Lesson 05 Demo 03

Building Dashboards and Visualizations in Kibana

Objective: To build dashboards and visualizations in Kibana for monitoring application performance and system health, which aids in quickly identifying issues

Tools required: Kibana

Prerequisites: None

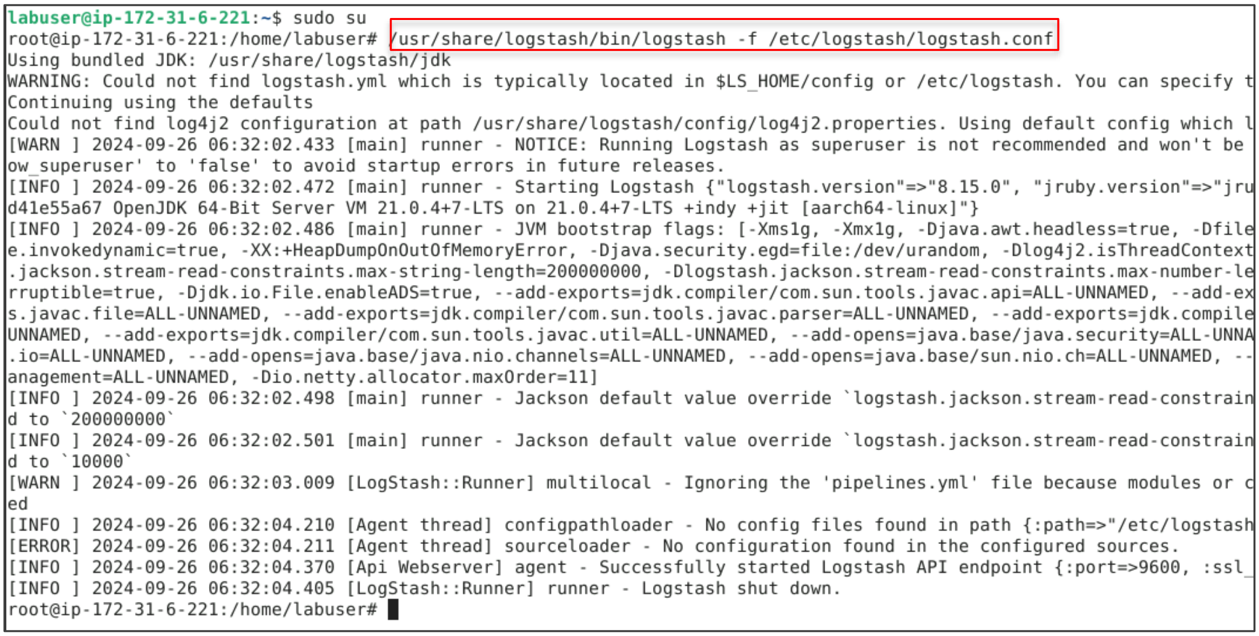
Steps to be followed:

1. Configure the Kibana dashboard
2. Connect with Elasticsearch

Step 1: Configure the Kibana dashboard

1.1 Open the terminal and run Logstash using the following command:

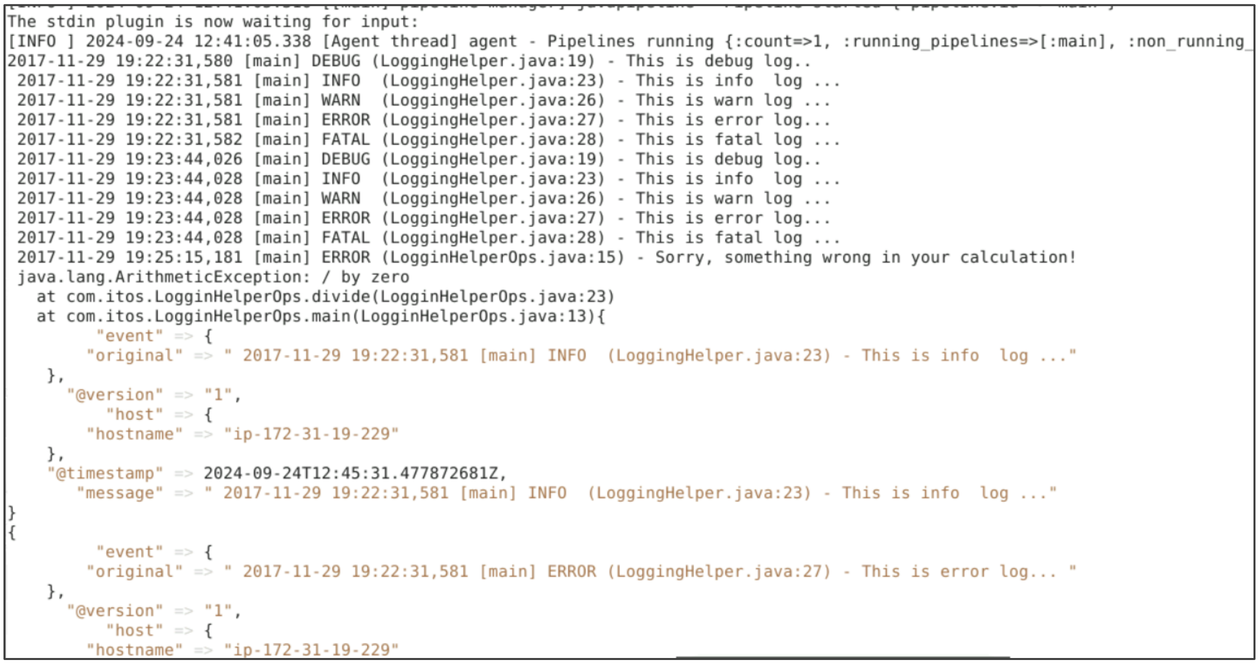
sudo su
/usr/share/logstash/bin/logstash -f /etc/logstash/logstash.conf



```
labuser@ip-172-31-6-221:~$ sudo su
root@ip-172-31-6-221:/home/labuser# /usr/share/logstash/bin/logstash -f /etc/logstash/logstash.conf
Using bundled JDK: /usr/share/logstash/jdk
WARNING: Could not find logstash.yml which is typically located in $LS_HOME/config or /etc/logstash. You can specify t
Continuing using the defaults
Could not find log4j2 configuration at path /usr/share/logstash/config/log4j2.properties. Using default config which l
[WARN ] 2024-09-26 06:32:02.433 [main] runner - NOTICE: Running Logstash as superuser is not recommended and won't be 
ow_superuser' to 'false' to avoid startup errors in future releases.
[INFO ] 2024-09-26 06:32:02.472 [main] runner - Starting Logstash {"logstash.version"=>"8.15.0", "jruby.version"=>"jru
d41e55a67 OpenJDK 64-Bit Server VM 21.0.4+7-LTS on 21.0.4+7-LTS +indy +jit [aarch64-linux]"}
[INFO ] 2024-09-26 06:32:02.486 [main] runner - JVM bootstrap flags: [-Xms1g, -Xmx1g, -Djava.awt.headless=true, -Dfile
e.invokedynamic=true, -XX:+HeapDumpOnOutOfMemoryError, -Djava.security.egd=file:/dev/urandom, -Dlog4j2.isThreadContext
.jackson.stream-read-constraints.max-string-length=200000000, -Dlogstash.jackson.stream-read-constraints.max-number-le
rruptible=true, -Djdk.io.File.enableADS=true, --add-exports=jdk.compiler/com.sun.tools.javac.api=ALL-UNNAMED, --add-ex
s.javac.file=ALL-UNNAMED, --add-exports=jdk.compiler/com.sun.tools.javac.parser=ALL-UNNAMED, --add-exports=jdk.compile
UNNAMED, --add-exports=jdk.compiler/com.sun.tools.javac.util=ALL-UNNAMED, --add-opens=java.base/java.security=ALL-UNNA
.io=ALL-UNNAMED, --add-opens=java.base/java.nio.channels=ALL-UNNAMED, --add-opens=java.base/sun.nio.ch=ALL-UNNAMED, --
anagement=ALL-UNNAMED, -Dio.netty.allocator.maxOrder=11]
[INFO ] 2024-09-26 06:32:02.498 [main] runner - Jackson default value override `logstash.jackson.stream-read-constrain
d to `200000000`
[INFO ] 2024-09-26 06:32:02.501 [main] runner - Jackson default value override `logstash.jackson.stream-read-constrain
d to `10000`
[WARN ] 2024-09-26 06:32:03.009 [LogStash::Runner] multilocal - Ignoring the 'pipelines.yml' file because modules or c
ed
[INFO ] 2024-09-26 06:32:04.210 [Agent thread] configpathloader - No config files found in path {:path=>"/etc/logstash
[ERROR] 2024-09-26 06:32:04.211 [Agent thread] sourceloader - No configuration found in the configured sources.
[INFO ] 2024-09-26 06:32:04.370 [Api Webserver] agent - Successfully started Logstash API endpoint {:port=>9600, :ssl_
[INFO ] 2024-09-26 06:32:04.405 [LogStash::Runner] runner - Logstash shut down.
root@ip-172-31-6-221:/home/labuser# █
```

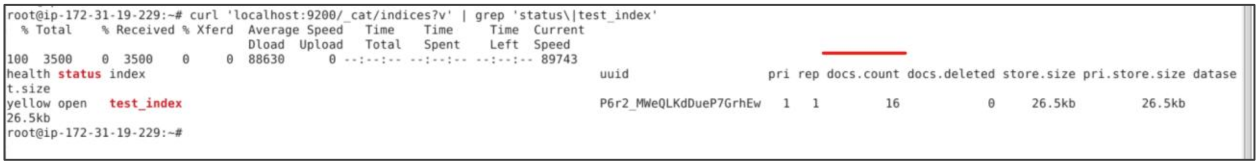
1.2 Once it prompts for a log message, provide the following log content and press Enter:

```
2017-11-29 19:22:31,580 [main] DEBUG (LoggingHelper.java:19) - This is debug log..
2017-11-29 19:22:31,581 [main] INFO  (LoggingHelper.java:23) - This is info  log ...
2017-11-29 19:22:31,581 [main] WARN  (LoggingHelper.java:26) - This is warn log ...
2017-11-29 19:22:31,581 [main] ERROR (LoggingHelper.java:27) - This is error log...
2017-11-29 19:22:31,582 [main] FATAL (LoggingHelper.java:28) - This is fatal log ...
2017-11-29 19:23:44,026 [main] DEBUG (LoggingHelper.java:19) - This is debug log..
2017-11-29 19:23:44,028 [main] INFO  (LoggingHelper.java:23) - This is info  log ...
2017-11-29 19:23:44,028 [main] WARN  (LoggingHelper.java:26) - This is warn log ...
2017-11-29 19:23:44,028 [main] ERROR (LoggingHelper.java:27) - This is error log...
2017-11-29 19:23:44,028 [main] FATAL (LoggingHelper.java:28) - This is fatal log ...
2017-11-29 19:25:15,181 [main] ERROR (LogginHelperOps.java:15) - Sorry,
something wrong in your calculation!
java.lang.ArithmeticException: / by zero
  at com.itos.LogginHelperOps.divide(LogginHelperOps.java:23)
  at com.itos.LogginHelperOps.main(LogginHelperOps.java:13)
```



```
The stdin plugin is now waiting for input:
[INFO ] 2024-09-24 12:41:05.338 [Agent thread] agent - Pipelines running {:count=>1, :running_pipelines=>[:main], :non_running_
2017-11-29 19:22:31,580 [main] DEBUG (LoggingHelper.java:19) - This is debug log..
 2017-11-29 19:22:31,581 [main] INFO  (LoggingHelper.java:23) - This is info  log ...
 2017-11-29 19:22:31,581 [main] WARN  (LoggingHelper.java:26) - This is warn log ...
 2017-11-29 19:22:31,581 [main] ERROR (LoggingHelper.java:27) - This is error log...
 2017-11-29 19:22:31,582 [main] FATAL (LoggingHelper.java:28) - This is fatal log ...
 2017-11-29 19:23:44,026 [main] DEBUG (LoggingHelper.java:19) - This is debug log..
 2017-11-29 19:23:44,028 [main] INFO  (LoggingHelper.java:23) - This is info  log ...
 2017-11-29 19:23:44,028 [main] WARN  (LoggingHelper.java:26) - This is warn log ...
 2017-11-29 19:23:44,028 [main] ERROR (LoggingHelper.java:27) - This is error log...
 2017-11-29 19:23:44,028 [main] FATAL (LoggingHelper.java:28) - This is fatal log ...
 2017-11-29 19:25:15,181 [main] ERROR (LogginHelperOps.java:15) - Sorry, something wrong in your calculation!
 java.lang.ArithmeticException: / by zero
   at com.itos.LogginHelperOps.divide(LogginHelperOps.java:23)
   at com.itos.LogginHelperOps.main(LogginHelperOps.java:13){
         "event" => {
        "original" => " 2017-11-29 19:22:31,581 [main] INFO  (LoggingHelper.java:23) - This is info  log ..."
    },
      "@version" => "1",
          "host" => {
        "hostname" => "ip-172-31-19-229"
    },
    "@timestamp" => 2024-09-24T12:45:31.477872681Z,
       "message" => " 2017-11-29 19:22:31,581 [main] INFO  (LoggingHelper.java:23) - This is info  log ..."
}
{
         "event" => {
        "original" => " 2017-11-29 19:22:31,581 [main] ERROR (LoggingHelper.java:27) - This is error log... "
    },
      "@version" => "1",
          "host" => {
        "hostname" => "ip-172-31-19-229"
```

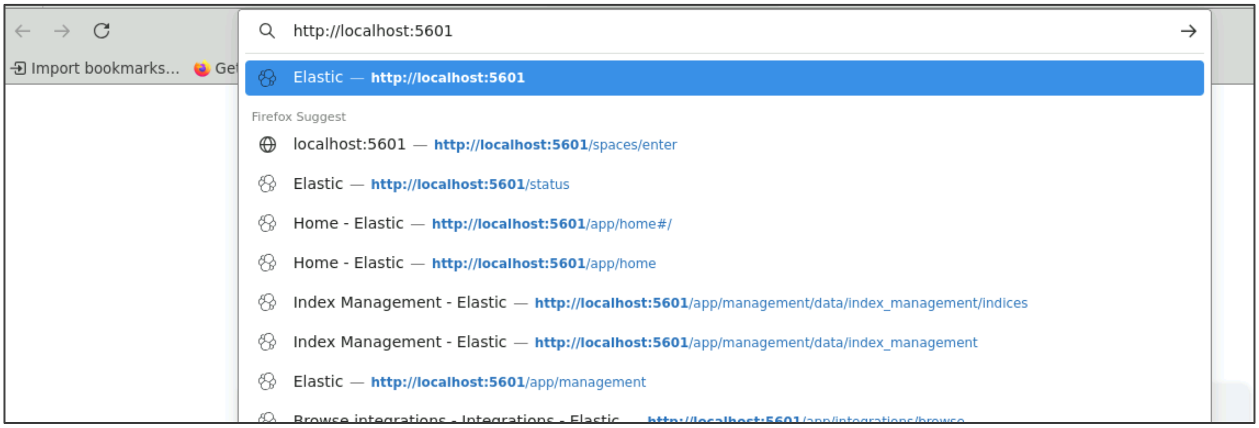
1.3 Enter the following command to validate the test_index created:
curl 'localhost:9200/_cat/indices?v' | grep 'status\|test_index'



```
root@ip-172-31-19-229:~# curl 'localhost:9200/_cat/indices?v' | grep 'status\|test_index'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3500    0  3500    0     0  88630      0 --:--:-- --:--:-- --:--:-- 89743
health status index                                                          uuid                   pri rep docs.count docs.deleted store.size pri.store.size datase
t.size
yellow open   test_index                                                     P6r2_MWeQLKdDueP7GrhEw   1   1         16            0     26.5kb         26.5kb
26.5kb
root@ip-172-31-19-229:~#
```

Step 2: Connect with Elasticsearch

2.1 Enter the following URL to access the Kibana web interface to visualize logs:
http://localhost:5601



http://localhost:5601

Elastic — http://localhost:5601

Firefox Suggest

localhost:5601 — http://localhost:5601/spaces/enter

Elastic — http://localhost:5601/status

Home - Elastic — http://localhost:5601/app/home#/

Home - Elastic — http://localhost:5601/app/home

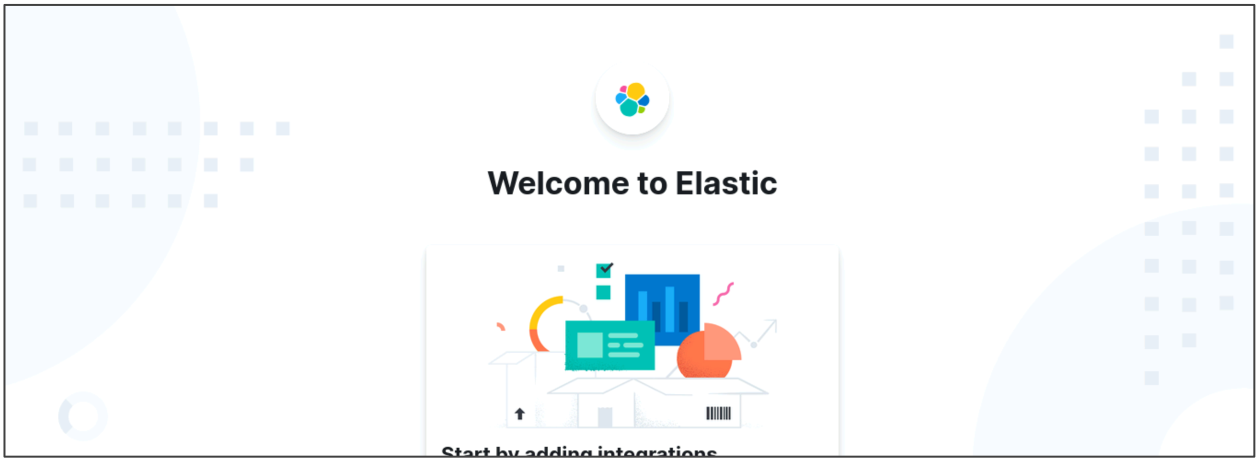
Index Management - Elastic — http://localhost:5601/app/management/data/index_management/indices

Index Management - Elastic — http://localhost:5601/app/management/data/index_management

Elastic — http://localhost:5601/app/management

Browse integrations - Integrations - Elastic — http://localhost:5601/app/integrations/browse

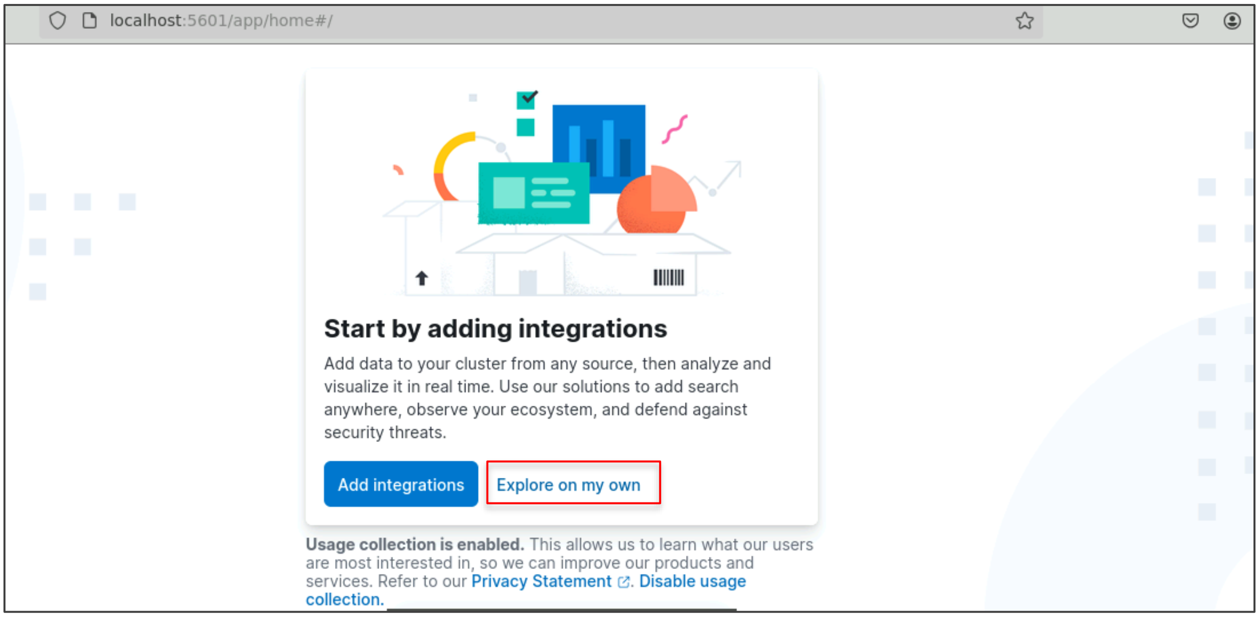
You will see the following screen:



Welcome to Elastic

Start by adding integrations

2.2 Click on **Explore on my own**

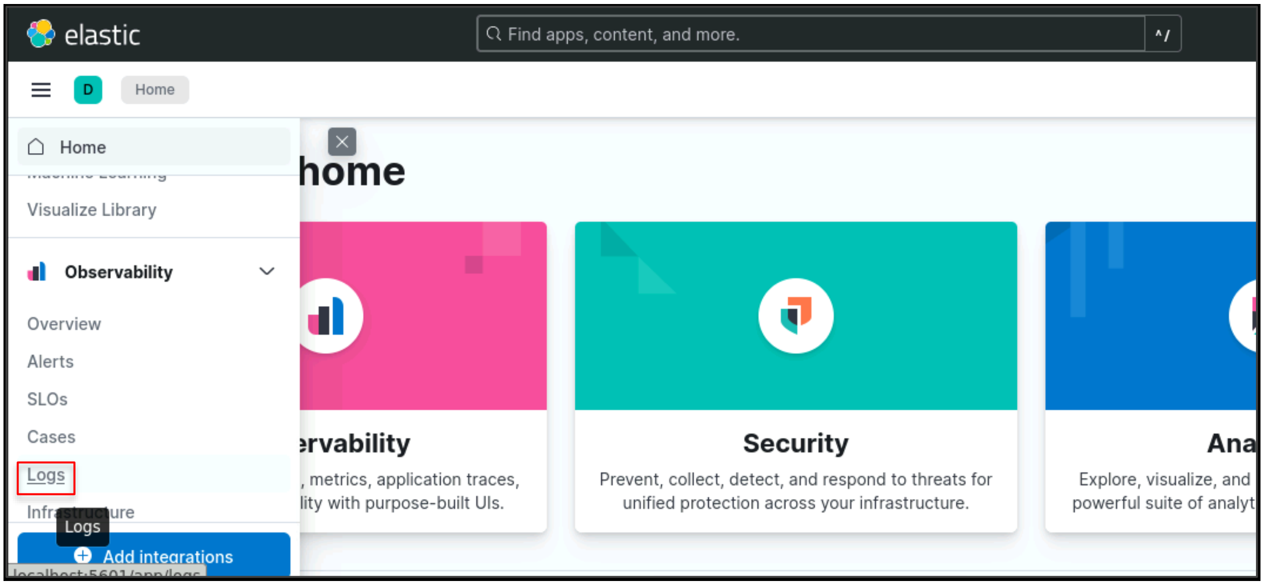


Start by adding integrations

Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and defend against security threats.

Usage collection is enabled. This allows us to learn what our users are most interested in, so we can improve our products and services. Refer to our Privacy Statement. Disable usage collection.

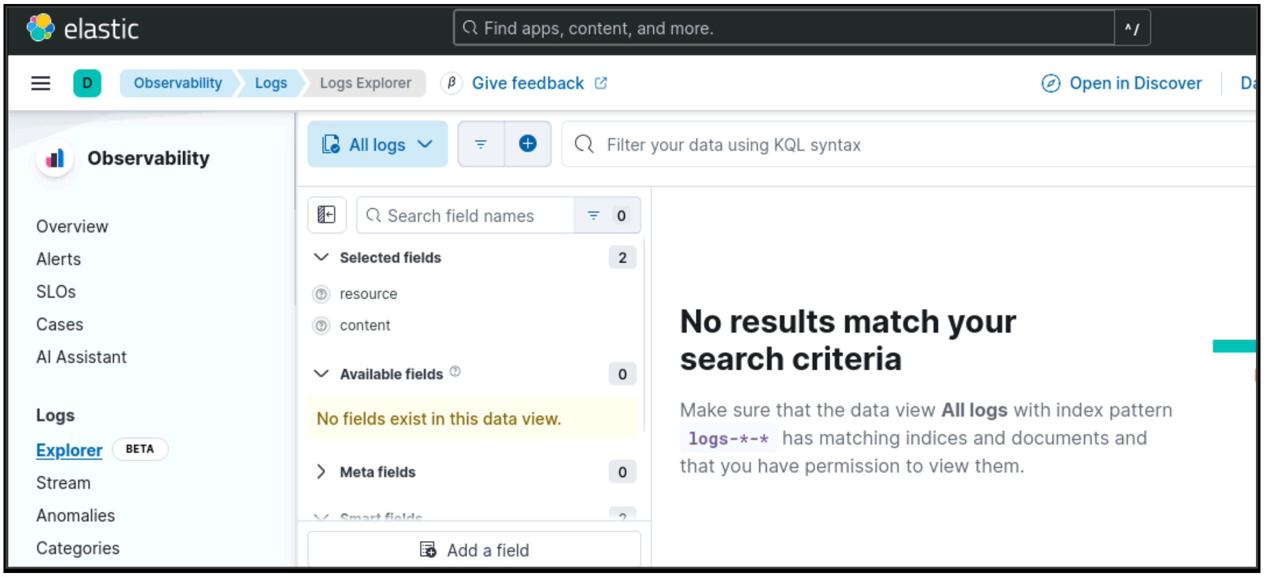
2.3 Click on **Home** and then on **Logs** to check the system logs in Kibana



, metrics, application traces, lity with purpose-built UIs.

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Explore, visualize, and powerful suite of analyt

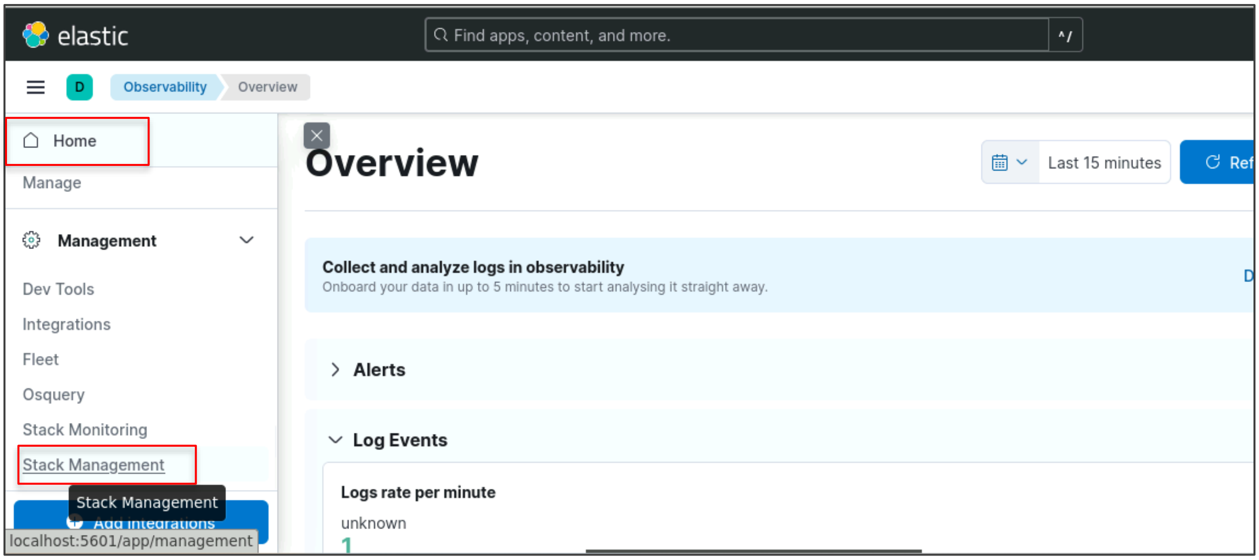


No fields exist in this data view.

No results match your search criteria

Make sure that the data view **All logs** with index pattern `logs-*-*` has matching indices and documents and that you have permission to view them.

2.4 Navigate back to **Home** and click on **Stack Management**



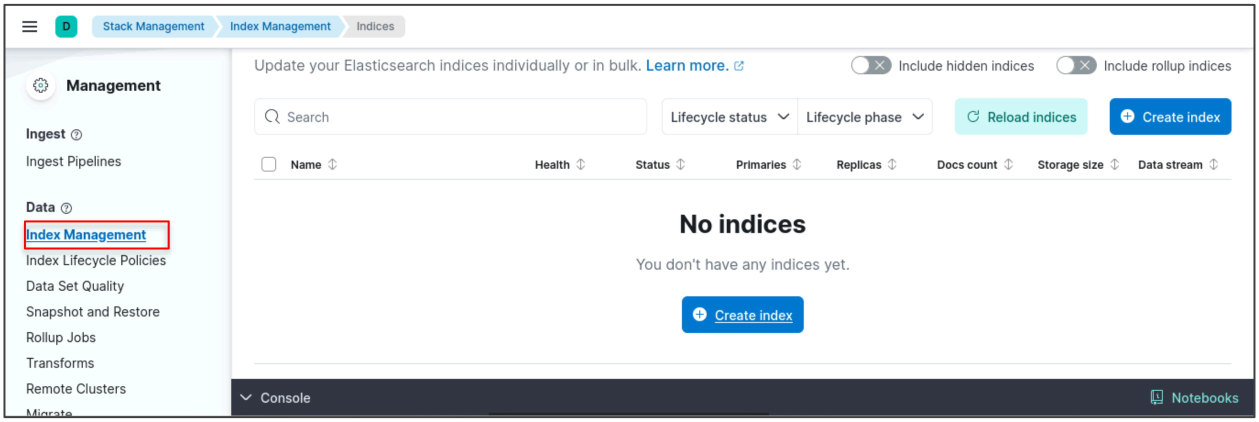
Collect and analyze logs in observability

Onboard your data in up to 5 minutes to start analysing it straight away.

Logs rate per minute

unknown

2.5 Click on **Index Management**

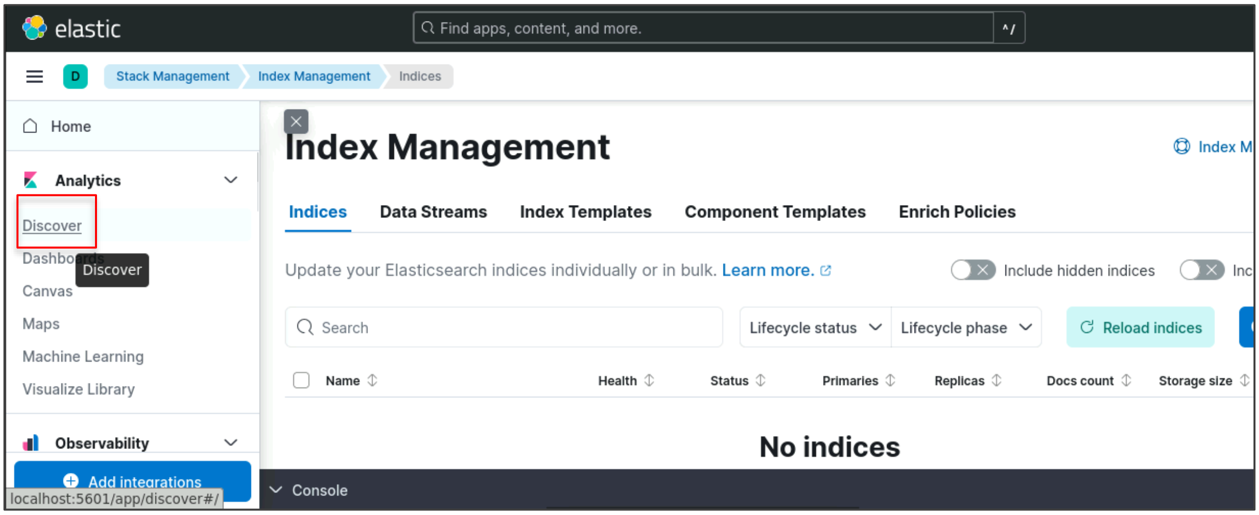


Update your Elasticsearch indices individually or in bulk. Learn more.

No indices

You don't have any indices yet.

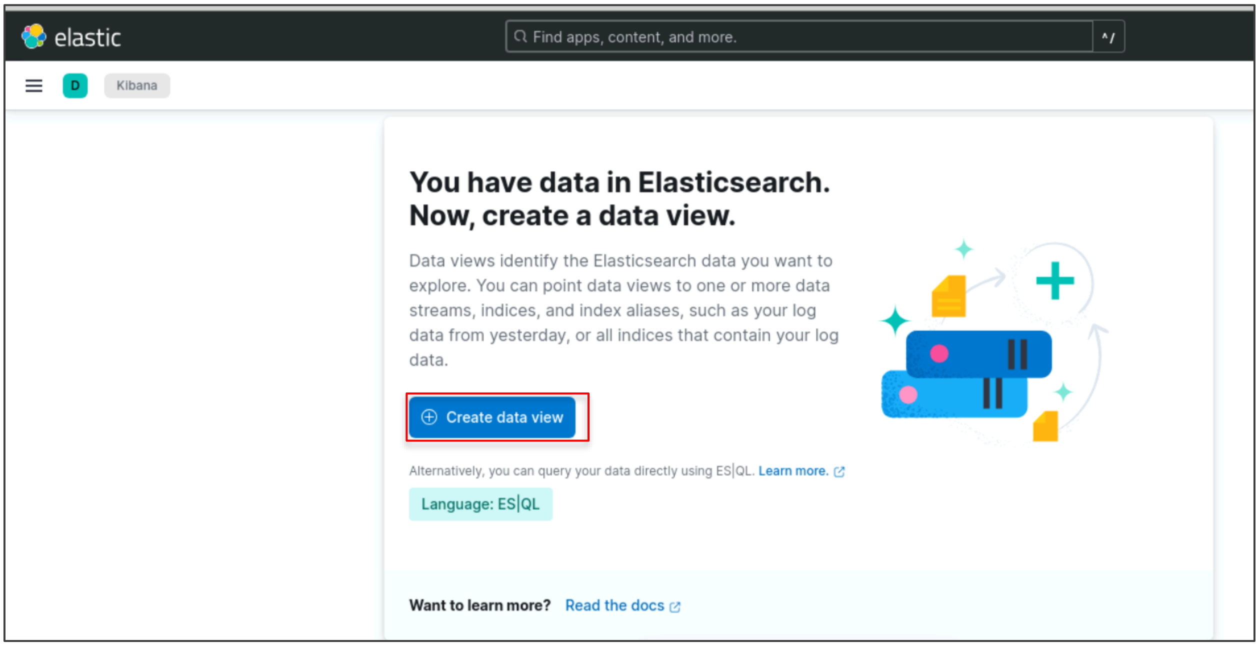
2.6 Under **Analytics**, click on **Discover**



Update your Elasticsearch indices individually or in bulk. Learn more.

No indices

2.7 Click on **Create data view**



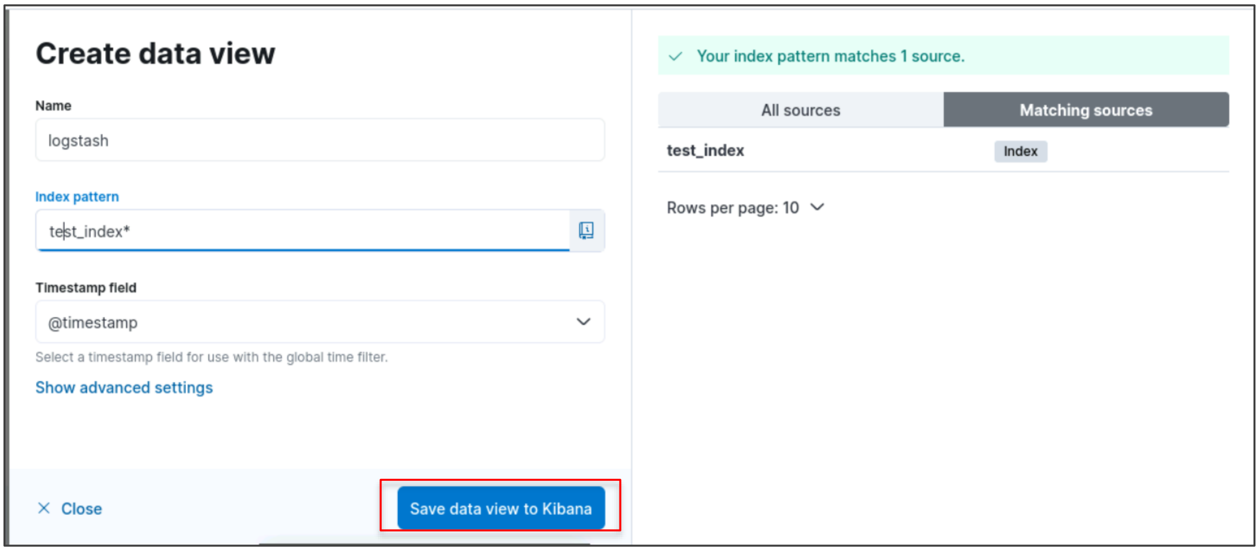
You have data in Elasticsearch. Now, create a data view.

Data views identify the Elasticsearch data you want to explore. You can point data views to one or more data streams, indices, and index aliases, such as your log data from yesterday, or all indices that contain your log data.

Alternatively, you can query your data directly using ES|QL. Learn more.

Want to learn more? Read the docs

2.8 Fill in the details as shown in the screenshot and click on **Save data view to Kibana**



Create data view

Name: logstash

Index pattern: test_index*

Timestamp field: @timestamp

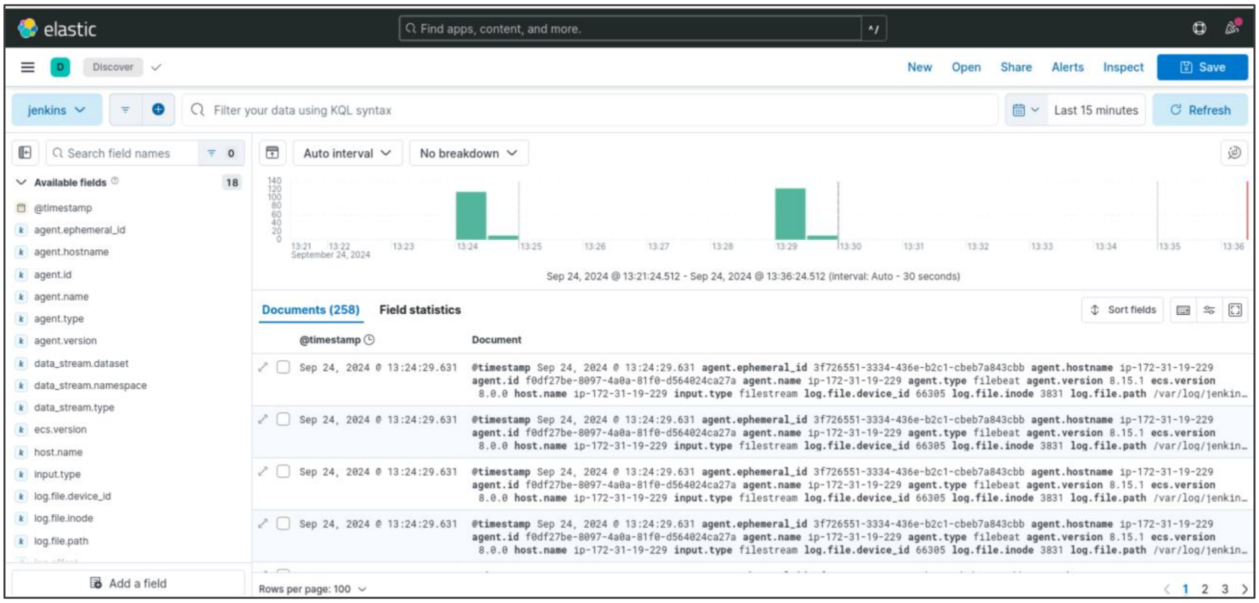
Select a timestamp field for use with the global time filter.

Your index pattern matches 1 source.

All sources	Matching sources
test_index	Index

Rows per page: 10

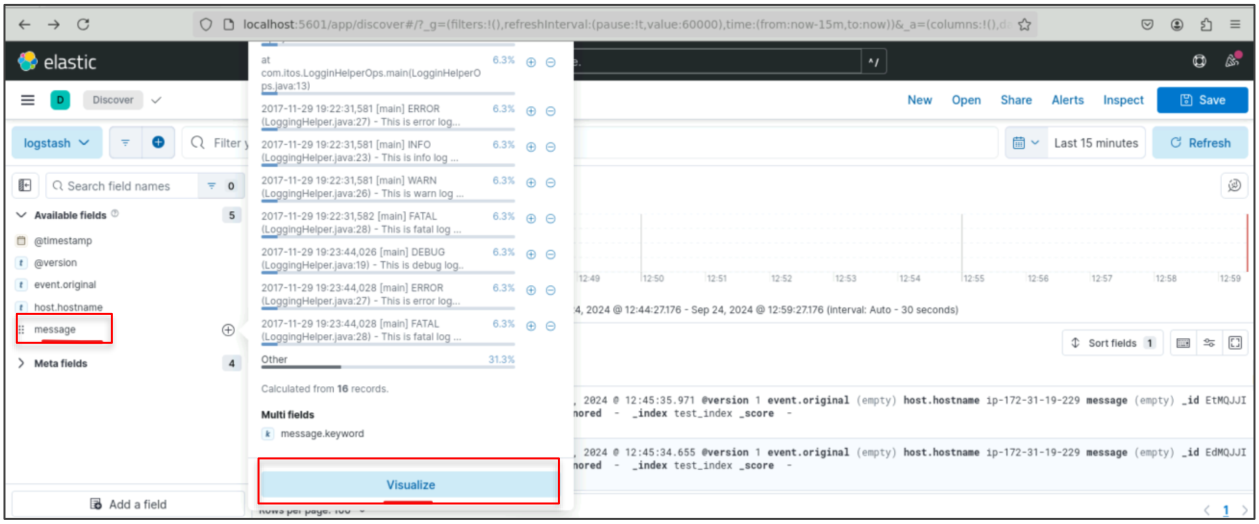
You can visualize the logs as shown below:



Sep 24, 2024 @ 13:21:24.512 - Sep 24, 2024 @ 13:36:24.512 (interval: Auto - 30 seconds)

```
Sep 24, 2024 @ 13:24:29.631  @timestamp Sep 24, 2024 @ 13:24:29.631 agent.ephemeral_id 3f726551-3334-436e-b2c1-cbeb7a843cbb agent.hostname ip-172-31-19-229
                             agent.id f0df27be-8097-4a0a-81f0-d564024ca27a agent.name ip-172-31-19-229 agent.type filebeat agent.version 8.15.1 ecs.version
                              8.0.0 host.name ip-172-31-19-229 input.type filestream log.file.device_id 66305 log.file.inode 3831 log.file.path /var/log/jenkin…
Sep 24, 2024 @ 13:24:29.631  @timestamp Sep 24, 2024 @ 13:24:29.631 agent.ephemeral_id 3f726551-3334-436e-b2c1-cbeb7a843cbb agent.hostname ip-172-31-19-229
                             agent.id f0df27be-8097-4a0a-81f0-d564024ca27a agent.name ip-172-31-19-229 agent.type filebeat agent.version 8.15.1 ecs.version
                              8.0.0 host.name ip-172-31-19-229 input.type filestream log.file.device_id 66305 log.file.inode 3831 log.file.path /var/log/jenkin…
Sep 24, 2024 @ 13:24:29.631  @timestamp Sep 24, 2024 @ 13:24:29.631 agent.ephemeral_id 3f726551-3334-436e-b2c1-cbeb7a843cbb agent.hostname ip-172-31-19-229
                             agent.id f0df27be-8097-4a0a-81f0-d564024ca27a agent.name ip-172-31-19-229 agent.type filebeat agent.version 8.15.1 ecs.version
                              8.0.0 host.name ip-172-31-19-229 input.type filestream log.file.device_id 66305 log.file.inode 3831 log.file.path /var/log/jenkin…
Sep 24, 2024 @ 13:24:29.631  @timestamp Sep 24, 2024 @ 13:24:29.631 agent.ephemeral_id 3f726551-3334-436e-b2c1-cbeb7a843cbb agent.hostname ip-172-31-19-229
                             agent.id f0df27be-8097-4a0a-81f0-d564024ca27a agent.name ip-172-31-19-229 agent.type filebeat agent.version 8.15.1 ecs.version
                              8.0.0 host.name ip-172-31-19-229 input.type filestream log.file.device_id 66305 log.file.inode 3831 log.file.path /var/log/jenkin…
```

2.9 Choose the **message** field on the left and click on **Visualize**



localhost:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:now-15m,to:now))&_a=(columns:!(),d

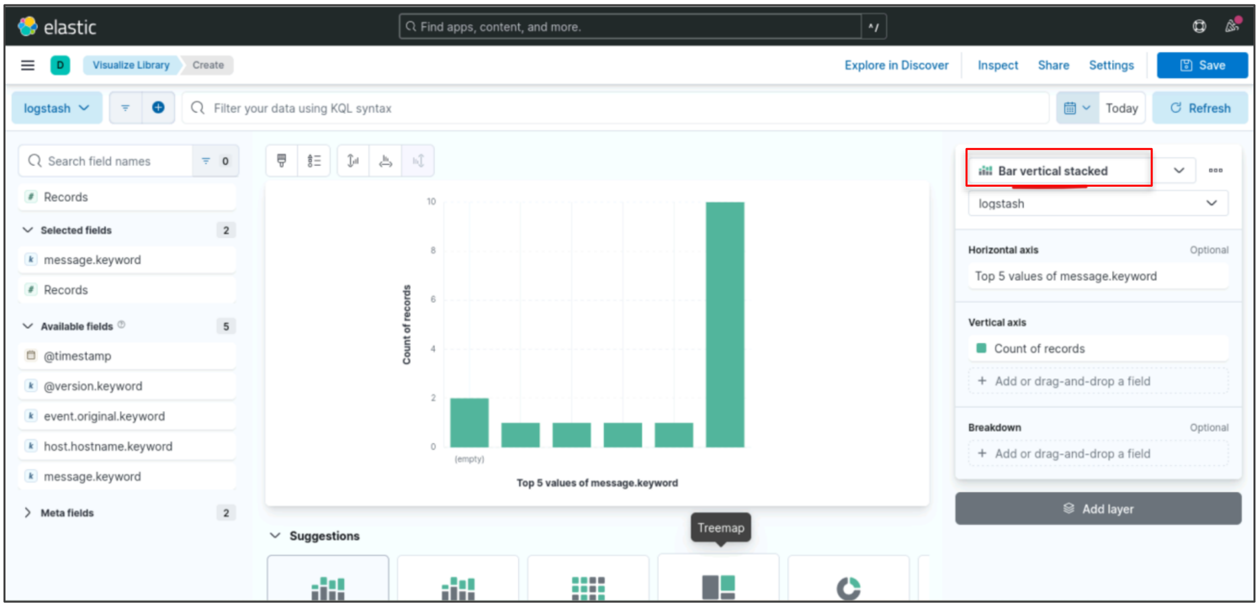
```
at
com.itos.LogginHelperOps.main(LogginHelperOps.java:13)                                        6.3%
2017-11-29 19:22:31,581 [main] ERROR (LoggingHelper.java:27) - This is error log...           6.3%
2017-11-29 19:22:31,581 [main] INFO (LoggingHelper.java:23) - This is info log ...            6.3%
2017-11-29 19:22:31,581 [main] WARN (LoggingHelper.java:26) - This is warn log ...            6.3%
2017-11-29 19:22:31,582 [main] FATAL (LoggingHelper.java:28) - This is fatal log ...          6.3%
2017-11-29 19:23:44,026 [main] DEBUG (LoggingHelper.java:19) - This is debug log..            6.3%
2017-11-29 19:23:44,028 [main] ERROR (LoggingHelper.java:27) - This is error log...           6.3%
2017-11-29 19:23:44,028 [main] FATAL (LoggingHelper.java:28) - This is fatal log ...          6.3%
Other                                                                                         31.3%
```

Calculated from 16 records.

4, 2024 @ 12:44:27.176 - Sep 24, 2024 @ 12:59:27.176 (interval: Auto - 30 seconds)

```
, 2024 @ 12:45:35.971 @version 1 event.original (empty) host.hostname ip-172-31-19-229 message (empty) _id EtMQJJI
nored  -  _index test_index _score  -
, 2024 @ 12:45:34.655 @version 1 event.original (empty) host.hostname ip-172-31-19-229 message (empty) _id EdMQJJI
nored  -  _index test_index _score  -
```

2.10 Select the **Bar vertical stacked** chart; you will see the stats from the logs



Bar vertical stacked

logstash

Horizontal axis: Top 5 values of message.keyword

Vertical axis: Count of records

Breakdown: + Add or drag-and-drop a field

By following these steps, you have successfully built dashboards and visualizations in Kibana for monitoring application performance and system health, which aids in quickly identifying issues.