Zusatzaufgabe zu Elasticsearch

1. Tun Sie sich als team von 3 Personen zusammen
2. Bringen Sie ein Elasticsearch Cluster aus mind. drei physikalischen oder virtuellen Maschinen zum Laufen
3. Indexieren Sie Daten auf dem Cluster, so dass auf jedem Knoten Daten indexiert werden
4. Seien Sie in der Lage, Daten vom Cluster abzufragen
5. Zeigen Sie, dass Sie in der Lage sind, eine Übersicht über die Cluster Health zu erlangen (dafür gibt es ebenfalls eine API)

**Start a single-node cluster**

If using Docker Desktop, make sure to allocate at least 4GB of memory. You can adjust memory usage in Docker Desktop by going to Settings > Resources.

Create a new docker network.

docker network create elastic

Pull the Elasticsearch Docker image.

docker pull docker.elastic.co/elasticsearch/elasticsearch:8.11.4

Start an Elasticsearch container.

docker run --name es01 --net elastic -p 9200:9200 -it -m 1GB docker.elastic.co/elasticsearch/elasticsearch:8.11.4

The command prints the elastic user password and an enrollment token for Kibana.

━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

✅ Elasticsearch security features have been automatically configured!

✅ Authentication is enabled and cluster connections are encrypted.

ℹ️ Password for the elastic user (reset with `bin/elasticsearch-reset-password -u elastic`):

LpGwEK=V0=2mRT+20d\_V

ℹ️ HTTP CA certificate SHA-256 fingerprint:

3a6ffc99fc95e89407943a52b8238b58d4a0c28ed4d3a75e3d2803846aff5a0d

ℹ️ Configure Kibana to use this cluster:

• Run Kibana and click the configuration link in the terminal when Kibana starts.

• Copy the following enrollment token and paste it into Kibana in your browser (valid for the next 30 minutes):

eyJ2ZXIiOiI4LjExLjQiLCJhZHIiOlsiMTcyLjE4LjAuMjo5MjAwIl0sImZnciI6IjNhNmZmYzk5ZmM5NWU4OTQwNzk0M2E1MmI4MjM4YjU4ZDRhMGMyOGVkNGQzYTc1ZTNkMjgwMzg0NmFmZjVhMGQiLCJrZXkiOiJIRnJfRW8wQlpOc3d1T3JQNW0zdTp0VkJpM3F6a1RUZTN5dlhva0dBTFp3In0=

ℹ️ Configure other nodes to join this cluster:

• Copy the following enrollment token and start new Elasticsearch nodes with `bin/elasticsearch --enrollment-token <token>` (valid for the next 30 minutes):

eyJ2ZXIiOiI4LjExLjQiLCJhZHIiOlsiMTcyLjE4LjAuMjo5MjAwIl0sImZnciI6IjNhNmZmYzk5ZmM5NWU4OTQwNzk0M2E1MmI4MjM4YjU4ZDRhMGMyOGVkNGQzYTc1ZTNkMjgwMzg0NmFmZjVhMGQiLCJrZXkiOiJIbHJfRW8wQlpOc3d1T3JQNTIwRjprS3pqR05DTVRyS0c5dE1NOWNleHlRIn0=

If you're running in Docker, copy the enrollment token and run:

`docker run -e "ENROLLMENT\_TOKEN=<token>" docker.elastic.co/elasticsearch/elasticsearch:8.11.4`

Copy the generated elastic password and enrollment token. These credentials are only shown when you start Elasticsearch for the first time. You can regenerate the credentials using the following commands.

docker exec -it es01 /usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic

docker exec -it es01 /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana

We recommend storing the elastic password as an environment variable in your shell. Example:

export ELASTIC\_PASSWORD="your\_password"

Copy the http\_ca.crt SSL certificate from the container to your local machine.

docker cp es01:/usr/share/elasticsearch/config/certs/http\_ca.crt .

Make a REST API call to Elasticsearch to ensure the Elasticsearch container is running.

curl --cacert http\_ca.crt -u elastic:$ELASTIC\_PASSWORD https://localhost:9200

**Add more nodes**

Use an existing node to generate an enrollment token for the new node.

docker exec -it es01 /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s node

The enrollment token is valid for 30 minutes.

Start a new Elasticsearch container. Include the enrollment token as an environment variable.

docker run -e ENROLLMENT\_TOKEN="<token>" --name es02 --net elastic -it -m 1GB docker.elastic.co/elasticsearch/elasticsearch:8.11.4

Call the cat nodes API to verify the node was added to the cluster.

curl --cacert http\_ca.crt -u elastic:$ELASTIC\_PASSWORD <https://localhost:9200/_cat/nodes>

**Run Kibana**

Pull the Kibana Docker image.

docker pull docker.elastic.co/kibana/kibana:8.11.4

Start a Kibana container.

docker run --name kib01 --net elastic -p 5601:5601 docker.elastic.co/kibana/kibana:8.11.4

When Kibana starts, it outputs a unique generated link to the terminal. To access Kibana, open this link in a web browser.

In your browser, enter the enrollment token that was generated when you started Elasticsearch.

To regenerate the token, run:

docker exec -it es01 /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana

Log in to Kibana as the elastic user with the password that was generated when you started Elasticsearch.

To regenerate the password, run:

docker exec -it es01 /usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic

**Nodes erzeugen**

docker exec -it node1 /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s node

docker run -e ENROLLMENT\_TOKEN="eyJ2ZXIiOiI4LjEyLjAiLCJhZHIiOlsiMTcyLjE4LjAuMjo5MjAwIl0sImZnciI6IjJhZWJmYTRmNmM5NGMwZGNjNjRhY2RhN2U5ZTExY2E3YTA3ZTkwMTA3ZDIzODJhYjg2NzM3MWY1ZmJmNjZmMjciLCJrZXkiOiJwbUlaSVkwQklGQkhCNTZmUTFTRTp2MUk0QjExV1NWLV9kdDRrUUNrd3d3In0=

" --name node\_2 --net elastic -it -m 1GB docker.elastic.co/elasticsearch/elasticsearch:8.12.0

alalnx@alalnx-ThinkPad-P50:~/PycharmProjects/verteilte\_systeme\_23/elasticPython3nodes/pythonProject1$ docker exec -it node1 /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s node

eyJ2ZXIiOiI4LjEyLjAiLCJhZHIiOlsiMTcyLjE4LjAuMjo5MjAwIl0sImZnciI6IjJhZWJmYTRmNmM5NGMwZGNjNjRhY2RhN2U5ZTExY2E3YTA3ZTkwMTA3ZDIzODJhYjg2NzM3MWY1ZmJmNjZmMjciLCJrZXkiOiJ5V0lySVkwQklGQkhCNTZmWDFTcTpHZ3FGcC1OelNGT3pJSXVsRHVVNUNBIn0=

alalnx@alalnx-ThinkPad-P50:~/PycharmProjects/verteilte\_systeme\_23/elasticPython3nodes/pythonProject1$ docker run -e ENROLLMENT\_TOKEN="eyJ2ZXIiOiI4LjEyLjAiLCJhZHIiOlsiMTcyLjE4LjAuMjo5MjAwIl0sImZnciI6IjJhZWJmYTRmNmM5NGMwZGNjNjRhY2RhN2U5ZTExY2E3YTA3ZTkwMTA3ZDIzODJhYjg2NzM3MWY1ZmJmNjZmMjciLCJrZXkiOiJ5V0lySVkwQklGQkhCNTZmWDFTcTpHZ3FGcC1OelNGT3pJSXVsRHVVNUNBIn0=

" --name node\_3 --net elastic -it -m 1GB docker.elastic.co/elasticsearch/elasticsearch:8.12.0