- •Wazuh deployed using Docker compose.
  Guide: https://documentation.wazuh.com/current/deployment-options/docker/wazuh-container.html#single-node-deployment
- •Outlook account

Docker compose Configuration:

To allow Wazuh have the capability to authenticate to the outlook SMTP, I will leverage the use of Postfix image from https://github.com/juanluisbaptiste/docker-postfix.

- •The environment variables `SMTP_USERNAME` & `SMTP_PASSWORD` needs to be configured with your Outlook accounts credentials within the `docker-compose.yml` which would look like the below:

```
# Wazuh App Copyright (C) 2017, Wazuh Inc. (License GPLv2)
version: '3.7'
services:
 smtp-relay:
  image: juanluisbaptiste/postfix
  environment:
   SMTP_SERVER: smtp-mail.outlook.com
   SMTP_USERNAME: MYEMAIL@outlook.com
   SMTP_PASSWORD: MYPASSWORD
   SERVER_HOSTNAME: wazuh.com
  ports:
   - 25:25/tcp
 wazuh.manager:
  image: wazuh/wazuh-manager:4.3.4
  hostname: wazuh.manager
  restart: always
  ports:
   - "1514:1514"
   - "1515:1515"
   - "514:514/udp"
   - "55000:55000"
  environment:
   - INDEXER_URL=https://wazuh.indexer:9200
   - INDEXER_USERNAME=admin
   - INDEXER_PASSWORD=SecretPassword
   - FILEBEAT_SSL_VERIFICATION_MODE=full
```

```
    - SSL_CERTIFICATE_AUTHORITIES=/etc/ssl/root-ca.pem
    - SSL_CERTIFICATE=/etc/ssl/filebeat.pem
    - SSL_KEY=/etc/ssl/filebeat.key
    - API_USERNAME=wazuh-wui
    - API_PASSWORD=Mypassword
  volumes:
    - wazuh_api_configuration:/var/ossec/api/configuration
    - wazuh_etc:/var/ossec/etc
    - wazuh_logs:/var/ossec/logs
    - wazuh_queue:/var/ossec/queue
    - wazuh_var_multigroups:/var/ossec/var/multigroups
    - wazuh_integrations:/var/ossec/integrations
    - wazuh_active_response:/var/ossec/active-response/bin
    - wazuh_agentless:/var/ossec/agentless
    - wazuh_wodles:/var/ossec/wodles
    - filebeat_etc:/etc/filebeat
    - filebeat_var:/var/lib/filebeat
    - ./config/wazuh_indexer_ssl_certs/root-ca-manager.pem:/etc/ssl/root-ca.pem
    - ./config/wazuh_indexer_ssl_certs/wazuh.manager.pem:/etc/ssl/filebeat.pem
    - ./config/wazuh_indexer_ssl_certs/wazuh.manager-key.pem:/etc/ssl/filebeat.key
    - ./config/wazuh_cluster/wazuh_manager.conf:/wazuh-config-mount/etc/ossec.conf
 wazuh.indexer:
  image: wazuh/wazuh-indexer:4.3.4
  hostname: wazuh.indexer
  restart: always
  ports:
    - "9200:9200"
  environment:
    - "OPENSEARCH_JAVA_OPTS=-Xms2048m -Xmx2048m"
  ulimits:
    memlock:
      soft: -1
      hard: -1
    nofile:
      soft: 65536
      hard: 65536
  volumes:
    - wazuh-indexer-data:/var/lib/wazuh-indexer
    - ./config/wazuh_indexer_ssl_certs/root-ca.pem:/usr/share/wazuh-indexer/config/certs/
root-ca.pem
    - ./config/wazuh_indexer_ssl_certs/wazuh.indexer-key.pem:/usr/share/wazuh-indexer/
config/certs/wazuh.indexer.key
    - ./config/wazuh_indexer_ssl_certs/wazuh.indexer.pem:/usr/share/wazuh-indexer/
config/certs/wazuh.indexer.pem
```

```
    - ./config/wazuh_indexer_ssl_certs/admin.pem:/usr/share/wazuh-indexer/config/certs/
admin.pem
    - ./config/wazuh_indexer_ssl_certs/admin-key.pem:/usr/share/wazuh-indexer/config/
certs/admin-key.pem
    - ./config/wazuh_indexer/wazuh.indexer.yml:/usr/share/wazuh-indexer/config/
opensearch.yml
    - ./config/wazuh_indexer/internal_users.yml:/usr/share/wazuh-indexer/plugins/
opensearch-security/securityconfig/internal_users.yml
 wazuh.dashboard:
   image: wazuh/wazuh-dashboard:4.3.4
   hostname: wazuh.dashboard
   restart: always
   ports:
    - 443:5601
   environment:
    - "--max-old-space-size=4096"
    - INDEXER_USERNAME=admin
    - INDEXER_PASSWORD=SecretPassword
    - WAZUH_API_URL=https://wazuh.manager
    - API_USERNAME=wazuh-wui
    - API_PASSWORD=MyS3cr37P450r.*-
   volumes:
    - ./config/wazuh_indexer_ssl_certs/wazuh.dashboard.pem:/usr/share/wazuh-
dashboard/certs/wazuh-dashboard.pem
    - ./config/wazuh_indexer_ssl_certs/wazuh.dashboard-key.pem:/usr/share/wazuh-
dashboard/certs/wazuh-dashboard-key.pem
    - ./config/wazuh_indexer_ssl_certs/root-ca.pem:/usr/share/wazuh-dashboard/certs/root-
ca.pem
    - ./config/wazuh_dashboard/opensearch_dashboards.yml:/usr/share/wazuh-
dashboard/config/opensearch_dashboards.yml
    - ./config/wazuh_dashboard/wazuh.yml:/usr/share/wazuh-dashboard/data/wazuh/
config/wazuh.yml
   depends_on:
    - wazuh.indexer
   links:
    - wazuh.indexer:wazuh.indexer
    - wazuh.manager:wazuh.manager
volumes:
 wazuh_api_configuration:
 wazuh_etc:
 wazuh_logs:
 wazuh_queue:
 wazuh_var_multigroups:
 wazuh_integrations:
```

```
wazuh_active_response:
wazuh_agentless:
wazuh_wodles:
filebeat_etc:
filebeat_var:
wazuh-indexer-data:
```

- Run `docker-compose up -d`
- Retrieve the Postfix container IP to be used in Wazuh configuration:

```
docker inspect -f '{{range.NetworkSettings.Networks}}
{{.IPAddress}}{{end}}' $(docker ps | grep -i smtp | awk '{print
$1}')
```

Wazuh configuration:

- Navigate to the Wazuh UI, `Management` then `configuration` :

- Edit the configuration specifying the SMTP server (IP retrieved previously) and enabling the email notification:

- After restarting the Wazuh manager and having an alert triggered (In my case I've configured it to email all alerts starting from level 3), you should receive an email similar to below (Check the spam):

Wazuh notification - wazuh - Alert level 3 Spam ×

Wazuh [redacted]
À moi

Pourquoi ce message figure-t-il dans les spams ? Il est semblable à

Signaler comme non-spam

anglais > français Traduire le message

Wazuh Notification.
2022 Jun 18 00:27:45

Received From: wazuh->wazuh-monitord
Rule: 502 fired (level 3) -> "Ossec server started."
Portion of the log(s):

ossec: Ossec started.