**ELK Stack – KT Document**

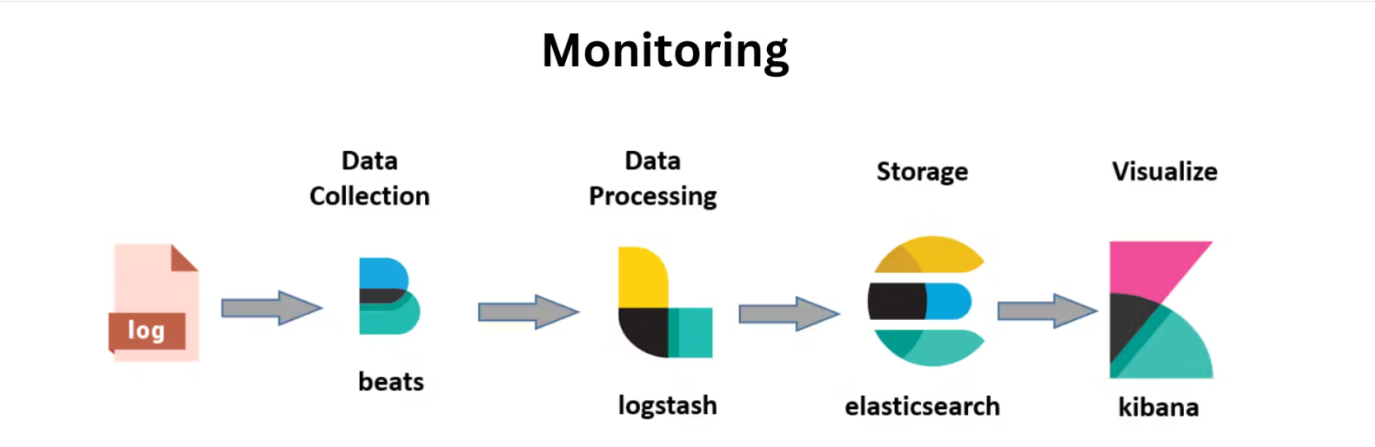
**Prepared by: \*\*Ravindra Mahato\*\***

**DevOps Engineer | Parity Infotech Solutions Pvt. Ltd.**

**📆 April 2025**

**📧** [**ravindra.m@paritysystems.in**](mailto:ravindra.m@paritysystems.in)

**ELK Stack Installation and Configuration Guide (Company VMs: 10.231.2.19, 10.231.2.20, 10.231.2.21)**

****

**Overview**

This document outlines the complete setup, configuration, troubleshooting, and security integration process of the ELK Stack (Elasticsearch, Logstash, Kibana) with Metricbeat and Filebeat for monitoring and log collection on internal VMs:

* **10.231.2.19** → Elasticsearch
* **10.231.2.20** → Logstash
* **10.231.2.21** → Kibana + Nginx Reverse Proxy

This KT ensures any new team member or client can replicate or maintain the environment.

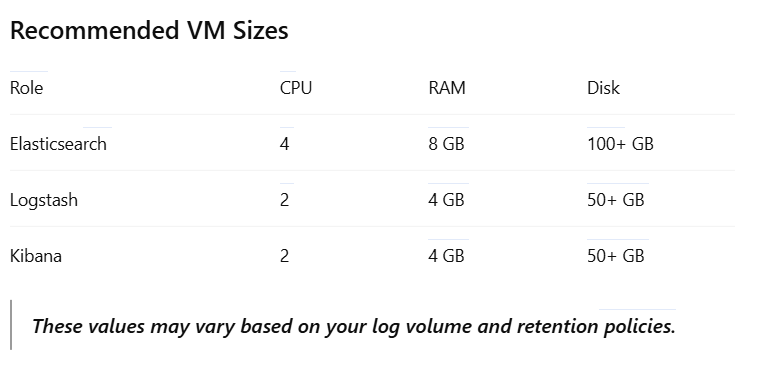
**VM-Wise Role Distribution:**

| **VM IP** | **Role** | **Purpose** |
| --- | --- | --- |
| 10.231.2.19 | Elasticsearch | Stores all logs and metrics |
| 10.231.2.20 | Logstash | Collects and filters data from Beats |
| 10.231.2.21 | Kibana + Nginx | Visualizes the logs; secured proxy |

**1. Pre-requisites on All VMs**

sudo apt update -y

sudo apt install openjdk-11-jre –y



**2. Elasticsearch Installation (10.231.2.19)**

curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

echo "deb 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 -y

sudo apt install elasticsearch -y

Edit config:

sudo nano /etc/elasticsearch/elasticsearch.yml

network.host: 0.0.0.0

http.port: 9200

xpack.security.enabled: true

Start service:

sudo systemctl enable elasticsearch

sudo systemctl start elasticsearch

**3. Secure Elasticsearch User Setup**

sudo /usr/share/elasticsearch/bin/elasticsearch-setup-passwords interactive

Set passwords for: elastic, kibana\_system, logstash\_system

**4. Logstash Installation (10.231.2.20)**

sudo apt install logstash -y

Create Logstash pipeline:

sudo nano /etc/logstash/conf.d/beats-input.conf

input {

beats {

port => 5044

}

}

filter {

}

output {

elasticsearch {

hosts => ["http://10.231.2.19:9200"]

user => "elastic"

password => "<your\_password>"

index => "%{[@metadata][beat]}-%{+YYYY.MM.dd}"

}

}

Restart service:

sudo systemctl daemon-reexec

sudo systemctl restart logstash

**5. Kibana + Nginx Installation (10.231.2.21)**

sudo apt install kibana nginx apache2-utils -y

sudo systemctl enable kibana

sudo systemctl start kibana

Edit config:

sudo nano /etc/kibana/kibana.yml

server.host: "localhost"

elasticsearch.hosts: ["http://10.231.2.19:9200"]

elasticsearch.username: "kibana\_system"

elasticsearch.password: "<your\_password>"

xpack.security.enabled: true

Configure reverse proxy:

sudo htpasswd -c /etc/nginx/htpasswd.users admin

sudo nano /etc/nginx/sites-enabled/default

server {

listen 80;

server\_name 10.231.2.21;

auth\_basic "Restricted Access";

auth\_basic\_user\_file /etc/nginx/htpasswd.users;

location / {

proxy\_pass http://localhost:5601;

proxy\_http\_version 1.1;

proxy\_set\_header Upgrade $http\_upgrade;

proxy\_set\_header Connection 'upgrade';

proxy\_set\_header Host $host;

proxy\_cache\_bypass $http\_upgrade;

}

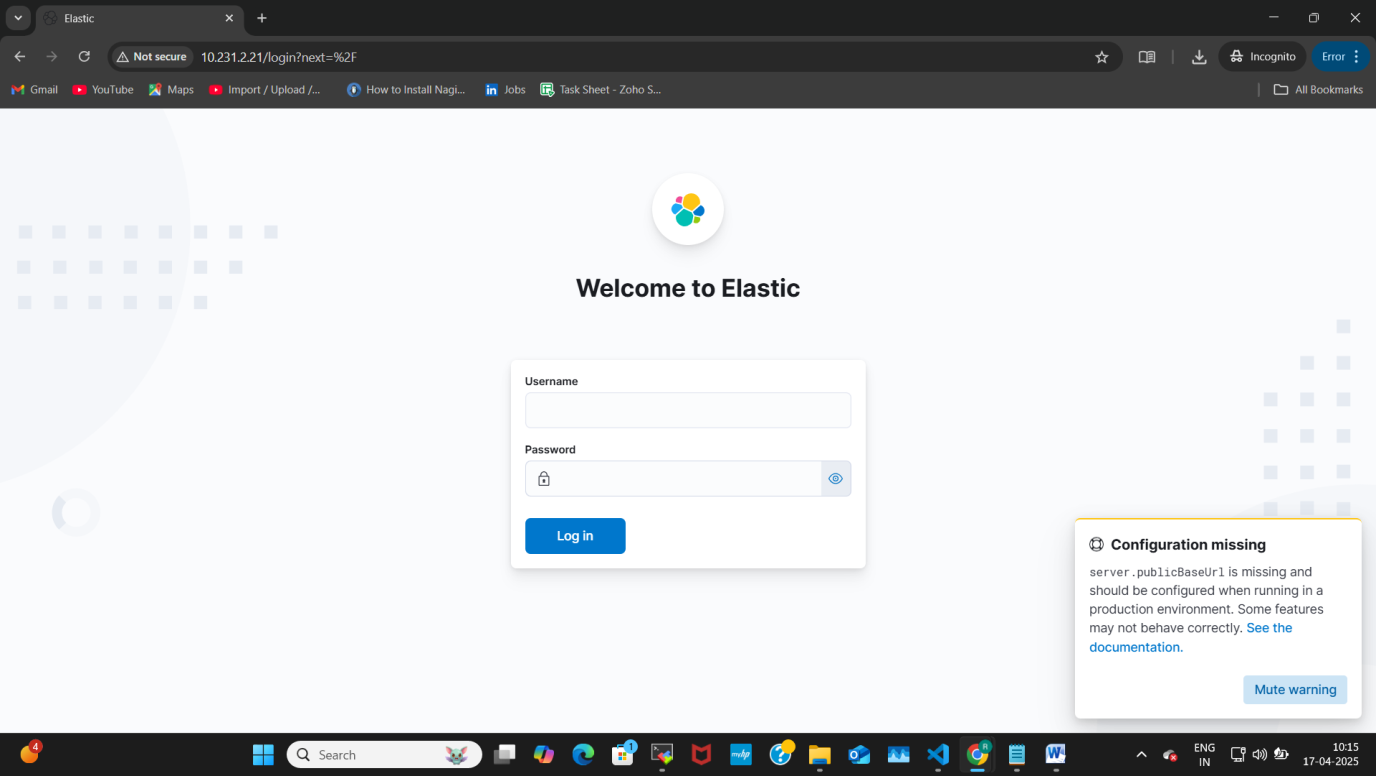
}

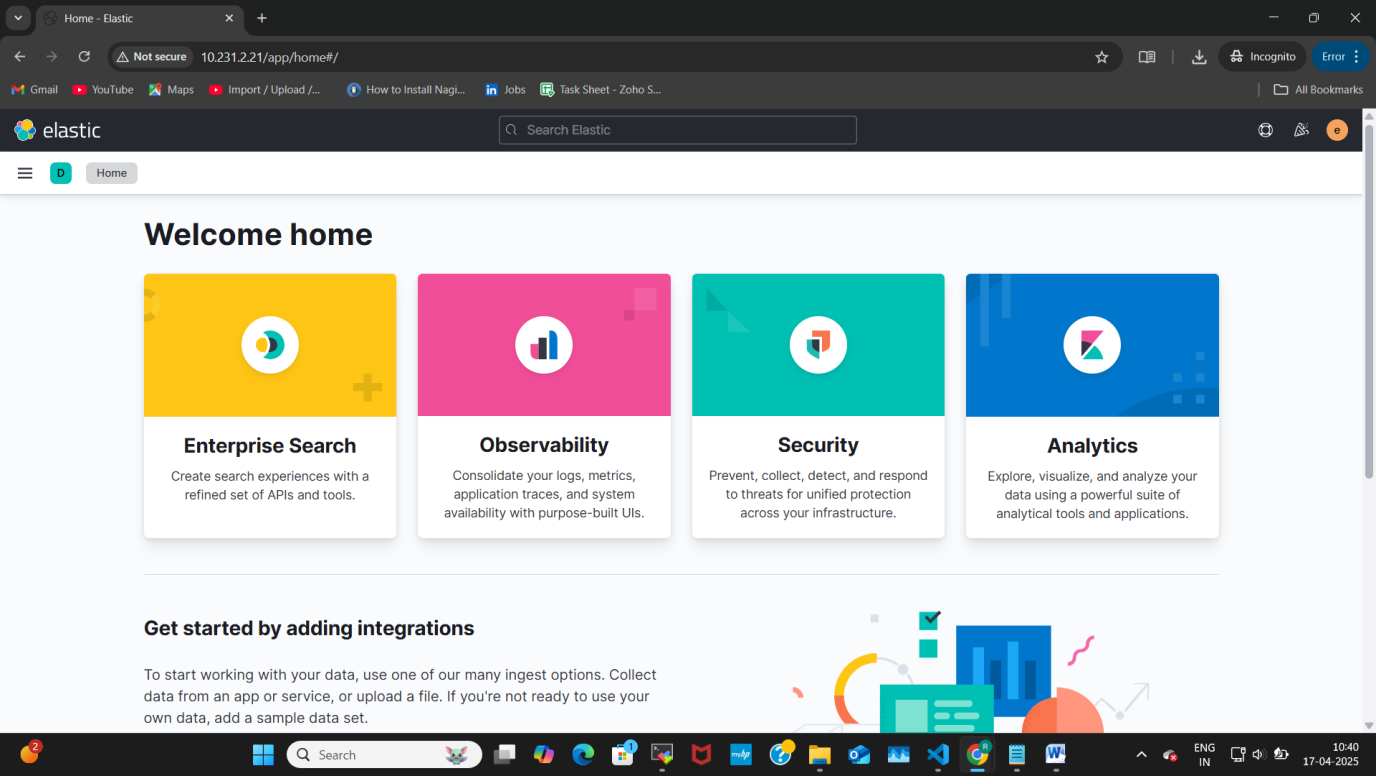
Restart services:

sudo systemctl restart nginx

sudo systemctl restart kibana

Access Kibana at: <http://10.231.2.21>



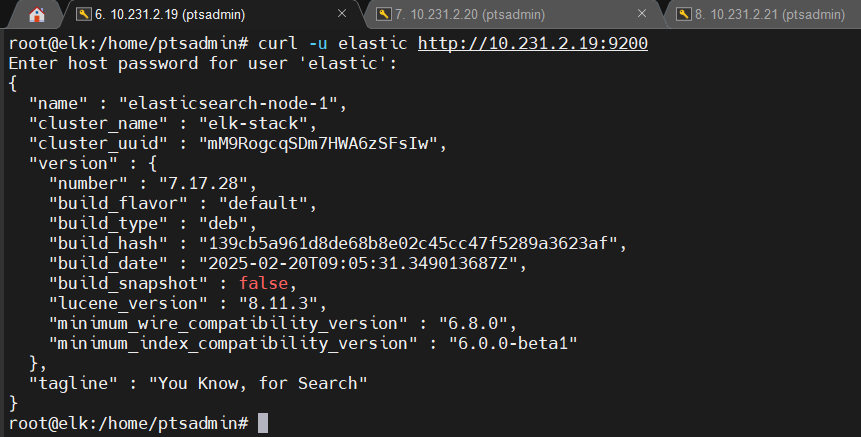


**✅ Check if ELK Components are Installed**

**Elasticsearch:**

curl -u elastic <http://10.231.2.19:9200>

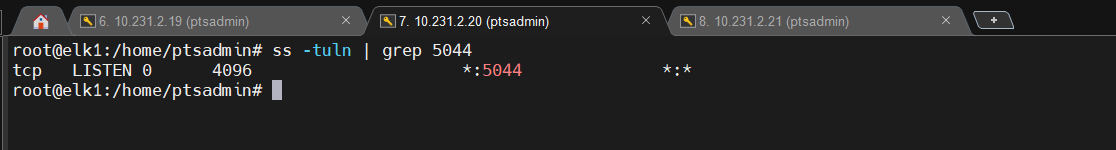
Expected output includes version, node name, and cluster info.

****

**Logstash:**

ss -tuln | grep 5044

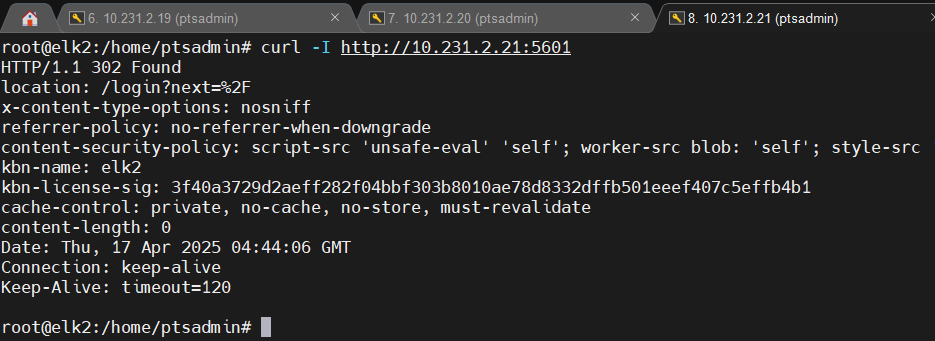
Expected to see Logstash listening on port 5044.



**Kibana:**

curl -I http://10.231.2.21:5601

Expected: HTTP/1.1 302 Found (redirect to login page)



**6. Filebeat & Metricbeat Installation (on all monitored VMs)**

sudo apt install filebeat metricbeat -y

sudo filebeat modules enable nginx

sudo metricbeat modules enable system

**Configure Filebeat:**

sudo nano /etc/filebeat/filebeat.yml

output.logstash:

hosts: ["10.231.2.20:5044"]

**Configure Metricbeat:**

sudo nano /etc/metricbeat/metricbeat.yml

Inside this file search for **Elasticsearch Output**, replace localhost with Logstash IP if on different machine.

output.logstash:

hosts: ["10.231.2.20:5044"]

Start Services:

sudo systemctl start filebeat

sudo systemctl start metricbeat

To list available modules:

sudo metricbeat modules list

**7. Verify Data Flow**

* Check Elasticsearch indices:

curl -X GET "http://10.231.2.19:9200/\_cat/indices?v"

* filebeat-\* and metricbeat-\* should appear

**8. Kibana Dashboards & Index Setup**

1. Go to Kibana > Stack Management > Index Patterns
2. Create:
   * filebeat-\*
   * metricbeat-\*
3. Save → Go to **Discover** → Raw log data appears
4. Load Dashboards:

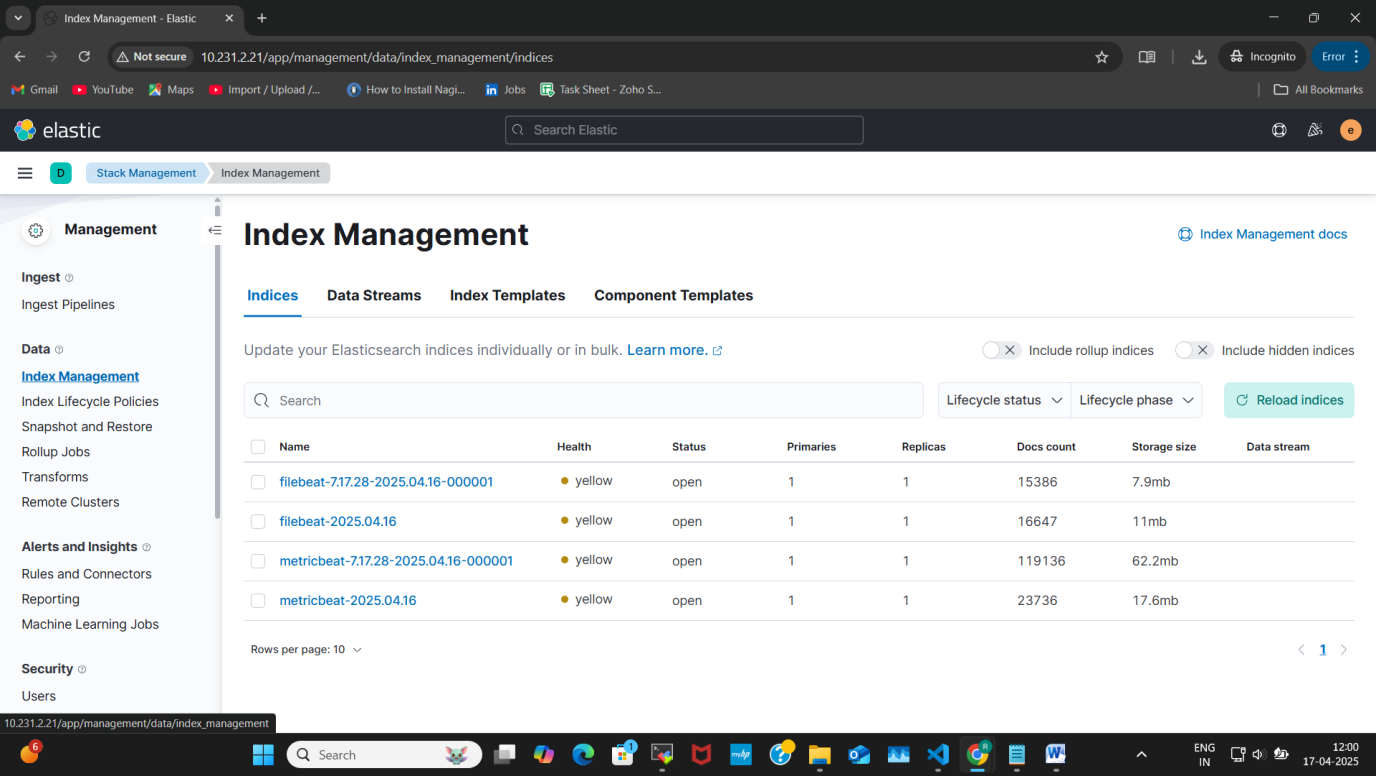
sudo filebeat setup

1. Go to **Dashboard** → Metricbeat/Filebeat Dashboards → View:

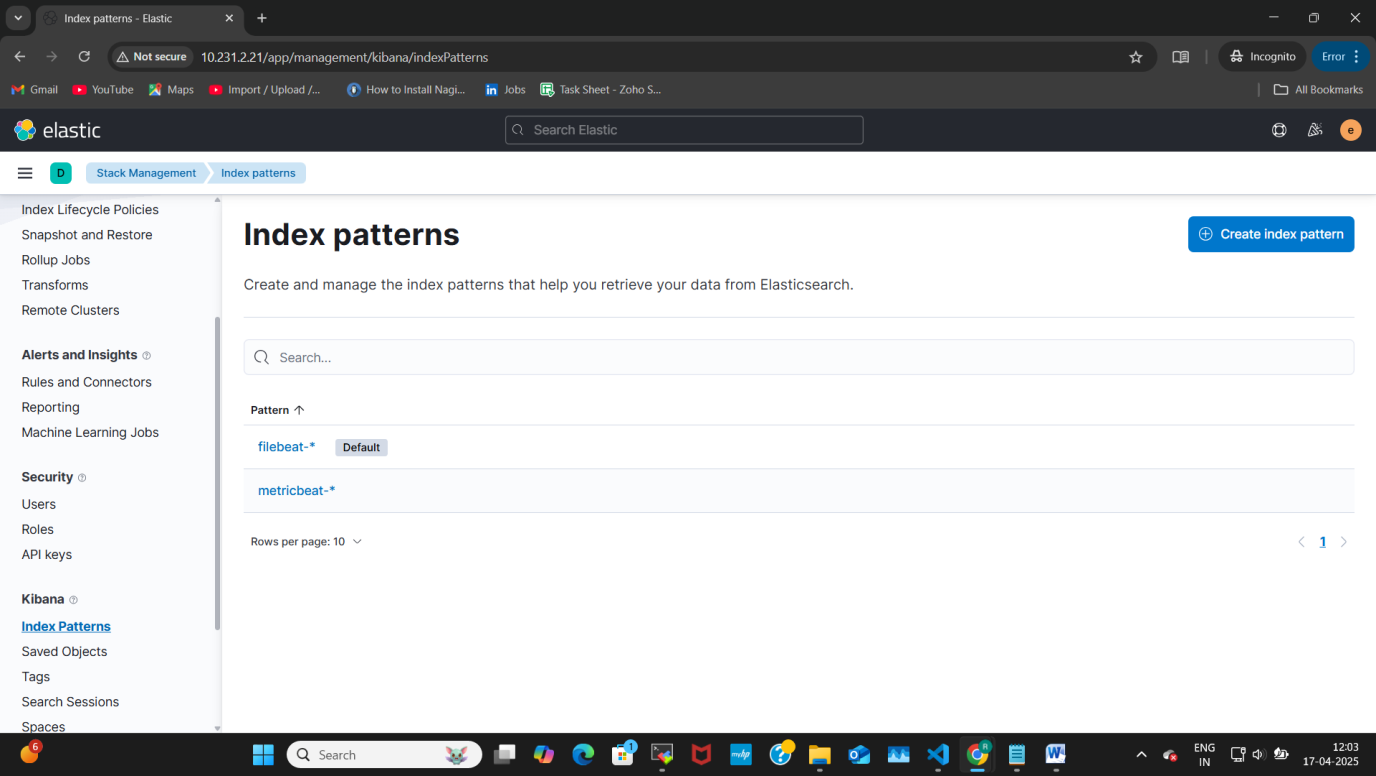
* Host overview
* Log maps
* Raw data

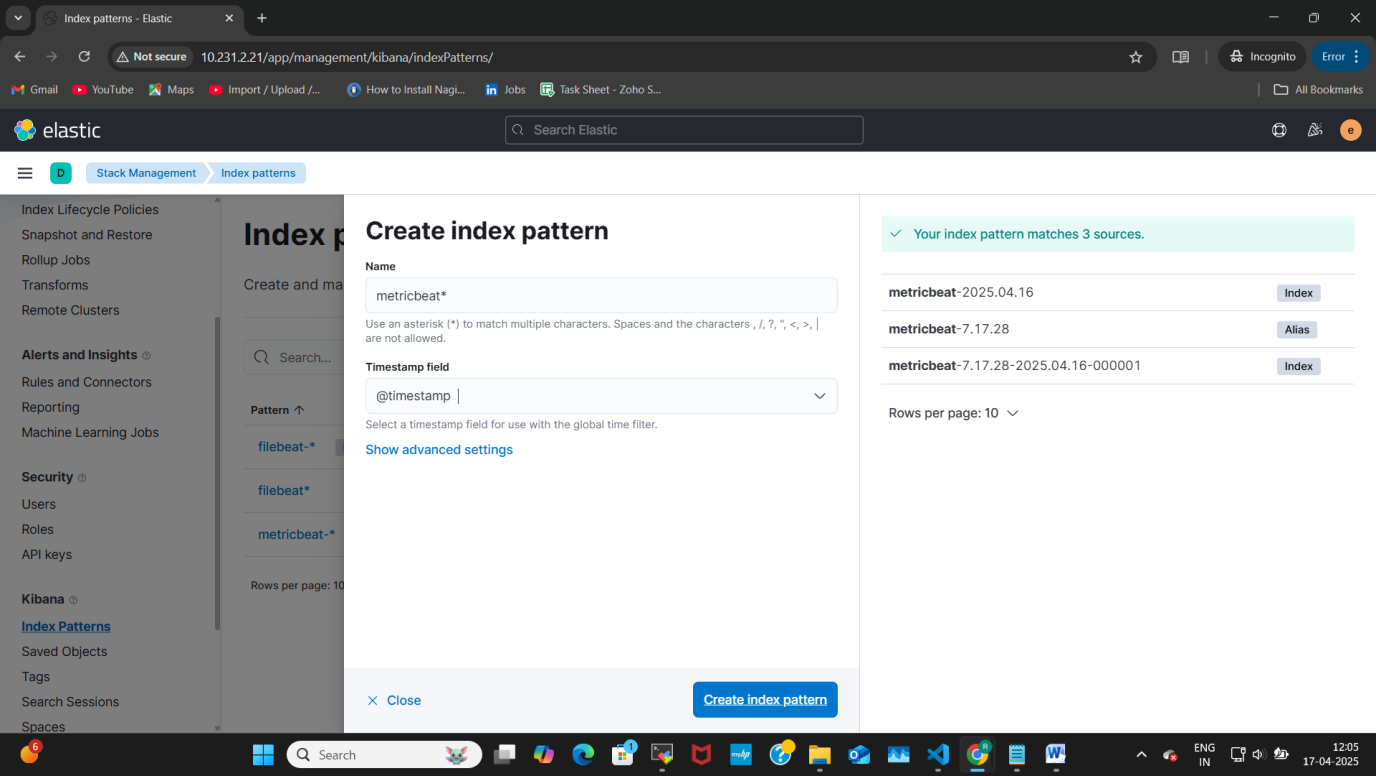
In the dashboard section, you'll find the multiple dashboards for multiple services

Stack Management > Index Management



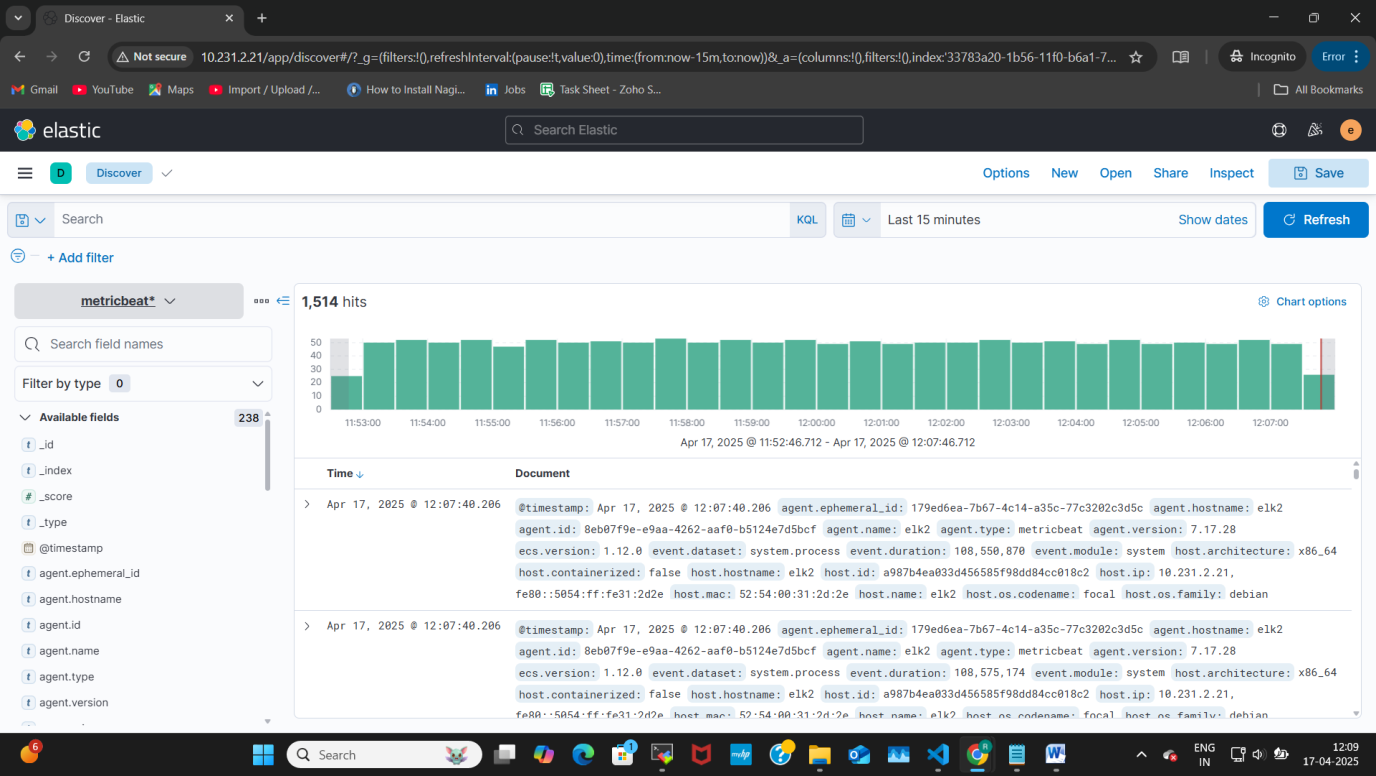
Now we have to create an Index pattern without creating this we won't be able to visualize the data in Kibana



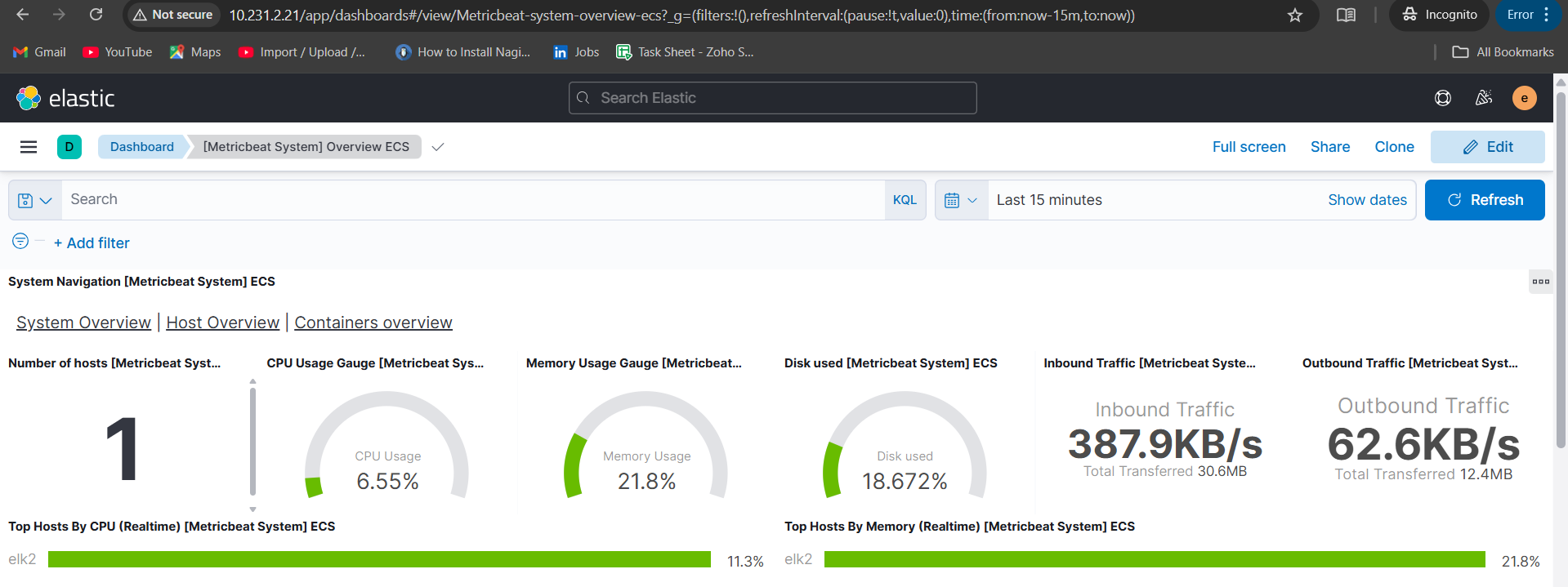


After adding the index pattern click to discover

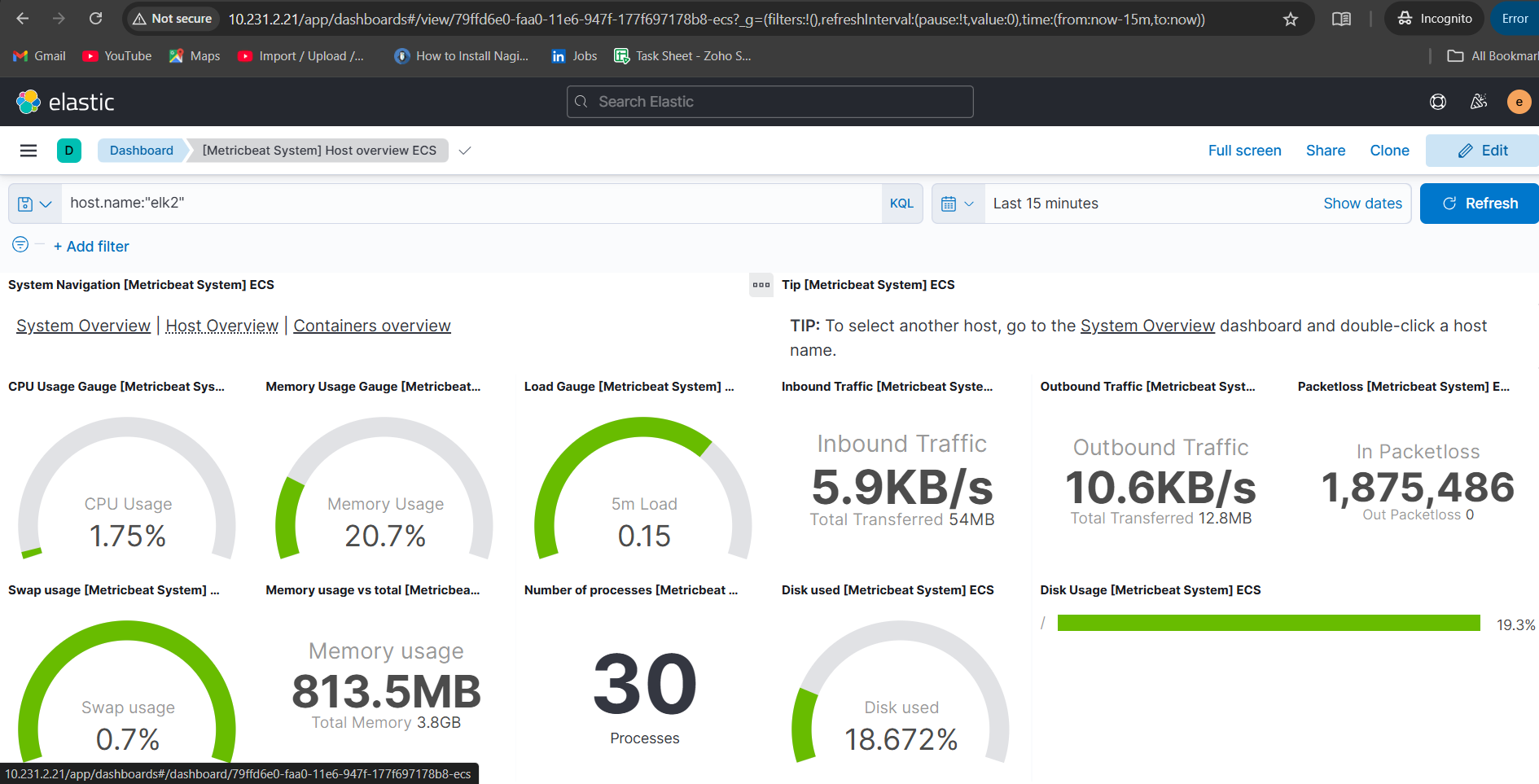
Right now, we can see the data but it's in the raw format



**System Overview**

****

**Host Overview**

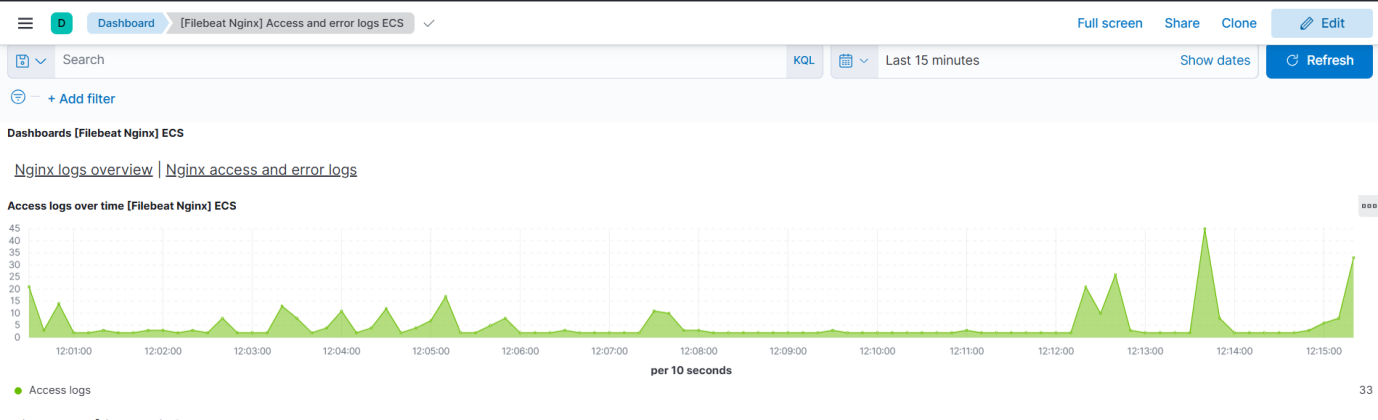
****

**Filebeat – Nginx Logs Visualization in Kibana**

Filebeat is responsible for collecting and forwarding log files such as Nginx access and error logs to Logstash, which are then stored in Elasticsearch and visualized in Kibana.

**Nginx Access Log Overview (Graph Format)**

* This dashboard provides a time-based graph showing the number of access requests to the Nginx web server over the selected time range (e.g., last 15 minutes).
* The spikes indicate high traffic moments, and the line graph helps visualize request patterns per 10-second intervals.

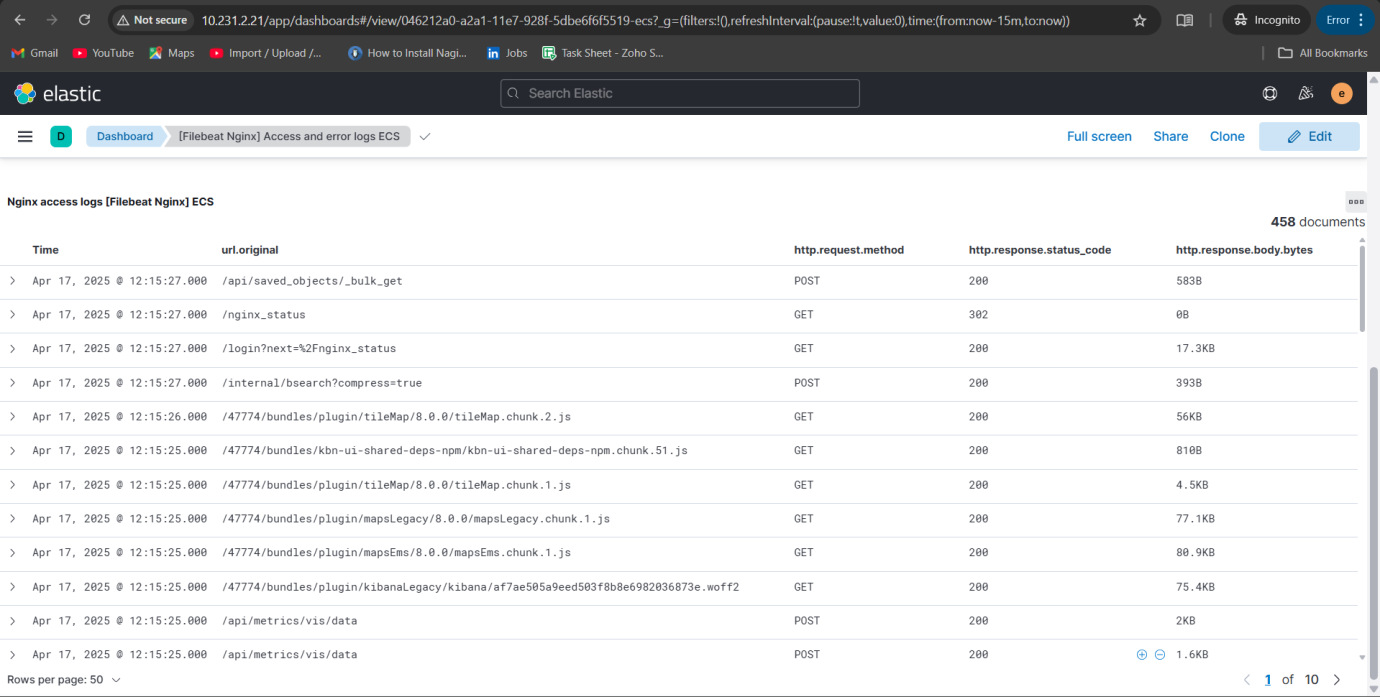


Nginx Access Logs (Table Format)

This dashboard provides a detailed table view of each request received by the Nginx server.

Fields shown include:

* Time of the request
* Request URL (url.original)
* HTTP Method (GET, POST, etc.)
* Response Code (200, 302, etc.)
* Useful for debugging, security auditing, and performance monitoring.



**9. Types of Monitoring Enabled**

**1. Uptime Monitoring**

* ICMP (ping): check server availability
* HTTP (curl): check application availability
* TCP (telnet): check port response

**2. Server Monitoring**

* CPU, Memory, Disk, Network, Swap, Process
* Tools: top, htop, Metricbeat dashboards

**3. Log Monitoring**

* App/System logs: /var/log/nginx/, /var/log/httpd/, /var/log/apache2/
* Error messages, HTTP status, client IP, event details

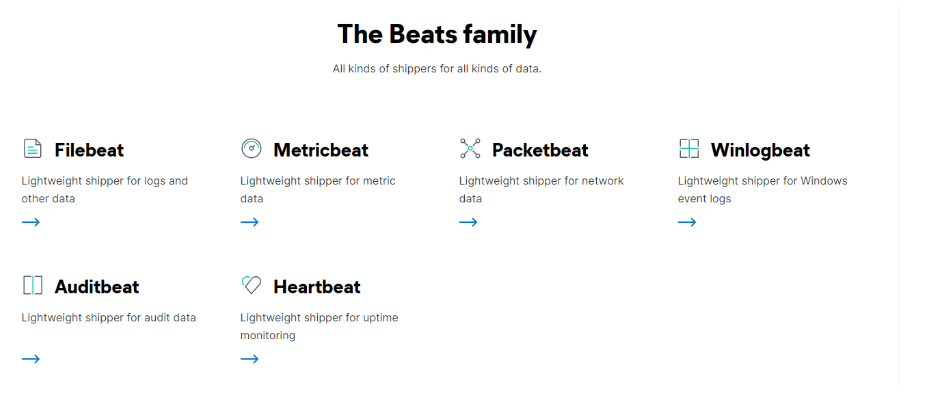
**4. Security Monitoring**

* Ubuntu: /var/log/auth.log
* CentOS: /var/log/secure
* Audit Logs: /var/log/audit

**10. Beats Types Summary**

|  |  |
| --- | --- |
| Beat | Use Case |
| Filebeat | Logs and application data |
| Metricbeat | System metrics |
| Packetbeat | Network data |
| Winlogbeat | Windows event logs |
| Auditbeat | Audit logs |
| Heartbeat | Uptime/availability checks |

**Install any beat by using the command**



**11. Common Troubleshooting Steps**

* If Logstash fails:
  + Check /etc/logstash/conf.d/ for config syntax errors
  + Restart with:

sudo systemctl daemon-reexec

sudo systemctl restart logstash

* If data not visible in Kibana:
  + Ensure Kibana index pattern is created
  + Verify beats with:

filebeat test output

metricbeat test output

* Log review:
  + Logstash: /var/log/logstash/logstash-plain.log
  + Elasticsearch: /var/log/elasticsearch/elasticsearch.log

**12. Final Security Setup Summary**

* Never log in with kibana\_system
* Always log in with:
  + elastic (superuser)
  + or a user with kibana\_admin role

**To create a user:**

Kibana → Stack Management → Security → Users → Create User