<https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elastic-stack-on-ubuntu-22-04>

<https://www.digitalocean.com/community/tutorials/how-to-install-java-with-apt-on-ubuntu-22-04>

The Elastic Stack has four main components:

* [**Elasticsearch**](https://www.elastic.co/products/elasticsearch): a distributed [*RESTful*](https://en.wikipedia.org/wiki/Representational_state_transfer) search engine which stores all of the collected data. **9200** sudo vi /etc/elasticsearch/elasticsearch.yml
* [**Logstash**](https://www.elastic.co/products/logstash): the data processing component of the Elastic Stack which sends incoming data to Elasticsearch. **9600** /etc/logstash/conf.d/02-beats-input.conf
* [**Kibana**](https://www.elastic.co/products/kibana): a web interface for searching and visualizing logs. **5601**
* [**Beats**](https://www.elastic.co/products/beats): lightweight, single-purpose data shippers that can send data from hundreds or thousands of machines to either Logstash or Elasticsearch.

/etc/filebeat/filebeat.yml **5044**

1 cd

2 clear

3 curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch |sudo gpg --dearmor -o /usr/share/keyrings/elastic.gpg

4 echo "deb [signed-by=/usr/share/keyrings/elastic.gpg] https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

5 sudo apt update

6 sudo apt install elasticsearch

7 sudo vi /etc/elasticsearch/elasticsearch.yml

8 sudo systemctl start elasticsearch

9 sudo systemctl enable elasticsearch

10 curl -X GET "localhost:9200"

11 sudo apt install kibana

12 sudo systemctl enable kibana

13 sudo systemctl start kibana

14 sudo apt update

15 sudo apt install nginx

16 systemctl status nginx

17 clear

18 echo "kibanaadmin:`openssl passwd -apr1`" | sudo tee -a /etc/nginx/htpasswd.users

19 cd /etc/nginx/sites-enabled/

20 vi default

21 nginx -t

22 sudo systemctl reload nginx

23 sudo apt install logstash

24 cd

25 clear

26 sudo vi /etc/logstash/conf.d/02-beats-input.conf

27 sudo vi /etc/logstash/conf.d/30-elasticsearch-output.conf

28 sudo -u logstash /usr/share/logstash/bin/logstash --path.settings /etc/logstash -t

29 java -version

30 sudo apt install default-jre

31 java -version

32 sudo apt install default-jdk

33 clear

34 sudo -u logstash /usr/share/logstash/bin/logstash --path.settings /etc/logstash -t

35 sudo systemctl start logstash

36 sudo systemctl enable logstash

37 sudo apt install filebeat

38 sudo vi /etc/filebeat/filebeat.yml

39 sudo filebeat modules enable system

40 sudo filebeat modules list

41 clear

42 sudo filebeat setup --pipelines --modules system

43 sudo filebeat setup --index-management -E output.logstash.enabled=false -E 'output.elasticsearch.hosts=["localhost:9200"]'

44 sudo filebeat setup -E output.logstash.enabled=false -E output.elasticsearch.hosts=['localhost:9200'] -E setup.kibana.host=localhost:5601

45 sudo systemctl start filebeat

46 sudo systemctl enable filebeat

47 clear

48 curl -XGET 'http://localhost:9200/filebeat-\*/\_search?pretty'

49 cat /etc/filebeat/filebeat.yml

50 cd /etc/nginx/sites-available/

51 ls -lrt

52 history