

Министерство образования и науки Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»  
(МОСКОВСКИЙ ПОЛИТЕХ)**

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ  
КАФЕДРА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

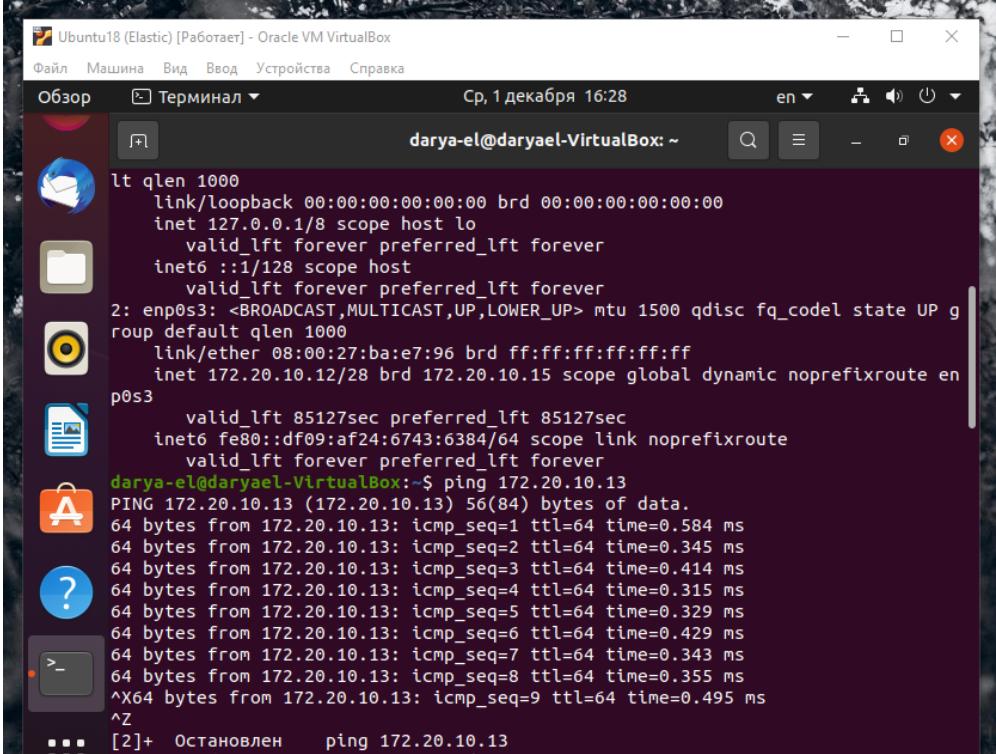
Практика построения центров мониторинга и управления инцидентами  
ИБ

**Отчет по лабораторной работе №3  
ELK**

Выполнила студентка 5 курса группы 171-341  
Решетникова Дарья

Москва 2021 г.

Для выполнения лабораторной работы нам потребуется 2 виртуальные машины, расположенных в одной локальной сети. Поэтому сперва проверим их доступность друг для друга. На первой виртуальной машине будет установлен Elasticsearch. На второй Elasticsearch, Kibana и Logstash. Команда ping с 1 ВМ на 2 ВМ.



Ubuntu18 (Elastic) [Работает] - Oracle VM VirtualBox

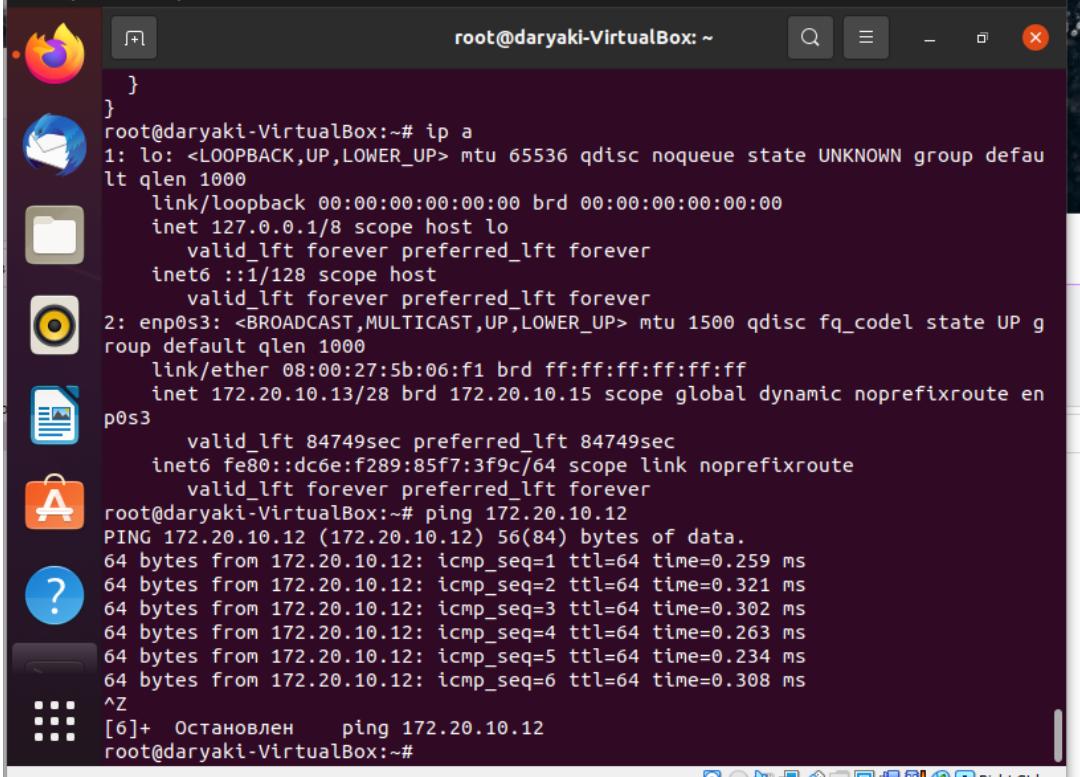
Файл Машина Вид Ввод Устройства Справка

Обзор Терминал Ср, 1 декабря 16:28 en

darya-el@daryael-VirtualBox: ~

```
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ba:e7:96 brd ff:ff:ff:ff:ff:ff
    inet 172.20.10.12/28 brd 172.20.10.15 scope global dynamic noprefixroute enp0s3
        valid_lft 85127sec preferred_lft 85127sec
        inet6 fe80::df09:af24:6743:6384/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
darya-el@daryael-VirtualBox:~$ ping 172.20.10.13
PING 172.20.10.13 (172.20.10.13) 56(84) bytes of data.
64 bytes from 172.20.10.13: icmp_seq=1 ttl=64 time=0.584 ms
64 bytes from 172.20.10.13: icmp_seq=2 ttl=64 time=0.345 ms
64 bytes from 172.20.10.13: icmp_seq=3 ttl=64 time=0.414 ms
64 bytes from 172.20.10.13: icmp_seq=4 ttl=64 time=0.315 ms
64 bytes from 172.20.10.13: icmp_seq=5 ttl=64 time=0.329 ms
64 bytes from 172.20.10.13: icmp_seq=6 ttl=64 time=0.429 ms
64 bytes from 172.20.10.13: icmp_seq=7 ttl=64 time=0.343 ms
64 bytes from 172.20.10.13: icmp_seq=8 ttl=64 time=0.355 ms
^X64 bytes from 172.20.10.13: icmp_seq=9 ttl=64 time=0.495 ms
^Z
[2]+ Остановлен ping 172.20.10.13
```

И обратный ping:



root@daryaki-VirtualBox: ~

```
}
```

```
root@daryaki-VirtualBox:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:5b:06:f1 brd ff:ff:ff:ff:ff:ff
    inet 172.20.10.13/28 brd 172.20.10.15 scope global dynamic noprefixroute enp0s3
        valid_lft 84749sec preferred_lft 84749sec
        inet6 fe80::dc6e:f289:85f7:3f9c/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
root@daryaki-VirtualBox:~# ping 172.20.10.12
PING 172.20.10.12 (172.20.10.12) 56(84) bytes of data.
64 bytes from 172.20.10.12: icmp_seq=1 ttl=64 time=0.259 ms
64 bytes from 172.20.10.12: icmp_seq=2 ttl=64 time=0.321 ms
64 bytes from 172.20.10.12: icmp_seq=3 ttl=64 time=0.302 ms
64 bytes from 172.20.10.12: icmp_seq=4 ttl=64 time=0.263 ms
64 bytes from 172.20.10.12: icmp_seq=5 ttl=64 time=0.234 ms
64 bytes from 172.20.10.12: icmp_seq=6 ttl=64 time=0.308 ms
^Z
[6]+ Остановлен ping 172.20.10.12
root@daryaki-VirtualBox:~#
```

Скачиваем и устанавливаем Elasticsearch из Deb пакетов, но сначала установим HTTP-веб-сервер с открытым исходным кодом nginx и проверим его работу. Он потребуется для функционирования Elasticsearch.

```
root@daryaki-VirtualBox:~# apt-get install nginx -y
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
  libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter
  libnginx-mod-mail libnginx-mod-stream nginx-common nginx-core
Предлагаемые пакеты:
  fcgiwrap nginx-doc

root@daryael-VirtualBox:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ba:e7:96 brd ff:ff:ff:ff:ff:ff
        inet 172.20.10.12/28 brd 172.20.10.15 scope global dynamic noprefixroute enp0s3
            valid_lft 85495sec preferred_lft 85495sec
            inet6 fe80::df09:af24:6743:6384/64 scope link noprefixroute
                valid_lft forever preferred_lft forever
root@daryael-VirtualBox:~#
```

▲ 172.20.10.12

## Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](http://nginx.org).  
Commercial support is available at [nginx.com](http://nginx.com).

*Thank you for using nginx.*

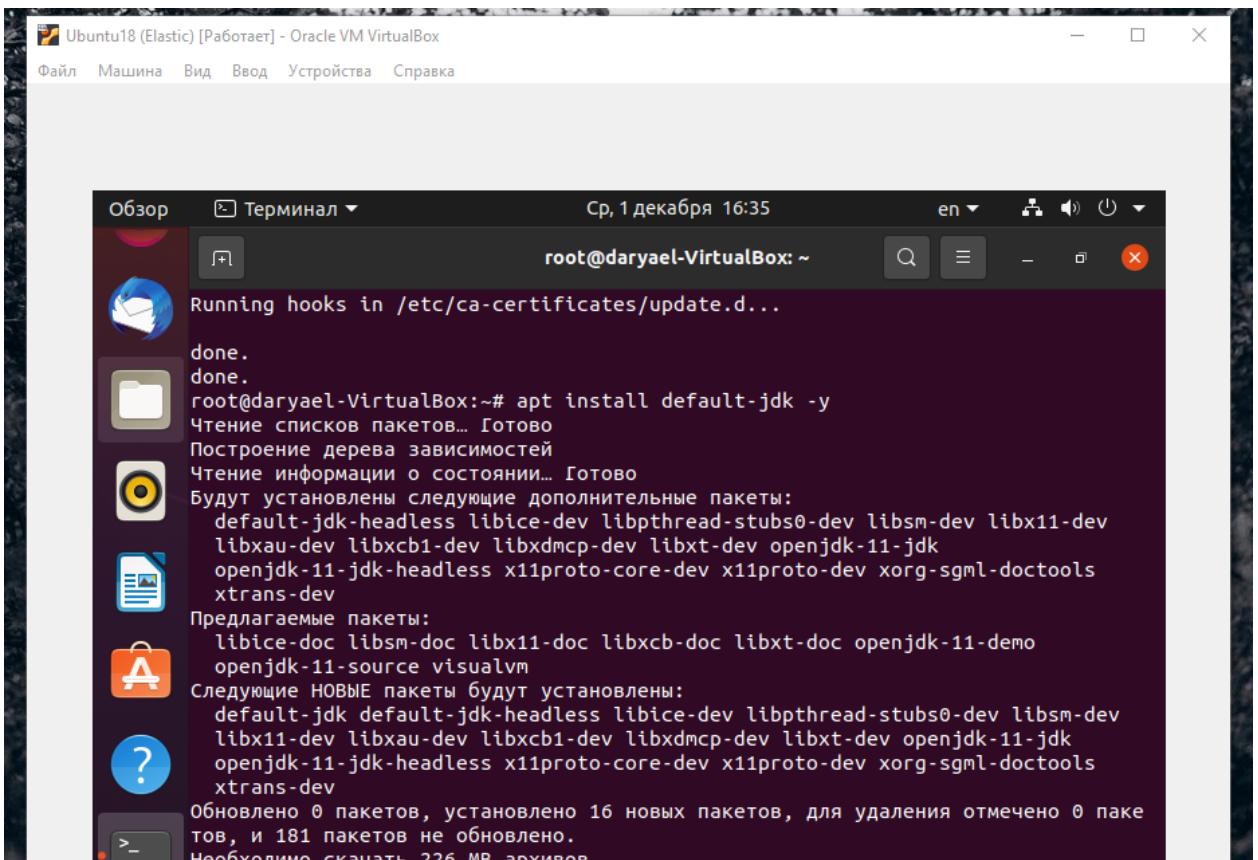
Обновим список пакетов:

```
root@daryael-VirtualBox:~# sudo apt update
Пол:1 http://ru.archive.ubuntu.com/ubuntu focal InRelease [265 kB]
Пол:2 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Пол:3 http://ru.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Пол:4 http://ru.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Пол:5 http://ru.archive.ubuntu.com/ubuntu focal/main amd64 Packages [970 kB]
Пол:6 http://ru.archive.ubuntu.com/ubuntu focal/main i386 Packages [718 kB]
Пол:7 http://security.ubuntu.com/ubuntu focal-security/main i386 Packages [343 kB]
Пол:8 http://ru.archive.ubuntu.com/ubuntu focal/main Translation-ru [345 kB]
Пол:9 http://ru.archive.ubuntu.com/ubuntu focal/main Translation-en [506 kB]
Пол:10 http://ru.archive.ubuntu.com/ubuntu focal/main amd64 DEP-11 Metadata [49 kB]
Пол:11 http://ru.archive.ubuntu.com/ubuntu focal/main DEP-11 48x48 Icons [98,4 kB]
Пол:12 http://ru.archive.ubuntu.com/ubuntu focal/main DEP-11 64x64 Icons [163 kB]
Пол:13 http://ru.archive.ubuntu.com/ubuntu focal/main DEP-11 64x64@2 Icons [15,8 kB]
Пол:14 http://ru.archive.ubuntu.com/ubuntu focal/main amd64 c-n-f Metadata [29,5 kB]
```

Установим среду Java Runtime Environment (JRE). Она позволяет запускать практически любое программное обеспечение Java.

```
root@daryael-VirtualBox:~# apt install default-jre -y
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
  ca-certificates-java default-jre-headless fonts-dejavu-extra java-common
  libatk-wrapper-java libatk-wrapper-java-jni openjdk-11-jre
  openjdk-11-jre-headless
Предлагаемые пакеты:
  fonts-ipafont-gothic fonts-ipafont-mincho fonts-wqy-microhei
  | fonts-wqy-zenhei
Следующие НОВЫЕ пакеты будут установлены:
  ca-certificates-java default-jre default-jre-headless fonts-dejavu-extra
  java-common libatk-wrapper-java libatk-wrapper-java-jni openjdk-11-jre
  openjdk-11-jre-headless
Обновлено 0 пакетов, установлено 9 новых пакетов, для удаления отмечено 0 пакетов, и 181 пакетов не обновлено.
Необходимо скачать 39,5 MB архивов.
После данной операции объём занятого дискового пространства возрастёт на 179 MB .
Пол:1 http://ru.archive.ubuntu.com/ubuntu focal/main amd64 java-common all 0.72 [6 816 kB]
Пол:2 http://ru.archive.ubuntu.com/ubuntu focal-updates/main amd64 openjdk-11-jre-headless amd64 11.0.11+9-0ubuntu2~20.04 [37,2 MB]
Пол:3 http://ru.archive.ubuntu.com/ubuntu focal/main amd64 default-jre-headless amd64 2:1.11-72 Г3 192 kB
```

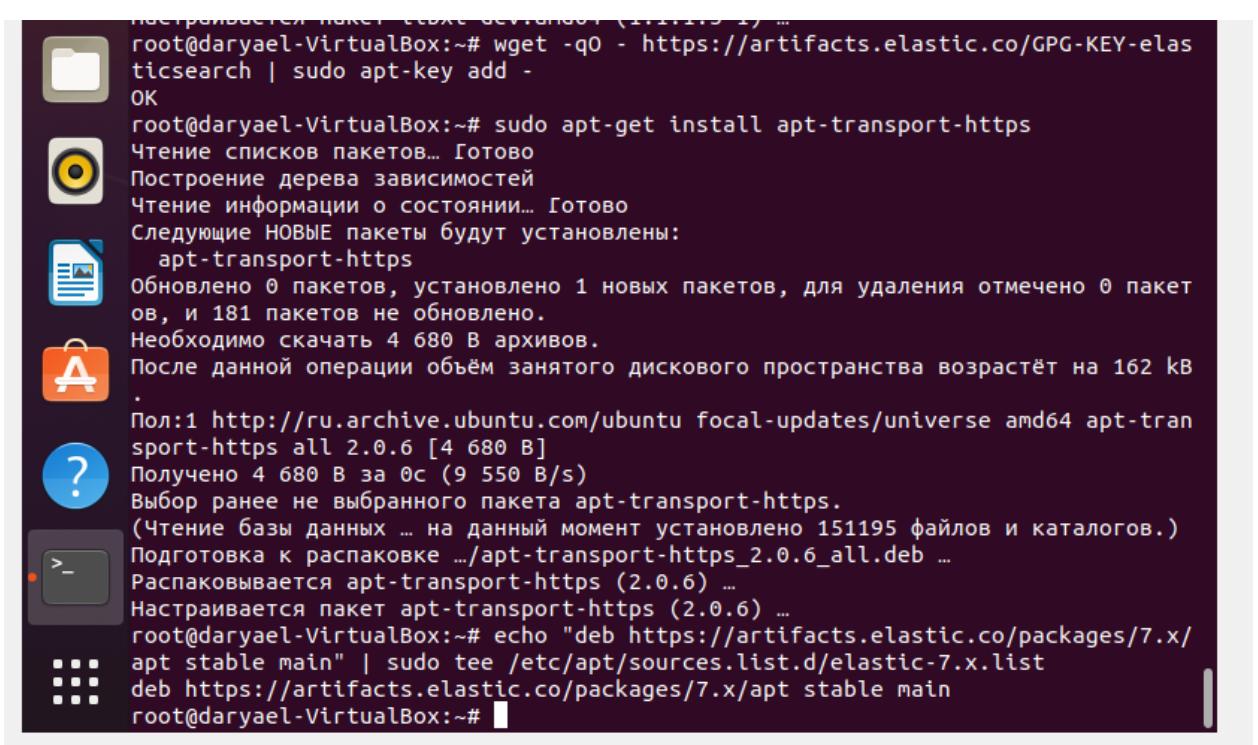
А также для компиляции и запуска некоторых специфических программ на базе Java в дополнение к JRE потребуется комплект разработчика Java Development Kit (JDK):



```
Ubuntu18 (Elastic) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка

Обзор Терминал
Ср, 1 декабря 16:35
en
Running hooks in /etc/ca-certificates/update.d...
done.
done.
root@daryael-VirtualBox:~# apt install default-jdk -y
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
  default-jdk-headless libice-dev libpthread-stubs0-dev libsm-dev libx11-dev
  libxau-dev libxcb1-dev libxdmcp-dev libxt-dev openjdk-11-jdk
  openjdk-11-jdk-headless x11proto-core-dev x11proto-dev xorg-sgml-doctools
  xtrans-dev
Предлагаемые пакеты:
  libice-doc libsm-doc libx11-doc libxcb-doc libxt-doc openjdk-11-demo
  openjdk-11-source visualvm
Следующие НОВЫЕ пакеты будут установлены:
  default-jdk default-jdk-headless libice-dev libpthread-stubs0-dev libsm-dev
  libx11-dev libxau-dev libxcb1-dev libxdmcp-dev libxt-dev openjdk-11-jdk
  openjdk-11-jdk-headless x11proto-core-dev x11proto-dev xorg-sgml-doctools
  xtrans-dev
Обновлено 0 пакетов, установлено 16 новых пакетов, для удаления отмечено 0 пакетов, и 181 пакетов не обновлено.
Необходимо скачать 226 МБ архивов.
```

Приступим непосредственно к установке Elasticsearch.



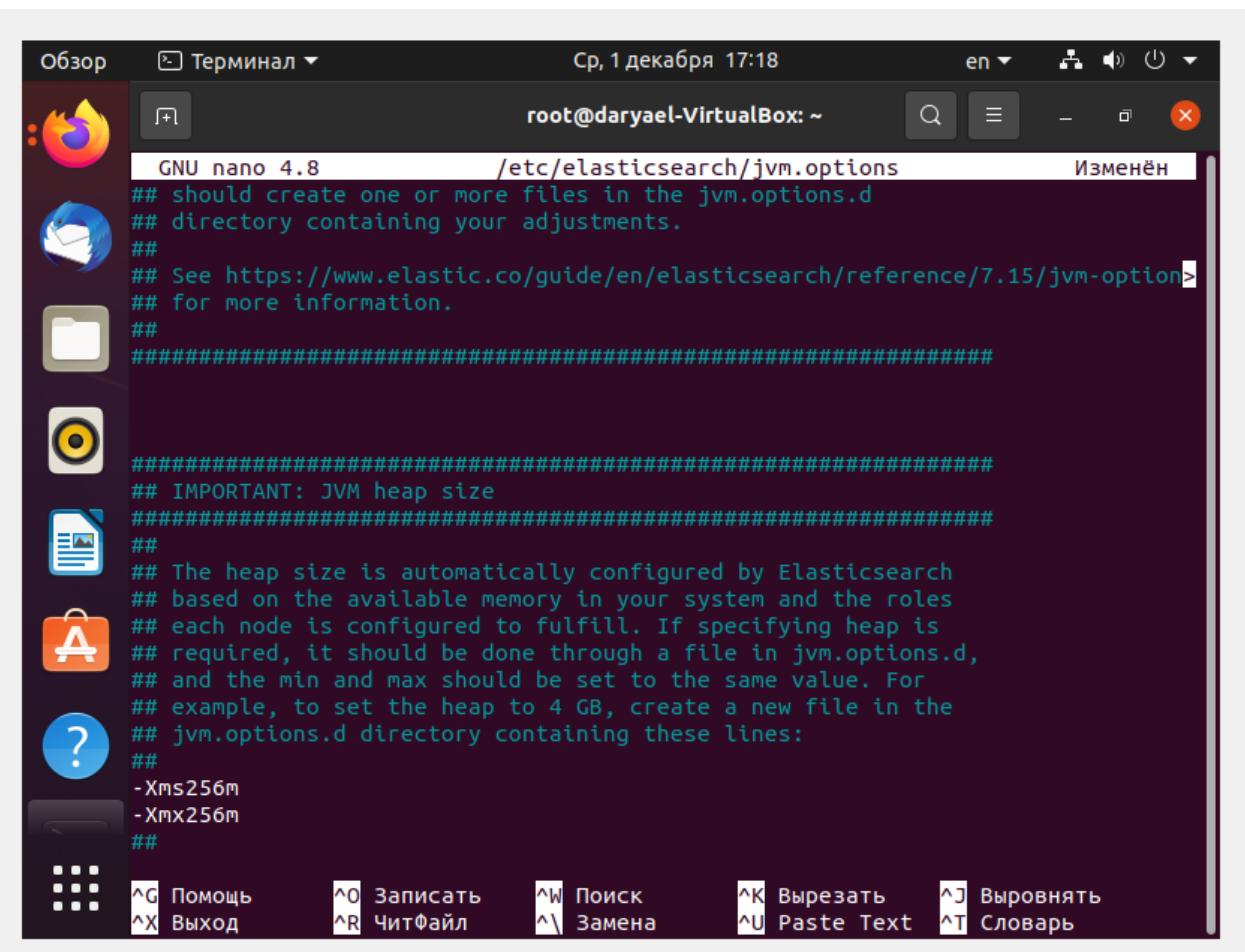
```
получен пакет apt-transport-https (2.0.6-1) ...
root@daryael-VirtualBox:~# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
OK
root@daryael-VirtualBox:~# sudo apt-get install apt-transport-https
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Следующие НОВЫЕ пакеты будут установлены:
  apt-transport-https
Обновлено 0 пакетов, установлено 1 новых пакетов, для удаления отмечено 0 пакетов, и 181 пакетов не обновлено.
Необходимо скачать 4 680 В архивов.
После данной операции объём занятого дискового пространства возрастёт на 162 kB .
.
Пол:1 http://ru.archive.ubuntu.com/ubuntu focal-updates/universe amd64 apt-transport-https all 2.0.6 [4 680 B]
Получено 4 680 В за 0с (9 550 B/s)
Выбор ранее не выбранного пакета apt-transport-https.
(Чтение базы данных ... на данный момент установлено 151195 файлов и каталогов.)
Подготовка к распаковке .../apt-transport-https_2.0.6_all.deb ...
Распаковывается apt-transport-https (2.0.6) ...
Настраивается пакет apt-transport-https (2.0.6) ...
root@daryael-VirtualBox:~# echo "deb https://artifacts.elastic.co/packages/7.x/
apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list
deb https://artifacts.elastic.co/packages/7.x/apt stable main
root@daryael-VirtualBox:~#
```

```
deb http://artifacts.elastic.co/packages/7.x/apt stable main
root@daryael-VirtualBox:~# sudo apt-get update && sudo apt-get install elasticsearch
Сущ:1 http://ru.archive.ubuntu.com/ubuntu focal InRelease
Сущ:2 http://ru.archive.ubuntu.com/ubuntu focal-updates InRelease
Сущ:3 http://ru.archive.ubuntu.com/ubuntu focal-backports InRelease
Пол:4 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Пол:5 https://artifacts.elastic.co/packages/7.x/apt stable InRelease [13,6 kB]
Пол:6 https://artifacts.elastic.co/packages/7.x/apt stable/main i386 Packages [64,9 kB]
Пол:7 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 Packages [84,6 kB]

root@daryael-VirtualBox:~# sudo /bin/systemctl daemon-reload && sudo /bin/systemctl enable elasticsearch.service
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/system/elasticsearch.service.
root@daryael-VirtualBox:~#
```

Далее сразу же изменим некоторые настройки для нормальной работы кластера:

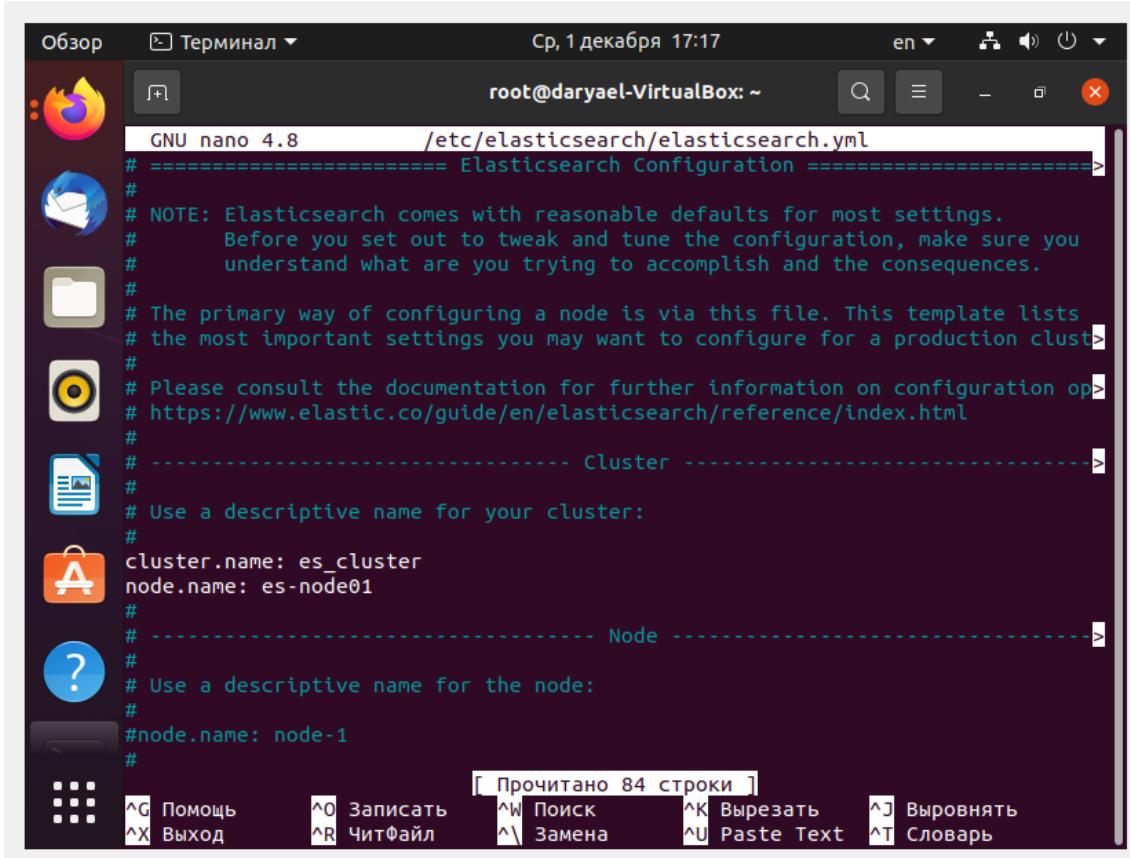
```
root@daryael-VirtualBox:~# sudo nano /etc/elasticsearch/jvm.options
```



```
GNU nano 4.8          /etc/elasticsearch/jvm.options      Изменён
## should create one or more files in the jvm.options.d
## directory containing your adjustments.
##
## See https://www.elastic.co/guide/en/elasticsearch/reference/7.15/jvm-option.html
## for more information.
##
#####
## IMPORTANT: JVM heap size
#####
## The heap size is automatically configured by Elasticsearch
## based on the available memory in your system and the roles
## each node is configured to fulfill. If specifying heap is
## required, it should be done through a file in jvm.options.d,
## and the min and max should be set to the same value. For
## example, to set the heap to 4 GB, create a new file in the
## jvm.options.d directory containing these lines:
##
-Xms256m
-Xmx256m
##
```

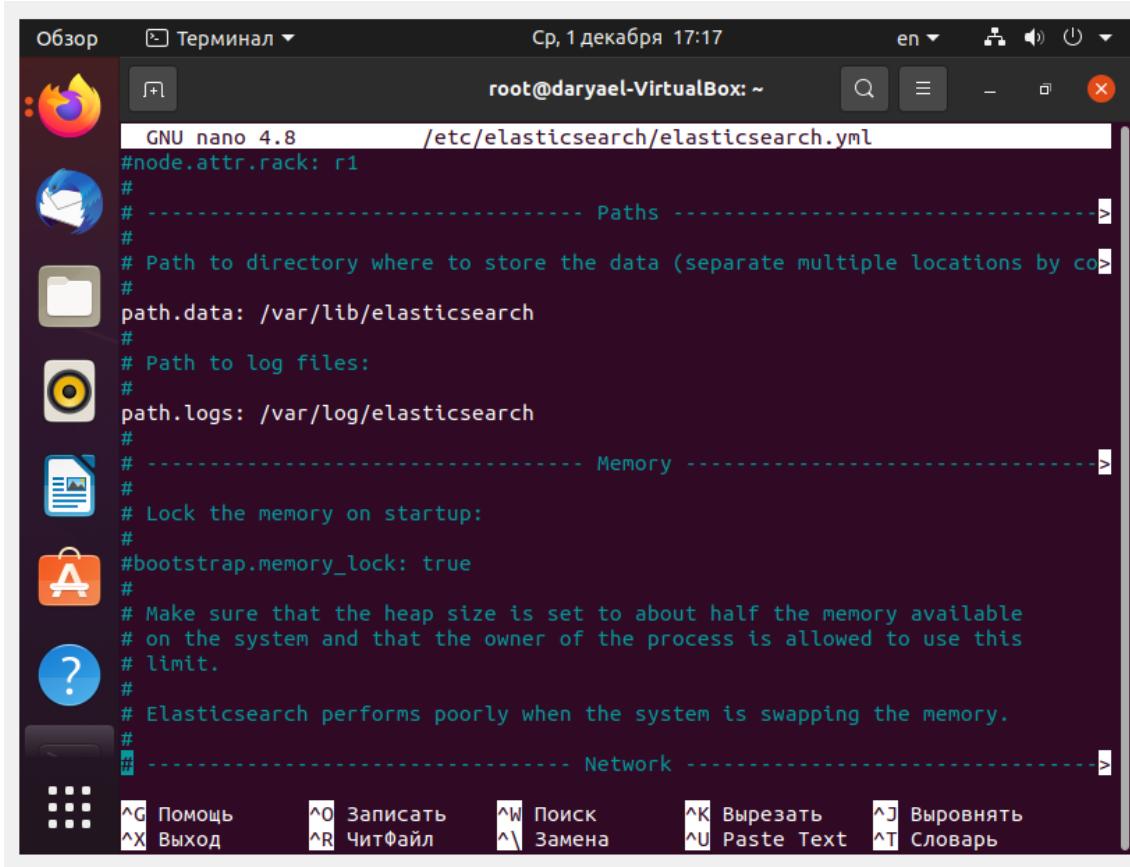
Настраиваем кластер

```
root@daryael-VirtualBox:~# sudo nano /etc/elasticsearch/elasticsearch.yml
```



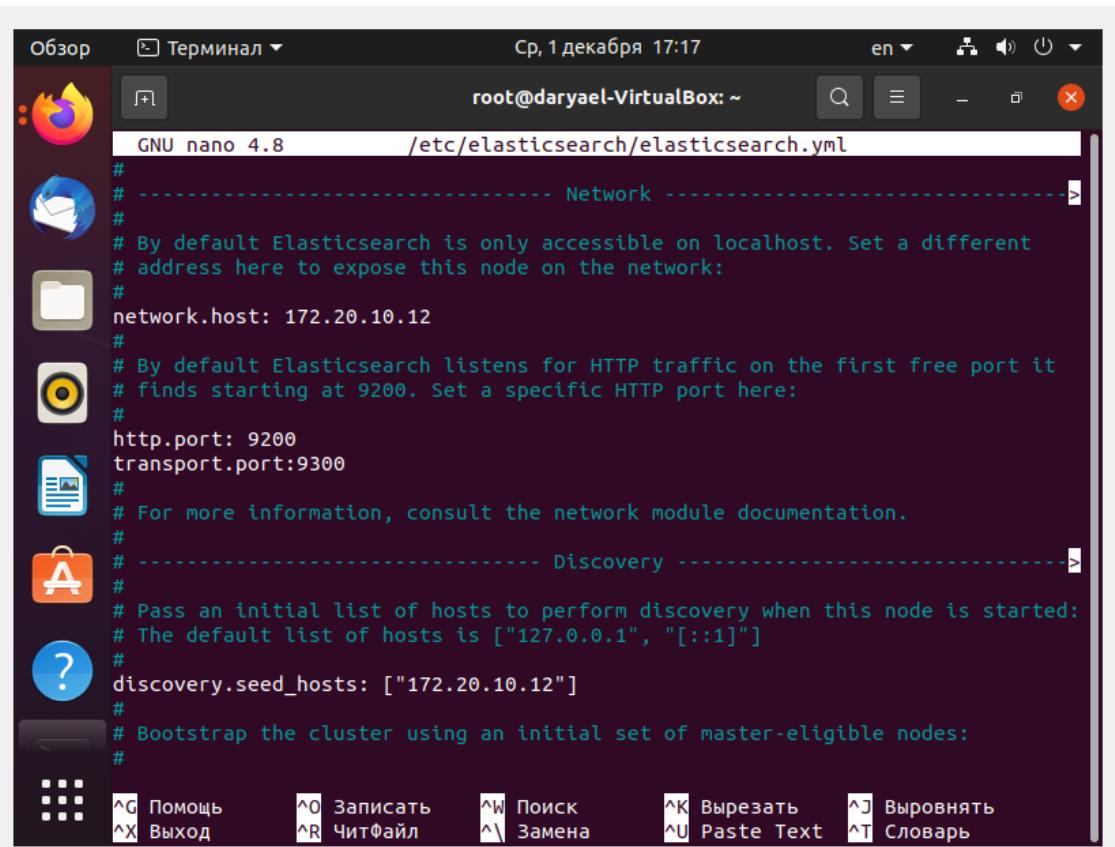
```
GNU nano 4.8      /etc/elasticsearch/elasticsearch.yml
# ===== Elasticsearch Configuration =====>
#
# NOTE: Elasticsearch comes with reasonable defaults for most settings.
# Before you set out to tweak and tune the configuration, make sure you
# understand what are you trying to accomplish and the consequences.
#
# The primary way of configuring a node is via this file. This template lists
# the most important settings you may want to configure for a production clust>
#
# Please consult the documentation for further information on configuration op>
# https://www.elastic.co/guide/en/elasticsearch/reference/index.html
#
# ----- Cluster -----
#
# Use a descriptive name for your cluster:
#
cluster.name: es_cluster
node.name: es-node01
#
# ----- Node -----
#
# Use a descriptive name for the node:
#
#node.name: node-1
#
[ Прочитано 84 строки ]
```

^G Помощь ^O Записать ^W Поиск ^K Вырезать ^J Выровнять  
^X Выход ^R ЧитФайл ^A Замена ^U Paste Text ^T Словарь

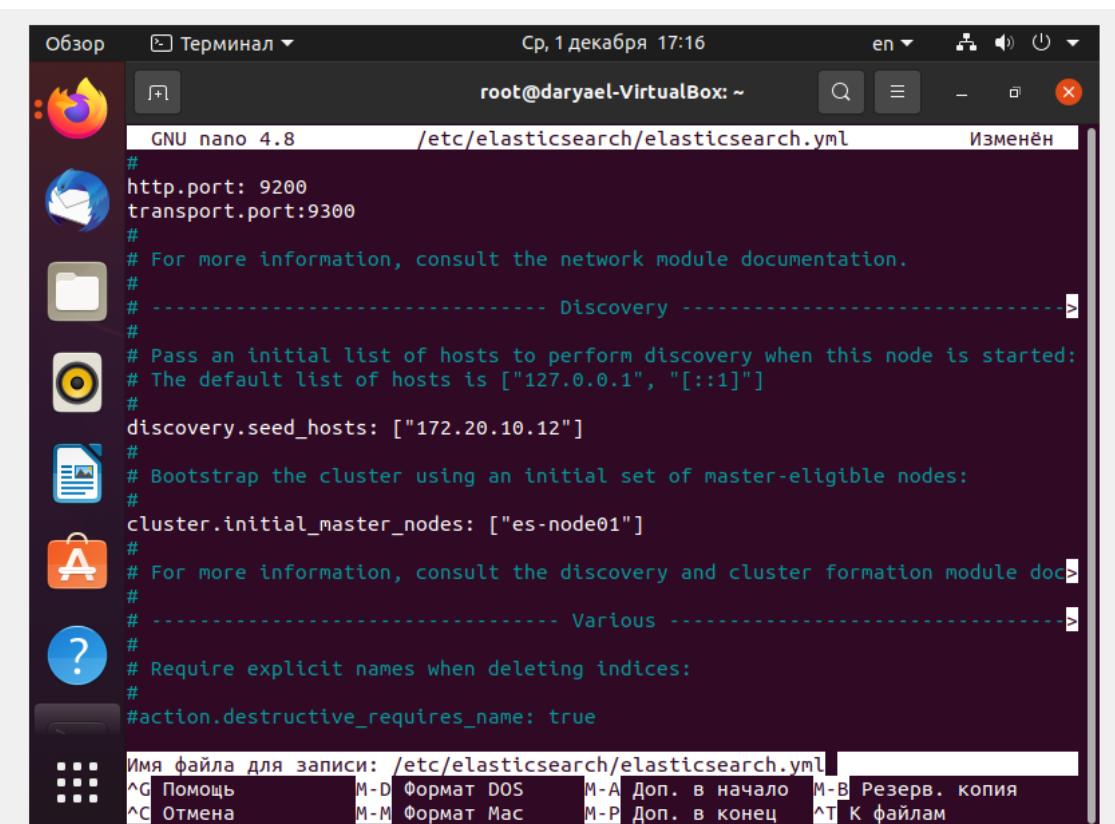


```
GNU nano 4.8      /etc/elasticsearch/elasticsearch.yml
#node.attr.rack: r1
#
# ----- Paths -----
#
# Path to directory where to store the data (separate multiple locations by co>
#
path.data: /var/lib/elasticsearch
#
# Path to log files:
#
path.logs: /var/log/elasticsearch
#
# ----- Memory -----
#
# Lock the memory on startup:
#
#bootstrap.memory_lock: true
#
# Make sure that the heap size is set to about half the memory available
# on the system and that the owner of the process is allowed to use this
# limit.
#
# Elasticsearch performs poorly when the system is swapping the memory.
#
# ----- Network ----->
```

^G Помощь ^O Записать ^W Поиск ^K Вырезать ^J Выровнять  
^X Выход ^R ЧитФайл ^A Замена ^U Paste Text ^T Словарь



```
GNU nano 4.8 /etc/elasticsearch/elasticsearch.yml
#
# ----- Network -----
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: 172.20.10.12
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
transport.port:9300
#
# For more information, consult the network module documentation.
#
# ----- Discovery -----
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
discovery.seed_hosts: ["172.20.10.12"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
```



```
GNU nano 4.8 /etc/elasticsearch/elasticsearch.yml Изменён
#
http.port: 9200
transport.port:9300
#
# For more information, consult the network module documentation.
#
# ----- Discovery -----
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
discovery.seed_hosts: ["172.20.10.12"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
cluster.initial_master_nodes: ["es-node01"]
#
# For more information, consult the discovery and cluster formation module doc
#
# ----- Various -----
#
# Require explicit names when deleting indices:
#
#action.destructive_requires_name: true
```

Запускаем и проверяем службу Elasticsearch:

```
Обзор Терминал Ср, 1 декабря 17:29
root@daryael-VirtualBox: ~
^X
[2]+ Остановлен journalctl -xe
^Z

root@daryael-VirtualBox:~# sudo nano /etc/elasticsearch/elasticsearch.yml
root@daryael-VirtualBox:~# sudo systemctl start elasticsearch.service
root@daryael-VirtualBox:~# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
    Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor>
    Active: active (running) since Wed 2021-12-01 17:29:37 MSK; 13s ago
      Docs: https://www.elastic.co
        Main PID: 11794 (java)
          Tasks: 53 (limit: 4651)
         Memory: 537.2M
        CGroup: /system.slice/elasticsearch.service
                └─11794 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.n>
                  └─11950 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux>

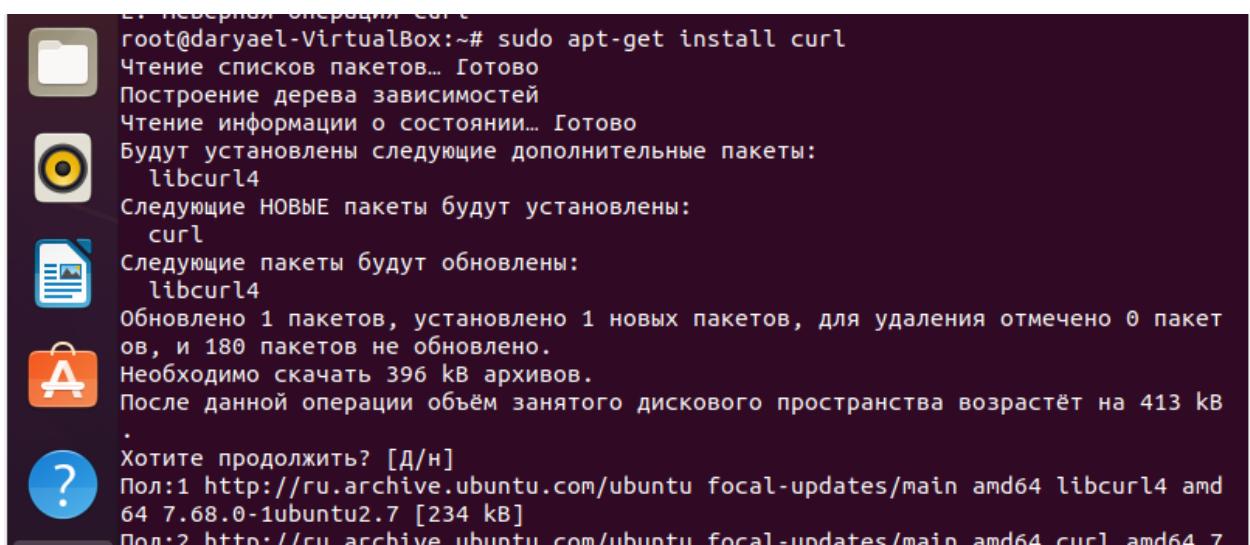
дек 01 17:29:03 daryael-VirtualBox systemd[1]: Starting Elasticsearch...
дек 01 17:29:06 daryael-VirtualBox systemd-entrypoint[11794]: WARNING: A termi>
дек 01 17:29:06 daryael-VirtualBox systemd-entrypoint[11794]: WARNING: System:>
дек 01 17:29:06 daryael-VirtualBox systemd-entrypoint[11794]: WARNING: Please >
дек 01 17:29:06 daryael-VirtualBox systemd-entrypoint[11794]: WARNING: System:>
дек 01 17:29:10 daryael-VirtualBox systemd-entrypoint[11794]: WARNING: A termi>
дек 01 17:29:10 daryael-VirtualBox systemd-entrypoint[11794]: WARNING: System:>
дек 01 17:29:10 daryael-VirtualBox systemd-entrypoint[11794]: WARNING: Please >
дек 01 17:29:10 daryael-VirtualBox systemd-entrypoint[11794]: WARNING: System:>
дек 01 17:29:37 daryael-VirtualBox systemd[1]: Started Elasticsearch.
lines 1-21/21 (END)
```

172.20.10.12:9200

```
{
  "name" : "es-node01",
  "cluster_name" : "es_cluster",
  "cluster_uuid" : "uUcsyEA-SISfCy7vWC6KbQ",
  "version" : {
    "number" : "7.15.2",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "93d5a7f6192e8a1a12e154a2b81bf6fa7309da0c",
    "build_date" : "2021-11-04T14:04:42.515624022Z",
    "build_snapshot" : false,
    "lucene_version" : "8.9.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Elasticsearch теперь активен.

Установим утилиту командной строки, которая позволяет выполнять HTTP-запросы с различными параметрами и методами.



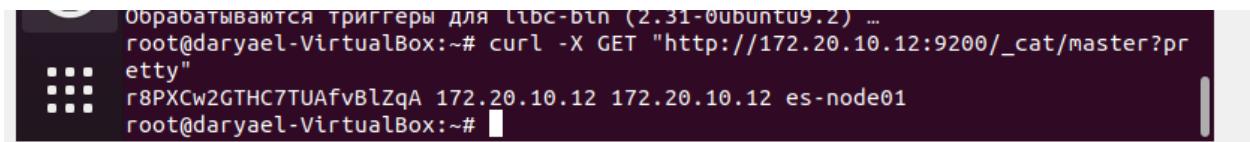
```
[root@daryael-VirtualBox:~# sudo apt-get install curl
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
  libcurl4
Следующие НОВЫЕ пакеты будут установлены:
  curl
Следующие пакеты будут обновлены:
  libcurl4
Обновлено 1 пакетов, установлено 1 новых пакетов, для удаления отмечено 0 пакетов, и 180 пакетов не обновлено.
Необходимо скачать 396 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 413 kB.
Хотите продолжить? [Д/н]
Пол:1 http://ru.archive.ubuntu.com/ubuntu focal-updates/main amd64 libcurl4 amd64 7.68.0-1ubuntu2.7 [234 kB]
Пол:2 http://ru.archive.ubuntu.com/ubuntu focal-updates/main amd64 curl amd64 7.
```

Проверяем состояние кластера, обратившись к его узлу:



```
[root@daryael-VirtualBox:~# curl -X GET "http://172.20.10.12:9200/_cluster/health?pretty"
{
  "cluster_name" : "es_cluster",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 1,
  "number_of_data_nodes" : 1,
  "active_primary_shards" : 1,
  "active_shards" : 1,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
root@daryael-VirtualBox:~#
```

Узнаем, какой узел взял на себя роль master. Так как мы указывали один адрес, то это он и есть:



```
[root@daryael-VirtualBox:~# curl -X GET "http://172.20.10.12:9200/_cat/master?pretty"
r8PXCw2GTHC7TUAfVBlZqA 172.20.10.12 172.20.10.12 es-node01
root@daryael-VirtualBox:~#
```

Теперь отключаем подкачку полностью. После перезапускаем Elasticsearch и посмотрим активный SWAP:

## Настройка потоков

```
root@daryael-VirtualBox:~# ulimit -u 4096
root@daryael-VirtualBox:~# ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority      (-e) 0
file size                (blocks, -f) unlimited
pending signals          (-i) 15504
max locked memory        (kbytes, -l) 65536
max memory size          (kbytes, -m) unlimited
open files               (-n) 1024
pipe size                 (512 bytes, -p) 8
POSIX message queues     (bytes, -q) 819200
real-time priority        (-r) 0
stack size                (kbytes, -s) 8192
cpu time                  (seconds, -t) unlimited
max user processes        (-u) 4096
virtual memory             (kbytes, -v) unlimited
file locks                  (-x) unlimited
root@daryael-VirtualBox:~#
```

Скачиваем и устанавливаем Kibana. Данное действие производим на 2 ВМ с ip 172.20.10.13:

```
root@daryaki-VirtualBox:~# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
OK
root@daryaki-VirtualBox:~# sudo apt-get install apt-transport-https
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Следующие НОВЫЕ пакеты будут установлены:
  apt-transport-https
Обновлено 0 пакетов, установлено 1 новых пакетов, для удаления отмечено 0 пакетов, и 181 пакетов не обновлено.
Необходимо скачать 4 680 B архивов.
После данной операции объём занятого дискового пространства возрастёт на 162 kB .
Пол:1 http://ru.archive.ubuntu.com/ubuntu focal-updates/universe amd64 apt-transport-https all 2.0.6 [4 680 B]
Получено 4 680 B за 0с (19,5 kB/s)
Выбор ранее не выбранного пакета apt-transport-https.
(Чтение базы данных ... на данный момент установлено 151195 файлов и каталогов.)
Подготовка к распаковке .../apt-transport-https_2.0.6_all.deb ...
Распаковывается apt-transport-https (2.0.6) ...
Настраивается пакет apt-transport-https (2.0.6) ...
root@daryaki-VirtualBox:~#
```

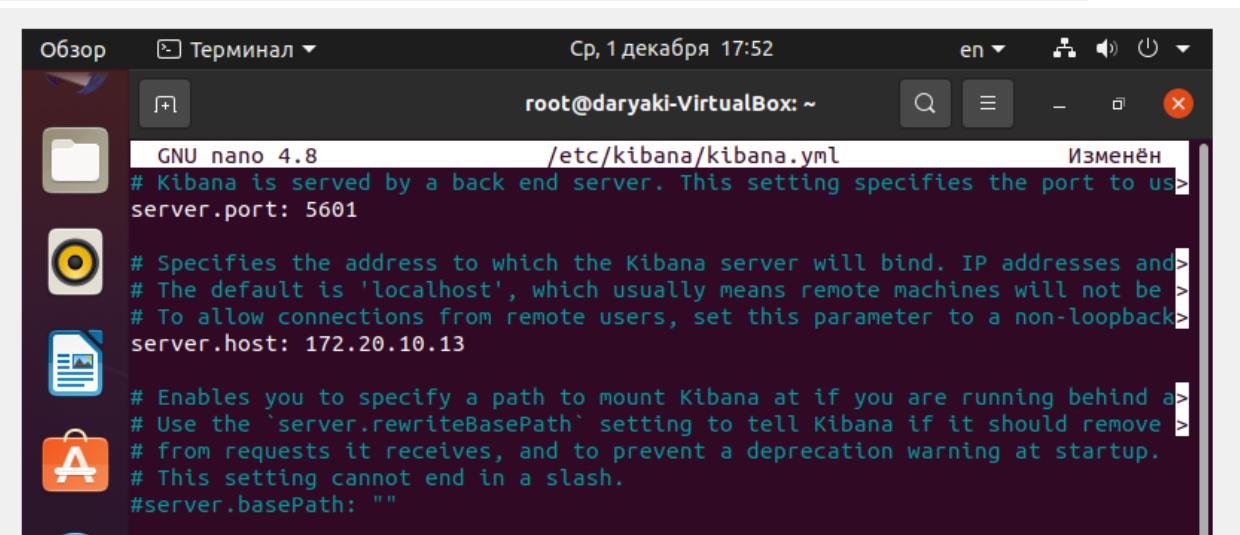
```
root@daryaki-VirtualBox:~# sudo apt-get update && sudo apt-get install kibana
Сущ:1 http://ru.archive.ubuntu.com/ubuntu focal InRelease
Сущ:2 http://ru.archive.ubuntu.com/ubuntu focal-updates InRelease
Сущ:3 http://ru.archive.ubuntu.com/ubuntu focal-backports InRelease
Сущ:4 http://security.ubuntu.com/ubuntu focal-security InRelease
Пол:5 https://artifacts.elastic.co/packages/7.x/apt stable InRelease [13,6 kB]
Пол:6 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 Packages [84,6 kB]
Пол:7 https://artifacts.elastic.co/packages/7.x/apt stable/main i386 Packages [64,9 kB]
Получено 163 kB за 1с (144 kB/s)
Чтение списков пакетов... Готово
```

```
.10.2-amd64.deb
root@daryaki-VirtualBox:~# sudo /bin/systemctl daemon-reload && sudo /bin/systemctl enable kibana.service
```

```
.10.2-amd64.deb
root@daryaki-VirtualBox:~# sudo /bin/systemctl daemon-reload && sudo /bin/systemctl enable kibana.service
Synchronizing state of kibana.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable kibana
root@daryaki-VirtualBox:~#
```

Настраиваем Kibana для работы с кластером Elasticsearch:

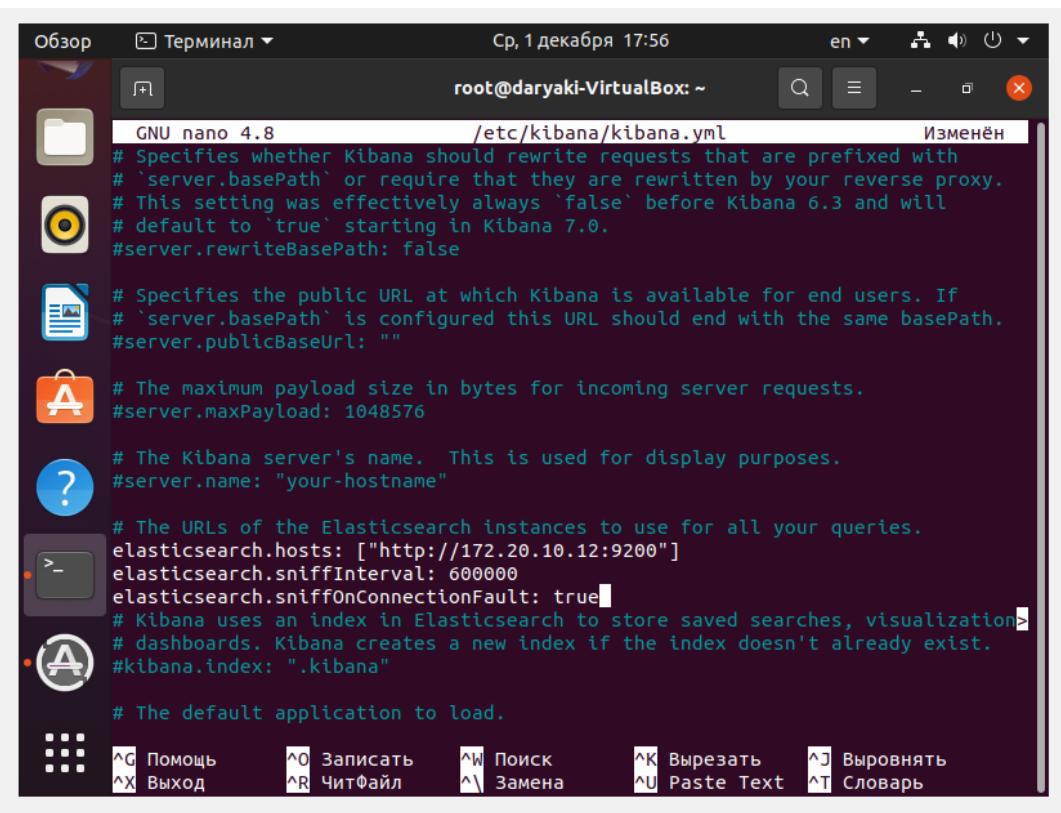
```
Valid_lrt forever preferred_lrt forever
root@daryaki-VirtualBox:~# nano /etc/kibana/kibana.yml
```



```
GNU nano 4.8          /etc/kibana/kibana.yml      Изменён
# Kibana is served by a back end server. This setting specifies the port to us>
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and >
# The default is 'localhost', which usually means remote machines will not be >
# To allow connections from remote users, set this parameter to a non-loopback >
server.host: 172.20.10.13

# Enables you to specify a path to mount Kibana at if you are running behind a >
# Use the 'server.rewriteBasePath' setting to tell Kibana if it should remove >
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#serverbasePath: ""
```



```
GNU nano 4.8          /etc/kibana/kibana.yml      Изменён
# Specifies whether Kibana should rewrite requests that are prefixed with
# `server.basePath` or require that they are rewritten by your reverse proxy.
# This setting was effectively always 'false' before Kibana 6.3 and will
# default to 'true' starting in Kibana 7.0.
#server.rewriteBasePath: false

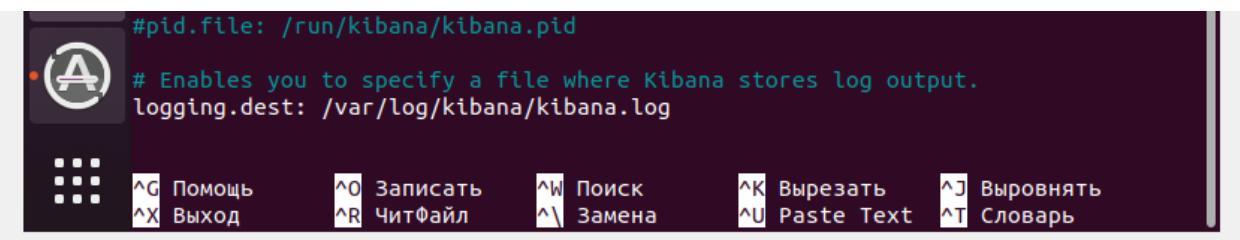
# Specifies the public URL at which Kibana is available for end users. If
# `server.basePath` is configured this URL should end with the same basePath.
#server.publicBaseUrl: ""

# The maximum payload size in bytes for incoming server requests.
#server.maxPayload: 1048576

# The Kibana server's name. This is used for display purposes.
#server.name: "your-hostname"

# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://172.20.10.12:9200"]
elasticsearch.sniffInterval: 600000
elasticsearch.sniffOnConnectionFault: true
# Kibana uses an index in Elasticsearch to store saved searches, visualizations >
# dashboards. Kibana creates a new index if the index doesn't already exist.
#kibana.index: ".kibana"

# The default application to load.
```



```
#pid.file: /run/kibana/kibana.pid

# Enables you to specify a file where Kibana stores log output.
logging.dest: /var/log/kibana/kibana.log
```

Запускаем службу kibana:

```
root@daryaki-VirtualBox:~# sudo systemctl start kibana.service
root@daryaki-VirtualBox:~#
```

Проверяем в браузере на стационарном компьютере:

The screenshot shows the Elasticsearch home page. At the top left is the URL '172.20.10.13:5601/app/home#/'. The main header is 'Welcome to Elastic'. Below it is a decorative graphic of various charts and data visualizations. A call-to-action button says 'Start by adding your data'. Below that, a text block encourages adding data from any source and visualizing it in real time. It includes links for 'Add data' and 'Explore on my own'. At the bottom, there's a note about privacy and data collection.

Устанавливаем Elasticsearch на машину с Kibana:

```
root@daryaki-VirtualBox:~# sudo apt-get update && sudo apt-get install elasticsearch
Сущ:1 http://ru.archive.ubuntu.com/ubuntu focal InRelease
Сущ:2 http://ru.archive.ubuntu.com/ubuntu focal-updates InRelease
Сущ:3 http://ru.archive.ubuntu.com/ubuntu focal-backports InRelease
Сущ:4 http://security.ubuntu.com/ubuntu focal-security InRelease
Сущ:5 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Чтение списков пакетов... Готово
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Следующие НОВЫЕ пакеты будут установлены:
  elasticsearch
Обновлено 0 пакетов, установлено 1 новых пакетов, для удаления отмечено 0 пакетов, и 181 пакетов не обновлено.
Необходимо скачать 341 MB архивов.
После этого операции общий объем занятого дискового пространства будет 549 MB

root@daryaki-VirtualBox:~# sudo /bin/systemctl daemon-reload && sudo /bin/systemctl enable elasticsearch.service
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/system/elasticsearch.service.
root@daryaki-VirtualBox:~#
```

Настраиваем новому узлу роль Coordinating only:

```
root@daryaki-VirtualBox:~# sudo nano /etc/elasticsearch/elasticsearch.yml
```

Обзор Терминал Ср, 1 декабря 18:12 en

```
GNU nano 4.8 /etc/elasticsearch/elasticsearch.yml Изменён
# Before you set out to tweak and tune the configuration, make sure you
# understand what are you trying to accomplish and the consequences.
#
# The primary way of configuring a node is via this file. This template lists
# the most important settings you may want to configure for a production clus>
#
# Please consult the documentation for further information on configuration op>
# https://www.elastic.co/guide/en/elasticsearch/reference/index.html
#
# ----- Cluster -----
#
# Use a descriptive name for your cluster:
#
cluster.name: es_cluster
#
# ----- Node -----
#
# Use a descriptive name for the node:
#
node.name: es-nlb01
#
# Add custom attributes to the node:
node.master: false
node.data: false
node.ingest: false

^G Помощь ^O Записать ^W Поиск ^K Вырезать ^J Выровнять
^X Выход ^R ЧитФайл ^L Замена ^U Paste Text ^T Словарь
```

Обзор Терминал Ср, 1 декабря 18:13 en

```
GNU nano 4.8 /etc/elasticsearch/elasticsearch.yml Изменён
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
#network.host: 192.168.0.1
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
#http.port: 9200
#
# For more information, consult the network module documentation.
#
# ----- Discovery -----
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
discovery.seed_hosts: ["172.20.10.12"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
```

Обзор Терминал Ср, 1 декабря 18:16 en

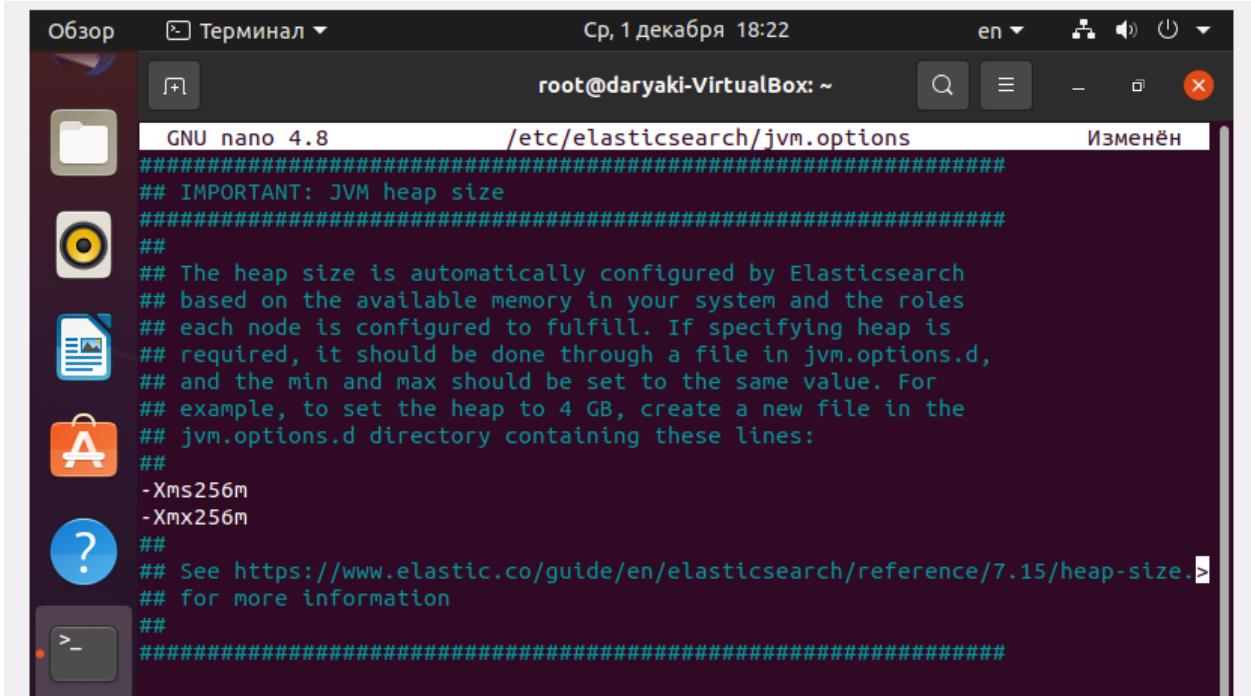
root@daryaki-VirtualBox: ~

GNU nano 4.8 /etc/elasticsearch/elasticsearch.yml ИЗМЕНЁН

```
# address here to expose this node on the network:  
#  
network.host: 172.20.10.13  
transport.host: 172.20.10.13  
#  
# By default Elasticsearch listens for HTTP traffic on the first free port it  
# finds starting at 9200. Set a specific HTTP port here:  
#  
http.port: 9200  
transport.tcp.port: 9300-9400  
#  
# For more information, consult the network module documentation.  
#  
# ----- Discovery ----->  
#  
# Pass an initial list of hosts to perform discovery when this node is started:  
# The default list of hosts is ["127.0.0.1", "[::1]"]  
#  
discovery.seed_hosts: ["172.20.10.12"]  
#  
# Bootstrap the cluster using an initial set of master-eligible nodes:  
#  
#cluster.initial_master_nodes: ["node-1", "node-2"]  
#  
# For more information, consult the discovery and cluster formation module doc  
# ----- Paths ----->  
#  
# Path to directory where to store the data (separate multiple locations by comma)  
#  
path.data: /var/lib/elasticsearch  
#  
# Path to log files:  
#  
path.logs: /var/log/elasticsearch  
#  
# ----- Memory ----->  
#  
# Lock the memory on startup:  
#
```

^G Помощь ^O Записать ^W Поиск ^K Вырезать ^J Выровнять  
^X Выход ^R ЧитФайл ^\ Замена ^U Paste Text ^T Словарь

root@daryaki-VirtualBox:~# sudo nano /etc/elasticsearch/jvm.options



```
GNU nano 4.8          /etc/elasticsearch/jvm.options      Изменён
#####
## IMPORTANT: JVM heap size
#####
## The heap size is automatically configured by Elasticsearch
## based on the available memory in your system and the roles
## each node is configured to fulfill. If specifying heap is
## required, it should be done through a file in jvm.options.d,
## and the min and max should be set to the same value. For
## example, to set the heap to 4 GB, create a new file in the
## jvm.options.d directory containing these lines:
##
-Xms256m
-Xmx256m
##
## See https://www.elastic.co/guide/en/elasticsearch/reference/7.15/heap-size.>
## for more information
##
#####
```

Запускаем Elasticsearch и проверяем, что узел присоединился к кластеру:

```
root@daryaki-VirtualBox:~# sudo systemctl start elasticsearch.service
root@daryaki-VirtualBox:~# sudo systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
  Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor>
  Active: active (running) since Wed 2021-12-01 18:23:41 MSK; 15s ago
    Docs: https://www.elastic.co
  Main PID: 11055 (java)
     Tasks: 43 (limit: 4651)
    Memory: 463.9M
   CGroup: /system.slice/elasticsearch.service
           └─11055 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.n>
               ├─11213 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux>

дек 01 18:23:06 daryaki-VirtualBox systemd[1]: Starting Elasticsearch...
дек 01 18:23:09 daryaki-VirtualBox systemd-entrypoint[11055]: WARNING: A termi>
дек 01 18:23:09 daryaki-VirtualBox systemd-entrypoint[11055]: WARNING: System:>
дек 01 18:23:09 daryaki-VirtualBox systemd-entrypoint[11055]: WARNING: Please >
дек 01 18:23:09 daryaki-VirtualBox systemd-entrypoint[11055]: WARNING: System:>
дек 01 18:23:14 daryaki-VirtualBox systemd-entrypoint[11055]: WARNING: A termi>
дек 01 18:23:14 daryaki-VirtualBox systemd-entrypoint[11055]: WARNING: System:>
дек 01 18:23:14 daryaki-VirtualBox systemd-entrypoint[11055]: WARNING: Please >
дек 01 18:23:14 daryaki-VirtualBox systemd-entrypoint[11055]: WARNING: System:>
дек 01 18:23:41 daryaki-VirtualBox systemd[1]: Started Elasticsearch.
lines 1-21/21 (END)
```

Также отключаем подкачку и на 2 ВМ для Elasticsearch:

```
darya-ki@daryaki-VirtualBox:~$ sudo swapoff -a
```

## Проверяем Elasticsearch:

```
root@daryaki-VirtualBox:~# apt-get install curl
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
  libcurl4
Следующие НОВЫЕ пакеты будут установлены:
  curl
Следующие пакеты будут обновлены:
  libcurl4
Обновлено 1 пакетов, установлено 1 новых пакетов, для удаления отмечено 0 пакетов, и 180 пакетов не обновлено.
Необходимо скачать 396 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 413 kB
...
Хотите продолжить? [Д/н]
```

```
root@daryaki-VirtualBox:~# curl -X GET "http://172.20.10.13:9200/_cluster/health?pretty"
{
  "cluster_name" : "es_cluster",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 2,
  "number_of_data_nodes" : 1,
  "active_primary_shards" : 7,
  "active_shards" : 7,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
root@daryaki-VirtualBox:~#
```

В конфигурации Kibana указываем адрес Coordinating only узла `elasticsearch.hosts`:

```
root@daryaki-VirtualBox:~# nano /etc/kibana/kibana.yml
```

```
Обзор Терминал Ср, 1 декабря 18:30 en
root@daryaki-VirtualBox: ~
GNU nano 4.8 /etc/kibana/kibana.yml Изменён
#server.rewriteBasePath: false

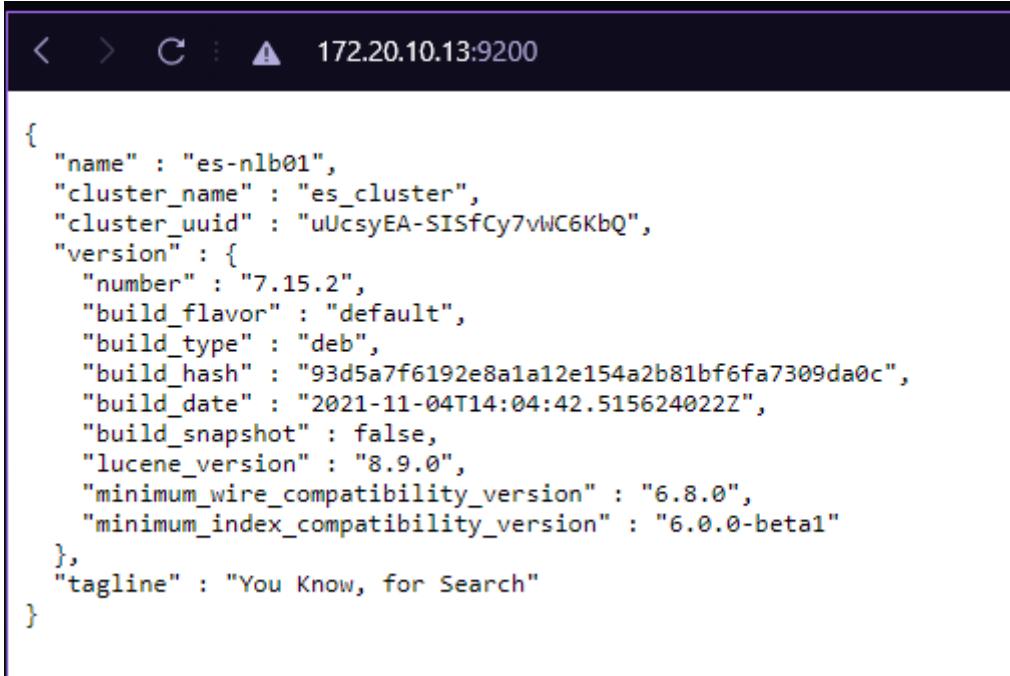
# Specifies the public URL at which Kibana is available for end users. If
# `server.basePath` is configured this URL should end with the same basePath.
#server.publicBaseUrl: ""

# The maximum payload size in bytes for incoming server requests.
#server.maxPayload: 1048576

# The Kibana server's name. This is used for display purposes.
#server.name: "your-hostname"

# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://172.20.10.12:9200", "http://172.20.10.13:9200"]
elasticsearch.sniffInterval: 600000
elasticsearch.sniffOnConnectionFault: true
```

Служба запустилась, а UI Kibana открывается в браузере:



The screenshot shows a browser window with the URL 172.20.10.13:9200. The page displays the Elasticsearch cluster configuration in JSON format. Key details include the cluster name 'es\_cluster', UUID 'uUcsyEA-SISfCy7vWC6KbQ', and version information (7.15.2). The tagline 'You Know, for Search' is also visible.

```
{
  "name" : "es-nlb01",
  "cluster_name" : "es_cluster",
  "cluster_uuid" : "uUcsyEA-SISfCy7vWC6KbQ",
  "version" : {
    "number" : "7.15.2",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "93d5a7f6192e8a1a12e154a2b81bf6fa7309da0c",
    "build_date" : "2021-11-04T14:04:42.515624022Z",
    "build_snapshot" : false,
    "lucene_version" : "8.9.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Скачиваем и устанавливаем Logstash

```
root@daryaki-VirtualBox:~# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
OK
root@daryaki-VirtualBox:~# sudo apt-get update && sudo apt-get install logstash
Пол:1 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Сущ:2 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Пол:3 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metadata [35,7 kB]
Пол:4 http://security.ubuntu.com/ubuntu focal-security/universe amd64 DEP-11 Metadata [64,4 kB]
Пол:5 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 DEP-11 Metadata [2 464 B]
Сущ:6 http://ru.archive.ubuntu.com/ubuntu focal InRelease
Сущ:7 http://ru.archive.ubuntu.com/ubuntu focal-updates InRelease
Сущ:8 http://ru.archive.ubuntu.com/ubuntu focal-backports InRelease
Получено 216 kB за 6с (38,4 kB/s)
```

```
root@daryaki-VirtualBox:~# sudo /bin/systemctl daemon-reload && sudo /bin/systemctl enable logstash.service
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service →
/etc/systemd/system/logstash.service.
root@daryaki-VirtualBox:~#
```

Настраиваем Logstash для чтения данных из файла:

```
/etc/systemd/system/logstash.service.
root@daryaki-VirtualBox:~# nano /etc/logstash/conf.d/logstash.conf
```

Обзор Терминал Ср, 1 декабря 19:03 root@daryaki-VirtualBox: ~

GNU nano 4.8 /etc/logstash/conf.d/logstash.conf Изменён

```
# Читаем файл
input {
    file {
        path => ["/var/log/logstash/*.log"]
        start_position => "beginning"
    }
}

# Извлекаем данные из событий
filter {
    grok {
        match => { "message" => "\[%{TIMESTAMP_ISO8601:timestamp}\]\[%{DATA:severity}\] %{DATA:log_level} %{DATA:log_message}" }
        overwrite => [ "message" ]
    }
}

# Сохраняем все в Elasticsearch
output {
    elasticsearch {
        hosts => ["http://172.20.10.12:9200"]
        index => "logstash-logs-%{+YYYY.MM}"
    }
}
```

Помощь Записать Поиск Вырезать Выровнять  
Выход ЧитФайл Замена Paste Text Словарь

Запускаем Logstash:

```
root@daryaki-VirtualBox:~# nano /etc/logstash/conf.d/logstash.conf
root@daryaki-VirtualBox:~# sudo systemctl start logstash.service
root@daryaki-VirtualBox:~# sudo systemctl status logstash.service
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor pre>
   Active: active (running) since Wed 2021-12-01 19:04:27 MSK; 15s ago
     Main PID: 13258 (java)
        Tasks: 14 (limit: 4651)
       Memory: 229.1M
      CGroup: /system.slice/logstash.service
              └─13258 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseCo>

дек 01 19:04:27 daryaki-VirtualBox systemd[1]: Started logstash.
дек 01 19:04:27 daryaki-VirtualBox logstash[13258]: Using bundled JDK: /usr/sh>
дек 01 19:04:28 daryaki-VirtualBox logstash[13258]: OpenJDK 64-Bit Server VM w>
```

Смотрим полученные данные в Kibana

Welcome to Elastic

Start by adding your data

Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and protect against security threats.

Add data Explore on my own

To learn about how usage data helps us manage and improve our products and services, see our [Privacy Statement](#). To stop collection, [disable usage data here](#).

Configuration missing

server.publicBaseUrl is missing and should be configured when running in a production environment. Some features may not behave correctly. See the documentation.

Mute warning

Your data is not secure

Don't lose one bit. Enable our free security features.

Don't show again

Enable security Dismiss

## Add data

All Logs Metrics Security Sample data Upload file

Now generally available: Elastic Agent integrations

Elastic Agent integrations provide a simple, unified way to add monitoring for logs, metrics, and other types of data to your hosts. You no longer need to install multiple Beats, which makes it easier and faster to deploy policies across your infrastructure. For more information, read our [announcement blog post](#).

Try Integrations Dismiss message

<b>ActiveMQ logs</b> Collect ActiveMQ logs with Filebeat.	<b>ActiveMQ metrics</b> Fetch monitoring metrics from ActiveMQ instances.	<b>Aerospike metrics</b> Fetch internal metrics from the Aerospike server.	<b>Apache logs</b> Collect and parse access and error logs created by the Apache HTTP server.
<b>Apache metrics</b> Fetch internal metrics from the Apache 2	<b>APM</b> Collect in-depth performance metrics	<b>Arbor Peakflow logs</b> Collect Netscout Arbor Peakflow SP logs over	<b>Auditbeat</b> Collect audit data from your hosts.

Открываем Kibana, нажимаем меню и в секции Management выбираем Stack Management. Далее выбираем Index patterns и нажимаем кнопку Create Index Pattern. В поле Index pattern name описываем шаблон logstash\*, в который попадут все индексы, начинающиеся с logstash.

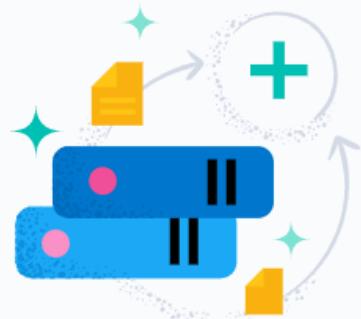
The screenshot shows the Kibana navigation menu on the left with various sections like Alerts, Hosts, Network, Timelines, Cases, Endpoints, Management, Dev Tools, Integrations, Fleet, Osquery, Stack Monitoring, and Stack Management. The Stack Management section is highlighted. To the right, there's a list of pre-defined index patterns: CockroachDB metrics, Couchbase metrics, and Docker metrics, each with a brief description and icon.

The screenshot shows the Elasticsearch Stack Management interface under the Index patterns section. The left sidebar includes Management, Ingest, Data, Alerts and Insights, and Kibana sections. The main area has a search bar and a 'Create index pattern' button. A message on the right says 'You have data in Elasticsearch. Now, create an index pattern.' with a small illustration of a stack of boxes. Below it, a link says 'Want to learn more? Read documentation'.

# You have data in Elasticsearch. Now, create an index pattern.

Kibana requires an index pattern to identify which data streams, indices, and index aliases you want to explore. An index pattern can point to a specific index, for example, your log data from yesterday, or all indices that contain your log data.

[+ Create index pattern](#)



Want to learn more? [Read documentation](#)

### Create index pattern

Name: logstash\*

Timestamp field: @timestamp

Index: logstash-logs-2021.12

После создания шаблона индексов [Kibana](#) покажет информацию об имеющихся полях, типе данных и возможности делать агрегацию по этим полям.

elastic

Stack Management > Index patterns > logstash\*

**logstash\***

Time field: @timestamp

View and edit fields in **logstash\***. Field attributes, such as type and searchability, are based on [field mappings](#) in Elasticsearch.

Fields (21) Scripted fields (0) Field filters (0)

Name ↑	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		●	●	✎
@version	keyword		●	●	✎
_id	_id		●	●	✎
_index	_index		●	●	✎
_score					✎
_source	_source				✎
_type	_type		●	●	✎
geoip.ip	ip		●	●	✎
geoip.latitude	half_float		●	●	✎
geoip.location	geo_point		●	●	✎

Rows per page: 10 < 1 2 3 >

Saved 'logstash\*' ✎

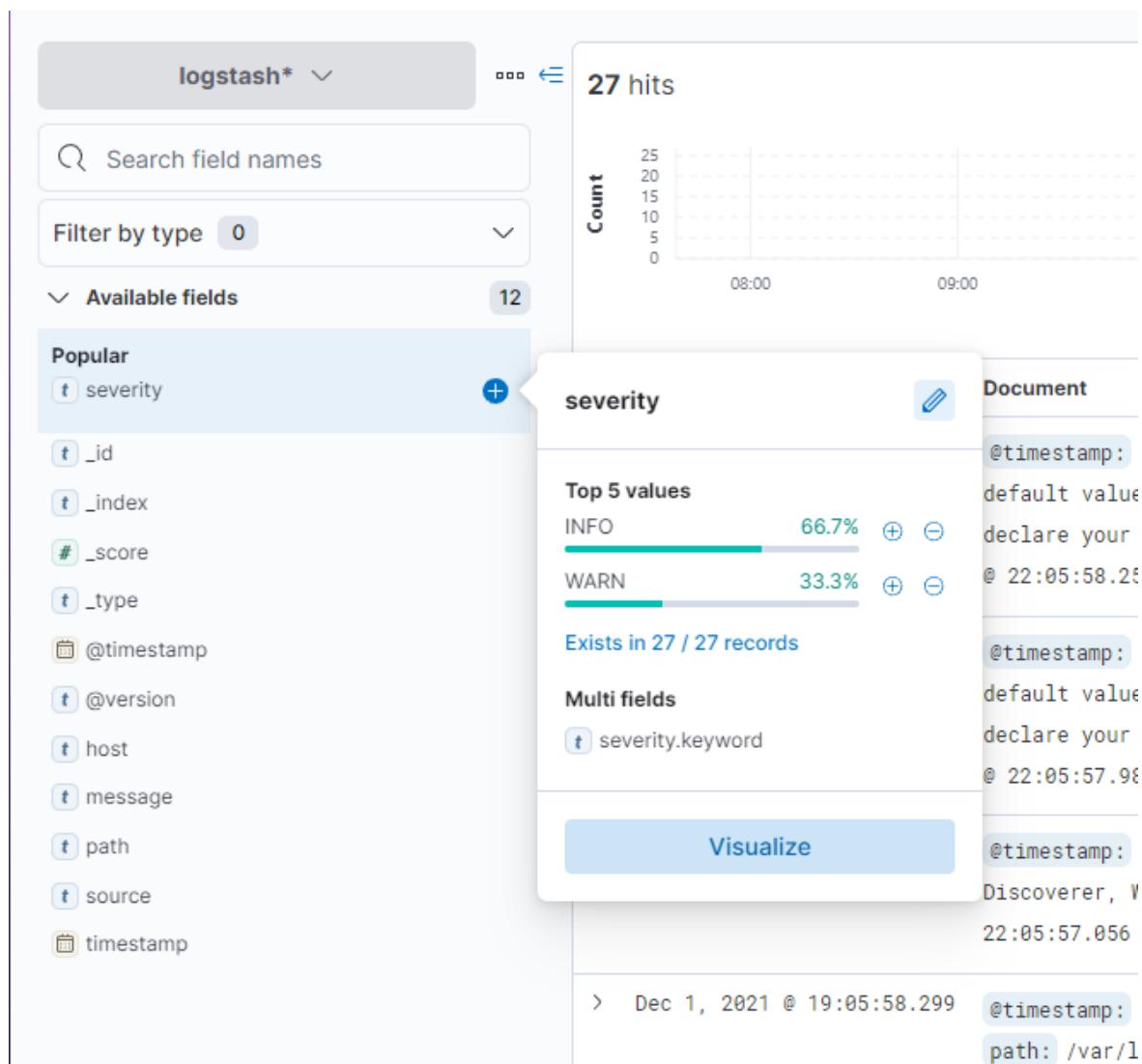
Чтобы посмотреть полученные данные на основе созданного шаблона нажимаем меню и в секции Kibana выбираем Discover.

The screenshot shows the Kibana Discover interface. At the top, there are buttons for Options, New, Save, Open, Share, and Inspect. Below that is a search bar with a dropdown set to 'logstash\*' and a 'Search' button. To the right are buttons for 'KQL' (selected), 'Last 24 hours' (selected), 'Show dates', and a 'Refresh' button. A chart area shows a histogram of document counts over time, with a peak around 20 hits per 30 minutes. The main table lists 27 hits from Dec 1, 2021, at 19:05:59.349. Each hit includes a timestamp, host information, message content, and various log fields like \_id, \_index, \_score, \_type, @version, host, message, path, severity, source, and timestamp. The messages describe Logstash's startup and configuration details, such as ECS compatibility mode and pipeline settings.

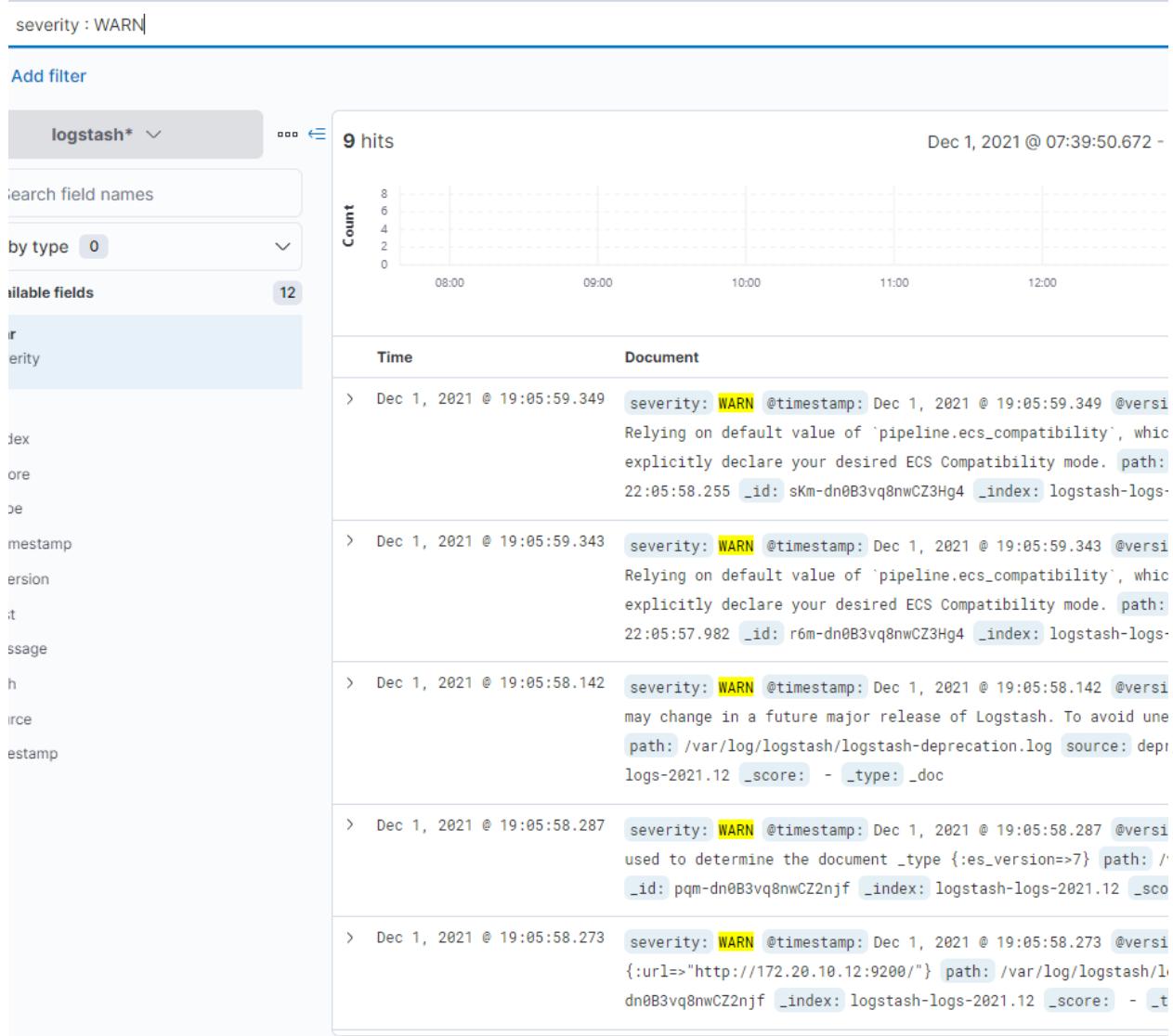
Выбираем интервал в рамках которого будут отображаться данные:

The screenshot shows the Kibana Discover interface with the date range selector expanded. The top bar has buttons for Options, New, Save, and Open. Below is a search bar with 'logstash\*' selected and a 'Search' button. The date range selector is open, showing 'Last 24 hours' as the current selection. It includes a 'Quick select' section with dropdowns for 'Last' and '12' followed by 'hours' and an 'Apply' button. Below this are sections for 'Commonly used' and 'Recently used date ranges' with links to 'Today', 'This week', 'Last 15 minutes', 'Last 30 minutes', 'Last 1 hour', 'Last 24 hours', and 'Last 15 minutes'. At the bottom is a 'Refresh every' section with a '10' input field, a 'seconds' dropdown, and a 'Stop' checkbox.

Выбираем шаблон индекса или поля для отображения из списка Available fields. При нажатии на доступные поля можно получить топ-5 значений.



Для фильтрации данных используем Kibana Query Language (KQL). Запрос пишем в поле Search.



Для визуализации полученных данных нажимаем меню и в секции Kibana выбираем Visualize. Нажав Create new visualization , откроется окно с перечнем доступных типов визуализации. В данном случае указан также второй способ создать визуализацию:



☰

D

Discover



Search



+ Add filter

logstash\*



Search field names

Filter by type 0

Available fields

12

## Popular

\_index

host

severity

\_id

\_score

\_type

@timestamp

@version

message

path

source

timestamp

27 hits

Count



Time ↓

&gt; Dec 1, 2021 @ 19:05:59.349

Documents

@times

default

declare

@ 22:01

@times

default

declare

@ 22:01

@times

Discover

22:05:1

@times

{:since}

severity



## Top 5 values

INFO 66.7% + ⊖WARN 33.3% + ⊖

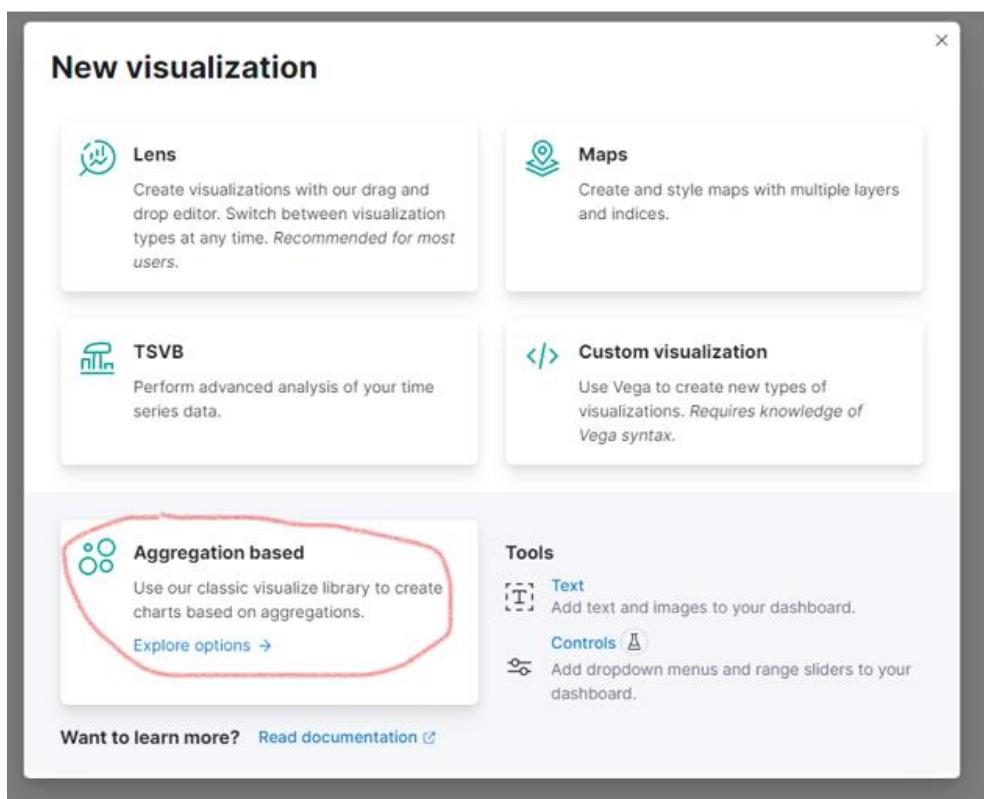
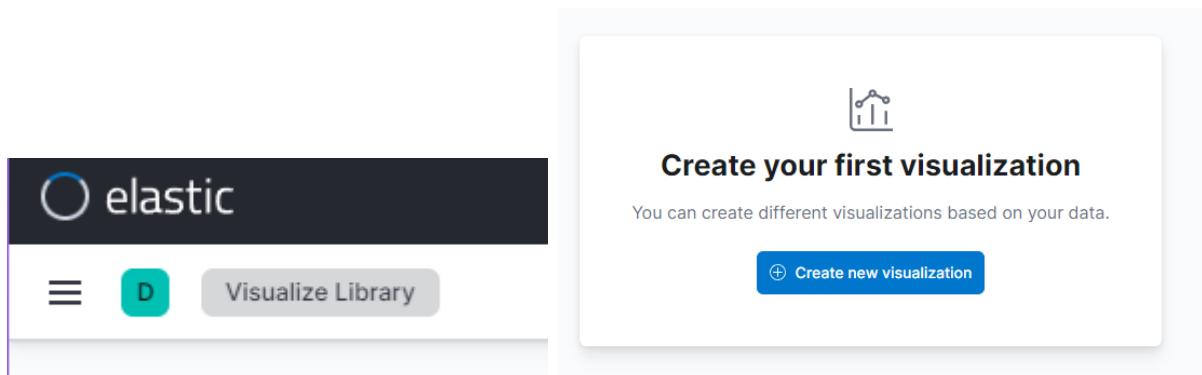
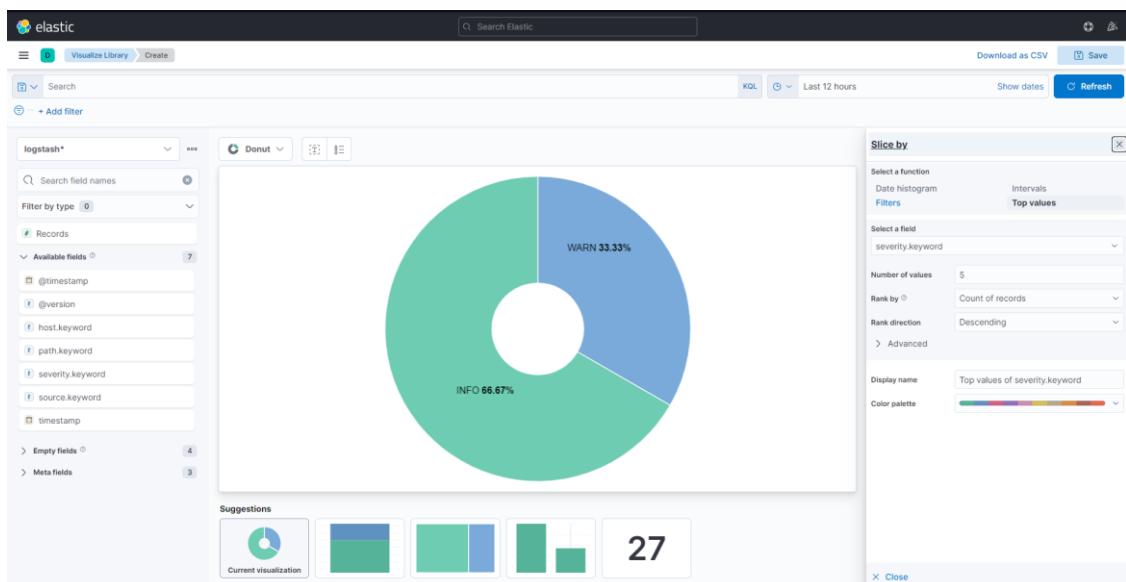
Exists in 27 / 27 records

## Multi fields

severity.keyword

Visualize

&gt; Dec 1, 2021 @ 19:05:08.299



## New visualization

- Area**  
Emphasize the data between an axis and a line.
- Data table**  
Display data in rows and columns.
- Gauge**  
Show the status of a metric.
- Goal**  
Track how a metric progresses to a goal.
- Heat map**  
Shade data in cells in a matrix.
- Horizontal bar**  
Present data in horizontal bars on an axis.
- Line**  
Display data as a series of points.
- Metric**  
Show a calculation as a single number.
- Pie**  
Compare data in proportion to a whole.
- Tag cloud**  
Display word frequency with font size.
- Timeline**  
Show time series data on a graph.
- Vertical bar**  
Present data in vertical bars on an axis.

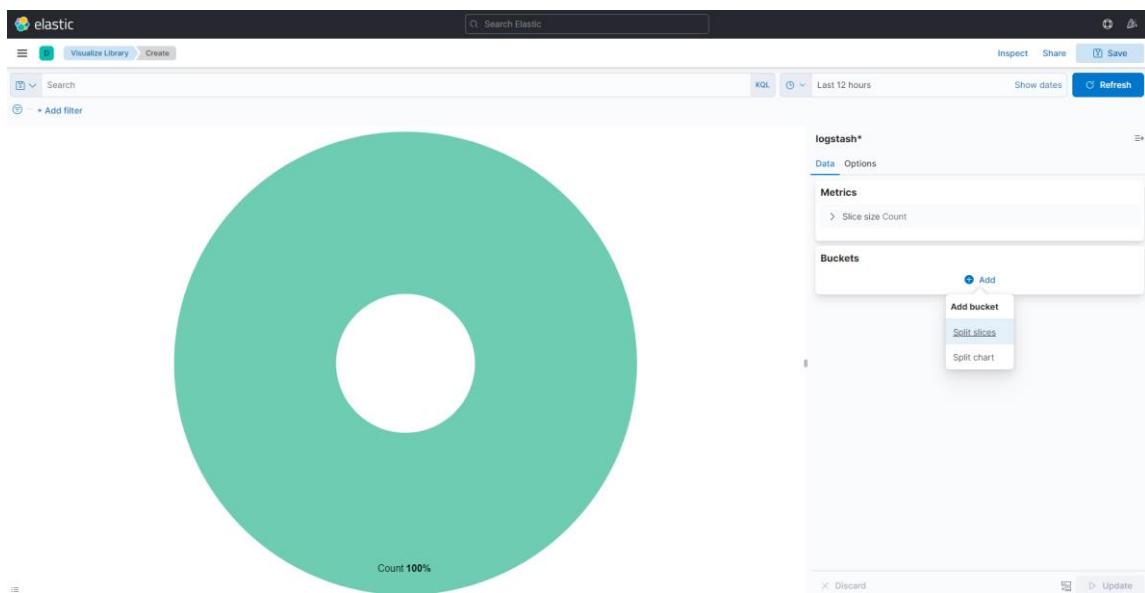
### New Pie / Choose a source

[Select a different visualization](#)

Sort ▾ Types 2 ▾

- logstash\*

В правой части в секции Buckets жмем Add , далее - Split slices. Тип агрегации выбираем Terms, поле severity.keyword. Жмем Update в правом нижнем углу и получаем готовую диаграмму.



## Buckets

∨ Split slices ✖

Aggregation Terms help ↗

Terms

Field

severity.keyword

Order by

Metric: Count

Order

Size

Descending

5

Group other values in separate bucket

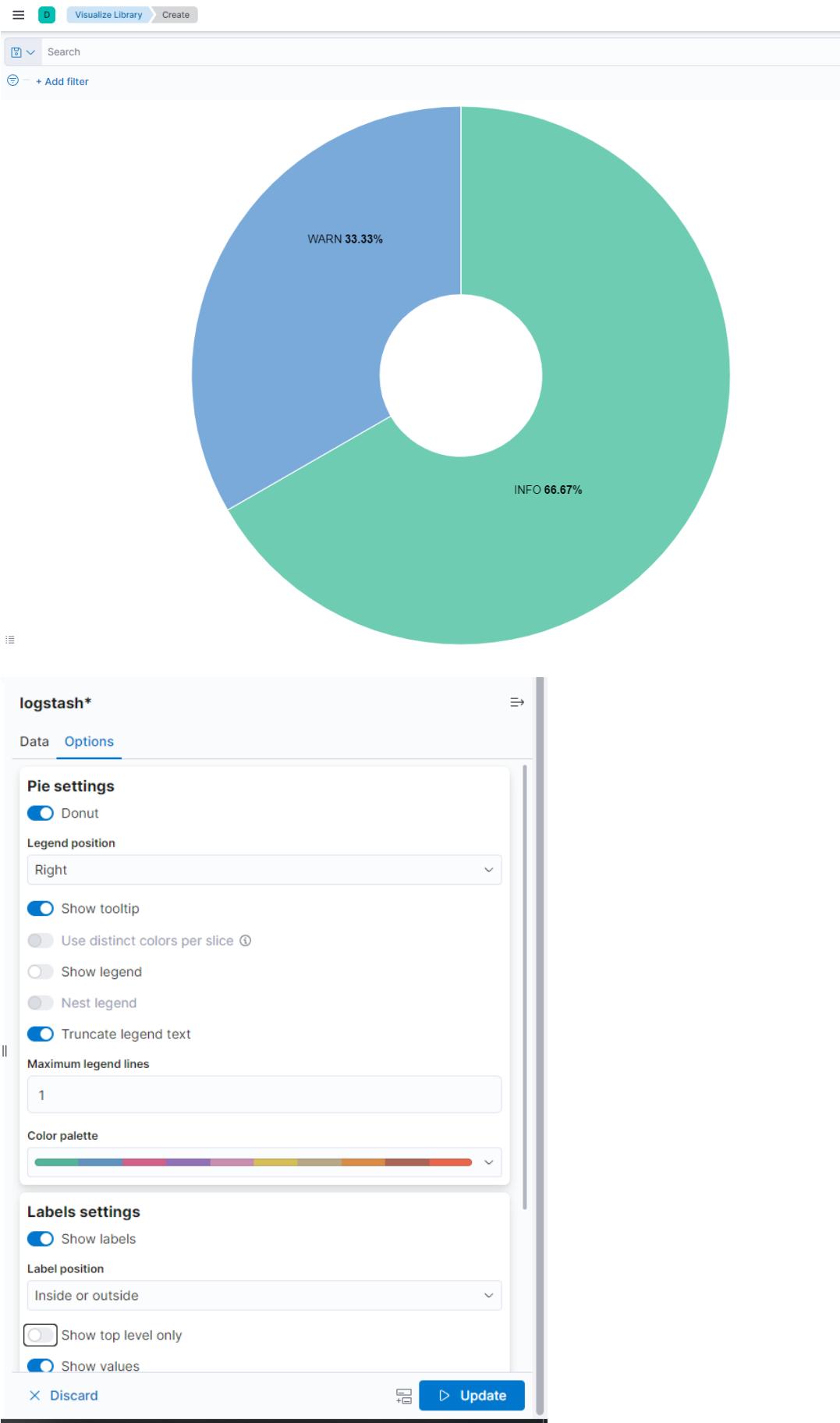
Show missing values

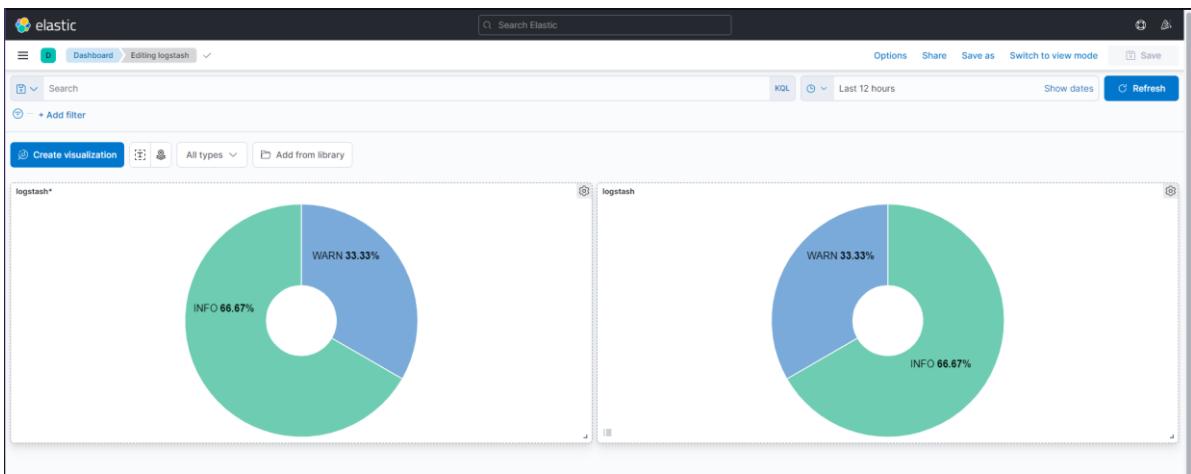
Custom label

> Advanced

✖ Discard

+ ↗ Update





Посмотрим данные в Elasticsearch с помощью GET запроса /имя\_индекса/\_search к любому узлу кластера. Добавление параметра pretty позволит отобразить данные в читабельном виде. По умолчанию вывод состоит из 10 записей, чтобы увеличить это количество необходимо использовать параметр size:

```

    "status" : 404
}
root@daryaki-VirtualBox:~# curl -X GET "http://172.20.10.13:9200/logstash-logs-2021.12/_search?pretty&size=100"
{
  "took" : 139,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 27,
      "relation" : "eq"
    },
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "logstash-logs-2021.12",
        "_type" : "_doc",
        "_id" : "lqm-dn0B3vq8nwCZ2XiR",
        "_score" : 1.0,
        "_source" : {
          "source" : "deprecation.logstash.codecs/plain",
          "path" : "/var/log/logstash/logstash-deprecation.log",
          "@timestamp" : "2021-12-01T16:05:58.048Z",
          "type" : "deprecation"
        }
      }
    ]
  }
}

```

```
atibility mode.",
    "severity" : "WARN",
    "@version" : "1",
    "timestamp" : "2021-12-01T19:05:48,909"
}
},
{
    "_index" : "logstash-logs-2021.12",
    "_type" : "_doc",
    "_id" : "l6m-dn0B3vq8nwCZ2XiR",
    "_score" : 1.0,
    "_source" : {
        "source" : "deprecation.logstash.inputs.file",
        "path" : "/var/log/logstash/logstash-deprecation.log",
        "@timestamp" : "2021-12-01T16:05:58.136Z",
        "host" : "daryaki-VirtualBox",
        "message" : "Relying on default value of `pipeline.ecs_compatibility` , which may change in a future major release of Logstash. To avoid unexpected changes when upgrading Logstash, please explicitly declare your desired ECS Compatibility mode.",
        "severity" : "WARN",
        "@version" : "1",
        "timestamp" : "2021-12-01T19:05:49,109"
}
},
{
    "_index" : "logstash-logs-2021.12",
    "_type" : "_doc",
    "_id" : "mKm-dn0B3vq8nwCZ2XiR",
```

## Вывод.

Была рассмотрена процедура установки и настройки Elasticsearch, Kibana и Logstash. Собраны первые данные с помощью Logstash, мы также посмотрели на данные с помощью Kibana Discover и построили первую визуализацию.