

System Admin

Training Assignments

|  |  |
| --- | --- |
| Program Code |  |
| Issue/Revision | x/y |
| Effective date | 04/Aug /2023 |

Assignment Day 12. Logging

Mục Lục:

[Hướng dẫn cài đặt và cấu hình hệ thống log tập trung sử dụng ELK (Elastic Logstash Kibana) 2](#_Toc594734658)

[Prerequisites 3](#_Toc712577533)

[Install Required Dependencies 3](#_Toc1467095405)

[Install Elasticsearch 3](#_Toc152681837)

[Install and Configure Logstash 4](#_Toc2031089786)

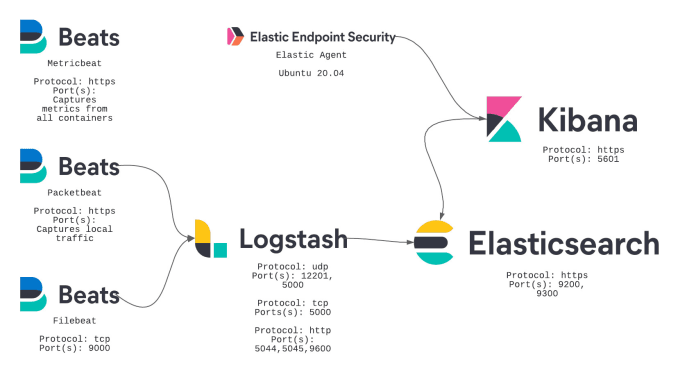
[Install and Configure Kibana 5](#_Toc486646501)

[Install and Configure Filebeat 6](#_Toc202270980)

[Access Kibana Web Interface 7](#_Toc1239521550)

# Hướng dẫn cài đặt và cấu hình hệ thống log tập trung sử dụng ELK (Elastic Logstash Kibana)





## Prerequisites

An Ubuntu 20.04 VPS (we’ll be using our NVMe 8 VPS hosting plan)

Access to the root user account (or access to an admin account with root privileges)

Log in to the Server & Update the Server OS Packages

First, log in to your Ubuntu 20.04 server via SSH as the root user:

ssh root@IP\_Address -p Port\_number

Before starting, you have to make sure that all Ubuntu OS packages installed on the server are up to date. You can do this by running the following commands:

apt-get update -y  
apt-get upgrade -y

## Install Required Dependencies

Before starting, you will need to install Java and other required dependencies in your server. You can install all of them using the following command:

apt-get install openjdk-11-jdk wget apt-transport-https curl gnupg2 -y

Once all the packages are installed, verify the installed version of Java with the following command:

java -version

You should get the following output:

openjdk version "11.0.9.1" 2020-11-04  
OpenJDK Runtime Environment (build 11.0.9.1+1-Ubuntu-0ubuntu1.20.04)  
OpenJDK 64-Bit Server VM (build 11.0.9.1+1-Ubuntu-0ubuntu1.20.04, mixed mode, sharing)

## Install Elasticsearch

By default, Elasticsearch is not available in the Ubuntu standard repository. So you will need to add the Elasticsearch repository to your system.

First, add the Elasticsearch signing key with the following command:

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -

Next, add the repository with the following command:

echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | tee -a /etc/apt/sources.list.d/elastic-7.x.list

Once the repository is added, update the repository and install the Elasticsearch package with the following command:

apt-get update -y  
apt-get install elasticsearch -y

Once the Elasticsearch is installed, start the Elasticsearch service and enable it to start at system reboot:

systemctl start elasticsearch  
systemctl enable elasticsearch

At this point, Elasticsearch is started and listening on port 9200. You can verify it with the following command:

ss -antpl | grep 9200

You should get the following output:

LISTEN 0 4096 [::ffff:127.0.0.1]:9200 \*:\* users:(("java",pid=27757,fd=257)) LISTEN 0 4096 [::1]:9200 [::]:\* users:(("java",pid=27757,fd=256))

You can also check the Elasticsearch by sending an HTTP request:

curl -X GET <http://localhost:9200>

You should get the following output:

{  
 "name" : "ubuntu2004",  
 "cluster\_name" : "elasticsearch",  
 "cluster\_uuid" : "LhG8-a\_eQHyyoRAlQQXBTQ",  
 "version" : {  
 "number" : "7.10.0",  
 "build\_flavor" : "default",  
 "build\_type" : "deb",  
 "build\_hash" : "51e9d6f22758d0374a0f3f5c6e8f3a7997850f96",  
 "build\_date" : "2020-11-09T21:30:33.964949Z",  
 "build\_snapshot" : false,  
 "lucene\_version" : "8.7.0",  
 "minimum\_wire\_compatibility\_version" : "6.8.0",  
 "minimum\_index\_compatibility\_version" : "6.0.0-beta1"  
 },  
 "tagline" : "You Know, for Search"  
}

## Install and Configure Logstash

Logstash is a log-parsing software used to collects logs and store them on Elasticsearch. You can install it easily with the following command:

apt-get install logstash -y

Once the Logstash is installed, you will need to configure the input, filter, and the output plugins. You can configure it by creating a new configuration file inside /etc/logstash/conf.d/ directory:

vim /etc/logstash/conf.d/logstash.conf

Add the following lines:

#Specify listening port for incoming logs from the beats  
  
input {  
 beats {  
 port => 5044  
 }  
}  
  
# Used to parse syslog messages and send it to Elasticsearch for storing  
  
filter {  
 if [type] == "syslog" {  
 grok {  
 match => { "message" => "%{SYSLOGLINE}" }  
 }  
 date {  
 match => [ "timestamp", "MMM d HH:mm:ss", "MMM dd HH:mm:ss" ]  
 }  
 }  
}  
  
# Specify an Elastisearch instance  
  
output {  
 elasticsearch {  
 hosts => ["localhost:9200"]  
 index => "%{[@metadata][beat]}-%{+YYYY.MM.dd}"  
 }  
}

Save and close the file then start the Logstash and enable it to start at system reboot.

systemctl start logstash  
systemctl enable logstash

## Install and Configure Kibana

Kibana visualizes the data stored on Elasticsearch through a web-based interface. You can install it with the following command:

apt-get install kibana -y

By default, Kibana listens on localhost. So you will need to configure it for external access. You can configure it by editing the file /etc/kibana/kibana.yml:

vim /etc/kibana/kibana.yml

Change the following lines:

server.host: "your-server-ip"  
elasticsearch.hosts: ["http://localhost:9200"]

Save and close the file then start the Kibana service and enable it to start at system reboot:

systemctl start kibana  
systemctl enable kibana

## Install and Configure Filebeat

Filebeat is used to send logs to the Logstash or Elasticsearch for parsing. In this section, we will install the Filebeat and configure it to send logs to the Logstash.

You can install it with the following command:

apt-get install filebeat -y

Once installed, edit the Filebeat main configuration file and configure it to send logs to the Logstash.

vim /etc/filebeat/filebeat.yml

Comment out the following lines:

#output.elasticsearch:  
# Array of hosts to connect to.  
# hosts: ["localhost:9200"]

Uncomment the following lines:

output.logstash:  
hosts: ["localhost:5044"]

Save and close the file then start the Filebeat service and enable it to start at system reboot:

systemctl start filebeat  
systemctl enable filebeat

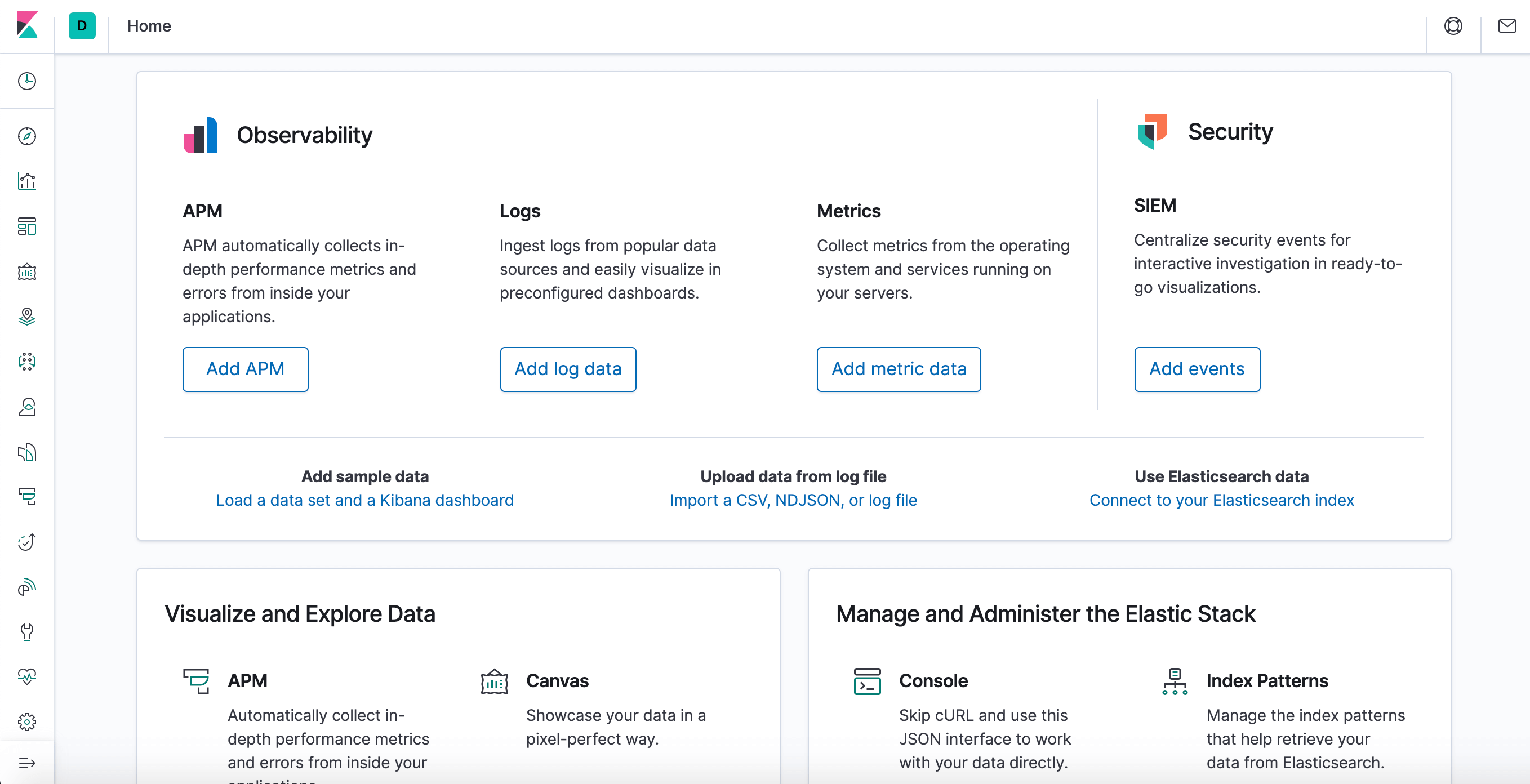
Next, enable the Filebeat system module, which will examine local system logs:

filebeat modules enable system

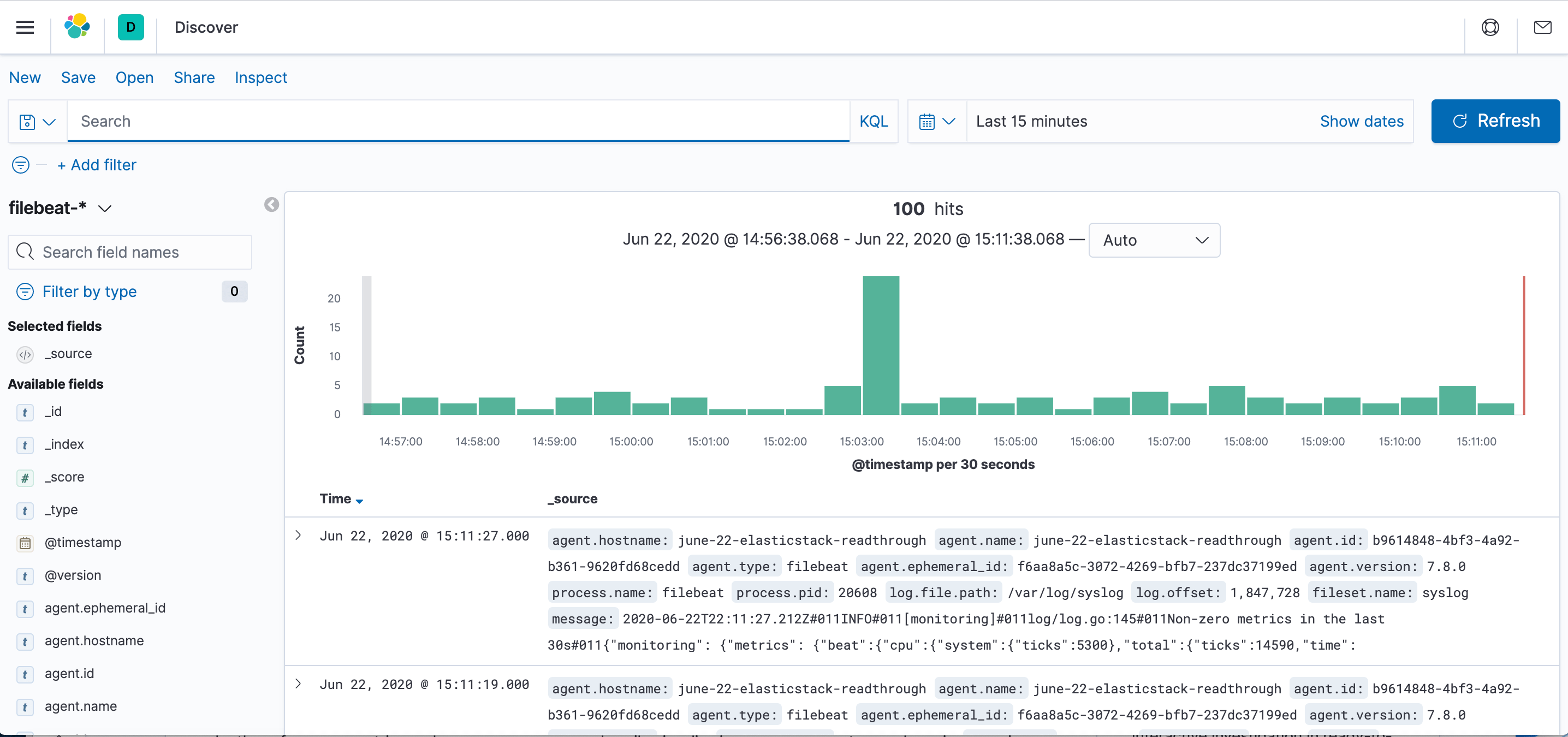
Next, load the index template with the following command:

## **Access Kibana Web Interface**

By default, Kibana listens on port **5601**. You can access it using the URL <http://your-server-ip:5601>. You should see the Kibana dashboard in the following screen:

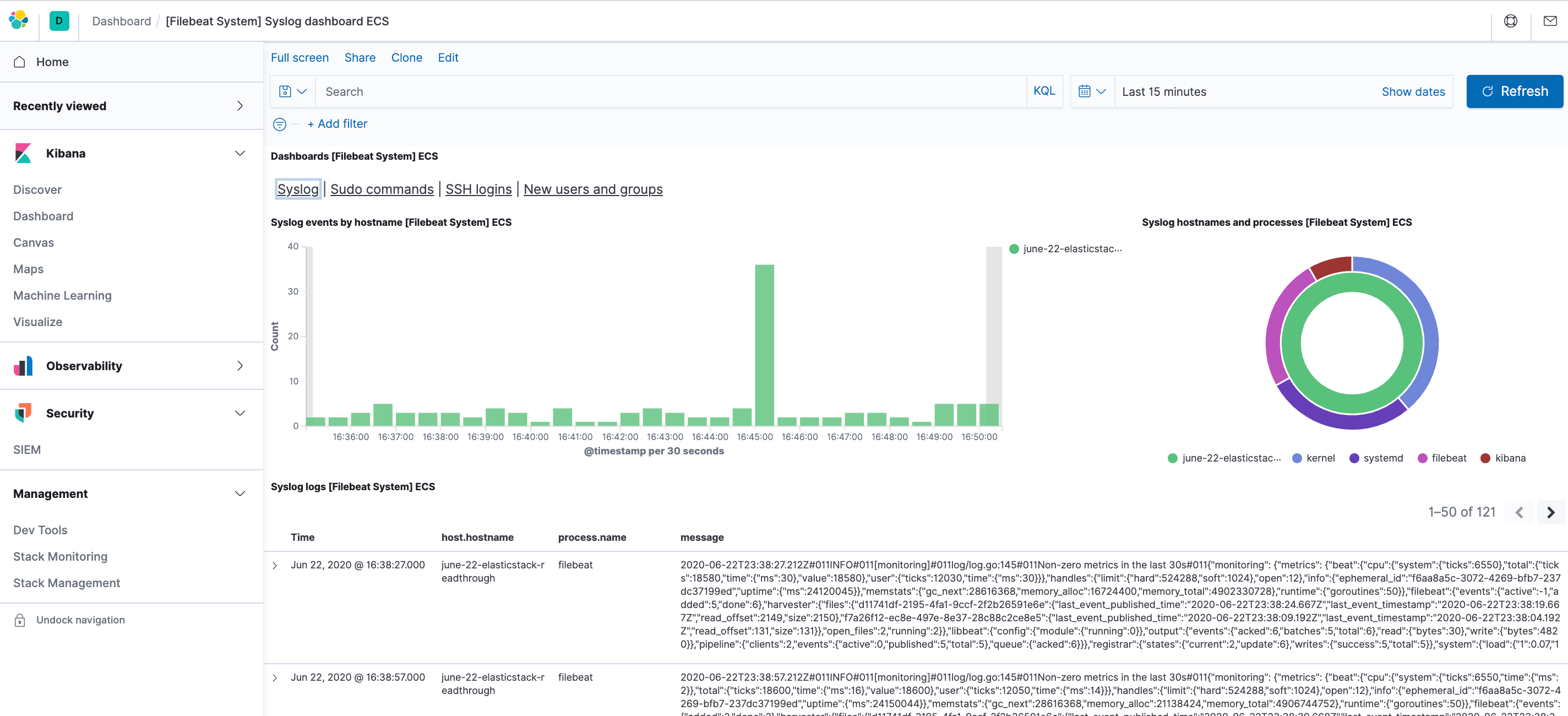


2. Now, click the Discover link in the left-hand navigation bar. You may have to click the Expand icon at the bottom left to see navigation menu items. Then, on the Discover page, select the predefined filebeat. By default, it will show you all of the log data over the last 15-minutes. Moreover, you will see a histogram with log-events, with log messages below:

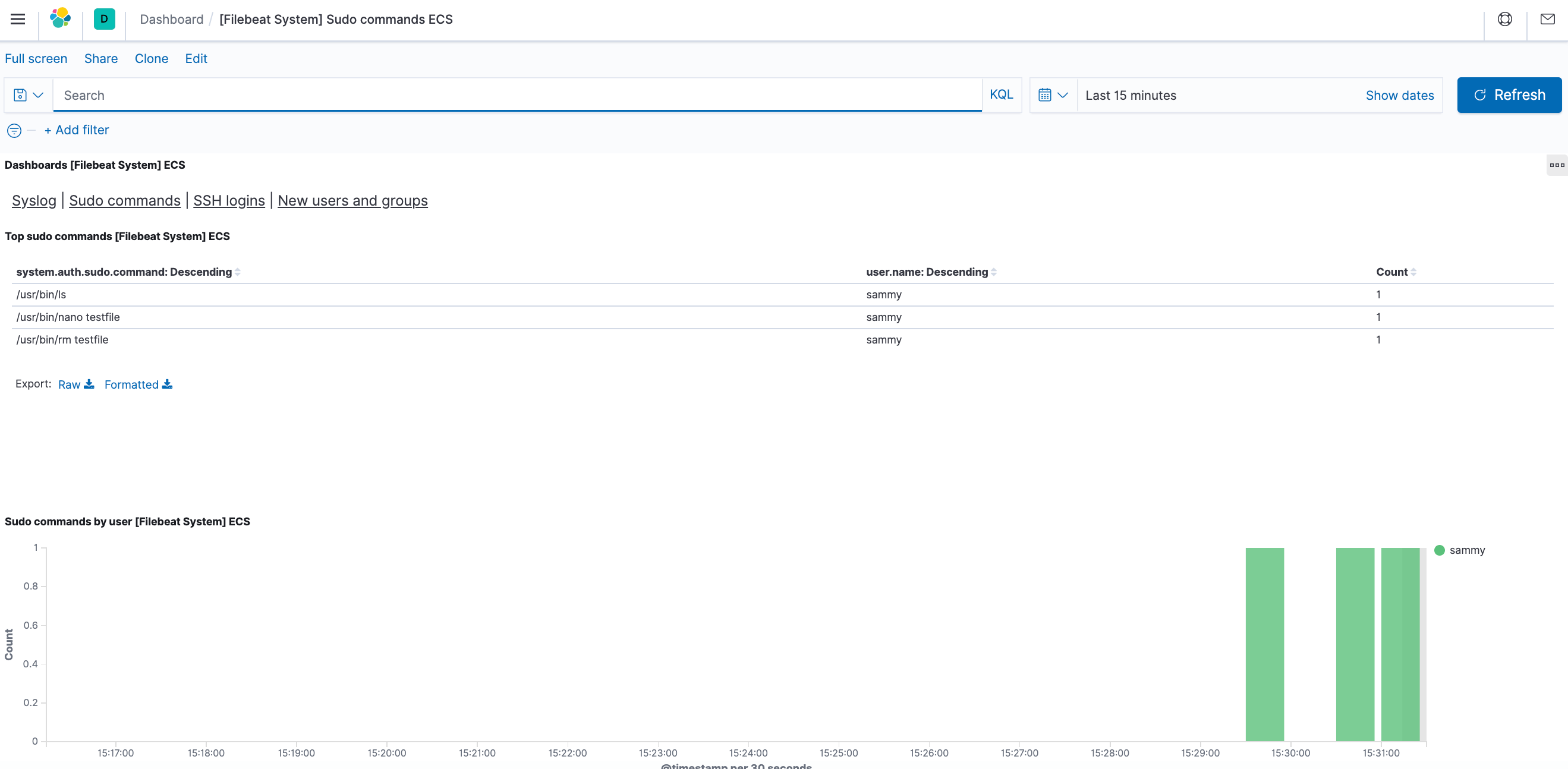


3. Here, you will search and browse via logs and even customize your dashboard. At this point, though, there will not be much in there as, here you are only gathering syslogs from Elastic Stack server.

4. You will next use the left-hand panel to navigate to the Dashboard page. Also, search for the Filebeat System dashboards. Once you are there, select the sample dashboards that has Filebeat’s system module. For instance, you will view details of stats on basis of your syslog-messages:



5. You can also see the users if they use sudo command and when:



Kibana has many features, like graphing and filtering, therefore, feel free to explore.