**GrayLog** это система сбора, обработки и визуализации логов. Справедливости ради хранятся данные в **noSQL** БД **ElasticSearch**. А **GrayLog** принимает данные, складывает в БД и может обрабатывать эти данные в рамках пользовательских настроек.

На данный момент существует уже 4-я версия **GrayLog**. С ней ты и познакомишься в этом уроке.

И **GrayLog** и **ElasticSearch** написаны на **Java**. А это значит что перед установкой и настройкой придется провести еще ряд манипуляций.

В качестве ОС традиционно возьмем **Ubuntu 22.04**

Если у тебя уже установлена и настроена **Java 11**, то можешь пропустить этот кусок урока.

sudo apt update

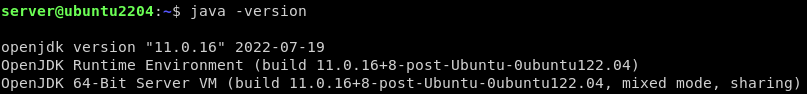
sudo apt install openjdk-11-jdk wget apt-transport-https curl gnupg2 nginx -y

Проверим, что установка прошла успешно:

java -version

Ответ должен быть похож на тот, что на скриншоте.

17:12



Дальше

17:12

После установки интерпретатора надо провести еще ряд манипуляций, чтобы все работало корректно (почему это не делается

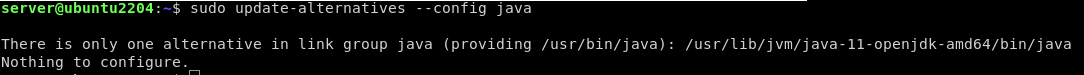
инсталляционным пакетом не представляю). Цель манипуляций - установка в системе переменной среды LS\_**JAVA\_HOME**.

А что же в нее писать? Сейчас узнаем с помощью следующей команды:

sudo update-alternatives --config java

Ты должен получить что-то похожее на скриншот ниже

17:12



Дальше

17:12

В списке может быть и несколько пунктов, если ты установил несколько версий **java**, то и пунктов в списке будет несколько.

Нужно выбрать тот, что соответствует 8-й версии и скопировать путь в скобках.

Теперь открывай текстовым редактором файл **/etc/environment** и давляй туда следующую строку (не забывай про sudo ;) ):

**LS\_JAVA\_HOME="/usr/lib/jvm/java-11-openjdk-amd64"**

17:12

Сохраняй файл. А теперь выполни вот эту команду:

**source /etc/environment**

Она применит внесенные нами изменения в текущем сеансе.

Дальше

17:12

17:12

Вот и все. **Java** установлена и готова к работе. Можно ставить написанные на этом языке приложения.

Дальше

17:12

Следующий шаг - установка **ElasticSearch**

17:12

На всякий случай предложу тот же выбор =). Вдруг у тебя уже все установлено =).

Установить ElasticSearch

17:13

**ElasticSearch** сама по себе заслуживает отдельного урока (а может и не одного) но сегодня мы не будем сильно заострять на ней

внимание. Нам важно знать, что эта БД будет хранить все наши логи и к ней будут обращаться установленные далее программы.

17:13

В стандартных репозиториях ElasticSearch нет. Поэтому сначала нужно подключить репозиторий:

curl -fsSL <https://artifacts.elastic.co/GPG-KEY-elasticsearch> |sudo gpg --dearmor -o /usr/share/keyrings/elastic.gpg

echo "deb [signed-by=/usr/share/keyrings/elastic.gpg] <https://artifacts.elastic.co/packages/7.x/apt> stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

apt update

Дальше

17:13

И теперь можно устанавливать.

apt install elasticsearch

17:13

Настройки хранятся в единственном файле конфигурации: **/etc/elasticsearch/elasticsearch.yml.** Обрати внимание, что файл в формате

**YAML**. Он вполне себе текстовый, но оформление специфическое. Постарайся не оставлять лишних отступов и пробелов.

Открываем файл:

sudo nano /etc/elasticsearch/elasticsearch.yml

Раскоментируйте и измените имя кластера на **graylog**

[**cluster.name**](https://cluster.name/)**: graylog**

Добавьте следующую информацию в тот же файл

[**action.auto**](https://action.auto/)**\_create\_index: false**

Дальше

17:13

Теперь пропишем сервис в автозагрузку и запустим его:

sudo systemctl daemon-reload

sudo systemctl enable elasticsearch

sudo systemctl start elasticsearch

Даже если запуск прошел успешно и ты увидел зеленое "ОК", все равно есть смысл все перепроверить.

Для начала введи

sudo netstat -lpn | grep 9200

17:13



Дальше

17:13

17:13

Сервис слушает порт **9200/tcp**. Как видишь сервис слушает его на адресе **127.0.0.1.** Это сделано для безопасности. Случаи с

открытым незапароленным доступом в интернет баз популярных сервисов не редкость. Поэтому по умолчанию доступа извне нет. Если

системный администратор его откроет, то это будет уже осознанный поступок.

Дальше

17:13

Теперь будем пробовать обратиться на этот порт. У **ElasticSearch** нет своего хитрого протокола, как у других БД. Общение идет

по http обычным текстом. Надо конечно соблюдать синтаксис, но в целом это же текст. Формат запросов - json. И поэтому проверку можно провести даже

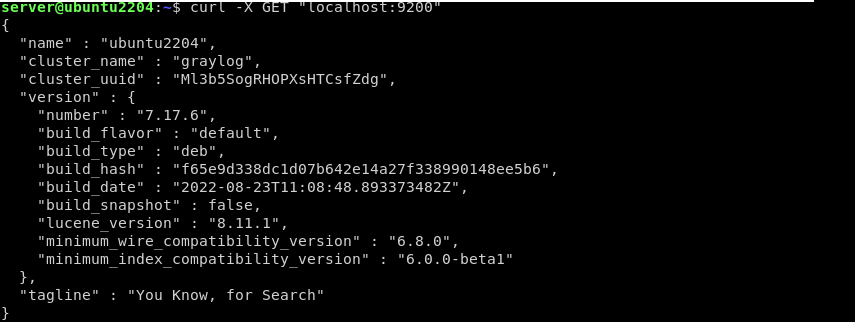
с помощью **curl** (если нету то установи).

Вводи вот такую команду:

curl -X GET "[localhost:9200](https://localhost:9200/)"

В ответ ты должен будешь получить тоже json.

17:13



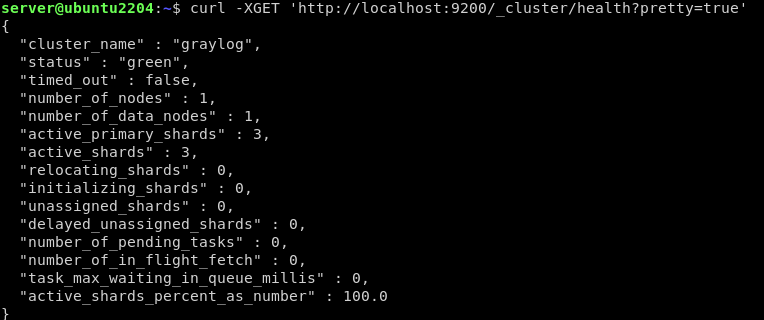
Дальше

17:13

А вот так можно посмотреть состояние сервиса (вид изнутри).

curl -XGET '<http://localhost:9200/_cluster/health?pretty=true>'

17:13



Дальше

17:13

17:13

Если **ElasticSearch** тебе ответил, то установка прошла успешно и БД готова к работе.

Дальше

17:13

Следующим этапом будет установка **MongoDB.**

17:13

В ранних версиях **GrayLog** она использовалась для всего. Однако ввиду ее недостаточной производительности перевели основную нагрузку в **ElasticSearch**.

Но **MongoDB** все еще требуется. В ней хранятся настройки **GrayLog**.

Дальше

17:13

17:13

Однако для начала надо поставить ряд пакетов, которые нам пригодятся в дальнейших шагах.

sudo apt install apt-transport-https openjdk-11-jre-headless uuid-runtime pwgen

Дальше

17:13

Итак. Приступим к установке **MongoDB**

Первым делом надо подключить репозиторий.

curl -fsSL [https://www.mongodb.org/static/pgp/server-5.0.asc|sudo](https://www.mongodb.org/static/pgp/server-5.0.asc%7Csudo) gpg --dearmor -o /etc/apt/trusted.gpg.d/mongodb.gpg

echo "deb [ arch=amd64,arm64 ] <https://repo.mongodb.org/apt/ubuntu> focal/mongodb-org/5.0 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-5.0.list

sudo apt update

И устанавливаем.

sudo apt install -y mongodb-org

17:13

Если будут проблемы с установкой, то тут можно найти решение.

<https://stackoverflow.com/questions/73656873/unable-to-install-mongodb-in-ubuntu-22-04-mongodb-org-libssl1-1>

Дальше

17:13

Прописываем в автозагрузку и включаем сервис.

sudo systemctl enable mongod.service

sudo systemctl start mongod.service

После включения естественно надо все проверить.

Для начала выполняем вот такую команду:

sudo systemctl --type=service --state=active | grep mongod

17:13



Дальше

17:13

Также проверим с помощь **netstat**, что сервис слушает порт.

sudo netstat -lpn | grep mongo



17:13

Как видишь эта БД тоже принимает подключения только от локальных сервисов. По умолчанию она тоже не запаролена =).

Дальше

17:13

17:13

И наконец мы добрались до установки самого **GrayLog**

Дальше

17:13

Установка **GrayLog** традиционно начинается с подключения репозитория =). Правда теперь другим способом =).

wget <https://packages.graylog2.org/repo/packages/graylog-4.3-repository_latest.deb>

sudo dpkg -i graylog-4.3-repository\_latest.deb

sudo apt update

17:13

А после этого устанавливаем.

sudo apt update && sudo apt-get install graylog-server graylog-enterprise-plugins graylog-integrations-plugins graylog-enterprise-integrations-plugins

Дальше

17:14

Конфигурация GrayLog хранится в файле **/etc/graylog/server/server.conf.** Он достаточно большой и по умолчанию предполагает, что **elasticsearch** и **mongodb** слушают на адресе **127.0.0.1** и не запаролены. Так, что если ты решил на предыдущих шагах посамовольничать, то лучше вернуть все на место =).

17:14

Дальше

17:14

1. Секретный пароль.

Он должен быть всегда размером 64 символа. И для его генерации и ставилась утилита pwgen. Итак:

pwgen -N 1 -s 96



17:14

Это строку нужно сохранить и подставить в конфигурационном файле как значение параметра **password\_secret**

Дальше

17:14

2. Пароль адмнистратора.

Этот пароль представляет собой хэш по алгоритму **sha256**

Генерируется он следующим образом:

echo -n **твой\_пароль** | sha256sum



17:14

Эту строчку нужно вписать, как значение параметра **root\_password\_sha2**

Дальше

17:14

17:14

3. Почта администратора.

Для того, чтобы GrayLog мог присылать уведомления, надо задать почтовый адрес администратора. Делается это вот таким параметром файла конфигурации:

**root\_email = “**[**example@domain.com**](mailto:example@domain.com)**”**

Дальше

17:14

4. Доступ к веб-интерфейсу.

По умолчанию **GrayLog**, как и все другие установленные нами сегодня сервисы, принимает подключения на адресе **127.0.0.1**

Но т.к. доступ запаролен и мы с тобой только что этот пароль задали - можем открыть доступ из локальной сети.

17:14

Для этого в конфигурационном файле нужно отредактировать параметр **http\_bind\_address**

**http\_bind\_address = ip-адрес:9000**

Дальше

17:14

На этом конфигурирование **GrayLog** закончено. Но нужно поправить ряд параметров конфигурации **ElasticSearch**.

17:14

Необходимо в конфигурации **ElasticSearch** задать имя кластера. Вот такой строкой:

(если вы еще не поменяли , как было сказано в начале урока)

[**сluster.name**](https://xn--luster-hrf.name/)**: graylog**

Дальше

17:14

Поправил конфигурацию **ElasticSearch**? Теперь надо применить изменения.

sudo systemctl restart elasticsearch

17:14

И вот теперь уже можно запускать **GrayLog**

sudo systemctl daemon-reload

sudo systemctl enable graylog-server

sudo systemctl restart mongod graylog-server

Дальше

17:14

Теперь проверим что веб-интерфейс включился.

sudo netstat -lpn | grep 9000

Не пугайся если порт недоступен сразу после старта. Это же Java, так что подожди секунд 10 перед тем как паниковать =).



17:14

Все. На этом установка закончена и можно переходить к конфигурированию.

Дальше

17:14

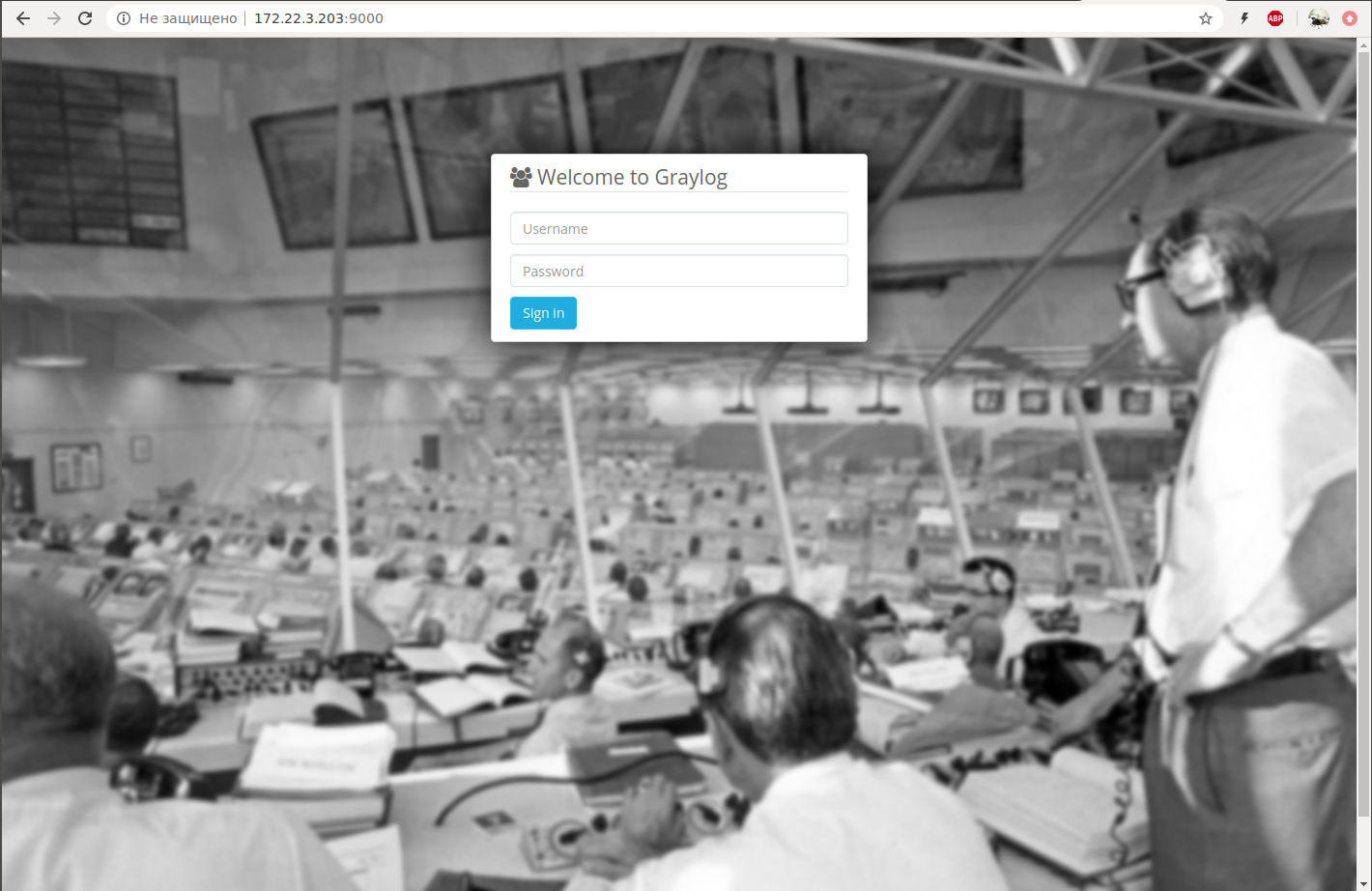
И вот пришло время зайти на веб-интерфейс и начать пользоваться нашим комплексом для сбора и обработки логов.

Набирай в адресной строке браузера:

[**http://ip\_graylog\_server:9000**](http://ip_graylog_server:9000/)

**ip\_graylog\_server** конечно надо заменить на адрес виртуалки или сервера, на котором ты только что поднимал **GrayLog**.

17:14



Дальше

17:14

17:14

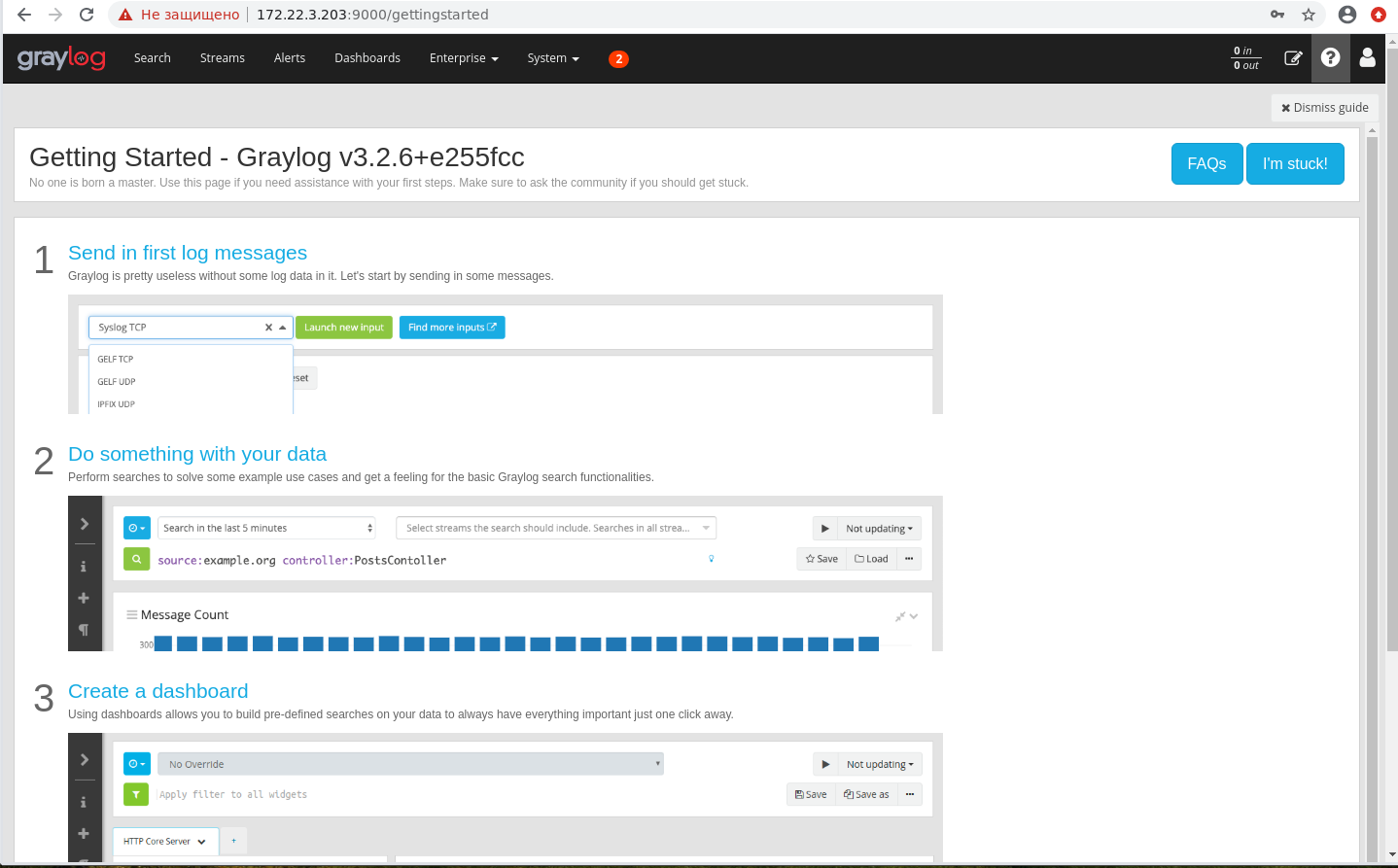
Логин администратора - **admin**

а пароль тот, который ты использовал при генерации хеша.

Дальше

17:14

Если ты ничего не напутал, то увидишь вот такую картинку.



17:14

Тут тебе разработчики **GrayLog** посказывают первоначальные настройки. Примерно это мы с тобой сейчас и выполним.

Дальше

17:14

Изначально **GrayLog** у нас практически без настроек. Он даже локальные логи никакие не видит. Исправим это.

Прием логов происходит посредством сетевого соединения. Туда может писать непосредственно syslog, а может и кто-то еще.

17:14

После приема система разбирает каждую строчку по специальному шаблону на части (date, time, source, message и т.д.). Сообщения можно искать по каждой из частей. К примеру вывести все сообщения с хоста **1.2.1.2.**

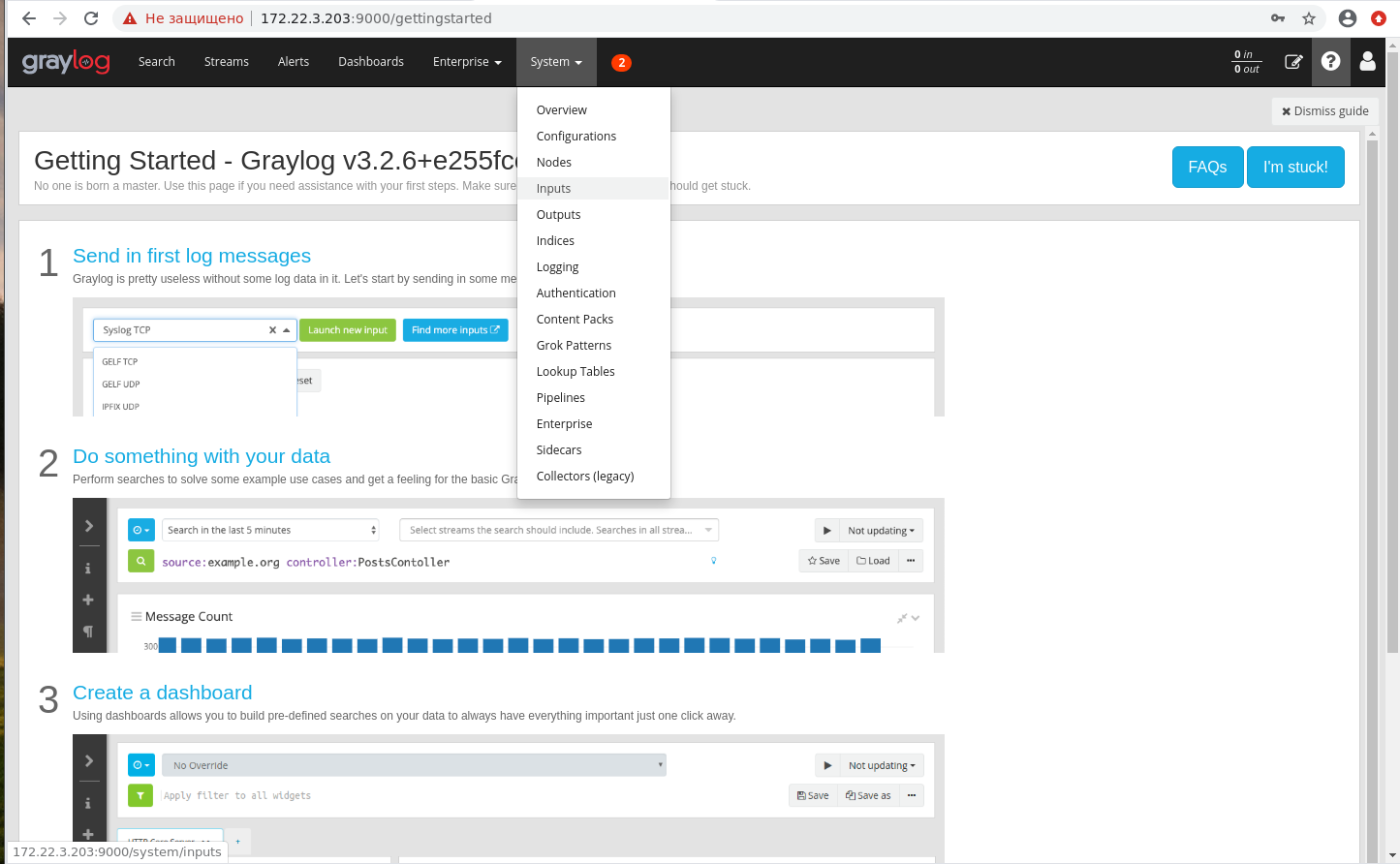
Дальше

17:14

Логично, что первым шагом будет настройка приемника логов.

Для этого обратимся к меню в верхней части сайта. Нажми на пункт **System**. В выпадающем меню выбери пункт **Input**

17:14



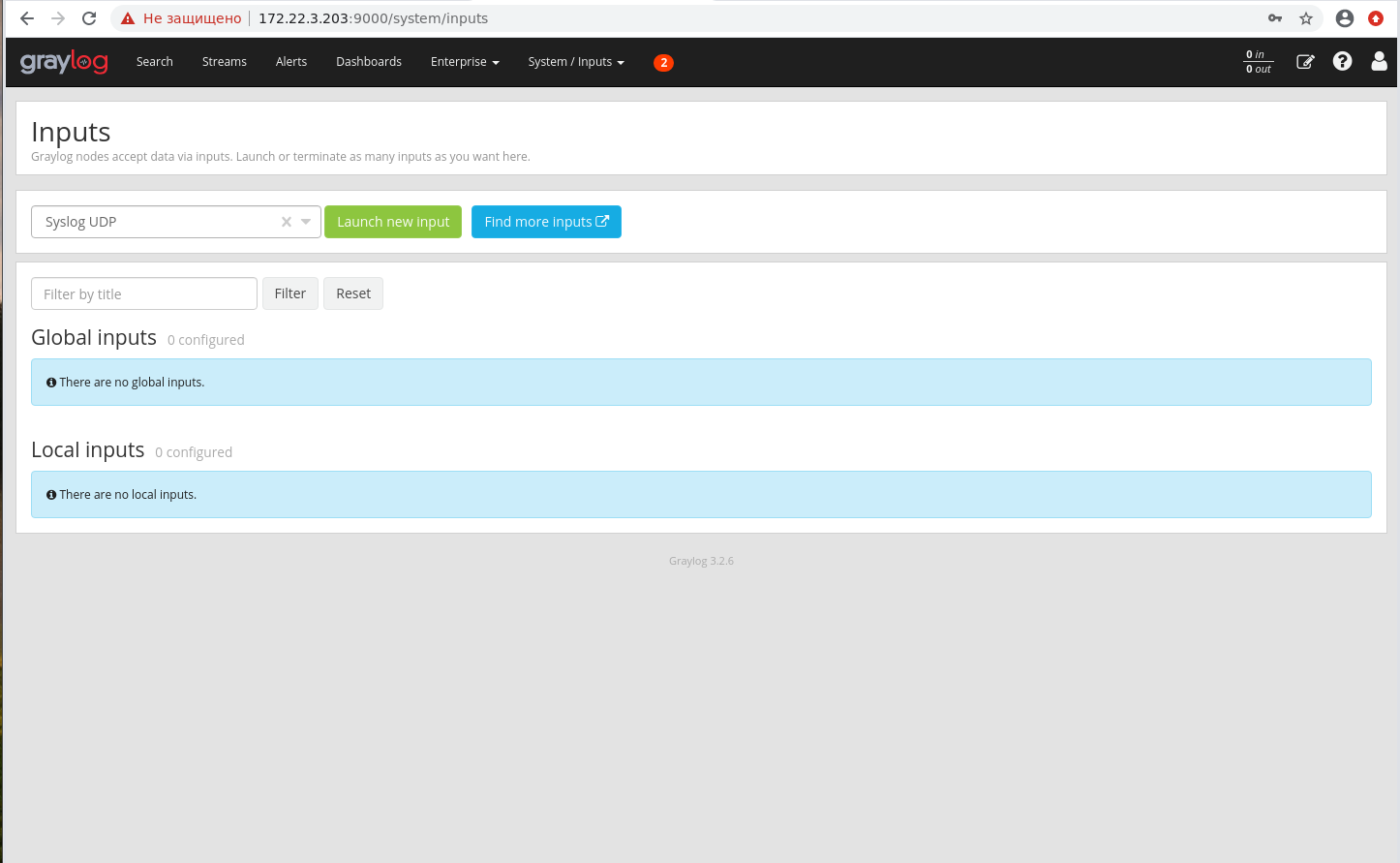
Дальше

17:14

Никаких приемников логов у тебя пока нет. Поэтому тебе предлагается создать новый.

В выпадающем списке надо выбрать **Syslog UDP** (или tcp. Главное чтобы совпадало с конфигом syslog, который будет слать эти логи).

И жми **Launch new input**



17:15

Как ты увидел по выпадающему списку, **GrayLog** умеет принимать логи в множестве форматов. Их мы рассматривать не будем, но ты сможешь позже сделать это самостоятельно.

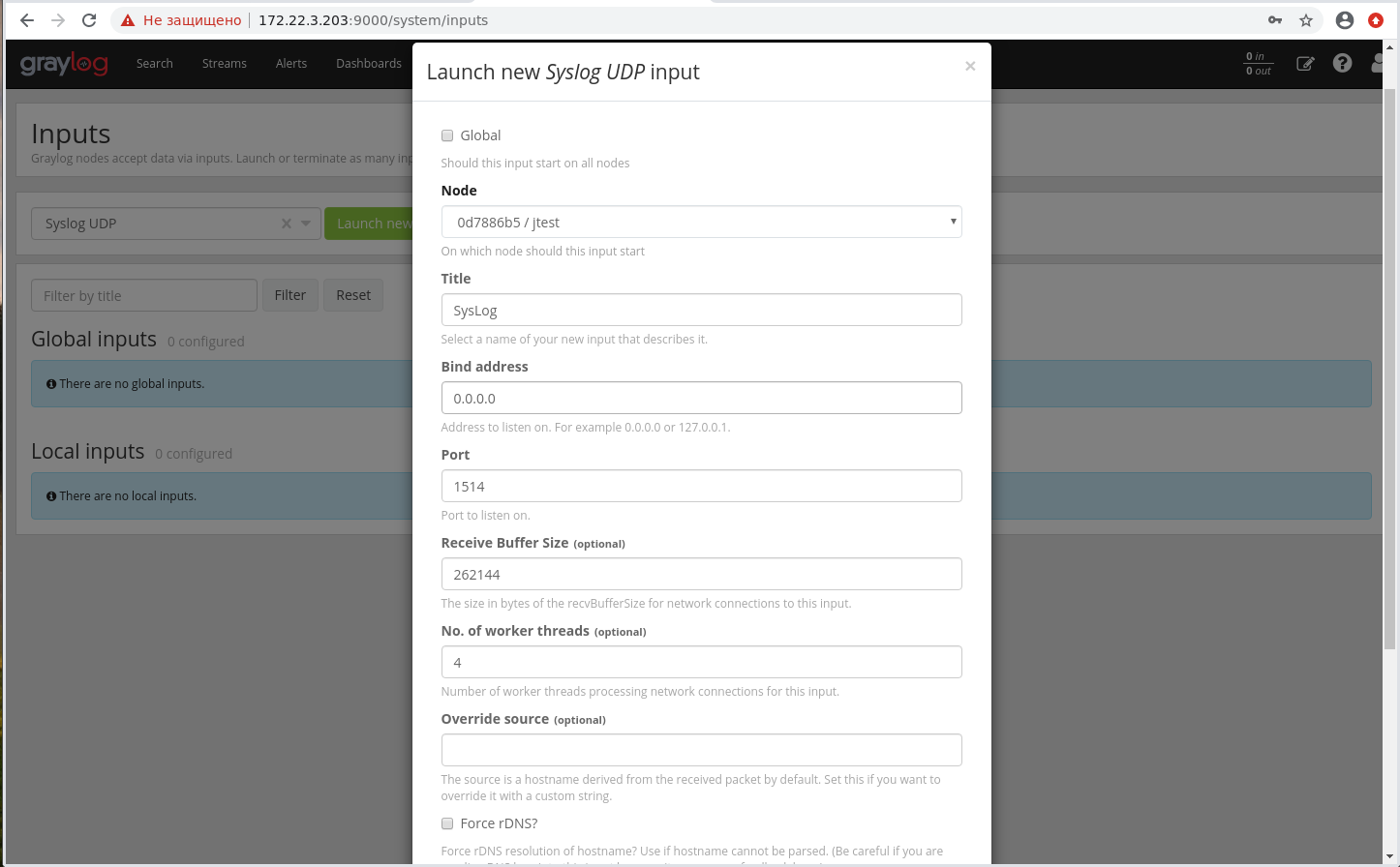
Дальше

17:15

Итак. Ты все нажал. Теперь перед тобой окно с настройками приемника.

Заполняй как на картинке.

Порт **1514** потому, что **514** занят имеющимся демоном **syslog** на сервере.



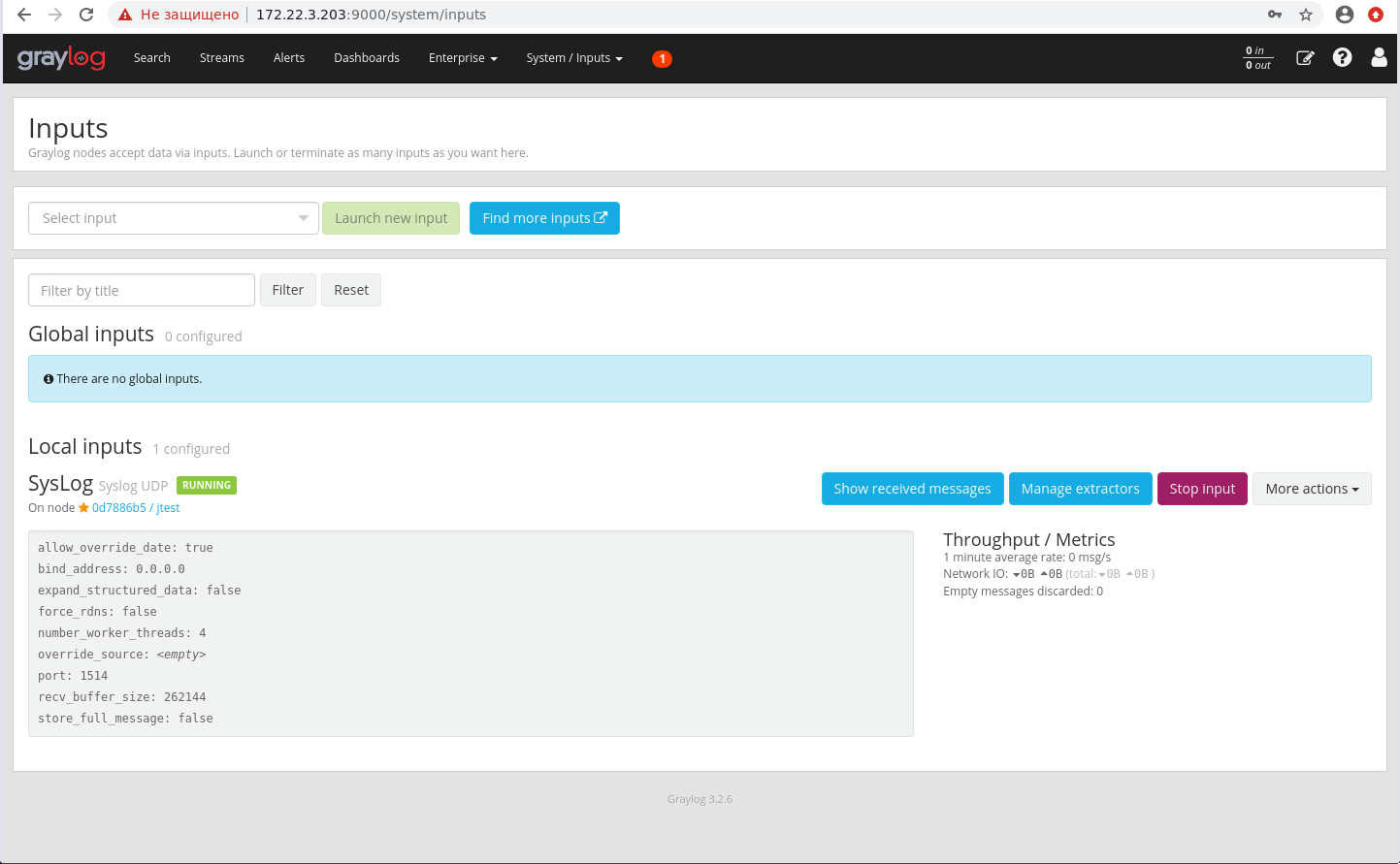
17:15

Заполнил? Жми **Save**

Дальше

17:15

Если ты все сделал правильно, то увидишь вот такую картинку.



17:15

По зеленому цвету надписи **RUNNING** можно понять что все получилось и приемник настроен и запущен.

Теперь сделай такой же приемник, но **TCP**.

А после этого попробуем направить хоть что-нибудь в эти приемники.

Дальше

17:15

Для начала направим логи локального syslog.

Т.к. у нас **Ubuntu** 22**.04**, то в качестве syslog-сервера используется **rsyslog**.

Открывай файл **/etc/rsyslog.d/all.conf** в текстовом редакторе и добавь туда вот такую строку:

***\*.\* @@127.0.0.1:1514***

17:15

После этого надо перезапустить сервис.

sudo service rsyslog restart

Дальше

17:15

И еще раз перезапустим...

sudo service rsyslog restart

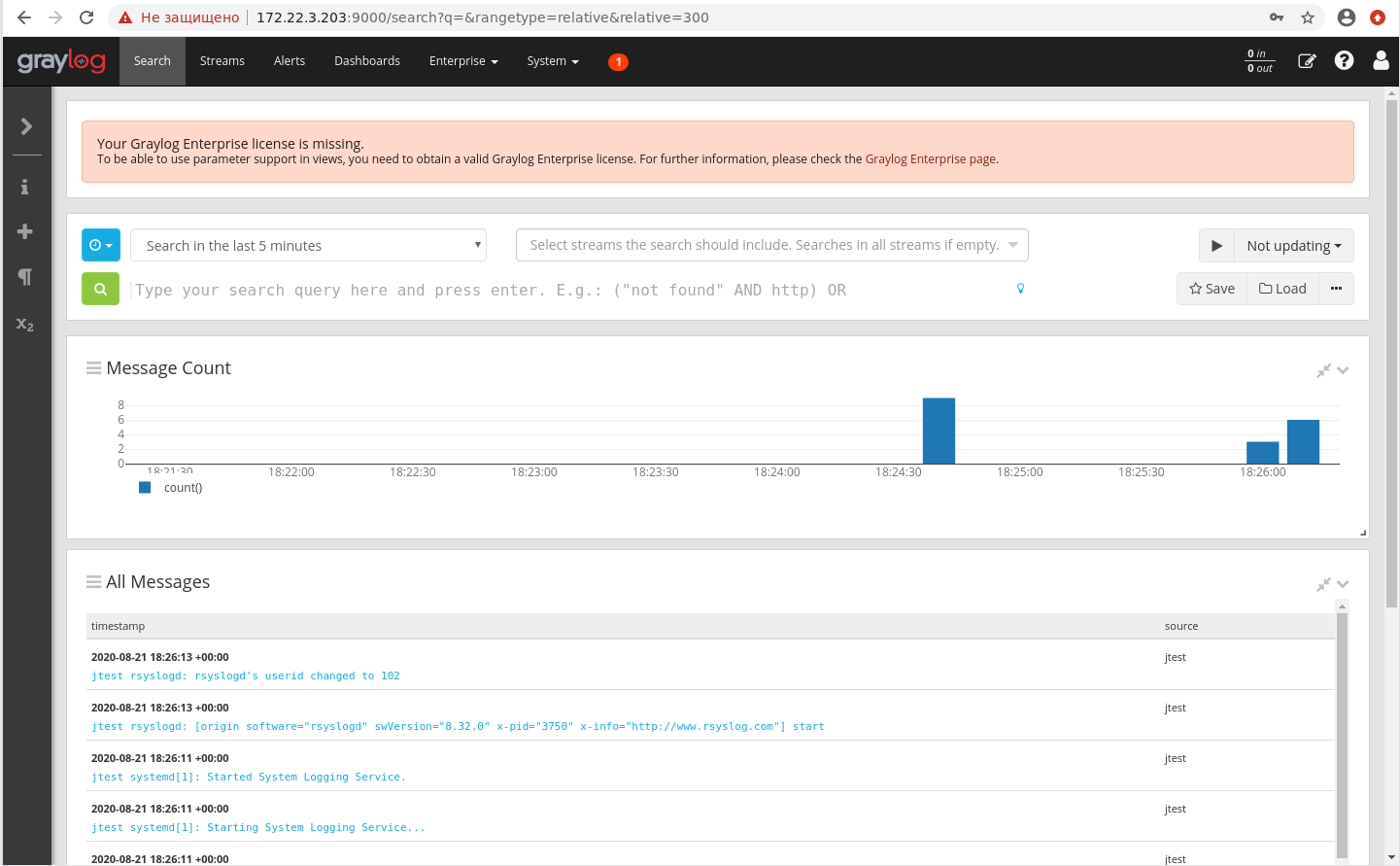
17:15

Теперь можно проверять что получилось.

Дальше

17:15

Возвращайся к веб-интерфейсу. Теперь тебе надо в верхней панели выбрать пункт **Search**



17:15

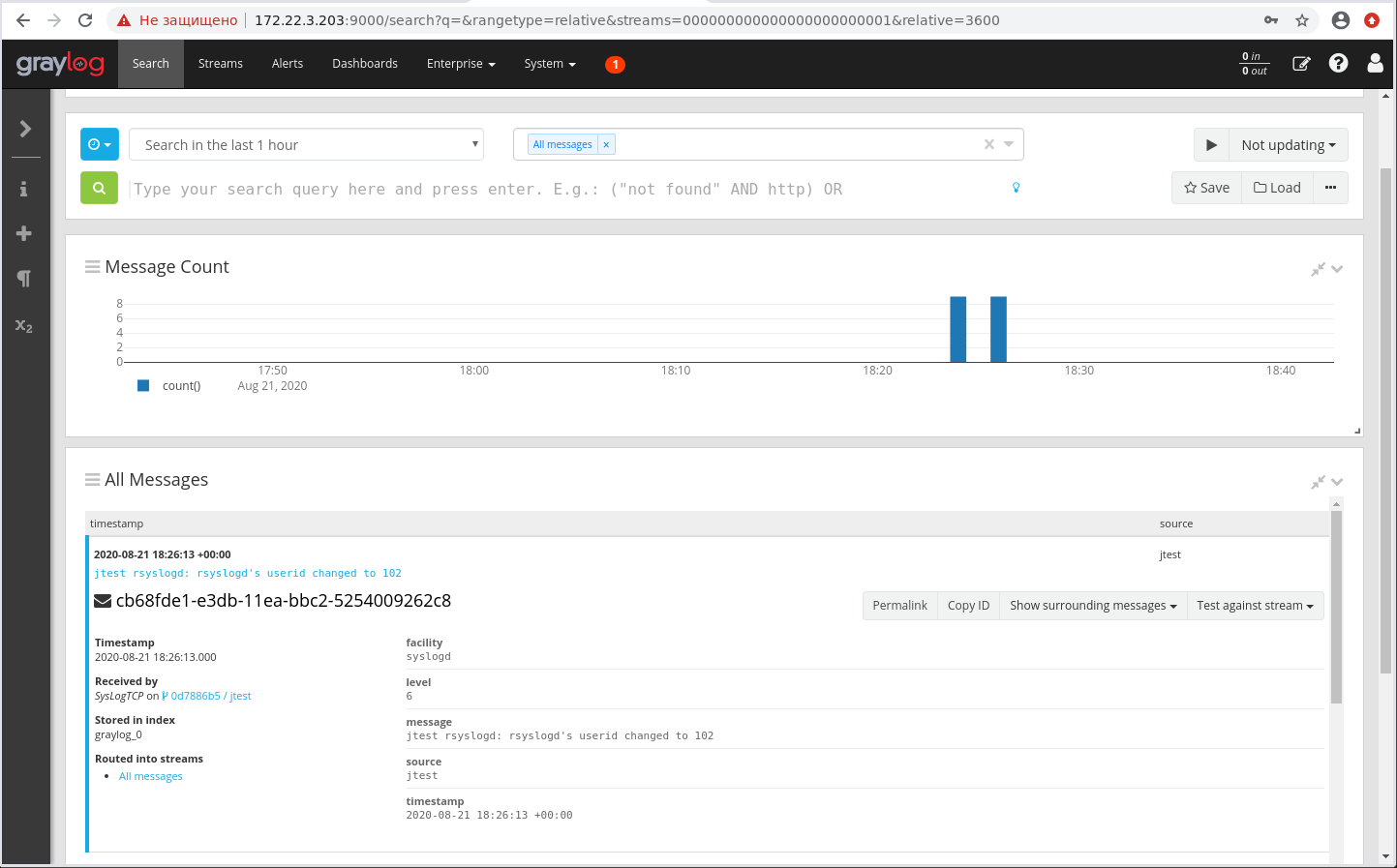
Круто. Да?

А теперь сделай ту же настройку rsyslog на других серверах. Только IP-адрес там нужно указать не локальной петли, а сервера GrayLog.

Дальше

17:15

А теперь нажми на одно из сообщений. Оно раскроется с подробностями. Можно увидеть названия полей.

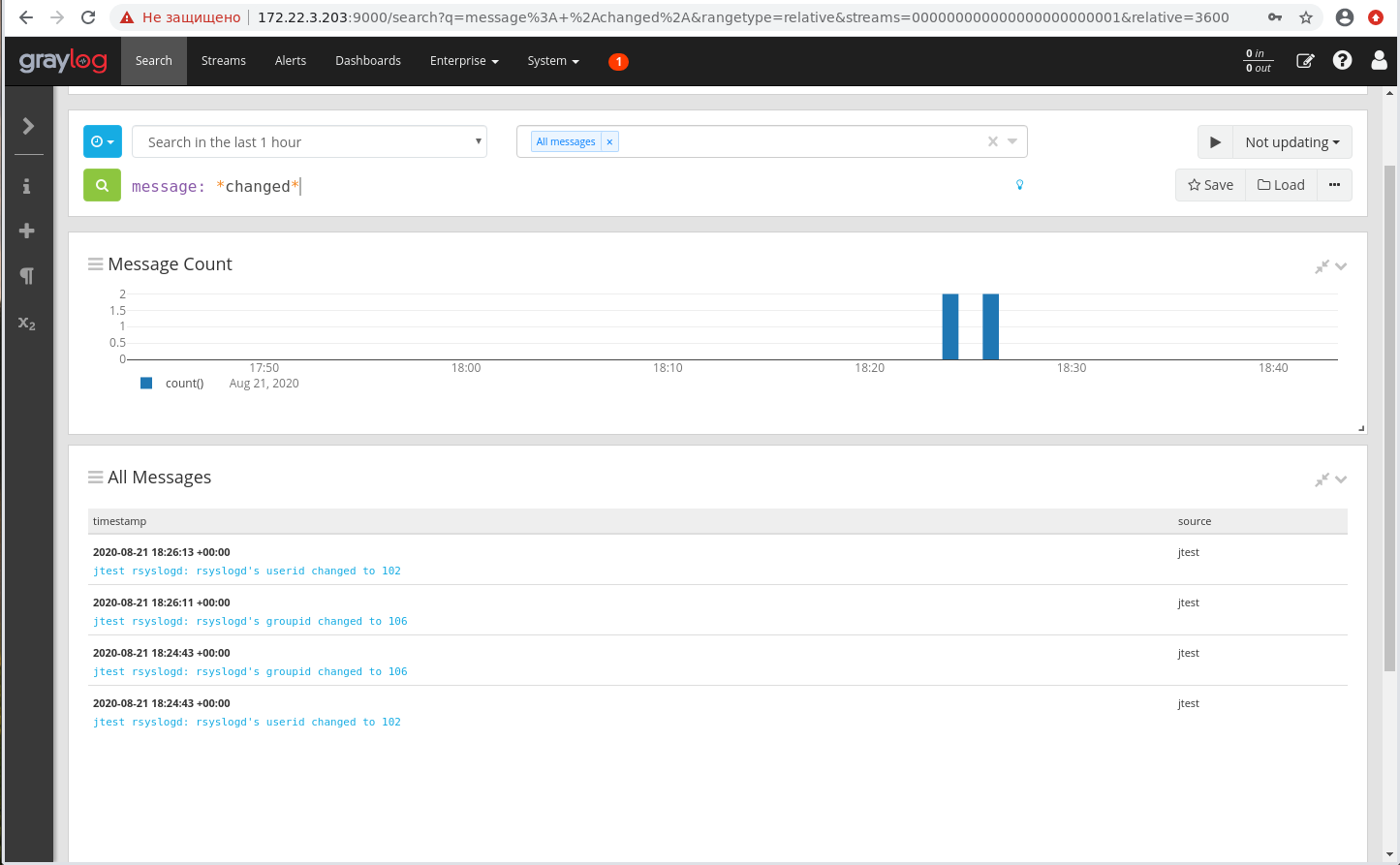


А теперь попробуй ввести в поле фильтра выражение для поиска:

**message: \*changed\***

(вообще можешь другое слово выбрать. но только чтобы оно было не в каждом сообщении)

17:15



Дальше

17:15

А теперь попробуй поиграться с фильтрами. Там помимо строки поиска можно еще выбирать и временные промежутки.

17:15

По сути сейчас у тебя получился централизованный syslog-сервер. Только ищешь ты по логам не **grep**-ом, а через удобный и красивый веб-интерфейс.

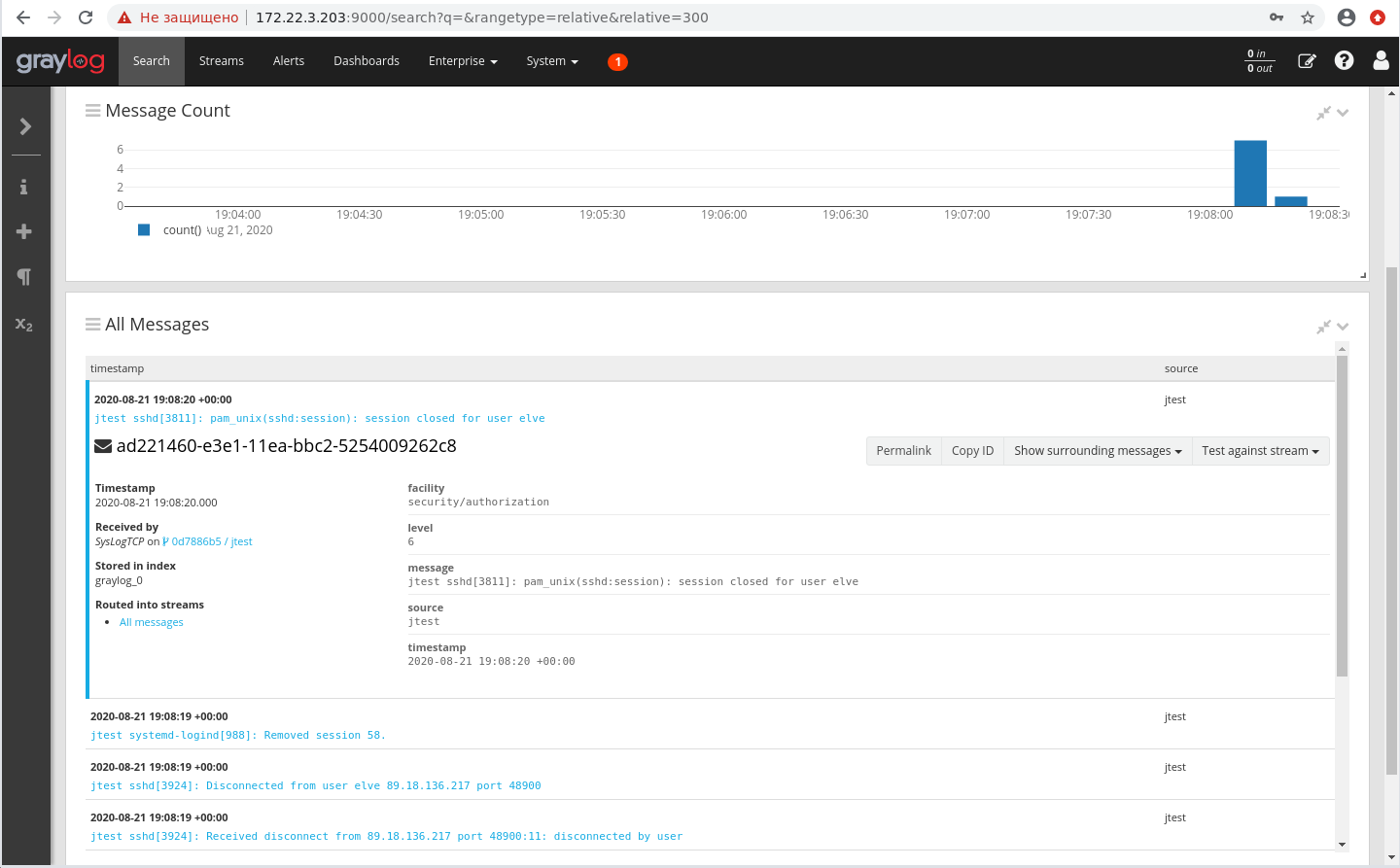
Уже хорошо. Но это далеко не все, что умеет **GrayLog** и не все, что я хочу тебе показать.

Дальше

17:16

Не уходим из раздела Search, но сбросим фильтры.

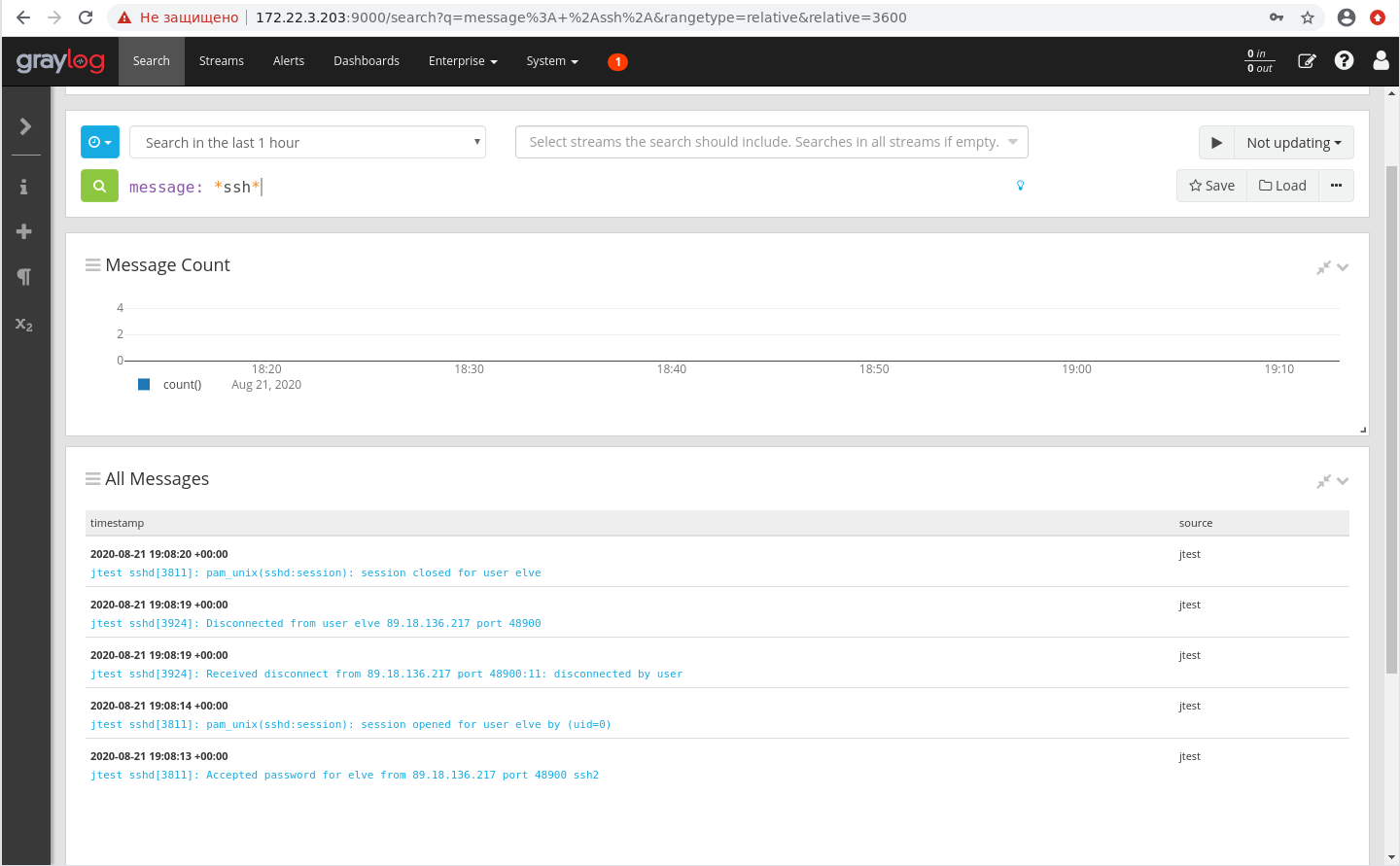
Теперь надо зайти на сервер и выйти с него по ssh. Это нужно, чтобы в логах отразилась эта информация.



Сделаем выборку по фильтру:

**message: \*ssh\***

17:16

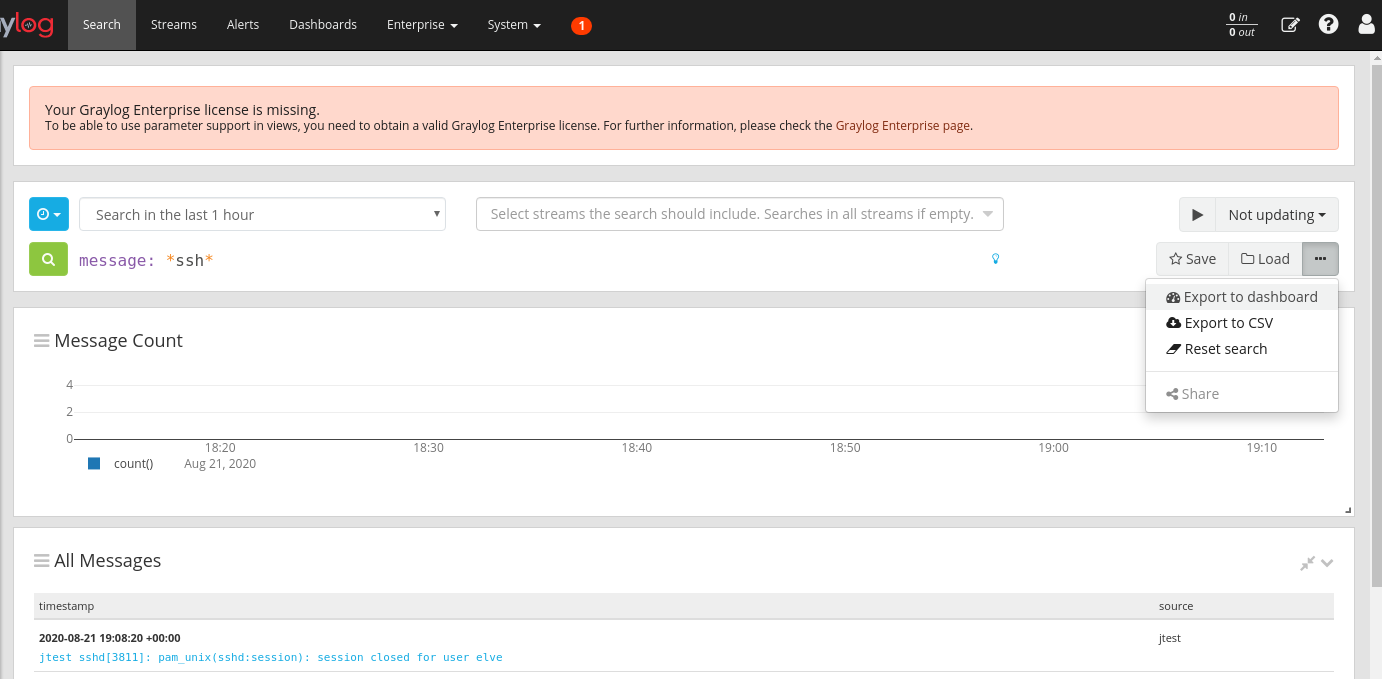


Дальше

17:16

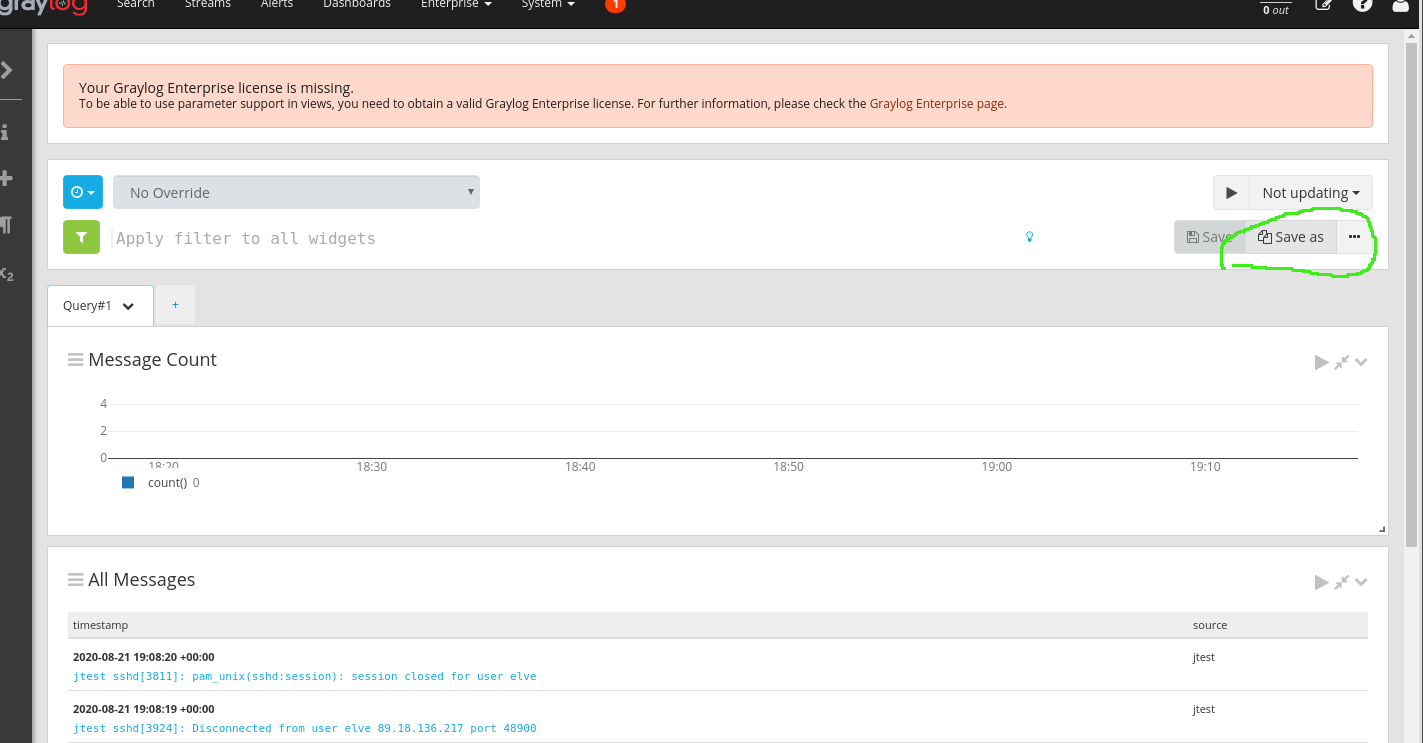
Эти настройки выборки можно сохранить в виде т.н. дашборда.

Делается это по кнопке на картинке



Нажал? В появившемся окне нужно нажать **Save As**

17:16

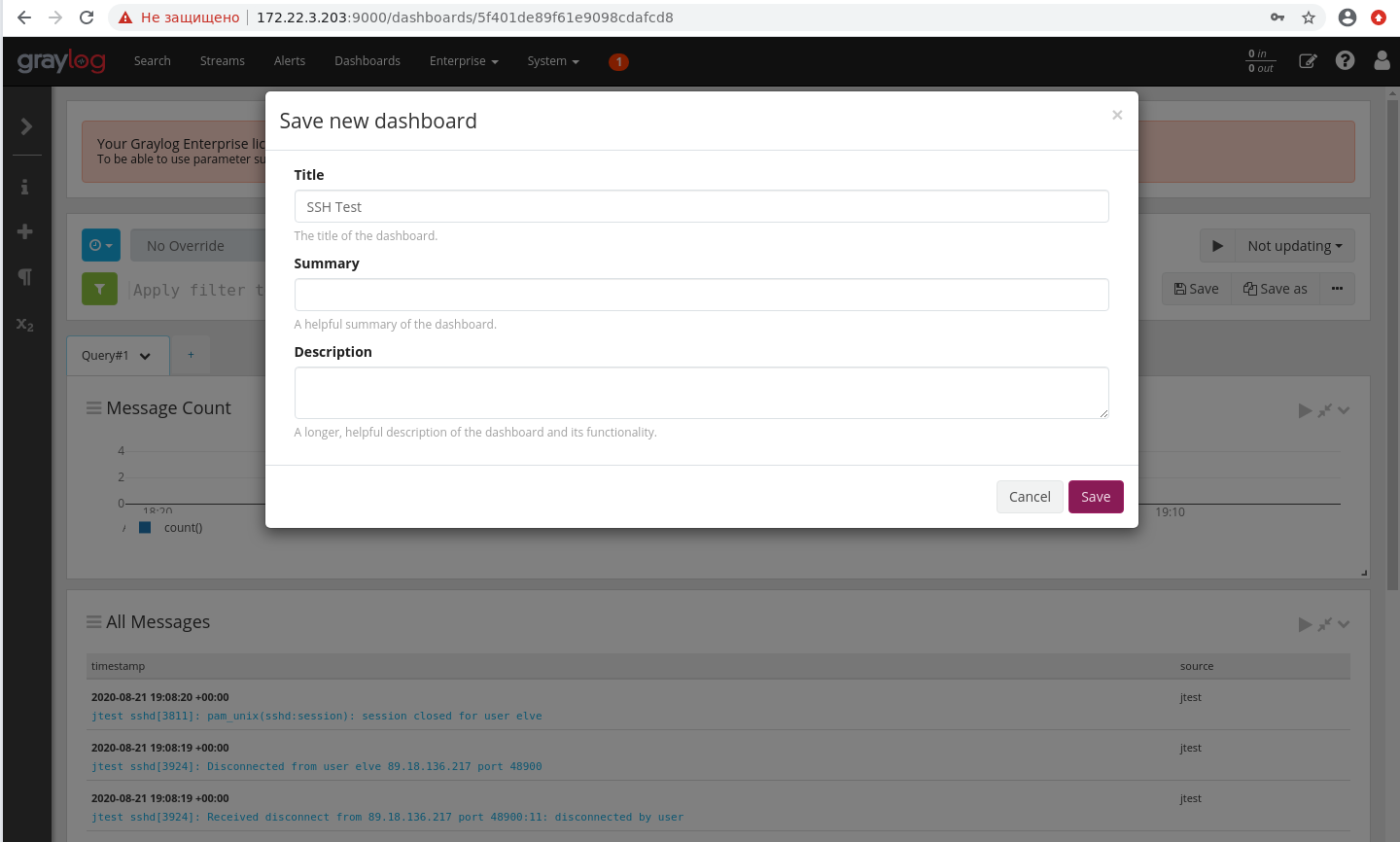


Дальше

17:16

Тебе будет предложено дать название новому дашборду и, если очень хочется, описание.

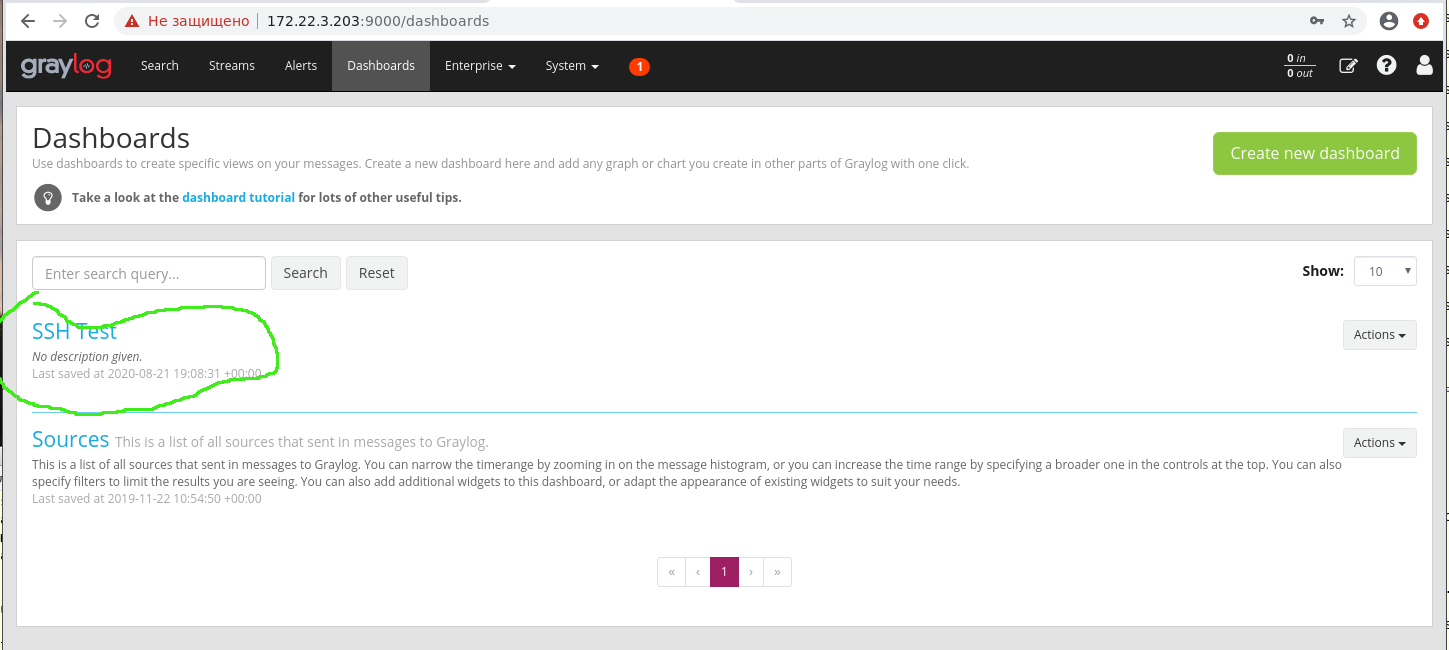
17:16



Дальше

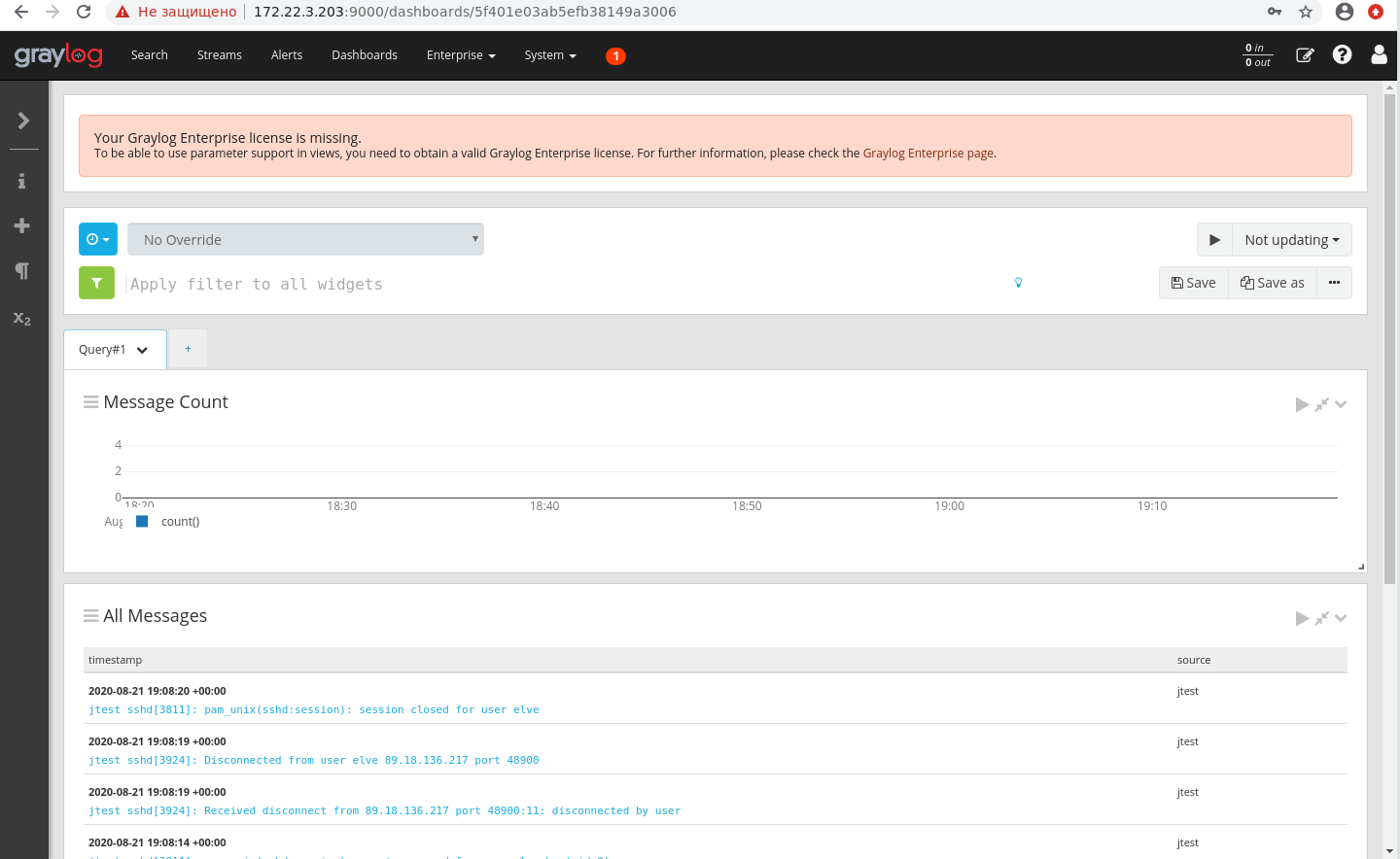
17:16

Так. А теперь иди в раздел **Dashboards**



Заходишь в него и видишь именно то, что в него и вкладывалось =)

17:16



Дальше

17:16

Это просто пример. Можно и выборки делать более интересными и осмысленными и комбинировать их с другими данными.

Со временем ты этому научишься. Но пока это уже достаточно мощный инструмент наблюдения за парком серверов.

К примеру можно в логе dhcp-сервера искать сообщения **DHCP** **NAK**, т.к. это аномалия.

Или в логах radius-сервера искать сообщения о двойной авторизации.

17:16

Согласись, удобно по нажатию одной кнопки получать всю эту информацию =). И при этом почти мгновенно в отличие от grep по гигабайтам логов.

Дальше

17:16

17:16

Итак. Ты получил в использование мощный инструмент. Многие его возможности тебе только придется освоить, но работать можно уже сейчас.

На этом я завершаю урок по **GrayLog**