Elasticsearch 7 Installation & Configuration (Ubuntu VM)

System Requirements

- **OS**: Ubuntu 20.04 or 22.04
- **Private IP**: `172.19.240.13`
- **Java**: OpenJDK 11
- **Public IP**: Not used (system is private)

Step 1: System Preparation

Update system:

```
sudo apt update && sudo apt upgrade -y
```

Install Java:

```
sudo apt install openjdk-11-jdk -y
java -version
```

Step 2: Install Elasticsearch 7.17.x

Add Elastic GPG key and repository:

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/elastic-7.x.list'

sudo apt update
```

Install Elasticsearch:

```
sudo apt install elasticsearch -y
```

Step 3: Configure Elasticsearch

Edit config:

```
sudo nano /etc/elasticsearch/elasticsearch.yml
```

Add the following:

```
network.host: 172.19.240.13
http.port: 9200
discovery.type: single-node

xpack.security.enabled: true
xpack.security.authc.api_key.enabled: true
```

Note: Replace `172.19.240.13` with your actual private IP if different.

Step 4: Start & Enable Elasticsearch

```
sudo systemctl enable elasticsearch
sudo systemctl start elasticsearch
sudo systemctl status elasticsearch
```

Step 5: Set Passwords for Built-in Users

Run the interactive password setup:

```
sudo /usr/share/elasticsearch/bin/elasticsearch-setup-passwords interactive
```

You will be prompted to set passwords for:

- `elastic`
- `kibana_system`
- `logstash_system`
- `beats_system`
- `apm_system`

Save the password for `elastic` — it is the admin user.

Step 6: Test Access

```
curl -u elastic http://172.19.240.13:9200
```

You should be prompted for a password and then see Elasticsearch cluster information.

Step 7: Verify Logs

View real-time logs:

```
sudo tail -f /var/log/elasticsearch/elasticsearch.log
```

View journal logs:

```
sudo journalctl -u elasticsearch
```

Optional: Secure Access (Firewall/Nginx/SSL)

If you need to expose it safely (e.g., within a VPN), consider:

- Allow only trusted IPs via firewall rules
- Use Nginx as a reverse proxy with HTTPS and basic auth
- Never bind `network.host` to `0.0.0.0` or public IP

Notes

- Elasticsearch runs on port **9200**
- Admin user is `elastic`
- Data folder: `/var/lib/elasticsearch/`
- Config folder: `/etc/elasticsearch/`
- Logs folder: `/var/log/elasticsearch/`