Lab 06 - ELK

Lab 06

Guide

- Lab 06 Guide
- Lab 06 Repository

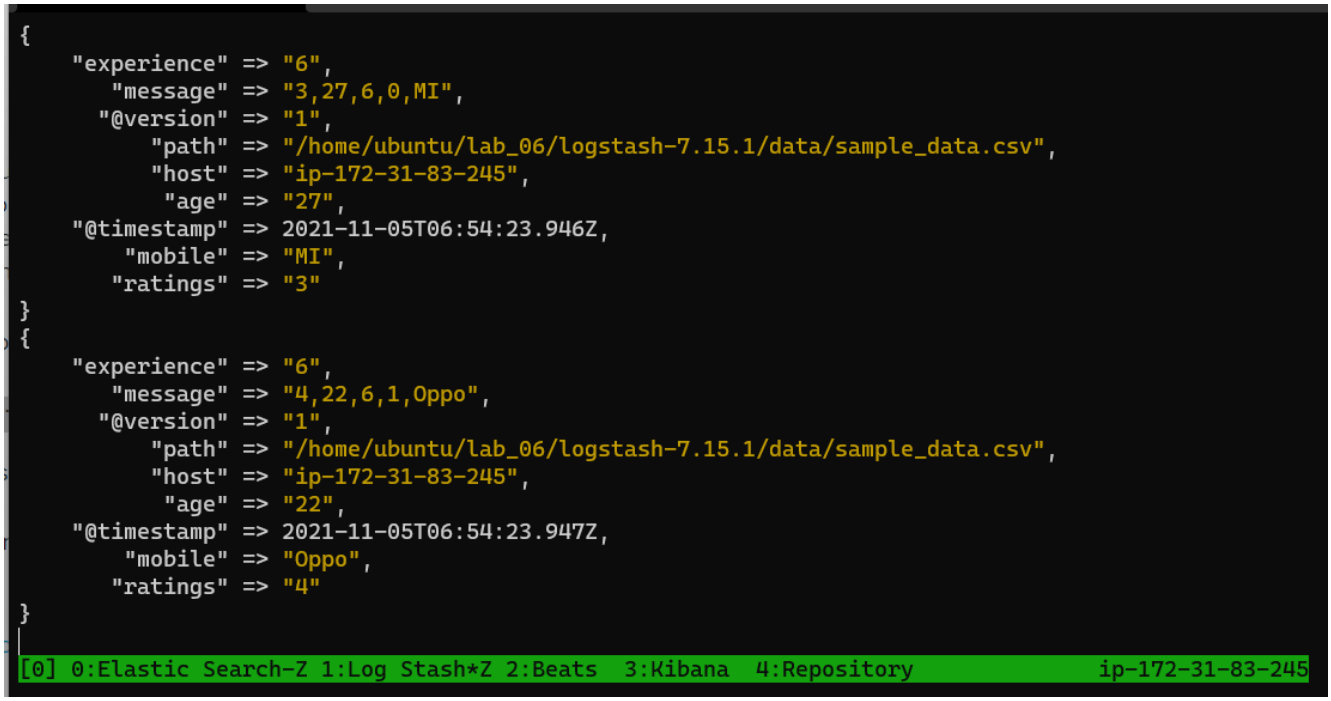
Applications

- Elastic Search

```
[2021-11-05T06:43:24,138][INFO ][o.e.t.LoggingTaskListener] [ip-172-31-83-245] 28585 finished with
 response BulkByScrollResponse[took=640ms,timed_out=false,sliceId=null,updated=735,created=0,delet
ed=0,batches=1,versionConflicts=0,noops=0,retries=0,throttledUntil=0s,bulk_failures=[],search_fail
ures=[]]
[2021-11-05T06:43:24,162][INFO ][o.e.t.LoggingTaskListener] [ip-172-31-83-245] 28593 finished with
 response BulkByScrollResponse[took=359.4ms,timed_out=false,sliceId=null,updated=15,created=0,dele
ted=0,batches=1,versionConflicts=0,noops=0,retries=0,throttledUntil=0s,bulk_failures=[],search_fai
lures=[]]
[2021-11-05T06:47:59,494][INFO ][o.e.t.LoggingTaskListener] [ip-172-31-83-245] 32379 finished with
 response BulkByScrollResponse[took=446.8ms,timed_out=false,sliceId=null,updated=740,created=0,del
eted=0,batches=1,versionConflicts=0,noops=0,retries=0,throttledUntil=0s,bulk_failures=[],search_fa
ilures=[]]
[2021-11-05T06:47:59,510][INFO ][o.e.t.LoggingTaskListener] [ip-172-31-83-245] 32386 finished with
 response BulkByScrollResponse[took=405.3ms,timed_out=false,sliceId=null,updated=15,created=0,dele
ted=0,batches=1,versionConflicts=0,noops=0,retries=0,throttledUntil=0s,bulk_failures=[],search_fai
lures=[]]
[2021-11-05T06:48:41,296][INFO ][o.e.c.m.MetadataIndexTemplateService] [ip-172-31-83-245] adding t
emplate [filebeat-7.15.1] for index patterns [filebeat-7.15.1-*]
[2021-11-05T06:54:24,648][INFO ][o.e.c.m.MetadataCreateIndexService] [ip-172-31-83-245] [sample_da
ta] creating index, cause [auto(bulk api)], templates [], shards [1]/[1]
[2021-11-05T06:54:24,790][INFO ][o.e.c.m.MetadataMappingService] [ip-172-31-83-245] [sample_data/A
Dh3K1AeTtCxifrRleK5LQ] create_mapping [_doc]

[0] 0:Elastic Search*Z 1:Log Stash-Z 2:Beats  3:Kibana  4:Repository                ip-172-31-83-245
```

- LogStash



- Beats

- Kibana

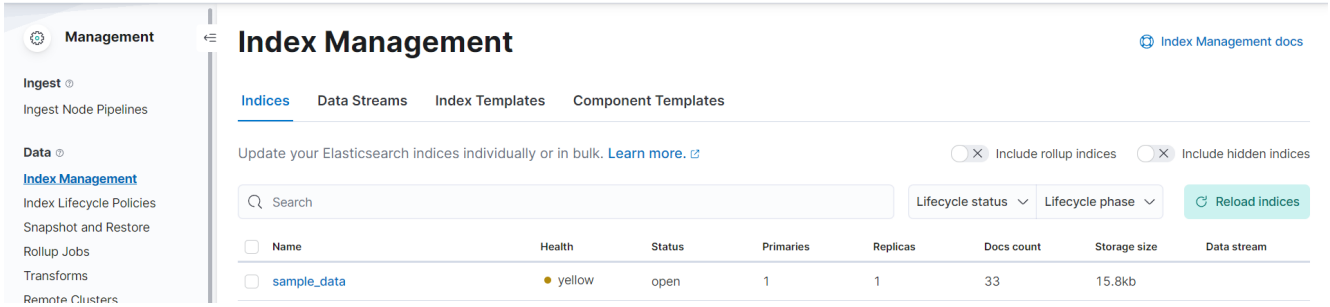
```
,visTypeTable,visTypePie,visTypeMetric,visTypeMarkdown,tileMap,regionMap,presentationUtil,expressi
onShape,expressionRevealImage,expressionRepeatImage,expressionMetric,expressionImage,timelion,inde
xPatternFieldEditor,home,searchprofiler,painlessLab,grokdebugger,graph,cloud,fleet,visTypeVega,man
agement,watcher,transform,snapshotRestore,savedObjectsTagging,licenseManagement,ingestPipelines,in
dexManagement,remoteClusters,crossClusterReplication,indexLifecycleManagement,dataEnhanced,indexPa
tternManagement,advancedSettings,discover,discoverEnhanced,dashboard,maps,lens,dataVisualizer,dash
boardMode,dashboardEnhanced,visualize,visTypeTimeseries,rollup,savedObjectsManagement,spaces,repor
ting,canvas,lists,eventLog,actions,alerting,triggersActionsUi,stackAlerts,ruleRegistry,ml,cases,ti
melines,securitySolution,observability,uptime,infra,upgradeAssistant,monitoring,logstash,enterpris
eSearch,console,apmOss,apm]
  log   [06:47:59.741] [warning][fleet][plugins] Fleet requires the security plugin to be enabled.
  log   [06:47:59.760] [info][monitoring][monitoring][plugins] config sourced from: production clu
ster
  log   [06:48:00.795] [info][server][Kibana][http] http server running at http://0.0.0.0:5601
  log   [06:48:01.046] [info][kibana-monitoring][monitoring][monitoring][plugins] Starting monitor
ing stats collection
  log   [06:48:01.052] [info][plugins][securitySolution] Dependent plugin setup complete - Startin
g ManifestTask
  log   [06:48:01.791] [info][plugins][reporting] Browser executable: /home/ubuntu/lab_06/kibana-7
.15.1-linux-x86_64/x-pack/plugins/reporting/chromium/headless_shell-linux_x64/headless_shell
  log   [06:48:01.832] [info][status] Kibana is now degraded
  log   [06:48:04.794] [info][status] Kibana is now available (was degraded)

[0] 0:Elastic SearchZ 1:Log StashZ 2:Beats-Z 3:Kibana*Z 4:Repository                ip-172-31-83-245
```

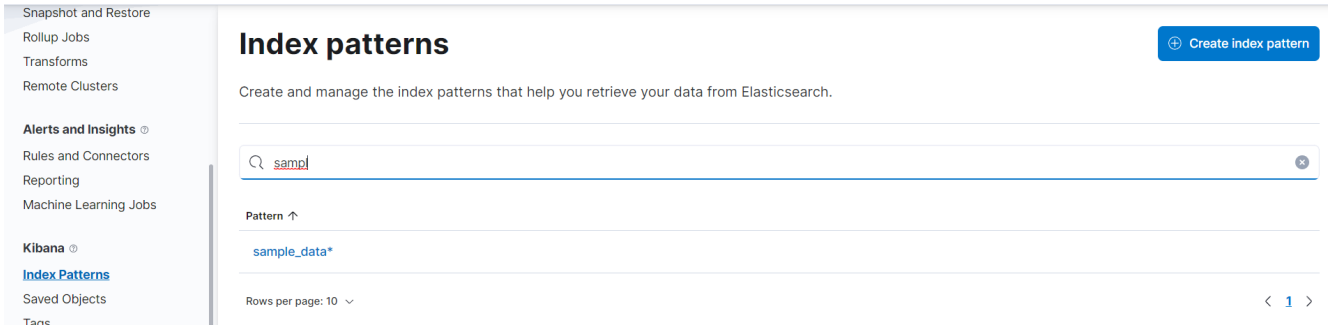
Sample Data

Transform data from the `sample_data.csv` in `LogStash` and then load the result into `ElasticSearch`

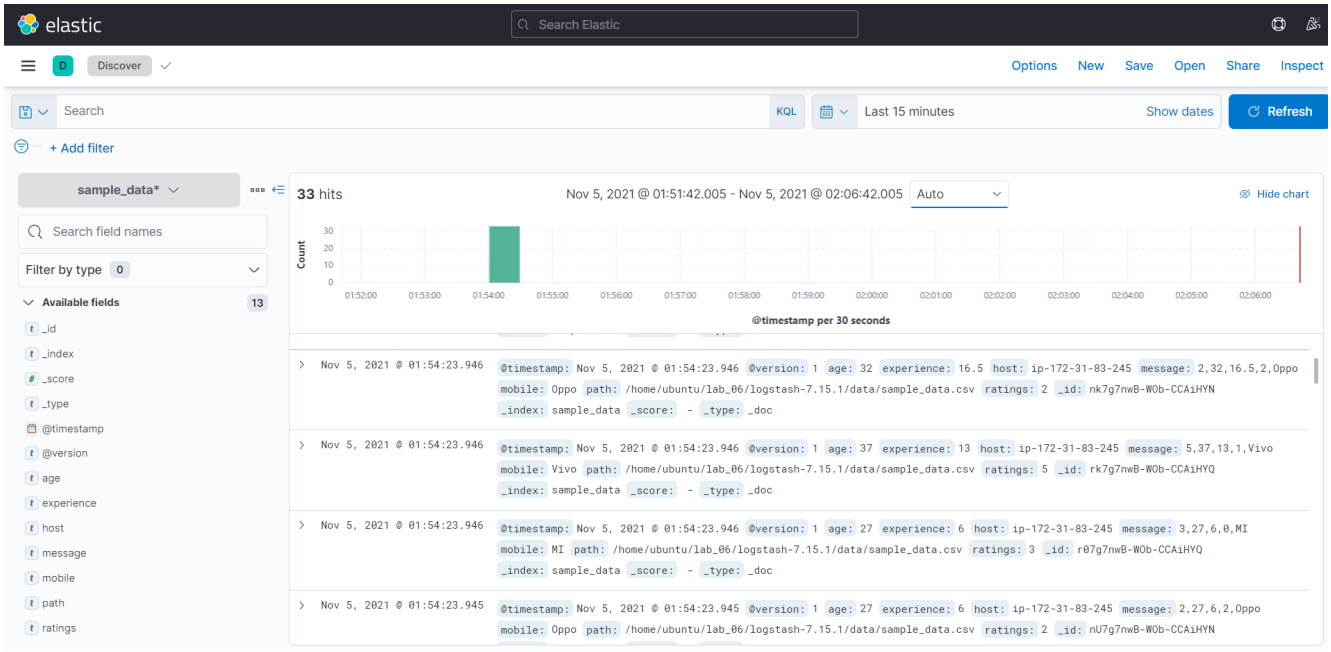
- Verify index was created



- Create the Index Pattern

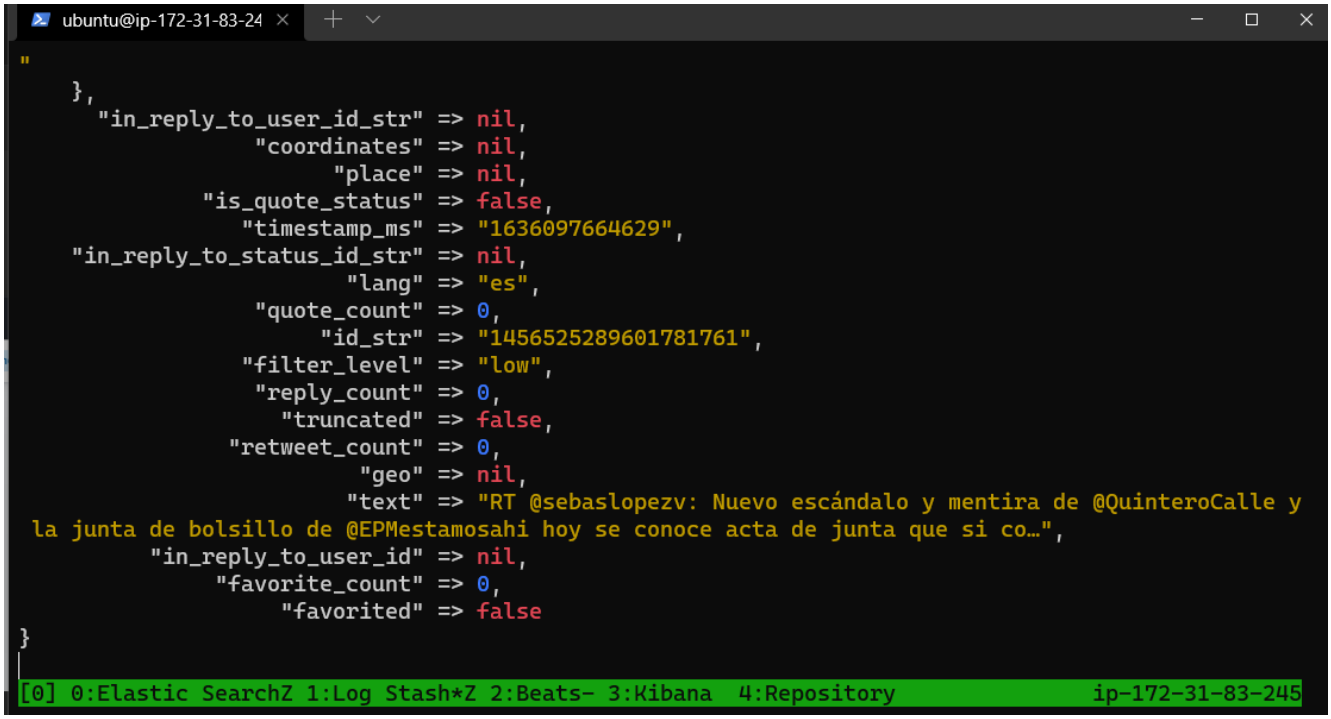


- Inspect the data

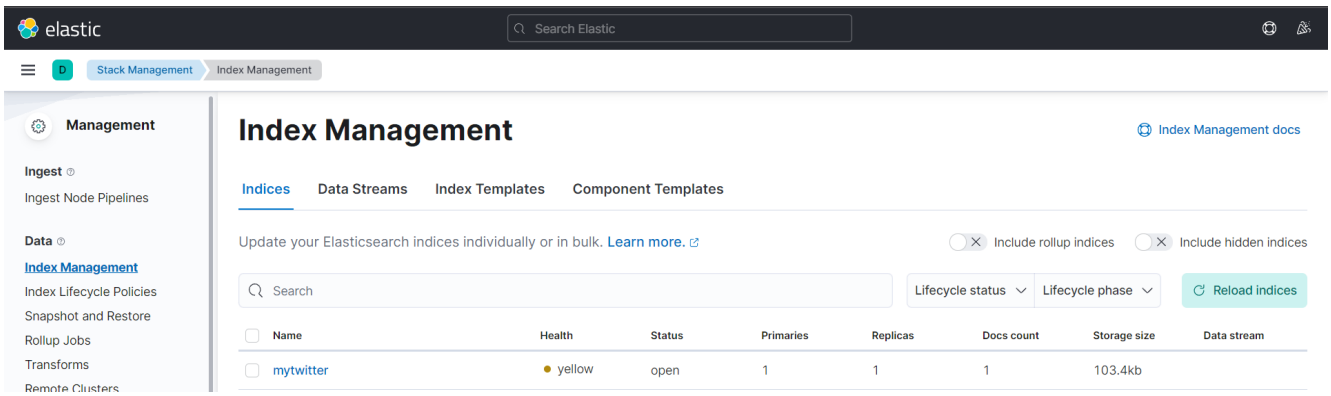


Twitter Feed

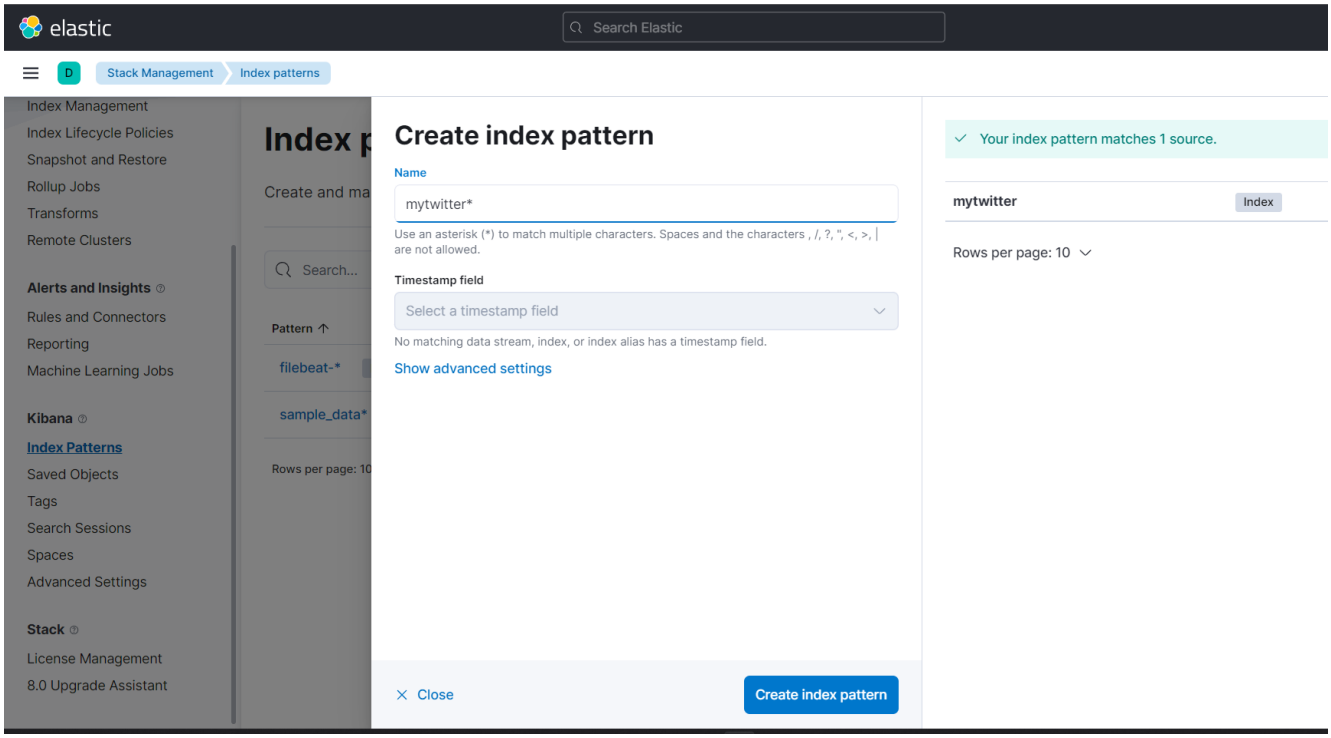
- LogStash with Twitter



- Kibana Twitter Index



- Create Twitter Index Pattern



- Check Twitter Data