


Graylog: централизованный сбор, хранение и анализ логов

 winitpro.ru/index.php/2024/04/11/graylog-sbor-analiz-logov

itpro

Graylog это полноценное open-source решение для централизованного сбора, хранения, визуализации, фильтрации и поиска логов, мониторинга и отправки оповещений. В Graylog можно отправлять логи и журналы событий с сотен сетевых устройств, будь то сервера Linux, Windows, сетевые устройства и оборудование. Graylog эта мощная платформа, которое может хранить терабайты логов и при этом позволяет поиск в логах выполняется практически моментально. В этой статье мы рассмотрим процесс развертывания стека Graylog и базовые возможности — это системы логирования.

Стек Graylog состоит из следующих компонентов:

- Сервер Graylog – веб интерфейс для визуализации и настройки
- MongoDB – используется для хранения метаданных
- Elasticsearch или его форк OpenSearch – для хранения и полнотекстового поиска в структурированных и неструктурированных логах
- Java (OpenJDK) – среда выполнения OpenSearch (ElasticSearch)

Для хранения журналов мы будем использовать стэк OpenSearch, который является бесплатным аналогом с открытым исходным кодом стеку ELK (Elasticsearch + Logstash + Kibana).

Установка стека Graylog на Linux

Инструкции по установке стека Graylog будут сильно отличаться от версии к версии. Поэтому рекомендуем вручную выбрать на сайте <https://go2docs.graylog.org> ваш дистрибутив Linux и версию Graylog. В нашем примере это Debian 12 и Graylog 5.2.

Graylog можно запустить через docker-compose, но в данном случае мы рассмотрим полноценное развертыванием всех компонентов.

Нам понадобятся:

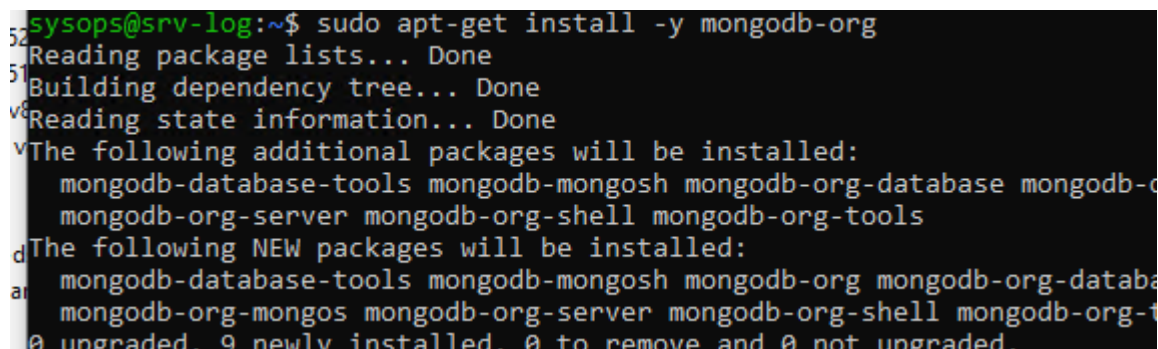
- OpenJDK 17
- OpenSearch 2.x (или Elasticsearch 7.10.2 – это единственная версия совместимая с Graylog 5.2)
- MongoDB 5.x или 6.x (использовать MongoDB 7 пока не рекомендуется)
- На сервере Graylog должно быть не менее 2GB RAM для небольшой инсталляции

Установка **MongoDB 6**:

```
$ sudo apt-get install gnupg curl
$ curl -fsSL https://www.mongodb.org/static/pgp/server-6.0.asc | sudo gpg -
o /usr/share/keyrings/mongodb-server-6.0.gpg --dearmor
$ echo "deb [ signed-by=/usr/share/keyrings/mongodb-server-6.0.gpg]
http://repo.mongodb.org/apt/debian bullseye/mongodb-org/6.0 main" | sudo
tee /etc/apt/sources.list.d/mongodb-org-6.0.list
$ sudo apt-get update
```

Теперь можно установить MongoDB:

```
$ sudo apt-get install -y mongodb-org
```



```
sysops@srv-log:~$ sudo apt-get install -y mongodb-org
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  mongodb-database-tools mongodb-mongosh mongodb-org-database mongodb-org-
  mongodb-org-server mongodb-org-shell mongodb-org-tools
The following NEW packages will be installed:
  mongodb-database-tools mongodb-mongosh mongodb-org mongodb-org-databa
  mongodb-org-mongos mongodb-org-server mongodb-org-shell mongodb-org-t
0 upgraded, 9 newly installed, 0 to remove and 0 not upgraded.
```

В моем случае для Debian 12 при установке mongodb появилась ошибка:

```
The following packages have unmet dependencies:
mongodb-org-mongos : Depends: libssl1.1 (>= 1.1.1) but it is not installable
mongodb-org-server : Depends: libssl1.1 (>= 1.1.1) but it is not installable
```

Пришлось установить:

```
$ sudo wget
http://archive.ubuntu.com/ubuntu/pool/main/o/openssl/libssl1.1_1.1.1f-
1ubuntu2_amd64.deb
$ sudo dpkg -i libssl1.1_1.1.1f-1ubuntu2_amd64.deb
```

Запустите сервис:

```
$ sudo systemctl daemon-reload
$ sudo systemctl enable mongod.service
$ sudo systemctl restart mongod.service
$ sudo systemctl --type=service --state=active | grep mongod
```

Затем переходим к развёртыванию OpenSearch:

```
$ sudo apt-get update && sudo apt-get -y install lsb-release ca-
certificates curl gnupg2
```

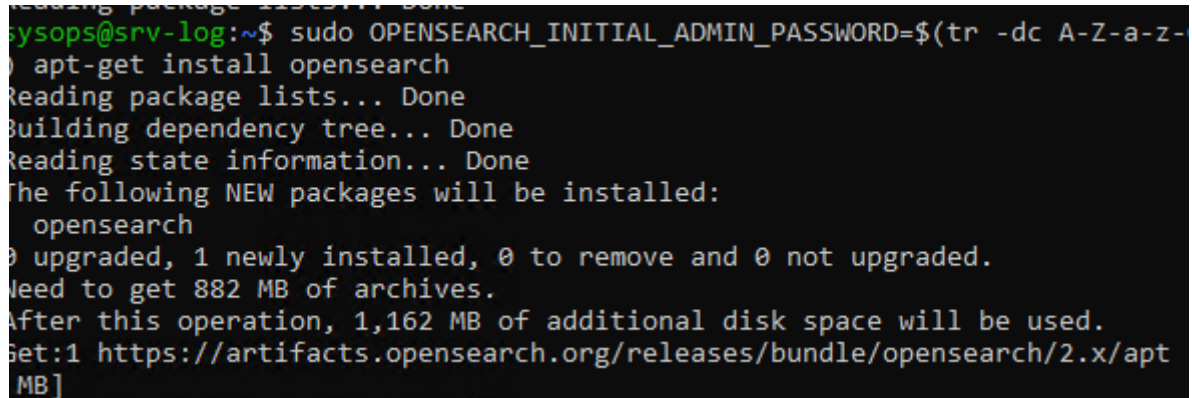
\$ Добавление репозитория:

```
$ curl -o- https://artifacts.opensearch.org/publickeys/opensearch.pgp |
sudo gpg --dearmor --batch --yes -o /usr/share/keyrings/opensearch-keyring
$ echo "deb [signed-by=/usr/share/keyrings/opensearch-keyring]
```

```
https://artifacts.opensearch.org/releases/bundle/opensearch/2.x/apt stable
main" | sudo tee /etc/apt/sources.list.d/opensearch-2.x.list
$ sudo apt update
```

Начиная с OpenSearch 2.12 при установке нужно сразу сгенерировать пароль администратора:

```
$ sudo OPENSEARCH_INITIAL_ADMIN_PASSWORD=$(tr -dc A-Z-a-z-0-9_@#%^-_=+ < /dev/urandom | head -c${1:-32}) apt-get install opensearch
```



```
sysops@srv-log:~$ sudo OPENSEARCH_INITIAL_ADMIN_PASSWORD=$(tr -dc A-Z-a-z-0-9_@#%^-_=+ < /dev/urandom | head -c${1:-32}) apt-get install opensearch
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  opensearch
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 882 MB of archives.
After this operation, 1,162 MB of additional disk space will be used.
Get:1 https://artifacts.opensearch.org/releases/bundle/opensearch/2.x/apt [MB]
```

Теперь нужно настроить параметры OpenSearch:

```
$ sudo nano /etc/opensearch/opensearch.yml
```

Для простейшей конфигурации из одной ноды достаточно настроить следующие параметры:

```
cluster.name: graylog
node.name: ${HOSTNAME}
path.data: /var/lib/opensearch
path.logs: /var/log/opensearch

discovery.type: single-node
network.host: 0.0.0.0
action.auto_create_index: false
plugins.security.disabled: true
indices.query.bool.max_clause_count: 32768
```

Настройте параметры SMTP сервера, через который вы будете отправлять email уведомления:

```
transport_email_enabled = true
transport_email_hostname = smtp.gmail.com
transport_email_port = 465
transport_email_use_auth = true
transport_email_use_tls = false
transport_email_use_ssl = true
transport_email_auth_username =
transport_email_auth_password =
transport_email_subject_prefix = [graylog]
transport_email_from_email =
transport_email_web_interface_url =
```

Затем изменить настройки Java:

```
$ sudo nano /etc/opensearch/jvm.options
```

В параметрах Xms и Xmx нужно указать сколько памяти может использовать виртуальная машина java. Здесь рекомендуется указать половину RAM сервера. Например, для хоста с 8 Гб, здесь нужно выделить 4 Гб:

```
-Xms4g
```

```
-Xmx4g
```

```
# Xms represents the initial size of total heap
# Xmx represents the maximum size of total heap

-Xms4g
-Xmx4g
#####
```

Измените параметры виртуальной памяти:

```
$ sudo sysctl -w vm.max_map_count=262144
```

```
$ sudo echo 'vm.max_map_count=262144' >> /etc/sysctl.conf
```

Запустите OpenSearch:

```
$ sudo systemctl enable --now opensearch
```

```
1[ | 0.7%] Load average: 1.6
2[ | 2.0%] Uptime: 01:00:21
3[ | 1.3%]
Mem[ | 4.65G/7.72G]
Swp[ | 0K/975M]

Main I/O
PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
6305 opensearch 20 0 7912M 4471M 26556 S 14.6 56.6 2:12.69 /usr/share
6470 opensearch 20 0 7912M 4471M 26556 S 14.6 56.6 0:12.72 /usr/share
```

Теперь нужно **установить сервер Graylog**. Есть две версии Graylog: бесплатная Graylog Open и enterprise версия Graylog Operations, доступная по подписке.

Для установки Graylog Open:

```
$ wget https://packages.graylog2.org/repo/packages/graylog-5.2-repository_latest.deb
```

```
$ sudo dpkg -i graylog-5.2-repository_latest.deb
```

```
$ sudo apt-get update && sudo apt-get install graylog-server
```

Сгенерируйте пароли для двух переменных password_secret и root_password_sha2, без которых Graylog не запустится.

Пароль password_secret должен содержать минимум 64 символа:

```
$ pwgen -N 1 -s 96
```

Затем нужно получить хэш пароля администратора Graylog. Следующая команда сгенерирует хэш введенного вами пароля:

```
$ echo -n "Enter Password: " && head -1 </dev/stdin | tr -d '\n' | sha256sum | cut -d" " -f1
```

Скопируйте полученные значения `password_secret` и `root_password_sha2` в файл `/etc/graylog/server/server.conf`.

В `http_bind_address` укажите IP адрес и порт, на котором будет запущен веб сервер Graylog.

Запустите сервер graylog:

```
$ sudo systemctl enable --now graylog-server
```

```
#http_bind_address = 127.0.0.1:9000
#http_bind_address = [2001:db8::1]:9000
http_bind_address = 0.0.0.0:9000_
#### HTTP publish URI
```

Пошаговая настройка Graylog

Теперь вы можете попробовать зайти в веб интерфейс Graylog под пользователем **admin** и пароль, хеш-сумму которого вы указали в файле конфигурации. Однако, при первом входе этот пароль не будет приниматься.

Если посмотреть логи сервера GrayLog, там вы обнаружите интересное сообщение:

```
$ cat /var/log/graylog-server/server.log
```

It seems you are starting Graylog for the first time. To set up a fresh install, a setup interface has been started. You must log in to it to perform the initial configuration and continue.

Initial configuration is accessible at 0.0.0.0:9000, with username 'admin' and password 'eDluAYfeaX'.

Try clicking on `http://admin::9000`

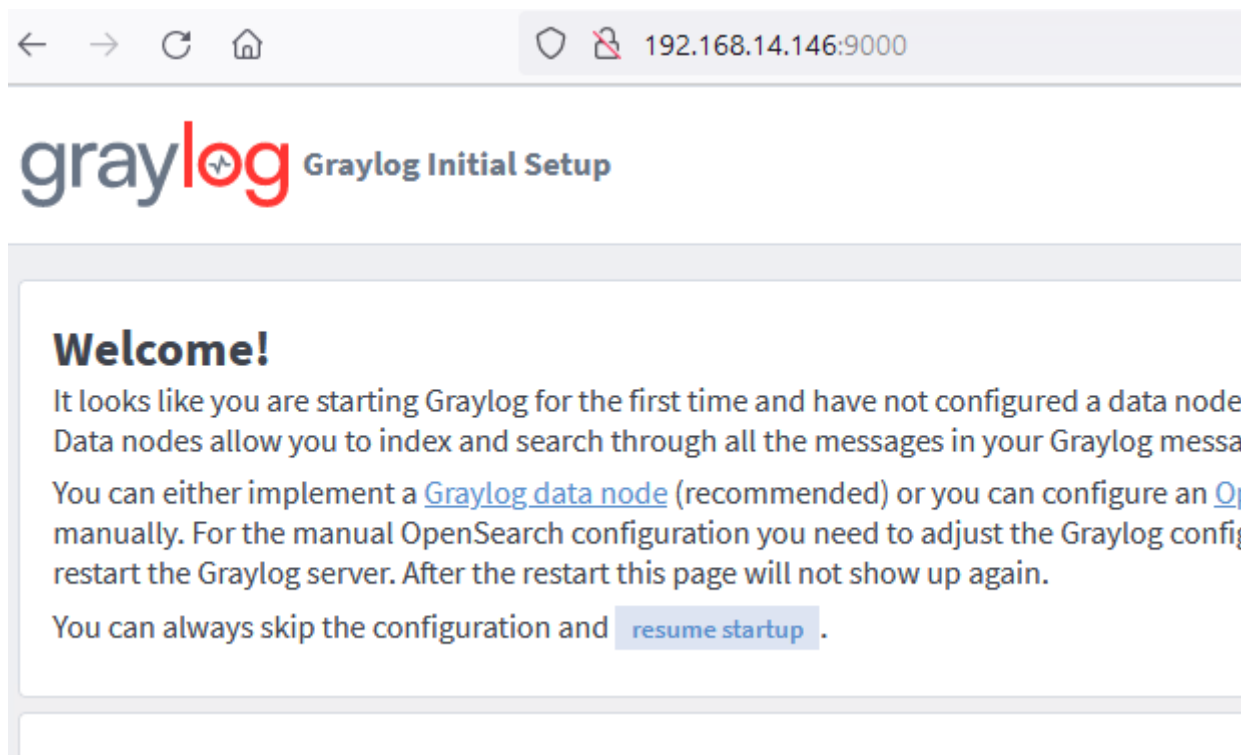
```
#####  
#####  
#####  
#####  
#####  
  
=====
```

t seems you are starting Graylog for the first time. To set up a fresh install, a setup interface has been started. You must log in to it to perform the initial configuration and continue.

Initial configuration is accessible at 0.0.0.0:9000, with username 'admin' and password 'eDluAYfeaX'. Try clicking on <http://admin:eDluAYfeaX@0.0.0.0:9000>

```
=====
```

В первый раз нужно зайти под временным паролем, который указан в лог файле. Воспользуйтесь простым мастером начальной конфигурации. Режим Graylog data node используется для настройки OpenSearch кластера из нескольких нод. Для простой конфигурации из одного сервера логов, этот этап можно пропустить.



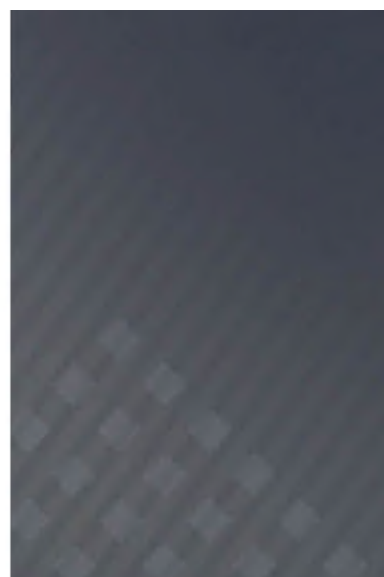
После этого вы сможете зайти в веб-интерфейс Graylog под пользователем **admin** и вашим паролем администратора, хэш которого вы указали в конфигурационном файле:

Welcome to Graylog

Username

Password

Sign in



После входа рекомендуем создать отдельного пользователя System-> User and Teams. Некоторые настройки встроенного администратора нельзя кастомизировать, поэтому лучше работать под отдельным пользователем. Назначьте пользователю роль admin и задайте email адрес.

Теперь нужно создать сборщики данных **Inputs**. Для каждого класса устройств лучше делать отдельный input (Linux сервера, сетевое оборудование, Windows хосты и т.д.).

Мы создадим input типа **Syslog UDP** для Linux. Нужно указать его название, и порт, на котором сервер будет принимать данные. Остальные настройки оставить по умолчанию.

Local inputs 1 configured

Linux Devices Syslog UDP (6614f4db92a371656f07b97f) **RUNNING**

On node ★ 17622ff2 / srv-log

```
allow_override_date: true
bind_address: 0.0.0.0
charset_name: UTF-8
expand_structured_data: false
force_rdns: false
number_worker_threads: 4
override_source: <empty>
port: 20514
recv_buffer_size: 262144
store_full_message: false
timezone: NotSet
```

Теперь перейдите в System -> Indices и создать отдельный индекс для класса Linux.

Нужно указать имя, описание и префикс (например `linux_indx`). Здесь можно также настроить сколько дней нужно хранить старые логи, и когда можно удалять старые индекс, а также максимальный размер индекса.

Linux Index Set

Index for Linux devices

Index prefix: linux_indx

Shards: 1

Replicas: 0

Field type refresh interval: 5 seconds

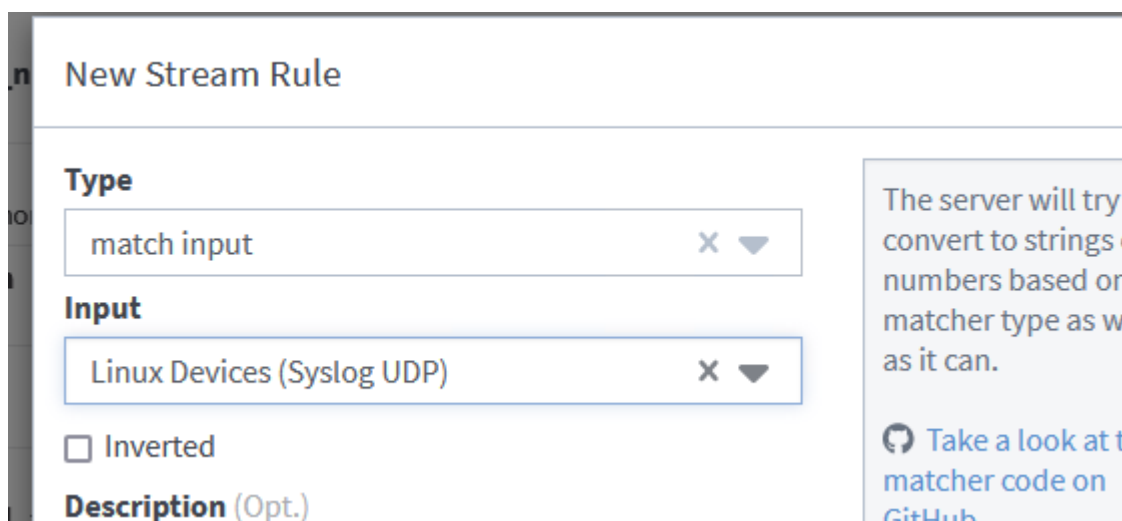
Index rotation strategy: |

Minimum lifetime: |

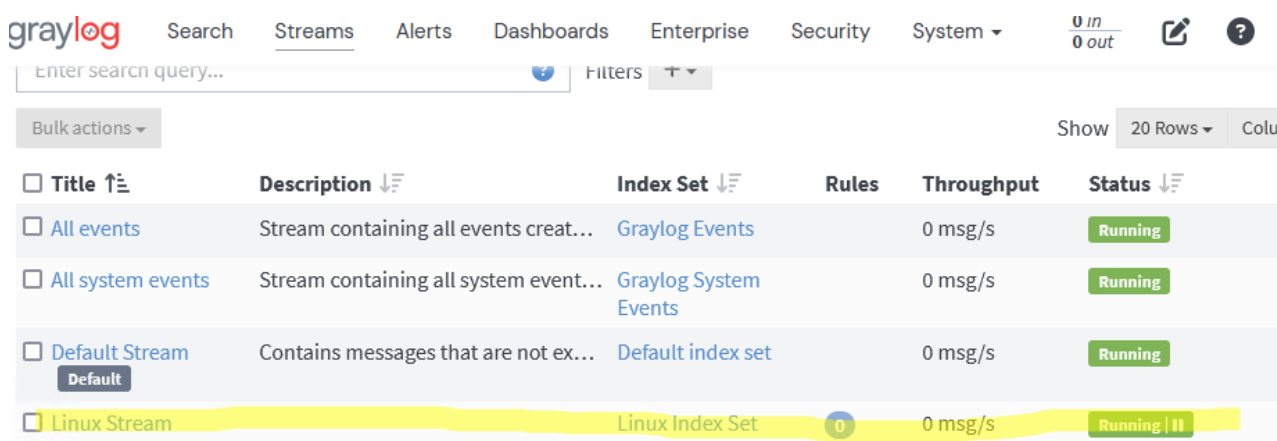
Maximum lifetime: |

Для каждого input лучше создать отдельный **Stream**. Так разные сообщений от разных классов устройства будут находится в разных индексах. Перейдите в Stream -> Create Stream -> укажите название потока и выберите индекс, который нужно использовать.

В настройках Stream добавьте новое правило. Правило определяют какие логи нужно отнести к этому потоку. В нашем случае выбираем match input -> выберите ваш Linux Input.



После этого запустите stream.



Title	Description	Index Set	Rules	Throughput	Status
All events	Stream containing all events creat...	Graylog Events		0 msg/s	Running
All system events	Stream containing all system event...	Graylog System Events		0 msg/s	Running
Default Stream	Contains messages that are not ex...	Default index set		0 msg/s	Running
Linux Stream		Linux Index Set	0	0 msg/s	Running

Настройка отправки логов с клиентов в Graylog

Теперь можно настроить отправку логов с ваших устройств в Graylog. Graylog позволяет получать данные из различных источников: Filebeat, Winlogbeat, Nxlog, Syslog, Rsyslog и т.д.

Для Linux серверов можно использовать rsyslog.

```
$ sudo apt install rsyslog
```

```
sysops@srv-ubun01:~$ sudo apt install rsyslog
Reading package lists... Done
Building dependency tree
Reading state information... Done
rsyslog is already the newest version (8.2001.0-1ubuntu1)
rsyslog set to manually installed.
```

```
$ sudo systemctl status rsyslog
```


После того, как служба rsyslog запущена, нужно настроить какие логи нужно отправлять в Graylog.

```
$ sudo nano /etc/rsyslog.d/60-graylog.conf
```

Добавьте в файл строку:

```
*.*@192.168.14.146:20514;RSYSLOG_SyslogProtocol23Format
```

В данном примере мы будем отправлять на Graylog сервер (192.168.14.146) на порт созданного вами Input (20514) все логи в формате Syslog (в реальной среде можно настроить отправку только определенных журналов).

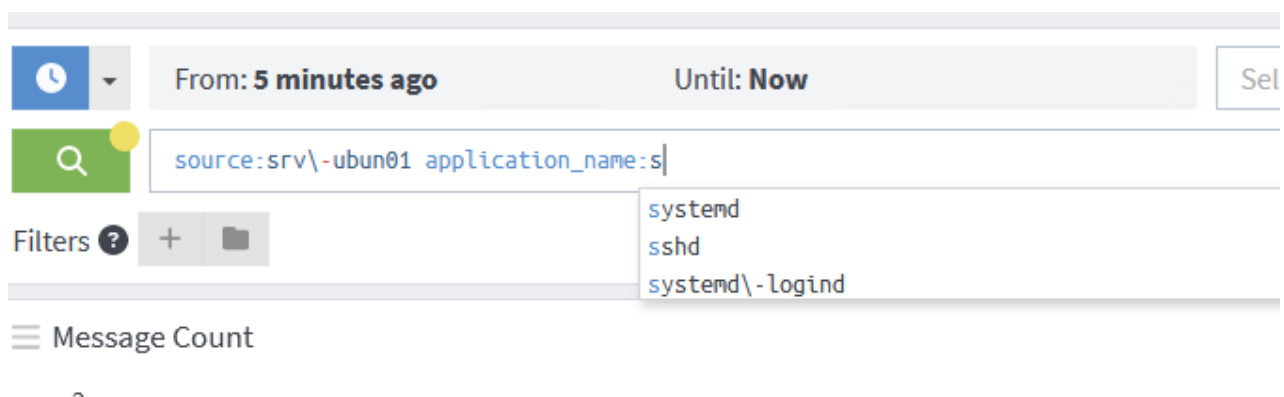
Перезапустите rsyslog:

```
$ sudo systemctl restart rsyslog
```

Просмотр, фильтрации и анализ логов в GrayLog

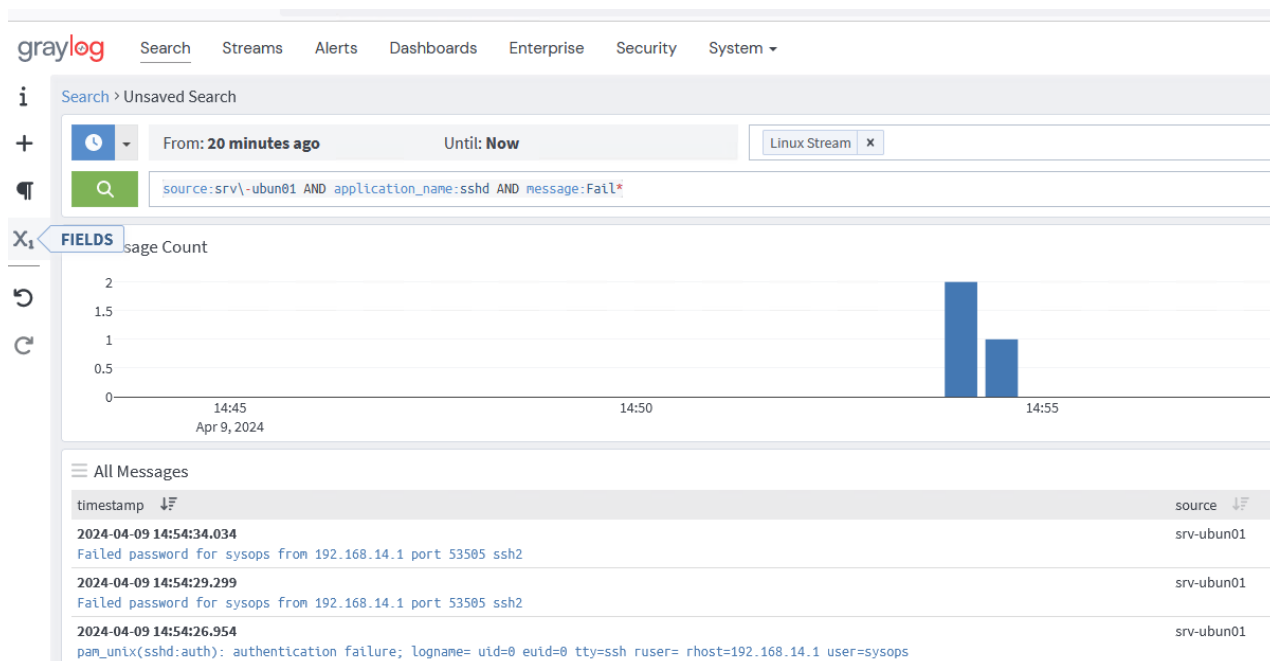
Теперь перейдите на вкладку Search Graylog, выберите в списке потоков Linux и вы увидите все события от вашего сервера, которые были получены за последние 5 минут (можно изменить диапазон).

С помощью простых фильтров можно найти определенные события. Поисковая строка Graylog интерактивная. Вы выбираете различные свойства событий и в поисковой строке выбираете из предложенных вариантов.



Например, для поиска всех событий неудачных попыток SSH подключений к серверу, настройте следующий поисковый фильтр:

```
source:srv\ -ubun01 AND application_name:sshd AND message:Fail*
```



В данном случае мы явно указываем что ищем события, которые удовлетворяют всем трем условиям (параметр **AND**). Если не указывать AND, graylog подразумевает что вы ищите события в режиме **OR** .

В таблице останутся события, которые соответствуют вашим критериям поиска. Вы можете развернуть и изучить их. Поисковые фильтры Graylog довольно простые и интуитивно понятны. Вы всегда можете развернуть любой событие, просмотреть его поля и использовать их значения для фильтрации и поиска событий.

В Graylog можно создать различные Dashboard-ы, в которых можно выводить информацию об интересующих вас событиях (количество событий, хосты, сгруппировать элементы, добавить графики или карты). Для кастомизации dashboard используются виджеты.

Dashboards > SSH Dashboard ☆

CREATE From: 8 hours ago Until: Now

application_name:sshd AND message:Fail*

Page#1 +

SSH logon sources

source	count(source)
srv-log	10
srv-ubun01	6

Failed SSH logons

20

Global Override: 8 hours ago - Now

Failed SSH Logon Table

timestamp	source
2024-04-09 16:59:07.737	srv-log
PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.1 user=sysops	
2024-04-09 16:59:07.737	srv-log
PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.1 user=sysops	
2024-04-09 16:59:07.725	srv-log
Failed password for sysops from 192.168.14.1 port 54271 ssh2	
2024-04-09 16:59:07.725	srv-log
Failed password for sysops from 192.168.14.1 port 54271 ssh2	
2024-04-09 16:59:06.498	srv-log
Failed password for sysops from 192.168.14.1 port 54271 ssh2	
2024-04-09 16:59:06.498	srv-log

Настройка оповещений в Graylog

Вы можете настроить автоматическую отправку оповещений из Graylog при появлении определенных событий. Например, я хочу, чтобы Graylog отправлял мне на почту письмо, когда кто-то зашел на один серверов по SSH.

Перейдите в **Alerts** -> **Alerts and Events**. На вкладке Notification добавьте email адреса, на которые нужно высылать письма.

В Graylog есть встроенные шаблоны для отправки алертов в MS Teams и Slack. С помощью плагинов можно настроить отправку сообщений из Graylog в Telegram.

Затем на Event Definition нужно создать шаблон для поиска событий, о которых нужно уведомлять. Для отслеживания SSH входов на Linux хосты нужно выбрать соответствующий Stream и указать поисковый запрос:

`application_name:sshd AND message:Accepted password*`

В правом столбце появится список событий, которые соответствуют вашим критериям. Проверьте, что найдены все события. Если нет, отредактируйте поисковый запрос.

Event Condition

Configure how Graylog should create Events of this kind. You can later use those Events as input on other Conditions, making it possible to build powerful Conditions based on others.

Condition Type

Filter & Aggregation

Choose the type of Condition for this Event.

Filter

Add information to filter the log messages that are relevant for this Event Definition.

Search Query

application_name:sshd AND message:Accepted password*

Search query that Messages should match. You can use the same syntax as in the Search page, including declaring Query Parameters from Lookup Tables by using the `$newParameter$` syntax.

Streams (Optional)

Linux Stream

Select streams the search should include. Searches in all streams if empty.

Search within the last

5 hours

Execute search every

5 minutes

Available Conditions

Filter & Aggregation

Create Events from log messages by filtering them and (optionally) aggregating them to match a given condition. These Events can be used as input for a Correlation Rule

How many Events will Filter & Aggregation create?

Filter Preview

Timestamp	Message
2024-04-09T11:24:59.707Z	Accepted password for sysops fr 192.168.14.1 port 54017 ssh2
2024-04-09T11:19:04.545Z	Accepted password for sysops fr 192.168.14.1 port 53916 ssh2
2024-04-09T09:58:17.093Z	Accepted password for sysops fr 192.168.14.1 port 53520 ssh2

Осталось выбрать тип уведомления -> email. И Graylog начнет высылать вам оповещение при появлении в логах определенного события.

В этой статье мы рассмотрели базовые вопросы развертывания и использования системы сбора и анализа логов Graylog. В следующей статье мы рассмотрим, как использовать Graylog для централизованного сбора и поиска в логах от серверов Windows.

1.



Иван 14.05.2024

При установке opensearch вылетела ошибка.

Обрабатываются триггеры для libc-bin (2.36-9+deb12u7) ...

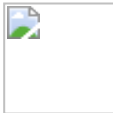
При обработке следующих пакетов произошли ошибки:

opensearch

E: Sub-process /usr/bin/dpkg returned an error code (1)

Ответить

o



Иван 14.05.2024

С первой проблемой разобрался но не стартует все равно жаль.

```
sudo systemctl enable --now opensearch
Synchronizing state of opensearch.service with SysV service script
with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable opensearch
Job for opensearch.service failed because the control process
exited with error code.
See "systemctl status opensearch.service" and "journalctl -xeu
opensearch.service" for details.
```

Ответить



Иван 14.05.2024

С первой проблемой разобрался но не стартует все равно жаль.

```
sudo systemctl enable --now opensearch
Synchronizing state of opensearch.service with SysV service script
with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable opensearch
Job for opensearch.service failed because the control process
exited with error code.
See "systemctl status opensearch.service" and "journalctl -xeu
opensearch.service" for details.
```

Ответить



itpro 14.05.2024

Выполните `journalctl -xeu opensearch.service` — там в логе могут быть прям подробные описания проблемы

Ответить



Иван 15.05.2024

Subject: Unit process exited

Defined-By: systemd

Support: <https://www.debian.org/support>

An ExecStart= process belonging to unit opensearch.service has exited.

The process' exit code is 'exited' and its exit status is 1.

мая 15 11:34:43 graylog systemd[1]: opensearch.service: Failed with result 'exit-code'.

Subject: Unit failed

Defined-By: systemd

Support: <https://www.debian.org/support>

The unit opensearch.service has entered the 'failed' state with result 'exit-code'.

мая 15 11:34:43 graylog systemd[1]: Failed to start opensearch.service — OpenSearch.

Subject: Ошибка юнита opensearch.service

Defined-By: systemd

Support: <https://www.debian.org/support>

Произошел сбой юнита opensearch.service.

Результат: failed.

мая 15 11:34:43 graylog systemd[1]: opensearch.service: Consumed 4.874s CPU time.

Subject: Потребленные юнитом ресурсы

Defined-By: systemd

Support: <https://www.debian.org/support>

Юнит opensearch.service завершен. Приводится статистика по потребленным им ресурсам

Не очень понятно по этому логу в чем проблема, и еще когда ставишь opensearch, он ставиться с демо конфигом, его комментим и можно взять ваш пример? Или его комментить не нужно?

В общем переставил раза три виртуалку на этом месте, просто не запускается opensearch, debian последний дальше все по ману.

Ответить



Arius 09.12.2024

В конфиге opensearch.yml по умолчанию уже есть значения:

path.data: /var/lib/opensearch

path.logs: /var/log/opensearch

Их нужно закомментировать

2.



Иван 15.05.2024

В общем как только я добавляю в конфиг вот это, или просто почтовые настройки, opensearch падает и не поднимается.

discovery.type: single-node

network.host: 0.0.0.0

transport_email_enabled = true

transport_email_hostname = smtp.gmail.com

transport_email_port = 465

transport_email_use_auth = true

transport_email_use_tls = false

transport_email_use_ssl = true

transport_email_auth_username =

transport_email_auth_password =

transport_email_subject_prefix = [graylog]

transport_email_from_email =

transport_email_web_interface_url =

Ответить



Ivan 17.07.2024

Настройки почты правятся тут /etc/graylog/server/server.conf

Ответить

3.



Илья 07.06.2024

Будет ли продолжение по настройке дашбордов?

Ответить

4.



Антон 22.08.2024

systemctl enable —now graylog-server прошу исправить systemctl enable —now graylog-server (2 типе)

поскольку чайник — изрядно потоптался по граблям 😊

Ответить



itpro 06.09.2024

Пофиксено)

Ответить

5.



Arius 09.12.2024

Не стартует база данных:

journalctl -u mongod.service

дек 09 15:45:52 graylog systemd[1]: Started mongod.service — MongoDB Database Server.

дек 09 15:45:52 graylog systemd[1]: mongod.service: Main process exited, code=killed, status=4/ILL

дек 09 15:45:52 graylog systemd[1]: mongod.service: Failed with result 'signal'.

При чем делал пару месяцев назад по этой же статье. Проблем не было Debian 12.8

Ответить

6.



Arius 09.12.2024

Поставил rsyslog. Так journalctl неинформативен. Теперь вот такое:

2024-12-09T15:49:40.034713+03:00 graylog systemd[1]: Started mongod.service
— MongoDB Database Server.

2024-12-09T15:49:40.048260+03:00 graylog systemd[1]: mongod.service: Main
process exited, code=killed, status=4/ILL

2024-12-09T15:49:40.048412+03:00 graylog systemd[1]: mongod.service: Failed
with result 'signal'.

2024-12-09T15:49:40.049851+03:00 graylog kernel: [465.222800] traps:
mongod[3886] trap invalid opcode ip:55ad3bd24eca sp:7fff93954f00 error:0 in
mongod[55ad36d2e000+630b000]

Ответить



Arius 09.12.2024

Погуглил, проблема в прохтох и решается она заменой ЦПУ на x86-64-v3

Ответить