######################### APM Server Configuration #########################

################################ APM Server ################################

apm-server:

# Defines the host and port the server is listening on. Use "unix:/path/to.sock" to listen on a unix domain socket.

host: "0.0.0.0:8200"

#---------------------------- APM Server - Secure Communication with Agents ----------------------------

# Enable authentication using Secret token

auth:

secret\_token: '${ELASTIC\_APM\_SECRET\_TOKEN}'

# Enable secure communication between APM agents and the server. By default ssl is disabled.

ssl:

enabled: true

# Path to file containing the certificate for server authentication.

# Needs to be configured when ssl is enabled.

certificate: "/certs/apm-server.crt"

# Path to file containing server certificate key.

# Needs to be configured when ssl is enabled.

key: "/certs/apm-server.key"

#================================ Outputs =================================

# Configure the output to use when sending the data collected by apm-server.

#-------------------------- Elasticsearch output --------------------------

output.elasticsearch:

# Array of hosts to connect to.

# Scheme and port can be left out and will be set to the default (`http` and `9200`).

# In case you specify and additional path, the scheme is required: `http://elasticsearch:9200/path`.

# IPv6 addresses should always be defined as: `https://[2001:db8::1]:9200`.

hosts: '${ELASTICSEARCH\_HOST\_PORT}'

# Boolean flag to enable or disable the output module.

enabled: true

# Protocol - either `http` (default) or `https`.

protocol: "https"

# Authentication credentials

username: '${ELASTIC\_USERNAME}'

password: '${ELASTIC\_PASSWORD}'

# Enable custom SSL settings. Set to false to ignore custom SSL settings for secure communication.

ssl.enabled: true

# List of root certificates for HTTPS server verifications.

ssl.certificate\_authorities: ["/certs/ca.crt"]

# Certificate for SSL client authentication.

ssl.certificate: "/certs/apm-server.crt"

# Client Certificate Key

ssl.key: "/certs/apm-server.key"

#============================= X-pack Monitoring =============================

# APM server can export internal metrics to a central Elasticsearch monitoring

# cluster. This requires x-pack monitoring to be enabled in Elasticsearch. The

# reporting is disabled by default.

# Set to true to enable the monitoring reporter.

monitoring.enabled: true

# Most settings from the Elasticsearch output are accepted here as well.

# Note that these settings should be configured to point to your Elasticsearch \*monitoring\* cluster.

# Any setting that is not set is automatically inherited from the Elasticsearch

# output configuration. This means that if you have the Elasticsearch output configured,

# you can simply uncomment the following line.

monitoring.elasticsearch:

# Protocol - either `http` (default) or `https`.

protocol: "https"

# Authentication credentials

username: '${ELASTIC\_USERNAME}'

password: '${ELASTIC\_PASSWORD}'

# Array of hosts to connect to.

# Scheme and port can be left out and will be set to the default (`http` and `9200`).

# In case you specify and additional path, the scheme is required: `http://elasticsearch:9200/path`.

# IPv6 addresses should always be defined as: `https://[2001:db8::1]:9200`.

hosts: '${ELASTICSEARCH\_HOST\_PORT}'

# Enable custom SSL settings. Set to false to ignore custom SSL settings for secure communication.

ssl.enabled: true

# List of root certificates for HTTPS server verifications.

ssl.certificate\_authorities: ["/certs/ca.crt"]

# Certificate for SSL client authentication.

ssl.certificate: "/certs/apm-server.crt"

# Client Certificate Key

ssl.key: "/certs/apm-server.key"