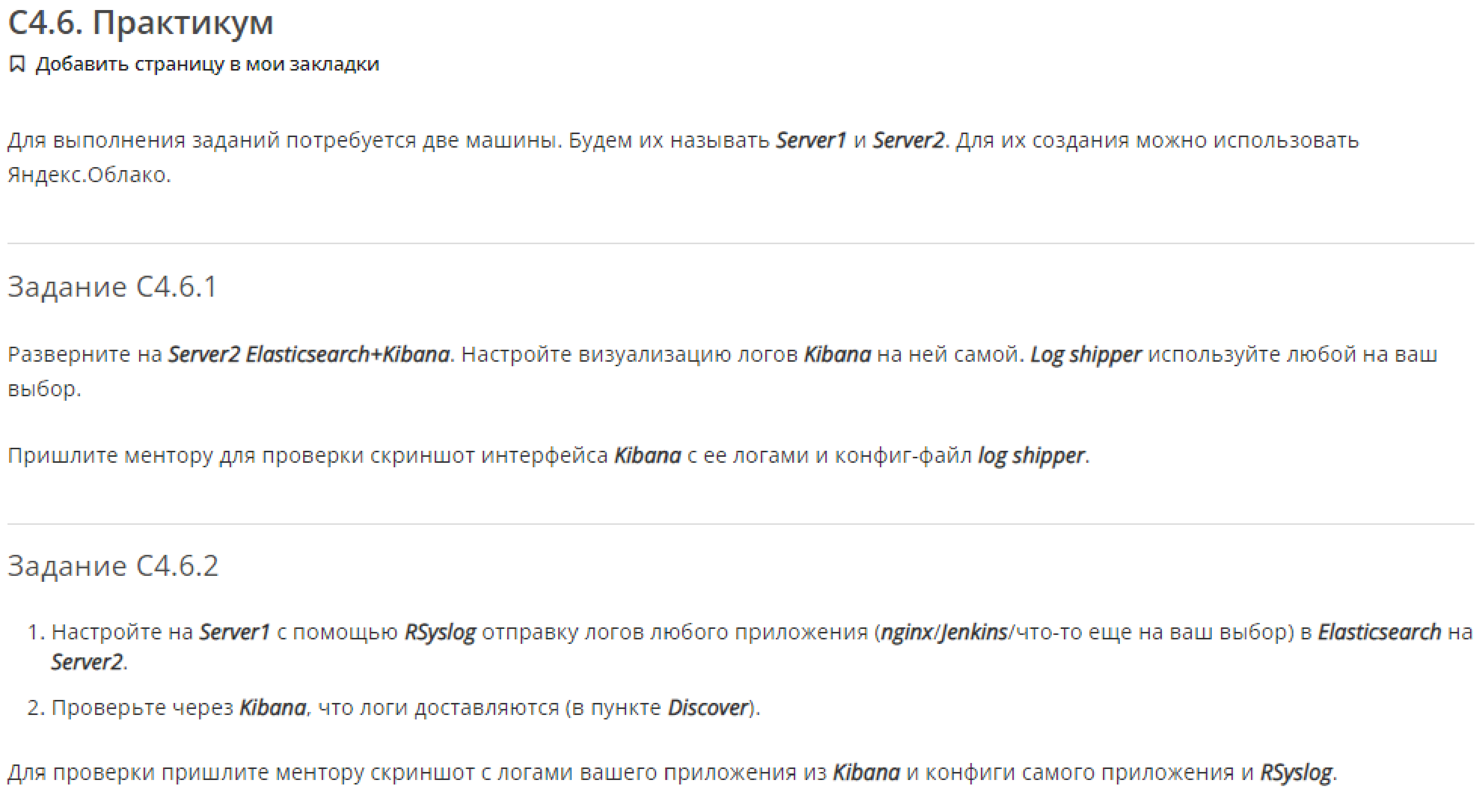
Module C4.6 Practical Work Report

Elasticsearch_Kibana_Logstash_Firebeat_RSyslog_NGINX



C4.6. Практикум

Добавить страницу в мои закладки

Для выполнения заданий потребуется две машины. Будем их называть ***Server1*** и ***Server2***. Для их создания можно использовать Яндекс.Облако.

Задание C4.6.1

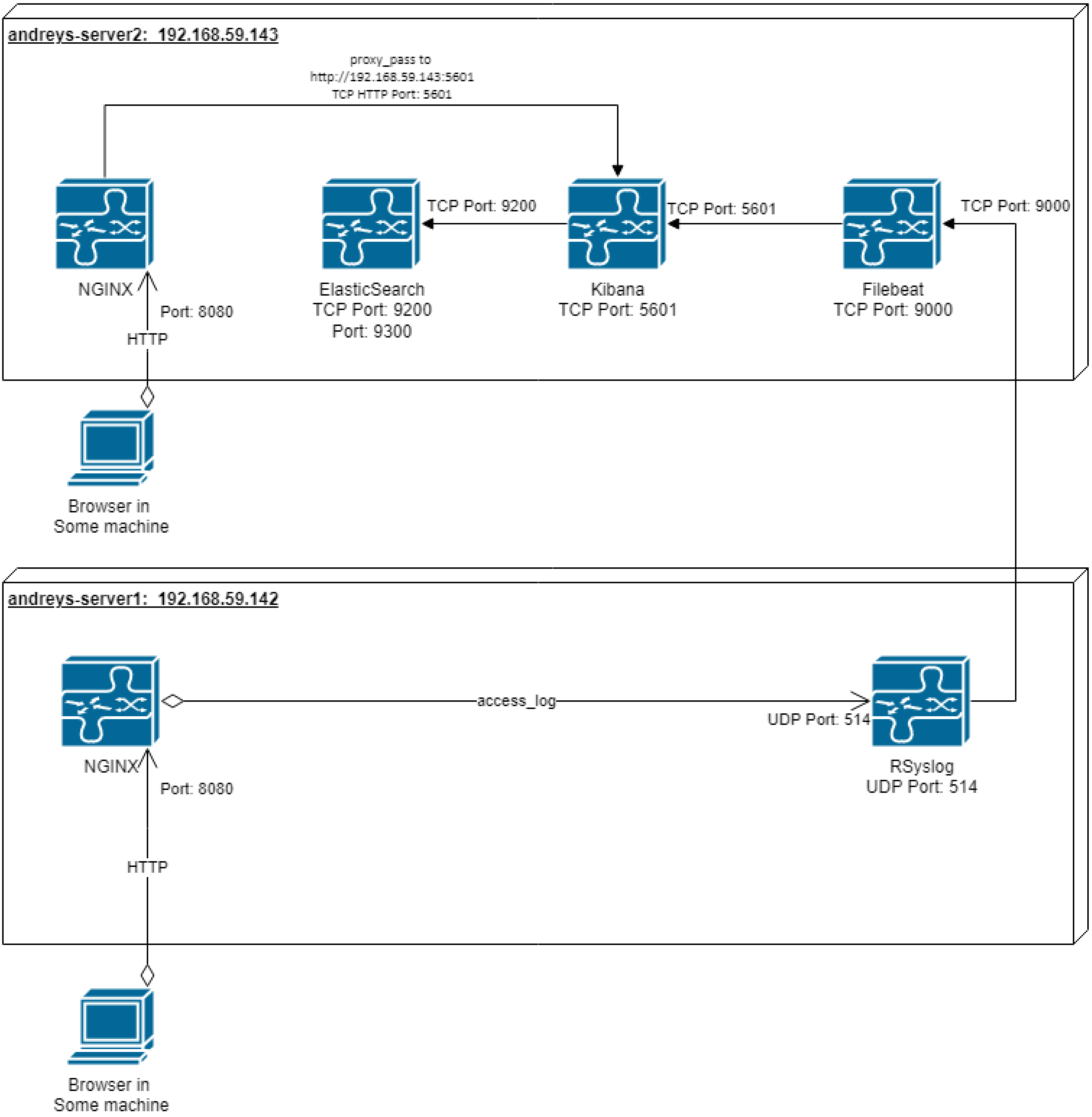
Разверните на ***Server2 Elasticsearch+Kibana***. Настройте визуализацию логов ***Kibana*** на ней самой. ***Log shipper*** используйте любой на ваш выбор.

Пришлите ментору для проверки скриншот интерфейса ***Kibana*** с ее логами и конфиг-файл ***log shipper***.

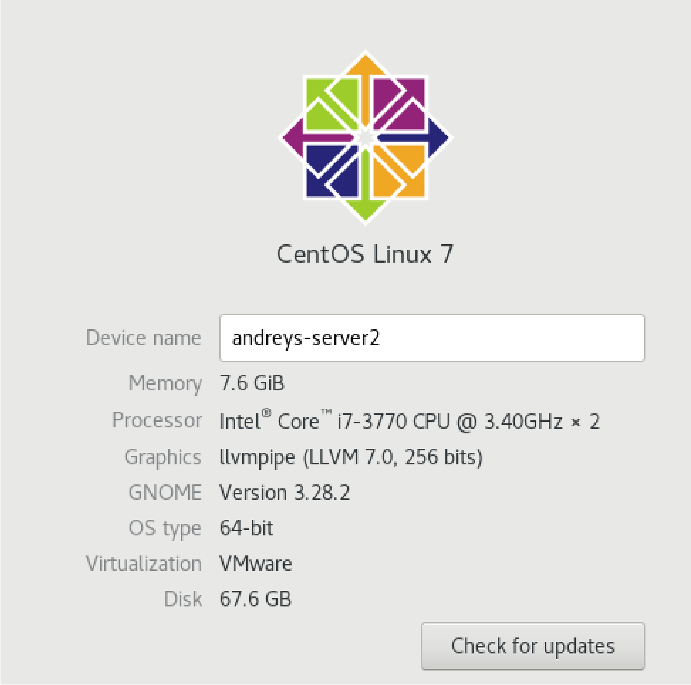
Задание C4.6.2

1. Настройте на ***Server1*** с помощью ***RSyslog*** отправку логов любого приложения (***nginx***/***Jenkins***/что-то еще на ваш выбор) в ***Elasticsearch*** на ***Server2***.
2. Проверьте через ***Kibana***, что логи доставляются (в пункте ***Discover***).

Для проверки пришлите ментору скриншот с логами вашего приложения из ***Kibana*** и конфиги самого приложения и ***RSyslog***.


andreys-server2: 192.168.59.143
proxy_pass to
http://192.168.59.143:5601
TCP HTTP Port: 5601
TCP Port: 9200
TCP Port: 5601
TCP Port: 9000
NGINX
Port: 8080
HTTP
ElasticSearch
TCP Port: 9200
Port: 9300
Kibana
TCP Port: 5601
Filebeat
TCP Port: 9000
Browser in
Some machine
andreys-server1: 192.168.59.142
access_log
UDP Port: 514
NGINX
Port: 8080
RSyslog
UDP Port: 514
HTTP
Browser in
Some machine

Server2 192.168.59.143



Device name andreys-server2

Memory 7.6 GiB

Processor Intel® Core™ i7-3770 CPU @ 3.40GHz × 2

Graphics llvmpipe (LLVM 7.0, 256 bits)

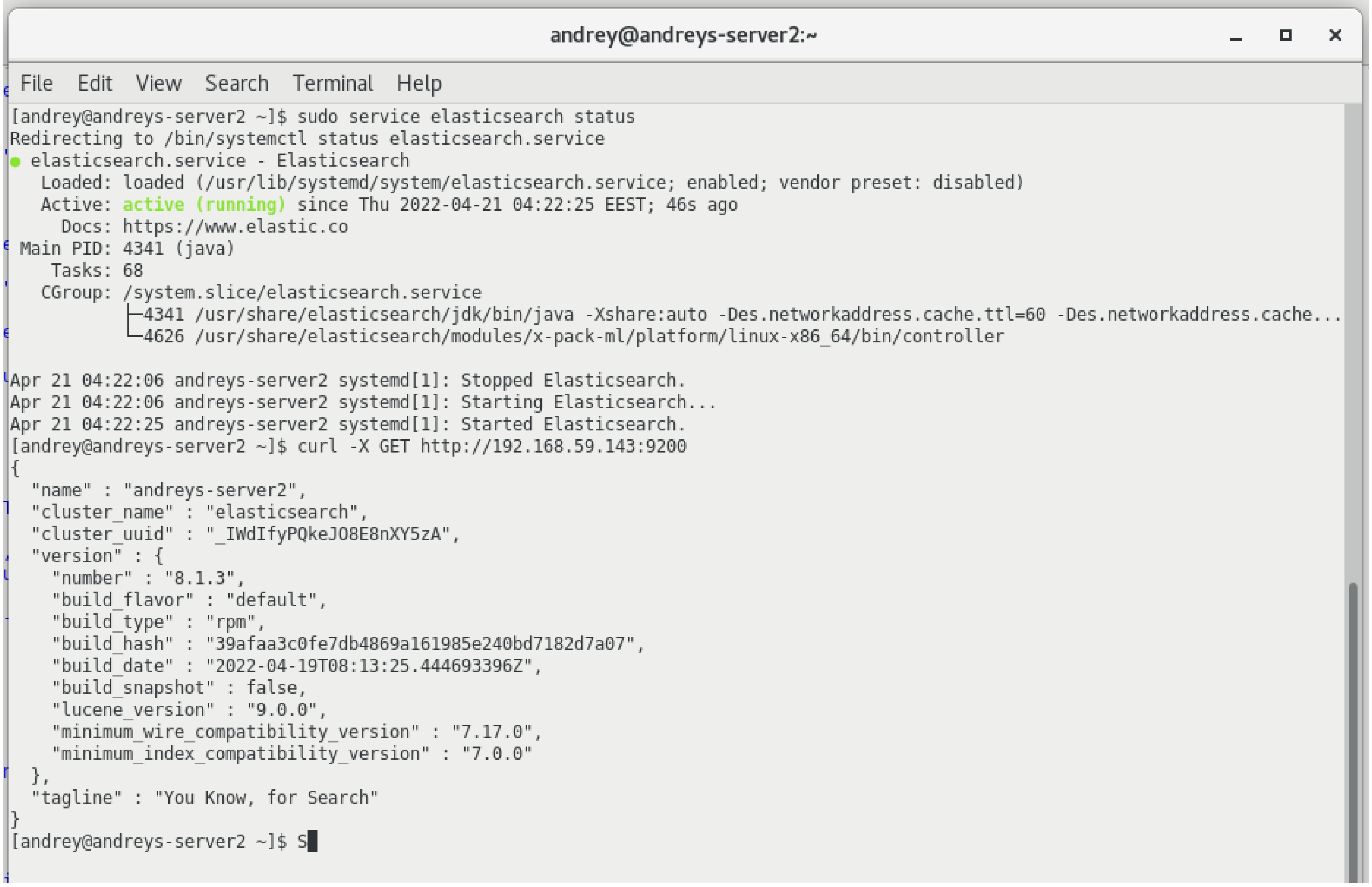
GNOME Version 3.28.2

OS type 64-bit

Virtualization VMware

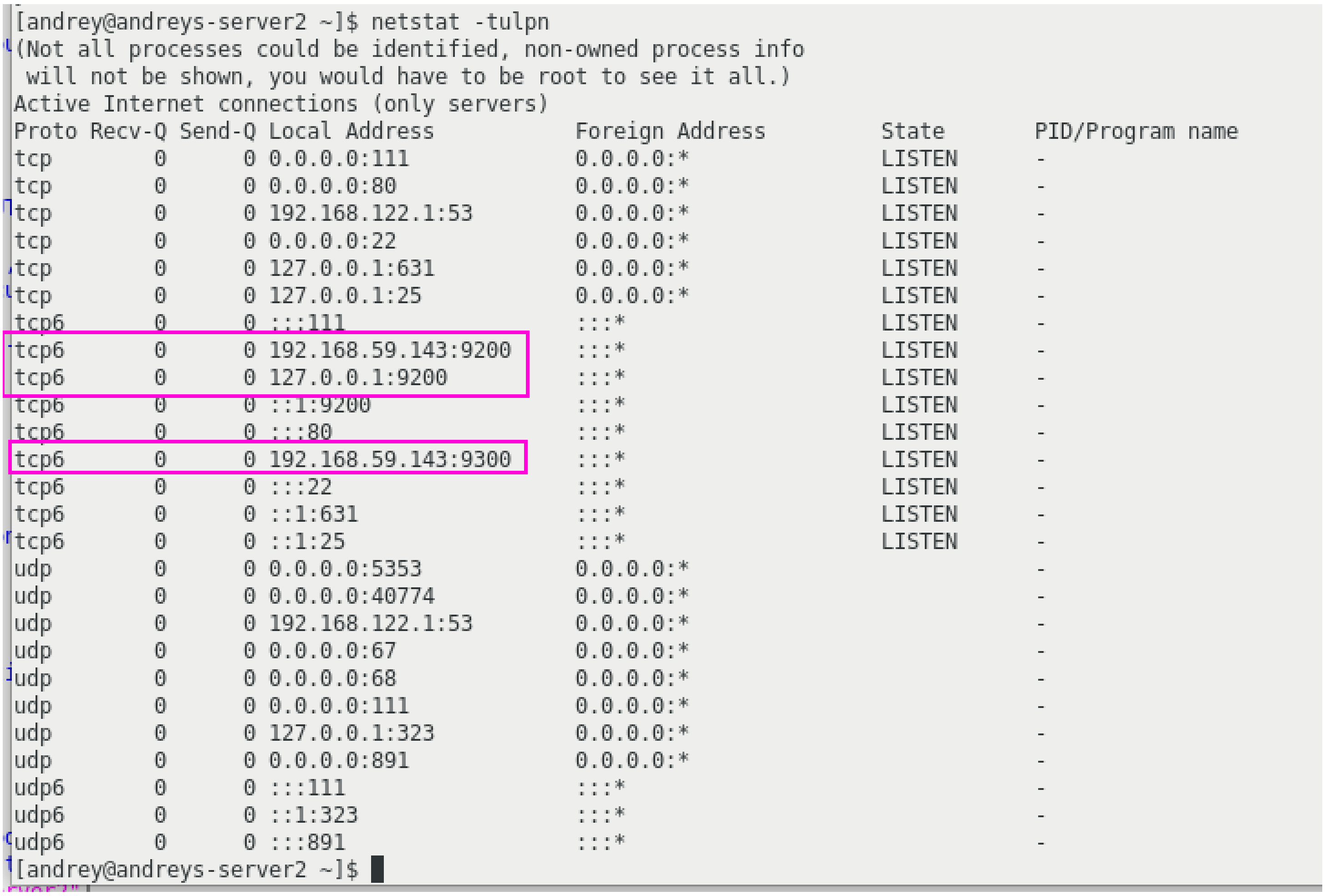
Disk 67.6 GB

ElasticSearch



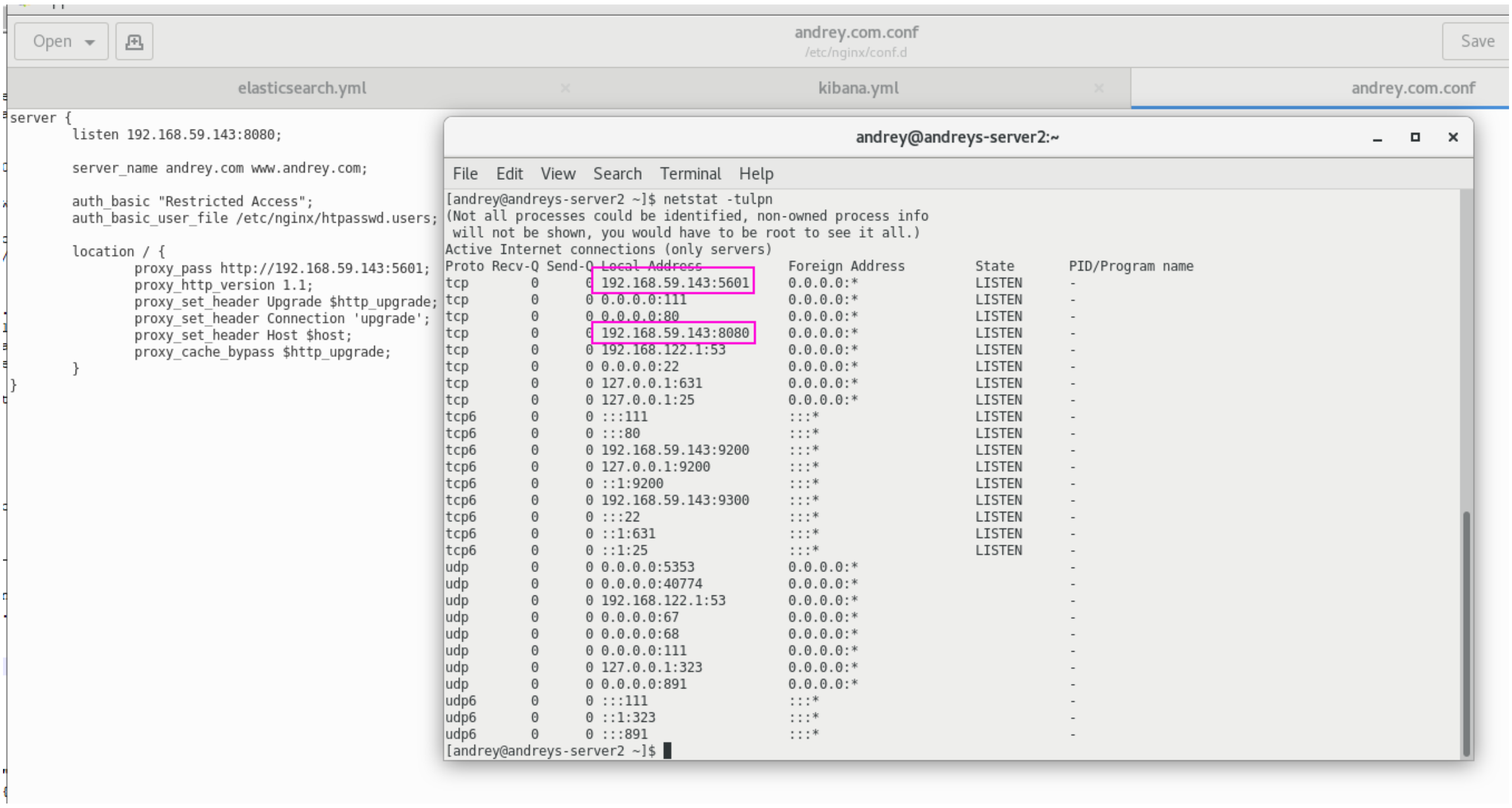
```
[andrey@andreys-server2 ~]$ sudo service elasticsearch status
Redirecting to /bin/systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2022-04-21 04:22:25 EEST; 46s ago
     Docs: https://www.elastic.co
 Main PID: 4341 (java)
    Tasks: 68
   CGroup: /system.slice/elasticsearch.service
           ├─4341 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache...
           └─4626 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Apr 21 04:22:06 andreys-server2 systemd[1]: Stopped Elasticsearch.
Apr 21 04:22:06 andreys-server2 systemd[1]: Starting Elasticsearch...
Apr 21 04:22:25 andreys-server2 systemd[1]: Started Elasticsearch.
[andrey@andreys-server2 ~]$ curl -X GET http://192.168.59.143:9200
{
  "name" : "andreys-server2",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "_IWdIfyPQkeJO8E8nXY5zA",
  "version" : {
    "number" : "8.1.3",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "39afaa3c0fe7db4869a161985e240bd7182d7a07",
    "build_date" : "2022-04-19T08:13:25.444693396Z",
    "build_snapshot" : false,
    "lucene_version" : "9.0.0",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
[andrey@andreys-server2 ~]$ S
```



```
[andrey@andreys-server2 ~]$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.122.1:53        0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
tcp6       0      0 :::111                  :::*                    LISTEN      -
tcp6       0      0 192.168.59.143:9200     :::*                    LISTEN      -
tcp6       0      0 127.0.0.1:9200          :::*                    LISTEN      -
tcp6       0      0 ::1:9200                :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 192.168.59.143:9300     :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
tcp6       0      0 ::1:25                  :::*                    LISTEN      -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
udp        0      0 0.0.0.0:40774           0.0.0.0:*                           -
udp        0      0 192.168.122.1:53        0.0.0.0:*                           -
udp        0      0 0.0.0.0:67              0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
udp        0      0 0.0.0.0:111             0.0.0.0:*                           -
udp        0      0 127.0.0.1:323           0.0.0.0:*                           -
udp        0      0 0.0.0.0:891             0.0.0.0:*                           -
udp6       0      0 :::111                  :::*                                -
udp6       0      0 ::1:323                 :::*                                -
udp6       0      0 :::891                  :::*                                -
[andrey@andreys-server2 ~]$
```

Kibana



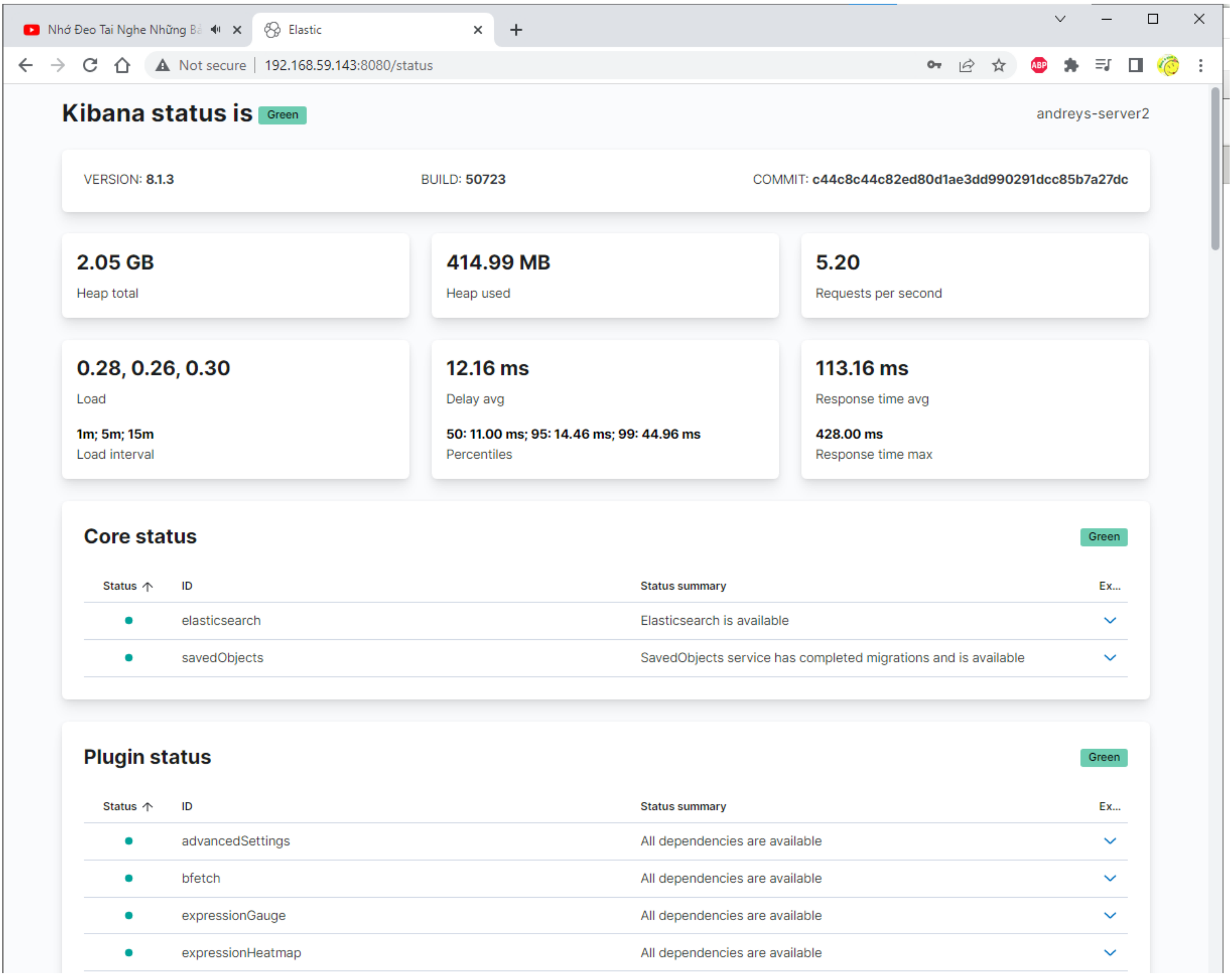
```
server {
        listen 192.168.59.143:8080;

        server_name andrey.com www.andrey.com;

        auth_basic "Restricted Access";
        auth_basic_user_file /etc/nginx/htpasswd.users;

        location / {
                proxy_pass http://192.168.59.143:5601;
                proxy_http_version 1.1;
                proxy_set_header Upgrade $http_upgrade;
                proxy_set_header Connection 'upgrade';
                proxy_set_header Host $host;
                proxy_cache_bypass $http_upgrade;
        }
}
```

```
[andrey@andreys-server2 ~]$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 192.168.59.143:5601     0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.59.143:8080     0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.122.1:53        0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
tcp6       0      0 :::111                  :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 192.168.59.143:9200     :::*                    LISTEN      -
tcp6       0      0 127.0.0.1:9200          :::*                    LISTEN      -
tcp6       0      0 ::1:9200                :::*                    LISTEN      -
tcp6       0      0 192.168.59.143:9300     :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
tcp6       0      0 ::1:25                  :::*                    LISTEN      -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
udp        0      0 0.0.0.0:40774           0.0.0.0:*                           -
udp        0      0 192.168.122.1:53        0.0.0.0:*                           -
udp        0      0 0.0.0.0:67              0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
udp        0      0 0.0.0.0:111             0.0.0.0:*                           -
udp        0      0 127.0.0.1:323           0.0.0.0:*                           -
udp        0      0 0.0.0.0:891             0.0.0.0:*                           -
udp6       0      0 :::111                  :::*                                -
udp6       0      0 ::1:323                 :::*                                -
udp6       0      0 :::891                  :::*                                -
[andrey@andreys-server2 ~]$
```



Nhớ Đeo Tai Nghe Những Bà
Elastic
Not secure | 192.168.59.143:8080/status

Kibana status is Green

andreys-server2

VERSION: 8.1.3 BUILD: 50723 COMMIT: c44c8c44c82ed80d1ae3dd990291dcc85b7a27dc

2.05 GB
Heap total

414.99 MB
Heap used

5.20
Requests per second

0.28, 0.26, 0.30
Load

1m; 5m; 15m
Load interval

12.16 ms
Delay avg

50: 11.00 ms; 95: 14.46 ms; 99: 44.96 ms
Percentiles

113.16 ms
Response time avg

428.00 ms
Response time max

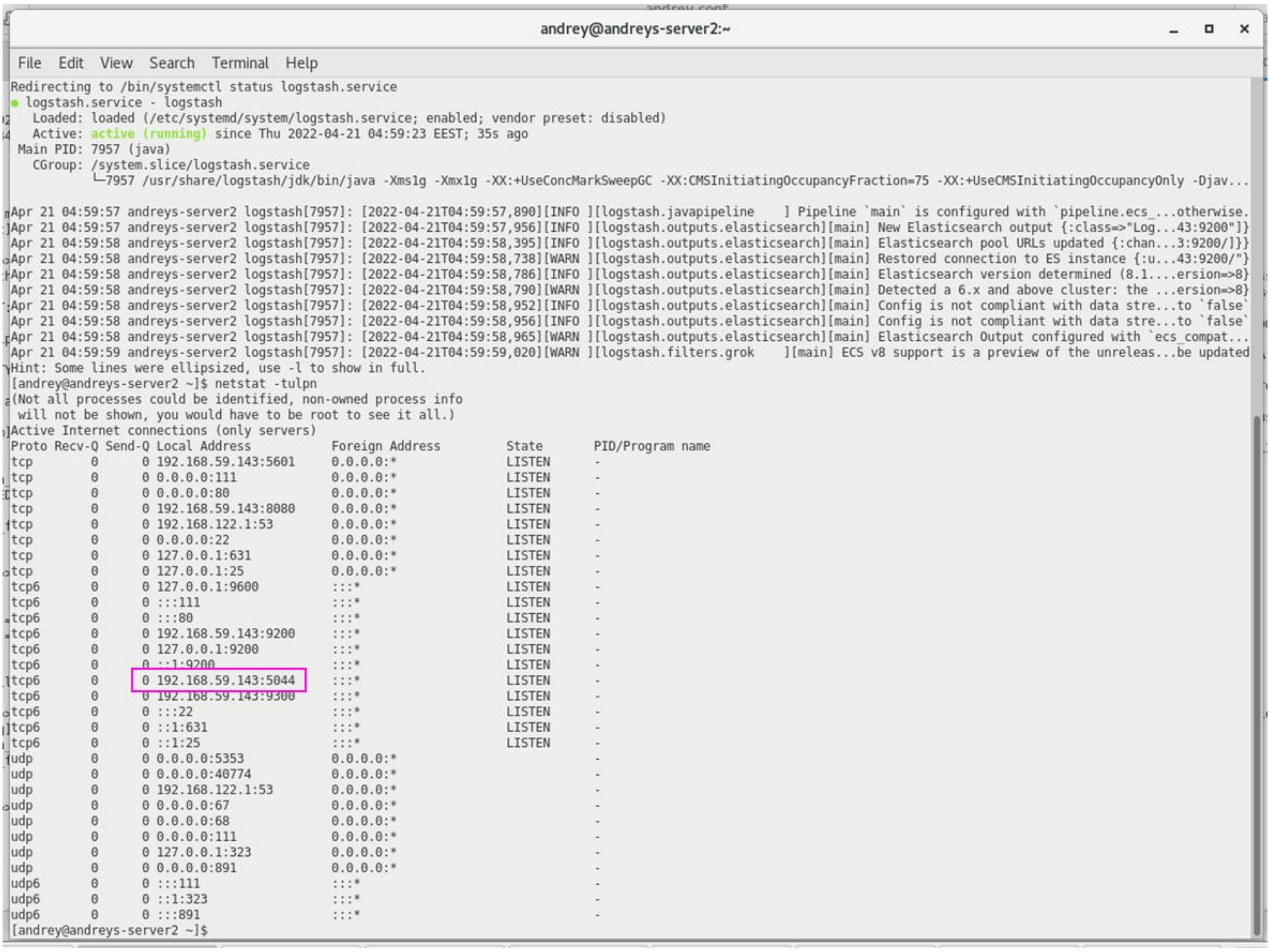
Core status Green

Status ↑	ID	Status summary	Ex...
●	elasticsearch	Elasticsearch is available	⌄
●	savedObjects	SavedObjects service has completed migrations and is available	⌄

Plugin status Green

Status ↑	ID	Status summary	Ex...
●	advancedSettings	All dependencies are available	⌄
●	bfetch	All dependencies are available	⌄
●	expressionGauge	All dependencies are available	⌄
●	expressionHeatmap	All dependencies are available	⌄

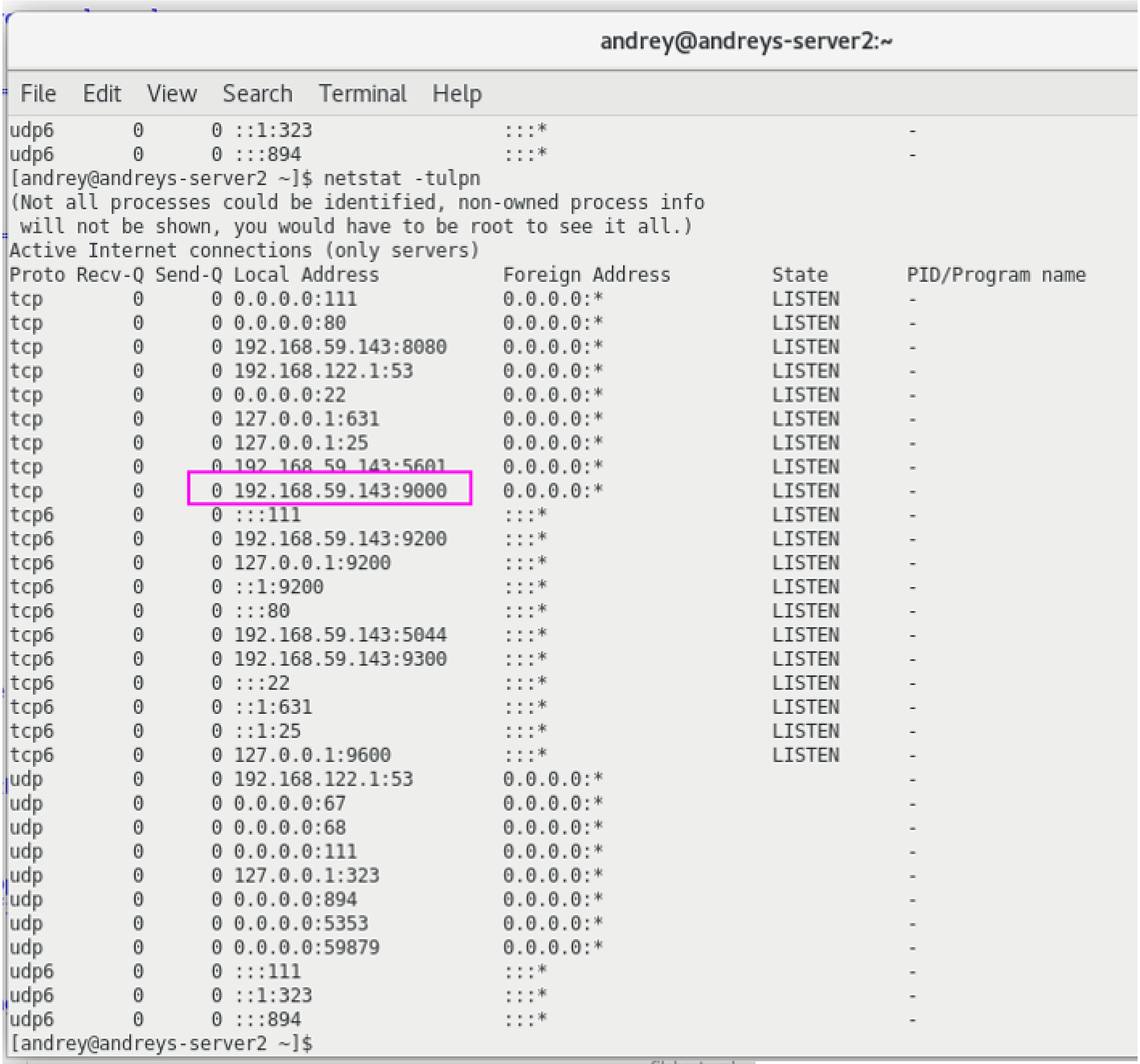
LOGSTASH



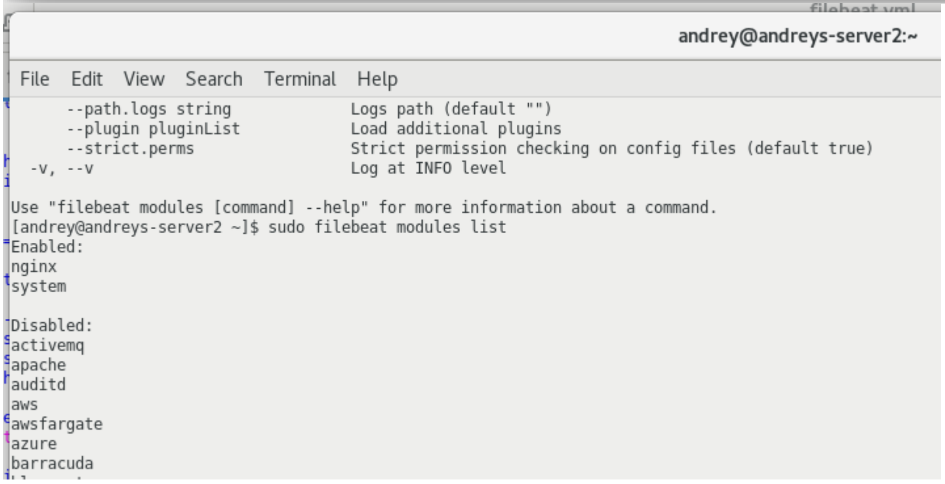
```
Redirecting to /bin/systemctl status logstash.service
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2022-04-21 04:59:23 EEST; 35s ago
 Main PID: 7957 (java)
   CGroup: /system.slice/logstash.service
           └─7957 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -Djav...

Apr 21 04:59:57 andreys-server2 logstash[7957]: [2022-04-21T04:59:57,890][INFO ][logstash.javapipeline    ] Pipeline `main` is configured with `pipeline.ecs_...otherwise.
Apr 21 04:59:57 andreys-server2 logstash[7957]: [2022-04-21T04:59:57,956][INFO ][logstash.outputs.elasticsearch][main] New Elasticsearch output {:class=>"Log...43:9200"]}
Apr 21 04:59:58 andreys-server2 logstash[7957]: [2022-04-21T04:59:58,395][INFO ][logstash.outputs.elasticsearch][main] Elasticsearch pool URLs updated {:chan...3:9200/]}}
Apr 21 04:59:58 andreys-server2 logstash[7957]: [2022-04-21T04:59:58,738][WARN ][logstash.outputs.elasticsearch][main] Restored connection to ES instance {:u...43:9200/"}
Apr 21 04:59:58 andreys-server2 logstash[7957]: [2022-04-21T04:59:58,786][INFO ][logstash.outputs.elasticsearch][main] Elasticsearch version determined (8.1....ersion=>8}
Apr 21 04:59:58 andreys-server2 logstash[7957]: [2022-04-21T04:59:58,790][WARN ][logstash.outputs.elasticsearch][main] Detected a 6.x and above cluster: the ...ersion=>8}
Apr 21 04:59:58 andreys-server2 logstash[7957]: [2022-04-21T04:59:58,952][INFO ][logstash.outputs.elasticsearch][main] Config is not compliant with data stre...to `false`
Apr 21 04:59:58 andreys-server2 logstash[7957]: [2022-04-21T04:59:58,956][INFO ][logstash.outputs.elasticsearch][main] Config is not compliant with data stre...to `false`
Apr 21 04:59:58 andreys-server2 logstash[7957]: [2022-04-21T04:59:58,965][WARN ][logstash.outputs.elasticsearch][main] Elasticsearch Output configured with `ecs_compat...
Apr 21 04:59:59 andreys-server2 logstash[7957]: [2022-04-21T04:59:59,020][WARN ][logstash.filters.grok    ][main] ECS v8 support is a preview of the unreleas...be updated
Hint: Some lines were ellipsized, use -l to show in full.
[andrey@andreys-server2 ~]$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 192.168.59.143:5601     0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.59.143:8080     0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.122.1:53        0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
tcp6       0      0 127.0.0.1:9600          :::*                    LISTEN      -
tcp6       0      0 :::111                  :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 192.168.59.143:9200     :::*                    LISTEN      -
tcp6       0      0 127.0.0.1:9200          :::*                    LISTEN      -
tcp6       0      0 ::1:9200                :::*                    LISTEN      -
tcp6       0      0 192.168.59.143:5044     :::*                    LISTEN      -
tcp6       0      0 192.168.59.143:9300     :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
tcp6       0      0 ::1:25                  :::*                    LISTEN      -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
udp        0      0 0.0.0.0:40774           0.0.0.0:*                           -
udp        0      0 192.168.122.1:53        0.0.0.0:*                           -
udp        0      0 0.0.0.0:67              0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
udp        0      0 0.0.0.0:111             0.0.0.0:*                           -
udp        0      0 127.0.0.1:323           0.0.0.0:*                           -
udp        0      0 0.0.0.0:891             0.0.0.0:*                           -
udp6       0      0 :::111                  :::*                                -
udp6       0      0 ::1:323                 :::*                                -
udp6       0      0 :::891                  :::*                                -
[andrey@andreys-server2 ~]$
```

FILEBEAT



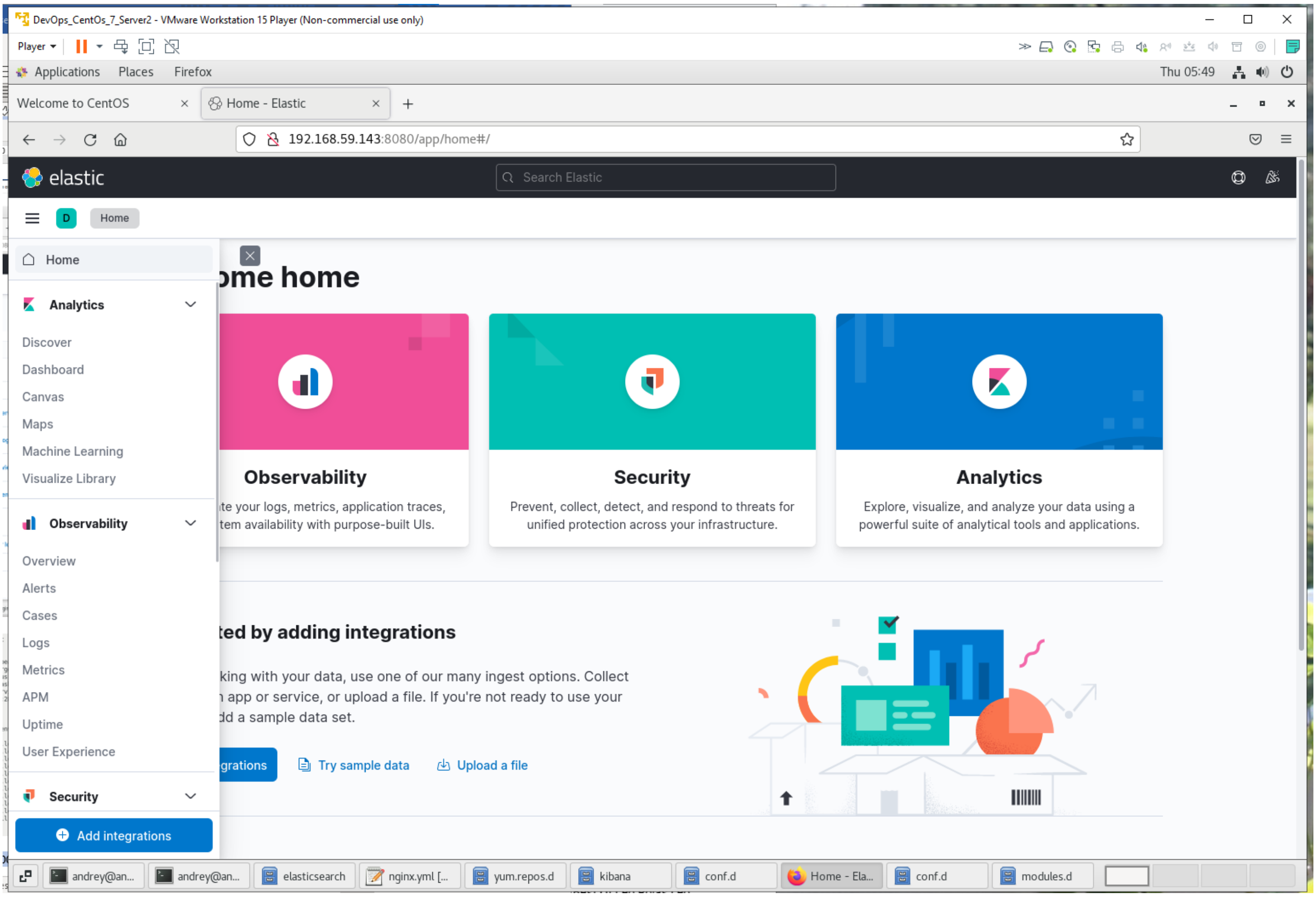
```
udp6       0      0 ::1:323                 :::*                                -
udp6       0      0 :::894                  :::*                                -
[andrey@andreys-server2 ~]$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.59.143:8080     0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.122.1:53        0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.59.143:5601     0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.59.143:9000     0.0.0.0:*               LISTEN      -
tcp6       0      0 :::111                  :::*                    LISTEN      -
tcp6       0      0 192.168.59.143:9200     :::*                    LISTEN      -
tcp6       0      0 127.0.0.1:9200          :::*                    LISTEN      -
tcp6       0      0 ::1:9200                :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 192.168.59.143:5044     :::*                    LISTEN      -
tcp6       0      0 192.168.59.143:9300     :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
tcp6       0      0 ::1:25                  :::*                    LISTEN      -
tcp6       0      0 127.0.0.1:9600          :::*                    LISTEN      -
udp        0      0 192.168.122.1:53        0.0.0.0:*                           -
udp        0      0 0.0.0.0:67              0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
udp        0      0 0.0.0.0:111             0.0.0.0:*                           -
udp        0      0 127.0.0.1:323           0.0.0.0:*                           -
udp        0      0 0.0.0.0:894             0.0.0.0:*                           -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
udp        0      0 0.0.0.0:59879           0.0.0.0:*                           -
udp6       0      0 :::111                  :::*                                -
udp6       0      0 ::1:323                 :::*                                -
udp6       0      0 :::894                  :::*                                -
[andrey@andreys-server2 ~]$
```



```
      --path.logs string            Logs path (default "")
      --plugin pluginList           Load additional plugins
      --strict.perms                Strict permission checking on config files (default true)
  -v, --v                           Log at INFO level

Use "filebeat modules [command] --help" for more information about a command.
[andrey@andreys-server2 ~]$ sudo filebeat modules list
Enabled:
nginx
system

Disabled:
activemq
apache
auditd
aws
awsfargate
azure
barracuda
```

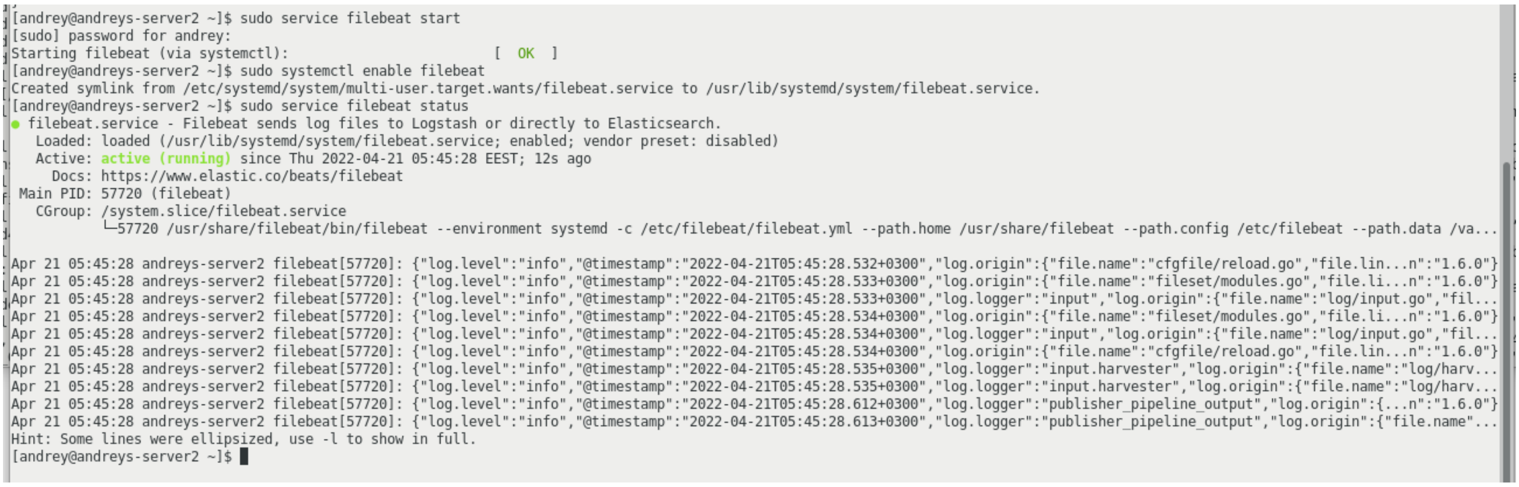


te your logs, metrics, application traces,
tem availability with purpose-built UIs.

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

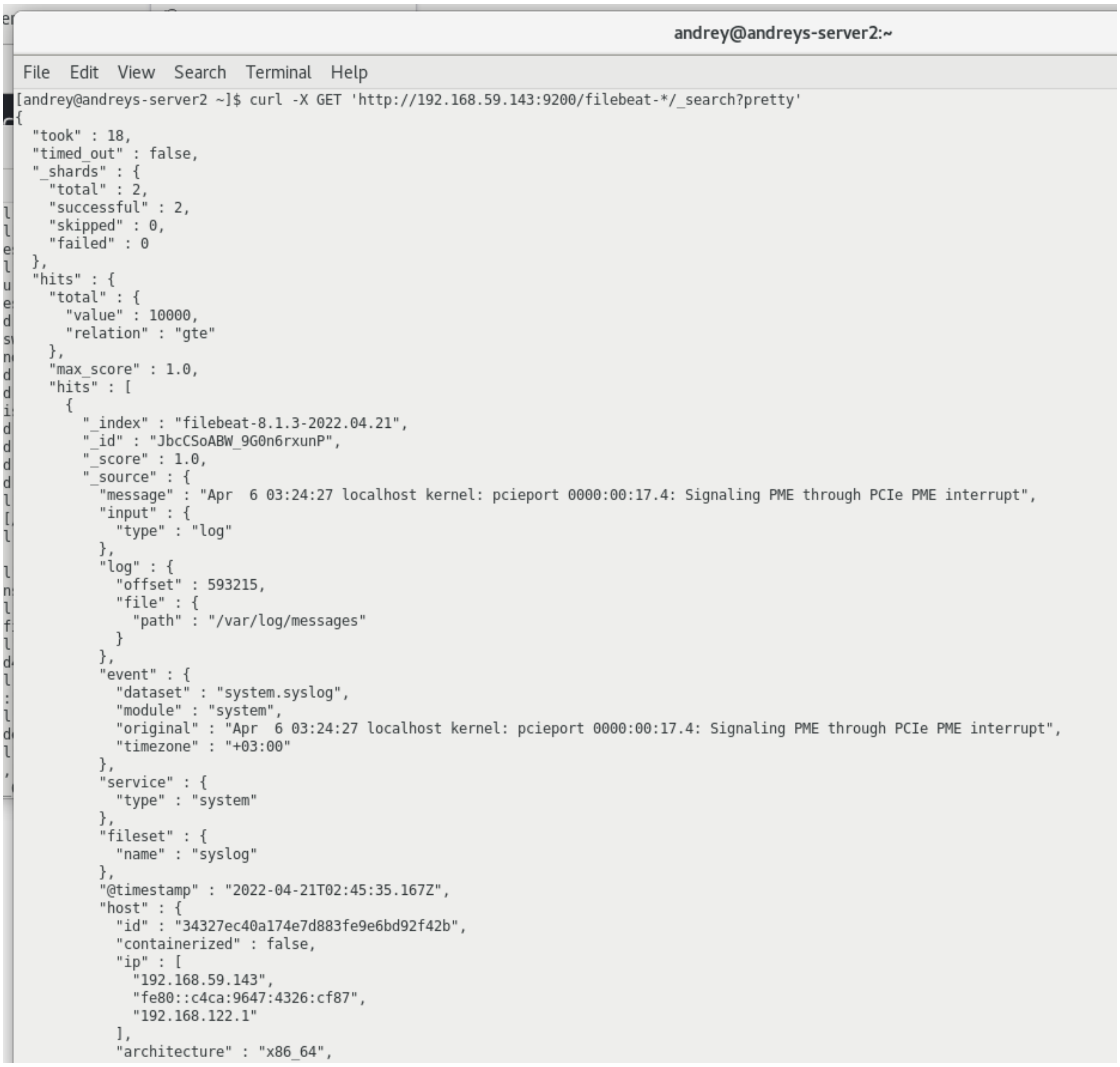
Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

king with your data, use one of our many ingest options. Collect
 app or service, or upload a file. If you're not ready to use your
dd a sample data set.



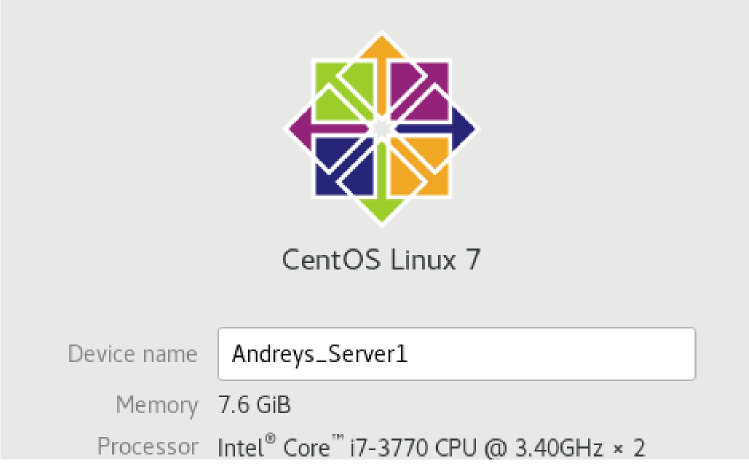
```
[andrey@andreys-server2 ~]$ sudo service filebeat start
[sudo] password for andrey:
Starting filebeat (via systemctl):                         [  OK  ]
[andrey@andreys-server2 ~]$ sudo systemctl enable filebeat
Created symlink from /etc/systemd/system/multi-user.target.wants/filebeat.service to /usr/lib/systemd/system/filebeat.service.
[andrey@andreys-server2 ~]$ sudo service filebeat status
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
   Loaded: loaded (/usr/lib/systemd/system/filebeat.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2022-04-21 05:45:28 EEST; 12s ago
     Docs: https://www.elastic.co/beats/filebeat
 Main PID: 57720 (filebeat)
   CGroup: /system.slice/filebeat.service
           └─57720 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/filebeat.yml --path.home /usr/share/filebeat --path.config /etc/filebeat --path.data /va...

Apr 21 05:45:28 andreys-server2 filebeat[57720]: {"log.level":"info","@timestamp":"2022-04-21T05:45:28.532+0300","log.origin":{"file.name":"cfgfile/reload.go","file.lin...n":"1.6.0"}
Apr 21 05:45:28 andreys-server2 filebeat[57720]: {"log.level":"info","@timestamp":"2022-04-21T05:45:28.533+0300","log.origin":{"file.name":"fileset/modules.go","file.li...n":"1.6.0"}
Apr 21 05:45:28 andreys-server2 filebeat[57720]: {"log.level":"info","@timestamp":"2022-04-21T05:45:28.533+0300","log.logger":"input","log.origin":{"file.name":"log/input.go","fil...
Apr 21 05:45:28 andreys-server2 filebeat[57720]: {"log.level":"info","@timestamp":"2022-04-21T05:45:28.534+0300","log.origin":{"file.name":"fileset/modules.go","file.li...n":"1.6.0"}
Apr 21 05:45:28 andreys-server2 filebeat[57720]: {"log.level":"info","@timestamp":"2022-04-21T05:45:28.534+0300","log.logger":"input","log.origin":{"file.name":"log/input.go","fil...
Apr 21 05:45:28 andreys-server2 filebeat[57720]: {"log.level":"info","@timestamp":"2022-04-21T05:45:28.534+0300","log.origin":{"file.name":"cfgfile/reload.go","file.lin...n":"1.6.0"}
Apr 21 05:45:28 andreys-server2 filebeat[57720]: {"log.level":"info","@timestamp":"2022-04-21T05:45:28.535+0300","log.logger":"input.harvester","log.origin":{"file.name":"log/harv...
Apr 21 05:45:28 andreys-server2 filebeat[57720]: {"log.level":"info","@timestamp":"2022-04-21T05:45:28.535+0300","log.logger":"input.harvester","log.origin":{"file.name":"log/harv...
Apr 21 05:45:28 andreys-server2 filebeat[57720]: {"log.level":"info","@timestamp":"2022-04-21T05:45:28.612+0300","log.logger":"publisher_pipeline_output","log.origin":{...n":"1.6.0"}
Apr 21 05:45:28 andreys-server2 filebeat[57720]: {"log.level":"info","@timestamp":"2022-04-21T05:45:28.613+0300","log.logger":"publisher_pipeline_output","log.origin":{"file.name"...
Hint: Some lines were ellipsized, use -l to show in full.
[andrey@andreys-server2 ~]$
```



```
[andrey@andreys-server2 ~]$ curl -X GET 'http://192.168.59.143:9200/filebeat-*/_search?pretty'
{
  "took" : 18,
  "timed_out" : false,
  "_shards" : {
    "total" : 2,
    "successful" : 2,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 10000,
      "relation" : "gte"
    },
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "filebeat-8.1.3-2022.04.21",
        "_id" : "JbcCSoABW_9G0n6rxunP",
        "_score" : 1.0,
        "_source" : {
          "message" : "Apr  6 03:24:27 localhost kernel: pcieport 0000:00:17.4: Signaling PME through PCIe PME interrupt",
          "input" : {
            "type" : "log"
          },
          "log" : {
            "offset" : 593215,
            "file" : {
              "path" : "/var/log/messages"
            }
          },
          "event" : {
            "dataset" : "system.syslog",
            "module" : "system",
            "original" : "Apr  6 03:24:27 localhost kernel: pcieport 0000:00:17.4: Signaling PME through PCIe PME interrupt",
            "timezone" : "+03:00"
          },
          "service" : {
            "type" : "system"
          },
          "fileset" : {
            "name" : "syslog"
          },
          "@timestamp" : "2022-04-21T02:45:35.167Z",
          "host" : {
            "id" : "34327ec40a174e7d883fe9e6bd92f42b",
            "containerized" : false,
            "ip" : [
              "192.168.59.143",
              "fe80::c4ca:9647:4326:cf87",
              "192.168.122.1"
            ],
            "architecture" : "x86_64",
```

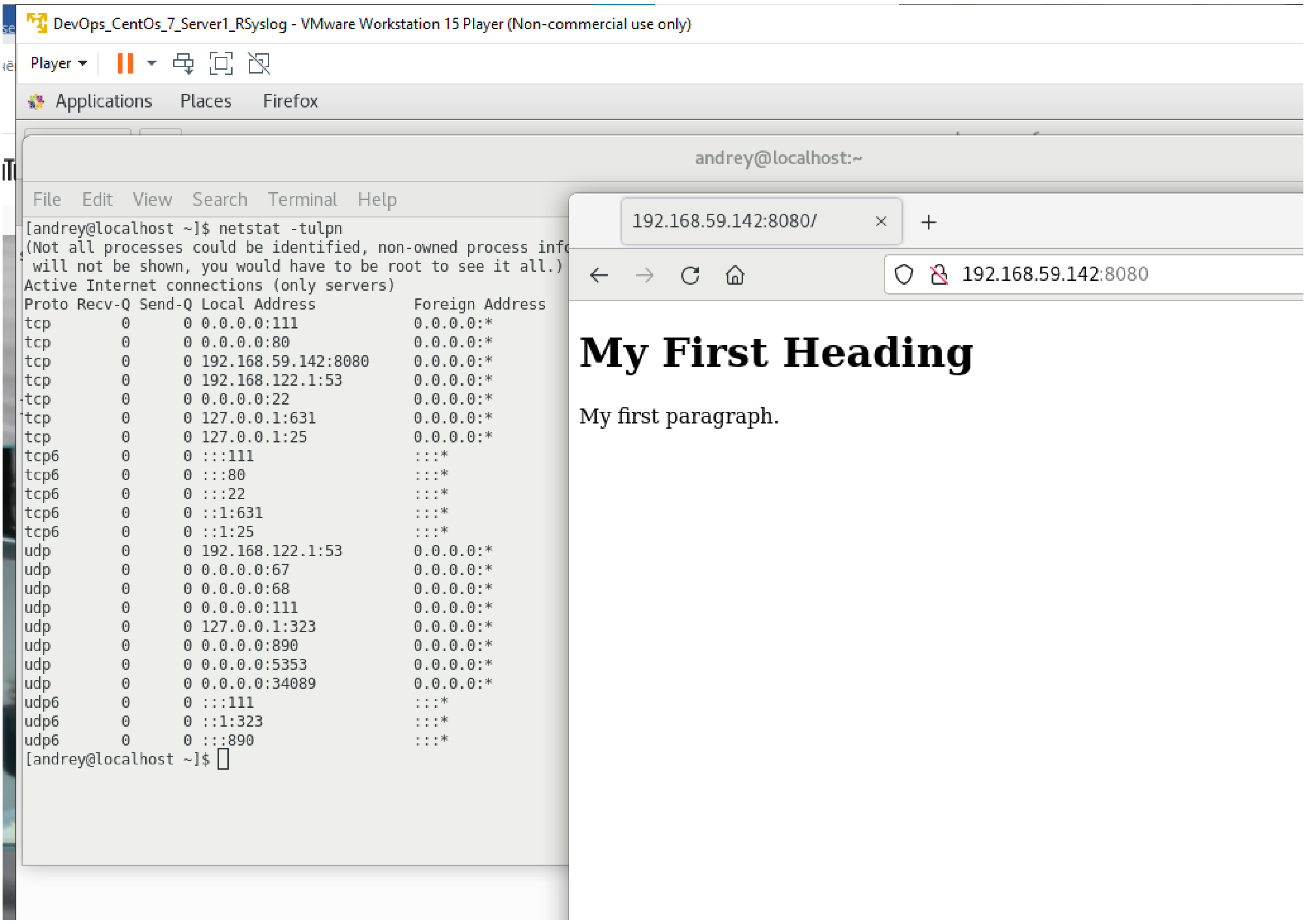
Server1 192.168.59.142


CentOS Linux 7

Device name Andreys_Server1

Memory 7.6 GiB

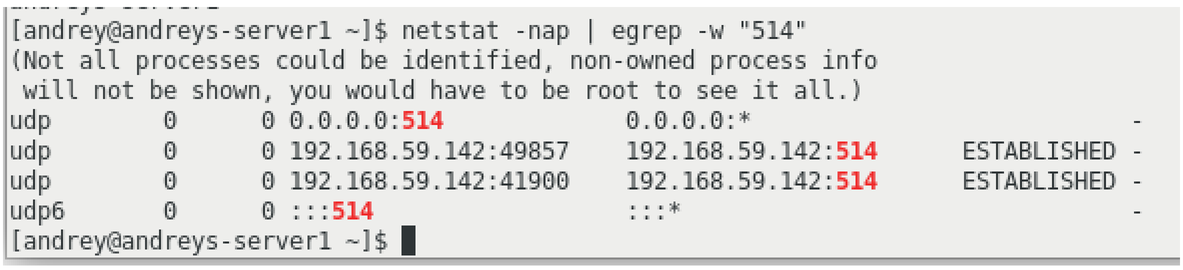
Processor Intel® Core™ i7-3770 CPU @ 3.40GHz × 2



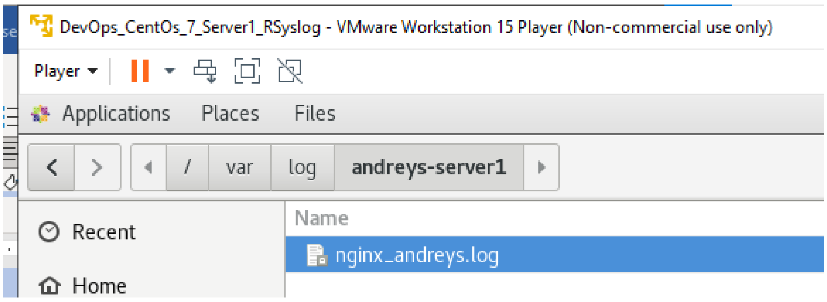
```
[andrey@localhost ~]$ netstat -tulpn
(Not all processes could be identified, non-owned process inf
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address
tcp        0      0 0.0.0.0:111             0.0.0.0:*
tcp        0      0 0.0.0.0:80              0.0.0.0:*
tcp        0      0 192.168.59.142:8080     0.0.0.0:*
tcp        0      0 192.168.122.1:53        0.0.0.0:*
tcp        0      0 0.0.0.0:22              0.0.0.0:*
tcp        0      0 127.0.0.1:631           0.0.0.0:*
tcp        0      0 127.0.0.1:25            0.0.0.0:*
tcp6       0      0 :::111                  :::*
tcp6       0      0 :::80                   :::*
tcp6       0      0 :::22                   :::*
tcp6       0      0 ::1:631                 :::*
tcp6       0      0 ::1:25                  :::*
udp        0      0 192.168.122.1:53        0.0.0.0:*
udp        0      0 0.0.0.0:67              0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 0.0.0.0:111             0.0.0.0:*
udp        0      0 127.0.0.1:323           0.0.0.0:*
udp        0      0 0.0.0.0:890             0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:34089           0.0.0.0:*
udp6       0      0 :::111                  :::*
udp6       0      0 ::1:323                 :::*
udp6       0      0 :::890                  :::*
[andrey@localhost ~]$
```

My First Heading

My first paragraph.

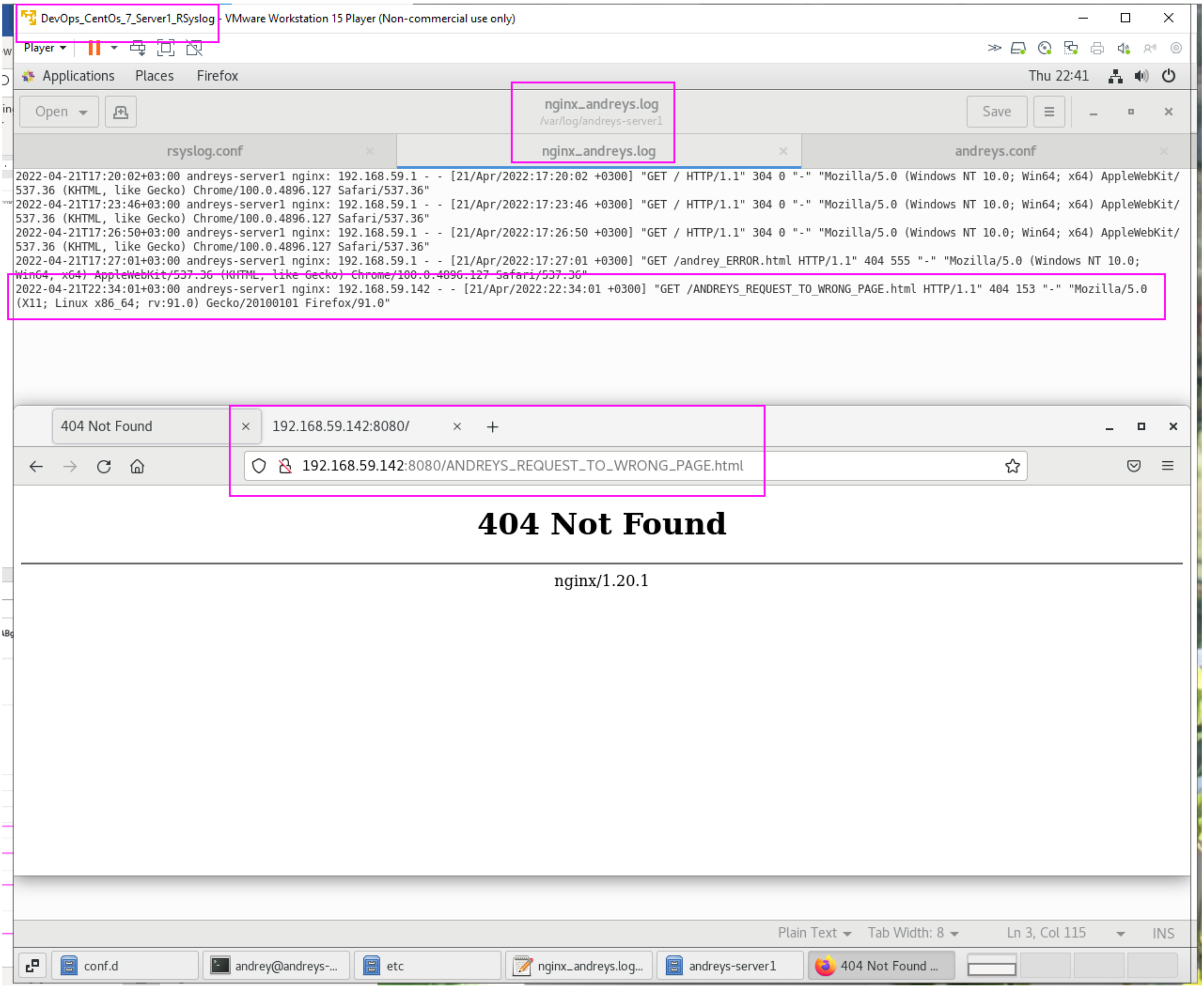


```
[andrey@andreys-server1 ~]$ netstat -nap | egrep -w "514"
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
udp        0      0 0.0.0.0:514             0.0.0.0:*                           -
udp        0      0 192.168.59.142:49857    192.168.59.142:514      ESTABLISHED -
udp        0      0 192.168.59.142:41900    192.168.59.142:514      ESTABLISHED -
udp6       0      0 :::514                  :::*                                -
[andrey@andreys-server1 ~]$
```



DevOps_CentOs_7_Server1_RSyslog - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Places
Files
/
var
log
andreys-server1
Recent
Home
Name
nginx_andreys.log

FINAL TESTING

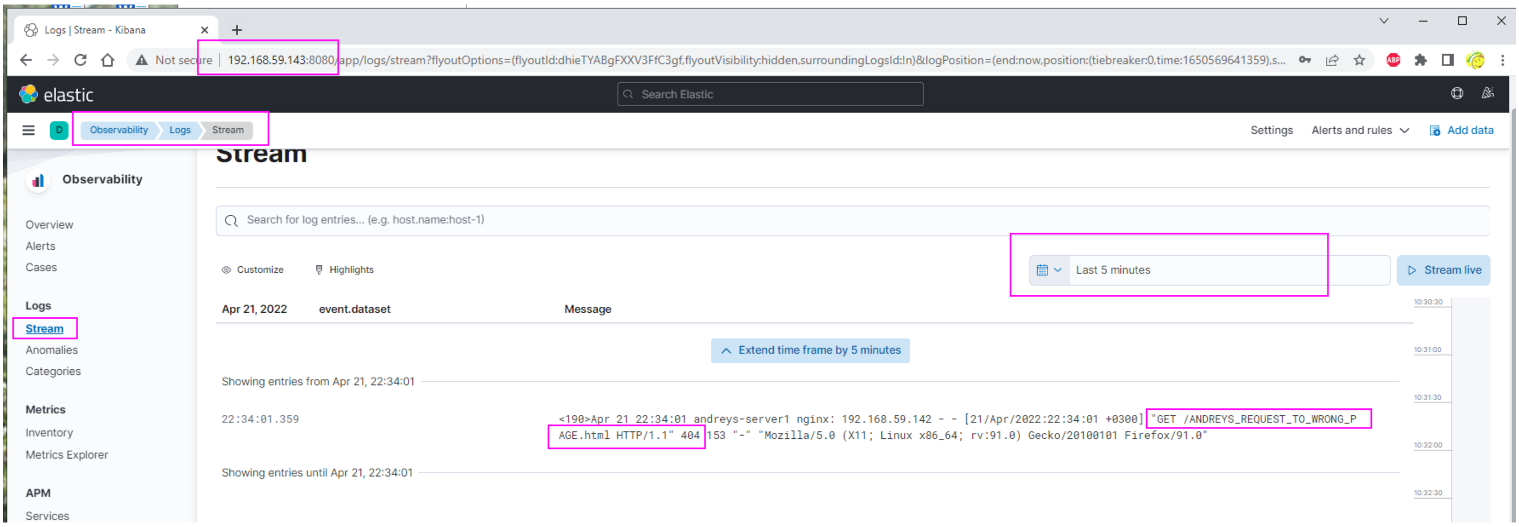


```
2022-04-21T17:20:02+03:00 andreys-server1 nginx: 192.168.59.1 - - [21/Apr/2022:17:20:02 +0300] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36"
2022-04-21T17:23:46+03:00 andreys-server1 nginx: 192.168.59.1 - - [21/Apr/2022:17:23:46 +0300] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36"
2022-04-21T17:26:50+03:00 andreys-server1 nginx: 192.168.59.1 - - [21/Apr/2022:17:26:50 +0300] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36"
2022-04-21T17:27:01+03:00 andreys-server1 nginx: 192.168.59.1 - - [21/Apr/2022:17:27:01 +0300] "GET /andrey_ERROR.html HTTP/1.1" 404 555 "-" "Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36"
2022-04-21T22:34:01+03:00 andreys-server1 nginx: 192.168.59.142 - - [21/Apr/2022:22:34:01 +0300] "GET /ANDREYS_REQUEST_TO_WRONG_PAGE.html HTTP/1.1" 404 153 "-" "Mozilla/5.0
(X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
```

192.168.59.142:8080/ANDREYS_REQUEST_TO_WRONG_PAGE.html

404 Not Found

nginx/1.20.1



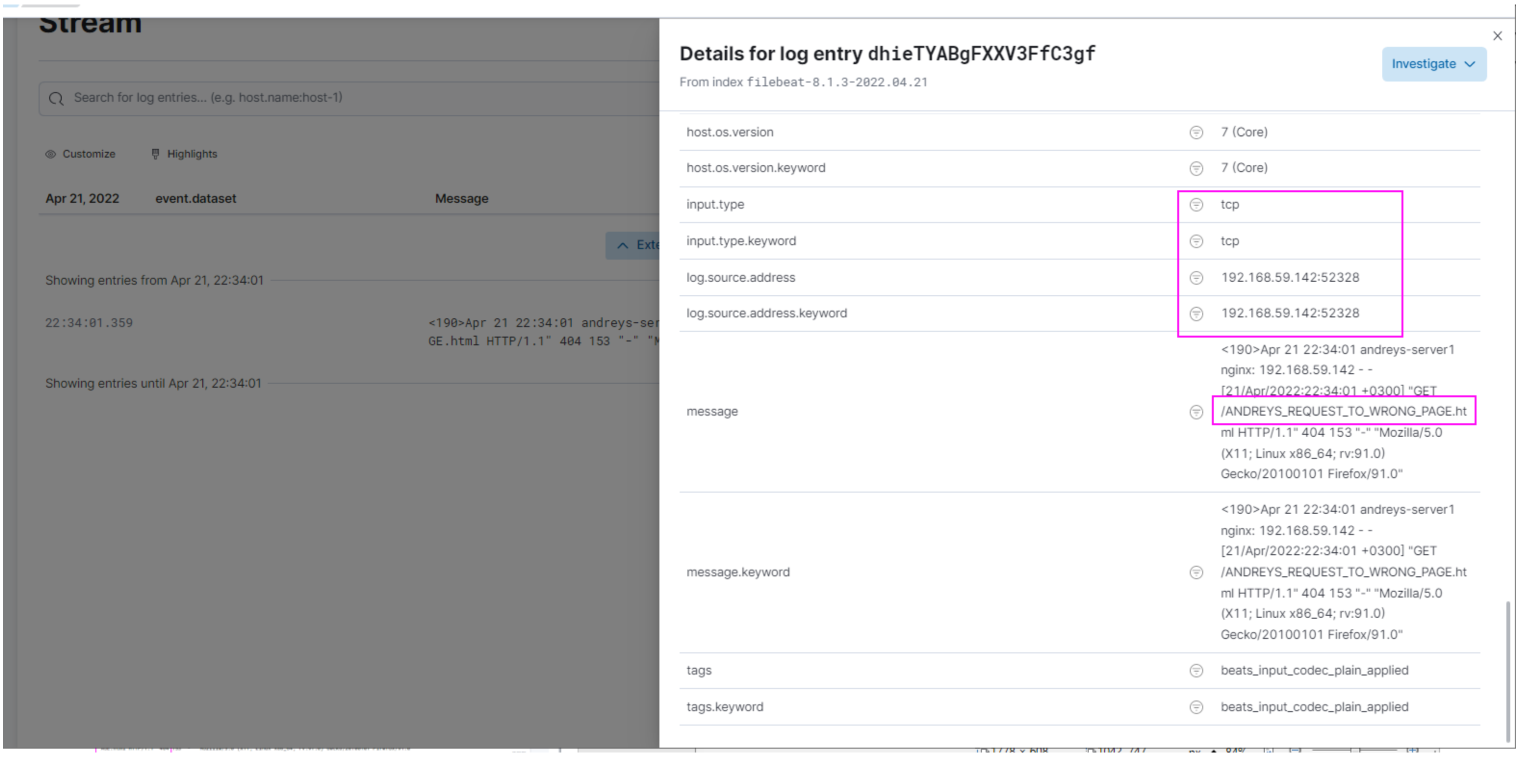
Stream

Apr 21, 2022	event.dataset	Message

Showing entries from Apr 21, 22:34:01

```
22:34:01.359        <190>Apr 21 22:34:01 andreys-server1 nginx: 192.168.59.142 - - [21/Apr/2022:22:34:01 +0300] "GET /ANDREYS_REQUEST_TO_WRONG_P
                    AGE.html HTTP/1.1" 404 153 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
```

Showing entries until Apr 21, 22:34:01

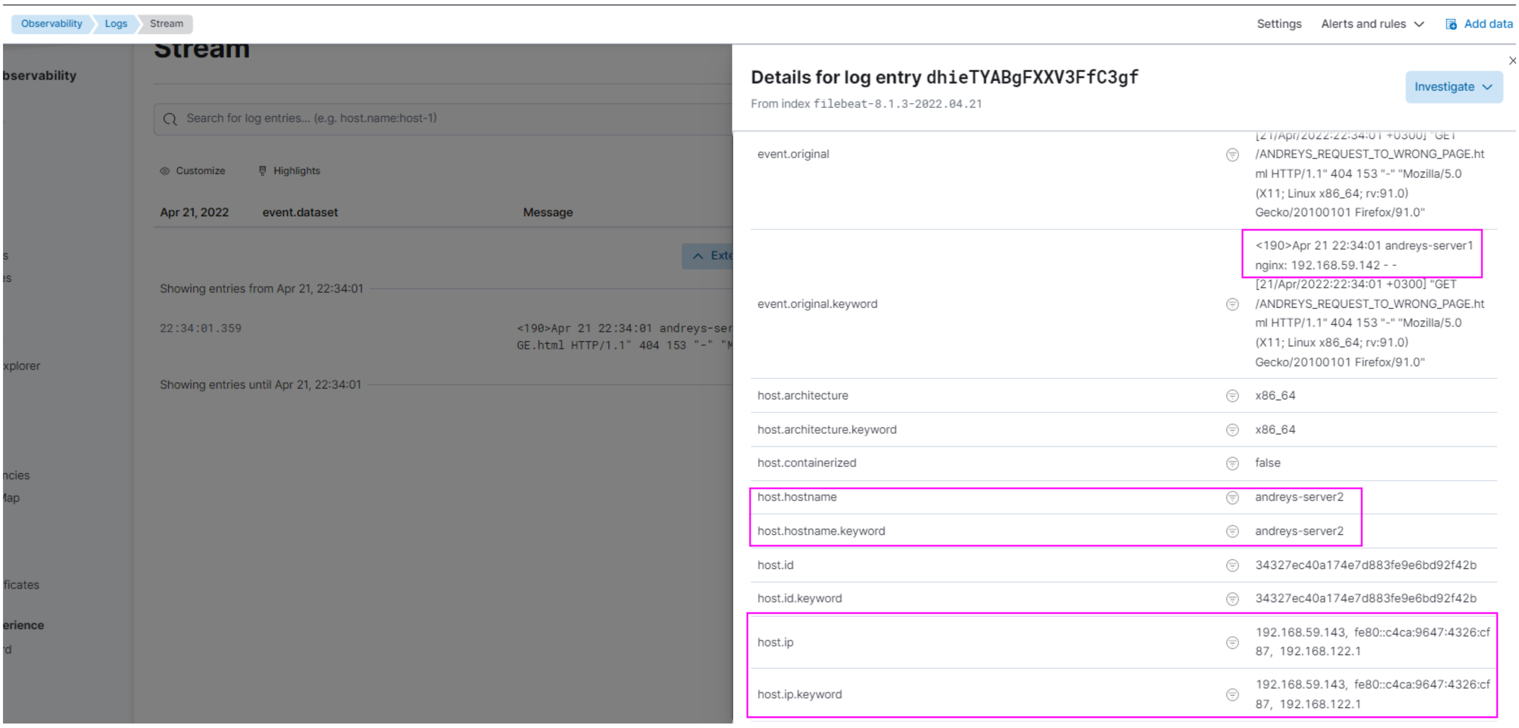


Stream
Search for log entries... (e.g. host.name:host-1)
Customize
Highlights
Apr 21, 2022
event.dataset
Message
Exte
Showing entries from Apr 21, 22:34:01
22:34:01.359
<190>Apr 21 22:34:01 andreys-ser
GE.html HTTP/1.1" 404 153 "-" "M
Showing entries until Apr 21, 22:34:01
Investigate

Details for log entry dhieTYABgFXXV3FfC3gf

From index filebeat-8.1.3-2022.04.21

host.os.version	7 (Core)
host.os.version.keyword	7 (Core)
input.type	tcp
input.type.keyword	tcp
log.source.address	192.168.59.142:52328
log.source.address.keyword	192.168.59.142:52328
message	<190>Apr 21 22:34:01 andreys-server1 nginx: 192.168.59.142 - - [21/Apr/2022:22:34:01 +0300] "GET /ANDREYS_REQUEST_TO_WRONG_PAGE.html HTTP/1.1" 404 153 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
message.keyword	<190>Apr 21 22:34:01 andreys-server1 nginx: 192.168.59.142 - - [21/Apr/2022:22:34:01 +0300] "GET /ANDREYS_REQUEST_TO_WRONG_PAGE.html HTTP/1.1" 404 153 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
tags	beats_input_codec_plain_applied
tags.keyword	beats_input_codec_plain_applied



Observability
Logs
Stream
Settings
Alerts and rules
Add data
Stream
bservability
s
s
xplorer
ncies
lap
ficates
erience
d
Search for log entries... (e.g. host.name:host-1)
Customize
Highlights
Apr 21, 2022
event.dataset
Message
Exte
Showing entries from Apr 21, 22:34:01
22:34:01.359
<190>Apr 21 22:34:01 andreys-ser
GE.html HTTP/1.1" 404 153 "-" "M
Showing entries until Apr 21, 22:34:01
Investigate

Details for log entry dhieTYABgFXXV3FfC3gf

From index filebeat-8.1.3-2022.04.21

event.original	[21/Apr/2022:22:34:01 +0300] "GET /ANDREYS_REQUEST_TO_WRONG_PAGE.html HTTP/1.1" 404 153 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
event.original.keyword	<190>Apr 21 22:34:01 andreys-server1 nginx: 192.168.59.142 - - [21/Apr/2022:22:34:01 +0300] "GET /ANDREYS_REQUEST_TO_WRONG_PAGE.html HTTP/1.1" 404 153 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
host.architecture	x86_64
host.architecture.keyword	x86_64
host.containerized	false
host.hostname	andreys-server2
host.hostname.keyword	andreys-server2
host.id	34327ec40a174e7d883fe9e6bd92f42b
host.id.keyword	34327ec40a174e7d883fe9e6bd92f42b
host.ip	192.168.59.143, fe80::c4ca:9647:4326:cf87, 192.168.122.1
host.ip.keyword	192.168.59.143, fe80::c4ca:9647:4326:cf87, 192.168.122.1