How to install Elasticsearch on ClearOS

2021-07-20: WikiSuite will now support all major Linux distros. Thus, the information below is no longer updated. It may still be valid, or not. It will be eventually removed from this site, so anything relevant should be moved to the appropriate site. For anything related to ClearOS, please search among the following: ClearOS site, code base, Developer docs, Wiki or forum.

Please contact us if you would like to help out.

Elasticsearch is a search server. This is useful once your project is quite big and you start hitting limits of the default search in Tiki Wiki CMS Groupware. Elasticsearch integrates well with Kibana. See also: How to install Kibana on ClearOS

Status as of 2018-04-28: Elasticsearch is at v5.6.8. There are some minor issues with Adminer, which are being looked into.

Log4j vulnerability

Ref:
https://discuss.elastic.co/t/elasticsearch-5-0-0-5-6-10-and-6-0-0-6-3-2-log4j-cve-2021-44228-cve-2021-45046-remediation/292054

```
find Elasticsearch

cd /usr/share/elasticsearch

Remove class

zip -d lib/log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class

Check (result should be empty)

unzip -l lib/log4j-core-*.jar | grep -i jndilookup

Restart

systemctl restart elasticsearch
```

How to install

On ClearOS 7.x

yum install app-elasticsearch

Comments: RAM: You need at least 3 GB of system RAM to run Elasticsearch (1 gig for ClearOS and 2 gigs for
Elasticsearch). A warning message is shown in webconfig if the requirement is not met. If you are just hacking around, you can change the default Elasticsearch usage from 2 GB to 1 GB. To do so, update the following options in /etc/elasticsearch/jvm.options:
- Xms1g
- Xmx1g

Then, visit https://example.org:81/app/elasticsearch and activate it

Once activated and running you can use the integrated web interface using Adminer. The adminer-elasticsearch package provides the glue to connect Adminer to a local Elasticsearch system. By default you can use your ClearOs root credential to login.

Example of install log

[+]

How to upgrade

<table>
<thead>
<tr>
<th>How to upgrade</th>
</tr>
</thead>
<tbody>
<tr>
<td>yum upgrade app-elasticsearch elasticsearch adminer-elasticsearch</td>
</tr>
</tbody>
</table>

From 2.x to 5.x

When running Elasticsearch with small amount of memory, the service may not start properly. Even using the hack above, Elasticsearch will die when indexing documents. So it is better to have at least 4gb RAM on server running Elasticsearch. When upgrading elasticsearch and also the server memory, these steps may be useful:

1. Set -Xms2g -Xmx3g on /etc/elasticsearch/jvm.options
2. Restart elasticsearch by typing systemctl restart elasticsearch
3. Destroy old indexes by curl -XDELETE localhost:9200/tiki_ppm16_main_5af2f8481bb8b (You need to find the name of your old indexes. You can also use the Adminer interface linked from your Elasticsearch app for ClearOS (https://example.org:81/app/elasticsearch)
4. Increase Tiki preference Search index rebuild memory limit to 2G
5. Rebuild the index by using php console.php index:rebuild -vvv
6. Clear all caches php console.php cache:clear

When index name is not known, it can be found on Tiki instance, at page http://example.org/tiki-admin.php?page=search. Also, you can list all your indexes by typing curl 'localhost:9200/_cat/indices'.

Full install log example

[+]
Key points

- Web interface is at https://example.org:81/app/elasticsearch
  - View your data via Adminer. Most things are working with Adminer 4.6.2 but data edits are not yet working as of 2018-04-28
- By default, Elasticsearch only listens to localhost. Do not change this unless you know what you are doing. If you do so, make sure http://example.org:9200 does not answer to unauthorized users or systems. If it does, you need to configure the firewall. Potential future todo: tighten this up even more by password protecting connections from localhost.
- By default, it's set to auto restart on each boot
- As of 2016-11-24, it's installing Elasticsearch 2.x, but the plan is to offer 5.x as soon as Tiki is confirmed working with it. 2017-04-21: Now that recent versions of Tiki (which ones?) support Elasticsearch 5.x the app will upgrade to 5.x in May or June 2017.
- Elasticsearch 1.x is known to have issues with some of the advanced features of trackers, so it's not supported.
- Elasticsearch can require a lot of RAM if you have a lot data.
- Upgrades to major versions will happen according to the Tiki requirements. Ex.: support for 6.x will only be added once Tiki supports it.

To test

Wait a few minutes after the initial install. Then you can check if all is okay.

```
Test if Elasticsearch is running
[root@example ~]# curl localhost:9200
{
  "name" : "Chtylok",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "UmE4ikI2Q3eM5ik7kbkkdg",
  "version" : {
    "number" : "2.4.1",
    "build_hash" : "c67dc32e24162035d18d6fe1e952c4cbcbe79d16",
    "build_timestamp" : "2016-09-27T18:57:55Z",
    "build_snapshot" : false,
    "lucene_version" : "5.5.2"
  },
  "tagline" : "You Know, for Search"
}
```

How to configure with Tiki

1. In your Tiki instance, at tiki-admin.php?page=search -> Advanced Search -> Unified Search Engine ->
WikiSuite: The most comprehensive and integrated Open Source enterprise solution.

Elasticsearch (All the other default settings work out of the box)
- You may need to set your "Preference Filters" to include "Advanced"

2. To test, click "Rebuild Index"
3. Optional but recommended, add the rebuild command to a daily cron job
   `php console.php index:rebuild`

Related links
- https://doc.tiki.org/Elasticsearch
- https://dev.tiki.org/Elasticsearch
- https://github.com/WikiSuite/app-elasticsearch
- https://github.com/WikiSuite/adminer-elasticsearch
- https://www.clearos.com/resources/documentation/clearos/content:en_us:kb_howtos_elasticsearch (needs a cleanup)