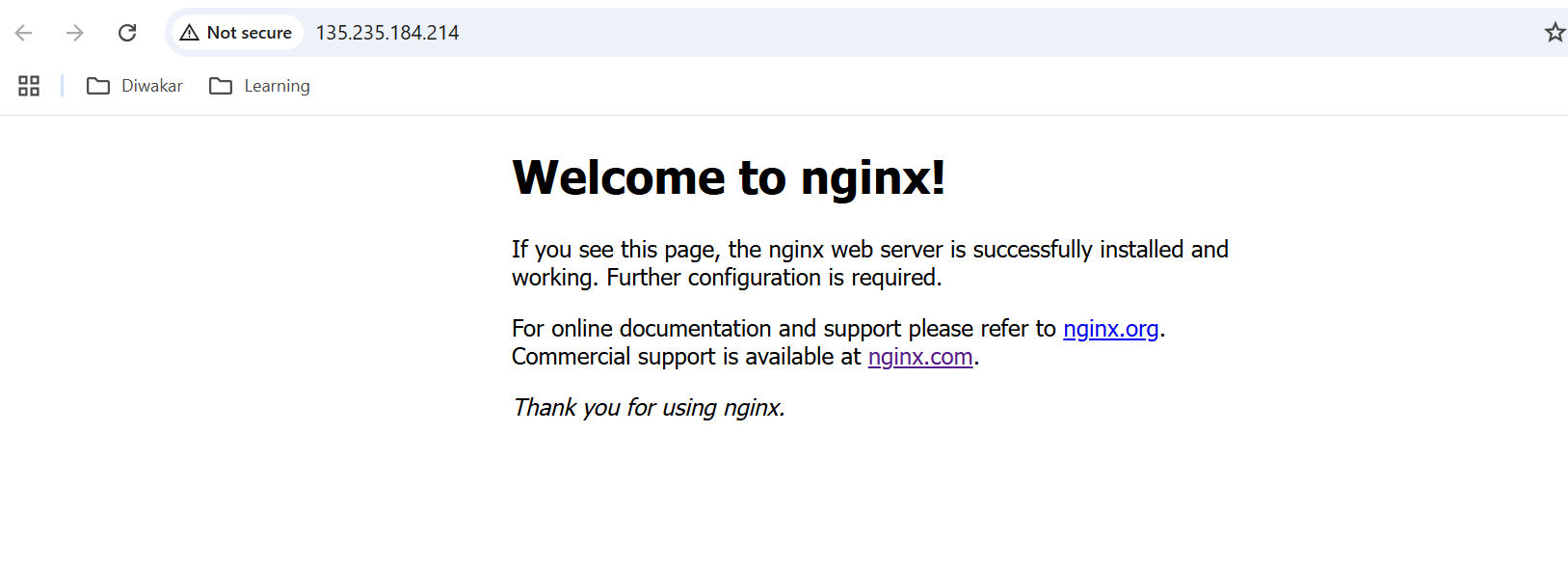
**ELK stack with AKS**

1. Here we will be using FEK stack not elk. (Filebeat 🡪 Elasticsearch 🡪 Kibana). We are skipping Logstash, as it is just another intermediatory.
2. Create AKS from azure portal (initially you would need to ask for increase\_quota, as Azure has introduced this new system before allocation VCpus. It gets approved in 15 mins)
3. Once AKS is created, we shall deploy a simple nginx deployment and its service. [All Yaml files are embedded at the EOF]
4. Once Nginx created check the services tab and see if its working, 
5. Now we run below helm command to add elastic stack repo in our cluster
   1. helm repo add elastic https://helm.elastic.co
   2. helm repo update
   3. helm search repo (to confirm whether repo is added or not)
6. Now install, elasticsearch:
   1. helm install elasticsearch elastic/elasticsearch \

--set replicas=1 \

--set minimumMasterNodes=1

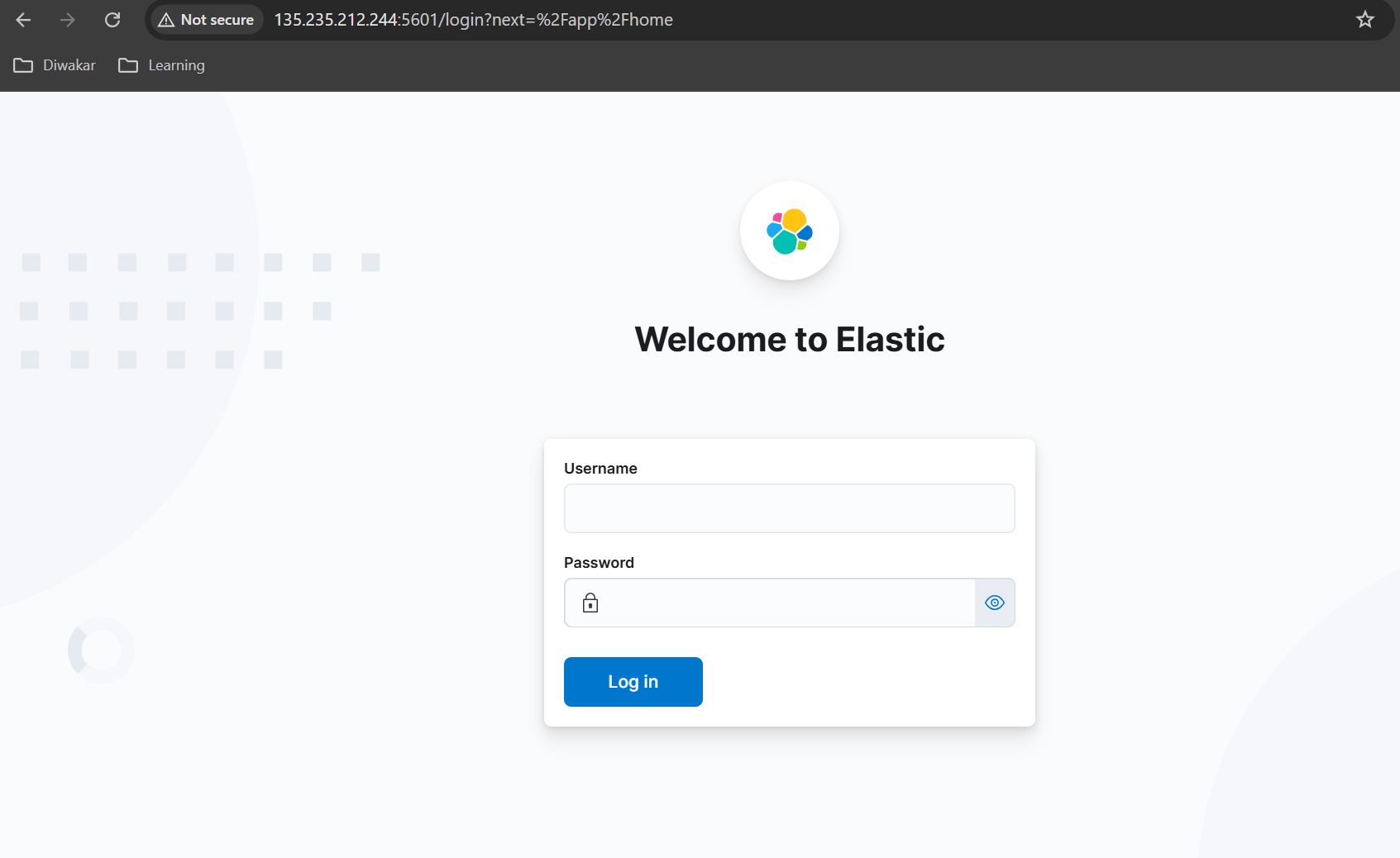
7. Now install Kibana

a. helm install kibana elastic/kibana \

--set service.type=LoadBalancer

8. Now create the config file for Filebeat (Filebeat-values.yaml) [The file is given at EOF] after saving that file, run below command:

a. helm install filebeat elastic/filebeat -f filebeat-values.yaml

9. Now when you will click on the loadbalancer ip of the Kibana service, you will now see a login page. 

10. For to get the credentials you can check either the filebeat-values.yaml file where we explicitly mentioned the credentials or else use below commands:

a. kubectl get secrets | grep elastic

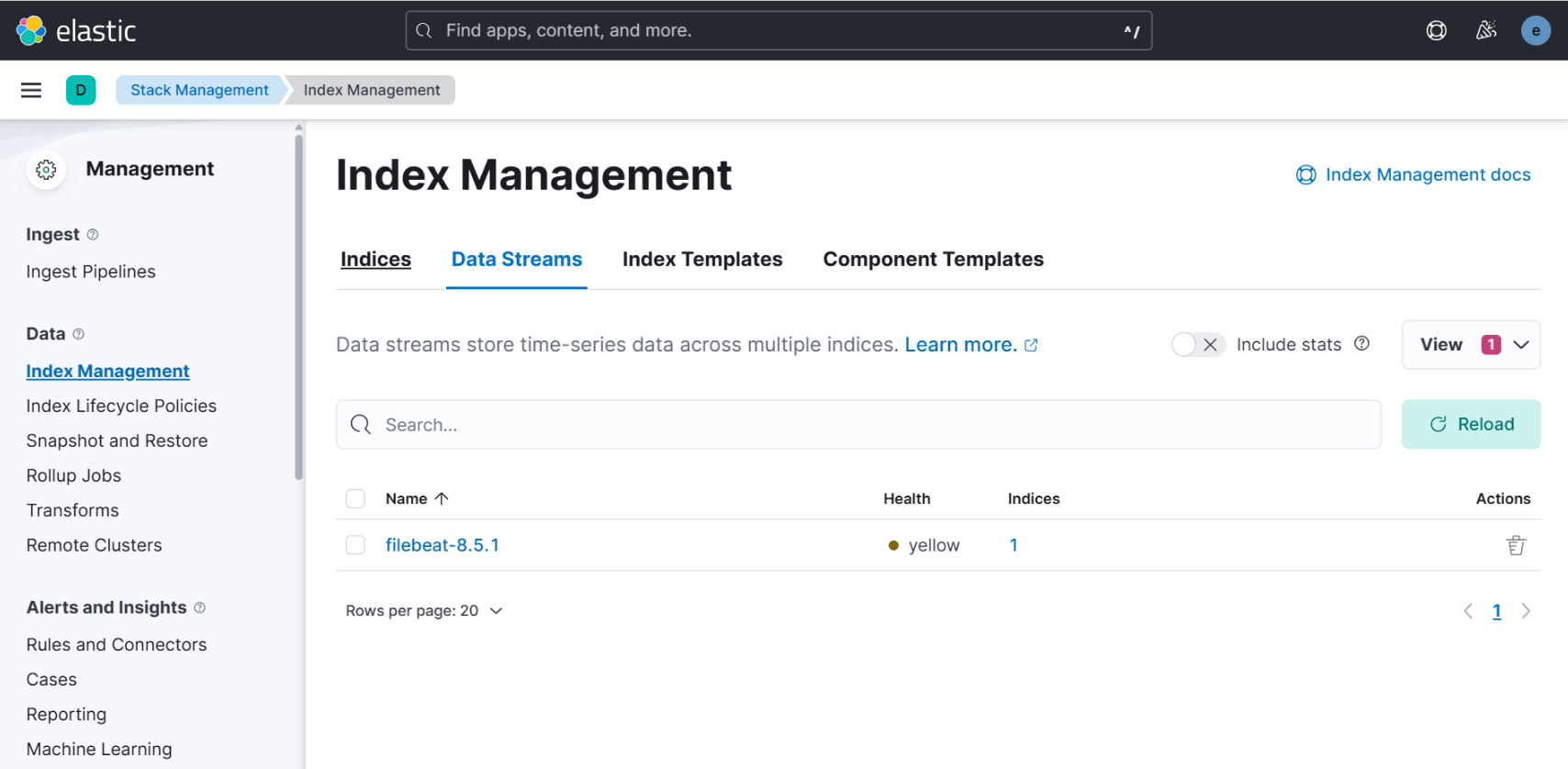
b. kubectl get secret <secret-name> -o=jsonpath='{.data.username}' | base64 –decode

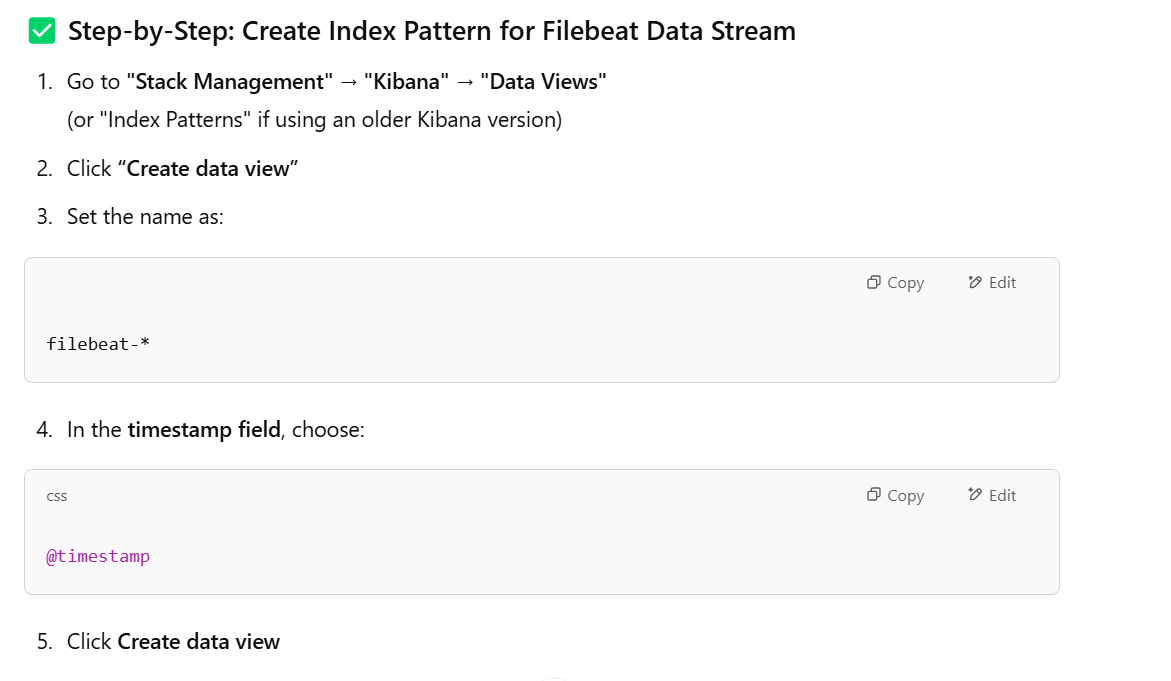
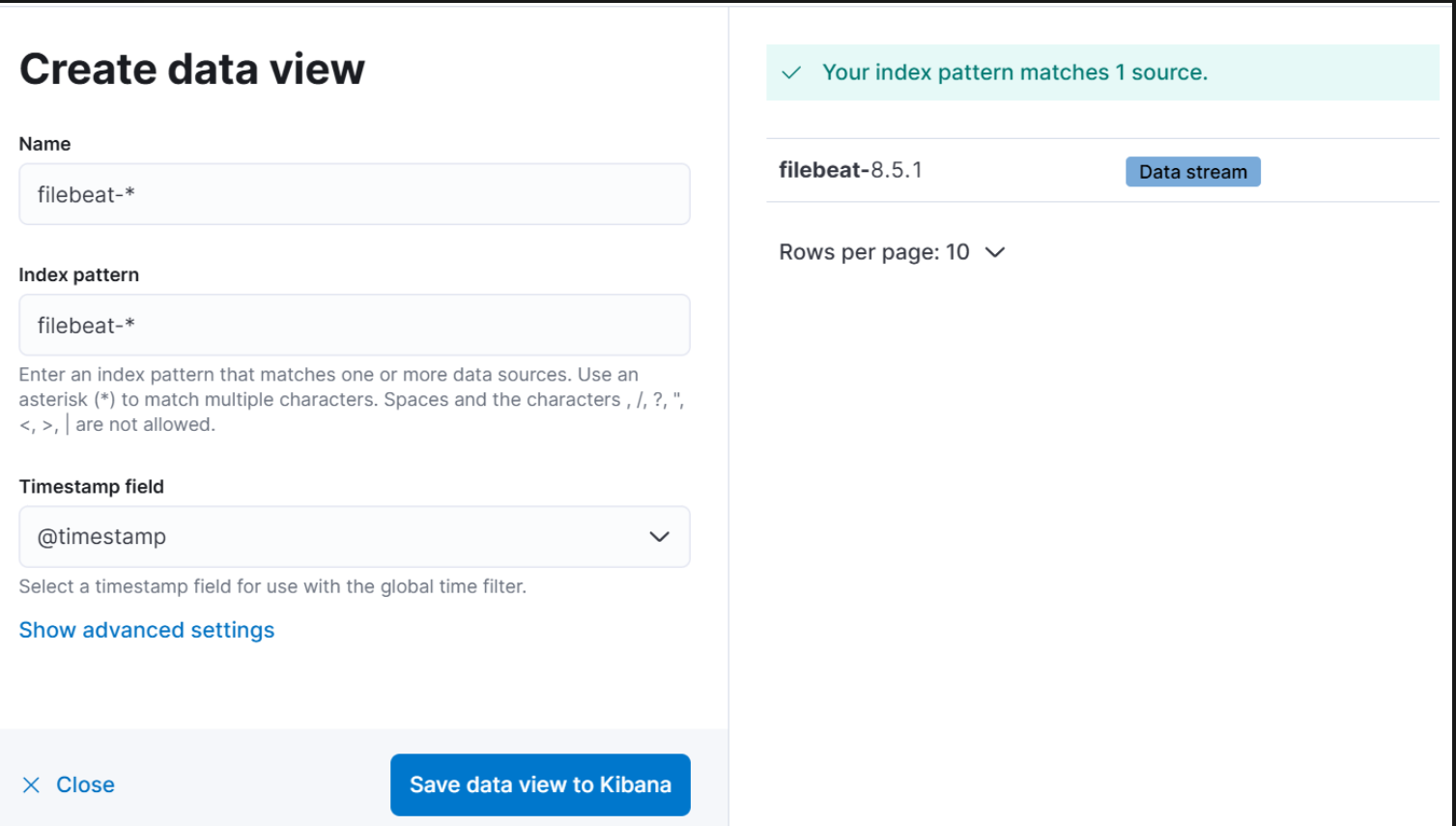
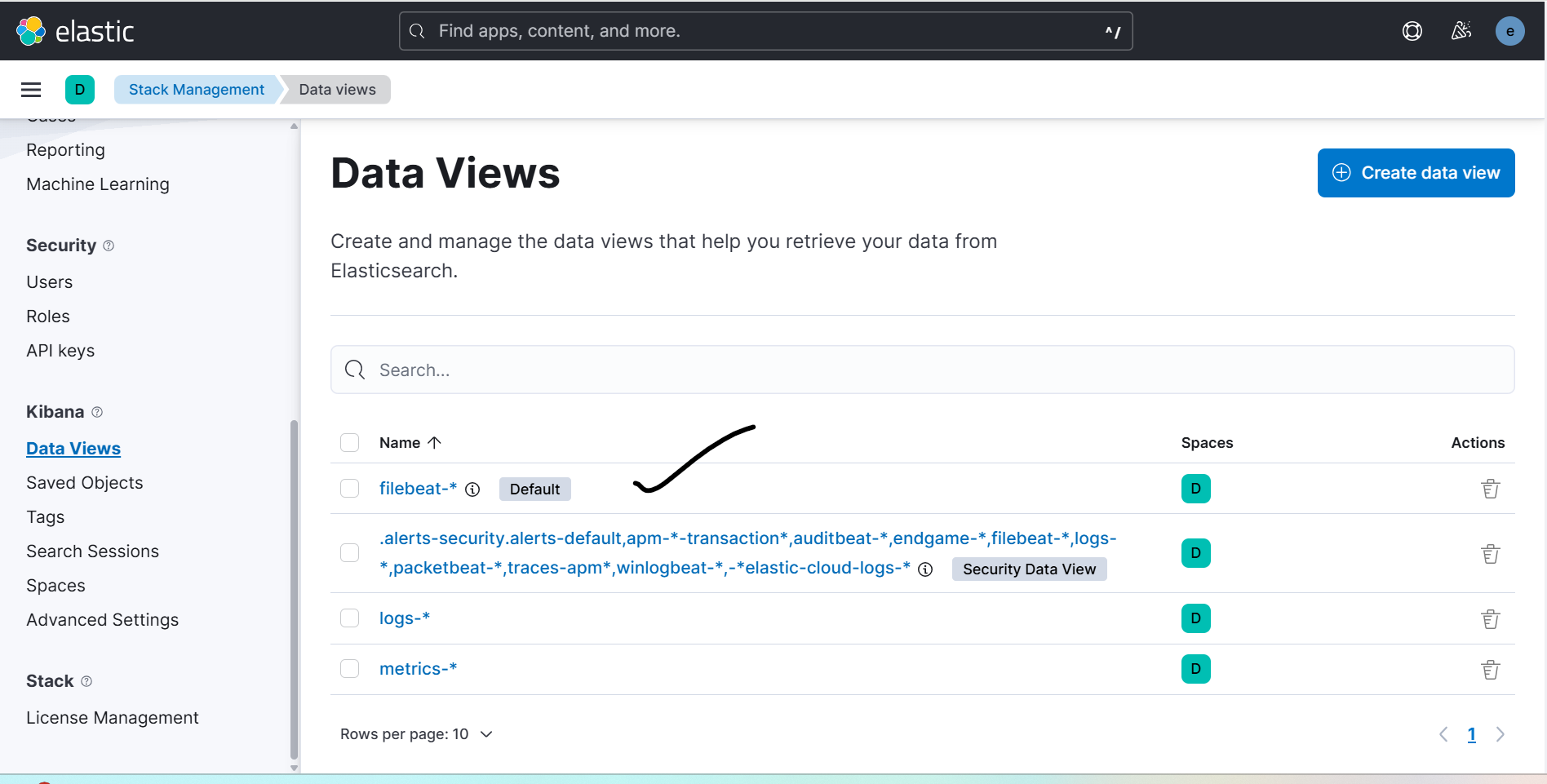
c. kubectl get secret <secret-name> -o=jsonpath='{.data.password}' | base64 –decode

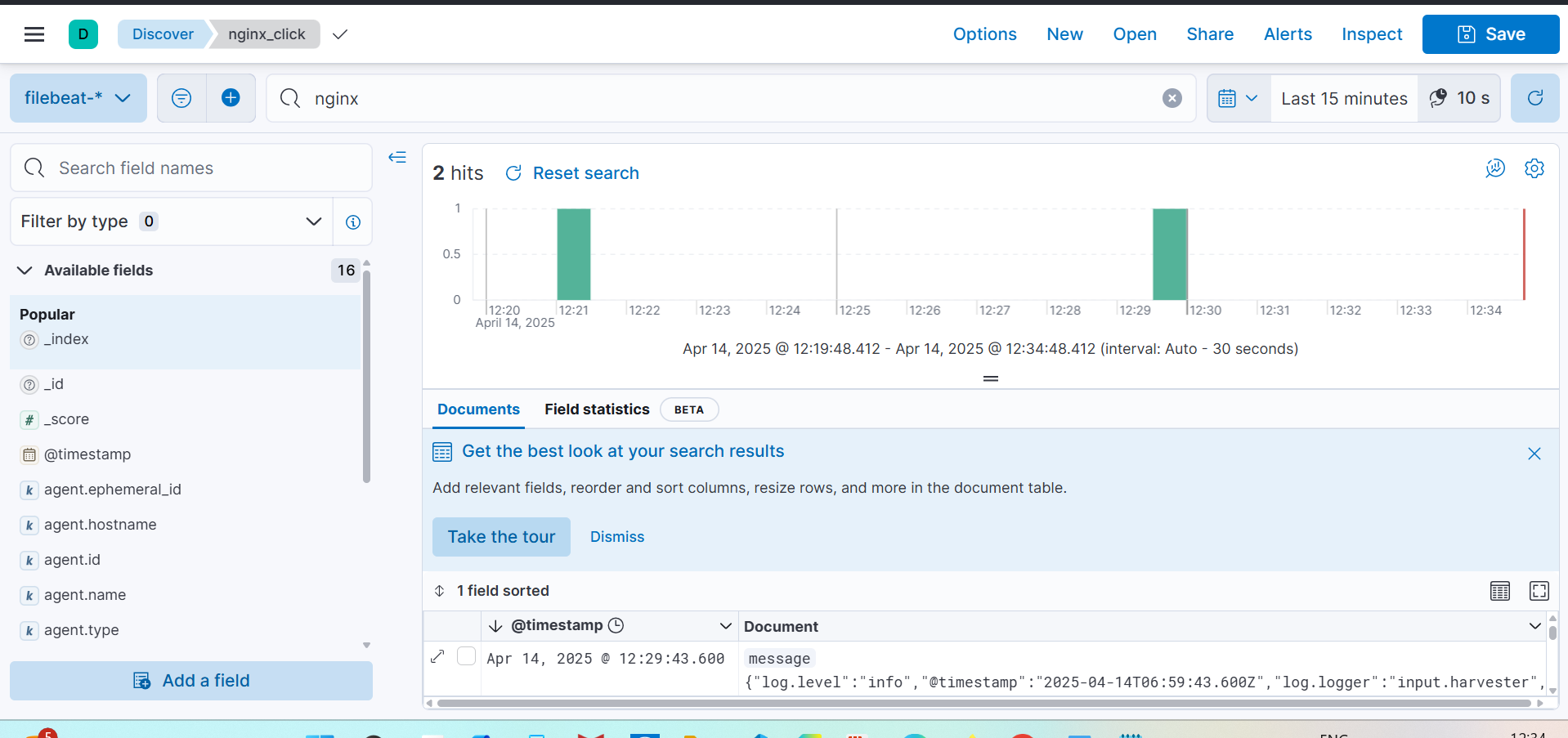
11. Once you get the creds, you can log in into the Kibana. Also make sure all the filebeat pods and everything else is running, run below command

a. kubectl get pods -A | grep -v Running (Excludes the pod which are in running state)

12. Check if filebeat is coming in below path, if it is then that means filebeat is successfully sending the data to Kibana



13. Now, its time to create an index, use below steps,   

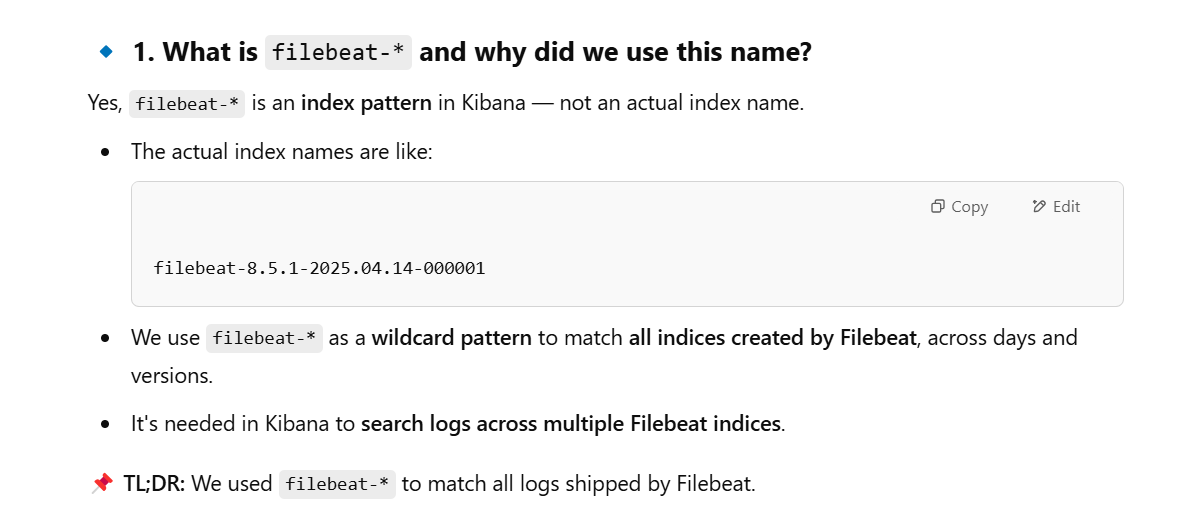
14. Now go to Discover, & you will be able to see the data coming, 

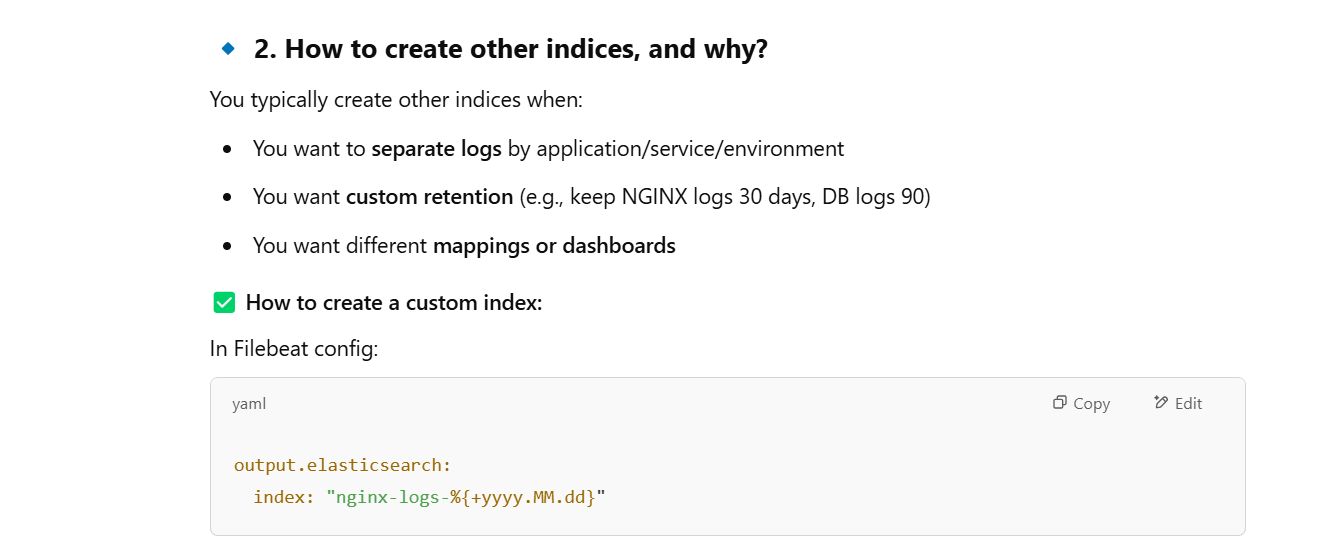
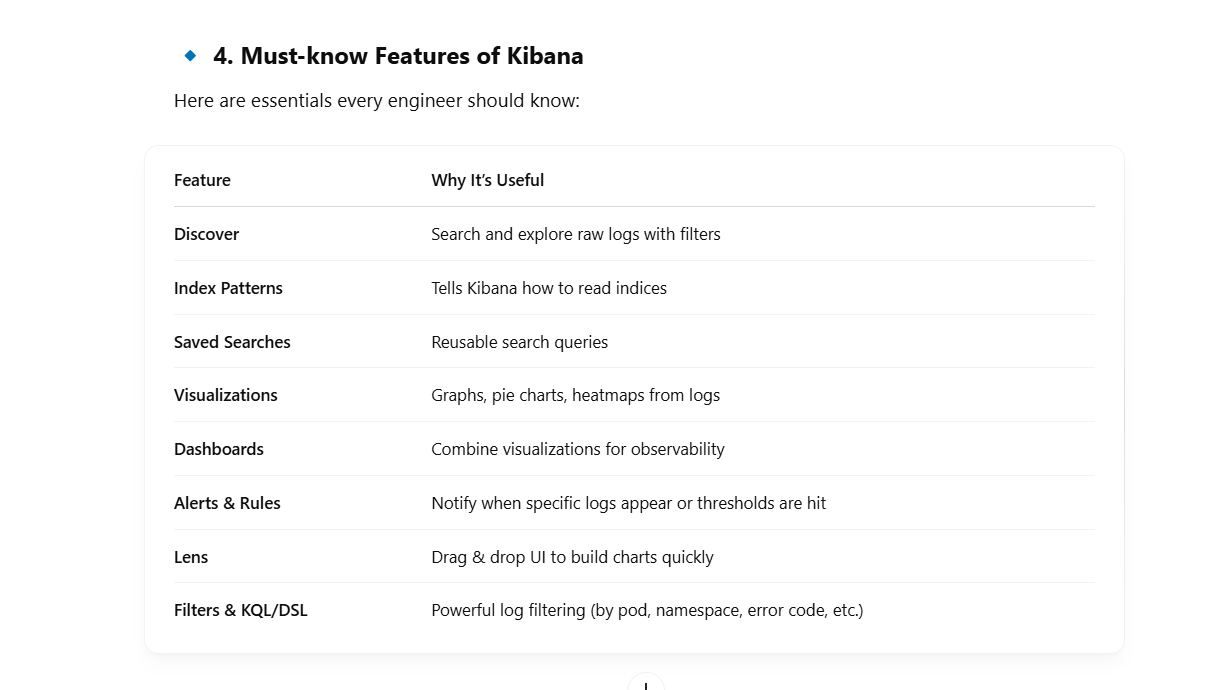
Also, I verified, the data is coming correctly, like when I accessed the nginx site from the phone, it showed the data is coming from phone.

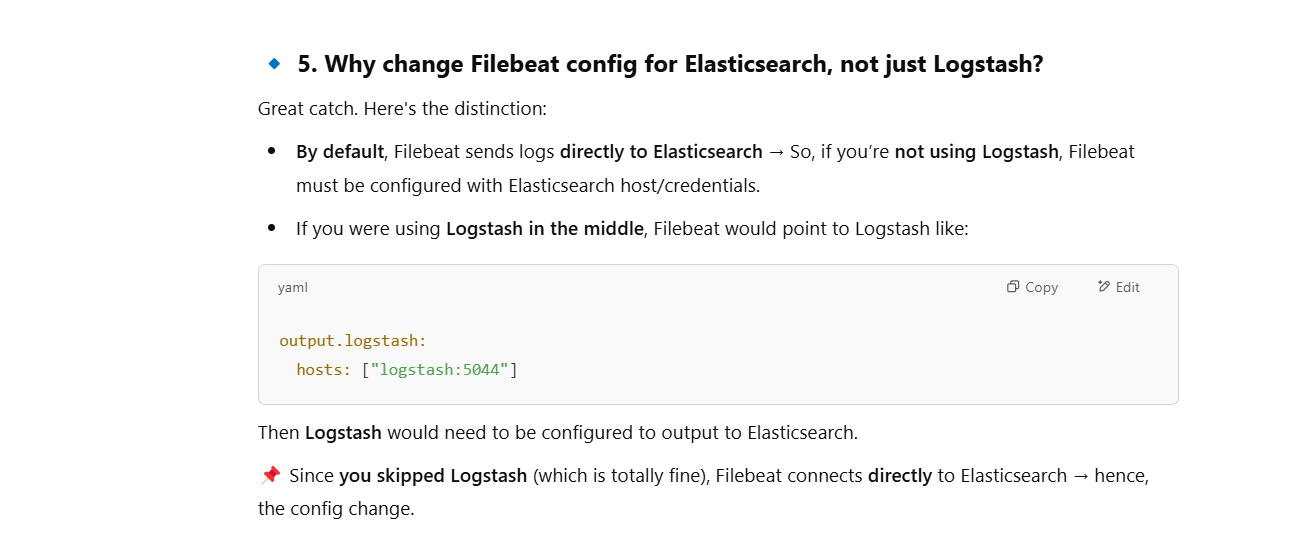
**IMP Observations:**

1. You can check the logs of each pod with command K logs <pod\_name> 🡪 These same logs are shipped to the Kibana
2. Filebeat runs as daemon-set & it ships logs of each and every single pod present on the cluster. You don’t need to mention any app labels or name while configuring. It just sends logs of all the containers & pods including the ones in kube-system too.
3. Even if you create new pod after creating the FEK stack, then also it automatically starts picking its log and sends to the kibana. [Apply the yaml of prasad-logger in the EOF file and you will the logs getting reflected in kibana dashboard]

**FAQs I asked ChatGPT:**



** [Double click on the Icon Te Get the Yaml Files]**

