

You can set up the via docker run manually via : `docker run --name elasticsearch2 --net somenetwork -p 9200:9200 -p 9300:9300 -e "discovery.type=single-node" -m 2g -t elasticsearch:8.10.2`

see the - t to get outpt in the tty

<https://www.youtube.com/watch?v=j61yfEfeJAE>

```
[{"previousHealth": "YELLOW", "reason": "Shards started [[security-]][]", "cd706e2"][masterService#updateTask][T#1]", "log.logger": "org.elasticsearch.clusterEGT0uJ0ROM87B4_A", "elasticsearch.node.name": "044c40d706e2", "elasticsearch.clus
```

---

✔ Elasticsearch security features have been automatically configured!  
✔ Authentication is enabled and cluster connections are encrypted.

i Password for the elastic user (reset with `bin/elasticsearch-reset-password Gsz=Pj\*ZA2khuKc6ILfC`)

i HTTP CA certificate SHA-256 fingerprint:  
cc540d4f746142c3ae264656cb009d530eddfе9а1cc43b9d4adff92cf21a6782

i 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  
eyJ2ZXI0i0iI4LjEwLjIiLCJhZHII0lsIMTCyLjI2LjAuMjo5MjAwIl0sImZnciI6ImNjNTQwZDRm1M3U0ZCVExhMm95OFZRIn0=

i Configure other nodes to join this cluster:

- Copy the following enrollment token and start new Elasticsearch nodes with `FJfrR0ZGeThwU2Z2N0inIn0=`

If you're running in Docker, copy the enrollment token and run:  
`docker run -e "ENROLLMENT\_TOKEN=<token>" docker.elastic.co/elasticsearch/el-

or to setup via docker compose read documentation or chatgpt

<https://www.elastic.co/guide/en/elasticsearch/reference/current/docker.html>

after following the steps by entering passwrod in .env u will get this error in which the fourth line states vm.max\_map\_count 65530 is too low

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS
fc61ae9c3e0	postgres:15	"docker-entrypoint.s..."	About an hour ago	Up Ab

```

maheboob@maheboob:~/Desktop/elastickibana compose/documentation$ docker compose
[+] Running 6/6
  ✓ Network documentation_default          Created
  ✓ Container documentation-setup-1        Healthy
  ✗ Container documentation-es01-1         Error
  ✗ Container documentation-es02-1         Error
  ✗ Container documentation-es03-1         Error
  ✓ Container documentation-kibana-1       Created
dependency failed to start: container documentation-es02-1 exited (78)
maheboob@maheboob:~/Desktop/elastickibana compose/documentation$ docker logs do
Error response from daemon: No such container: documentation-es01
maheboob@maheboob:~/Desktop/elastickibana compose/documentation$ docker logs do
Created elasticsearch keystore in /usr/share/elasticsearch/config/elasticsearch
{"@timestamp":"2023-10-09T06:31:24.349Z", "log.level": "INFO", "message":"Java
lasticsearch.server", "process.thread.name":"main", "log.logger":"org.apache.lucen
{"@timestamp":"2023-10-09T06:31:24.890Z", "log.level": "INFO", "message":"versi
-86-generic/amd64], JVM[Oracle Corporation/OpenJDK 64-Bit Server VM/20.0.2/20.0

```

```

{"@timestamp":"2023-10-09T06:31:35.549Z", "log.level": "INFO", "message":"bound
dataset":"elasticsearch.server", "process.thread.name":"main", "log.logger":"org.
{"@timestamp":"2023-10-09T06:31:35.553Z", "log.level": "ERROR", "message":"node v
starting Elasticsearch.\nbootstrap check failure [1] of [1]: max virtual memory a
vent.dataset":"elasticsearch.server", "process.thread.name":"main", "log.logger":"
ERROR: Elasticsearch did not exit normally - check the logs at /usr/share/elasti
{"@timestamp":"2023-10-09T06:31:35.556Z", "log.level": "WARN", "message":"unexper
lasticsearch.server", "process.thread.name":"Thread-0", "log.logger":"org.elasticsea
rent.ExecutionException", "error.message":"java.lang.IllegalStateException: Can't
ateException: Can't move to stopped state when not started\n\tat java.base/java.l
191)\n\tat org.elasticsearch.server@8.10.2/org.elasticsearch.node.Node.prepareFo
ch.java:466)\n\tat java.base/java.lang.Thread.run(Thread.java:1623)\nCaused by:
lasticsearch.common.component.Lifecycle.canMoveToStopped(Lifecycle.java:128)\n\tat
ent.java:73)\n\tat org.elasticsearch.server@8.10.2/org.elasticsearch.node.Node.l
more\n"}
{"@timestamp":"2023-10-09T06:31:35.556Z", "log.level": "INFO", "message":"stoppi
d-0", "log.logger":"org.elasticsearch.node.Node", "elasticsearch.node.name":"es01"
{"@timestamp":"2023-10-09T06:31:35.566Z", "log.level": "INFO", "message":"stoppe
'log.logger":"org.elasticsearch.node.Node", "elasticsearch.node.name":"es01", "ela
{"@timestamp":"2023-10-09T06:31:35.566Z", "log.level": "INFO", "message":"closing
-0", "log.logger":"org.elasticsearch.node.Node", "elasticsearch.node.name":"es01",
{"@timestamp":"2023-10-09T06:31:35.571Z", "log.level": "INFO", "message":"closed
log.logger":"org.elasticsearch.node.Node", "elasticsearch.node.name":"es01", "elas
{"@timestamp":"2023-10-09T06:31:35.572Z", "log.level": "INFO", "message":"Native
event.dataset":"elasticsearch.server", "process.thread.name":"ml-cpp-log-tail-thr
ster.name":"docker-cluster"}

ERROR: Elasticsearch exited unexpectedly, with exit code 78

```

to solve this read the documentation of elasticsearch with the heading Using docker images in produc

### **Set vm.max\_map\_count to at least 262144**[edit](#)

The vm.max\_map\_count kernel setting must be set to at least 262144 for production use.

How you set vm.max\_map\_count depends on your platform.

### **Linux**[edit](#)

To view the current value for the vm.max\_map\_count setting, run:

**Otherwise since the docker compose file in the documentation is of 3 nodes so instead use 1 single node of es 01**

**with same default vm max limit and memlimit of 1g it will work**