**WORKSHOP 1 .- MONITOREO TWITTER**

# **INSTALAR JAVA**

OPCION 1.- utilizando apt-get

*$ sudo add-apt-repository ppa:webupd8team/java  
$ sudo apt-get update  
$ sudo apt-get install oracle-java8-installer*

OPCION 2.- Descarga de la pagina principal (www.java.com) el archivo jre-8u171-linux-x64.tar.gz para linux:

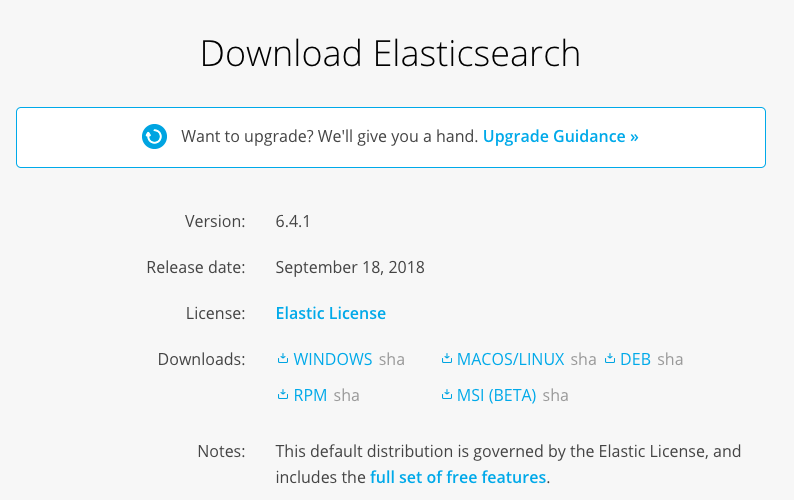
*$ sudo mkdir /usr/java  
$ sudo cp $HOME\_ARCHIVO\_GZ/jre-8u171-linux-x64.tar.gz /usr/java  
$ sudo /usr/java/tar xvfz jre-8u171-linux-x64.tar.gz  
$ sudo mv /usr/java/jre1.8.0\_171 /usr/java/jre  
$ sudo update-alternatives --install /usr/bin/java java /usr/java/jre/bin/java 100  
update-alternatives: using /usr/java/jre/bin/java to provide /usr/bin/java (java) in auto mode  
$ java -version  
java version "1.8.0\_171"  
Java(TM) SE Runtime Environment (build 1.8.0\_171-b11)  
Java HotSpot(TM) 64-Bit Server VM (build 25.171-b11, mixed mode)*

# **INSTALAR STACK ELASTIC**

## **ELASTICSEARCH:**

Descargamos el archivo para MACOS/LINUX de la pagina oficial de elastic.co:

<https://www.elastic.co/downloads/elasticsearch>



El archivo que descargamos tiene la extension .tar.gz, para descomprimirlo:

*$ ls*

*elasticsearch-6.4.1.tar.gz kibana-6.4.1-darwin-x86\_64.tar.gz logstash-6.4.1.tar.gz*

*$*

*$ tar -xvfz elasticsearch-6.4.1.tar.gz*

*x elasticsearch-6.4.1/*

*x elasticsearch-6.4.1/lib/*

*x elasticsearch-6.4.1/lib/elasticsearch-6.4.1.jar*

*x elasticsearch-6.4.1/lib/elasticsearch-x-content-6.4.1.jar*

*x elasticsearch-6.4.1/lib/elasticsearch-cli-6.4.1.jar*

*x elasticsearch-6.4.1/lib/elasticsearch-core-6.4.1.jar*

*x elasticsearch-6.4.1/lib/elasticsearch-secure-sm-6.4.1.jar*

*x elasticsearch-6.4.1/lib/lucene-core-7.4.0.jar*

*.*

*.*

*.*

*.*

*x elasticsearch-6.4.1/modules/x-pack-monitoring/NOTICE.txt*

*x elasticsearch-6.4.1/modules/x-pack-monitoring/elasticsearch-rest-client-sniffer-6.4.1.jar*

*x elasticsearch-6.4.1/modules/x-pack-monitoring/x-pack-monitoring-6.4.1.jar*

*x elasticsearch-6.4.1/plugins/*

*x elasticsearch-6.4.1/logs/*

*$*

Una vez descomprimido el archivo para arrancar el servicio de elasticsearch:

*$ ls*

*elasticsearch-6.4.1 kibana-6.4.1-darwin-x86\_64.tar.gz*

*elasticsearch-6.4.1.tar.gz logstash-6.4.1.tar.gz*

*$*

*$ cd elasticsearch-6.4.1*

*$ ls*

*LICENSE.txt NOTICE.txt README.textile bin config lib logs modules plugins*

*$*

*$ bin/elasticsearch*

*[2018-09-28T08:11:56,686][INFO ][o.e.n.Node ] [] initializing ...*

*[2018-09-28T08:11:56,812][INFO ][o.e.e.NodeEnvironment ] [\_Atq\_w9] using [1] data paths, mounts [[/ (/dev/disk1s1)]], net usable\_space [76.2gb], net total\_space [233.5gb], types [apfs]*

*[2018-09-28T08:11:56,812][INFO ][o.e.e.NodeEnvironment ] [\_Atq\_w9] heap size [990.7mb], compressed ordinary object pointers [true]*

*[2018-09-28T08:11:56,815][INFO ][o.e.n.Node ] [\_Atq\_w9] node name derived from node ID [\_Atq\_w9vS6yx6S5f47pHFw]; set [node.name] to override*

*[2018-09-28T08:11:56,816][INFO ][o.e.n.Node ] [\_Atq\_w9] version[6.4.1], pid[9910], build[default/tar/e36acdb/2018-09-13T22:18:07.696808Z], OS[Mac OS X/10.13.6/x86\_64], JVM[Oracle Corporation/Java HotSpot(TM) 64-Bit Server VM/1.8.0\_131/25.131-b11]*

*[2018-09-28T08:11:56,816][INFO ][o.e.n.Node ] [\_Atq\_w9] JVM arguments [-Xms1g, -Xmx1g, -XX:+UseConcMarkSweepGC, -XX:CMSInitiatingOccupancyFraction=75, -XX:+UseCMSInitiatingOccupancyOnly, -XX:+AlwaysPreTouch, -Xss1m, -Djava.awt.headless=true, -Dfile.encoding=UTF-8, -Djna.nosys=true, -XX:-OmitStackTraceInFastThrow, -Dio.netty.noUnsafe=true, -Dio.netty.noKeySetOptimization=true, -Dio.netty.recycler.maxCapacityPerThread=0, -Dlog4j.shutdownHookEnabled=false, -Dlog4j2.disable.jmx=true, -Djava.io.tmpdir=/var/folders/qv/zg2k0zyd6mzb2x421ktvrzlh0000gn/T/elasticsearch.6gWqwWvp, -XX:+HeapDumpOnOutOfMemoryError, -XX:HeapDumpPath=data, -XX:ErrorFile=logs/hs\_err\_pid%p.log, -XX:+PrintGCDetails, -XX:+PrintGCDateStamps, -XX:+PrintTenuringDistribution, -XX:+PrintGCApplicationStoppedTime, -Xloggc:logs/gc.log, -XX:+UseGCLogFileRotation, -XX:NumberOfGCLogFiles=32, -XX:GCLogFileSize=64m, -Des.path.home=/Users/sopgestion/elastic/6.4/elasticsearch-6.4.1, -Des.path.conf=/Users/sopgestion/elastic/6.4/elasticsearch-6.4.1/config, -Des.distribution.flavor=default, -Des.distribution.type=tar]*

*[2018-09-28T08:12:00,687][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [aggs-matrix-stats]*

*[2018-09-28T08:12:00,688][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [analysis-common]*

*[2018-09-28T08:12:00,689][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [ingest-common]*

*[2018-09-28T08:12:00,690][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [lang-expression]*

*[2018-09-28T08:12:00,690][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [lang-mustache]*

*[2018-09-28T08:12:00,690][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [lang-painless]*

*[2018-09-28T08:12:00,691][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [mapper-extras]*

*[2018-09-28T08:12:00,691][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [parent-join]*

*[2018-09-28T08:12:00,692][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [percolator]*

*[2018-09-28T08:12:00,692][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [rank-eval]*

*[2018-09-28T08:12:00,692][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [reindex]*

*[2018-09-28T08:12:00,692][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [repository-url]*

*[2018-09-28T08:12:00,693][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [transport-netty4]*

*[2018-09-28T08:12:00,693][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [tribe]*

*[2018-09-28T08:12:00,693][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [x-pack-core]*

*[2018-09-28T08:12:00,693][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [x-pack-deprecation]*

*[2018-09-28T08:12:00,693][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [x-pack-graph]*

*[2018-09-28T08:12:00,693][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [x-pack-logstash]*

*[2018-09-28T08:12:00,694][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [x-pack-ml]*

*[2018-09-28T08:12:00,694][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [x-pack-monitoring]*

*[2018-09-28T08:12:00,694][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [x-pack-rollup]*

*[2018-09-28T08:12:00,694][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [x-pack-security]*

*[2018-09-28T08:12:00,694][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [x-pack-sql]*

*[2018-09-28T08:12:00,695][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [x-pack-upgrade]*

*[2018-09-28T08:12:00,695][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] loaded module [x-pack-watcher]*

*[2018-09-28T08:12:00,695][INFO ][o.e.p.PluginsService ] [\_Atq\_w9] no plugins loaded*

*[2018-09-28T08:12:06,384][INFO ][o.e.x.s.a.s.FileRolesStore] [\_Atq\_w9] parsed [0] roles from file [/Users/sopgestion/elastic/6.4/elasticsearch-6.4.1/config/roles.yml]*

*[2018-09-28T08:12:07,425][INFO ][o.e.x.m.j.p.l.CppLogMessageHandler] [controller/9932] [Main.cc@109] controller (64 bit): Version 6.4.1 (Build 1df3104bc26648) Copyright (c) 2018 Elasticsearch BV*

*[2018-09-28T08:12:08,068][DEBUG][o.e.a.ActionModule ] Using REST wrapper from plugin org.elasticsearch.xpack.security.Security*

*[2018-09-28T08:12:08,380][INFO ][o.e.d.DiscoveryModule ] [\_Atq\_w9] using discovery type [zen]*

*[2018-09-28T08:12:09,894][INFO ][o.e.n.Node ] [\_Atq\_w9] initialized*

*[2018-09-28T08:12:09,895][INFO ][o.e.n.Node ] [\_Atq\_w9] starting ...*

*[2018-09-28T08:12:10,163][INFO ][o.e.t.TransportService ] [\_Atq\_w9] publish\_address {127.0.0.1:9300}, bound\_addresses {[::1]:9300}, {127.0.0.1:9300}, {127.94.0.1:9300}*

*[2018-09-28T08:12:13,245][INFO ][o.e.c.s.MasterService ] [\_Atq\_w9] zen-disco-elected-as-master ([0] nodes joined)[, ], reason: new\_master {\_Atq\_w9}{\_Atq\_w9vS6yx6S5f47pHFw}{Kbo1uQaqROqFvnSZaEaK5Q}{127.0.0.1}{127.0.0.1:9300}{ml.machine\_memory=4294967296, xpack.installed=true, ml.max\_open\_jobs=20, ml.enabled=true}*

*[2018-09-28T08:12:13,252][INFO ][o.e.c.s.ClusterApplierService] [\_Atq\_w9] new\_master {\_Atq\_w9}{\_Atq\_w9vS6yx6S5f47pHFw}{Kbo1uQaqROqFvnSZaEaK5Q}{127.0.0.1}{127.0.0.1:9300}{ml.machine\_memory=4294967296, xpack.installed=true, ml.max\_open\_jobs=20, ml.enabled=true}, reason: apply cluster state (from master [master {\_Atq\_w9}{\_Atq\_w9vS6yx6S5f47pHFw}{Kbo1uQaqROqFvnSZaEaK5Q}{127.0.0.1}{127.0.0.1:9300}{ml.machine\_memory=4294967296, xpack.installed=true, ml.max\_open\_jobs=20, ml.enabled=true} committed version [1] source [zen-disco-elected-as-master ([0] nodes joined)[, ]]])*

*[2018-09-28T08:12:13,295][INFO ][o.e.x.s.t.n.SecurityNetty4HttpServerTransport] [\_Atq\_w9] publish\_address {127.0.0.1:9200}, bound\_addresses {[::1]:9200}, {127.0.0.1:9200}, {127.94.0.1:9200}*

*[2018-09-28T08:12:13,296][INFO ][o.e.n.Node ] [\_Atq\_w9] started*

*[2018-09-28T08:12:13,316][WARN ][o.e.x.s.a.s.m.NativeRoleMappingStore] [\_Atq\_w9] Failed to clear cache for realms [[]]*

*[2018-09-28T08:12:13,513][INFO ][o.e.g.GatewayService ] [\_Atq\_w9] recovered [0] indices into cluster\_state*

*[2018-09-28T08:12:13,786][INFO ][o.e.c.m.MetaDataIndexTemplateService] [\_Atq\_w9] adding template [.triggered\_watches] for index patterns [.triggered\_watches\*]*

*[2018-09-28T08:12:13,828][INFO ][o.e.c.m.MetaDataIndexTemplateService] [\_Atq\_w9] adding template [.watches] for index patterns [.watches\*]*

*[2018-09-28T08:12:13,909][INFO ][o.e.c.m.MetaDataIndexTemplateService] [\_Atq\_w9] adding template [.watch-history-9] for index patterns [.watcher-history-9\*]*

*[2018-09-28T08:12:13,952][INFO ][o.e.c.m.MetaDataIndexTemplateService] [\_Atq\_w9] adding template [.monitoring-logstash] for index patterns [.monitoring-logstash-6-\*]*

*[2018-09-28T08:12:14,014][INFO ][o.e.c.m.MetaDataIndexTemplateService] [\_Atq\_w9] adding template [.monitoring-es] for index patterns [.monitoring-es-6-\*]*

*[2018-09-28T08:12:14,055][INFO ][o.e.c.m.MetaDataIndexTemplateService] [\_Atq\_w9] adding template [.monitoring-beats] for index patterns [.monitoring-beats-6-\*]*

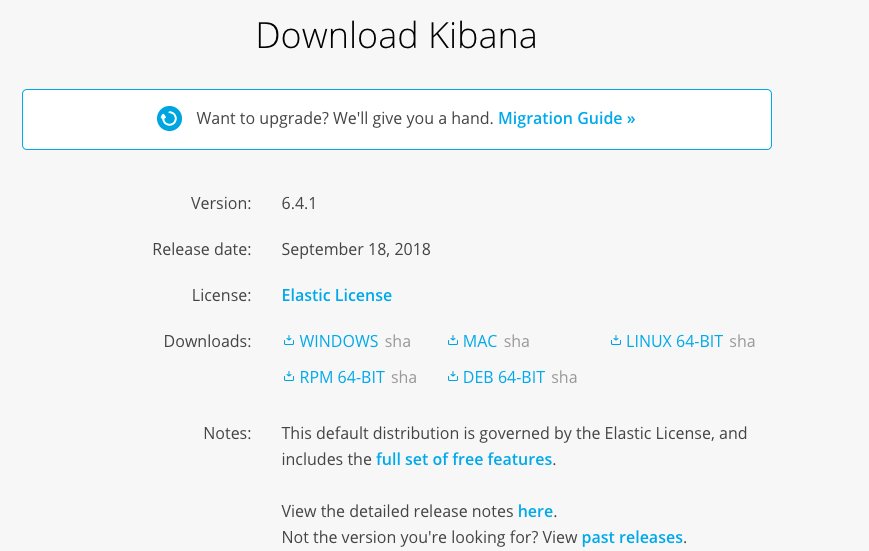
*[2018-09-28T08:12:14,090][INFO ][o.e.c.m.MetaDataIndexTemplateService] [\_Atq\_w9] adding template [.monitoring-alerts] for index patterns [.monitoring-alerts-6]*

*[2018-09-28T08:12:14,126][INFO ][o.e.c.m.MetaDataIndexTemplateService] [\_Atq\_w9] adding template [.monitoring-kibana] for index patterns [.monitoring-kibana-6-\*]*

*[2018-09-28T08:12:14,322][INFO ][o.e.l.LicenseService ] [\_Atq\_w9] license [3449cab8-b3ce-471e-950b-0b8243b429c6] mode [basic] - valid*

## **KIBANA**

<https://www.elastic.co/downloads/kibana>



Para este ejemplo, estoy descargando kibana para MAC, pero se puede observer que hay un instalador para linux, windows, e incluso paquetes debian.

*$ tar xvfz kibana-6.4.1-darwin-x86\_64.tar.gzx*

*x kibana-6.4.1-darwin-x86\_64/*

*x kibana-6.4.1-darwin-x86\_64/LICENSE.txt*

*x kibana-6.4.1-darwin-x86\_64/README.txt*

*x kibana-6.4.1-darwin-x86\_64/bin/*

*x kibana-6.4.1-darwin-x86\_64/bin/kibana-keystore*

*x kibana-6.4.1-darwin-x86\_64/bin/kibana-plugin*

*x kibana-6.4.1-darwin-x86\_64/bin/kibana*

*x kibana-6.4.1-darwin-x86\_64/package.json*

*x kibana-6.4.1-darwin-x86\_64/config/*

*x kibana-6.4.1-darwin-x86\_64/config/kibana.yml*

*x kibana-6.4.1-darwin-x86\_64/node/*

*x kibana-6.4.1-darwin-x86\_64/node/CHANGELOG.md*

*.*

*.*

*.*

*.*

*x kibana-6.4.1-darwin-x86\_64/optimize/bundles/logout.style.css*

*x kibana-6.4.1-darwin-x86\_64/optimize/bundles/status\_page.entry.js*

*x kibana-6.4.1-darwin-x86\_64/optimize/bundles/stateSessionStorageRedirect.style.css*

*x kibana-6.4.1-darwin-x86\_64/optimize/bundles/commons.style.css*

*x kibana-6.4.1-darwin-x86\_64/optimize/bundles/login.style.css*

*x kibana-6.4.1-darwin-x86\_64/optimize/.babelcache.json*

*x kibana-6.4.1-darwin-x86\_64/yarn.lock*

*$*

Arrancamos Kibana:

sopgestions-MacBook-Air:6.4 sopgestion$ ls

elasticsearch-6.4.1 kibana-6.4.1-darwin-x86\_64 logstash-6.4.1.tar.gz

elasticsearch-6.4.1.tar.gz kibana-6.4.1-darwin-x86\_64.tar.gz

$

$

$ cd kibana-6.4.1-darwin-x86\_64

$ bin/kibana

log [13:50:28.708] [info][status][plugin:kibana@6.4.1] Status changed from uninitialized to green - Ready

log [13:50:28.764] [info][status][plugin:elasticsearch@6.4.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch

log [13:50:28.769] [info][status][plugin:xpack\_main@6.4.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch

log [13:50:28.776] [info][status][plugin:searchprofiler@6.4.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch

log [13:50:28.783] [info][status][plugin:ml@6.4.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch

log [13:50:28.849] [info][status][plugin:tilemap@6.4.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch

log [13:50:28.851] [info][status][plugin:watcher@6.4.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch

log [13:50:28.872] [info][status][plugin:license\_management@6.4.1] Status changed from uninitialized to green - Ready

log [13:50:28.875] [info][status][plugin:index\_management@6.4.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch

log [13:50:29.124] [info][status][plugin:timelion@6.4.1] Status changed from uninitialized to green - Ready

log [13:50:29.127] [info][status][plugin:graph@6.4.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch

log [13:50:29.138] [info][status][plugin:monitoring@6.4.1] Status changed from uninitialized to green - Ready

log [13:50:29.141] [warning][security] Generating a random key for xpack.security.encryptionKey. To prevent sessions from being invalidated on restart, please set xpack.security.encryptionKey in kibana.yml

log [13:50:29.145] [warning][security] Session cookies will be transmitted over insecure connections. This is not recommended.

log [13:50:29.155] [info][status][plugin:security@6.4.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch

log [13:50:29.186] [info][status][plugin:grokdebugger@6.4.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch

log [13:50:29.193] [info][status][plugin:dashboard\_mode@6.4.1] Status changed from uninitialized to green - Ready

log [13:50:29.197] [info][status][plugin:logstash@6.4.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch

log [13:50:29.230] [info][status][plugin:apm@6.4.1] Status changed from uninitialized to green - Ready

log [13:50:29.240] [info][status][plugin:console@6.4.1] Status changed from uninitialized to green - Ready

log [13:50:29.246] [info][status][plugin:console\_extensions@6.4.1] Status changed from uninitialized to green - Ready

log [13:50:29.251] [info][status][plugin:notifications@6.4.1] Status changed from uninitialized to green - Ready

log [13:50:29.257] [info][status][plugin:metrics@6.4.1] Status changed from uninitialized to green - Ready

log [13:50:30.680] [warning][reporting] Generating a random key for xpack.reporting.encryptionKey. To prevent pending reports from failing on restart, please set xpack.reporting.encryptionKey in kibana.yml

log [13:50:30.683] [info][status][plugin:reporting@6.4.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch

log [13:50:31.595] [info][status][plugin:elasticsearch@6.4.1] Status changed from yellow to green - Ready

log [13:50:32.030] [info][license][xpack] Imported license information from Elasticsearch for the [data] cluster: mode: basic | status: active

log [13:50:32.043] [info][status][plugin:xpack\_main@6.4.1] Status changed from yellow to green - Ready

log [13:50:32.045] [info][status][plugin:searchprofiler@6.4.1] Status changed from yellow to green - Ready

log [13:50:32.046] [info][status][plugin:ml@6.4.1] Status changed from yellow to green - Ready

log [13:50:32.046] [info][status][plugin:tilemap@6.4.1] Status changed from yellow to green - Ready

log [13:50:32.047] [info][status][plugin:watcher@6.4.1] Status changed from yellow to green - Ready

log [13:50:32.048] [info][status][plugin:index\_management@6.4.1] Status changed from yellow to green - Ready

log [13:50:32.049] [info][status][plugin:graph@6.4.1] Status changed from yellow to green - Ready

log [13:50:32.058] [info][status][plugin:grokdebugger@6.4.1] Status changed from yellow to green - Ready

log [13:50:32.059] [info][status][plugin:logstash@6.4.1] Status changed from yellow to green - Ready

log [13:50:32.060] [info][status][plugin:reporting@6.4.1] Status changed from yellow to green - Ready

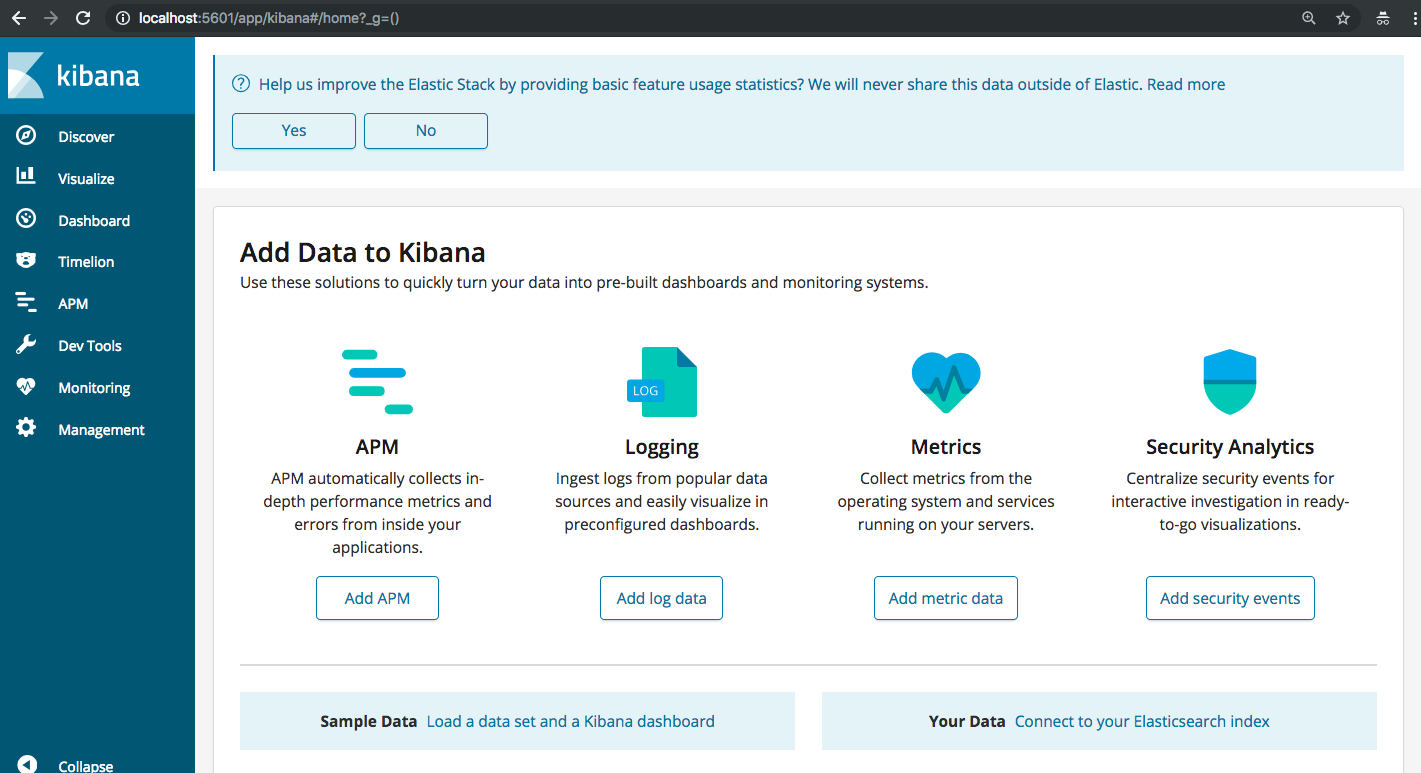
log [13:50:32.061] [info][kibana-monitoring][monitoring-ui] Starting monitoring stats collection

log [13:50:32.068] [info][status][plugin:security@6.4.1] Status changed from yellow to green - Ready

log [13:50:32.781] [info][license][xpack] Imported license information from Elasticsearch for the [monitoring] cluster: mode: basic | status: active

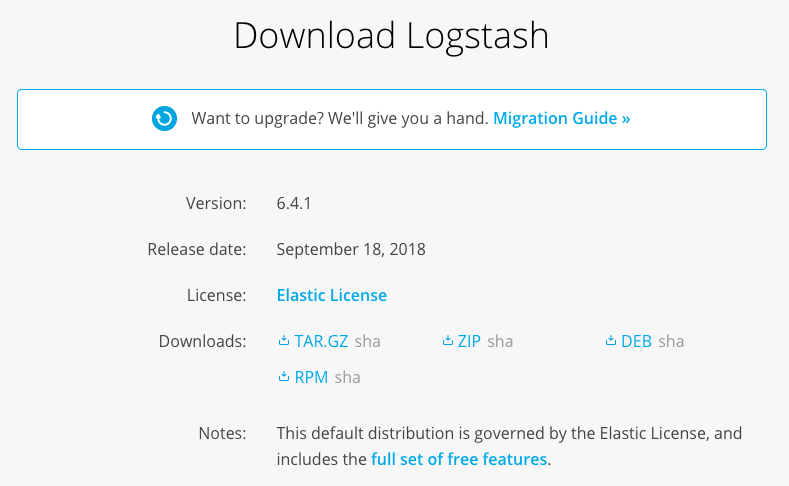
log [13:50:33.523] [info][listening][server][http] Server running at http://localhost:5601

Validamos que se encuentre arriba: accesamos a <http://localhost:5601>



**LOGSTASH:**

<https://www.elastic.co/downloads/logstash>



*$ pwd*

*/Users/sopgestion/elastic/6.4*

*$ tar xvfz logstash-6.4.1.tar.gz*

*$ tar xvfz logstash-6.4.1.tar.gz*

*x logstash-6.4.1/NOTICE.TXT*

*x logstash-6.4.1/CONTRIBUTORS*

*x logstash-6.4.1/bin/benchmark.sh*

*x logstash-6.4.1/bin/cpdump*

*x logstash-6.4.1/bin/dependencies-report*

*x logstash-6.4.1/bin/ingest-convert.sh*

*x logstash-6.4.1/bin/logstash*

*.*

*.*

*.*

*.*

*.*

*x logstash-6.4.1/x-pack/src/test*

*x logstash-6.4.1/x-pack/src/test/java*

*x logstash-6.4.1/x-pack/src/test/java/org*

*x logstash-6.4.1/x-pack/src/test/java/org/logstash*

*x logstash-6.4.1/x-pack/src/test/java/org/logstash/xpack*

*x logstash-6.4.1/x-pack/src/test/java/org/logstash/xpack/test*

*x logstash-6.4.1/x-pack/src/test/java/org/logstash/xpack/test/RSpecIntegrationTests.java*

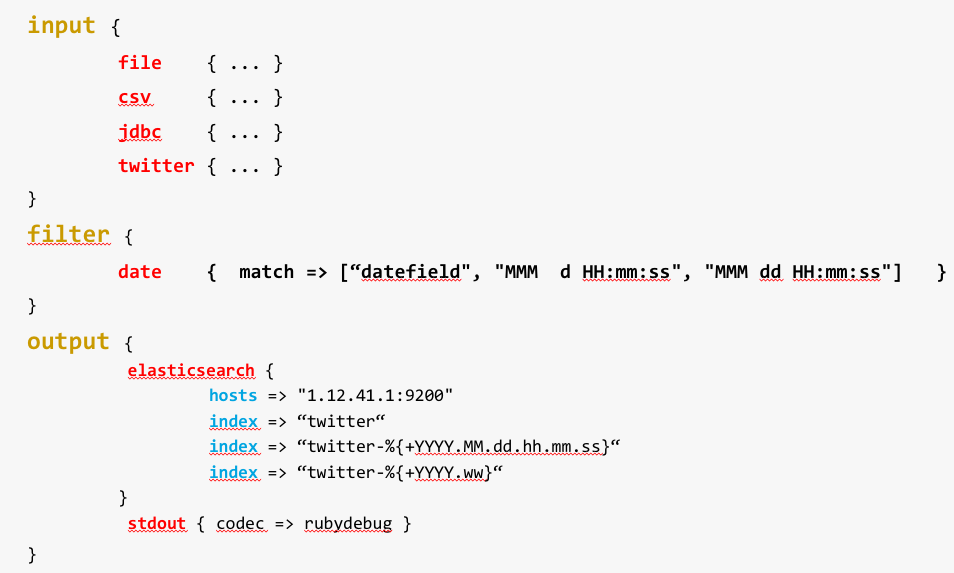
*x logstash-6.4.1/x-pack/src/test/java/org/logstash/xpack/test/RSpecTests.java*

*x logstash-6.4.1/LICENSE.txt*

*x logstash-6.4.1/logstash-core/lib/logstash/build.rb*

*$*

Para arrancarlo primero tenemos que definir un archivo de configuracion, en logstash existen 3 principales secciones, input que es de donde voy a tomar mi informacion, filter que es como voy a tratar los datos o modificarlos, output como voy a tratar la salida.

**

En el caso de twitter ocuparemos el plugin de input ya existente, mayor informacion: <https://www.elastic.co/guide/en/logstash/current/plugins-inputs-twitter.html>

Creamos un archivo que se llame twitter.conf y agregamos las siguientes lineas:

input {

twitter {

consumer\_key => "CopiarConsumerKey"

consumer\_secret => "CopiarConsumerSecret"

oauth\_token => "CopiarAccessToken"

oauth\_token\_secret => "CopiarAccessTokenSecret"

#follows => ["10946302", " 84512601", "149344048" ]

keywords => [ "oaxaca", "ask\_elastic", "elastic", "meetup" ]

full\_tweet => true

}

}

filter {

}

output {

stdout { codec => rubydebug }

}

Para inicializarlo:

*$ bin/logstash -f ./twitter.conf*

*Sending Logstash logs to /Users/sopgestion/elastic/6.4/logstash-6.4.1/logs which is now configured via log4j2.properties*

*[2018-09-28T09:56:10,725][WARN ][logstash.config.source.multilocal] Ignoring the 'pipelines.yml' file because modules or command line options are specified*

*[2018-09-28T09:56:12,367][INFO ][logstash.runner ] Starting Logstash {"logstash.version"=>"6.4.1"}*

*[2018-09-28T09:56:19,198][INFO ][logstash.pipeline ] Starting pipeline {:pipeline\_id=>"main", "pipeline.workers"=>4, "pipeline.batch.size"=>125, "pipeline.batch.delay"=>50}*

*[2018-09-28T09:56:19,831][INFO ][logstash.pipeline ] Pipeline started successfully {:pipeline\_id=>"main", :thread=>"#<Thread:0x5d1d330c run>"}*

*[2018-09-28T09:56:19,882][INFO ][logstash.inputs.twitter ] Starting twitter tracking {:track=>"3erTechDay,ask\_elastic,elastic,meetup"}*

*[2018-09-28T09:56:19,956][INFO ][logstash.agent ] Pipelines running {:count=>1, :running\_pipelines=>[:main], :non\_running\_pipelines=>[]}*

*[2018-09-28T09:56:20,885][INFO ][logstash.agent ] Successfully started Logstash API endpoint {:port=>9600}*

*En cuanto algun twitt corresponde con los parametros de filtrado podemos verlo en un format json como a continuacion:*

*{*

*"text" => "RT @JaredSawyerJr: From now on, Try to schedule your month with these:\n-1 Lunch date w/ a friend\n-24 hrs no Social Media\n-1 Day Outdoors\n-1…",*

*"place" => nil,*

*"in\_reply\_to\_status\_id\_str" => nil,*

*"id\_str" => "1045688700527468544",*

*"favorited" => false,*

*"id" => 1045688700527468544,*

*"in\_reply\_to\_user\_id" => nil,*

*"retweeted" => false,*

*"user" => {*

*"profile\_link\_color" => "DD2E44",*

*"id\_str" => "2228028259",*

*"id" => 2228028259,*

*"screen\_name" => "suhailasue\_",*

*"favourites\_count" => 25559,*

*"profile\_sidebar\_border\_color" => "000000",*

*"default\_profile\_image" => false,*

*"following" => nil,*

*"time\_zone" => nil,*

*"followers\_count" => 446,*

*"utc\_offset" => nil,*

*"profile\_text\_color" => "333333",*

*"default\_profile" => false,*

*"contributors\_enabled" => false,*

*"name" => "sue #TUR18",*

*"created\_at" => "Tue Dec 03 09:33:46 +0000 2013",*

*"protected" => false,*

*"profile\_background\_image\_url\_https" => "https://abs.twimg.com/images/themes/theme1/bg.png",*

*"profile\_image\_url" => "http://pbs.twimg.com/profile\_images/983522453170274304/vBoO1Bz6\_normal.jpg",*

*"profile\_banner\_url" => "https://pbs.twimg.com/profile\_banners/2228028259/1492652710",*

*"translator\_type" => "none",*

*"profile\_use\_background\_image" => true,*

*"description" => "Twenty two. IIUM. Najmi ✨",*

*"statuses\_count" => 20952,*

*"profile\_background\_image\_url" => "http://abs.twimg.com/images/themes/theme1/bg.png",*

*"follow\_request\_sent" => nil,*

*"notifications" => nil,*

*"location" => "kota bharu, kelantan",*

*"friends\_count" => 396,*

*"profile\_sidebar\_fill\_color" => "DDEEF6",*

*"url" => nil,*

*"profile\_background\_color" => "F5ABB5",*

*"verified" => false,*

*"geo\_enabled" => true,*

*"profile\_background\_tile" => true,*

*"profile\_image\_url\_https" => "https://pbs.twimg.com/profile\_images/983522453170274304/vBoO1Bz6\_normal.jpg",*

*"is\_translator" => false,*

*"lang" => "en",*

*"listed\_count" => 1*

*},*

*"favorite\_count" => 0,*

*"entities" => {*

*"user\_mentions" => [*

*[0] {*

*"screen\_name" => "JaredSawyerJr",*

*"indices" => [*

*[0] 3,*

*[1] 17*

*],*

*"id\_str" => "373432520",*

*"name" => "Jared Sawyer Jr.",*

*"id" => 373432520*

*}*

*],*

*"hashtags" => [],*

*"symbols" => [],*

*"urls" => []*

*},*

*"timestamp\_ms" => "1538146588819",*

*"contributors" => nil,*

*"created\_at" => "Fri Sep 28 14:56:28 +0000 2018",*

*"source" => "<a href=\"http://twitter.com/download/android\" rel=\"nofollow\">Twitter for Android</a>",*

*"geo" => nil,*

*"quote\_count" => 0,*

*"in\_reply\_to\_status\_id" => nil,*

*"in\_reply\_to\_user\_id\_str" => nil,*

*"coordinates" => nil,*

*"@version" => "1",*

*"in\_reply\_to\_screen\_name" => nil,*

*"filter\_level" => "low",*

*"retweet\_count" => 0,*

*"is\_quote\_status" => false,*

*"retweeted\_status" => {*

*"text" => "From now on, Try to schedule your month with these:\n-1 Lunch date w/ a friend\n-24 hrs no Social Media\n-1 Day Outdoo… https://t.co/txK8c1L9Eb",*

*"place" => nil,*

*"in\_reply\_to\_status\_id\_str" => nil,*

*"id\_str" => "1042518705324929025",*

*"favorited" => false,*

*"id" => 1042518705324929025,*

*"in\_reply\_to\_user\_id" => nil,*

*"extended\_tweet" => {*

*"display\_text\_range" => [*

*[0] 0,*

*[1] 277*

*],*

*"entities" => {*

*"user\_mentions" => [],*

*"hashtags" => [],*

*"symbols" => [],*

*"urls" => []*

*},*

*"full\_text" => "From now on, Try to schedule your month with these:\n-1 Lunch date w/ a friend\n-24 hrs no Social Media\n-1 Day Outdoors\n-1 Night Out w/ friends\n-1 Date Night (even w/ just yourself)\n-1 Breakfast Meetup w/ Friends\n-1 Movie NIght\n-1 Day Serving Others\n-1 Day completely to yourself"*

*},*

*"retweeted" => false,*

*"user" => {*

*"profile\_link\_color" => "0084B4",*

*"id\_str" => "373432520",*

*"id" => 373432520,*

*"screen\_name" => "JaredSawyerJr",*

*"favourites\_count" => 5711,*

*"profile\_sidebar\_border\_color" => "000000",*

*"default\_profile\_image" => false,*

*"following" => nil,*

*"time\_zone" => nil,*

*"followers\_count" => 56640,*

*"utc\_offset" => nil,*

*"profile\_text\_color" => "333333",*

*"default\_profile" => false,*

*"contributors\_enabled" => false,*

*"name" => "Jared Sawyer Jr.",*

*"created\_at" => "Wed Sep 14 15:31:36 +0000 2011",*

*"protected" => false,*

*"profile\_background\_image\_url\_https" => "https://abs.twimg.com/images/themes/theme1/bg.png",*

*"profile\_image\_url" => "http://pbs.twimg.com/profile\_images/998512442966663169/5k\_fyWyp\_normal.jpg",*

*"profile\_banner\_url" => "https://pbs.twimg.com/profile\_banners/373432520/1526896481",*

*"translator\_type" => "none",*

*"profile\_use\_background\_image" => true,*

*"description" => "🙏🏾 20 year old Preacher 🎬 Actor 📍 Atlanta 📚 #1 Bestselling Author of 4 books 📺 Host of New TV Show “Empower Today” debuting fall 2018",*

*"statuses\_count" => 15706,*

*"profile\_background\_image\_url" => "http://abs.twimg.com/images/themes/theme1/bg.png",*

*"follow\_request\_sent" => nil,*

*"notifications" => nil,*

*"location" => nil,*

*"friends\_count" => 43060,*

*"profile\_sidebar\_fill\_color" => "DDEEF6",*

*"url" => "http://www.jaredsawyerjr.com",*

*"profile\_background\_color" => "C0DEED",*

*"verified" => true,*

*"geo\_enabled" => false,*

*"profile\_background\_tile" => true,*

*"profile\_image\_url\_https" => "https://pbs.twimg.com/profile\_images/998512442966663169/5k\_fyWyp\_normal.jpg",*

*"is\_translator" => false,*

*"lang" => "en",*

*"listed\_count" => 230*

*},*

*"favorite\_count" => 41716,*

*"entities" => {*

*"user\_mentions" => [],*

*"hashtags" => [],*

*"symbols" => [],*

*"urls" => [*

*[0] {*

*"indices" => [*

*[0] 117,*

*[1] 140*

*],*

*"display\_url" => "twitter.com/i/web/status/1…",*

*"url" => "https://t.co/txK8c1L9Eb",*

*"expanded\_url" => "https://twitter.com/i/web/status/1042518705324929025"*

*}*

*]*

*},*

*"contributors" => nil,*

*"created\_at" => "Wed Sep 19 21:00:03 +0000 2018",*

*"source" => "<a href=\"http://www.crowdfireapp.com\" rel=\"nofollow\">Crowdfire - Go Big</a>",*

*"geo" => nil,*

*"quote\_count" => 1430,*

*"in\_reply\_to\_status\_id" => nil,*

*"in\_reply\_to\_user\_id\_str" => nil,*

*"coordinates" => nil,*

*"in\_reply\_to\_screen\_name" => nil,*

*"filter\_level" => "low",*

*"retweet\_count" => 19903,*

*"is\_quote\_status" => false,*

*"reply\_count" => 130,*

*"truncated" => true,*

*"lang" => "en"*

*},*

*"reply\_count" => 0,*

*"@timestamp" => 2018-09-28T14:56:28.000Z,*

*"truncated" => false,*

*"lang" => "en"*

*}*

El plugin stdout nos servira para analizar que las llaves de twitter este correctamente dadas de alta y se interprete todo correctamente, lo que prosigue es direccionar la salida a elasticsearch, para esto agregamos dentro de output las siguientes lineas

elasticsearch {

hosts => "http://localhost:9200"

# EJEMPLOS INDICES

index => "twitter-%{+YYYY.MM.dd}"

#index => "twitter-%{+YYYY.ww}"

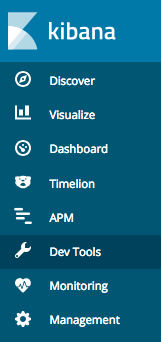
#index => "twitter-%{+YYYY.MM.dd.hh}"

#index => "twitter-%{+YYYY.MM.dd.hh.mm}"

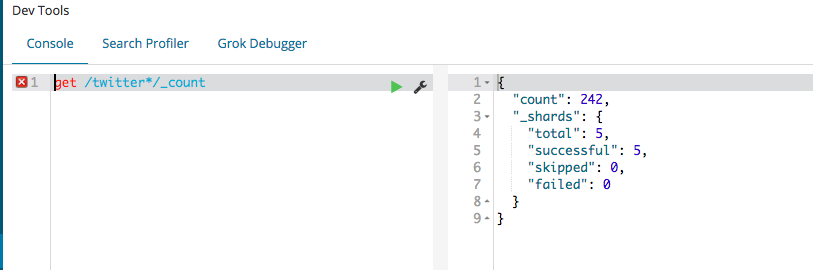
#index => "twitter-%{+YYYY.MM.dd.hh.mm.ss}"

}

Y volvemos a arrancar el servicio como se mostro anteriormente. Para validar que tenemos informacion podemos accesar a kibana en devtools:



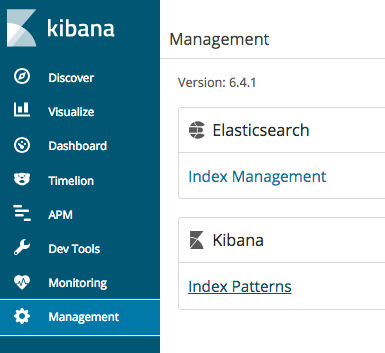
Dev Tools: es una herramienta que nos permite iteractuar con peticiones http, al abrirlo podemos hacer consultas, es como la consola de twitter, dentro podemos escribir el siguiente comando:



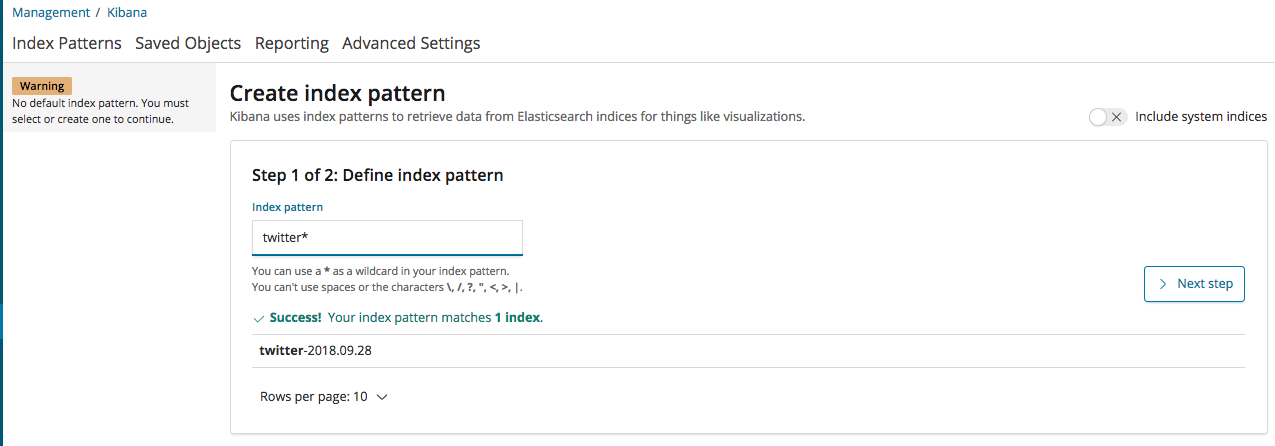
Lo que faltaria seria agregar el indice dentro de kibana para empezar a realizar las primeras visualizaciones y dashboards:

CREAR INDICE EN KIBANA:

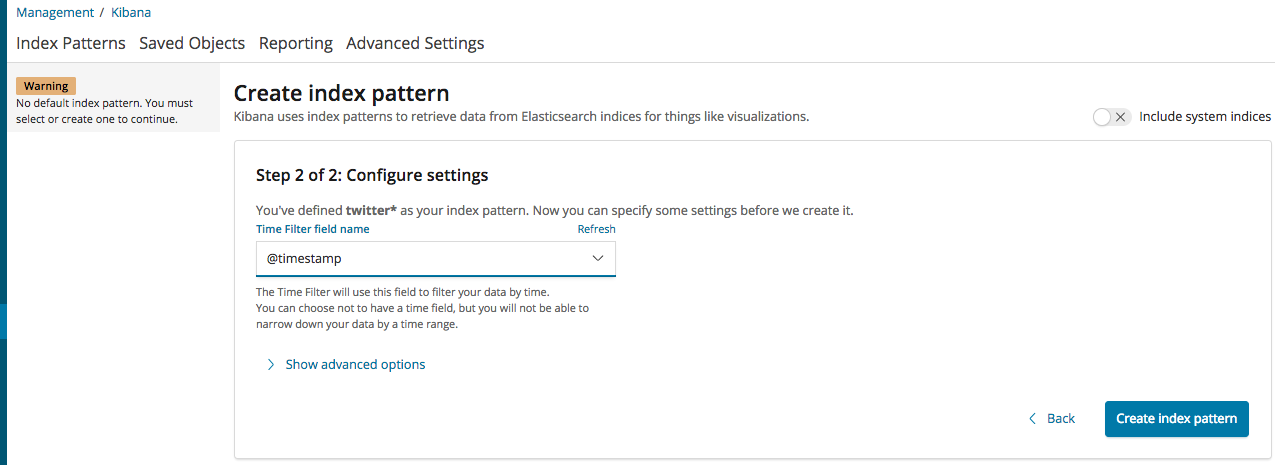
Para crear nuestro indice, debemos de accesar a Managment, en la seccion Kibana click en IndexPatterns:

Al crear un index pattern podemos accesar desde las diferentes herramientas como Discover a la informacion que esta indexada, en este caso recordemos que vamos a crear un indice por dia para el proyecto de twitter, al crearlo sugiero que lo den de alta como twitter-\* , el asterisco es un wildcard para especificar que no importa lo que venga despues de twitter-

Al accesar a IndexPattern podran ver una especie de wizard, que te indica como dar de alta tu indice:



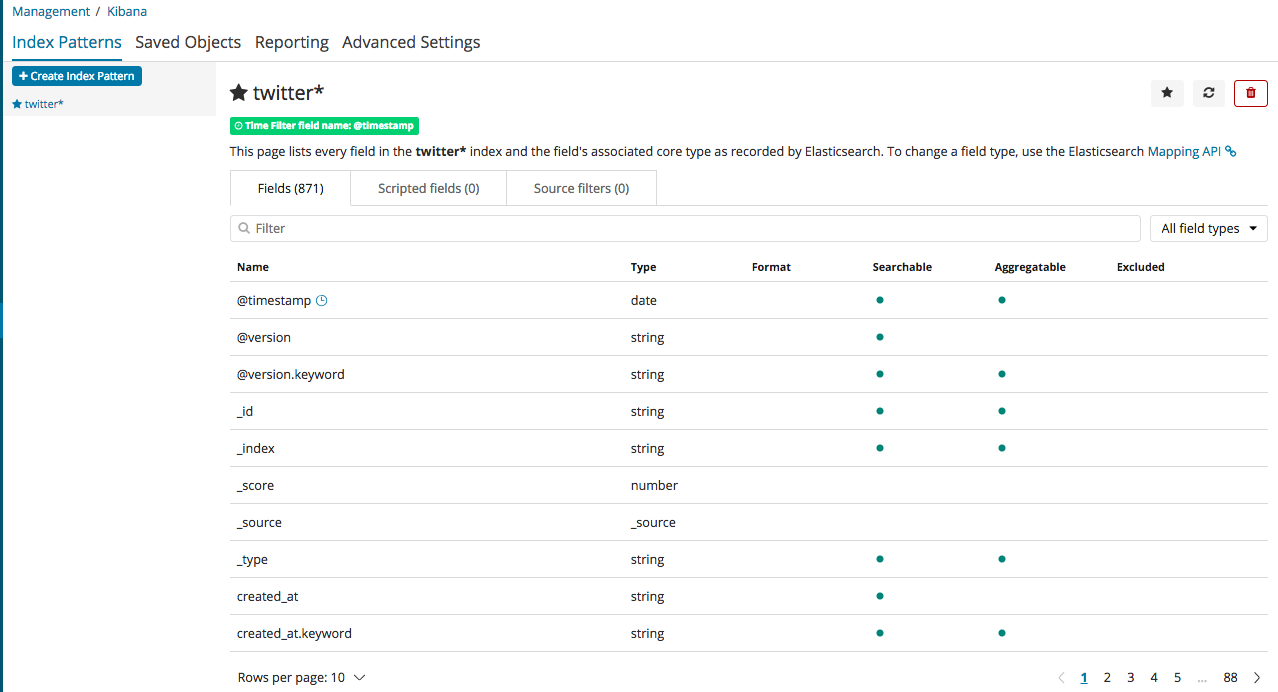
Como puedes observar el index pattern encontro un match, o un indice que corresponde con la busqueda, en este caso twitter-2018.09.28, damos click Next Step



Aquí definimos si queremos un indice donde podamos filtrar por fechas o tomar toda la informacion que se genere en ese indice, es decir no importa si tienes algun filtro por fecha en la selección de kibana, este indice tomara todos los datos.

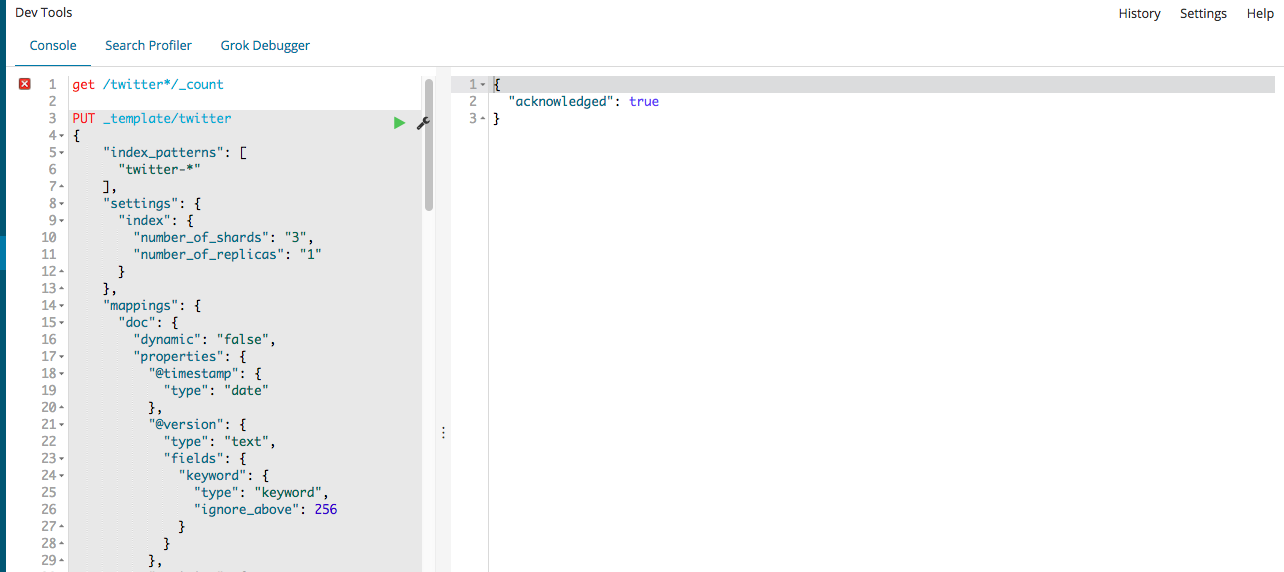
En este caso tomaremos como fecha el campo @timestamp, este campo es el que se genera automaticamente al indexar un documento o registro, tambien es el que ayuda a definir el patron del indice, me refiero a la parte que viene del lado derecho que definimos como YYYY.MM.dd en el nombre del indice, si los datos contienen algun campo con fecha podemos seleccionar ese como el que defina el filtro.

Al temrinar damos click en Create index pattern y observaremos que del lado izquierdo se crea el indice:

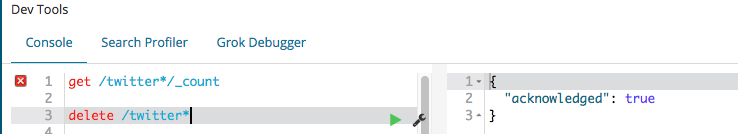


Para este caso como puedes observar cada campo que se indexa se agrega, el problema con twitter es que podemos llegar a tener mas de 1000 campos y esto ya es un problema porque apartir de la version 4.6 los indices estan definidos como maximos 1200 campos, ademas de que las busquedas se ven afectadas, para esto lo que podemos hacer es crear un template, para eso ocupamos el archivo template: template\_twitter.txt:

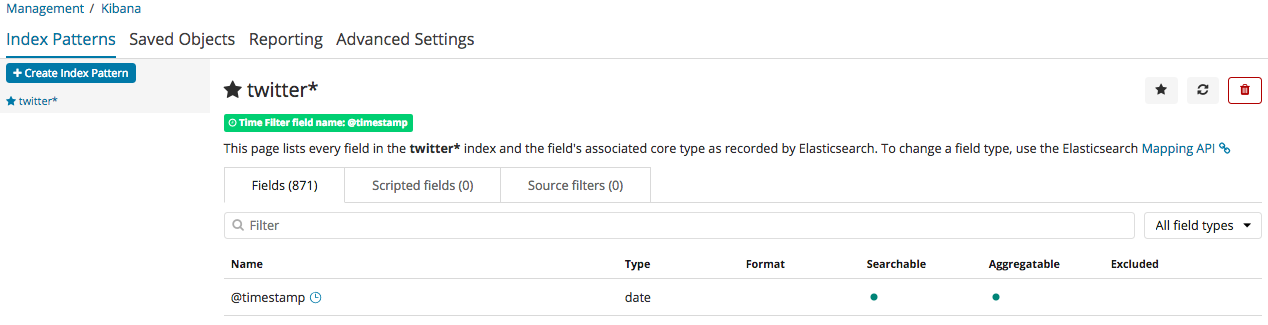
Copiamos el contenido a Dev Tools, le damos en play y se debe de visualizar de la siguiente manera:

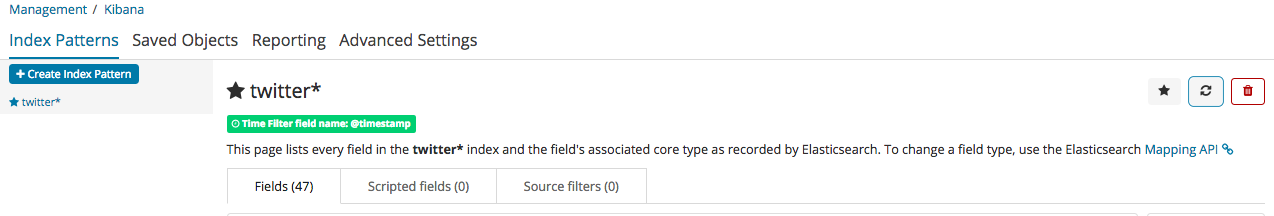


Borramos el indice que creamos:



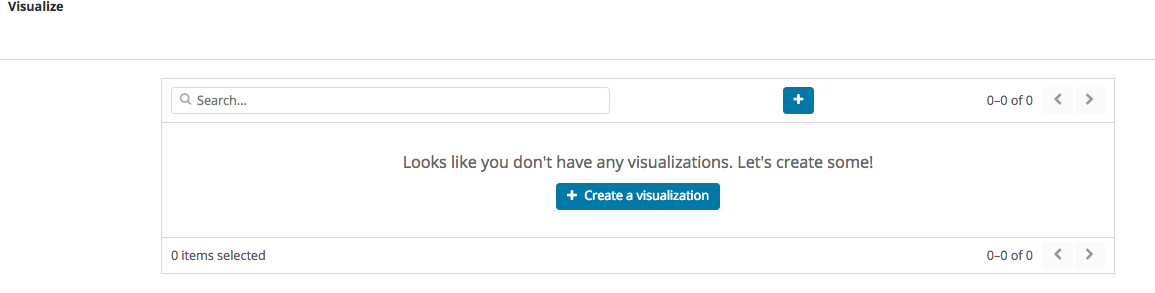
Y volvemos a arrancar logstash, con esto provocamos que se vuelva a crear el indice, pero ahora solo tomara la informacion que pusimos en el template. Ya solo queda hacer refresh en index patterns dentro de managment, y veremos que el numero de campos se reduce:



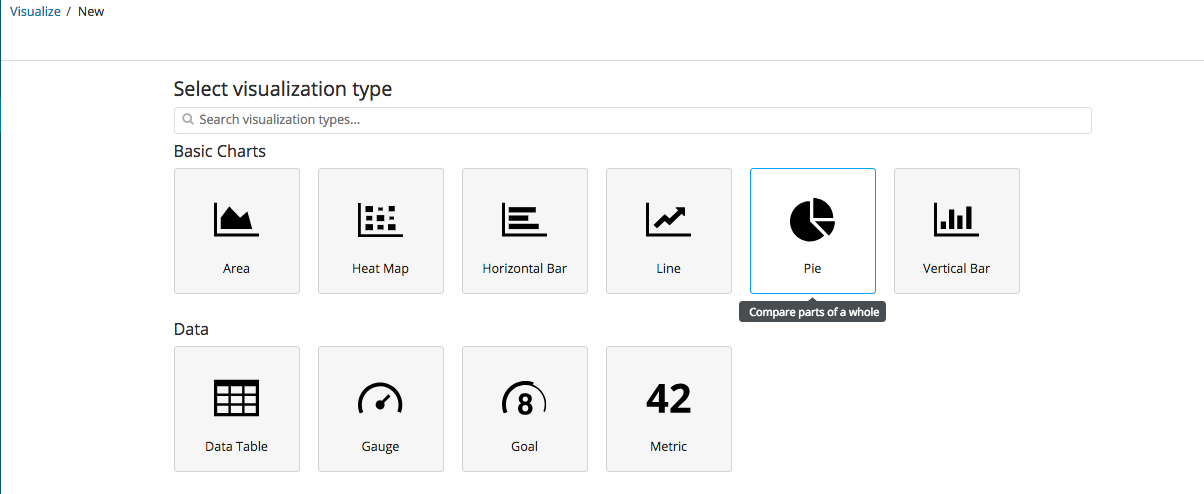


CREAR PRIMERA VISUALIZACION:

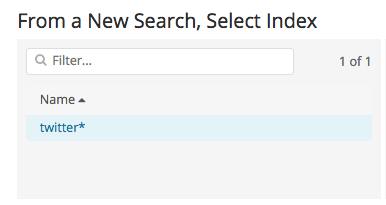
Vamos a crear la primer grafica donde nos indique que usuario es el que mas a twitteado, para esto accesamos al menu Visualize:



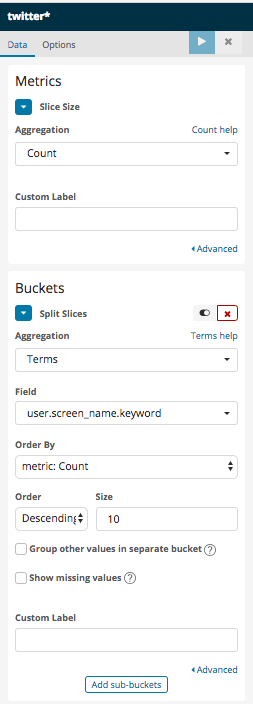
Click en el boton + y accesamos al catalogo de visualizaciones, para este ejemplo utilizaremos las graficas de Pie:



Una vez dentro nos pedira seleccionar la fuente de los datos, esta puede ser un indice, o bien alguna busqueda(busquedas hechas en Discover), para este ejercicio realizaremos la grafica del indice llamado twitter\*:



Ahora debemos de seleccionar cual sera nuestro campo que nos dara la informacion que deseamos graficar, en este caso procura seleccionar como a continuacion:

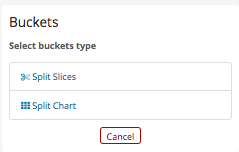
En la primer parte podemos observar el nombre del inidice:

twitter\*

En Metrics podemos seleccionar entre varias opciones, en este caso como deseamos saber el numero de twitts, seleccionamos conteo (count), en la parte de Custom Label podemos agregar un titulo

Buckets:

Esta opcion aparece al seleccionar split slices al inicio de la visualizacion:

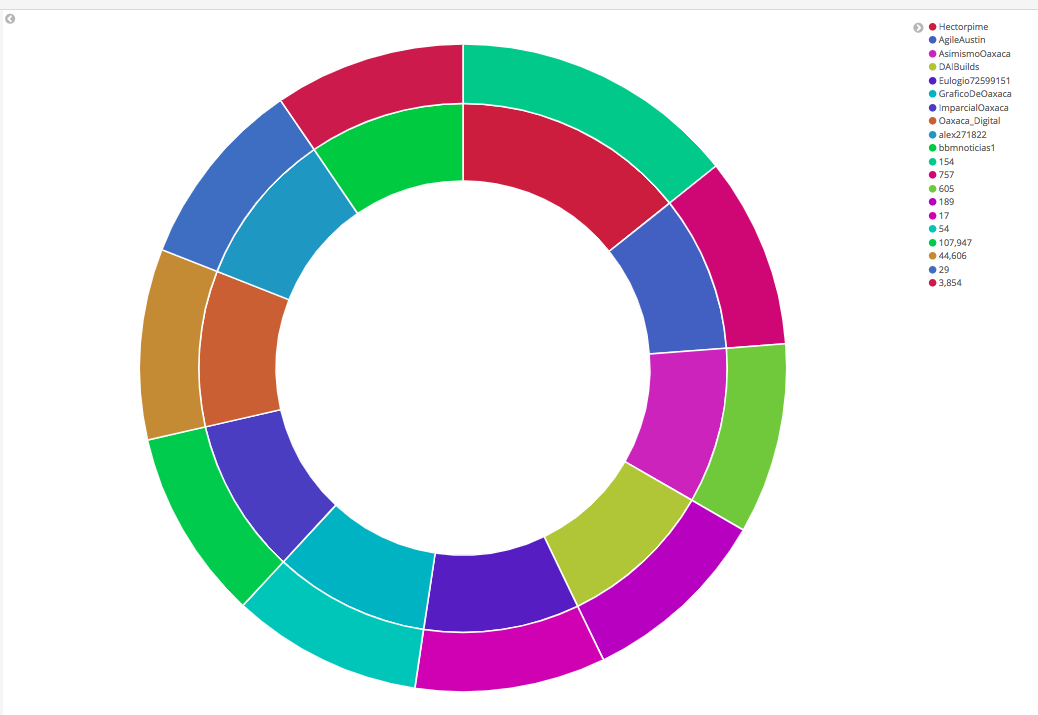
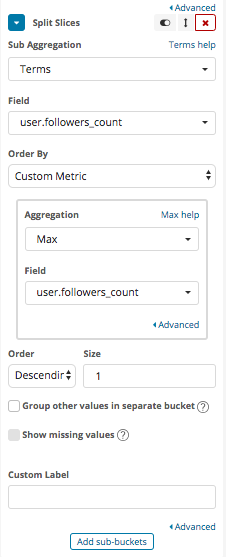


Y aquí debemos de seleccionar en Agregations Terms, que es el aggregation que me permite seleccionar el campo que deseo graficar, en este caso el campo para saber el username es: user.screen\_name.keyword

Order: como deseamos que se orden, descending es de mayor a menor, Ascending de menor a mayor

Size: el tamaño que deseo mostrar, en este ejemplo es el top10 de usuarios comentando.

En el boton add sub-buckets me permite agregar un nivel extra a la grafica de pie, al igual que el caso anterior debo de seleccionar que campo es el que me interesa saber, podemos seleccionar el numero de folowers, por ejemplo:



Anexo ejemplo encuesta:

input {

twitter {

consumer\_key => "CopiarConsumerKey"

consumer\_secret => "CopiarConsumerSecret"

oauth\_token => "CopiarAccessToken"

oauth\_token\_secret => "CopiarAccessTokenSecret"

#follows => ["10946302", " 84512601", "149344048" ]

keywords => [ "oaxaca", "ask\_elastic", "elastic", "meetup" ]

full\_tweet => true

}

}

filter {

grok {

match => { "text" => ".\*1. \(%{DATA:p1}\).\*" }

}

grok {

match => { "text" => ".\*2. \(%{DATA:p2}\).\*" }

}

grok {

match => { "text" => ".\*3. \(%{DATA:p3}\).\*" }

}

grok {

match => { "text" => ".\*4. \(%{DATA:p4}\).\*" }

}

grok {

match => { "text" => ".\*5. \(%{DATA:p5}\).\*" }

}

mutate {

lowercase => [ "p1", "p2", "p3", "p4", "p5" ]

}

}

output {

# stdout { codec => rubydebug }

elasticsearch {

index => "twitter-%{+YYYY.MM.dd}"

hosts => "http://172.16.44.18:9200"

# cacert => "/home/gestion/elastic/6.2.4/logstash-6.2.4/ca.crt"

# user => "elastic"

# password => "elastic123"

}

}

ANEXO: twitter\_template.txt

PUT \_template/twitter

{

"index\_patterns": [

"twitter-\*"

],

"settings": {

"index": {

"number\_of\_shards": "3",

"number\_of\_replicas": "1"

}

},

"mappings": {

"doc": {

"dynamic": "false",

"properties": {

"@timestamp": {

"type": "date"

},

"@version": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

},

"entities": {

"properties": {

"hashtags": {

"properties": {

"indices": {

"type": "long"

},

"text": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

}

}

}

}

},

"coordinates": {

"properties": {

"coordinates": {

"type": "geo\_point"

},

"type": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

}

}

},

"text": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

},

"p1": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

},

"p2": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

},

"p3": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

},

"p4": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

},

"p5": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

},

"user.name": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

},

"user.description": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

},

"user.location": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

},

"user.screen\_name": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

},

"user.followers\_count": {

"type": "long",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

},

"id": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

},

"place.country": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

},

"place.name": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

},

"place.country\_code": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

},

"retweet\_count": {

"type": "long"

},

"source": {

"type": "text",

"fields": {

"keyword": {

"type": "keyword",

"ignore\_above": 256

}

}

}

}

}

}

}