**Wazuh Setup Knowledge Base**

**Table of Contents**

1. Introduction
2. Prerequisites
3. Elasticsearch Installation and Configuration
4. Wazuh Manager Installation and Configuration
5. Filebeat Installation and Configuration
6. Kibana Installation and Configuration
7. Troubleshooting Tips

**1. Introduction**

This document provides a step-by-step guide to set up Wazuh with Elasticsearch, Filebeat, and Kibana. It also includes Postfix configuration for email notifications.

**2. Prerequisites**

* Ubuntu Server (20.04 or later)
* Sufficient disk space and memory
* Root or sudo access
* Network connectivity

**3. Elasticsearch Installation and Configuration**

**Step 1:** Install Prerequisites

echo "Installing prerequisites"

apt-get install -y apt-transport-https zip unzip lsb-release curl gnupg

**Step 2:** Install Elasticsearch

echo "Installing Elasticsearch"

curl -s https://artifacts.elastic.co/GPG-KEY-elasticsearch | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/elasticsearch.gpg --import && chmod 644 /usr/share/keyrings/elasticsearch.gpg

echo "deb [signed-by=/usr/share/keyrings/elasticsearch.gpg] https://artifacts.elastic.co/packages/7.x/apt stable main" | tee /etc/apt/sources.list.d/elastic-7.x.list

apt-get update

apt-get install -y elasticsearch=7.17.13

**Step 3:** Configure Elasticsearch

echo "Configuring Elasticsearch"

curl -so /etc/elasticsearch/elasticsearch.yml https://packages.wazuh.com/4.5/tpl/elastic-basic/elasticsearch\_all\_in\_one.yml

curl -so /usr/share/elasticsearch/instances.yml <https://packages.wazuh.com/4.5/tpl/elastic-basic/instances_aio.yml>

**Step 4:** Generate Certificates

echo "Generating certificates"

sudo /usr/share/elasticsearch/bin/elasticsearch-certutil cert ca --pem --in /usr/share/elasticsearch/instances.yml --keep-ca-key --out ~/certs.zip

unzip ~/certs.zip -d ~/certs

mkdir -p /etc/elasticsearch/certs/ca

cp -R ~/certs/ca/ ~/certs/elasticsearch/\* /etc/elasticsearch/certs/

chown -R elasticsearch: /etc/elasticsearch/certs

chmod -R 500 /etc/elasticsearch/certs

chmod 400 /etc/elasticsearch/certs/ca/ca.\* /etc/elasticsearch/certs/elasticsearch.\*

**Step 5:** Start Elasticsearch

echo "Starting Elasticsearch service"

systemctl daemon-reload

systemctl enable elasticsearch

systemctl start elasticsearch

**4. Wazuh Manager Installation and Configuration**

**Step 1:** Install Wazuh Manager

echo "Installing Wazuh server"

curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg

echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list

apt-get update

apt-get install -y wazuh-manager=4.5.4-1

**Step 2:** Start Wazuh Manager

echo "Starting Wazuh Manager service"

systemctl daemon-reload

systemctl enable wazuh-manager

systemctl start wazuh-manager

systemctl status wazuh-manager

**5. Filebeat Installation and Configuration**

**Step 1:** Install Filebeat

echo "Installing Filebeat version 7.17.13"

apt-get install -y filebeat=7.17.13

**Step 2:** Configure Filebeat

echo "Configuring Filebeat"

curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/4.5/tpl/elastic-basic/filebeat\_all\_in\_one.yml

curl -so /etc/filebeat/wazuh-template.json https://raw.githubusercontent.com/wazuh/wazuh/v4.5.4/extensions/elasticsearch/7.x/wazuh-template.json

chmod go+r /etc/filebeat/wazuh-template.json

**Step 3:** Install Wazuh Module for Filebeat

echo "Installing Wazuh Filebeat module"

curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.2.tar.gz | tar -xvz -C /usr/share/filebeat/module

**Step 4:** Start Filebeat

echo "Starting Filebeat service"

systemctl daemon-reload

systemctl enable filebeat

systemctl start filebeat

filebeat test output

**6. Kibana Installation and Configuration**

**Step 1:** Install Kibana

echo "Installing Kibana version 7.17.13"

apt-get install -y kibana=7.17.13

**Step 2:** Configure Certificates

echo "Setting up certificates for Kibana"

mkdir -p /etc/kibana/certs/ca

cp -R /etc/elasticsearch/certs/ca/ /etc/kibana/certs/

cp /etc/elasticsearch/certs/elasticsearch.key /etc/kibana/certs/kibana.key

cp /etc/elasticsearch/certs/elasticsearch.crt /etc/kibana/certs/kibana.crt

chown -R kibana:kibana /etc/kibana/

chmod -R 500 /etc/kibana/certs

chmod 440 /etc/kibana/certs/ca/ca.\* /etc/kibana/certs/kibana.\*

**Step 3:** Install Wazuh Plugin

echo "Installing Wazuh plugin for Kibana"

sudo -u kibana /usr/share/kibana/bin/kibana-plugin install <https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana-4.5.4_7.17.13-1.zip>

**Step 4:** Start Kibana

echo "Starting Kibana service"

systemctl daemon-reload

systemctl enable kibana

systemctl start kibana

**7. Troubleshooting Tips**

* Check Elasticsearch logs: journalctl -u elasticsearch
* Check Wazuh Manager logs: journalctl -u wazuh-manager
* Check Filebeat logs: journalctl -u filebeat
* Check Kibana logs: journalctl -u kibana