

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,deleted=0,batches=1,versionConflicts=0,noops=0,retries=0,throttledUntil=0s,bulk_failures=[],search_failures=[]]
[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,deleted=0,batches=1,versionConflicts=0,noops=0,retries=0,throttledUntil=0s,bulk_failures=[],search_failures=[]]
[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,deleted=0,batches=1,versionConflicts=0,noops=0,retries=0,throttledUntil=0s,bulk_failures=[],search_failures=[]]
[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,deleted=0,batches=1,versionConflicts=0,noops=0,retries=0,throttledUntil=0s,bulk_failures=[],search_failures=[]]
[2021-11-05T06:48:41,296][INFO ][o.e.c.m.MetadataIndexTemplateService] [ip-172-31-83-245] adding template [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_data] 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

```
{
  "experience" => "6",
  "message" => "3,27,6,0,MI",
  "@version" => "1",
  "path" => "/home/ubuntu/lab_06/logstash-7.15.1/data/sample_data.csv",
  "host" => "ip-172-31-83-245",
  "age" => "27",
  "@timestamp" => 2021-11-05T06:54:23.946Z,
  "mobile" => "MI",
  "ratings" => "3"
}
{
  "experience" => "6",
  "message" => "4,22,6,1,Oppo",
  "@version" => "1",
  "path" => "/home/ubuntu/lab_06/logstash-7.15.1/data/sample_data.csv",
  "host" => "ip-172-31-83-245",
  "age" => "22",
  "@timestamp" => 2021-11-05T06:54:23.947Z,
  "mobile" => "Oppo",
  "ratings" => "4"
}
[0] 0:Elastic Search-Z 1:Log Stash*Z 2:Beats 3:Kibana 4:Repository ip-172-31-83-245
```

- Beats

```
e":0}}, "pipeline":{"clients":0,"events":{"active":0}}, "registrar":{"states":{"current":0}}, "system":{"load":{"1":0.18,"15":0.21,"5":0.22,"norm":{"1":0.09,"15":0.105,"5":0.11}}}}}
2021-11-05T07:01:47.908Z INFO [monitoring] log/log.go:184 Non-zero metrics in the last 30s {"monitoring":{"metrics":{"beat":{"cgroup":{"cpuacct":{"total":{"ns":1438042763},"memory":{"mem":{"usage":{"bytes":2617344}}},"cpu":{"system":{"ticks":100,"time":{"ms":5},"total":{"ticks":410,"time":{"ms":9},"value":410},"user":{"ticks":310,"time":{"ms":4}}},"handles":{"limit":{"hard":1048576,"soft":1024},"open":10},"info":{"ephemeral_id":"a9beea00-5a7d-4154-a8ed-3f2d4a62e780"},"uptime":{"ms":690082},"version":"7.15.1"},"memstats":{"gc_next":19419008,"memory_alloc":11297856,"memory_total":70011256,"rss":112226304},"runtime":{"goroutines":20},"filebeat":{"harvester":{"open_files":0,"running":0},"libbeat":{"config":{"module":{"running":0},"output":{"events":{"active":0}}, "pipeline":{"clients":0,"events":{"active":0}}, "registrar":{"states":{"current":0}}, "system":{"load":{"1":0.11,"15":0.2,"5":0.2,"norm":{"1":0.055,"15":0.1,"5":0.1}}}}}
2021-11-05T07:02:17.908Z INFO [monitoring] log/log.go:184 Non-zero metrics in the last 30s {"monitoring":{"metrics":{"beat":{"cgroup":{"cpuacct":{"total":{"ns":1120240475},"memory":{"mem":{"usage":{"bytes":2093056}}},"cpu":{"system":{"ticks":100,"time":{"ms":1},"total":{"ticks":420,"time":{"ms":5},"value":420},"user":{"ticks":320,"time":{"ms":4}}},"handles":{"limit":{"hard":1048576,"soft":1024},"open":10},"info":{"ephemeral_id":"a9beea00-5a7d-4154-a8ed-3f2d4a62e780"},"uptime":{"ms":720080},"version":"7.15.1"},"memstats":{"gc_next":19419008,"memory_alloc":11647112,"memory_total":70360512,"rss":112226304},"runtime":{"goroutines":20},"filebeat":{"harvester":{"open_files":0,"running":0},"libbeat":{"config":{"module":{"running":0},"output":{"events":{"active":0}}, "pipeline":{"clients":0,"events":{"active":0}}, "registrar":{"states":{"current":0}}, "system":{"load":{"1":0.13,"15":0.2,"5":0.2,"norm":{"1":0.065,"15":0.1,"5":0.1}}}}}
[0] 0:Elastic SearchZ 1:Log Stash-Z 2:Beats*Z 3:Kibana 4:Repository ip-172-31-83-245
```

- Kibana

```
,visTypeTable,visTypePie,visTypeMetric,visTypeMarkdown,tileMap,regionMap,presentationUtil,expressionShape,expressionRevealImage,expressionRepeatImage,expressionMetric,expressionImage,timelion,indexPatternFieldEditor,home,searchProfiler,painlessLab,grokDebugger,graph,cloud,fleet,visTypeVega,management,watcher,transform,snapshotRestore,savedObjectsTagging,licenseManagement,ingestPipelines,indexManagement,remoteClusters,crossClusterReplication,indexLifecycleManagement,dataEnhanced,indexPatternManagement,advancedSettings,discover,discoverEnhanced,dashboard,maps,lens,dataVisualizer,dashboardMode,dashboardEnhanced,visualize,visTypeTimeSeries,rollup,savedObjectsManagement,spaces,reporting,canvas,lists,eventLog,actions,alerting,triggersActionsUi,stackAlerts,ruleRegistry,ml,cases,timelines,securitySolution,observability,uptime,infra,upgradeAssistant,monitoring,logstash,enterpriseSearch,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 cluster
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 monitoring stats collection
log [06:48:01.052] [info][plugins][securitySolution] Dependent plugin setup complete - Starting 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

The screenshot shows the Kibana Index Management interface. On the left is a sidebar with navigation links: Management, Ingest, Data, Index Management (selected), Index Lifecycle Policies, Snapshot and Restore, Rollup Jobs, Transforms, and Remote Clusters. The main content area is titled 'Index Management' and has tabs for Indices, Data Streams, Index Templates, and Component Templates. Below the tabs, there's a search bar and a table of indices. The table has columns: Name, Health, Status, Primaries, Replicas, Docs count, Storage size, and Data stream. One index is listed: 'sample_data' with a health of 'yellow', status of 'open', 1 primary, 1 replica, 33 docs, and 15.8kb storage.

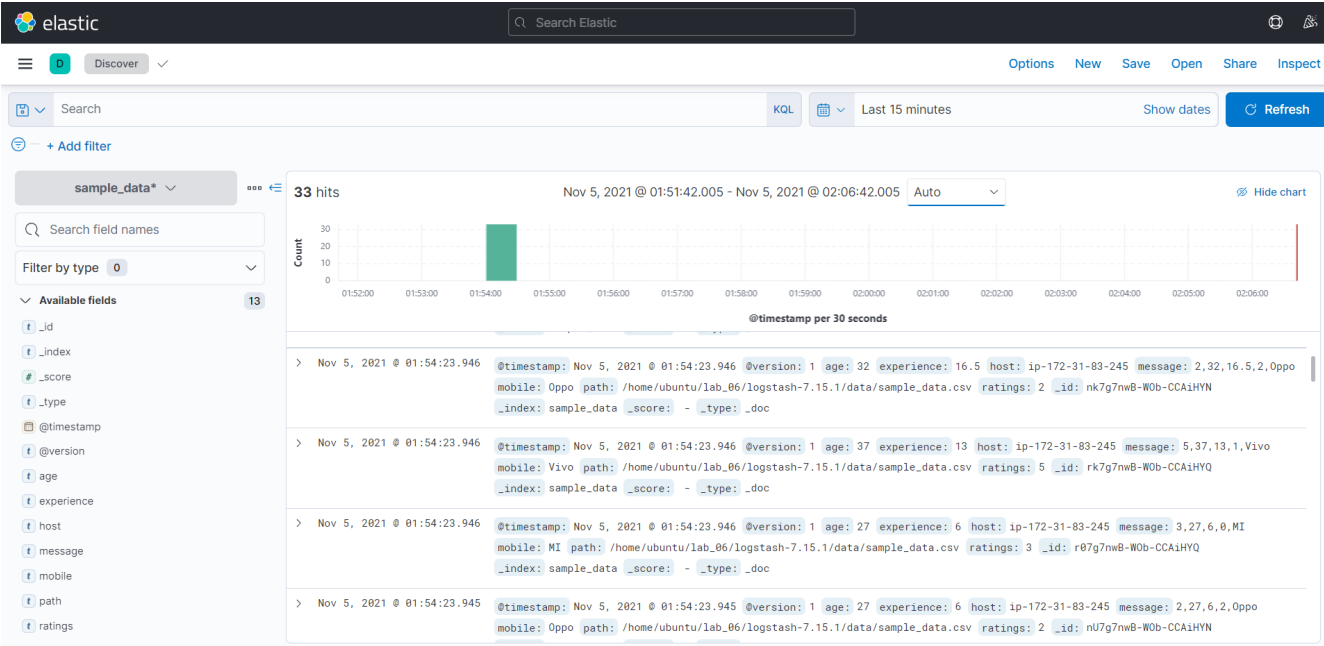
Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
sample_data	yellow	open	1	1	33	15.8kb	

- Create the Index Pattern

The screenshot shows the Kibana Index Patterns interface. On the left is a sidebar with navigation links: Snapshot and Restore, Rollup Jobs, Transforms, Remote Clusters, Alerts and Insights, Rules and Connectors, Reporting, Machine Learning Jobs, Kibana, Index Patterns (selected), Saved Objects, and Tools. The main content area is titled 'Index patterns' and has a 'Create index pattern' button. Below the title, there's a search bar with 'sample' entered. A table shows the index pattern 'sample_data*'. At the bottom, there's a 'Rows per page' dropdown set to 10 and a pagination link '1'.

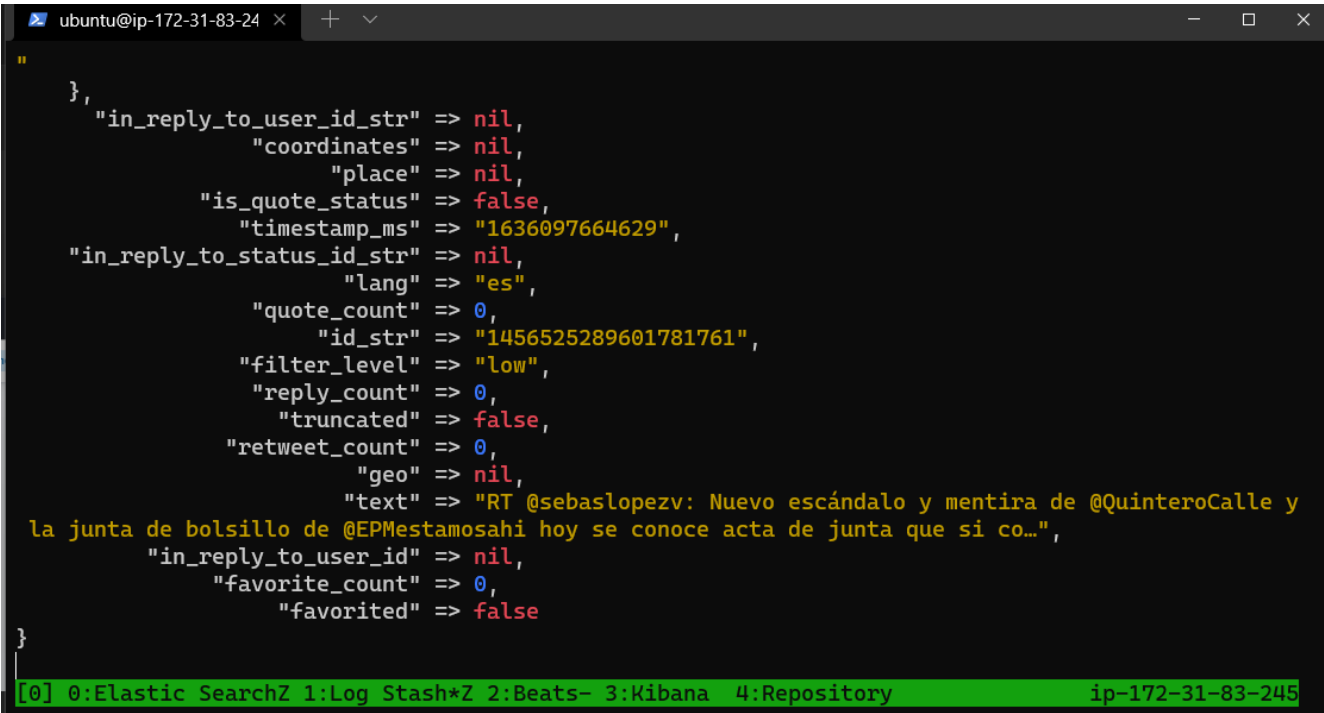
Pattern
sample_data*

- Inspect the data

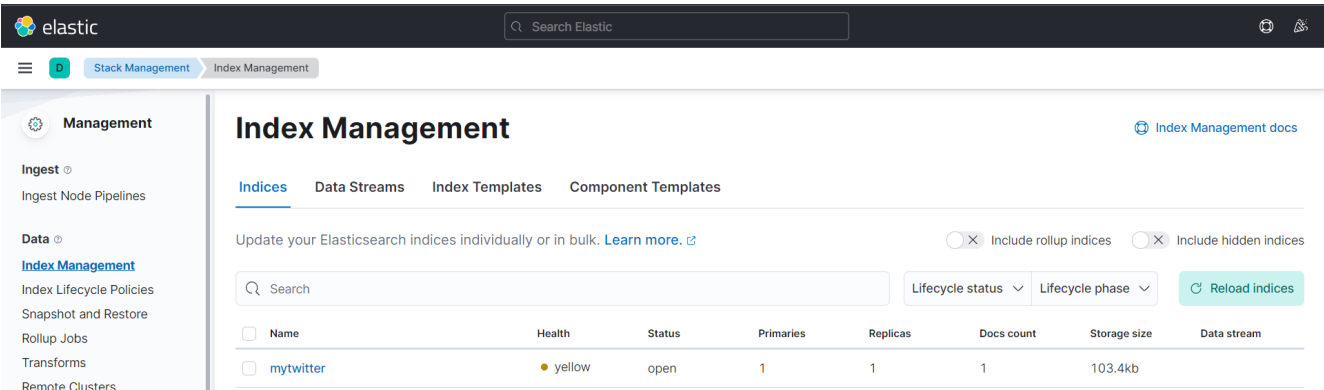


Twitter Feed

- LogStash with Twitter



- Kibana Twitter Index



- Create Twitter Index Pattern

The screenshot shows the 'Create index pattern' dialog in the Elastic Stack Management interface. The 'Name' field is set to 'mytwitter*'. A message states: 'Your index pattern matches 1 source.' The 'Timestamp field' dropdown is set to 'Select a timestamp field', with a note: 'No matching data stream, index, or index alias has a timestamp field.' The 'Rows per page' is set to 10. At the bottom, there are 'Close' and 'Create index pattern' buttons.

- Check Twitter Data

The screenshot shows the Elastic Discover search results for the 'mytwitter*' index pattern. The search bar shows 'mytwitter*' and '7 hits'. The left sidebar shows the 'Available fields' list, including '_id', '_index', '_score', '_type', 'created_at', 'display_text_range', 'entities.urls.display_url', 'entities.urls.expanded_url', 'entities.urls.indices', 'entities.urls.uri', and 'entities.user_mentions.id'. The main area displays three document hits. The first hit is a tweet from Daniel Quintero Calle. The second hit is a tweet from Sebastián López, Daniel Quintero Calle, and EPM estamos ahí. The third hit is a tweet from Daniel Quintero Calle that is a quote of another tweet.