

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)

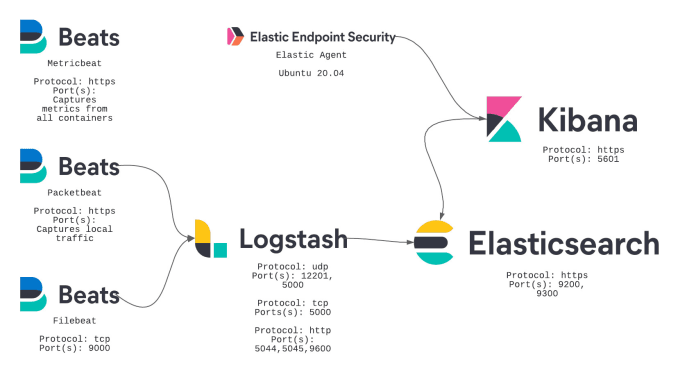
[Install and Configure Kibana 5](#_Toc486646501)

[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 # example command

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:

**root@ElasticSearch:~# apt-get install openjdk-11-jdk wget apt-transport-https curl gnupg2 -y**

*Reading package lists... Done*

*Building dependency tree... Done*

*Reading state information... Done*

*wget is already the newest version (1.21.4-1ubuntu4).*

*wget set to manually installed.*

*curl is already the newest version (8.5.0-2ubuntu10.1).*

*curl set to manually installed.*

*The following additional packages will be installed:*

*alsa-topology-conf alsa-ucm-conf at-spi2-common at-spi2-core ca-certificates-java dconf-gsettings-backend*

*dconf-service fonts-dejavu-extra gsettings-desktop-schemas java-common libasound2-data libasound2t64*

*libatk-bridge2.0-0t64 libatk-wrapper-java libatk-wrapper-java-jni libatk1.0-0t64 libatspi2.0-0t64*

…

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

**root@ElasticSearch:~# java -version**

*openjdk version "11.0.23" 2024-04-16*

*OpenJDK Runtime Environment (build 11.0.23+9-post-Ubuntu-1ubuntu1)*

*OpenJDK 64-Bit Server VM (build 11.0.23+9-post-Ubuntu-1ubuntu1, 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:

**root@ElasticSearch:~# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -**

*Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).*

*OK*

Next, add the repository with the following command:

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

*deb https://artifacts.elastic.co/packages/7.x/apt stable main*

**root@ElasticSearch:~# ll /etc/apt/sources.list.d/**

**total 16**

*drwxr-xr-x 2 root root 4096 May 10 04:26 ./*

*drwxr-xr-x 8 root root 4096 May 10 04:25 ../*

*-rw-r--r-- 1 root root 62 May 10 04:26 elastic-7.x.list*

*-rw-r--r-- 1 root root 3036 May 10 04:14 ubuntu.sources*

root@ElasticSearch:~#

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

**root@ElasticSearch:~# apt-get update -y**

*Hit:1 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble InRelease*

*Hit:2 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease*

*Hit:3 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease*

*Get:4 https://artifacts.elastic.co/packages/7.x/apt stable InRelease [13.7 kB]*

*Hit:5 http://security.ubuntu.com/ubuntu noble-security InRelease*

*Get:6 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 Packages [131 kB]*

*Fetched 144 kB in 1s (176 kB/s)*

*Reading package lists... Done*

*W: https://artifacts.elastic.co/packages/7.x/apt/dists/stable/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details*.

**root@ElasticSearch:~# apt-get install elasticsearch -y**

*Reading package lists... Done*

*Building dependency tree... Done*

*Reading state information... Done*

*The following NEW packages will be installed:*

*elasticsearch*

…

**# Optional**

*Or we can download file .deb of ElasticSearch to install locally:*

***(****Refence link: https://www.cyberithub.com/how-to-install-elasticsearch-on-ubuntu-22-04-lts-jammy-jellyfish/)*

*wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.8.1-amd64.deb*

*sudo dpkg -i elasticsearch-8.8.1-amd64.deb*

We need to configure ElasticSearch Before start the service

**root@ElasticSearch:~# vi /etc/elasticsearch/elasticsearch.yml**

Other setting can be keep as default, set the feature xpack to false by add this line in the end of elasticsearch.yml:

*# Disable security features*

*xpack.security.enabled: false*

*network.host: 10.0.0.188 # This is local IP of your ElasticSearch server*

*http.port: 9200*

*discovery.type: single-node*

**root@ElasticSearch:~# cat /etc/elasticsearch/elasticsearch.yml | grep -E -v '^#|^$'**

*path.data: /var/lib/elasticsearch*

*path.logs: /var/log/elasticsearch*

*network.host: 10.0.0.188*

*http.port: 9200*

*discovery.type: single-node*

*xpack.security.enabled: false*

After edit the configure file, reload the daemon

**root@ElasticSearch:~# systemctl daemon-reload**

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

**root@ElasticSearch:~# systemctl start elasticsearch** *# wait a min for elasticsearch start the service.*

**root@ElasticSearch:~# systemctl enable elasticsearch.service**

*Synchronizing state of elasticsearch.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.*

*Executing: /usr/lib/systemd/systemd-sysv-install enable elasticsearch*

*Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /usr/lib/systemd/system/elasticsearch.service.*

**root@ElasticSearch:~# systemctl status elasticsearch**

● *elasticsearch.service - Elasticsearch*

*Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: enabled)*

*Active: active (running) since Fri 2024-05-10 06:25:44 UTC; 2min 39s ago*

*Docs: https://www.elastic.co*

*Main PID: 1139 (java)*

*Tasks: 60 (limit: 1078)*

*Memory: 629.6M (peak: 663.2M)*

*CPU: 1min 14.724s*

*CGroup: /system.slice/elasticsearch.service*

*├─1139 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cach>*

*└─1291 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86\_64/bin/contro>*

*May 10 06:25:12 ELK systemd[1]: Starting elasticsearch.service - Elasticsearch...*

*May 10 06:25:17 ELK systemd-entrypoint[1139]: May 10, 2024 6:25:17 AM sun.util.locale.provider.>*

*May 10 06:25:17 ELK systemd-entrypoint[1139]: WARNING: COMPAT locale provider will be removed i>*

*May 10 06:25:44 ELK systemd[1]: Started elasticsearch.service - Elasticsearch.*

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

**root@ElasticSearch:~# ss -antpl | grep 9200**

*LISTEN 0 4096 [::1]:9200 [::]:\* users:(("java",pid=1139,fd=295))*

*LISTEN 0 4096 [::ffff:127.0.0.1]:9200 \*:\* users:(("java",pid=1139,fd=296))*

root@ElasticSearch:~#

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

**root@elasticsearch:~# curl -X GET http://10.0.0.188:9200**

*{*

*"name" : "elasticsearch",*

*"cluster\_name" : "elasticsearch",*

*"cluster\_uuid" : "ywlbVyrpRoispeIfTgGCpQ",*

*"version" : {*

*"number" : "7.17.21",*

*"build\_flavor" : "default",*

*"build\_type" : "deb",*

*"build\_hash" : "d38e4b028f4a9784bb74de339ac1b877e2dbea6f",*

*"build\_date" : "2024-04-26T04:36:26.745220156Z",*

*"build\_snapshot" : false,*

*"lucene\_version" : "8.11.3",*

*"minimum\_wire\_compatibility\_version" : "6.8.0",*

*"minimum\_index\_compatibility\_version" : "6.0.0-beta1"*

*},*

*"tagline" : "You Know, for Search"*

*}*

*root@elasticsearch:~#*

## 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:

*#If install in different Sever, you need to install Java and add repository again, same as when your install ElasticSearch.*

*# apt install openjdk-11-jdk*

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

*# apt-get install apt-transport-https*

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

*# apt-get update*

*# apt-get upgrade -y*

**root@log-kibana:~# apt-get install logstash -y**

*Reading package lists... Done*

*Building dependency tree... Done*

*Reading state information... Done*

*The following NEW packages will be installed:*

*logstash*

*0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.*

*Need to get 367 MB of archives.*

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:

**root@log-kibana:~# vi /etc/logstash/conf.d/beats.conf**

**root@log-kibana:~# cat /etc/logstash/conf.d/ beats.conf**

*input {*

*beats {*

*port => 5044*

*}*

*}*

*filter {*

*# Put your log filter in here.*

*}*

*output {*

*if [@metadata][pipeline] {*

*elasticsearch {*

*hosts => ["10.0.0.188:9200"]*

*manage\_template => false*

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

*pipeline => "%{[@metadata][pipeline]}"*

*}*

*} else {*

*elasticsearch {*

*hosts => ["10.0.0.188:9200"]*

*manage\_template => false*

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

*}*

*}*

**root@log-kibana:~# sudo -u logstash /usr/share/logstash/bin/logstash --path.settings /etc/logstash -t**

*…..*

*[2024-05-17T08:06:23,336][INFO ][logstash.runner ] Using config.test\_and\_exit mode. Config Validation* ***Result: OK. Exiting Logstash***

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

**root@log-kibana:~# systemctl enable logstash.service**

*Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /etc/systemd/system/logstash.service.*

**root@log-kibana:~# systemctl start logstash.service**

**root@log-kibana:~# systemctl status logstash.service**

● *logstash.service - logstash*

*Loaded: loaded (/etc/systemd/system/logstash.service; enabled; preset: enabled)*

*Active: active (running) since Fri 2024-05-10 08:06:22 UTC; 13s ago*

*Main PID: 3650 (java)*

*Tasks: 15 (limit: 2274)*

*Memory: 328.0M (peak: 328.2M)*

*CPU: 25.591s*

*CGroup: /system.slice/logstash.service*

*└─3650 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:>*

*May 10 08:06:22 log-kibana systemd[1]: Started logstash.service - logstash.*

*May 10 08:06:22 log-kibana logstash[3650]: Using bundled JDK: /usr/share/logstash/jdk*

*May 10 08:06:22 log-kibana logstash[3650]: OpenJDK 64-Bit Server VM warning: Option UseConcMark>*

*lines 1-13/13 (END)*

## Install and Configure Kibana

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

**root@log-kibana:~# apt-get install kibana -y**

*Reading package lists... Done*

*Building dependency tree... Done*

*Reading state information... Done*

*The following NEW packages will be installed:*

*kibana*

*0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.*

*Need to get 304 MB of archives.*

Because Kibana is configured to only listen on localhost, we must set up a reverse proxy to allow external access to it, so we need to install nginx

**root@log-kibana:~# sudo apt install nginx -y**

*Reading package lists... Done*

*Building dependency tree... Done*

*Reading state information... Done*

*The following additional packages will be installed:*

*nginx-common*

*Suggested packages:*

*fcgiwrap nginx-doc ssl-cert*

*The following NEW packages will be installed:*

*nginx nginx-common*

Create an administrative Kibana user, the user name will be “kibanaadmin”, password: 123456, you can change username and password as your own.

***root@log-kibana:~# echo "kibanaadmin:`openssl passwd -apr1`" | sudo tee -a /etc/nginx/htpasswd.users***

*Password: 123456 # change to your password*

*Verifying - Password: 123456 # change to your password*

*kibanaadmin:$apr1$WzVdubNr$3ITIcO5x4bVAwnKFSeasI.*

*root@log-kibana:~#*

**root@log-kibana:~# vi /etc/nginx/sites-available/18.143.181.247**

**root@log-kibana:~# cat /etc/nginx/sites-available/18.143.181.247**

*server {*

*listen 80;*

*server\_name 18.143.181.247; # This is kibana public IP, you can change this to your kibana server name. But after that, you have to register it to hosts file in your laptop.*

*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;*

*}*

*}*

root@log-kibana:~#

**root@log-kibana:~# ln -s /etc/nginx/sites-available/18.143.181.247 /etc/nginx/sites-enabled/18.143.181.247**

**root@log-kibana:~# nginx -t**

*nginx: the configuration file /etc/nginx/nginx.conf syntax is ok*

*nginx: configuration file /etc/nginx/nginx.conf test is successful*

**root@log-kibana:~# sudo systemctl reload nginx**

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:

**root@log-kibana:~# vi /etc/kibana/kibana.yml**

**root@log-kibana:~#**

Change the following lines:

**root@log-kibana:~# cat /etc/kibana/kibana.yml | grep -E -v '^#|^$'**

*server.host: 0.0.0.0 # Allow remote user to connect to kibana*

*server.name: "* *Kibana-Log-Server"*

*elasticsearch.hosts: ["http://10.0.0.188:9200"]* #Change to your ElasticSearch server IP

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

**root@log-kibana:~# systemctl enable kibana.service**

*Synchronizing state of kibana.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.*

*Executing: /usr/lib/systemd/systemd-sysv-install enable kibana*

*Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /etc/systemd/system/kibana.service*.

**root@log-kibana:~# systemctl start kibana.service**

**root@log-kibana:~# systemctl status kibana.service**

*● kibana.service - Kibana*

*Loaded: loaded (/etc/systemd/system/kibana.service; enabled; preset: enabled)*

*Active: active (running) since Fri 2024-05-10 11:08:24 UTC; 5s ago*

*Docs: https://www.elastic.co*

*Main PID: 21501 (node)*

*Tasks: 7 (limit: 2274)*

*Memory: 142.0M (peak: 142.0M)*

*CPU: 3.391s*

*CGroup: /system.slice/kibana.service*

*└─21501 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/dist --loggin>*

*May 10 11:08:24 log-kibana systemd[1]: Started kibana.service - Kibana.*

*May 10 11:08:24 log-kibana kibana[21501]: Kibana is currently running with legacy OpenSSL providers enable>*

*lines 1-13/13 (END)*

## 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, remember to update the elastic repository:

**root@demo:~# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -**

*Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).*

*OK*

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

*deb https://artifacts.elastic.co/packages/7.x/apt stable main*

**root@demo:~# apt update**

*Hit:1 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble InRelease*

*Get:2 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [89.7 kB]*

*Get:3 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [89.7 kB]*

*Get:4 https://artifacts.elastic.co/packages/7.x/apt stable InRelease [13.7 kB]*

**root@demo:~# apt install filebeat -y**

*Reading package lists... Done*

*Building dependency tree... Done*

*Reading state information... Done*

*The following NEW packages will be installed:*

*filebeat*

*0 upgraded, 1 newly installed, 0 to remove and 8 not upgraded.*

*Need to get 36.9 MB of archives.*

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

root@demo:~# vi /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: ["http://10.0.0.117:5044 "] # Change to your logstash IP

Add the follow lines:

setup.kibana: # Find this line

host: "10.0.0.117:5601" # Add this line with your logstash IP

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

**root@demo:~# systemctl start filebeat  
root@demo:~# systemctl enable filebeat**

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

**root@demo:~# filebeat modules enable system**

*Enabled system*

**root@demo:~# filebeat modules list**

*Enabled:*

*system*

*Disabled:*

*activemq*

*apache*

*auditd*

*aws*

*awsfargate*

*azure*

*barracuda*

*bluecoat*

*…*

Next, load the index template with the following command:

**root@demo:~# filebeat setup --pipelines --modules system**

**root@demo:~# sudo filebeat setup --index-management -E output.logstash.enabled=false -E 'output.elasticsearch.hosts=["10.0.0.188:9200"]'**

*Overwriting ILM policy is disabled. Set `setup.ilm.overwrite: true` for enabling.*

*Index setup finished.*

**root@demo:~# sudo filebeat setup -E output.logstash.enabled=false -E output.elasticsearch.hosts=['10.0.0.188:9200'] -E setup.kibana.host=10.0.0.117:5601**

*Overwriting ILM policy is disabled. Set `setup.ilm.overwrite: true` for enabling.*

*Index setup finished.*

*Loading dashboards (Kibana must be running and reachable)*

*Loaded dashboards*

*Setting up ML using setup --machine-learning is going to be removed in 8.0.0. Please use the ML app instead.*

*See more: https://www.elastic.co/guide/en/machine-learning/current/index.html*

*It is not possble to load ML jobs into an Elasticsearch 8.0.0 or newer using the Beat.*

*Loaded machine learning job configurations*

*Loaded Ingest pipelines*

**root@demo:~# sudo systemctl restart filebeat**

**root@demo:~# sudo systemctl status filebeat**

*● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.*

*Loaded: loaded (/usr/lib/systemd/system/filebeat.service; enabled; preset: enabled)*

*Active: active (running) since Fri 2024-05-17 10:46:22 UTC; 7s ago*

*Docs: https://www.elastic.co/beats/filebeat*

*Main PID: 3593 (filebeat)*

*Tasks: 6 (limit: 1130)*

*Memory: 33.4M (peak: 37.5M)*

*CPU: 164ms*

*CGroup: /system.slice/filebeat.service*

*└─3593 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/filebeat.yml >*

*May 17 10:46:22 demo filebeat[3593]: 2024-05-17T10:46:22.736Z INFO [input] log/input>*

*May 17 10:46:22 demo filebeat[3593]: 2024-05-17T10:46:22.737Z INFO [input] log/input>*

*May 17 10:46:22 demo filebeat[3593]: 2024-05-17T10:46:22.737Z INFO cfgfile/reload.go:224 >*

*May 17 10:46:22 demo filebeat[3593]: 2024-05-17T10:46:22.738Z INFO [input.harvester] >*

*May 17 10:46:22 demo filebeat[3593]: 2024-05-17T10:46:22.739Z INFO [input.harvester]*

Verify that ElasticSearch is receiving data, the output should be similar as below:

**root@demo:~# curl -XGET 'http://10.0.0.188:9200/filebeat-\*/\_search?pretty'**

*{*

*"took" : 9,*

*"timed\_out" : false,*

*"\_shards" : {*

*"total" : 2,*

*"successful" : 2,*

*"skipped" : 0,*

*"failed" : 0*

*},*

*"hits" : {*

*"total" : {*

*"value" : 8186,*

*"relation" : "eq"*

*},*

*"max\_score" : 1.0,*

*"hits" : [*

*{*

*"\_index" : "filebeat-7.17.21-2024.05.17",*

*"\_type" : "\_doc",*

*"\_id" : "sLUpho8BshWLPdBmSTGH",*

*"\_score" : 1.0,*

*"\_source" : {*

*"agent" : {*

*"hostname" : "demo",*

*"name" : "demo",*

*"id" : "7e6d8129-b9c6-49c8-8527-c2a8e00921e9",*

*"ephemeral\_id" : "b6460e13-ee42-421d-8ce7-38c945cca1e5",*

*"type" : "filebeat",*

*"version" : "7.17.21"*

*},*

*"process" : {*

*"name" : "sudo"*

*},*

*"log" : {*

*"file" : {*

*"path" : "/var/log/auth.log"*

*},*

*"offset" : 12868*

*},*

*"fileset" : {*

*"name" : "auth"*

*},*

*"message" : "pam\_unix(sudo:session): session closed for user root",*

*"tags" : [*

*"beats\_input\_codec\_plain\_applied"*

*],*

*"cloud" : {*

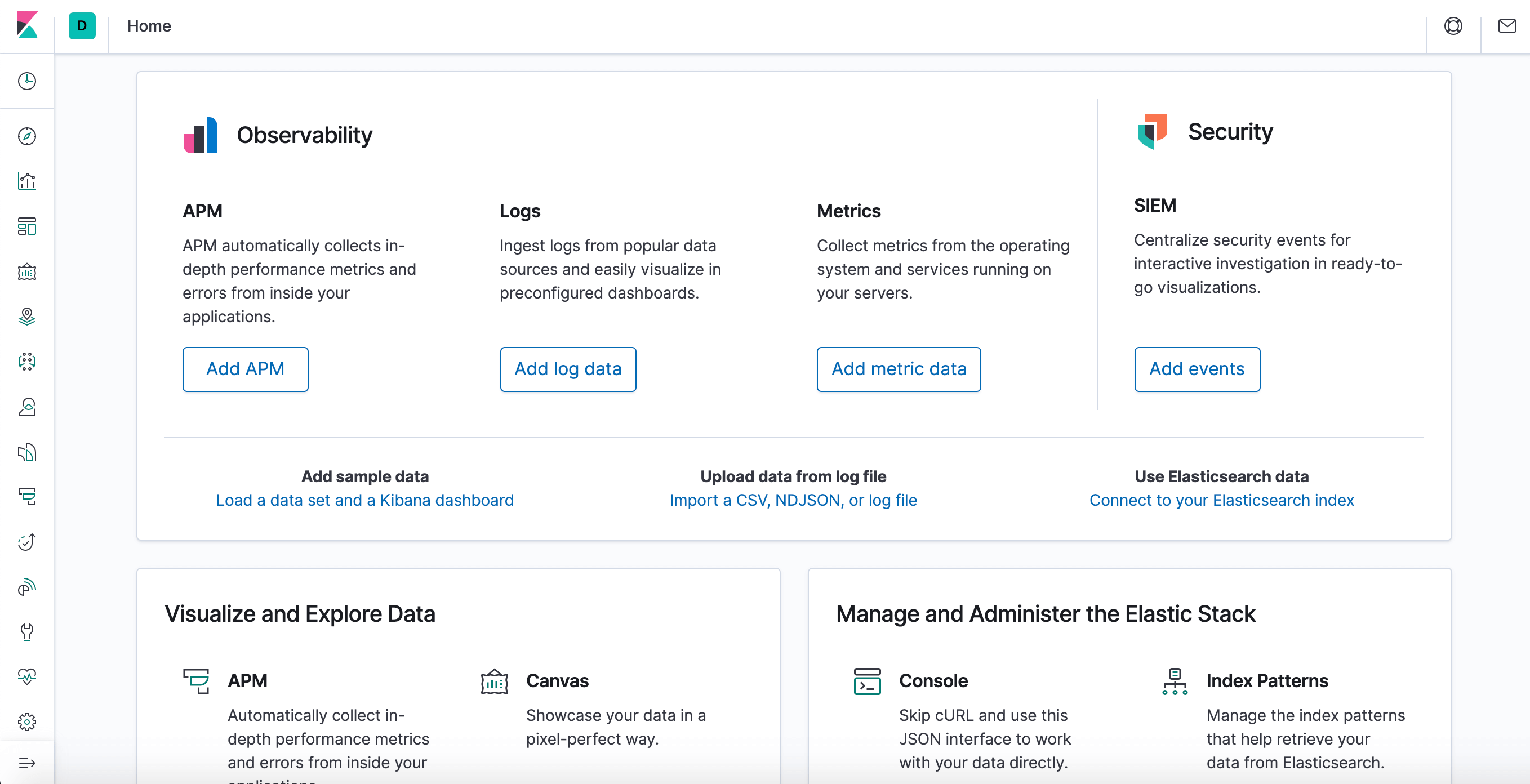
*"image" : {*

*"id" : "ami-003c463c8207b4dfa"*

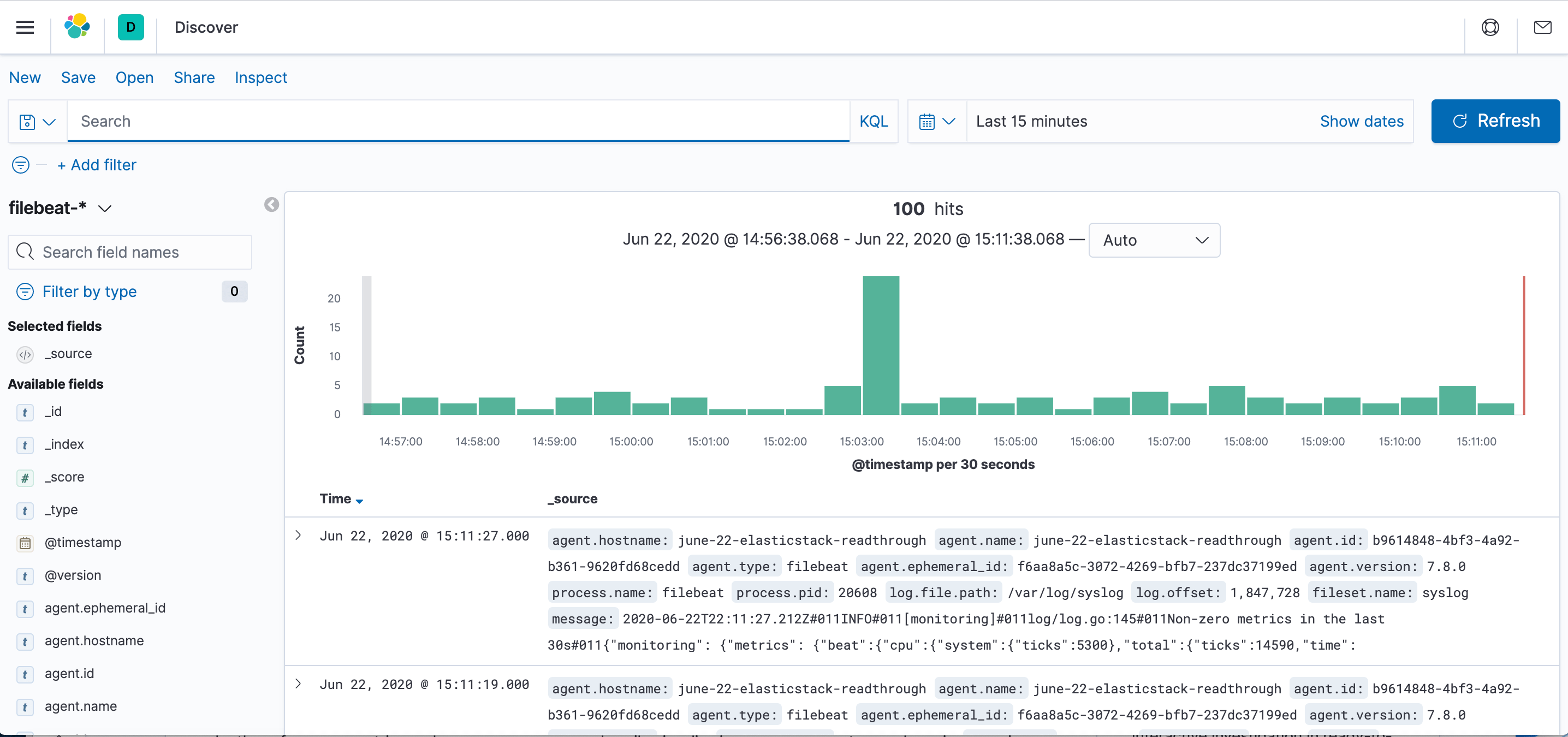
*…*

## 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:

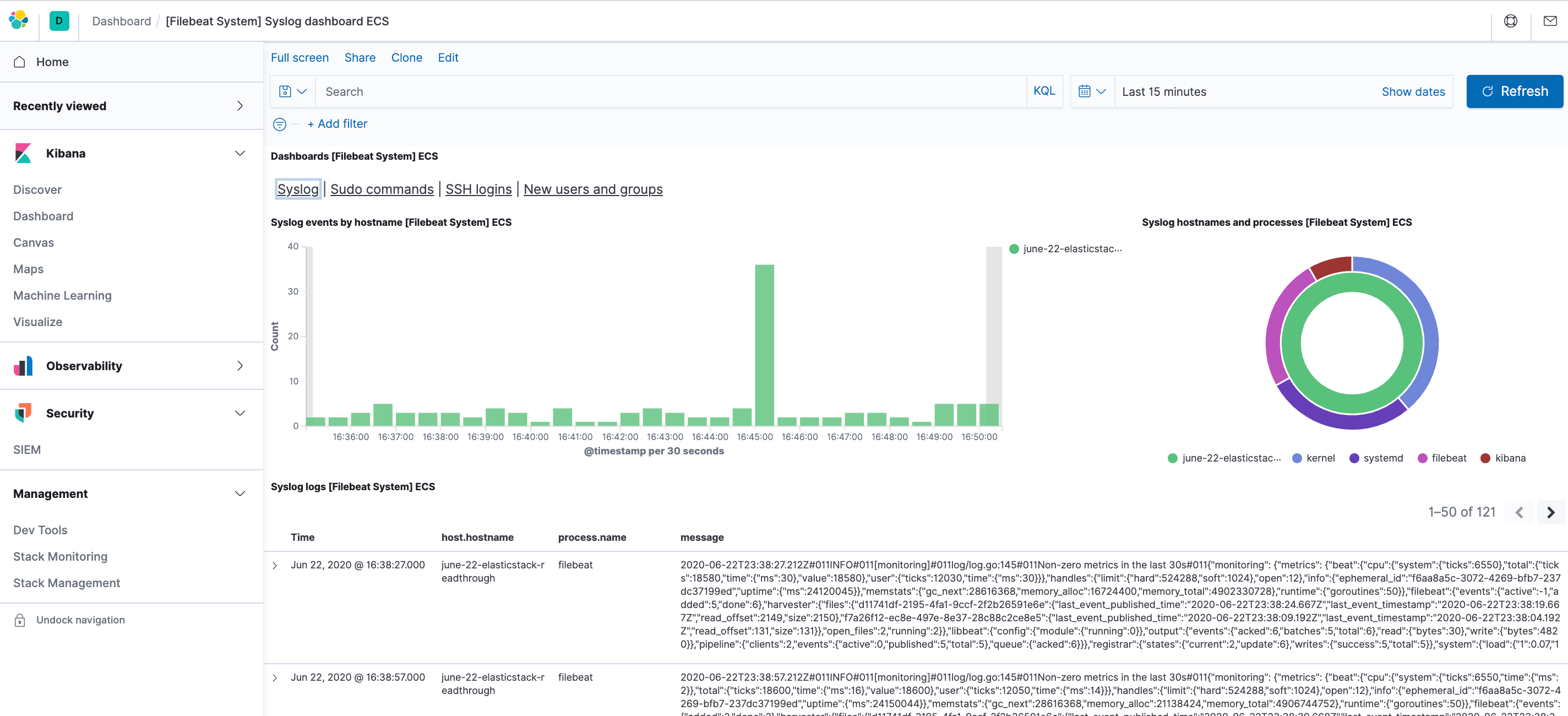


2. Now, click the Discover link in the left-hand navigation bar. You may have to click the Expand icon at the bottom left to see navigation menu items. Then, on the Discover page, select the predefined filebeat. By default, it will show you all of the log data over the last 15-minutes. Moreover, you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

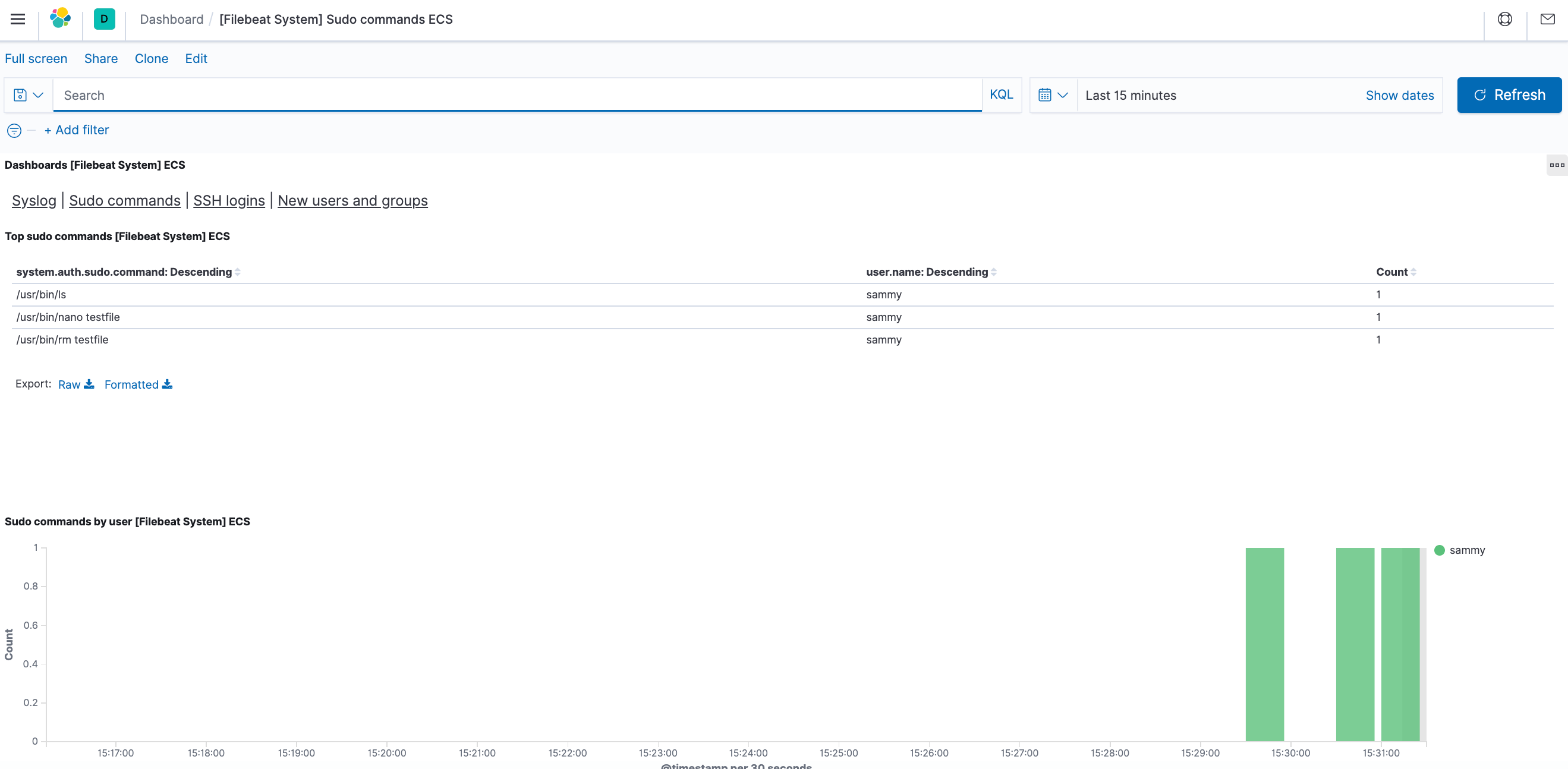


3. Here, you will search and browse via logs and even customize your dashboard. At this point, though, there will not be much in there as, here you are only gathering syslogs from Elastic Stack server.

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.