Wazuh-indexer issues

Got it! You opened the **original service file** for wazuh-indexer at:

/usr/lib/systemd/system/wazuh-indexer.service

sudo nano /usr/lib/systemd/system/wazuh-indexer.service

**Important:**

* **Editing this original file directly is possible** but **not recommended** because:
  + Package updates can overwrite your changes.
  + Systemd supports "drop-in" overrides (the /etc/systemd/system/wazuh-indexer.service.d/override.conf file you tried before), which are safer and persist after updates.

**Best Practice: Use drop-in override file to modify the service**

If you want to change settings like TimeoutStartSec or environment variables, do it with:

sudo systemctl edit wazuh-indexer

and add your changes there, for example:

[Service]

TimeoutStartSec=600

**But if you want to edit the original file directly:**

1. Open it with nano:

bash

CopyEdit

sudo nano /usr/lib/systemd/system/wazuh-indexer.service

1. Add or modify the timeout inside the [Service] section:

ini

CopyEdit

[Service]

TimeoutStartSec=600

1. Save and exit.
2. Reload systemd daemon:

bash

CopyEdit

sudo systemctl daemon-reload

1. Restart the service:

bash

CopyEdit

sudo systemctl restart wazuh-indexer

**Summary:**

* Using the **override file** is safer and recommended.
* But if you modify the original file, **always run daemon-reload** afterward.
* Increasing timeout helps if the service needs more startup time.

To check if **Filebeat** or **Logstash** is running and properly forwarding logs to your **Wazuh Indexer**, follow the steps below. These tools are usually used for forwarding logs to Elasticsearch or the Wazuh Indexer in Wazuh setups.

**🧩 Step-by-Step: Check Filebeat and Logstash Status**

**🔹 1. Check if Filebeat is installed and running**

bash

CopyEdit

sudo systemctl status filebeat

**Expected output:**

* active (running) indicates it's running correctly.
* If it’s inactive or failed, logs are your next stop.

**🔹 View Filebeat logs:**

bash

CopyEdit

sudo journalctl -u filebeat -n 50 --no-pager

Or:

bash

CopyEdit

sudo tail -n 50 /var/log/filebeat/filebeat.log

Look for errors like “connection refused”, “unauthorized”, or issues related to Wazuh Indexer/Elasticsearch.

**🔹 2. Check if Logstash is installed and running**

bash

CopyEdit

sudo systemctl status logstash

**Expected output:**

* active (running) means it’s operational.

**🔹 View Logstash logs:**

bash

CopyEdit

sudo journalctl -u logstash -n 50 --no-pager

Or:

bash

CopyEdit

sudo tail -n 50 /var/log/logstash/logstash-plain.log

Look for errors such as pipeline failures, output connection errors, or parsing issues.

**🔍 Step 3: Verify That Logs Are Being Forwarded**

**Option A: Check Output from Filebeat to Wazuh Indexer**

If you're using Filebeat to forward logs directly to Wazuh Indexer:

1. Open Filebeat config:

bash

CopyEdit

sudo nano /etc/filebeat/filebeat.yml

1. Look for the output.elasticsearch or output.logstash section.

Example:

yaml

CopyEdit

output.elasticsearch:

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

1. Test the connection manually:

bash

CopyEdit

curl -X GET http://localhost:9200/\_cluster/health?pretty

or if Wazuh Indexer is running on port 9200:

bash

CopyEdit

curl -X GET http://localhost:9200

You should see JSON output showing cluster\_name, status, etc.

**Option B: View Live Logs Being Sent (Optional)**

You can also “watch” logs being picked up:

bash

CopyEdit

sudo tail -f /var/log/filebeat/filebeat.log

Or for Logstash:

bash

CopyEdit

sudo tail -f /var/log/logstash/logstash-plain.log

**🛠 If Filebeat or Logstash is not running:**

* Start or restart them:

bash

CopyEdit

sudo systemctl restart filebeat

sudo systemctl restart logstash

* Enable them to start on boot:

bash

CopyEdit

sudo systemctl enable filebeat

sudo systemctl enable logstash

**🧠 Summary**

| **Tool** | **Check Status** | **View Logs** |
| --- | --- | --- |
| **Filebeat** | systemctl status filebeat | journalctl -u filebeat or tail /var/log/filebeat/filebeat.log |
| **Logstash** | systemctl status logstash | journalctl -u logstash or tail /var/log/logstash/logstash-plain.log |