог-файлов. При выявлении программой неадекватной активности какого-то узла, его IP-адрес помещается в чёрный список, а все пакеты с этого адреса блокируются. Блокировка настраивается путём внесения изменений в правила межсетевого экрана.

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

Основной файл конфигурации конкретных служб в Fail2ban — /etc/fail2ban/jail.conf, для нас приорететнее собственный настройки, размещенные в файле customisation.local

1. Как настроить оповещение администратора при срабатывании Fail2ban?

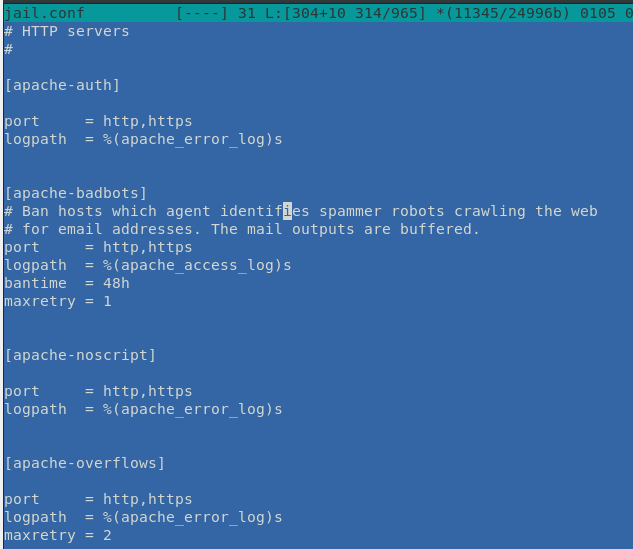
Настройки оповещения о срабатывании блокировки Fail2ban находятся в разделе [DEFAULT]. Если на машине был настроен почтовый сервер, он отправит письма на внешний адрес. Иначе все письма будут доставлены к локальной учетной записи Linux.

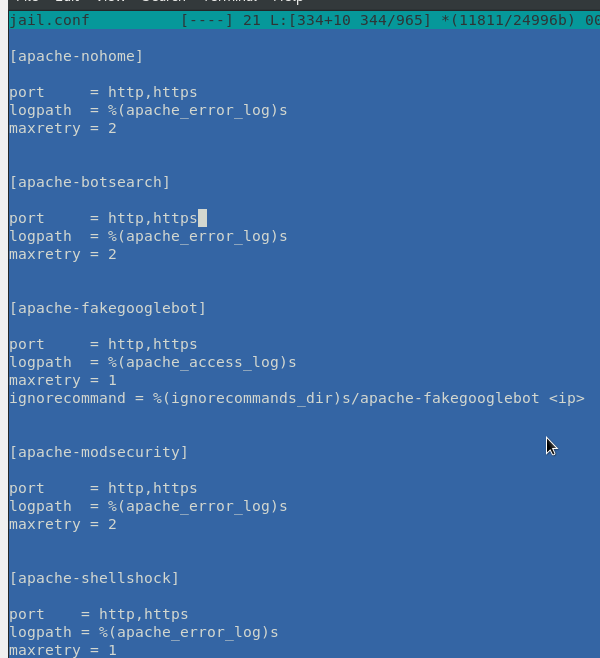
Для настройки используются два параметра:

* **destemail** - этот параметр задает адрес электронной почты, на который вы хотите получать сообщения. Значение по умолчанию root@localhost;
* **mta** - определяет почтовый агент, который будет использоваться для доставки почты. Если же письма нужно доставлять на локальную машину поменяйте значение на mail.

Также для локальной почты нужно заменить строчку **action\_mw** на**action\_mwl**:

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





apache-auth, apache-overflows, apache-auth, apache-nohome, apache-botsearch, apache-auth, apache-auth, apache-auth – сервисы(jails) веб-сервера apache

**maxretry**-количество срабатываний правил, после которого надо применять фильтр (бан)

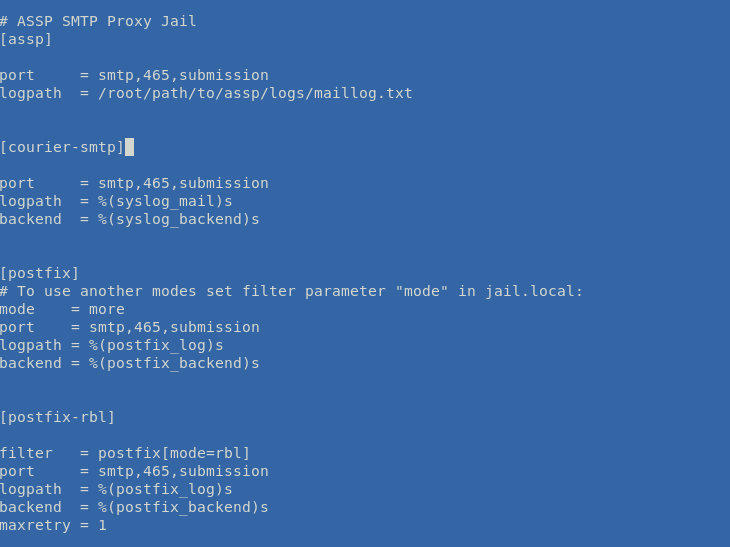
bantime - Указывается в секундах. Определяет на которой период времени будет блокироваться доступ, в случае срабатывания правила

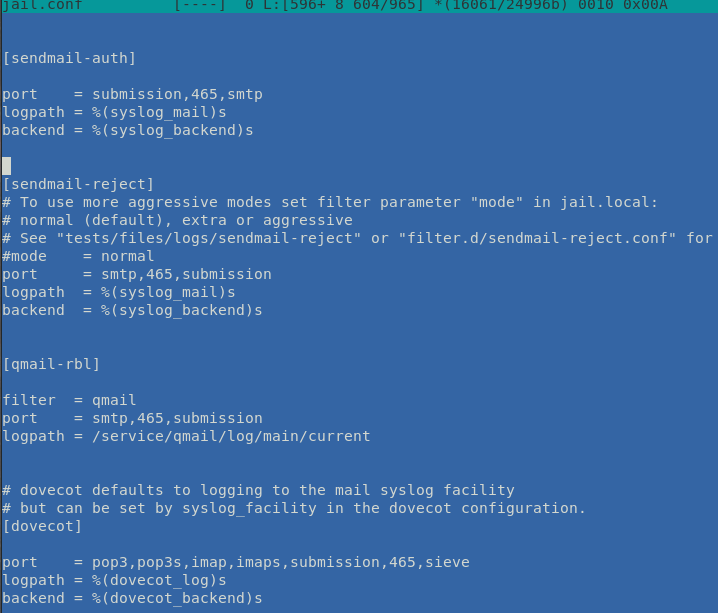
Параметр filter определяет является ли строка в логах индикатором об ошибочной авторизации или нет.

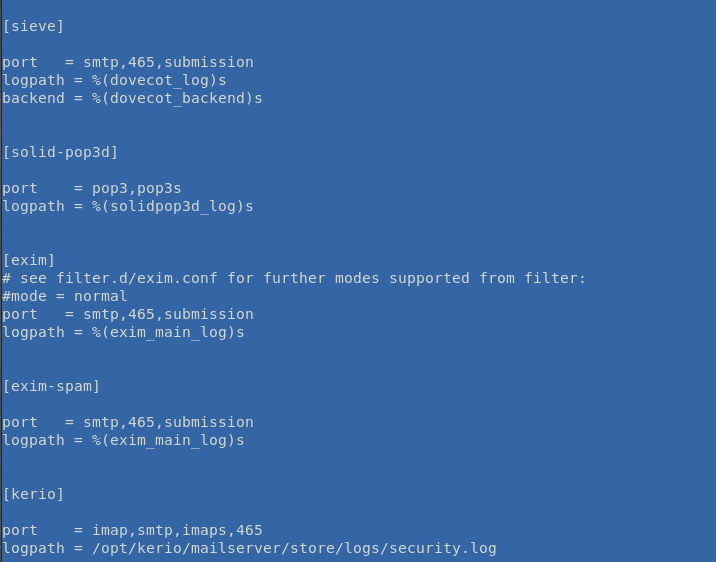
logpath – логи которые необходимо анализировать на предмет атаки

port- номера портов, которые необходимо блокировать

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





  
logpath – логи, которые необходимо анализировать на предмет атаки

port- номера портов, которые необходимо блокировать

assp – служба системы защиты от спама, распространяемая бесплатно.

exim (experimental internet mailer) — агент пересылки сообщений

postfix — агент передачи почты

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

Когда fail2ban мониторит логи сервиса, он смотрит на настроенный для этого сервиса фильтр. Фильтр предназначен для определения сбоев аутентификации этого конкретного сервиса на основе сложных регулярных выражений. Когда строка в файле лога сервиса совпадает с параметром failregex в соответствующем фильтре, fail2ban выполняет заданное фильтром действие. Действие определяется в переменной action.

Действие по умолчанию – блокировка потенциально вредоносного хоста/IP-адреса путем изменения правил брандмауэра iptables. Мы можем расширить это действие –  настроить электронные уведомления администратора с данными о злоумышленнике или строками лога, которые вызвали указанное действие. Доступные действия можно посмотреть в файле /etc/fail2ban/action.d.

1. Как получить список действующих правил Fail2ban?

**Команда:** *fail2ban-client status*

1. Как получить статистику заблокированных Fail2ban адресов?

**Команда:** *fail2ban-client -v status sshd*

1. Как разблокировать IP-адрес?

**Команда:** *fail2ban-client set sshd unbanip <ip-адрес клиента*