Wazuh Configuration:

1. **Wazuh Manager Installed and Running:**
2. **Wazuh Web UI Configured:**
3. **Configure Filebeat to send Wazuh logs to Elasticsearch**.

Wazuh Manager produces logs and alerts.**Filebeat** reads those logs and ships them to **Elasticsearch**, where they can be visualized in the **Wazuh Dashboard**.

**Password z6NAo3c?e1EXnc.FH5jYXe.v+NW7an8q**

**unmae= admin z6NAo3c?e1EXnc.FH5jYXe.v+NW7an8q**

**Wazuh Configuration:**

Step 1: Update your system

sudo apt update && sudo apt upgrade -y

Step 2: Run Wazuh's official installation script

This script will install everything: Wazuh Manager, OpenSearch, Filebeat, and Wazuh Dashboard.

curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh

chmod +x wazuh-install.sh

sudo ./wazuh-install.sh -a

after that put on ip on browser and put admin and password = hv7C2z9?L5jZmoACIc\*KNVImVFD?ujbh

sudo systemctl status wazuh-manager

sudo systemctl status wazuh-dashboard

sudo systemctl status filebeat

sudo systemctl status wazuh-indexer

sudo systemctl restart wazuh-manager wazuh-dashboard filebeat wazuh-indexer

sudo systemctl enable wazuh-manager wazuh-dashboard filebeat wazuh-indexer

Installing Wazuh agent:

wazuh-authd:

wazuh-authd is the **Wazuh authentication daemon**, used to **register agents automatically** to the Wazuh Manager without copying keys manually.

It is part of the **Wazuh Manager package** but **not always installed as a separate systemd service**.

On wazuh manager if wazuh-authd is not installed with wazuh manager package we have to configure it manually. Step for it:

1)sudo systemctl enable wazuh-authd --now

Use this command to check it is installed/created or not

1. sudo nano /etc/systemd/system/wazuh-authd.service

Paste following line:

[Unit]

Description=Wazuh Auth Daemon

After=network.target wazuh-manager.service

[Service]

ExecStart=/var/ossec/bin/wazuh-authd

Restart=always

User=root

[Install]

WantedBy=multi-user.target

1. sudo systemctl daemon-reexec
2. sudo systemctl daemon-reload
3. sudo systemctl enable wazuh-authd --now
4. ps aux | grep wazuh-authd

Verify is it running or not using above command.

1. On mail server:

wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent\_4.12.0-1\_amd64.debt

dpkg -i wazuh-agent\_4.12.0-1\_amd64.debt

nano /var/ossec/etc/ossec.conf

<server>

<address>192.168.80.176</address>

</server>

systemctl enable wazuh-agent

systemctl start wazuh-agent

sudo /var/ossec/bin/agent-auth -m 192.168.80.176

Above command securely registers agent to wazuh and exchange keys.

Adding custom log collection

Why custom logs(logs of postfix,dovecot,roundcube)- because wazuh agent only collects system logs not application logs because application logs files differ in different system .so we have to forward application specific logs to wazuh manually by configuring agent to do this.

Steps:

sudo nano /var/ossec/etc/ossec.conf

Paste following lines:

<localfile>

<log\_format>syslog</log\_format>

<location>/var/log/mail.log</location>

</localfile>

sudo systemctl restart wazuh-agent

For prometeheus:

Same as above

To add application logs as prometheus donot directly store log sin .log file therefore we are directing logs from journalctl to /var/log/prometheus.log file.

Steps:

sudo systemctl edit prometheus.service

[Service]

ExecStart=

ExecStart=/usr/local/bin/prometheus --config.file=/etc/prometheus/prometheus.yml --log.level=info --log.format=logfmt >> /var/log/prometheus.log 2>&1

sudo systemctl daemon-reexec

sudo systemctl daemon-reload

sudo systemctl restart prometheus

Now create file in directory /var/log/prometheus.log in this logs will get stored.

Adding custom/application logs:

/var/ossec/etc/ossec.conf

<localfile>

<log\_format>syslog</log\_format>

<location>/var/log/prometheus.log</location>

</localfile>

<localfile>

<log\_format>syslog</log\_format>

<location>/var/log/grafana/grafana.log</location>

</localfile>

sudo systemctl restart wazuh-agent

1. opnsense:

Adding it to wazuh as agent

To monitor **OPNsense** using **Wazuh**, we cannot install a Wazuh agent directly on OPNsense because it's based on FreeBSD and the Wazuh agent is not officially supported there.

However, we **can still integrate OPNsense logs into Wazuh** using **remote syslog forwarding**. Here’s how to do it **step-by-step**, along with **why** each step is necessary.

**Forward OPNsense logs to Wazuh server** via syslog → **analyze and visualize** in the Wazuh dashboard.

### Step 1: Enable Remote Syslog in OPNsense

📌 **Why:** To forward logs to your Wazuh manager for analysis.

Login to the **OPNsense Web UI**.

Go to:

System → Settings → Logging / targets

Click ➕ “Add” to create a new log target:

**Target:** 192.168.80.176 (your Wazuh server IP)

**Port:** 514

**Transport:** UDP

**Format:** BSD syslog

**Facility:** any

**Severity:** info

Check ✅ “Enable”

Click **Save** and **Apply**

### Step 2: Configure Wazuh Manager to Receive Syslog Logs

📌 **Why:** Wazuh needs to listen for logs on port 514 (UDP) and process them with decoders/rules.

Open /var/ossec/etc/ossec.conf on the Wazuh Manager.

Add the following inside the <ossec\_config> block:

<remote>

<connection>syslog</connection>

<port>514</port>

<protocol>udp</protocol>

</remote>

Save and close the file.

Allow port 514 in your firewall (if using ufw):

sudo ufw allow 514/udp

Restart Wazuh Manager:

sudo systemctl restart wazuh-manager

### Step 3: Check Logs on Wazuh

📌 **Why:** Confirm that Wazuh is receiving OPNsense logs.

Run this command:

sudo tail -f /var/ossec/logs/ossec.log

You should see log entries from the OPNsense IP.

### Step 4: Use Filebeat (optional) to forward OPNsense logs to Wazuh Dashboard

📌 **Why:** If logs don’t show in the Wazuh Dashboard, Filebeat helps ship them to the indexer (OpenSearch) correctly.

Check /var/ossec/logs/active-responses.log or /var/ossec/logs/alerts/alerts.json.

If needed, modify Filebeat config:

Path: /etc/filebeat/filebeat.yml

Example:

filebeat.inputs:

- type: log

enabled: true

paths:

- /var/ossec/logs/alerts/alerts.json

output.elasticsearch:

hosts: ["https://localhost:9200"]

username: "admin"

password: "admin"

setup.kibana:

host: "https://localhost:5601"

Restart Filebeat:

sudo systemctl restart filebeat

### Step 5: Add Custom Wazuh Decoders & Rules (if needed)

📌 **Why:** To parse OPNsense log format for accurate alerts.

Decoder path:

/var/ossec/etc/decoders/local\_decoder.xml

Rules path:

/var/ossec/etc/rules/local\_rules.xml

We can write rules like:

<rule id="100020" level="5">

<decoded\_as>syslog</decoded\_as>

<program\_name>filterlog</program\_name>

<description>OPNsense firewall event</description>

</rule>

Then restart Wazuh manager:

sudo systemctl restart wazuh-manager

## ✅ Summary

| **Step** | **Action** | **Why** |
| --- | --- | --- |
| 1 | Enable syslog forwarding in OPNsense | To send logs to Wazuh |
| 2 | Configure Wazuh to receive UDP logs | To accept incoming OPNsense logs |
| 3 | Check logs | Verify successful log forwarding |
| 4 | (Optional) Configure Filebeat | Ensure logs appear in Wazuh dashboard |
| 5 | Add custom decoders/rules | Improve parsing and alerting |

Whatsare components of wazuh ? what each does?

It contain rule baesd detection, can I modify that rule or add my own rules.

How authentication is done here? Key baesd or pass word based?

From opnsense does not support wazuh agent so we have to configure it to send syslog logs but it is transferred in plain text then how we can encrypt it or protect it.?

wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent\_4.12.0-1\_arm64.deb && sudo WAZUH\_MANAGER='192.168.80.131' WAZUH\_AGENT\_GROUP='default' WAZUH\_AGENT\_NAME='jenkins' dpkg -i ./wazuh-agent\_4.12.0-1\_arm64.deb

sudo systemctl daemon-reload sudo systemctl enable wazuh-agent sudo systemctl start wazuh-agent