**Installation of Elasticsearch Logtash and Kibana**

**Requirements**

* Docker 17.05 or higher
* Docker-Compose 3 or higher
* 4GB RAM (For Windows and MacOS make sure Docker's VM has more than 4GB+ memory.)

1. Clone the Repository

$ git clone https://github.com/sherifabdlnaby/elastdocker.git

1. Initialize Elasticsearch Keystore and TLS Self-Signed Certificates

$ cd elastdocker  
$ make setup

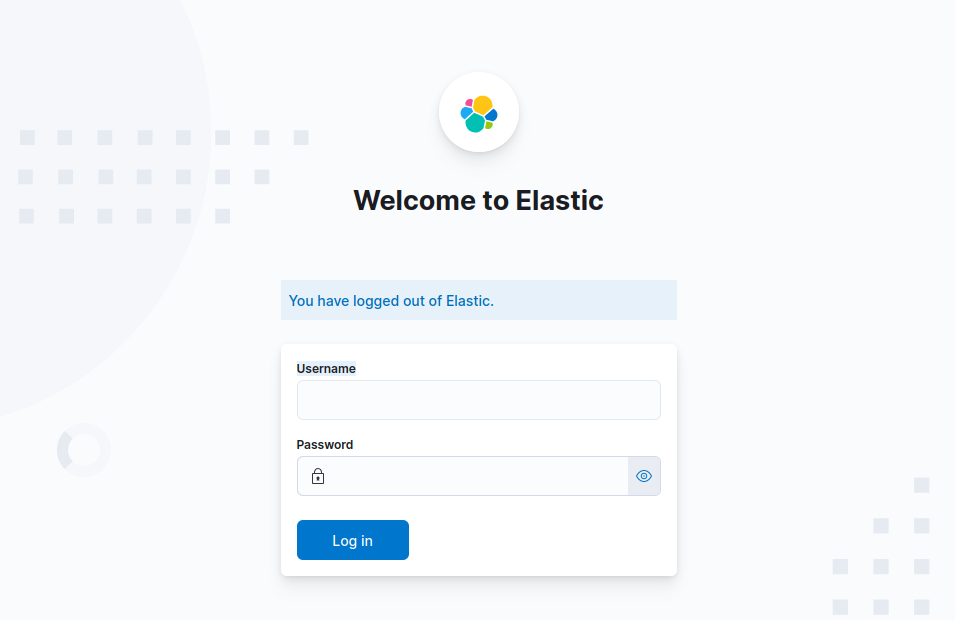
Note:  
For Linux's docker hosts only. By default virtual memory is not enough so run the next command as root sysctl -w vm.max\_map\_count=262144

1. Start Elastic Stack

$ make elk    
​  
OR       
​  
$ docker-compose up -d

1. Visit Kibana at <https://localhost:5601> or https://<your\_ip>:5601

* Default Username: elastic, Password: changeme



Note: ​Kibana is configured to use HTTPS, so you'll need to write https:// before localhost:5601 in the browser.

Modify .env file for your needs, most importantly ELASTIC\_PASSWORD that setup your superuser elastic's password.

## **Create ELK Snapshot**

1. Create a local directory inside elastic\_elasticsearch\_1 container to store the Snapshot.

Edit the docker-compose configuration file named: docker-compose.yml

Add the following:

es\_backup:     
es\_backup:/usr/share/elasticsearch/es\_backup

Like this

version: '3.5'  
​  
# To Join any other app setup using another network, change name and set external = true  
networks:  
 default:  
   name: elastic  
   external: false  
​  
# will contain all elasticsearch data.  
volumes:  
 elasticsearch-data:  
 es\_backup:          
​  
secrets:  
 elasticsearch.keystore:  
   file: ./secrets/keystore/elasticsearch.keystore  
 elastic.ca:  
   file: ./secrets/certs/ca/ca.crt  
 elasticsearch.certificate:  
   file: ./secrets/certs/elasticsearch/elasticsearch.crt  
 elasticsearch.key:  
   file: ./secrets/certs/elasticsearch/elasticsearch.key  
 kibana.certificate:  
   file: ./secrets/certs/kibana/kibana.crt  
 kibana.key:  
   file: ./secrets/certs/kibana/kibana.key  
​  
services:  
 elasticsearch:  
   image: docker.elastic.co/elasticsearch/elasticsearch:${ELK\_VERSION}  
   restart: unless-stopped  
   environment:  
     ELASTIC\_USERNAME: ${ELASTIC\_USERNAME}  
     ELASTIC\_PASSWORD: ${ELASTIC\_PASSWORD}  
     ELASTIC\_CLUSTER\_NAME: ${ELASTIC\_CLUSTER\_NAME}  
     ELASTIC\_NODE\_NAME: ${ELASTIC\_NODE\_NAME}  
     ELASTIC\_INIT\_MASTER\_NODE: ${ELASTIC\_INIT\_MASTER\_NODE}  
     ELASTIC\_DISCOVERY\_SEEDS: ${ELASTIC\_DISCOVERY\_SEEDS}  
     ES\_JAVA\_OPTS: "-Xmx${ELASTICSEARCH\_HEAP} -Xms${ELASTICSEARCH\_HEAP} -Des.enforce.bootstrap.checks=true -Dlog4j2.formatMsgNoLookups=true"  
     bootstrap.memory\_lock: "true"  
   volumes:  
     - elasticsearch-data:/usr/share/elasticsearch/data  
     - es\_backup:/usr/share/elasticsearch/es\_backup    
     - ./elasticsearch/config/elasticsearch.yml:/usr/share/elasticsearch/config/elasticsearch.yml  
     - ./elasticsearch/config/log4j2.properties:/usr/share/elasticsearch/config/log4j2.properties  
   secrets:  
     - source: elasticsearch.keystore  
       target: /usr/share/elasticsearch/config/elasticsearch.keystore  
     - source: elastic.ca  
       target: /usr/share/elasticsearch/config/certs/ca.crt  
     - source: elasticsearch.certificate  
       target: /usr/share/elasticsearch/config/certs/elasticsearch.crt  
     - source: elasticsearch.key  
       target: /usr/share/elasticsearch/config/certs/elasticsearch.key

1. Change the ownership of the es\_backup.

Access elasticsearch terminal

docker exec -it elastic\_elasticsearch\_1 bash

Change the ownership

chown -R elasticsearch:elasticsearch es\_backup

1. Edit the Elasticsearch configuration file named: elasticsearch.yml

vi elasticsearch/config/elasticsearch.yml

Add the following line at the end of the file.

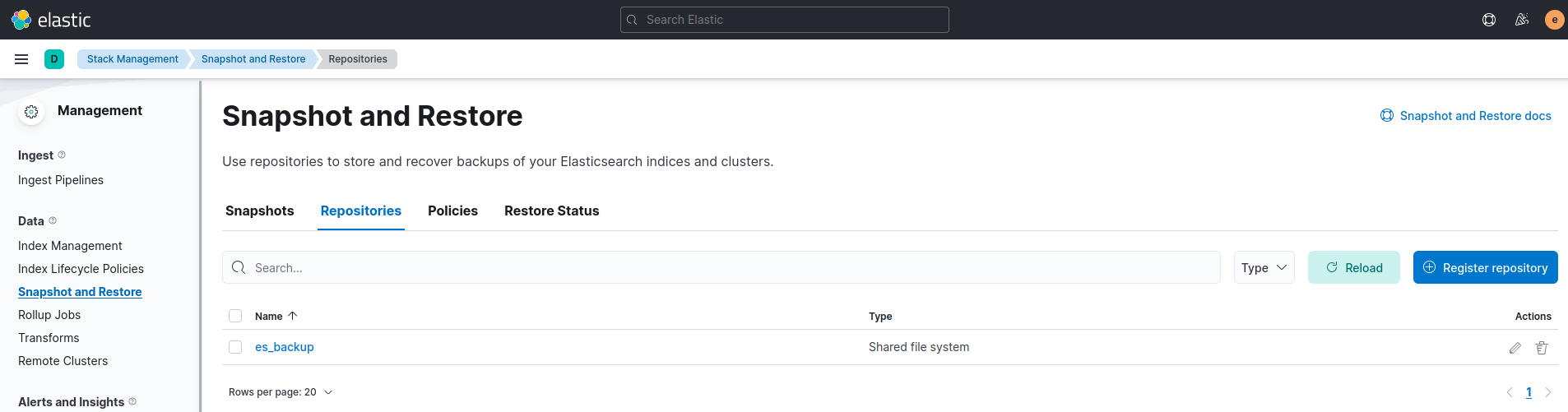
path.repo: ["/usr/share/elasticsearch/es\_backup"]

Stop and start ELK containers

$ docker-compose down  
​  
$ docker-compose up -d

1. Register a new Snapshot repository

Open Kibana goto Management > Stack Management > Snapshot and Restore > Repositories > Register repository

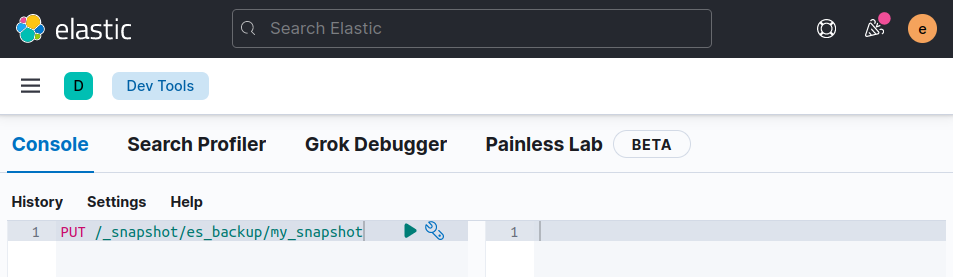


1. Create snapshot of all the indices

Open Kibana goto Management > Dev Tools

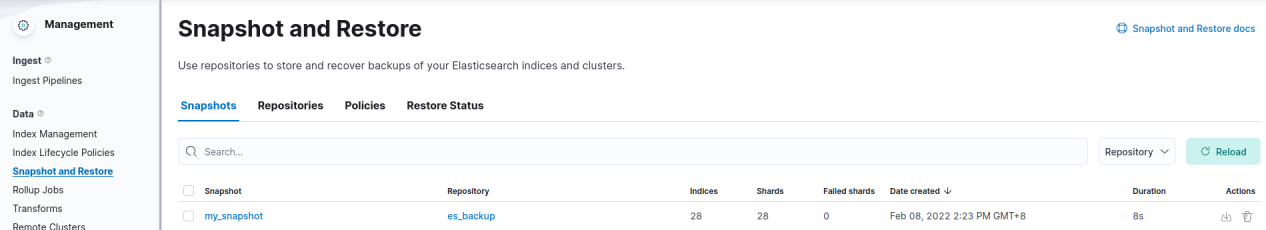
PUT /\_snapshot/es\_backup/my\_snapshot

* In our example, we created a snapshot named: my\_snapshot.
* In our example, we stored this snapshot inside the repository named: es\_backup



Check the snapshot is created.

Open Kibana goto Management > Stack Management > Snapshot and Restore > Snapshots



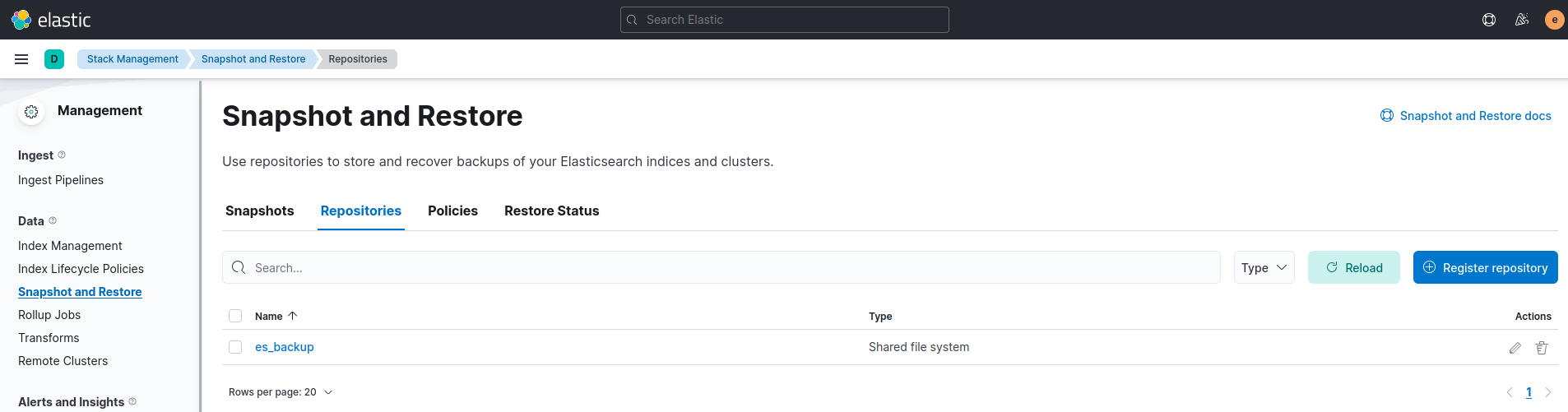
## **Restore ELK Snapshot**

1. Copy repository folder in elastic\_elasticsearch\_1 container

docker cp -a es\_backup/. elastic\_elasticsearch\_1:/usr/share/elasticsearch/es\_backup/

1. Register a new Snapshot repository

Open Kibana goto Management > Stack Management > Snapshot and Restore > Repositories and click Register repository



1. Restore the snapshot

Open Kibana goto Management > Stack Management > Snapshot and Restore and click restore

