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.

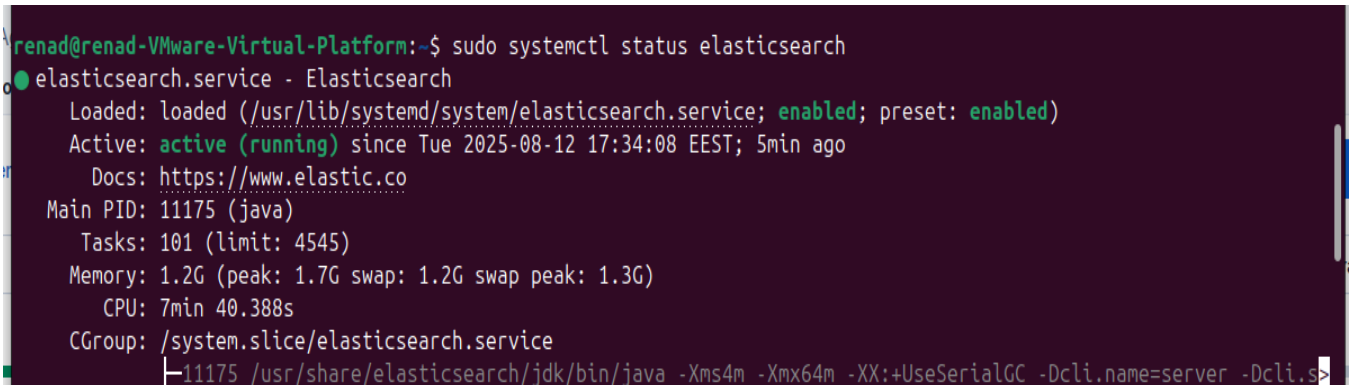
```
elasticsearch | sudo gpg --dearmor -o
/usr/share/keyrings/elasticsearch-keyring.gpg

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
```

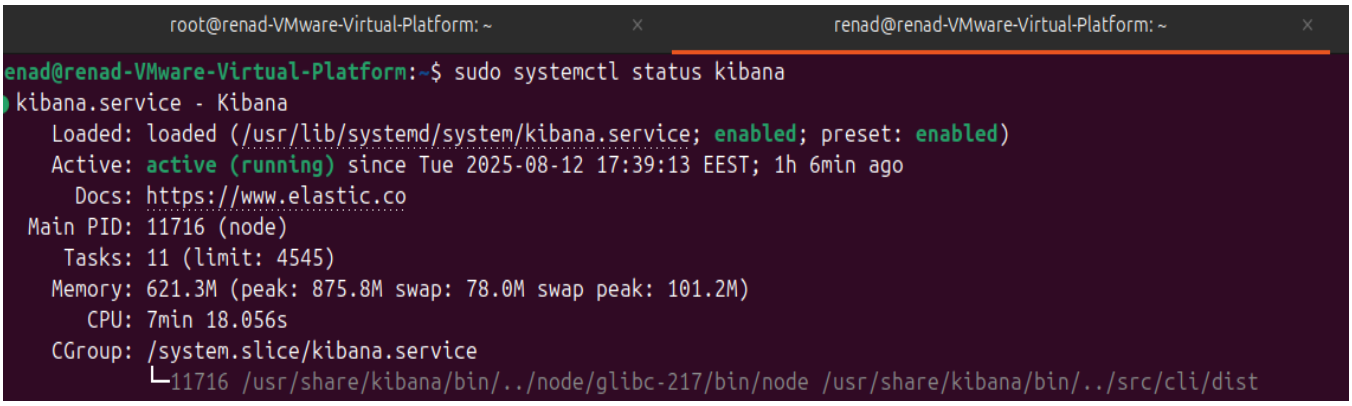
3- Install Elasticsearch, Kibana, .

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

4- Enable and start services.

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

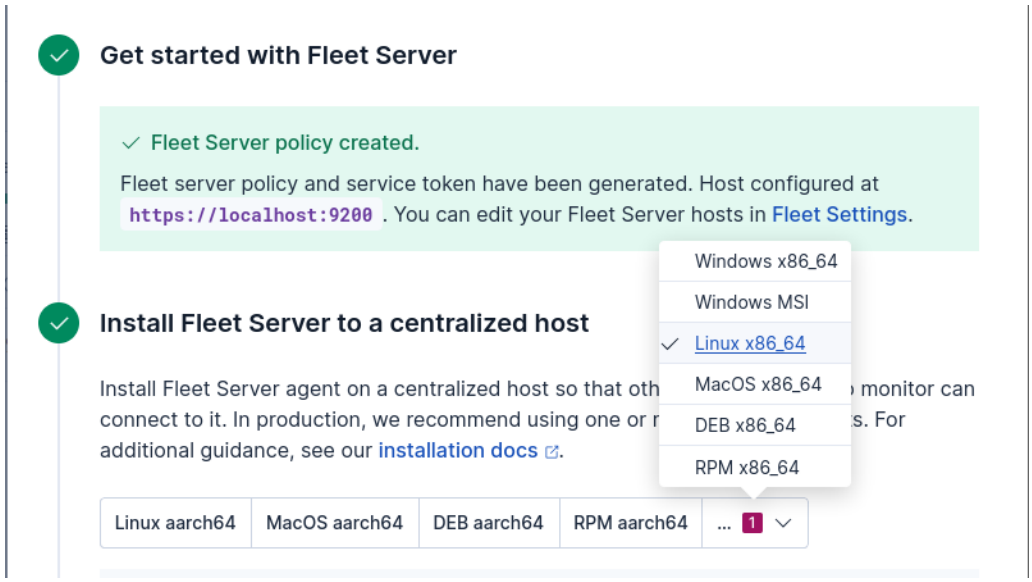


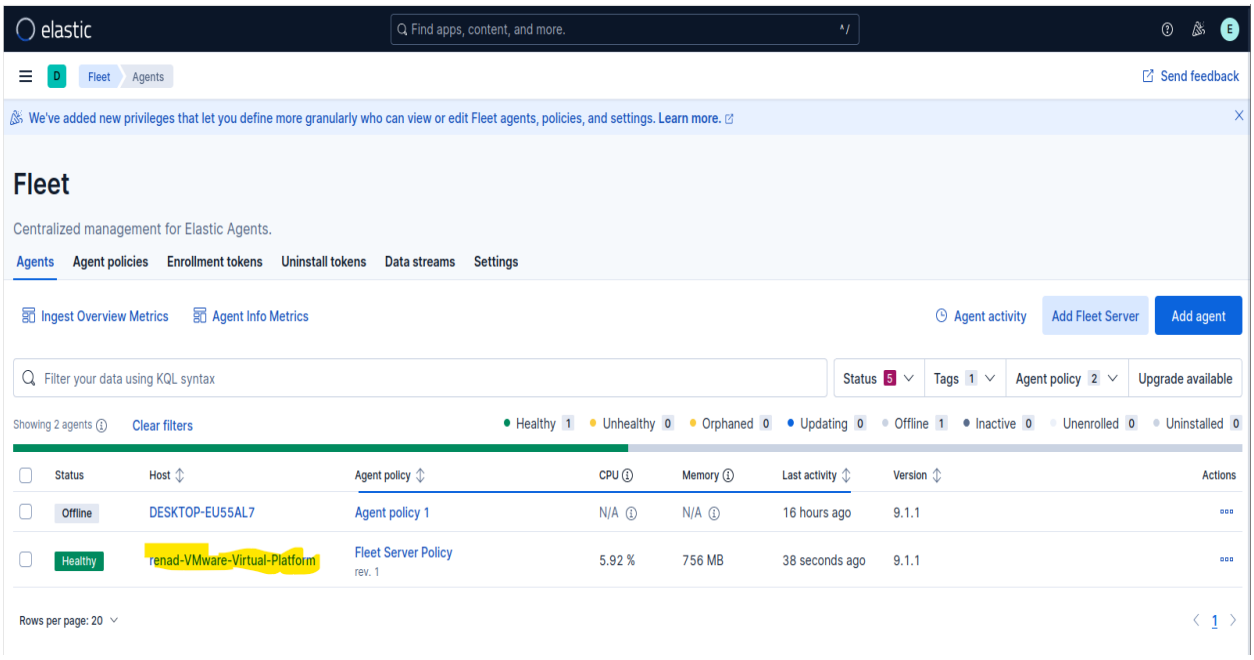


Setting Up Fleet Server

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>
```





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>
```