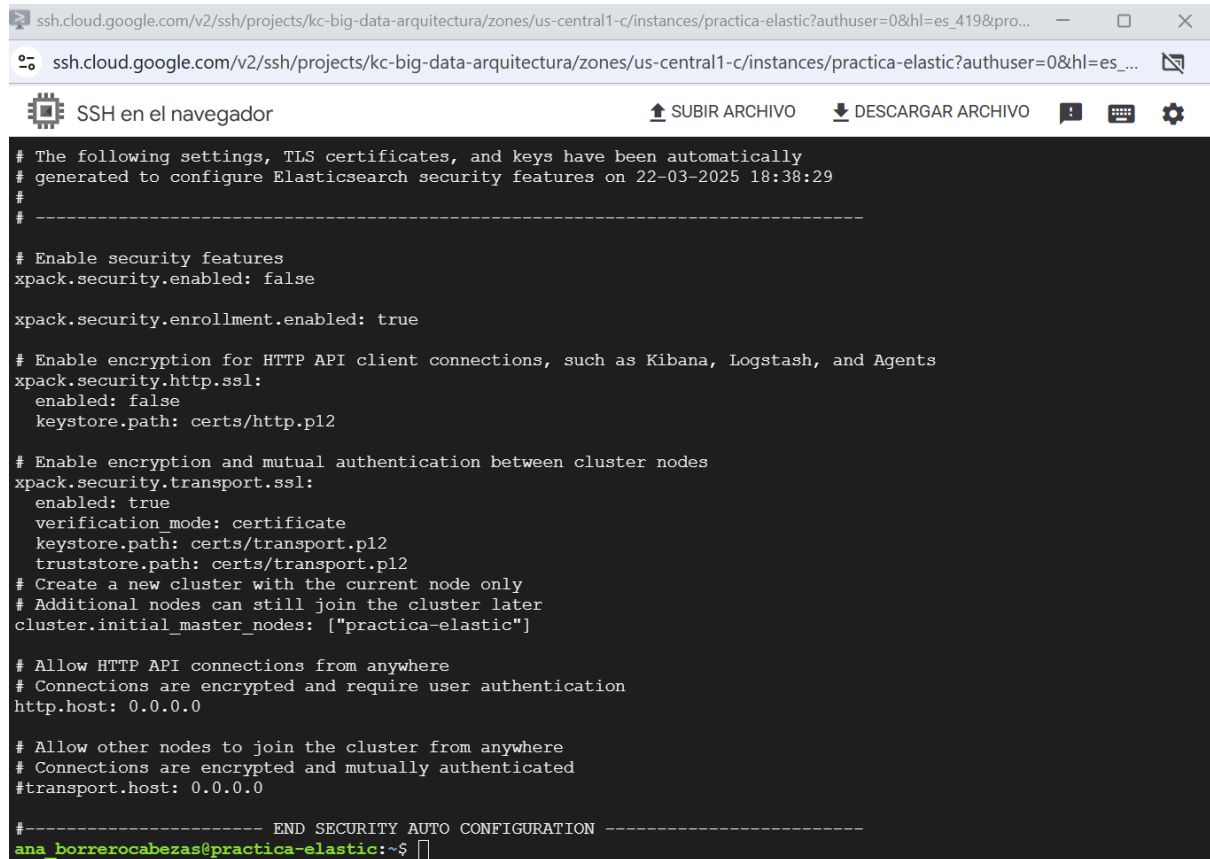


PARTE 2 - Configuración server Elasticsearch

“Captura de pantalla de la consola del server Elastic donde se vea la configuración de elastic, desde 'Enable security features' hasta el final”

He configurado tanto Elasticsearch como Kibana por si me hacía falta para el apartado 5.



The screenshot shows a web browser window with the address bar displaying `ssh.cloud.google.com/v2/ssh/projects/kc-big-data-arquitectura/zones/us-central1-c/instances/practica-elastic?authuser=0&hl=es_4198&pro...`. The browser interface includes a title bar, a toolbar with icons for SSH, file upload, file download, and settings, and a terminal window. The terminal window displays the following configuration for Elasticsearch security features:

```
# The following settings, TLS certificates, and keys have been automatically
# generated to configure Elasticsearch security features on 22-03-2025 18:38:29
#
# -----

# 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: false
  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: ["practica-elastic"]

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

# 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 -----
ana_borrerocabezas@practica-elastic:~$
```