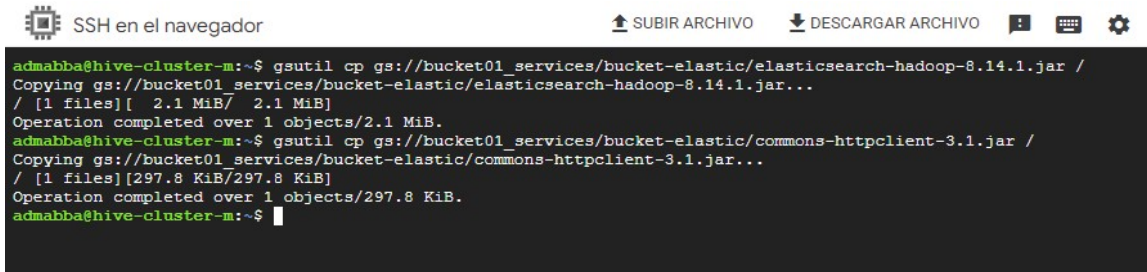


## Elasticsearch for Apache Hadoop

### Parte 1 – Configuración ES-Hadoop

Se crea clúster con nombre hive-cluster, en la foto se realiza la copia de los recursos .jar al filesystem del clúster.

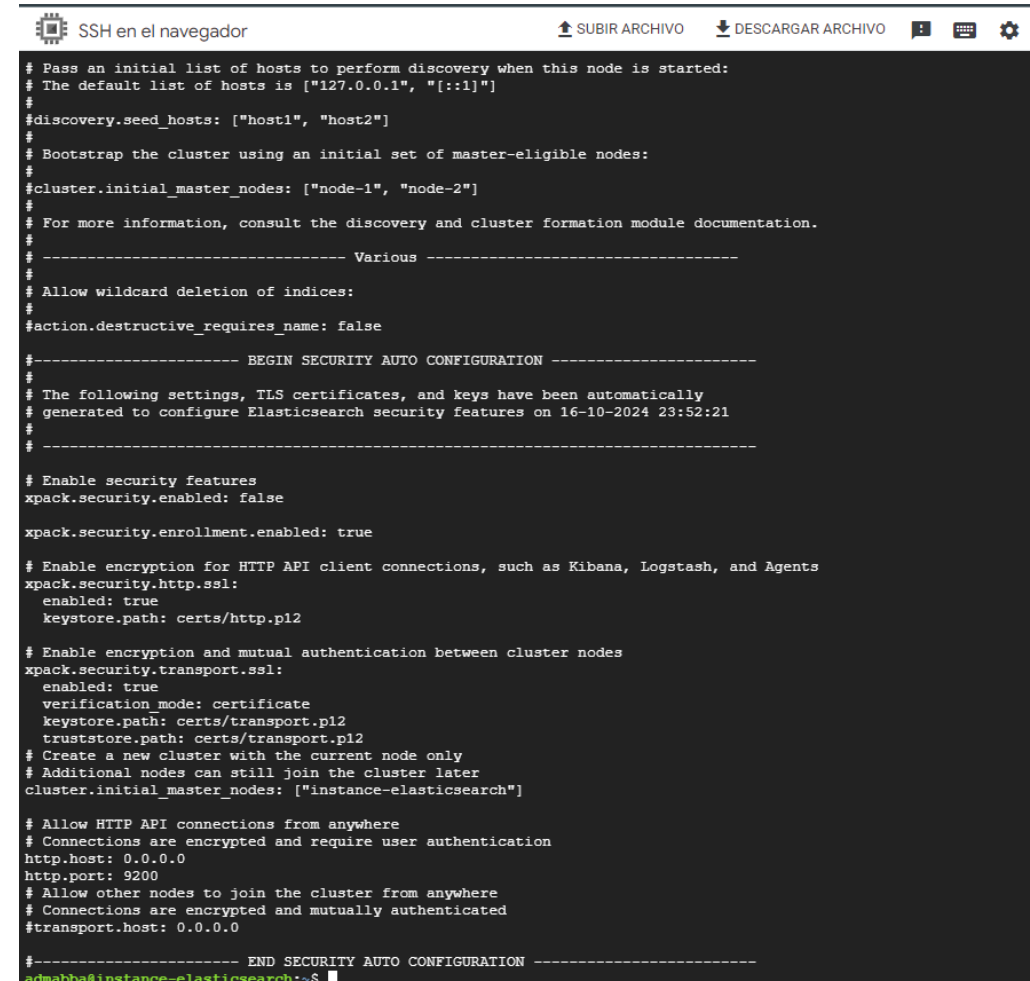


```
SSH en el navegador SUBIR ARCHIVO DESCARGAR ARCHIVO

admabba@hive-cluster-m:~$ gsutil cp gs://bucket01_services/bucket-elastic/elasticsearch-hadoop-8.14.1.jar /
Copying gs://bucket01_services/bucket-elastic/elasticsearch-hadoop-8.14.1.jar...
/ [1 files][ 2.1 MiB/ 2.1 MiB]
Operation completed over 1 objects/2.1 MiB.
admabba@hive-cluster-m:~$ gsutil cp gs://bucket01_services/bucket-elastic/commons-httpclient-3.1.jar /
Copying gs://bucket01_services/bucket-elastic/commons-httpclient-3.1.jar...
/ [1 files][297.8 KiB/297.8 KiB]
Operation completed over 1 objects/297.8 KiB.
admabba@hive-cluster-m:~$
```

### Parte 2 – Configuración server Elasticsearch

Se crea instancia instancia-elasticsearch se agrega a la red las ip de mi local y la de la instancia hive-cluster donde se encuentra el clúster, y se crean dos reglas firewall, allow-elasticsearch y allow-kibana. Por otra parte, se configura el archivo elasticsearch.yml



```
SSH en el navegador SUBIR ARCHIVO DESCARGAR ARCHIVO

# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
#discovery.seed_hosts: ["host1", "host2"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#cluster.initial_master_nodes: ["node-1", "node-2"]
#
# For more information, consult the discovery and cluster formation module documentation.
#
# ----- Various -----
#
# Allow wildcard deletion of indices:
#
#action.destructive_requires_name: false
#
#----- BEGIN SECURITY AUTO CONFIGURATION -----
#
# The following settings, TLS certificates, and keys have been automatically
# generated to configure Elasticsearch security features on 16-10-2024 23:52:21
#
# -----
#
# Enable security features
xpack.security.enabled: false

xpack.security.enrollment.enabled: true

# Enable encryption for HTTP API client connections, such as Kibana, Logstash, and Agents
xpack.security.http.ssl:
  enabled: true
  keystore.path: certs/http.p12

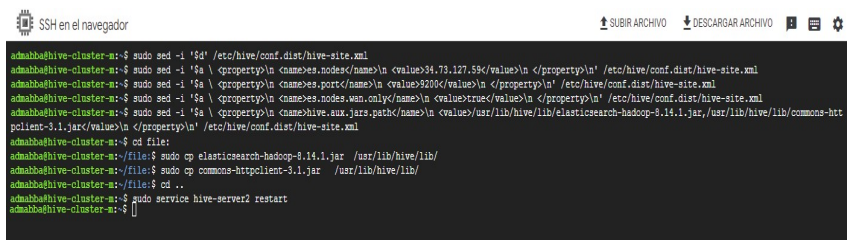
# Enable encryption and mutual authentication between cluster nodes
xpack.security.transport.ssl:
  enabled: true
  verification_mode: certificate
  keystore.path: certs/transport.p12
  truststore.path: certs/transport.p12
# Create a new cluster with the current node only
# Additional nodes can still join the cluster later
cluster.initial_master_nodes: ["instance-elasticsearch"]

# Allow HTTP API connections from anywhere
# Connections are encrypted and require user authentication
http.host: 0.0.0.0
http.port: 9200

# Allow other nodes to join the cluster from anywhere
# Connections are encrypted and mutually authenticated
#transport.host: 0.0.0.0

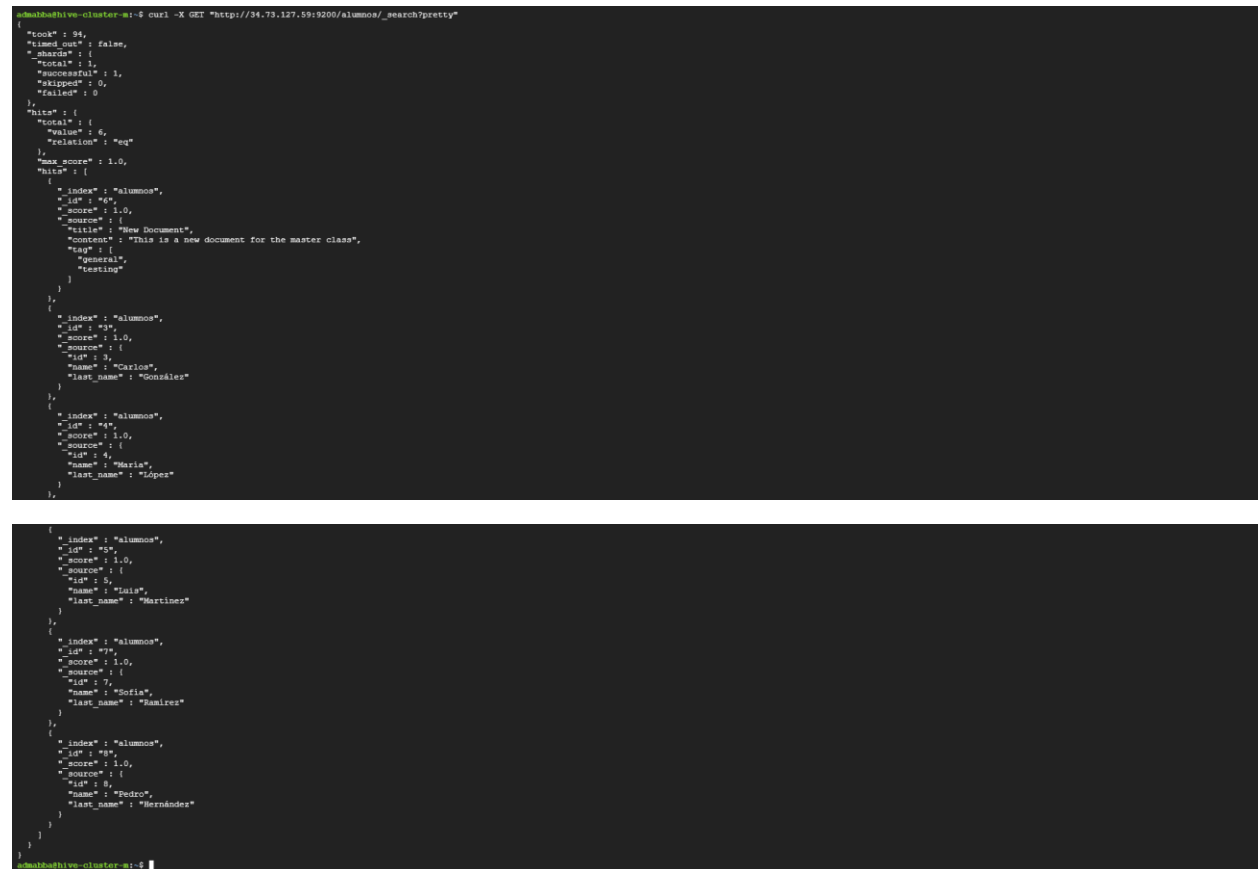
#----- END SECURITY AUTO CONFIGURATION -----
admabba@instance-elasticsearch:~$
```

## Parte 3 – Configuración del Clúster Hadoop de conexión



## Parte 4 – A conectar datos

Se crea a través del POST la creación del índice de alumnos y se realiza una petición GET al `_search` para obtener todos los documentos que pertenecen al índice.



## Parte 5 – Kibana

