# Installation suite Elastic

# Part. 1

sudo apt install curl

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 -a /etc/apt/sources.list.d/elastic-7.x.list

sudo apt update

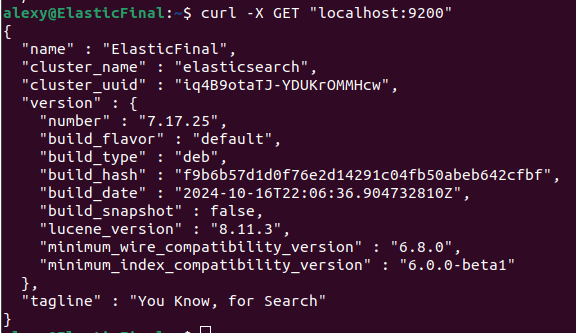
sudo apt install elasticsearch

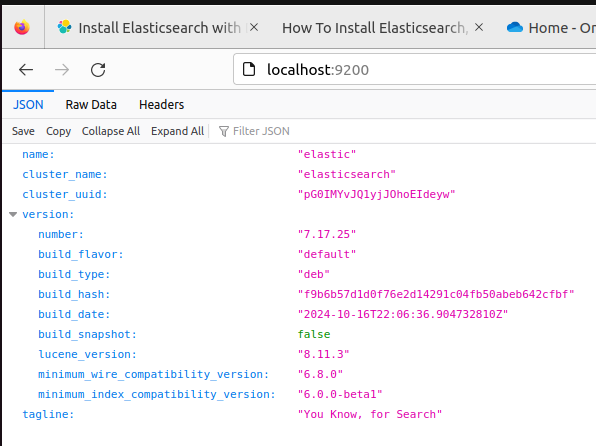
sudo nano /etc/elasticsearch/elasticsearch.yml

network.host: localhost

sudo systemctl start elasticsearch

sudo systemctl enable elasticsearch



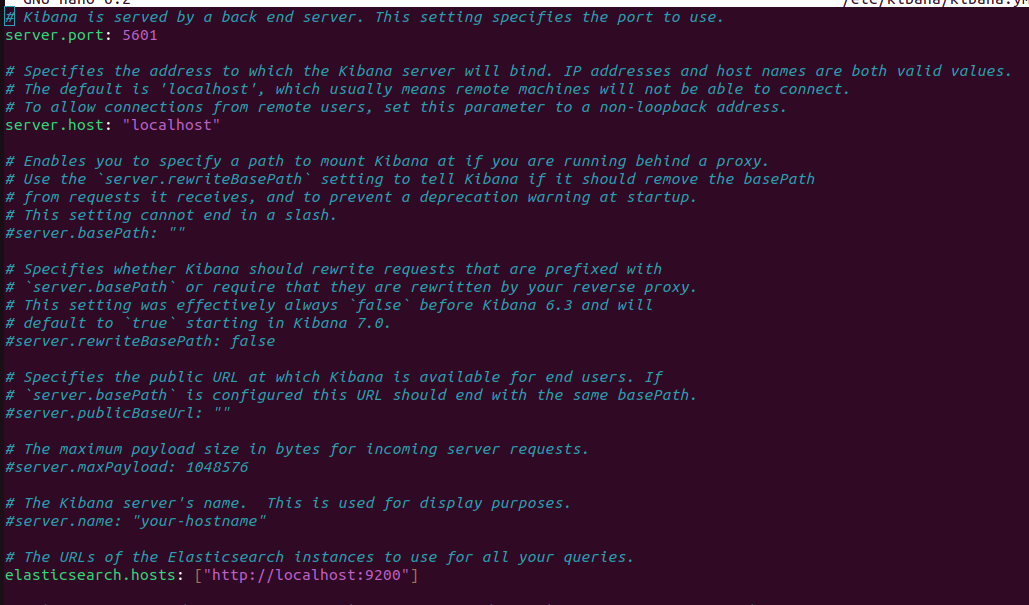


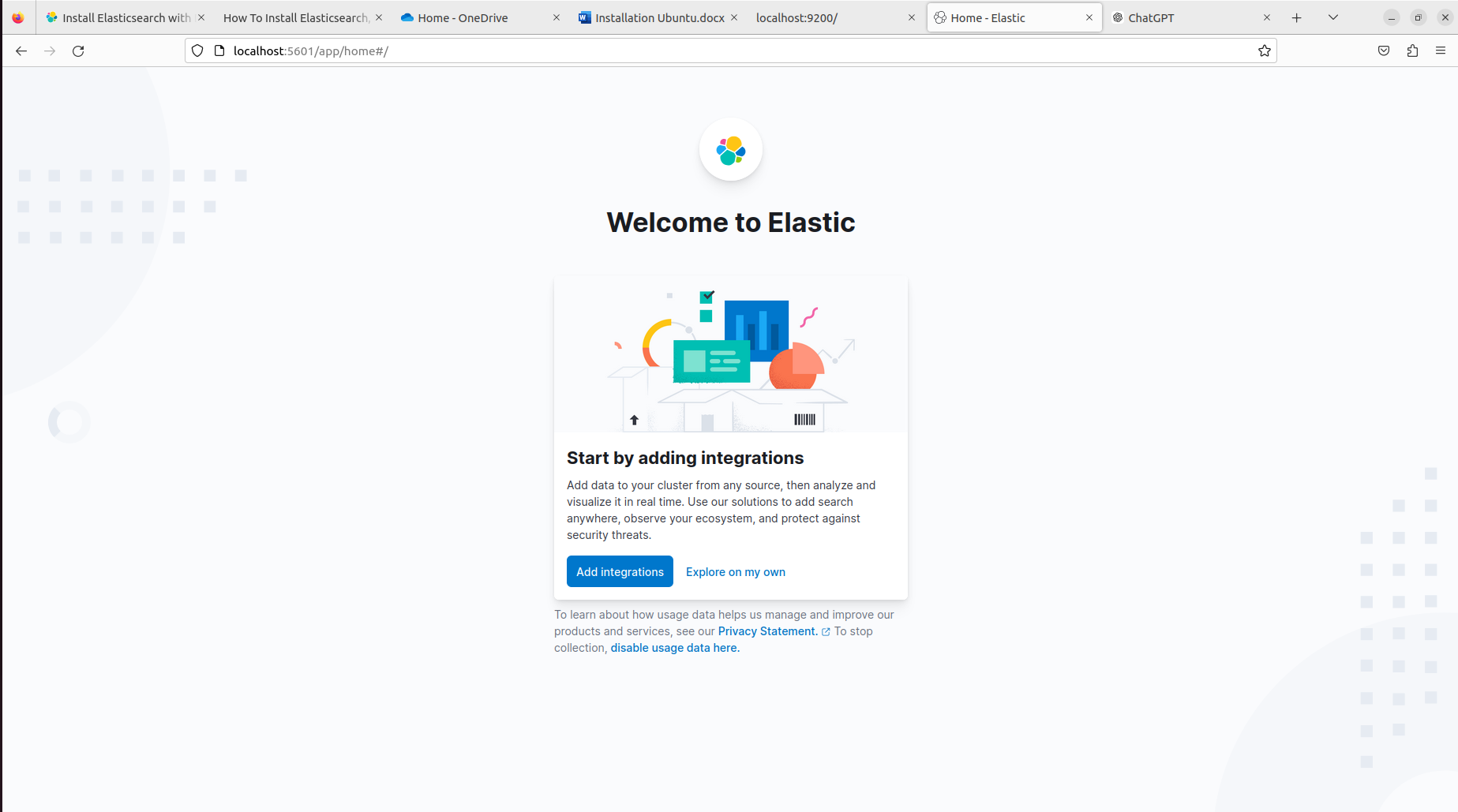
sudo apt install kibana

sudo systemctl start kibana

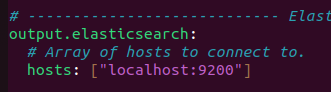
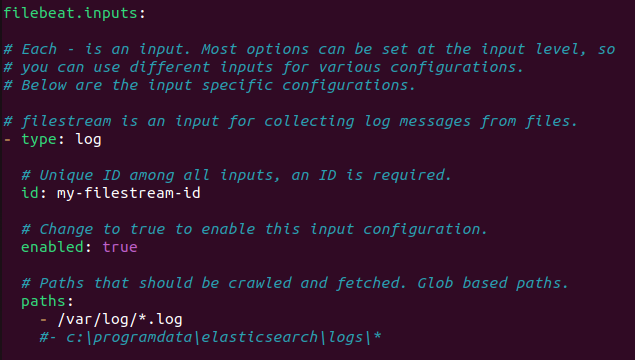
sudo systemctl enable kibana

sudo nano /etc/kibana/kibana.yml

sudo systemctl restart kibana

sudo apt install filebeat

sudo nano /etc/filebeat/filebeat.yml

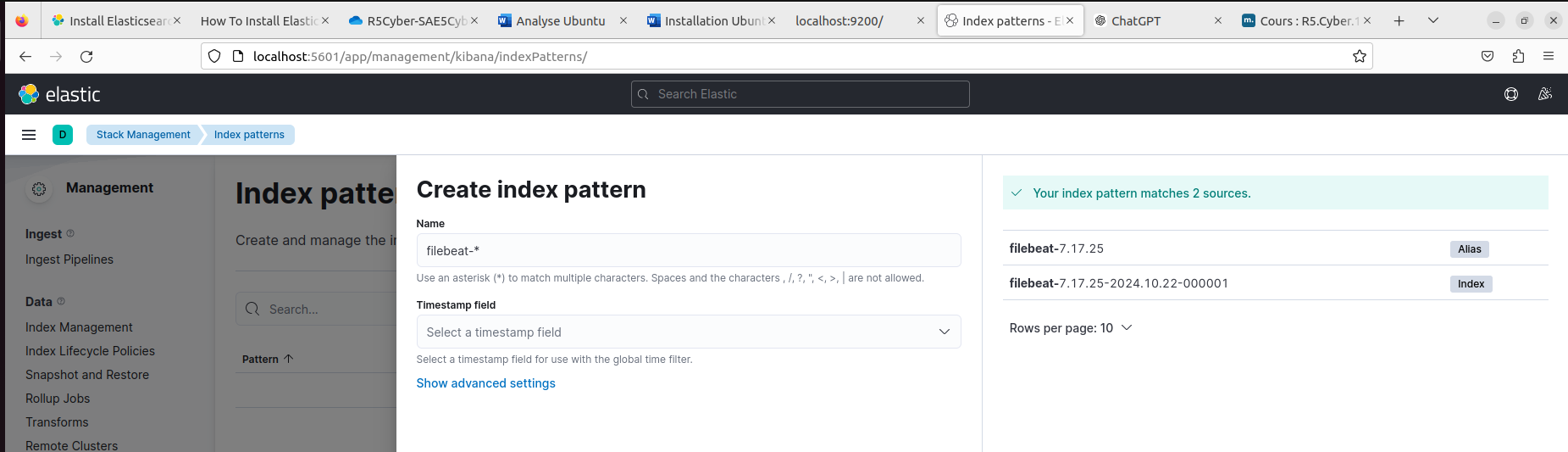


sudo filebeat modules enable system

sudo systemctl start filebeat

sudo systemctl enable filebeat

Dans kibana > dashboard > create index pattern :



Sudo filebeat setup –-pipelines –-modules system

filebeat setup -dashboard

1. Dans dashboard, sélectionner le template : [Filebeat System] Syslog dashboard ECS

