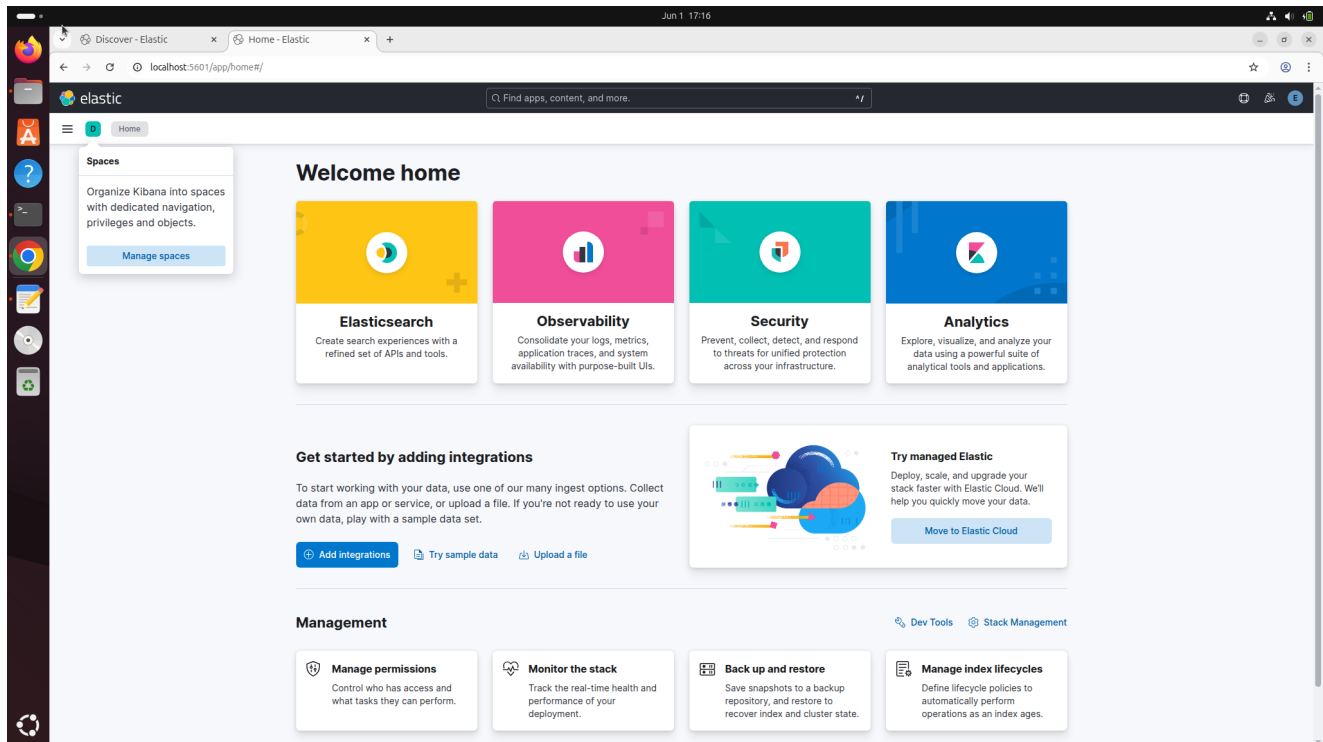


Задание 1

Интерфейс Kibana

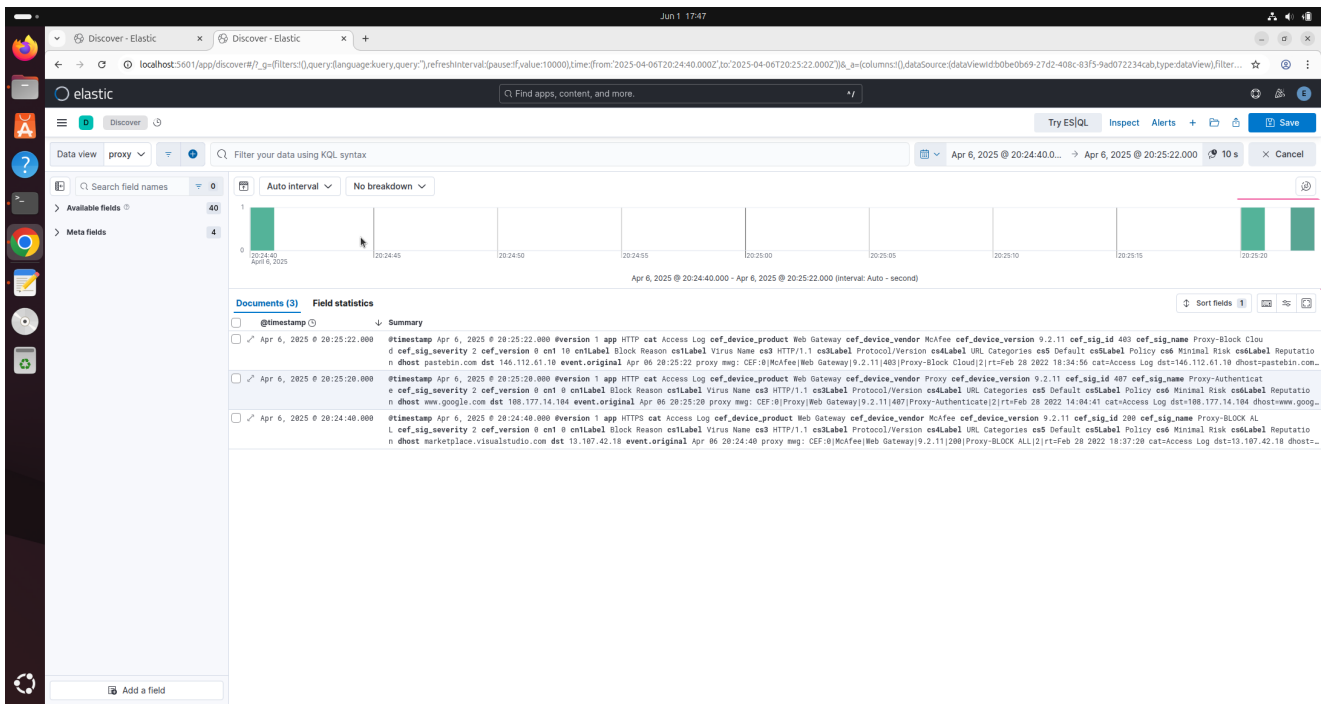


Список отрываемых портов

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

Задание 2

Содержимое лога proxy.log



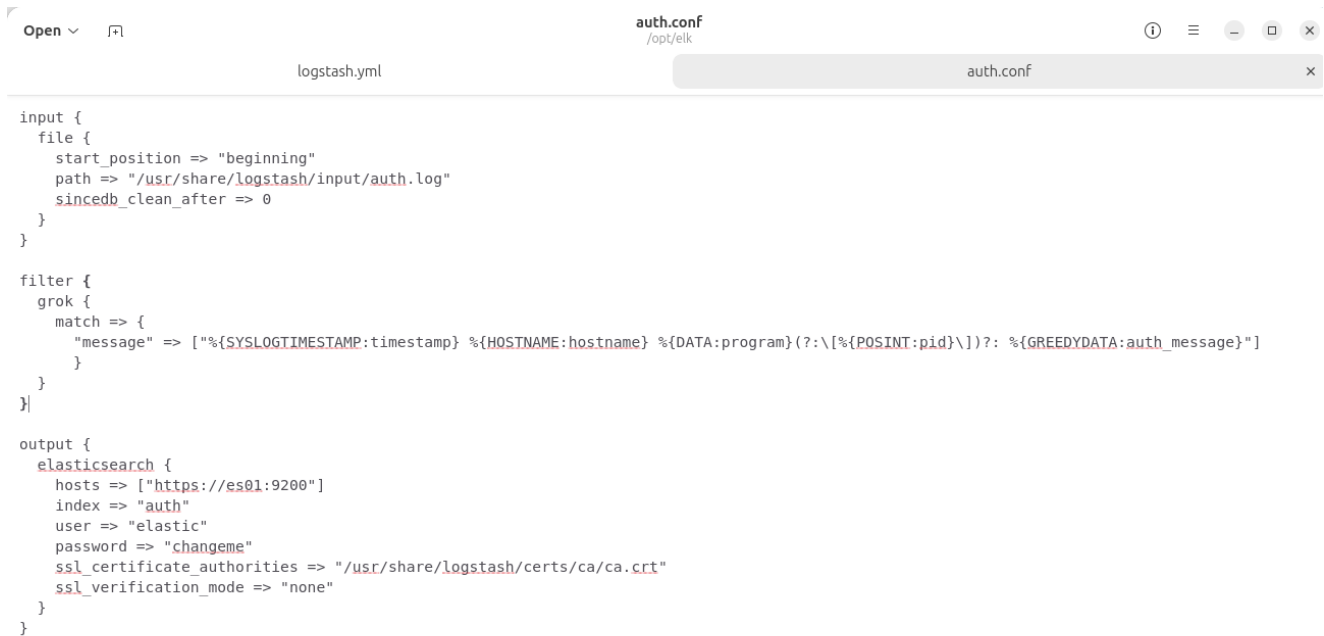
Название индекса во вкладке Index Management.

The screenshot shows the Elastic Index Management interface. The left sidebar contains a navigation menu with sections: Management, Ingest, Data, Alerts and Insights, Security, and Kibana. The main content area is titled "Index Management" and contains a table of indices. The table has columns: Name, Health, Status, Primaries, Replicas, Documents count, Storage size, and Data stream. The first row shows an index named "proxy" with a Health of "green", Status of "open", 1 Primary, 1 Replica, 3 Documents, and a Storage size of 194.72kb. The table is sorted by Name. There are buttons for "Include hidden indices", "Include rollout indices", "Reload indices", and "Create index".

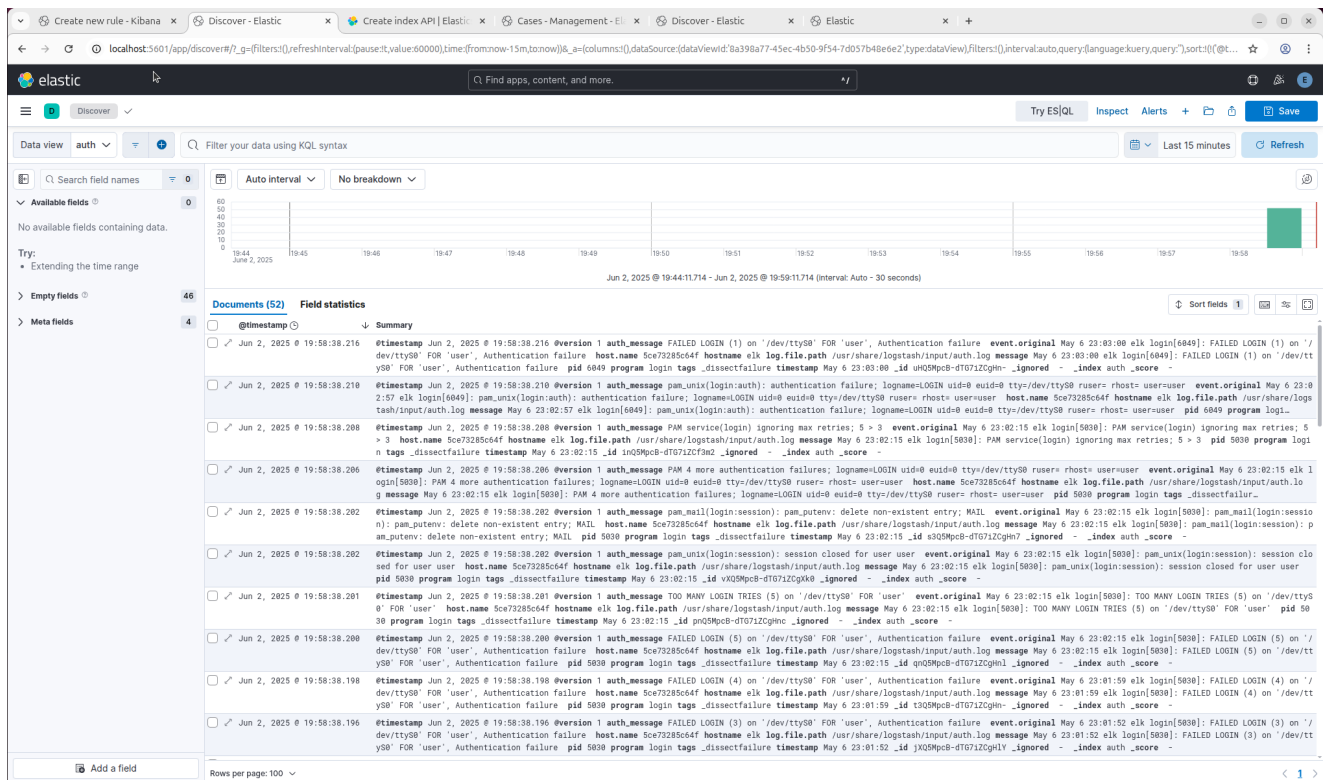
Name	Health	Status	Primaries	Replicas	Documents count	Storage size	Data stream
proxy	green	open	1	1	3	194.72kb	

Задание 3

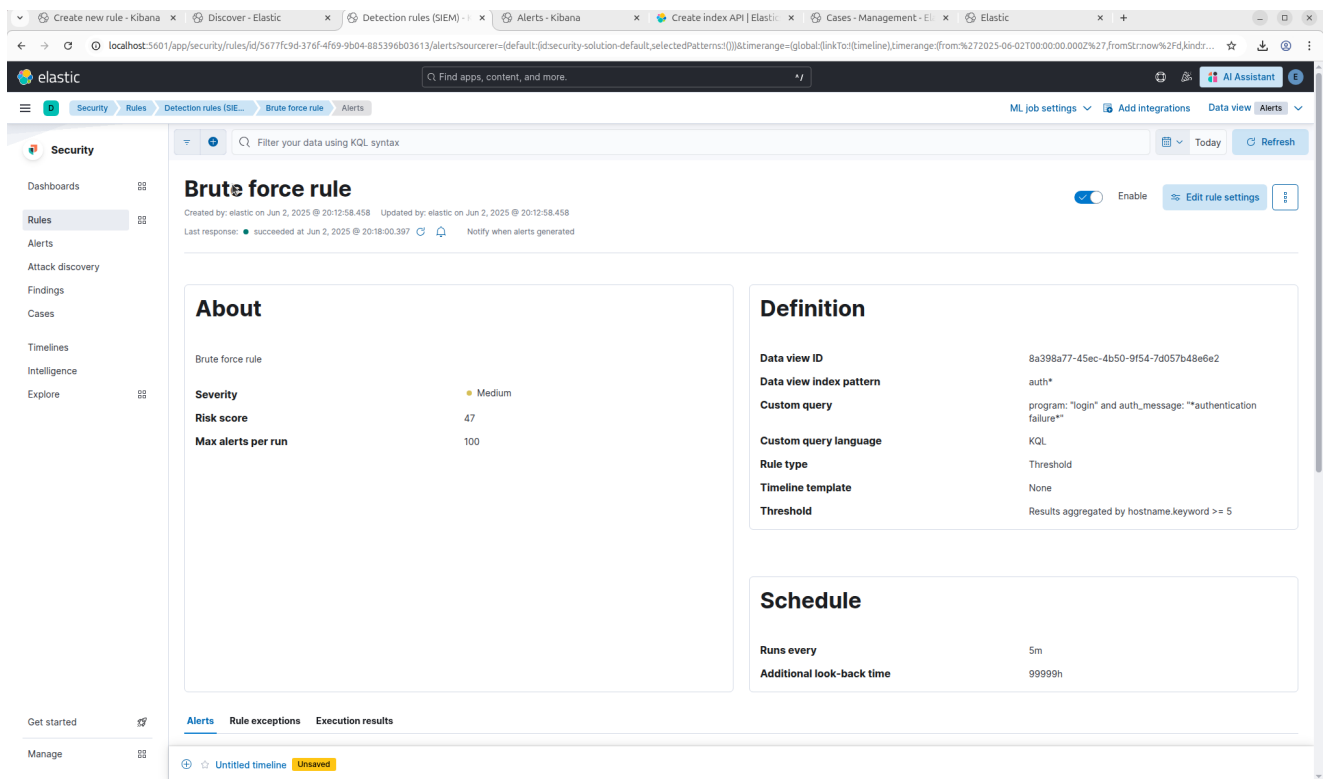
Правила фильтрации в auth.conf



Скриншоты DataView auth-лога



Правило определения brute force



Сработка правила

