**Elasticsearch** You Know, for Search

Bedapudi Praneeth

**Installing:**

* Installing ES is pretty straight forward.
* Download and double click on the .deb file from
  + [ES 2.3.3 (latest)](https://download.elastic.co/elasticsearch/release/org/elasticsearch/distribution/deb/elasticsearch/2.3.3/elasticsearch-2.3.3.deb)
  + [ES 2.2.0](https://download.elasticsearch.org/elasticsearch/release/org/elasticsearch/distribution/deb/elasticsearch/2.2.0/elasticsearch-2.2.0.deb)
  + [ES 1.7.0](https://download.elastic.co/elasticsearch/elasticsearch/elasticsearch-1.7.0.deb)

To install.

* We can also run ES by download zip/ tar.gz files, without installing but for a new user installing from deb file is recommended.
  + Why?

There is absolutely no difference in features or functionality between installed ES and directly-run ES except that, it is easy to configure installed ES in future and also easier to install plugins because all of them use default ES locations by default and it would be a newbie’s nightmare to change the default locations to custom locations while configuring ES or while installing plugin.

**Installing and Configuring shield:**

1. Go into your elasticsearch directory " **cd /usr/share/elasticsearch/** "

2. Install plugin license with " **bin/plugin install license** "

3. Install shield with " **bin/plugin install shield** "

4. Restart elasticsearch service “ **sudo service elasticsearch restart** “

* Adding admin user:

" **bin/shield/esusers useradd user\_name -p pass\_word -r admin** "

* Check if shield is working by visiting <http://localhost:9200> (you will be asked to enter username and password)
* **Adding custom users:**

Note: See **roles.yml** file at **/etc/elasticsearch/shield/roles.yml** to see the predefined roles. " cat users\_roles " for seeing all users and their roles.

To add custom users edit roles.yml to add their role information.

Eg:

dummy\_reader:

indices:

'dummy':

privileges: indices:data/read/get, indices:data/read/search

In this example a user having **dummy\_reader** role can search and get only from the index dummy

To create a new user with a role use

" **bin/shield/esusers useradd user\_name -p pass\_word -r role\_name** "

**Note:** After configuring shield, you have to add the username in each curl command

Eg: “ curl -XGET “url” goes to “ **curl -XGET --user user\_name “url”** “

**Note:** In roles.yml file while adding new user role, please note that **indentation** is important.

**Setting up Cluster with more than one nodes in ES**

Add the following lines modified as per your requirement to "elasticsearch.yml" file

* All your machines should have **same cluster name**. In the following example cluster name is dummy.

**cluster.name:** dummy

* Each machine is a node and every node's name should be different.

**node.name:** node1

* Add the following line to config file if your node is not discoverable by other machines.

**network.host:** 0.0.0.0

* Add the following line with all the nodes ip addresses. New master selection will follow this order in case master goes down.

**discovery.zen.ping.unicast.hosts:** ["127.0.0.1", "node1\_ip", "node2\_ip"]

**Logging in ES:**

All logs generated by ES are located in “ /logs “ in your install location.

We can modify logging.yml to change logging level etc.

Logging options can also be changed with http request

Eg:

PUT /\_cluster/settings  
{  
 "transient" : {  
 "logger.discovery" : "DEBUG"  
 }  
}

Here logging level is changed to DEBUG

**What is slowlog?**

The purpose of this log is to catch queries and indexing requests that take over a certain threshold of time. By default, the slowlog is not enabled. It can be enabled by defining the action (query, fetch, or index), the level that you want the event logged at (WARN, DEBUG, and so forth) and a time threshold.

Eg:

PUT /my\_index/\_settings  
{  
 "index.search.slowlog.threshold.query.warn" : "10s",   
 "index.search.slowlog.threshold.fetch.debug": "500ms",   
 "index.indexing.slowlog.threshold.index.info": "5s"   
}

This emits a warn log when queries are slower than 10seconds, debug level log when queries are slower than 500ms ..