**Getting Started with ELK Stack**

*(A Hello World)*

# **Downloading the ELK**

1. Head over to [elastic.co/downloads](https://www.elastic.co/downloads) and download ELK (ElasticSearch, Logstash and Kibana).

For reference, following URLs are used in this document for windows environment:

* ElasticSearch: [elasticsearch-6.5.1.zip](https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.5.1.zip)
* Logstash: [logstash-6.5.1.zip](https://artifacts.elastic.co/downloads/logstash/logstash-6.5.1.zip)
* Kibana: [kibana-6.5.1-windows-x86\_64.zip](https://artifacts.elastic.co/downloads/kibana/kibana-6.5.1-windows-x86_64.zip)

1. Unzip the packages and we’re good to go.

# **Setting up the ELK**

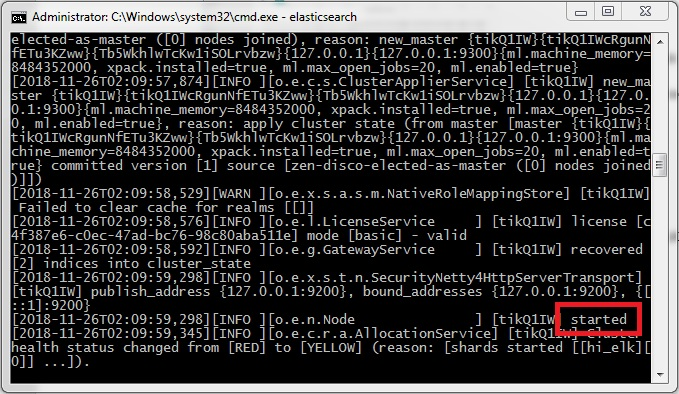
## **ElasticSearch Setup:**

1. Open command prompt in “elasticsearch-6.5.1\bin” and execute command:



Note: Make sure Java path is set in environment variables.

1. After getting “started” message, we can proceed to next step.



## **Logstash Setup:**

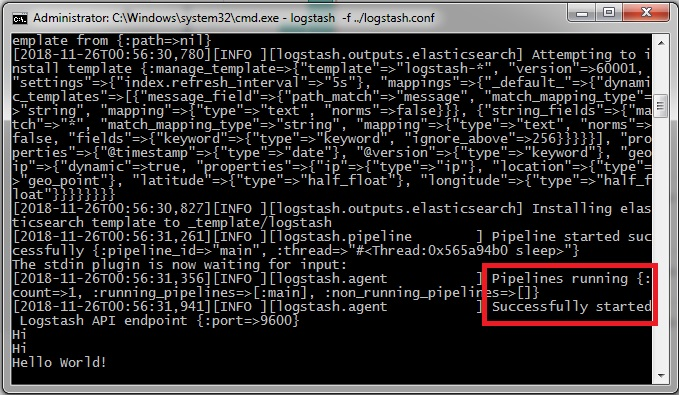
1. Create a file named “logstash.conf” inside directory “logstash-6.5.1” with contents:



1. Open command prompt in “logstash-6.5.1\bin” directory and execute command:



1. After getting “pipelines running” or “Successfully started API Endpoint” message, we can proceed to next step. Hereafter, this window will be referred as “**Logstash Console**”. Write any message here and hit Enter. Get ready to see your message in Kibana!



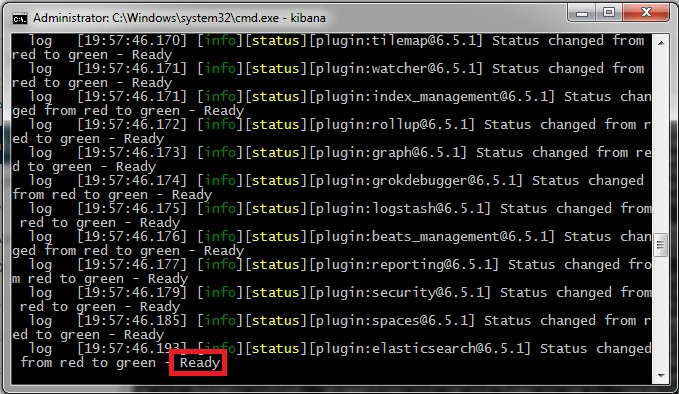
## **Kibana Setup:**

1. Open command prompt in “kibana-6.5.1-windows-x86\_64\bin” and execute command:

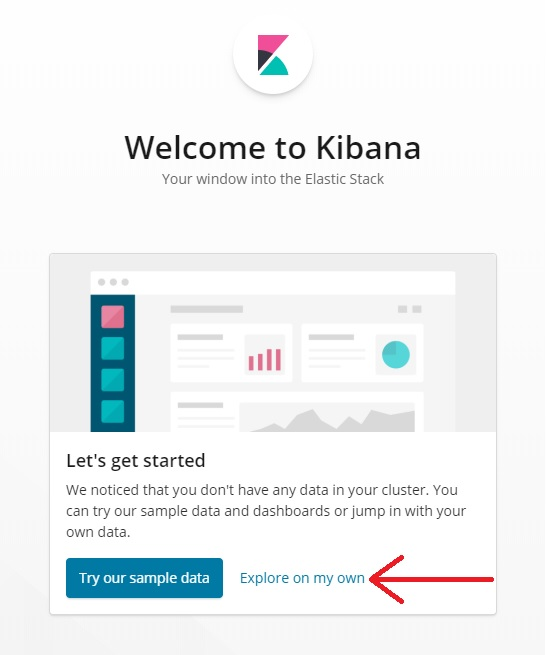


Note: Make sure Java path is set in environment variables.

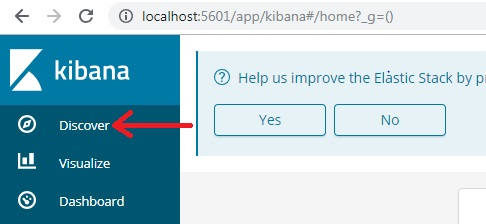
1. After getting “Ready” message, we can proceed to next step.



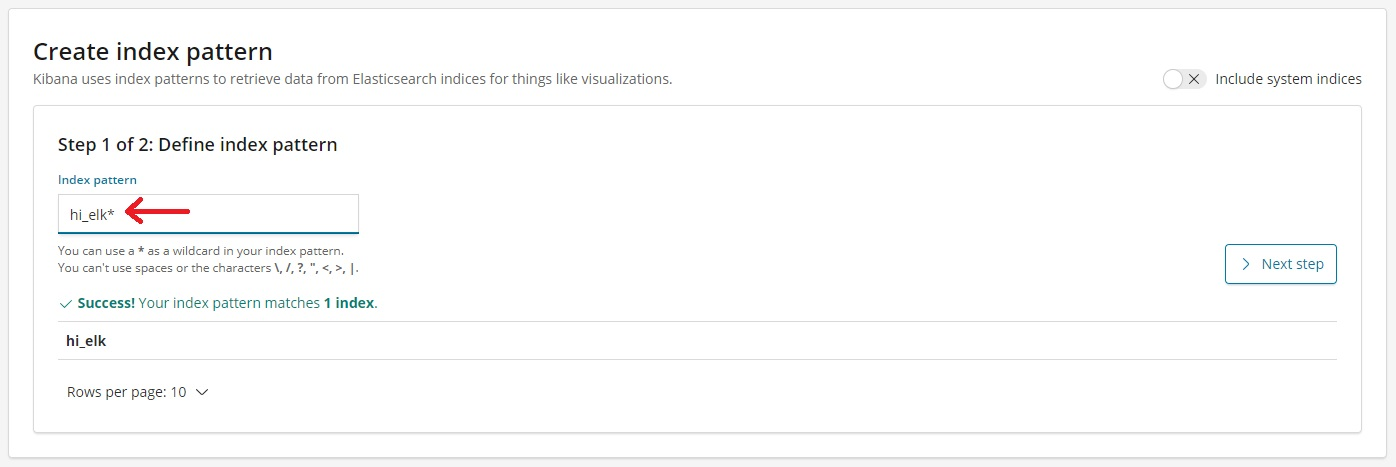
1. Open localhost:5601 in browser.
2. If Kibana Welcome Screen shows up, select “Explore on my own”.



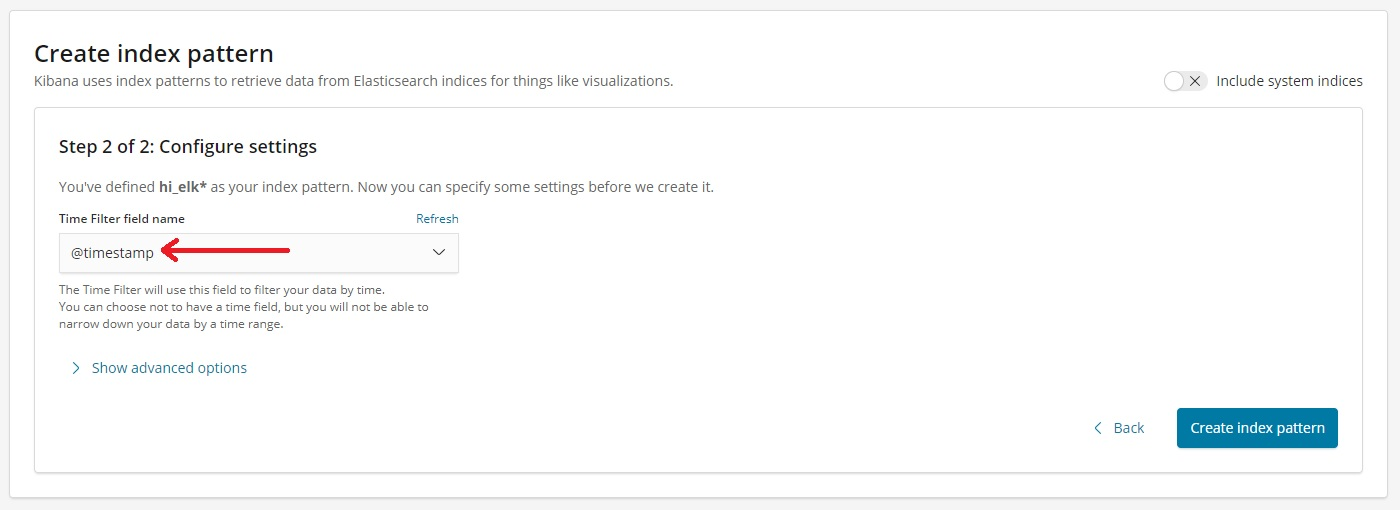
1. Head over to “Discover”.



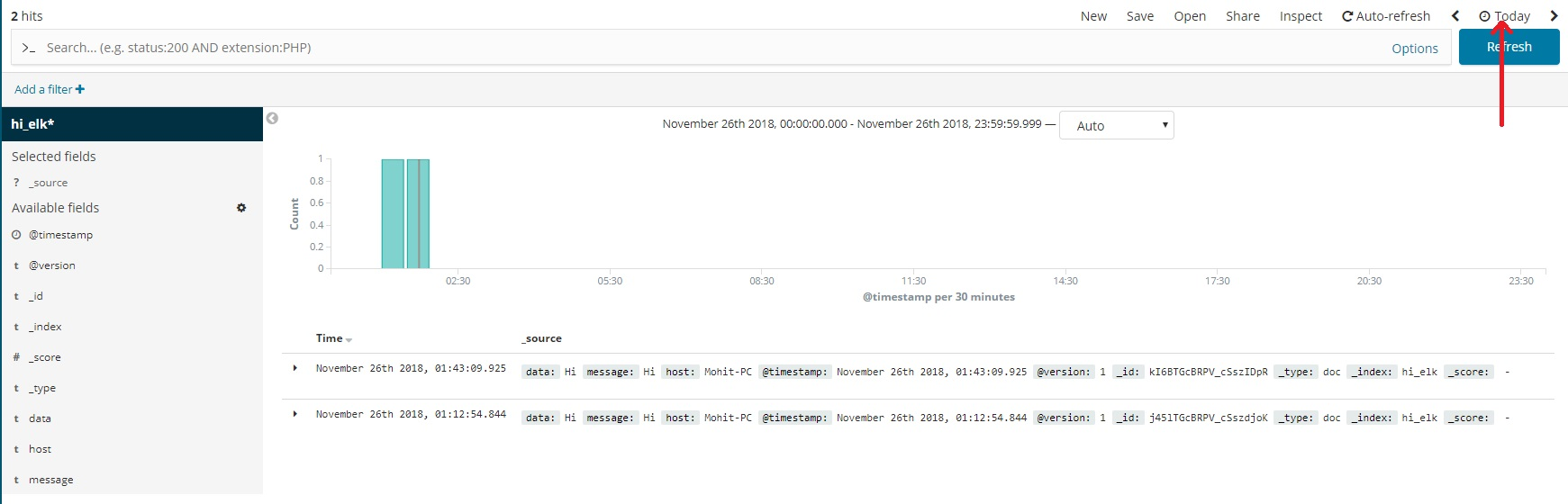
1. You will be asked to create a “Index Pattern”. Enter “Index Name” (which we created in logstash.conf file) and hit “Next Step”.



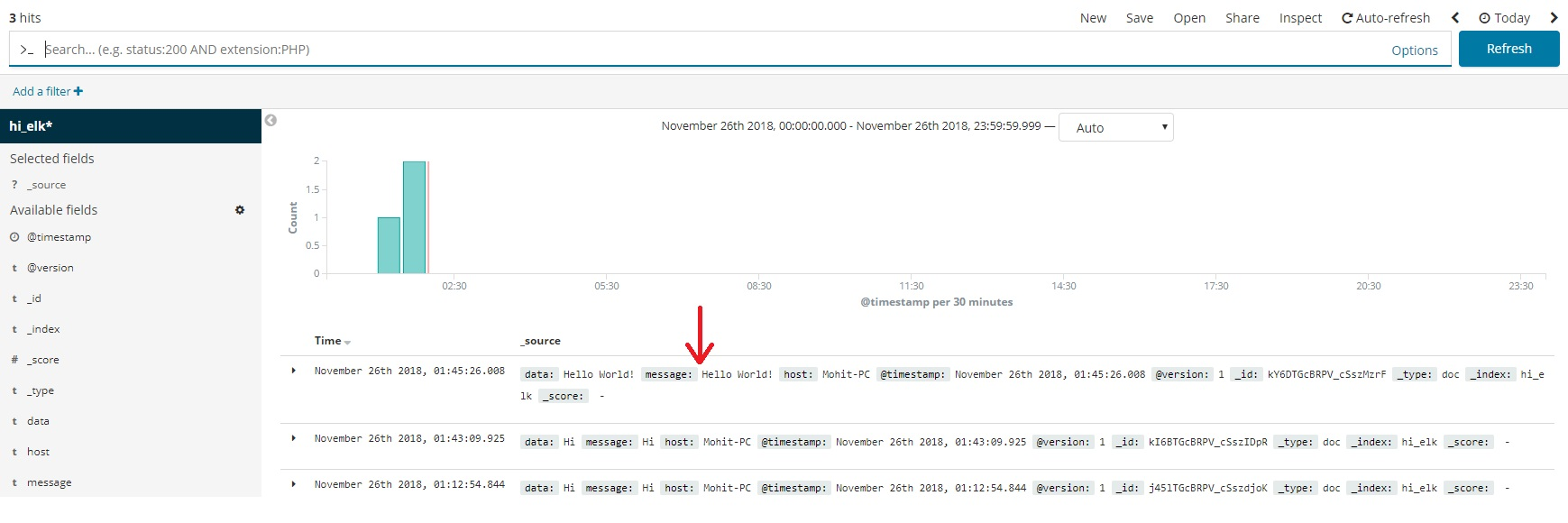
1. Select Timestamp from dropdown and hit “Create index pattern”.



1. You will be shown Index Pattern Screen. Head over back to “Discover” Section (Step 5) and Select “Today” in the Time Range:



1. You can see your messages (Sent from Logstash in Step 3 of Logstash setup) in Kibana now.
2. To play along, enter new messages in Logstash Console, Head over back to Kibana and hit Refresh. Your messages will show up in Kibana.



We are now done with ELK Stack Hello World! We have successfully setup up ELK and created Logstash pipeline.