logz.io

#ELK Installation   #Google Cloud Platform (GCP)   #Tutorials

How to Install the ELK Stack on Google Cloud Platform

PJ Hagerty

Trying to find the right cloud provider can be difficult, even when you are looking at it for your log and analytics needs. Here at Logz.io, we use the ELK Stack to monitor our cloud infrastructure as well as offer the log analytics platform as an AI-powered and enterprise-grade cloud service. So, we are

Forrester Obs

logz.io

This post is just a proof of concept, but Google Cloud offers a $300 credit for trial users that should be more than enough to deploy an application, get the ELK Stack set up, and prove that it will cover your needs should you want to move forward with Google Cloud.

Logistical Setup

First, you'll need to set up a Google Cloud Platform account. This is relatively straightforward. Fill out the forms, and you will have your $300/360 Free Trial setup. Setting up your application is easy, it just requires getting the Gcloud SDK setup for CLI deployment.

For this example, we will use a simple ToDo application — the code can be found here. Since the application isn't the focus here, we can deploy it and hit it a couple of times to ensure that there are some logs to export once we reach this step. The assumption here is that your application will be much more robust and in need of log management.

More on the subject:

Creating Custom Kibana Visualizations

Introducing On-Demand Logging with Logz.io Drop Filters

10 Ways to Simplify Cloud Monitoring
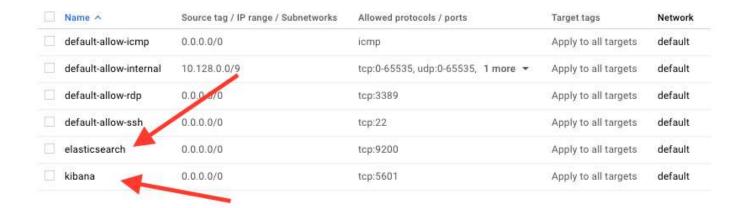
Getting Started with ELK Setup

We'll add Elasticsearch and Kibana with the IP range set to 0.0.0.0/0 and TCP protocols set to 9200 for Elasticsearch and 5601 for Kibana. (Note: Both are all lowercase as the method prescribed by the Google Cloud Firewall Rules interface.) They should appear in the firewall list as follows:

Name ^	Source tag / IP range / Subnetworks	Allowed protocols / ports	Target tags	Network
default-allow-icmp	0.0.0.0/0	icmp	Apply to all targets	default
default-allow-internal	10.128.0.0/9	tcp:0-65535, udp:0-65535, 1 more ▾	Apply to all targets	default
default-allow-rdp	0.0.0.0/0	tcp:3389	Apply to all targets	default
default-allow-ssh	0.0.0.0/0	tcp:22	Apply to all targets	default
elasticsearch	0.0.0.0/0	tcp:9200	Apply to all targets	default
kibana	0.0.0.0/0	tcp:5601	Apply to all targets	default

Now, you can begin to set up the actual ELK Stack. The first step is to set up an instance in Google Cloud Platform. Once the instance is set up, you can SSH into it using the following command:

```
$ gcloud compute ssh #{instancename}
```

(This assumes that you have gone through the steps with the CLI to establish a connection.)

logz.io

Install Java

Java installation is simple and straightforward. If you have experience with the programming language, you know to use the following command to make sure that you have the latest, stable version of Java on the instance:

```
$ sudo apt-get install default-jre


# Installs java and ensures we are using an up to date version. ELK
stack requires version 1.8+
```

Install Elasticsearch

```
$ wget -qO - https://packages.elastic.co/GPG-KEY-elasticsearch | sudo
apt-key add -
# This will fetch the latest ElasticSearch Version for us


$ sudo apt-get install elasticsearch
# This will complete the installation
```

You will need to adjust the configuration of Elasticsearch so that you can ensure that the network host is correct. To do so, edit the *elasticsearch.yml* file:

```
$ sudo vi /etc/elasticsearch/elasticsearch.yml
```

logz.io

Install Logstash

Your next step is to install Logstash. To do so, use the following commands:

```
$ sudo apt-get install apt-transport-https
# This setups installs for logstash in your system


$ echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main"
| sudo tee -a /etc/apt/sources.list.d/elastic-5.x.list
# This will establish the source for Logstash


$ sudo apt-get update
$ sudo apt-get install logstash
# Setting up for Logstash installation


$ sudo service logstash start
# Start the logstash service so we can start shipping logs
```

Install Kibana

Finally, do the same for the Kibana service so that you will get nice visualizations on your logs:

logz.io   ≡

```
$ sudo apt-get update
$ sudo apt-get install kibana
# Setting up for Kibana installation
```

Similar to Elasticsearch, Kibana will need some configuration adjustments to work. Take a look at *kibana.yml* to make these changes:

```
$ sudo vi /etc/kibana/kibana.yml
```

Find the lines referring to *server.port* and ensure they say *server.port: 5601* and *server.host: "0.0.0.0"*. It should only be necessary to uncomment these lines. It may also be necessary to adjust the SSL verify line *elasticsearch.ssl.verificationMode: none* if you are seeing problems once everything is up and running.

Once this is done, you can start the Kibana service:

```
$ sudo service kibana start
```

Success! Well… Mostly

If everything works as planned, you should be able to use the server's IP with port 5601 specified to see if your setup was successful:

logz.io

You've come a long way and things are looking up, but you still need to pipe in some logs. For this example, we are going to install MetricBeat to snag system metrics. The installation steps are as follows:

logz.io

```
$ sudo service metricbeat start
```

Once MetricBeat is up and running, set it as an index pattern in the Kibana management screen as *metricbeat-**. This will begin the shipping of logs, and you will have your ELK Stack set up:

logz.io

Observability at scale, powered by open source

See Plans

YOU MIGHT ALSO LIKE

News

logz.io

Join us at ScaleUP, the Logz.io User Conference for Monitoring & Observability

News

logz.io

Finding the Bug in the Haystack with Machine Learning: Logz.io Exceptions in Kibana

DevOps

Reducing Supply Chain Attack Surface through SaaS

← Back to Blog

Forrester Obs

logz.io

just plain wrong! Especially considering the latest trend of blackmail targeting systems (e.g. MongoDB & ElasticSearch) still using authentication defaults.

- *Patrick J. Hagerty* says:
  [April 3, 2017 at 3:21 pm](#)

  Hey Nicolas – we covered that a bit in this post: https://logz.io/blog/securing-elasticsearch-clusters/

  For this post, we wanted to keep in the scope of introducing new ELK stackers with the specifics on how-to install the stack. As such, security was outside the scope of this particular piece. We'd also like folks to know we make this issue easier by ensuring the security of anyone using Logz.io for their logging needs.

  If you might be interested in writing up a piece on ELK stack security, please let us know!

  - [*Nicolas Frankel*](#) says:
    [April 3, 2017 at 3:32 pm](#)

    1. Cool that it's mentioned in an unrelated post. It's also mentioned all around the Internet. It doesn't change the fact that you don't mention it.
    2. Thanks for your kind proposal. That's an idea, but I've already a lot to write about – besides, I've my own blog and don't need a platform.

2. *Saviour Gidi* says:
   [June 5, 2017 at 7:51 pm](#)

   Its not accesible from outside. But with curl internal on the 0.0.0.0:5601, its running alright.

   - [*PJ Hagerty*](#) says:
     [June 5, 2017 at 8:51 pm](#)

     Good to know – did you find this was the case with ELK stack 5.3 or a different version?

3. *JB* says:
   [July 5, 2017 at 7:34 am](#)

   PJ, I followed these instructions but I get a red status when I launch Kibana using the

logz.io

Alsp, which version of ELK stack are you installing? This article was looking at 5.1.0, but some things may have changed since then.

- *JB* says:
  July 6, 2017 at 2:16 am

  PJ, thanks for the response! I also used your firewall specifications. Doesn't hang this code ensure the latest version is used?

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

  I just checked the website, and the version available now is 5.4.3. Would it be possible to use your same tutorial and change the code above to specify version 5.1.0?

  - *PJ Hagerty* says:
    July 6, 2017 at 4:00 pm

    Hey JB – I'm not sure if that will resolve the error, but as that is the version I used, it may help.

    Did you also make sure to adjust the SSL verification line elasticsearch.ssl.verificationMode: none in the kibana.yml?

    - *JB* says:
      July 6, 2017 at 6:56 pm

      PJ, yes, I adjusted the SSL verification line. Do you have a suggestion for how to change that code for the elastic install that would use version 5.1.0? Or do you think I should try something else to get it to work with then new version? It seems like Kibana is working fine, but Elastic is trying to call to the localhost instead of the server. Thanks for any help you can offer!

      - *PJ Hagerty* says:
        July 7, 2017 at 3:43 pm

        JB – this seems like an interesting problem. I'm trying to figure it out

logz.io

July 19, 2017 at 6:52 pm

Hey JB – I looked into it and it may have something to do with the version of Java setup by default. Are you sure you have Java 1.8? I was looking through my notes and I found a similar problem when I ran sudo apt-get install default-jre and it installed a previous version. Can you check that out an let me know?

- *JB* says:
  July 19, 2017 at 10:41 pm

  PJ, I just checked the version and it is 1.8.0_131, so that shouldn't be the problem. Are you having the same issue when you try install with the new version of ELK?

- *PJ Hagerty* says:
  July 20, 2017 at 5:43 pm

  Hey JB,

  I'm trying things out now with 5.5 and I seem to be having the same issue. Once I get it resolved, I'll let you know what the answer was.

- *JB* says:
  July 20, 2017 at 10:08 pm

  Thanks, PJ!! I really appreciate you troubleshooting this issue!

- *JB* says:
  July 13, 2017 at 8:41 pm

  PJ, thanks again for looking into this. I was just curious if you had any success or insight into the issues with the new version of elastic/kibana.

- *Daniel Berman* says:
  July 16, 2017 at 9:45 am

  Hi JB – no updates on this yet. Did you try installing the latest version of the stack (5.5)? As soon as we have news, we'll update the post.

  JB says:

This website uses cookies. By continuing to browse this site, you agree to this use. **Learn more.**

Okay, thanks

Privacy Policy

Terms Of Use

Trademarks Legal Notice

Logz.io SLA