

Installing the ELK Stack, Setting Up Fleet Server, and Deploying the Elastic Agent on Windows

Overview:

In this project, I set up a complete **ELK Stack** (Elasticsearch, Logstash, Kibana) to collect, store, and visualize logs.

I configured **Fleet Server** to centrally manage Elastic Agents and their integrations.

Finally, I installed and connected an **Elastic Agent** on a Windows machine so it can send system logs and metrics to the ELK environment.

The setup involved:

1. Installing and configuring the ELK Stack on a Ubuntu machine.
2. Setting up **Fleet Server** inside the ELK environment to manage agents.
3. Installing the **Elastic Agent** on Windows and enrolling it into the Fleet Server.
4. Verifying that the data from the Windows agent appears in Kibana dashboards.

Installing the ELK Stack (Elasticsearch, Kibana)

1. **Update and install dependencies on the Ubuntu machine.**

```
sudo apt update && sudo apt upgrade -y  
sudo apt install apt-transport-https openjdk-17-jdk -y  
curl -fsSL https://artifacts.elastic.co/GPG-KEY-
```

2-Add Elastic repository and GPG key.

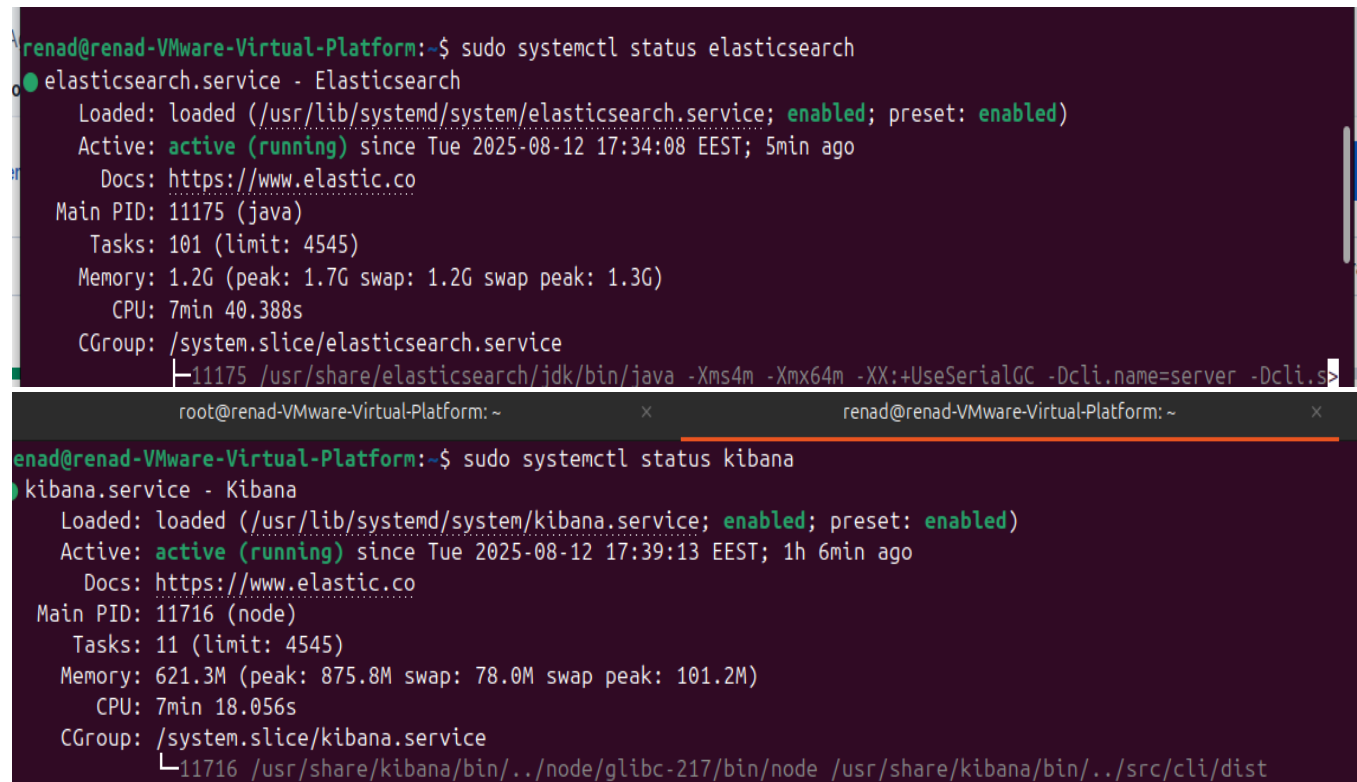
```
elasticsearch | sudo gpg --dearmor -o  
/usr/share/keyrings/elasticsearch-keyring.gpg  
  
echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg]  
https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee  
/etc/apt/sources.list.d/elastic-8.x.list
```

3- Install Elasticsearch, Kibana, .

```
sudo apt update  
sudo apt install elasticsearch kibana -y
```

4- Enable and start services.

```
sudo systemctl enable elasticsearch --now  
sudo systemctl enable kibana --now
```



The image shows a terminal window with two tabs. The top tab is titled 'renad@renad-VMware-Virtual-Platform: ~' and shows the command 'sudo systemctl status elasticsearch'. The output indicates that the 'elasticsearch.service' is loaded, enabled, and active (running) since Tue 2025-08-12 17:34:08 EEST. The bottom tab is titled 'renad@renad-VMware-Virtual-Platform: ~' and shows the command 'sudo systemctl status kibana'. The output indicates that the 'kibana.service' is loaded, enabled, and active (running) since Tue 2025-08-12 17:39:13 EEST.

```
renad@renad-VMware-Virtual-Platform:~$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: enabled)
   Active: active (running) since Tue 2025-08-12 17:34:08 EEST; 5min ago
     Docs: https://www.elastic.co
   Main PID: 11175 (java)
    Tasks: 101 (limit: 4545)
   Memory: 1.2G (peak: 1.7G swap: 1.2G swap peak: 1.3G)
      CPU: 7min 40.388s
   CGroup: /system.slice/elasticsearch.service
           └─11175 /usr/share/elasticsearch/idk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.s>

root@renad-VMware-Virtual-Platform: ~
renad@renad-VMware-Virtual-Platform: ~$ sudo systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; preset: enabled)
   Active: active (running) since Tue 2025-08-12 17:39:13 EEST; 1h 6min ago
     Docs: https://www.elastic.co
   Main PID: 11716 (node)
    Tasks: 11 (limit: 4545)
   Memory: 621.3M (peak: 875.8M swap: 78.0M swap peak: 101.2M)
      CPU: 7min 18.056s
   CGroup: /system.slice/kibana.service
           └─11716 /usr/share/kibana/bin/./node/glibc-217/bin/node /usr/share/kibana/bin/./src/cli/dist
```

Setting Up Fleet Server

1. **Generate an enrollment token** from Kibana → **Management** → **Fleet** → **Fleet Servers**.
2. **Run the Elastic Agent** in Fleet mode on the server.

```
sudo ./elastic-agent install --url=https://<Fleet_Server_IP>:8220  
--enrollment-token=<TOKEN>
```

✓

Get started with Fleet Server

✓ Fleet Server policy created.

Fleet server policy and service token have been generated. Host configured at <https://localhost:9200>. You can edit your Fleet Server hosts in [Fleet Settings](#).

✓

Install Fleet Server to a centralized host

Install Fleet Server agent on a centralized host so that other hosts can connect to it. In production, we recommend using one or more hosts. For additional guidance, see our [installation docs](#).

Windows x86_64

Windows MSI

✓ [Linux x86_64](#)

MacOS x86_64

DEB x86_64

RPM x86_64

Linux aarch64

MacOS aarch64

DEB aarch64

RPM aarch64

... 1

elastic

Find apps, content, and more.

🔔 🛠️ 👤

🔑

Fleet Agents

📄 Send feedback

🔔

We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. [Learn more.](#)

✕

Fleet

Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Uninstall tokens](#) [Data streams](#) [Settings](#)

📊 Ingest Overview Metrics

📊 Agent Info Metrics

🕒 Agent activity

Add Fleet Server

Add agent

🔍 Filter your data using KQL syntax

Status 5

Tags 1

Agent policy 2

Upgrade available

Showing 2 agents

Clear filters

● Healthy 1 ● Unhealthy 0 ● Orphaned 0 ● Updating 0 ● Offline 1 ● Inactive 0 ● Unenrolled 0 ● Uninstalled 0

<input type="checkbox"/>	Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
<input type="checkbox"/>	Offline	DESKTOP-EU55AL7	Agent policy 1	N/A	N/A	16 hours ago	9.1.1	⋮
<input type="checkbox"/>	Healthy	tenad-VMware-Virtual-Platform	Fleet Server Policy rev. 1	5.92 %	756 MB	38 seconds ago	9.1.1	⋮

Rows per page: 20

< 1 >

Installing Elastic Agent on Windows

1. **Download Elastic Agent** for Windows from [Elastic Downloads](#).
2. **Open PowerShell as Administrator.**
3. Run the installation command:

```
.\elastic-agent.exe install --url=https://<Fleet_Server_IP>:8220 --enrollment-token=<TOKEN>
```

Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

⚠ Root privileges required

This agent policy contains the following integrations that require root privileges. To ensure that all data required by the integrations can be collected, you must use an account with root privileges. For more information, see [Agent Guide](#).

- System

To install Elastic Agent without root privileges, add the `--no-root` flag to the `elastic-agent install` command below. For more information, see [Agent Guide](#).

Linux aarch64 MacOS aarch64 DEB aarch64 RPM aarch64 ... 1 ▾

```
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent-9.1.1-windows-x86_64.zip -DestinationPath .
cd elastic-agent-9.1.1-windows-x86_64
.\elastic-agent.exe install --url=https://localhost:9200 --enrollment-token=
```

🔒 We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. [Learn more.](#)

Fleet

Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Uninstall tokens](#) [Data streams](#) [Settings](#)

[Ingest Overview Metrics](#) [Agent Info Metrics](#)

[Agent activity](#) [Add Fleet Server](#) [Add agent](#)

🔍 Filter your data using KQL syntax

Status 5 ▾ Tags 1 ▾ Agent policy 2 ▾ Upgrade available

Showing 2 agents [Clear filters](#) ● Healthy 1 ● Unhealthy 0 ● Orphaned 0 ● Updating 1 ● Offline 0 ● Inactive 0 ● Unenrolled 0 ● Uninstalled 0

<input type="checkbox"/>	Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
<input type="checkbox"/>	Updating	DESKTOP-EUJ5A...	Agent policy	N/A	N/A	10 seconds ago	9.1.1	...
<input type="checkbox"/>	Healthy	renad-VMware-Virtual-Platform	Fleet Server Policy rev. 1	8.93 %	756 MB	30 seconds ago	9.1.1	...

