ELK Stack SIEM on Ubuntu 24.04.3 LTS with a Windows 11 Agent

Below is a Detailed, Tested, end-to-end installation and configuration guide.

---

1. VMware Networking & VM Sizing

- Set the Ubuntu VM's network adapter to **Bridged** mode so your Windows 11 host and Ubuntu VM share the same LAN subnet.
- If you must use NAT, configure port-forward rules for ports 5601, 9200, and 5044 in your VMware NAT settings.
- Allocate at least 4 GB RAM and 2 vCPUs to the Ubuntu VM.
- **I Recommend applying static IP before beginning.** I added it to the end in ✅ Option 1 Assign a Static IP to Your VM

---

2. Initial OS Update & Prerequisites

```
sudo apt update && sudo apt upgrade -y
sudo apt install -y apt-transport-https ca-certificates curl gnupg ufw
```

- **ufw** is installed now to simplify firewall rules later.
- No need to install Java separately: Elasticsearch 9.x bundles OpenJDK.

---

3. Kernel Tunables for Elasticsearch

Elasticsearch requires `vm.max_map_count >= 262144`. Set it:

```
# temporary (current session)
sudo sysctl -w vm.max_map_count=262144

# persist across reboots
echo "vm.max_map_count=262144" | sudo tee -a /etc/sysctl.conf
sudo sysctl -p
```

Verify:

```
sysctl vm.max_map_count    # should output 262144
```

---

4. Add Elastic's APT Repository & GPG Key

```
# Download and dearmor GPG key
curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch \
  | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg

# Add the 9.x apt source
echo \
"deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] \
https://artifacts.elastic.co/packages/9.x/apt stable main" \
| sudo tee /etc/apt/sources.list.d/elastic-9.x.list

# Refresh package lists
sudo apt update
```

---

5. Install Elasticsearch, Kibana, (Optional: Logstash)

```
sudo apt install -y elasticsearch kibana
# Optional, only if you plan to use Logstash (I downloded it)
sudo apt install -y logstash
```

---

6. Configure Elasticsearch (Single-Node Lab)

Edit `/etc/elasticsearch/elasticsearch.yml` and ensure the following lines (uncomment or add them):

```
cluster.name: my-elk-cluster
network.host: 0.0.0.0
http.port: 9200
discovery.type: single-node
```

also Comment out **cluster.initial_master_nodes:**

Tune the JVM heap to half of VM RAM by editing
For example if you use 2gb ram for ubuntu use 1gb for elk which is what i did.
`/etc/elasticsearch/jvm.options.d/heap.options` :

```
-Xms1g   # Initial memory size
-Xmx1g   # Max memory size
```

Reload, enable, and start:

```
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch
sudo systemctl start elasticsearch
sudo systemctl status elasticsearch
```

> On first startup Elasticsearch will print or log the **bootstrap password** for the `elastic` user and generate an **enrollment token**.
> To retrieve it later:
>
> ```
> sudo journalctl -u elasticsearch -b --no-pager \
>   | grep -Ei "Password for the elastic user" -A3
> ```

---

7. Configure & Start Kibana

Edit `/etc/kibana/kibana.yml` :

```
server.host: "0.0.0.0"
server.port: 5601
elasticsearch.hosts: ["https://localhost:9200"]
xpack.encryptedSavedObjects.encryptionKey: "your-32-character-key-here"
```

to generate encryption key use:

```
openssl rand -hex 16
```

Then:

```
sudo systemctl enable kibana
sudo systemctl start kibana
```

```
sudo systemctl status kibana
```

In your browser visit `http://<ubuntu_vm_ip>:5601`.

- Paste the **enrollment token** when prompted.
- verification code

```
sudo /usr/share/kibana/bin/kibana-verification-code
```

- Log in as `elastic` with the **bootstrap password** or set a new password.

If you need a new **enrollment token**:

```
sudo /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s
kibana
```

---

8. Ubuntu Firewall Configuration (Optional for Security)

```
sudo ufw allow 22/tcp       # (optional) SSH
sudo ufw allow 5601/tcp     # Kibana UI
sudo ufw allow 9200/tcp     # Elasticsearch HTTP
sudo ufw allow 9300/tcp     # (optional) Elasticsearch transport (if you use
mutli-node)
sudo ufw allow 5044/tcp     # Beats input (Logstash)
sudo ufw enable
sudo ufw status             # To see allow list
```

---

9. Service Validation on Ubuntu

```
# Elasticsearch info (self-signed cert, lab only)
# curl -k https://localhost:9200/

# If security is enabled, you'll need to use:
curl -u elastic -k https://localhost:9200/


# Secured cluster
#curl --cacert /etc/elasticsearch/certs/http_ca.crt \
```

```
    # -u elastic "https://localhost:9200/"

Kibana: visit http://<ubuntu_vm_ip>:5601 and log in.
```

---

10. Install Winlogbeat on Windows 11

1. Download the Winlogbeat ZIP for version **9.x** from https://www.elastic.co/downloads/beats/winlogbeat
2. Extract to `C:\Program Files\Winlogbeat`.
3. Open PowerShell **as Administrator** and navigate there.

---

11. Configure Winlogbeat

Edit `winlogbeat.yml`:

```yaml
winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h

  - name: System
    ignore_older: 72h

  - name: Security
    ignore_older: 72h

  - name: Microsoft-Windows-PowerShell/Operational
    event_id: 4103, 4104, 4105, 4106

# output.elasticsearch: (if you want to send logs to elasticsearch instead of
logstash)
 # hosts: ["https://<UBUNTU_VM_IP>:9200"]
  # username: "elastic"
  # password: "<ELASTIC_PASSWORD>"
  # For self-signed CA (lab only):
  #ssl.verification_mode: "none"

 output.logstash:
  hosts: ["<UBUNTU_VM_IP>:5044"]
```

```
setup.kibana:
  host: "http://<UBUNTU_VM_IP>:5601"
```

Test config and connectivity:

```
.\winlogbeat.exe test config -c .\winlogbeat.yml
.\winlogbeat.exe test output -c .\winlogbeat.yml
```

---

12. Install & Start Winlogbeat Service

```
.\install-service-winlogbeat.ps1
Start-Service winlogbeat
Get-Service winlogbeat
```

(Optional) Load index templates and dashboards:

```
.\winlogbeat.exe setup -e -c .\winlogbeat.yml
```

Within a minute, check Kibana's **Discover** or **Dashboards** → **Winlogbeat** for incoming events.

---

13. Verify in Kibana

1. In Kibana go to **Discover** → **Create index pattern** → `winlogbeat-*`.
2. Search for recent events, e.g. `winlog.event_id:4625`.
3. Explore prebuilt dashboards under **Dashboard** → **Winlogbeat**.

---

14. Logstash Pipeline

If you'd rather route Beats through Logstash for parsing/enrichment, create `/etc/logstash/conf.d/10-beats.conf`:

```
input {
  beats {
    port => 5044
  }
```

```
}

filter {
  # grok, date, geoip, etc.
}

output {
  elasticsearch {
    hosts => ["https://localhost:9200"]
    user => "elastic"
    password => "<ELASTIC_PASSWORD>"
    ssl_enabled => true
    ssl_certificate_authorities => ["/etc/logstash/certs/http_ca.crt"]
    index => "winlogbeat-%{+YYYY.MM.dd}"
  }
}
```

Enable and start:

```
sudo systemctl enable logstash
sudo systemctl start logstash
sudo journalctl -u logstash -f
```

---

15. Ports Summary

Service	Port	Protocol	Direction
Elasticsearch HTTP	9200	TCP (HTTPS)	client queries
Elasticsearch transport	9300	TCP	node-to-node
Kibana (UI/API)	5601	TCP (HTTP)	browser/API
Beats Input (Logstash)	5044	TCP	Beats → LS

Everything you listed is fundamentally correct. The above guide fills in key details on certificates, security enrollment, firewall, service management, and testing. Once you complete these steps, you'll have a secured, single-node ELK SIEM lab and a Winlogbeat-powered Windows 11 agent feeding logs into Kibana.

Happy logging!

16) To close and open the server:

Close the server:

```
sudo systemctl stop logstash
sudo systemctl stop elasticsearch
sudo systemctl stop kibana
```

Open the server:

```
sudo systemctl stop logstash
sudo systemctl stop elasticsearch
sudo systemctl stop kibana
```

17) Troubleshooting quick checklist

- `sudo systemctl status elasticsearch` and `sudo journalctl -u elasticsearch -f` — check Elasticsearch logs for bootstrap check errors.
- `curl -k https://<vm-ip>:9200/` — quick API check (use `--cacert` and `-u` when secured).
- For Winlogbeat: `.\\winlogbeat.exe test output` and check Windows Event Viewer + Winlogbeat logs in `C:\Program Files\Winlogbeat\logs`.
- If Kibana shows “enrollment token” page, generate a token on the Elasticsearch node: `/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana`. ([Elastic][6])

to test Logstash pipeline:

- sudo -u logstash /usr/share/logstash/bin/logstash --path.settings /etc/logstash --config.test_and_exit -f /etc/logstash/conf.d/

When you rebooted your Ubuntu Server, its IP address changed (likely because it's using **DHCP**), and now the **new IP doesn't match the SSL certificate's Subject Alternative Names (SANs)**. That’s why Elasticsearch is throwing a trust error — it’s trying to validate a certificate for an IP it wasn’t issued for.

🔧 How to Fix It

You’ve got two solid paths forward:

✅ Option 1: Assign a Static IP to Your VM

This prevents the IP from changing on reboot.

1. Edit your Netplan config:

```
sudo nano /etc/netplan/01-netcfg.yaml
```

2. Set a static IP like:

```
network:
version: 2
renderer: networkd
ethernets:
ens33:  # Replace with your actual interface name
  addresses:
    - 192.168.1.210/24
  routes:
    - to: default
      via: 192.168.1.1
  nameservers:
    addresses:
      - 8.8.8.8
      - 1.1.1.1
```

3. Apply changes:

```
sudo netplan apply
```

Now your VM will always boot with the same IP — and your certificate will stay valid.

✅ Option 2: Regenerate the Certificate with the New IP

If you want to keep using DHCP but still avoid trust errors:

1. Run:

```
sudo /usr/share/elasticsearch/bin/elasticsearch-certutil http
```

2. Add the new IP (`<your choosen static IP and 127.0.0.1>`) to the SAN list
3. Replace the old cert in `/etc/elasticsearch/certs/http.p12`
4. Restart Elasticsearch:

```
sudo systemctl restart elasticsearch
```

Sources / further reading (key official docs)

- Install Elasticsearch (Debian/Ubuntu) — Elastic docs. ([Elastic][1])
- Install Logstash — Elastic docs. ([Elastic][9])
- Install Kibana via Debian package + enrollment flow — Elastic docs. ([Elastic][3])
- Required Linux setting `vm.max_map_count` for Elasticsearch. ([Elastic][2])
- Winlogbeat quick start & Windows install instructions (agent). ([Elastic][4])

[1]: "Install Elasticsearch with a Debian package"
[2]: "Increase virtual memory | Elastic Docs"
[3]: "Install Kibana with Debian package"
[4]: "Winlogbeat quick start: installation and configuration | Beats"
[5]: "What is the difference between NAT / Bridged / Host-Only ..."
[6]: "elasticsearch-create-enrollment-token | Reference"
[7]: "Minimal security setup | Elastic Docs"
[8]: "Networking settings | Reference"
[9]: "Installing Logstash"
[10]: "General settings in Kibana"
[11]: "Configure the Logstash output | Beats - Elastic"

Made by Omar Mohamed