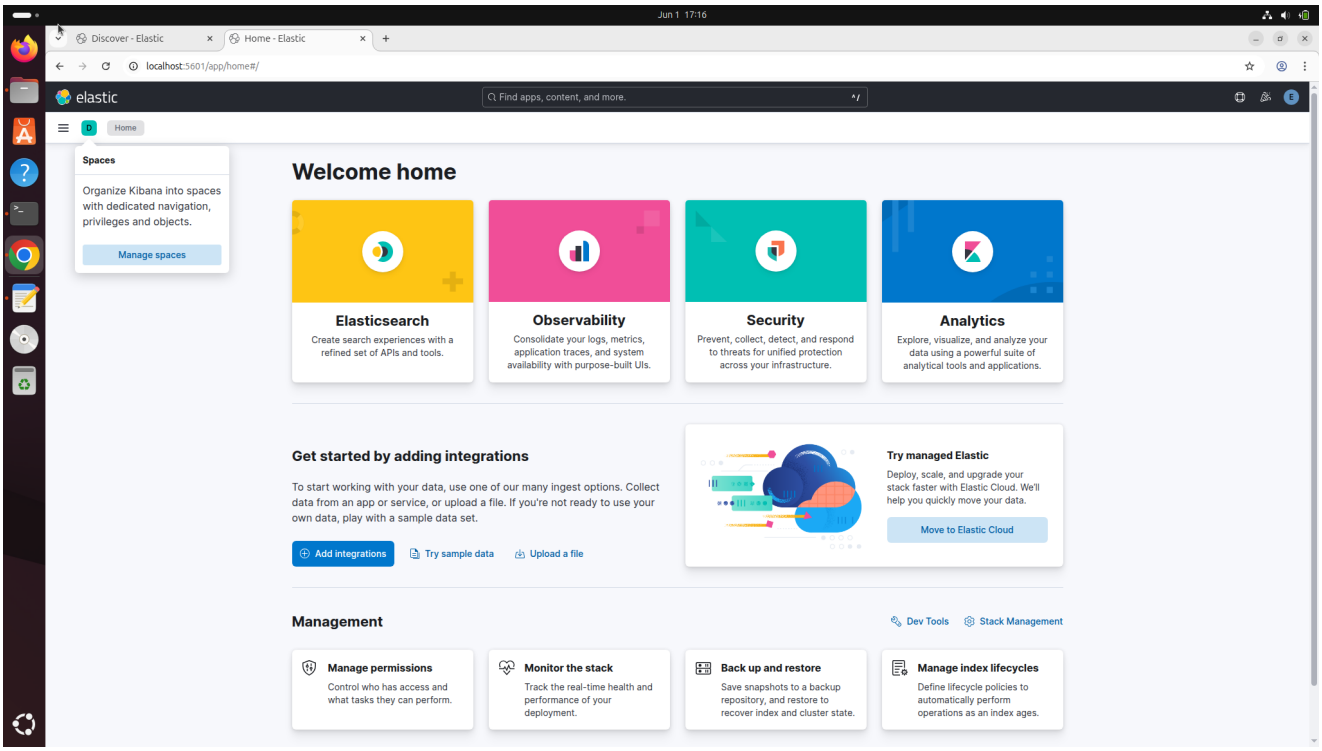
Задание 1

Интерфейс Kibana

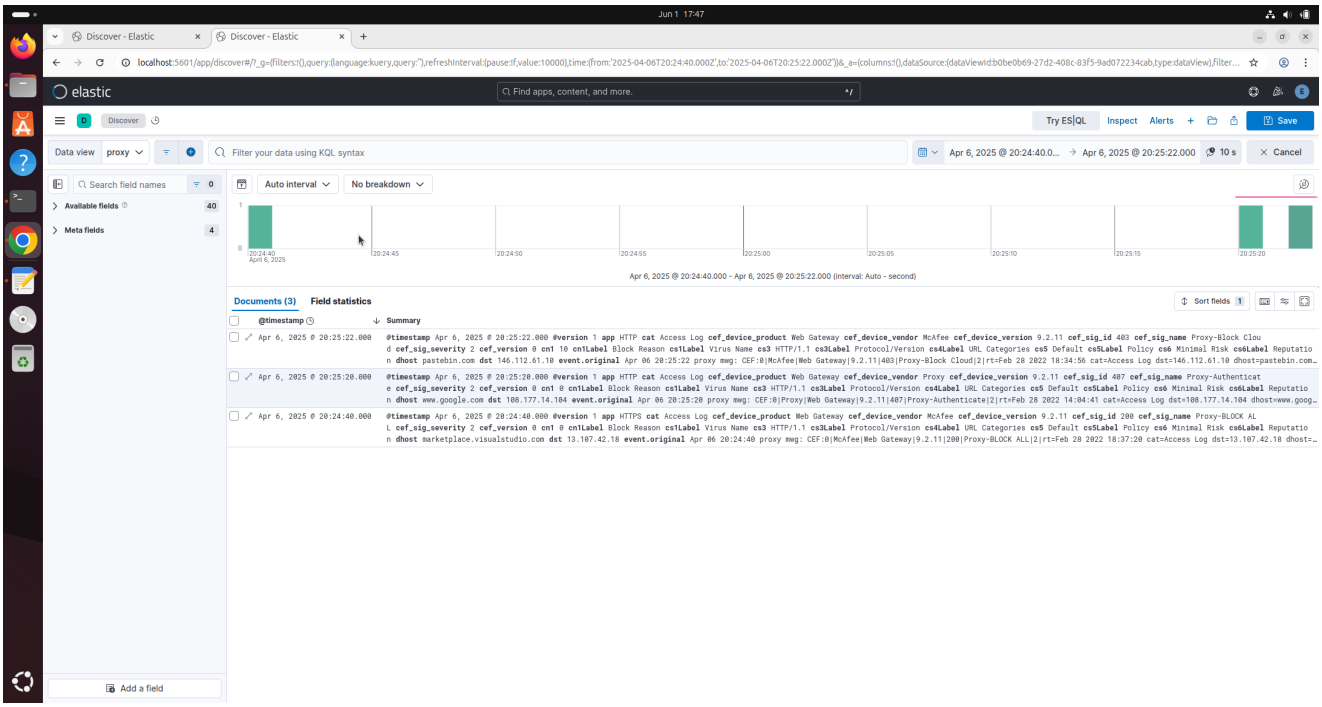


Список отрываемых портов

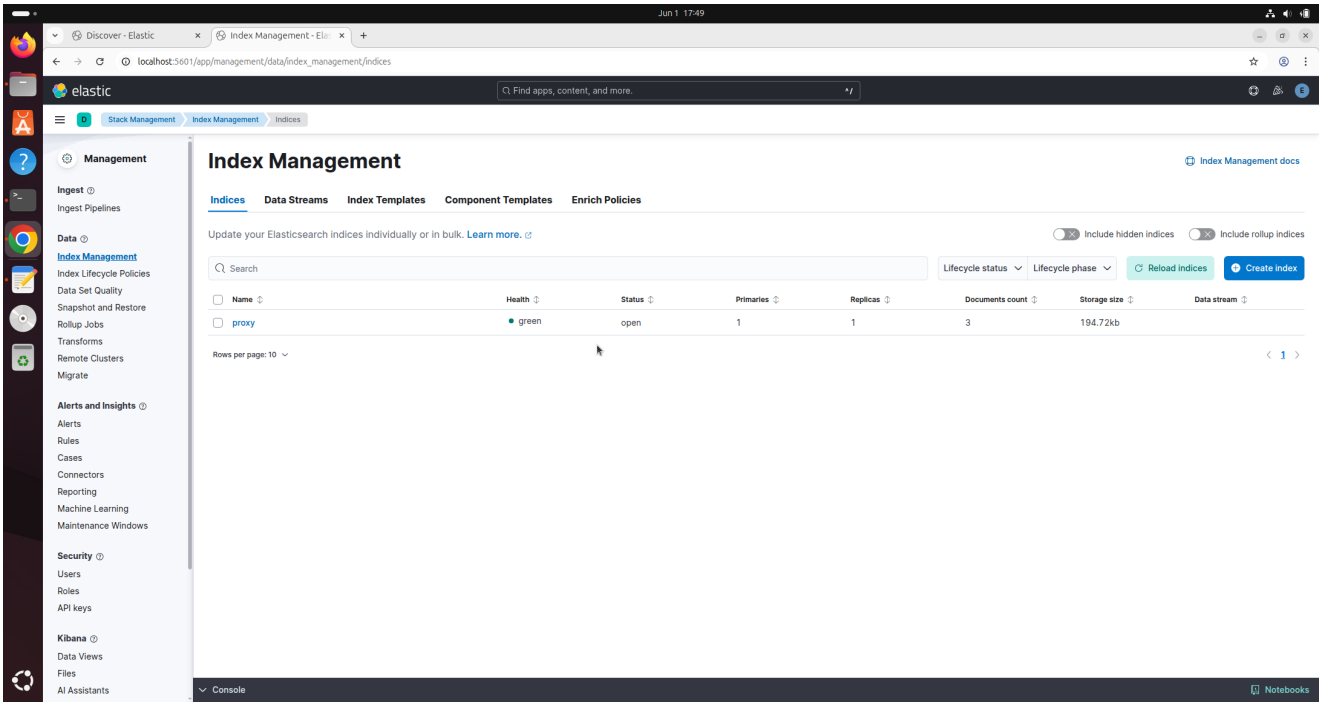
- 9200 - Elasticsearch
- 5601 - Kibana
- 5000-5001, 5044 - Logstash

Задание 2

Содержимое лога proxy.log



Название индекса во вкладке Index Management.



Задание 3

Правила фильтрации в auth.conf

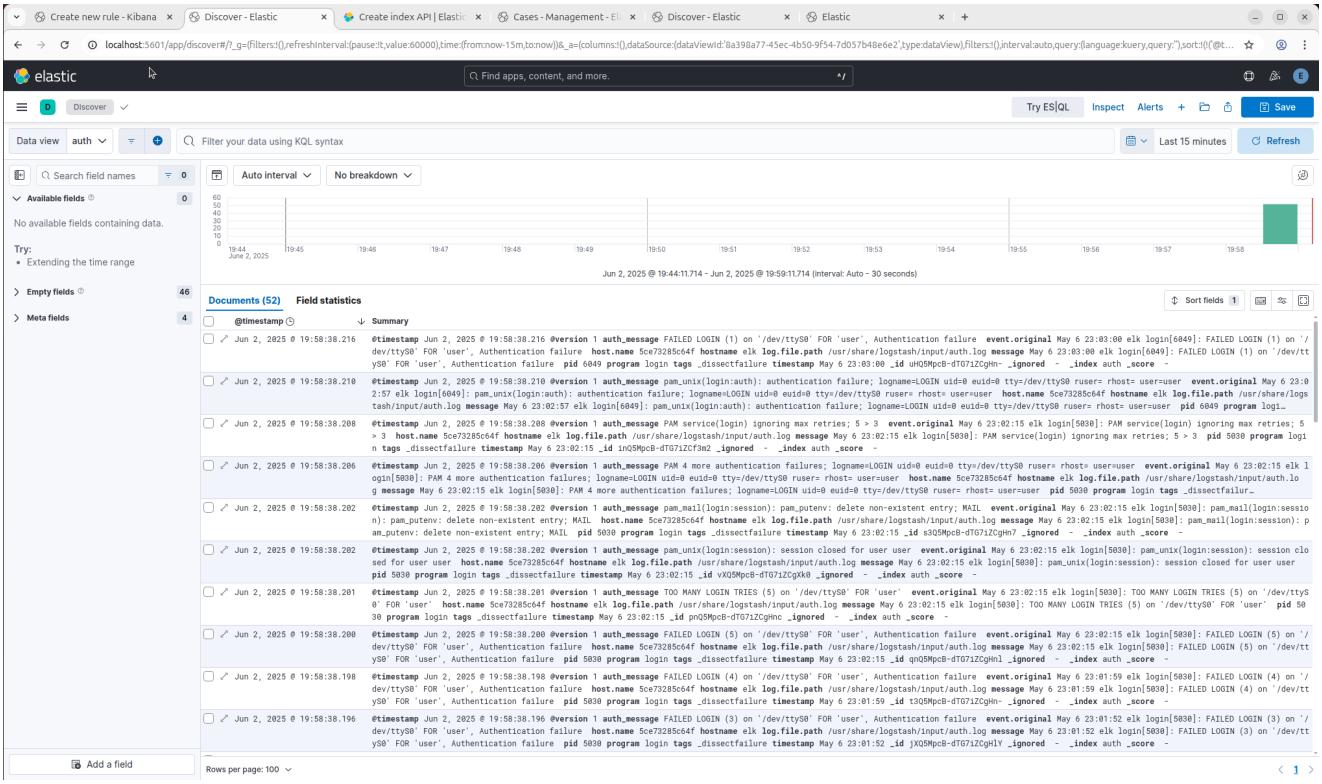
Open

auth.conf
/opt/elk

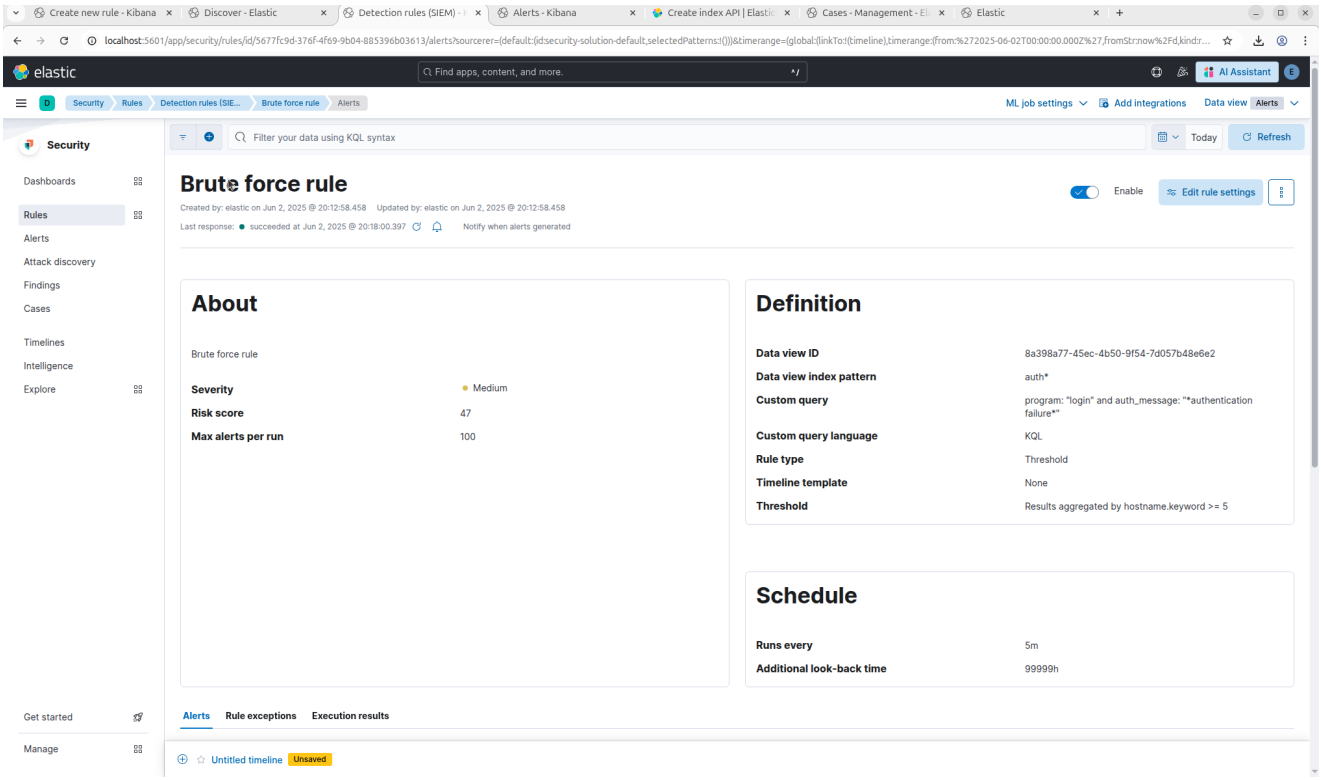
logstash.yml | auth.conf

```
input {
  file {
    start_position => "beginning"
    path => "/usr/share/logstash/input/auth.log"
    sincedb_clean_after => 0
  }
}

filter {
  grok {
    match => {
      "message" => ["%{SYSLOGTIMESTAMP:timestamp} %{HOSTNAME:hostname} %{DATA:program}(?:\[%{POSINT:pid}\])?: %{GREEDYDATA:auth_message}"]
      }
  }
}

output {
  elasticsearch {
    hosts => ["https://es01:9200"]
    index => "auth"
    user => "elastic"
    password => "changeme"
    ssl_certificate_authorities => "/usr/share/logstash/certs/ca/ca.crt"
    ssl_verification_mode => "none"
  }
}
```

Скриншоты DataView auth-лога



Правило определения brute force



Сработка правила