

# LAB 2 - Log and Infrastructure View

*Estimated Time for This Lab: 30 Min*

## Introduction

Now that we have workstation metrics and NGINX logs flowing into Elasticsearch, it's time to work with them. Elastic provides a powerful visualization layer (Kibana) to help accomplish this goal. This lab will look at two new visualizations introduced to Kibana in version 6.5.

### The Logs UI

You can use the Logs UI to explore logs for common servers, containers, and services. Kibana provides a compact, console-like display that you can customize. Key functionality:

- Use the power of Search -- The Search bar is always available. Use it to perform ad-hoc and structured searches.
- Jump to a specific time period -- Use the time selector to focus on a specific timeframe.
- Customize your view:
  - Use Customize to adjust your console view and to set the time scale of the log data.
  - Wrap long lines (Enable or disable line wrap).
  - Minimap Scale. Set the scale to year, month, week, day, hour, or minute.
- Stream or pause logs -- You can stream data for live logs tailing or pause streaming to focus on historical log data. When you are streaming logs, the most recent log appears at the bottom on the console. Historical data offers infinite scrolling.

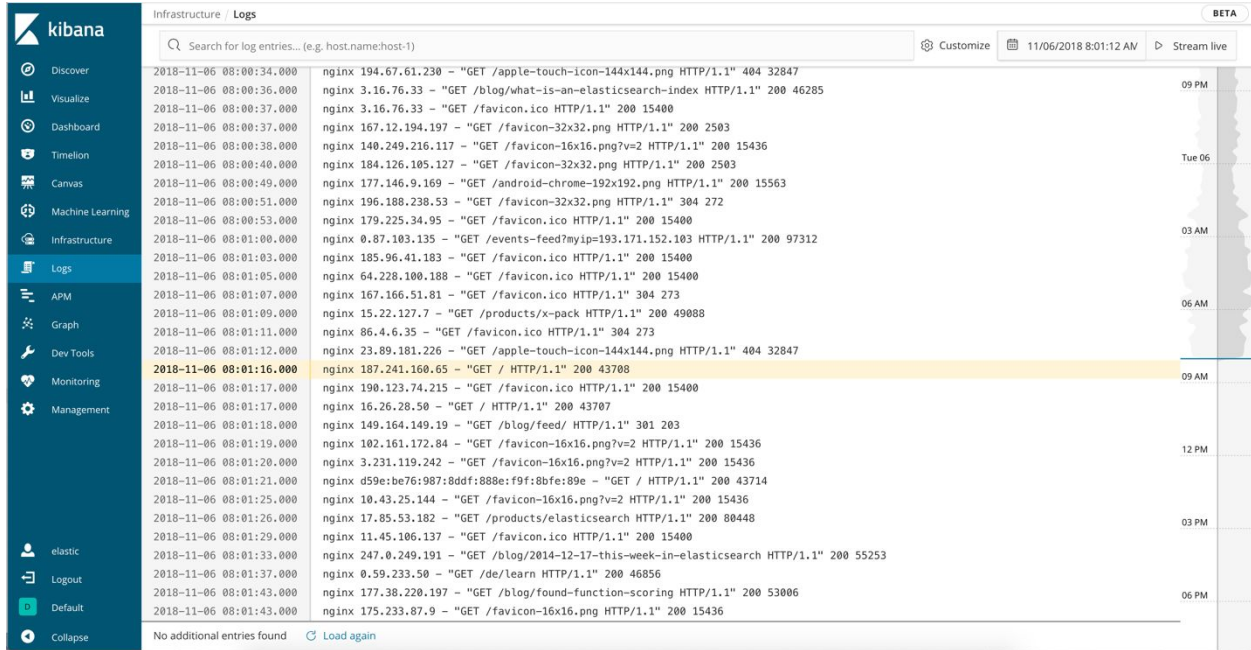
### The Infrastructure UI

Use the Infrastructure UI in Kibana to monitor your infrastructure and identify problems in real time.

- View your infrastructure by hosts or container -- Select the high-level view: Hosts, Kubernetes, or Docker. When you change views, you can see the same data through the perspective of a different category.
- Start at a high-level by selecting the metric -- This filter helps you start focusing on potential problem areas that may need further investigation. You'll see metrics that are most relevant for hosts or the container you selected.
- Group components -- The Group By selector offers grouping options that are native and specific for your physical, virtual, and container-based infrastructure. Examples include Availability Zone, Machine Type, Project ID, and Cloud Provider for Hosts, and Namespace and Node for Kubernetes.
- Auto-refresh or pause -- Set auto-refresh to keep up-to-date information coming in or stop refreshing to focus on historical data without new distractions.

Let's get started!

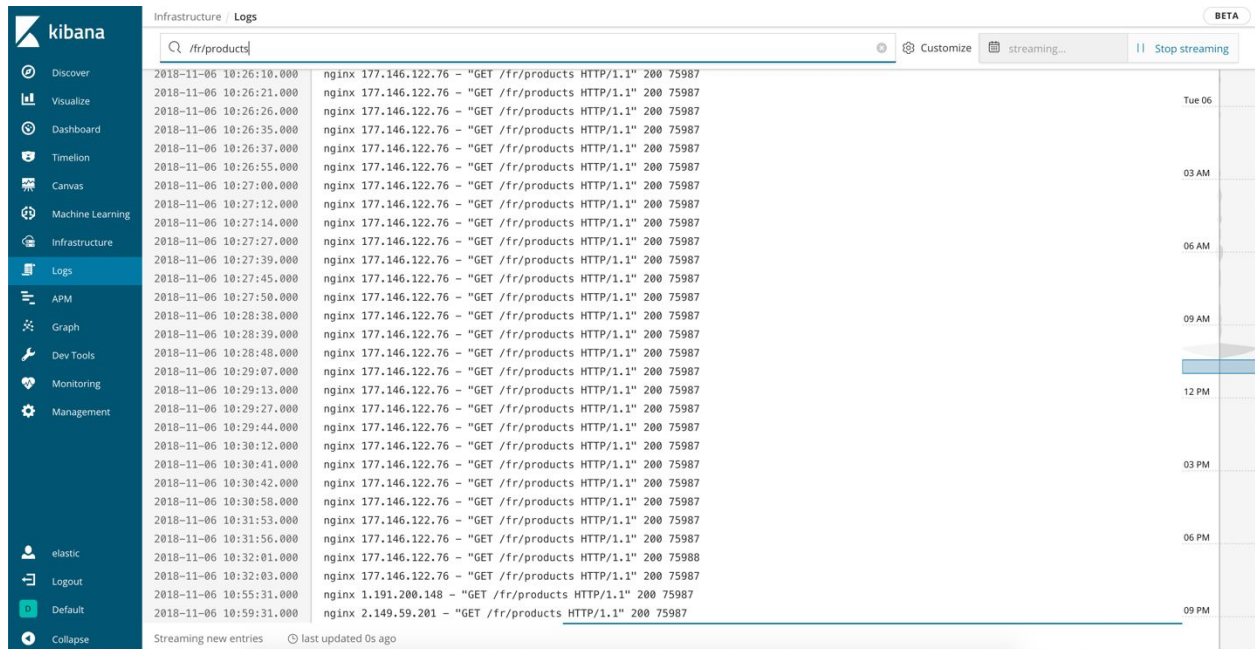
1. In Kibana click on “Logs” item in the menu. The data that you see below is coming from filebeat-\* indices.



The screenshot shows the Kibana Logs view. The left sidebar contains navigation links: Discover, Visualize, Dashboard, Timelion, Canvas, Machine Learning, Infrastructure, Logs (selected), APM, Graph, Dev Tools, Monitoring, and Management. The main content area displays a list of log entries. The search bar at the top contains the text "Search for log entries... (e.g. host.name:host-1)". The log entries are listed in a table with columns for timestamp, host, and log message. The 'Stream live' button is located in the top right corner.

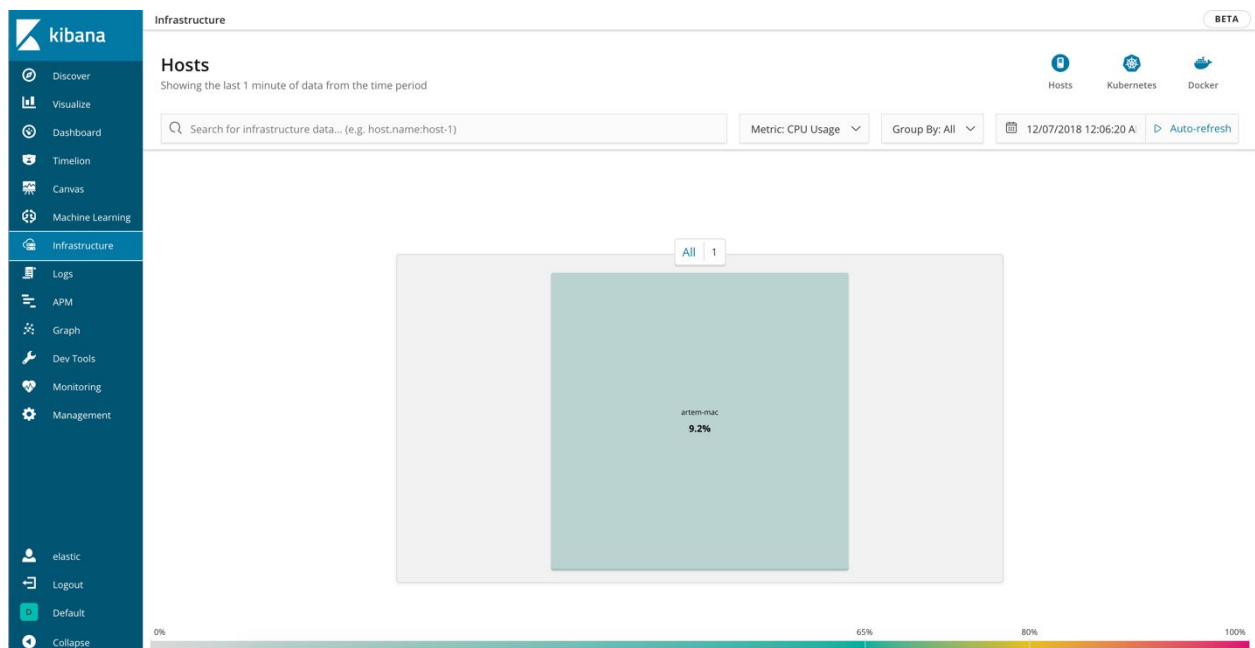
| Timestamp               | Host                                       | Log Message  |
|-------------------------|--|--|
| 2018-11-06 08:00:34.000 | nginx 194.67.61.230                        | - "GET /apple-touch-icon-144x144.png HTTP/1.1" 404 32847               |
| 2018-11-06 08:00:36.000 | nginx 3.16.76.33                           | - "GET /blog/what-is-an-elasticsearch-index HTTP/1.1" 200 46285        |
| 2018-11-06 08:00:37.000 | nginx 3.16.76.33                           | - "GET /favicon.ico HTTP/1.1" 200 15400                                |
| 2018-11-06 08:00:37.000 | nginx 167.12.194.197                       | - "GET /favicon-32x32.png HTTP/1.1" 200 2503                           |
| 2018-11-06 08:00:38.000 | nginx 140.249.216.117                      | - "GET /favicon-16x16.png?v=2 HTTP/1.1" 200 15436                      |
| 2018-11-06 08:00:40.000 | nginx 184.126.105.127                      | - "GET /favicon-32x32.png HTTP/1.1" 200 2503                           |
| 2018-11-06 08:00:49.000 | nginx 177.146.9.169                        | - "GET /android-chrome-192x192.png HTTP/1.1" 200 15563                 |
| 2018-11-06 08:00:51.000 | nginx 196.188.238.53                       | - "GET /favicon-32x32.png HTTP/1.1" 304 272                            |
| 2018-11-06 08:00:53.000 | nginx 179.225.34.95                        | - "GET /favicon.ico HTTP/1.1" 200 15400                                |
| 2018-11-06 08:01:00.000 | nginx 0.87.103.135                         | - "GET /events-feed?myip=193.171.152.103 HTTP/1.1" 200 97312           |
| 2018-11-06 08:01:03.000 | nginx 185.96.41.183                        | - "GET /favicon.ico HTTP/1.1" 200 15400                                |
| 2018-11-06 08:01:05.000 | nginx 64.228.100.188                       | - "GET /favicon.ico HTTP/1.1" 200 15400                                |
| 2018-11-06 08:01:07.000 | nginx 167.166.51.81                        | - "GET /favicon.ico HTTP/1.1" 304 273                                  |
| 2018-11-06 08:01:09.000 | nginx 15.22.127.7                          | - "GET /products/x-pack HTTP/1.1" 200 49088                            |
| 2018-11-06 08:01:11.000 | nginx 86.4.6.35                            | - "GET /favicon.ico HTTP/1.1" 304 273                                  |
| 2018-11-06 08:01:12.000 | nginx 23.89.181.226                        | - "GET /apple-touch-icon-144x144.png HTTP/1.1" 404 32847               |
| 2018-11-06 08:01:16.000 | nginx 187.241.160.65                       | - "GET / HTTP/1.1" 200 43708   |
| 2018-11-06 08:01:17.000 | nginx 190.123.74.215                       | - "GET /favicon.ico HTTP/1.1" 200 15400                                |
| 2018-11-06 08:01:17.000 | nginx 16.26.28.50                          | - "GET / HTTP/1.1" 200 43707   |
| 2018-11-06 08:01:18.000 | nginx 149.164.149.19                       | - "GET /blog/feed/ HTTP/1.1" 301 203                                   |
| 2018-11-06 08:01:19.000 | nginx 102.161.172.84                       | - "GET /favicon-16x16.png?v=2 HTTP/1.1" 200 15436                      |
| 2018-11-06 08:01:20.000 | nginx 3.231.119.242                        | - "GET /favicon-16x16.png?v=2 HTTP/1.1" 200 15436                      |
| 2018-11-06 08:01:21.000 | nginx d59e:be76:987:8ddf:888e:f9f:8bfe:89e | - "GET / HTTP/1.1" 200 43714   |
| 2018-11-06 08:01:25.000 | nginx 10.43.25.144                         | - "GET /favicon-16x16.png?v=2 HTTP/1.1" 200 15436                      |
| 2018-11-06 08:01:26.000 | nginx 17.85.53.182                         | - "GET /products/elasticsearch HTTP/1.1" 200 80448                     |
| 2018-11-06 08:01:29.000 | nginx 11.45.106.137                        | - "GET /favicon.ico HTTP/1.1" 200 15400                                |
| 2018-11-06 08:01:33.000 | nginx 247.0.249.191                        | - "GET /blog/2014-12-17-this-week-in-elasticsearch HTTP/1.1" 200 55253 |
| 2018-11-06 08:01:37.000 | nginx 0.59.233.50                          | - "GET /de/learn HTTP/1.1" 200 46856                                   |
| 2018-11-06 08:01:43.000 | nginx 177.38.220.197                       | - "GET /blog/found-function-scoring HTTP/1.1" 200 53006                |
| 2018-11-06 08:01:43.000 | nginx 175.233.87.9                         | - "GET /favicon-16x16.png HTTP/1.1" 200 15436                          |

2. In the top right corner click on “Stream live”. Notice how the screen starts to update as more logs flow into Elastic. This feature aims to simplify “tailing the log” experience.
3. In the search bar search for `"/fr/products"`. Make sure you include the double quotes.



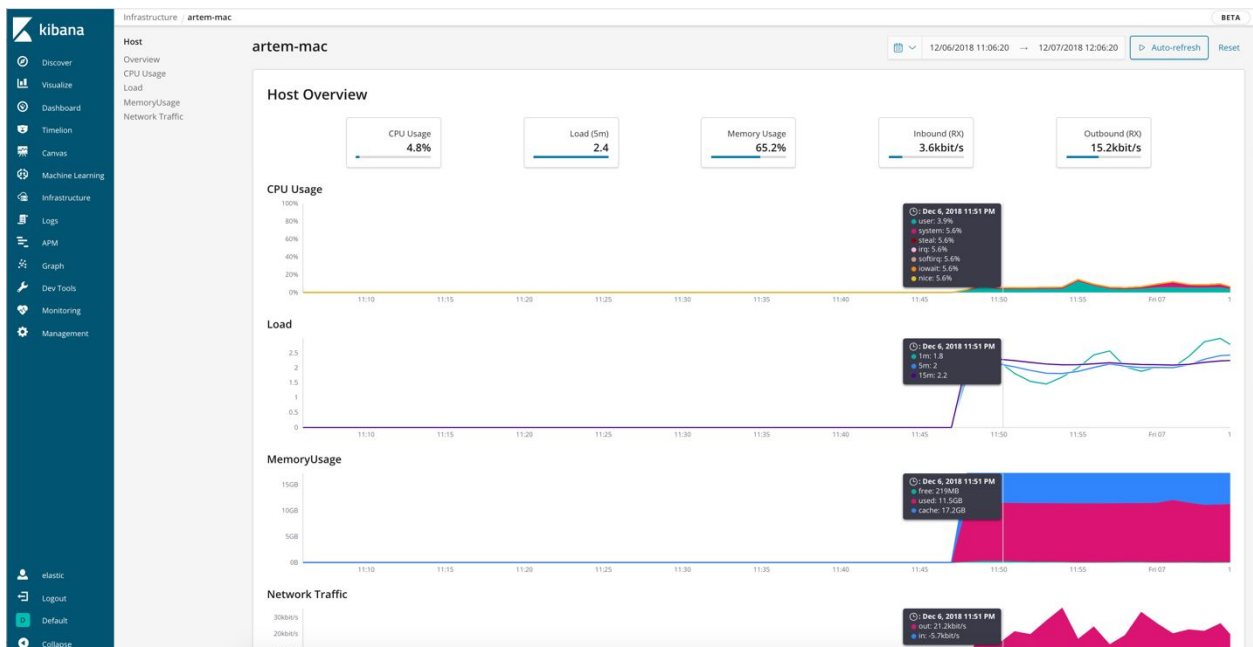
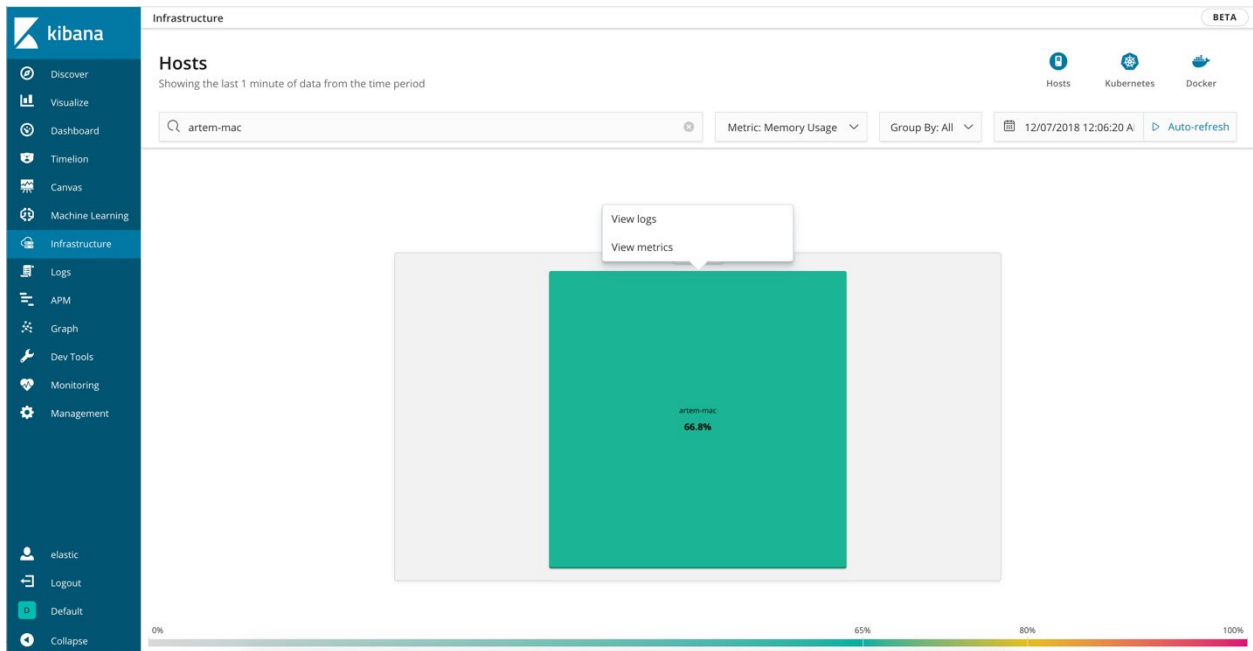
This functionality is powered by a search engine (Elasticsearch) and search features are still available to you.

4. Now click on the “Infrastructure” item in the menu.

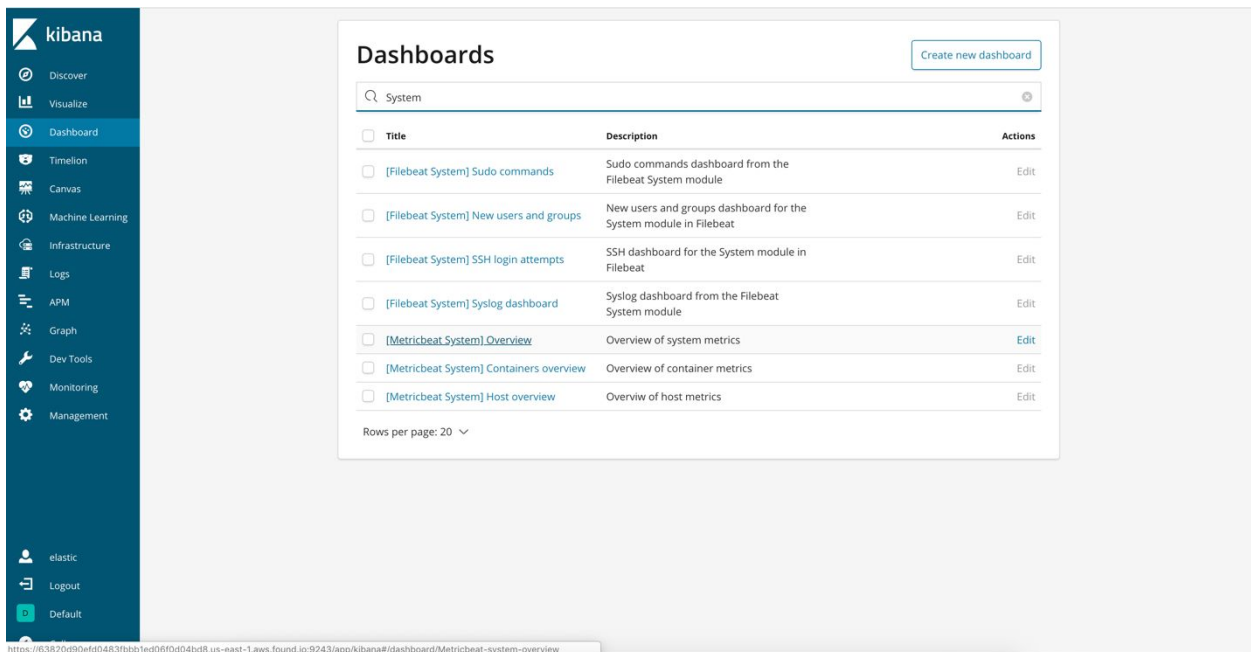


At the moment you see metrics only from one host, but imagine this same view (showcased in the presentation slides) where you have multiple hosts monitored here on one screen.

5. Current metric displayed is CPU Usage. Click on the dropdown and select Memory Usage, Load, and other metrics. Note – you might not have data for everything, but this will give you an idea of what kind of metrics could drive the display of the screen.
6. Click on the host and then click on “View Metrics”. You will end up on the quick summary metrics screen for the host.



7. Now let's take a look at the Dashboards that come OOB with Metricbeat and Filebeat. Click on Dashboards on the menu. A list with whole bunch of dashboards will display. Type in the search bar "System" and click on Host Overview. Make sure time picker in the top right corner is set for the "Last 15 min".



Dashboard / [Metricbeat System] Host overview

Full screen Share Clone Edit 30 seconds Last 15 minutes

Options Refresh

Add a filter

System Navigation [Metricbeat System]

System Overview | Host Overview | Containers overview

CPU Usage Gauge [Metricbeat System] 10.45%

Memory Usage Gauge [Metricbeat System] 65%

Load Gauge [Metricbeat System] 5m Load 2.33

Inbound Traffic [Metricbeat System] 8.593KB/s Total Transferred 20.416MB

Outbound Traffic [Metricbeat System] 56.726KB/s Total Transferred 30.107MB

In Packetloss 0 Out Packetloss 2,392

Swap usage [Metricbeat System] 76.5%

Memory usage vs total 10.395GB Total Memory 16GB

Number of processes [Metricbeat System] 24 Processes

Disk used [Metricbeat System] 0%

Disk Usage [Metricbeat System]

/private/var/vm 0%

/net 0%

/home 0%

/Volumes/Recovery 0%

/ 0%

CPU Usage [Metricbeat System]

System Load [Metricbeat System]

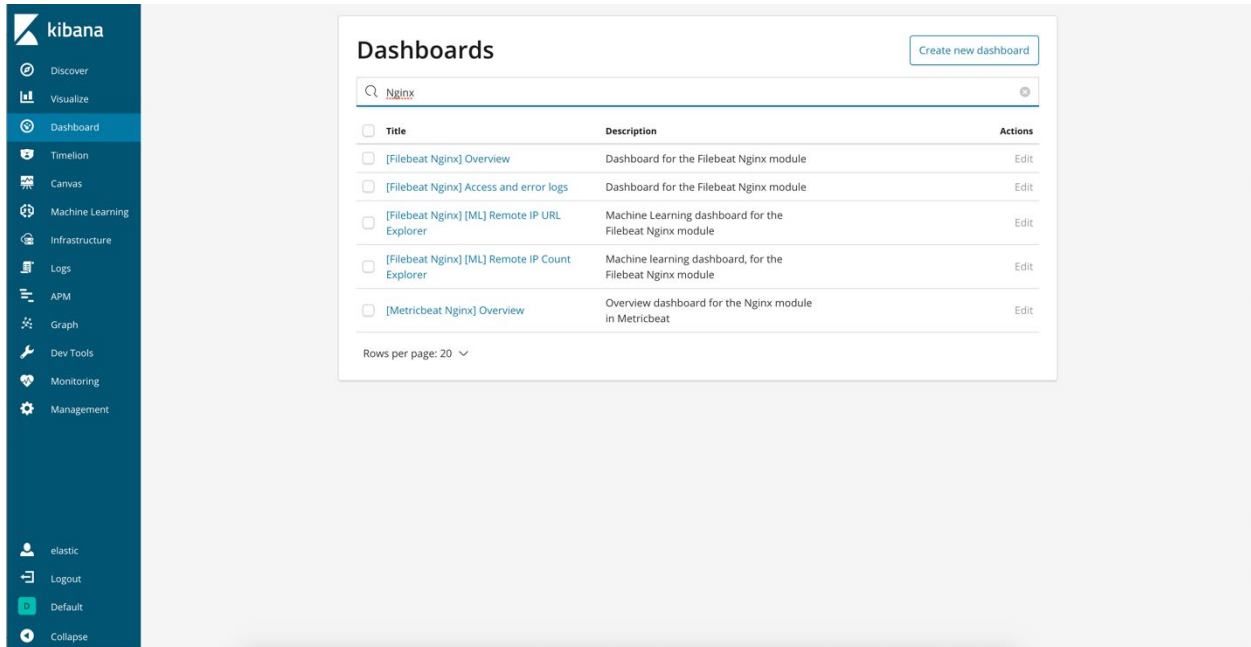
Legend: user 53.5%, system 30.1%, nice 0%, irq 0%, iofreq 0%, iowait 0%

System Load [Metricbeat System]

1m 2.49, 5m 2.33, 15m 2.27

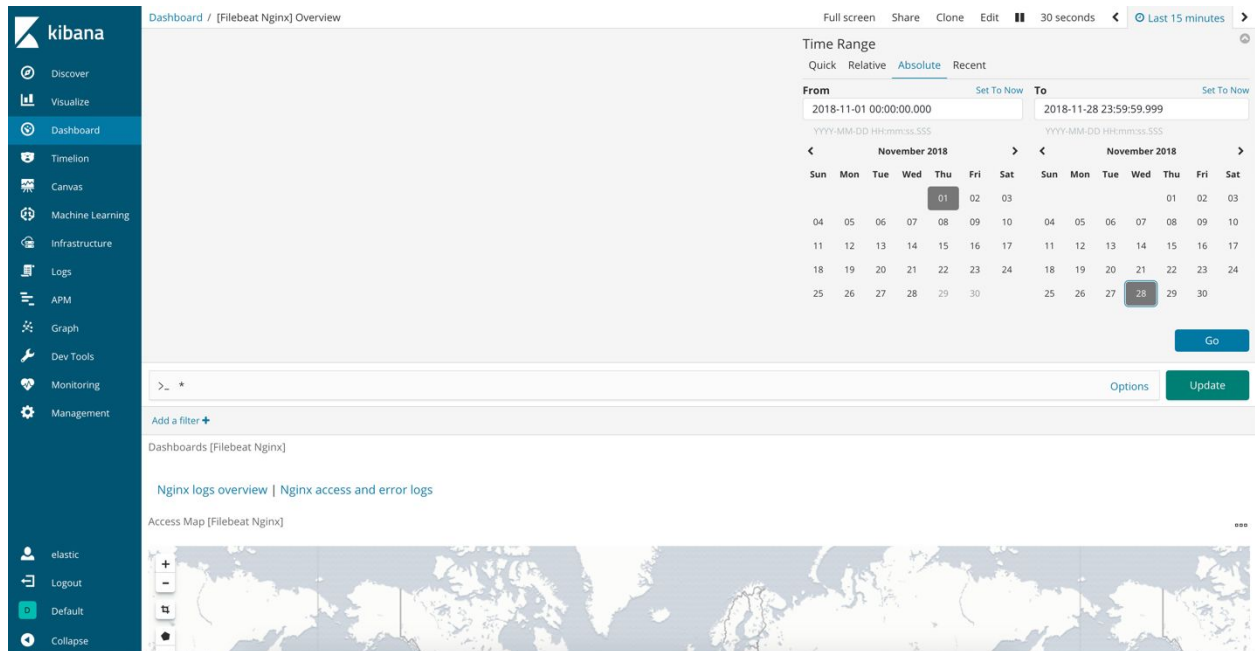
You end up on a dashboard that gives you complete metrics overview of the host where you have metricbeat running. Essentially with just running few commands you're now able to collect the metrics and have a graphic representation of your computer's performance. Imagine running this at scale and having that same real time view of 100s of hosts

8. Click on Dashboard again. This time search for "Nginx". Click on "Filebeat Nginx Overview" dashboard.

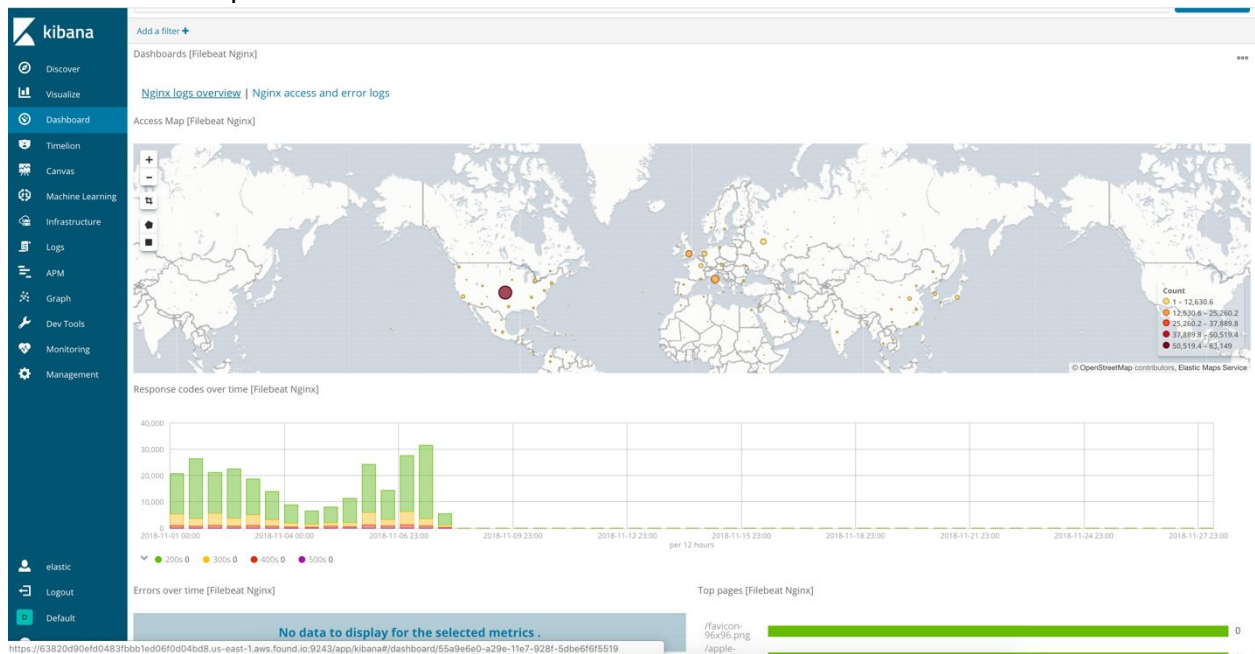


When the dashboard opens up in Date Picker select option "Absolute" and pick the dates between Nov 1<sup>st</sup> 2018 and Nov 28<sup>th</sup> 2018.



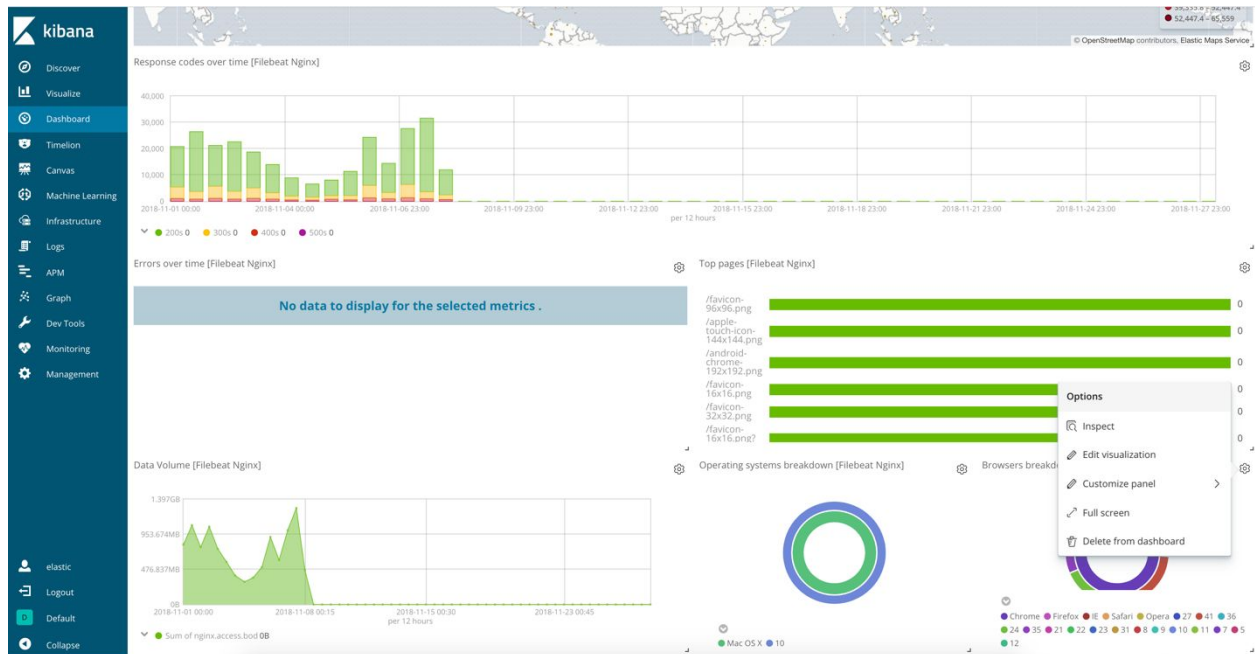


You end up on a dashboard that looks like this:



If you do not see the data all the way to November 28<sup>th</sup> it means it is still loading. Turn on Auto-Refresh (next to date picker) and see how your dashboards keeps updating in real time.

9. These dashboards are also a great example on how to build visualizations in Kibana. Feel free to click on “Edit” (next to Auto-Refresh option) and then edit a particular visualization to see how it was built.



Pie chart visualization:

