

How To Gather Infrastructure Metrics with Topbeat and ELK on Ubuntu 14.04

Posted Feb 1, 2016 3 20.5k [Logging](#) [Monitoring](#) [Elasticsearch](#) [Ubuntu](#)

Tutorial Series

This tutorial is part 2 of 5 in the series: [Centralized Logging with ELK Stack \(Elasticsearch, Logstash, and Kibana\) On Ubuntu 14.04](#)

Introduction

Topbeat, which is one of the several "Beats" data shippers that helps send various types of server data to an Elasticsearch instance, allows you to gather information about the CPU, memory, and process activity on your servers. When used with the ELK stack (Elasticsearch, Logstash, and Kibana), Topbeat can be used as an alternative to other system metrics visualization tools such as [Prometheus](#) or [Statsd](#).

In this tutorial, we will show you how to use an ELK stack to gather and visualize infrastructure metrics by using **Topbeat** on an Ubuntu 14.04 server.

Prerequisites

This tutorial assumes that you have the ELK Stack setup described in this tutorial: [How To Install Elasticsearch, Logstash, and Kibana on Ubuntu 14.04](#). If you do not already have an ELK server, please complete the linked tutorial before continuing.

We will also assume that, in addition to the ELK server, you have at least one client Ubuntu 14.04 server that you want to gather system metrics from by using Topbeat.

Load Kibana Dashboards on ELK Server

Note: This step is from the prerequisite tutorial but is also included here in case you skipped it while setting up your ELK stack. It is safe to load the sample dashboards multiple times.

Elastic provides several sample Kibana dashboards and Beats index patterns that can help you get started with Kibana. Although we won't use the dashboards in this tutorial, we'll load them anyway so we can use the Filebeat index pattern that it includes.

First, download the sample dashboards archive to your home directory:

- `cd ~`
- `curl -L -O https://download.elastic.co/beats/dashboards/beats-dashboards-1.1.0.zip`

Install the `unzip` package with this command:

- `sudo apt-get -y install unzip`

Next, extract the contents of the archive:

- `unzip beats-dashboards-*.zip`

And load the sample dashboards, visualizations and Beats index patterns into Elasticsearch with these commands:

- `cd beats-dashboards-*`
- `./load.sh`

These are the index patterns that we just loaded:

- `[packetbeat-]YYYY.MM.DD`
- `[topbeat-]YYYY.MM.DD`
- `[filebeat-]YYYY.MM.DD`
- `[winlogbeat-]YYYY.MM.DD`

Load Topbeat Index Template in Elasticsearch

Because we are planning on using Topbeat to ship logs to Elasticsearch, we should load the Topbeat index template. The index template will configure Elasticsearch to analyze incoming Topbeat fields in an intelligent way.

First, download the Topbeat index template to your home directory:

- `cd ~`
- `curl -O https://raw.githubusercontent.com/elastic/topbeat/master/etc/topbeat.template.`

Then load the template with this command:

- `curl -XPUT 'http://localhost:9200/_template/topbeat' -d@topbeat.template.json`

Now your ELK server is ready to accept data from Topbeat. Let's set up Topbeat on a client server next.

Set Up Topbeat (Add Client Servers)

Do these steps for each Ubuntu or Debian server that you want to send metrics data to Logstash on your ELK Server. For instructions on installing Topbeat on Red Hat-based Linux distributions (e.g. RHEL, CentOS, etc.), refer to the [CentOS variation of this tutorial](#).

Copy SSL Certificate

Note: This step is from the prerequisite tutorial but is also included here in case the client server you are setting up hasn't ever been connected to your ELK stack. You may skip this section if the client server already has the ELK server's SSL certificate in the appropriate place.

On your **ELK Server**, copy the SSL certificate—created in the prerequisite tutorial—to your **Client Server** (substitute the client server's address, and your own login):

- `scp /etc/pki/tls/certs/logstash-forwarder.crt user@client_server_private_address:/tmp`

After providing your login's credentials, ensure that the certificate copy was successful. It is required for communication between the client servers and the ELK Server.

Now, on your **Client Server**, copy the ELK Server's SSL certificate into the appropriate location (/etc/pki/tls/certs):

- `sudo mkdir -p /etc/pki/tls/certs`
- `sudo cp /tmp/logstash-forwarder.crt /etc/pki/tls/certs/`

Now we can install the Topbeat package.

Install Topbeat Package

On **Client Server**, ensure that the Beats source list exists.

Open `/etc/apt/sources.list.d/beats.list` for editing:

- `sudo vi /etc/apt/sources.list.d/beats.list`

Ensure that this line exists (paste it in if it isn't already present):

```
/etc/apt/sources.list.d/beats.list
```

- `deb https://packages.elastic.co/beats/apt stable main`

Save and exit.

Topbeat uses the same GPG key as Elasticsearch and Filebeat, which can be installed with this command:

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

Then install the Topbeat package:

- `sudo apt-get update`
- `sudo apt-get install topbeat`

Topbeat is now installed but not yet configured.

Configure Topbeat

Now we will configure Topbeat to connect to Logstash on our ELK Server. This section will step you through modifying the example configuration file that comes with Topbeat. When you complete the steps, you should have a file that looks something like [this](#).

On **Client Server**, create and edit Topbeat configuration file:

- `sudo vi /etc/topbeat/topbeat.yml`

Note: Topbeat's configuration file is in YAML format, which means that indentation is very important! Be sure to use the same number of spaces that are indicated in these instructions.

Near the top of the file, you will see the `input` section, which is where you can specify which metrics and statistics should be sent to the ELK server. We'll use the default input settings, but feel free to change it to fit your needs.

Under the `output` section, find the line that says `elasticsearch:`, which indicates the Elasticsearch output section (which we are not going to use). **Delete or comment out the entire Elasticsearch output section** (up to the line that says `#logstash:`).

Find the commented out Logstash output section, indicated by the line that says `#logstash:`, and uncomment it by deleting the preceding `#`. In this section, uncomment the `hosts: ["localhost:5044"]` line. Change `localhost` to the private IP address (or hostname, if you went with that option) of your ELK server:

topbeat.yml — 1 of 2

```
### Logstash as output
logstash:
  # The Logstash hosts
  hosts: ["ELK_server_private_IP:5044"]
```

This configures Topbeat to connect to Logstash on your ELK Server at port 5044 (the port that we specified a Logstash input for in the prerequisite tutorial).

Next, find the `tls` section, and uncomment it. Then uncomment the line that specifies `certificate_authorities`, and change its value to `["/etc/pki/tls/certs/logstash-forwarder.crt"]`. It should look something like this:

topbeat.yml — 2 of 2

```
...
tls:
  # List of root certificates for HTTPS server verifications
  certificate_authorities: ["/etc/pki/tls/certs/logstash-forwarder.crt"]
```

This configures Topbeat to use the SSL certificate that we created on the ELK Server in the prerequisite tutorial.

Save and quit.

Now restart Topbeat to put our changes into place:

- `sudo service topbeat restart`
- `sudo update-rc.d topbeat defaults 95 10`

Again, if you're not sure if your Topbeat configuration is correct, compare it against [this example Topbeat configuration](#).

Now Topbeat is sending your client server's system, processes, and filesystem metrics to your ELK server! Repeat this section for all of the other servers that you wish to Topbeat metrics for.

Test Topbeat Installation

If your ELK stack is setup properly, Topbeat (on your client server) should be shipping your logs to Logstash on your ELK server. Logstash should be loading the Topbeat data into Elasticsearch in an date-stamped index, `topbeat-YYYY.MM.DD`.

On your **ELK Server**, verify that Elasticsearch is indeed receiving the data by querying for the Topbeat index with this command:

- `curl -XGET 'http://localhost:9200/topbeat-*/_search?pretty'`

You should see a bunch of output that looks like this:

Sample Output:

```
{
  "_index" : "topbeat-2016.02.01",
  "_type" : "process",
  "_id" : "AVKeLSdP4HKUFv4CjZ7K",
  "_score" : 1.0,
  "_source": {"@timestamp": "2016-02-01T18:51:43.937Z", "beat": {"hostname": "topbeat-01",
}
```

If your output shows 0 total hits, Elasticsearch is not loading any Topbeat data under the

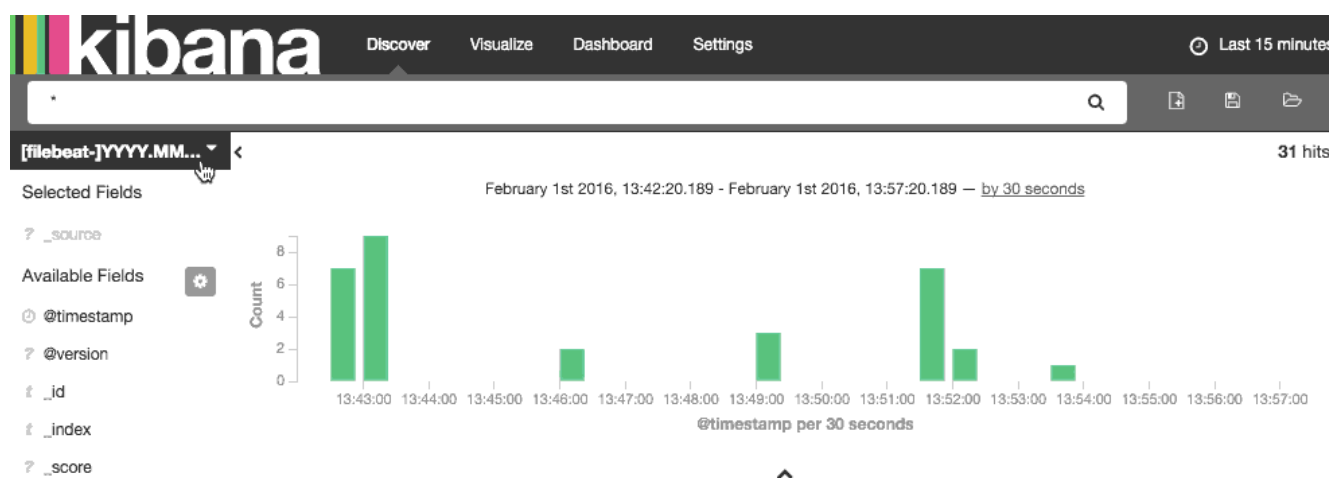
index you searched for, and you should review your setup for errors. If you received the expected output, continue to the next step.

Connect to Kibana

When you are finished setting up Topbeat on all of the servers that you want to gather system stats for, let's look at Kibana.

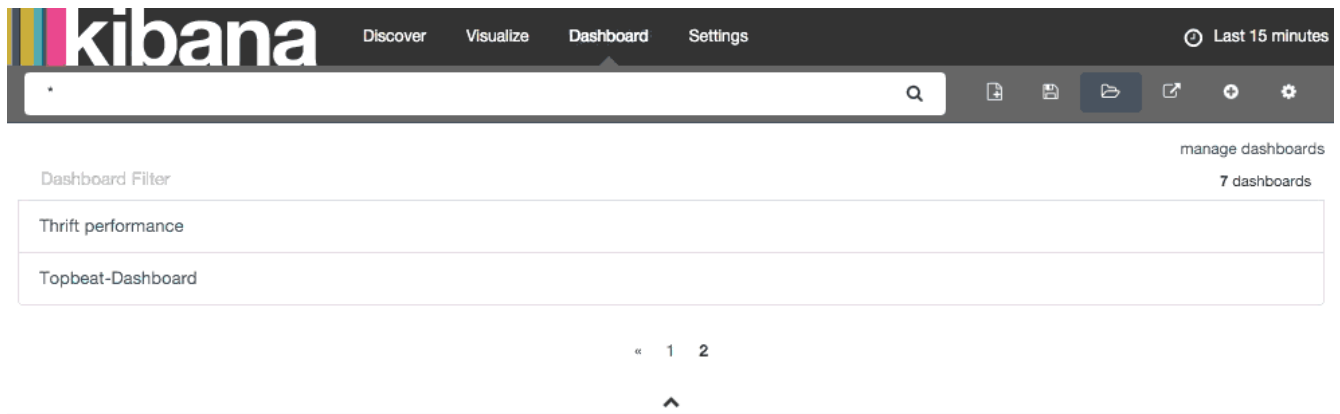
In a web browser, go to the FQDN or public IP address of your ELK Server. After entering your ELK server's credentials, you should see your Kibana Discover page.

Go ahead and select **[topbeat]-YYY.MM.DD** from the Index Patterns menu (left side) to view your Topbeat data in the Discover view:




Here, you can search and drill down your various Topbeat entries.

Next, you will want to check out the sample Topbeat dashboard that we loaded earlier. Click on **Dashboard** (top), then click the **Load Saved Dashboard** icon. Navigate to the second page of dashboards then click on **Topbeat-Dashboard**:



Ready to get started?

Click the  button in the menu bar above to add a visualization to the dashboard.
If you haven't setup a visualization yet visit the "Visualize" tab to create your first visualization.

Here, you will see a variety of metrics that were gathered from your client servers that you installed Topbeat on.

Conclusion

Now that your system metrics are centralized via Elasticsearch and Logstash, and you are able to visualize them with Kibana, you should be able to see what your servers are up to at a glance. Good luck!