ChatGPT

Setting Up ELK (Elasticsearch, Kibana, Filebeat) on Ubuntu WSL

You can run a minimal ELK stack on Ubuntu under WSL by using the Debian packages (apt) instead of RPMs. The steps below adapt your instructions for Ubuntu. We add Elastic's APT repository, install the packages, adjust configurations, and start each service. Because WSL typically lacks `systemd`, we use `service` (or run the binaries directly) to start services [1]. We also shrink the Elasticsearch JVM heap to fit low RAM and optionally add swap to avoid crashes [2] [3].

1. Install Elasticsearch

1. **Add Elastic's APT repo and install:** Import the Elastic GPG key and repository, then install the `elasticsearch` package [4] [5]. For example:

   ```
   curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch \
     | sudo gpg --dearmor -o /usr/share/keyrings/elastic.gpg
   echo "deb [signed-by=/usr/share/keyrings/elastic.gpg] https://
   artifacts.elastic.co/packages/7.x/apt stable main" \
     | sudo tee /etc/apt/sources.list.d/elastic-7.x.list
   sudo apt update
   sudo apt install elasticsearch
   ```

   This adds Elastic's package source and installs Elasticsearch [4] [5].

2. **Configure JVM heap:** By default ES tries to use ~50% of RAM. With only 1 GB available, edit `/etc/elasticsearch/jvm.options` and reduce the heap: e.g. change `-Xms256m` and `-Xmx256m` (or 512m) to fit your RAM. (DigitalOcean notes a **2 GB RAM** minimum for ES [2], so lowering the heap is necessary on a 1 GB system.)

3. **Edit `elasticsearch.yml`:** Open `/etc/elasticsearch/elasticsearch.yml` in an editor. Set the network and discovery for a single-node setup, for example:

   ```
   network.host: localhost
   http.port: 9200
   discovery.type: single-node
   ```

   This binds ES to localhost on port 9200 and avoids clustering checks (single-node mode) [6]. Save the file.

4. **Start Elasticsearch:** Use the service command (WSL lacks systemd) to start ES:

```
sudo service elasticsearch start
```

(Alternatively, run `/usr/share/elasticsearch/bin/elasticsearch -d` to start in the background.) **Do not use** `systemctl` **by default** on WSL [1]. Give ES a few moments to start, then test it:

```
curl http://localhost:9200
```

You should see a JSON response with ES info (e.g. version, cluster name) [7].

5. **Enable swap (optional):** On very low-memory systems, creating swap can prevent OOM crashes. For example, to add a 2 GB swap file:

```
sudo fallocate -l 2G /swapfile
sudo chmod 600 /swapfile
sudo mkswap /swapfile
sudo swapon /swapfile
echo '/swapfile none swap sw 0 0' | sudo tee -a /etc/fstab
```

This follows standard Ubuntu swap setup [3] [8]. Rebooting will then activate the swap file.

2. Install Kibana

1. **Install Kibana:** Using the same Elastic APT repo, install Kibana:

```
sudo apt install kibana
```

2. **Configure** `kibana.yml`**:** Edit `/etc/kibana/kibana.yml` and set:

```
server.host: "0.0.0.0"
elasticsearch.hosts: ["http://localhost:9200"]
```

Setting `server.host: 0.0.0.0` lets you access Kibana from your host machine [9]. The `elasticsearch.hosts` line tells Kibana where to find ES (localhost). Save the file.

3. **Start Kibana:** On WSL, start Kibana with:

```
sudo service kibana start
```

(If your WSL supports `systemd` [e.g. via `/etc/wsl.conf` modifications [10]], you could use `systemctl`, but this is optional.) By default, Kibana logs to `/var/log/kibana`.

4. **Access Kibana:** In a browser on your Windows host, go to `http://localhost:5601`. You should see the Kibana UI. (No firewall changes or public IP needed since it's all local.)

3. Install Filebeat (Log Shipping)

1. **Install Filebeat:** With the Elastic repo still enabled, run:

```
sudo apt install filebeat
```

2. **Configure Filebeat:** Edit `/etc/filebeat/filebeat.yml`. For example, enable a log input and set the Elasticsearch output:

```
filebeat.inputs:
- type: log
  enabled: true
  paths:
    - /home/<youruser>/app.log

output.elasticsearch:
  hosts: ["http://localhost:9200"]
```

(Replace `/home/<youruser>/app.log` with the actual path you want to monitor.) The `output.elasticsearch.hosts` should point to `localhost:9200` [11]. Save changes.

3. **Start Filebeat:** Run:

```
sudo service filebeat start
```

This starts Filebeat in the background. (Again, use `service` instead of `systemctl` on WSL [1].)

4. **Verify ingestion:** If you have a log file (e.g. generated by your `log-generator.sh`), Filebeat will index its entries into Elasticsearch. You can verify by searching ES:

```
curl -X GET "http://localhost:9200/filebeat-*/_search?pretty"
```

You should see results from your logs. Also check `/var/log/filebeat/filebeat` for any startup errors.

4. Notes on WSL and Memory

- **Systemd vs. `service`:** Traditional `systemctl` commands will fail on unmodified WSL (error "not booted with systemd") [1]. Use `sudo service <name> start` or run the program binary directly. (Modern WSL2 can be configured to support systemd via `/etc/wsl.conf` [10], but it's optional.)
- **Bootstrap warnings:** WSL's Linux kernel does not support seccomp filters, so Elasticsearch may warn about "syscall filters" failing [1]. These warnings can be ignored in a non-production (learning) setup.
- **RAM constraints:** Elasticsearch really prefers ≥2 GB RAM [2]. With only 1 GB, you should keep the heap very small (as above) and/or use swap. Expect performance limits; this setup is only for experimentation.

By following these steps (and citing the official docs above), you should have Elasticsearch, Kibana, and Filebeat running on your Ubuntu WSL instance. This lets you experiment with Kibana on `localhost:5601` as intended, without needing a heavy OCI VM.

Sources: Official Elastic install guides and community notes have been used to adapt commands and configurations [4] [5] [9] [11] [2] [3] [1].

---

[1] How do you configure Elasticsearch on Ubuntu Bash for Windows 10? - Elasticsearch - Discuss the Elastic Stack
https://discuss.elastic.co/t/how-do-you-configure-elasticsearch-on-ubuntu-bash-for-windows-10/194888

[2] [4] [5] [6] [7] How To Install and Configure Elasticsearch on Ubuntu 22.04 | DigitalOcean
https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-elasticsearch-on-ubuntu-22-04

[3] [8] How To Add Swap Space on Ubuntu 20.04 | DigitalOcean
https://www.digitalocean.com/community/tutorials/how-to-add-swap-space-on-ubuntu-20-04

[9] Install Kibana with Debian package | Elastic Docs
https://www.elastic.co/docs/deploy-manage/deploy/self-managed/install-kibana-with-debian-package

[10] Advanced settings configuration in WSL | Microsoft Learn
https://learn.microsoft.com/en-us/windows/wsl/wsl-config

[11] Elasticsearch: How to install and set up FileBeat on Ubuntu 20.04. | by Akintola L. F. ADJIBAO | Medium
https://akintola-lonlon.medium.com/elasticsearch-how-to-install-and-set-up-filebeat-on-ubuntu-20-04-66375c967798