

Atualização ELK em CentOS/Red Hat

- [Atualização ElasticSearch](#)
- [Atualização Kibana](#)

Atualização Elasticsearch

1. Efetuar login no servidor com um cliente SSH.
2. Para confirmar qual versão do Elasticsearch você possui instalada atualmente, execute o comando abaixo e em seguida verifique o campo de "number":

```
$ curl -X GET "localhost:9200?pretty"
```

```
{
  "name" : "edipo-dev",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "7RqI3a0uReyIKR5DTX45_g",
  "version" : {
    "number" : "7.4.0",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "22e1767283e61a198cb4db791ea66e3f11ab9910",
    "build_date" : "2019-09-27T08:36:48.569419Z",
    "build_snapshot" : false,
    "lucene_version" : "8.2.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

3. Pare os serviços do Elasticsearch:

```
$ sudo systemctl stop elasticsearch.service
```

```
[root@edipo-dev ~]# sudo systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
   Active: inactive (dead) since Thu 2022-02-03 18:27:06 -03; 4s ago
     Docs: http://www.elastic.co
   Process: 5556 ExecStart=/usr/share/elasticsearch/bin/elasticsearch -p ${PID_DIR}/elasticsearch.pid --quiet (code=exited, status=143)
  Main PID: 5556 (code=exited, status=143)

Feb 03 17:16:33 edipo-dev elasticsearch[5556]: at org.elasticsearch.bootstrap.Elasticsearch.main(Elasticsearch.java:115)
Feb 03 17:16:33 edipo-dev elasticsearch[5556]: at org.elasticsearch.bootstrap.Elasticsearch.main(Elasticsearch.java:92)
Feb 03 17:16:33 edipo-dev elasticsearch[5556]: Caused by: java.lang.IllegalArgumentException: Unconditional Delete not supported
Feb 03 17:16:33 edipo-dev elasticsearch[5556]: at org.apache.logging.log4j.core.appender.rolling.action.DeleteAction.<init>(DeleteAction.java:71)
Feb 03 17:16:33 edipo-dev elasticsearch[5556]: at org.apache.logging.log4j.core.appender.rolling.action.DeleteAction.createDeleteAction(DeleteAction.java:212)
Feb 03 17:16:33 edipo-dev elasticsearch[5556]: ... 25 more
Feb 03 17:16:33 edipo-dev elasticsearch[5556]: 2022-02-03 18:16:33,016 main ERROR Null object returned for Delete in DefaultRolloverStrategy.
Feb 03 17:17:02 edipo-dev systemd[1]: Started Elasticsearch.
Feb 03 18:27:05 edipo-dev systemd[1]: Stopping Elasticsearch...
Feb 03 18:27:06 edipo-dev systemd[1]: Stopped Elasticsearch.
```

4. Liste as versões disponíveis da aplicação:

```
$ yum --showduplicates list elasticsearch
```

```
[root@edipo-dev ~]# yum --showduplicates list elasticsearch
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.nbtelecom.com.br
 * epel: d2l2kl7pfhq30w.cloudfront.net
 * extras: mirror.nbtelecom.com.br
 * updates: mirror.nbtelecom.com.br
Installed Packages
elasticsearch.x86_64                                7.4.0-1                                @elasticsearch-7.x
Available Packages
elasticsearch.x86_64                                7.0.0-1                                elasticsearch-7.x
elasticsearch.x86_64                                7.0.0-1                                kibana-7.x
elasticsearch.x86_64                                7.0.1-1                                elasticsearch-7.x
elasticsearch.x86_64                                7.0.1-1                                kibana-7.x
elasticsearch.x86_64                                7.1.0-1                                elasticsearch-7.x
elasticsearch.x86_64                                7.1.0-1                                kibana-7.x
elasticsearch.x86_64                                7.1.1-1                                elasticsearch-7.x
elasticsearch.x86_64                                7.1.1-1                                kibana-7.x
elasticsearch.x86_64                                7.2.0-1                                elasticsearch-7.x
elasticsearch.x86_64                                7.2.0-1                                kibana-7.x
elasticsearch.x86_64                                7.2.1-1                                elasticsearch-7.x
elasticsearch.x86_64                                7.2.1-1                                kibana-7.x
elasticsearch.x86_64                                7.3.0-1                                elasticsearch-7.x
elasticsearch.x86_64                                7.3.0-1                                kibana-7.x
elasticsearch.x86_64                                7.3.1-1                                elasticsearch-7.x
elasticsearch.x86_64                                7.3.1-1                                kibana-7.x
elasticsearch.x86_64                                7.3.2-1                                elasticsearch-7.x
elasticsearch.x86_64                                7.3.2-1                                kibana-7.x
elasticsearch.x86_64                                7.4.0-1                                elasticsearch-7.x
elasticsearch.x86_64                                7.4.0-1                                kibana-7.x
elasticsearch.x86_64                                7.4.1-1                                elasticsearch-7.x
```

5. Selecionando a versão 7.10.0 do Elasticsearch:

```
$ sudo yum install elasticsearch-7.10.0-1.x86_64
```

```
[root@edipo-dev ~]# sudo yum install elasticsearch-7.10.0-1.x86_64
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.nbtelecom.com.br
 * epel: d2l2kl7pfhq30w.cloudfront.net
 * extras: mirror.nbtelecom.com.br
 * updates: mirror.nbtelecom.com.br
Resolving Dependencies
--> Running transaction check
--> Package elasticsearch.x86_64 0:7.4.0-1 will be updated
--> Package elasticsearch.x86_64 0:7.10.0-1 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                               Arch          Version        Repository      Size
=====
Updating:
elasticsearch                         x86_64        7.10.0-1       elasticsearch-7.x 304 M
=====
Transaction Summary
=====
Upgrade 1 Package

Total download size: 304 M
Is this ok [y/d/N]: y
Downloading packages:
Delta RPMs disabled because /usr/bin/applydeltarpm not installed.
elasticsearch-7.10.0-x86_64.rpm | 304 MB 00:00:47
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Updating : elasticsearch-7.10.0-1.x86_64                                1/2
warning: /etc/elasticsearch/jvm.options created as /etc/elasticsearch/jvm.options.rpmnew
warning: /etc/elasticsearch/log4j2.properties created as /etc/elasticsearch/log4j2.properties.rpmnew
  Cleanup : elasticsearch-7.4.0-1.x86_64                                2/2
Created elasticsearch keystore in /etc/elasticsearch/elasticsearch.keystore
  Verifying : elasticsearch-7.10.0-1.x86_64                                1/2
  Verifying : elasticsearch-7.4.0-1.x86_64                                2/2

Updated:
  elasticsearch.x86_64 0:7.10.0-1

Complete!
[root@edipo-dev ~]#
```

6. Após a atualização concluir, inicie os serviços do Elasticsearch:

```
$ sudo systemctl start elasticsearch.service
```

7. Execute o status do Elasticsearch para verificar se a aplicação foi iniciada com sucesso:

```
$ sudo systemctl status elasticsearch.service
```

8. Se caso ao verificar o status da aplicação você se deparar com a mensagem de erro abaixo:

```
-- Unit elasticsearch.service has begun starting up.
Feb 03 19:21:29 edipo-dev systemd-entrypoint[8158]: Exception in thread "main" java.lang.RuntimeException: starting java failed with [1]
Feb 03 19:21:29 edipo-dev systemd-entrypoint[8158]: output:
Feb 03 19:21:29 edipo-dev systemd-entrypoint[8158]: error:
Feb 03 19:21:29 edipo-dev systemd-entrypoint[8158]: Unrecognized VM option 'UseConcMarkSweepGC'
Feb 03 19:21:29 edipo-dev systemd-entrypoint[8158]: Error: Could not create the Java Virtual Machine.
Feb 03 19:21:29 edipo-dev systemd-entrypoint[8158]: Error: A fatal exception has occurred. Program will exit.
Feb 03 19:21:29 edipo-dev systemd-entrypoint[8158]: at org.elasticsearch.tools.launchers.JvmErgonomics.flagsFinal(JvmErgonomics.java:126)
Feb 03 19:21:29 edipo-dev systemd-entrypoint[8158]: at org.elasticsearch.tools.launchers.JvmErgonomics.finalJvmOptions(JvmErgonomics.java:88)
Feb 03 19:21:29 edipo-dev systemd-entrypoint[8158]: at org.elasticsearch.tools.launchers.JvmErgonomics.choose(JvmErgonomics.java:59)
Feb 03 19:21:29 edipo-dev systemd-entrypoint[8158]: at org.elasticsearch.tools.launchers.JvmOptionsParser.parseJvmOptions(JvmOptionsParser.java:137)
Feb 03 19:21:29 edipo-dev systemd-entrypoint[8158]: at org.elasticsearch.tools.launchers.JvmOptionsParser.main(JvmOptionsParser.java:95)
Feb 03 19:21:29 edipo-dev systemd[1]: elasticsearch.service: main process exited, code=exited, status=1/FAILURE
Feb 03 19:21:29 edipo-dev systemd[1]: Failed to start Elasticsearch.
-- Subject: Unit elasticsearch.service has failed
-- Defined-By: systemd
-- Support: http://lists.freedesktop.org/mailman/listinfo/systemd-devel
--
-- Unit elasticsearch.service has failed.
--
-- The result is failed.
Feb 03 19:21:29 edipo-dev systemd[1]: Unit elasticsearch.service entered failed state.
Feb 03 19:21:29 edipo-dev systemd[1]: elasticsearch.service failed.
```

9. Acesse o arquivo “jvm.options”:

```
$ vim /etc/elasticsearch/jvm.options
```

10. Substitua:

```
- XX: +UseConcMarkSweepGC
- XX: CMSInitiatingOccupancyFraction=75
- XX: +UseCMSInitiatingOccupancyOnly
```

Por:

```
8-13: - XX: +UseConcMarkSweepGC
8-13: - XX: CMSInitiatingOccupancyFraction=75
8-13: - XX: +UseCMSInitiatingOccupancyOnly
```

```
## GC configuration
8-13: -XX:+UseConcMarkSweepGC
8-13: -XX:CMSInitiatingOccupancyFraction=75
8-13: -XX:+UseCMSInitiatingOccupancyOnly
```

11. Recarregue os serviços:

```
$ sudo systemctl daemon-reload
```

12. Tente iniciar novamente os serviços do ElasticSearch:

```
$ sudo systemctl start elasticsearch.service
```

13. Verifique se a aplicação foi iniciada com sucesso:

```
$ sudo systemctl status elasticsearch.service
```

```
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2022-02-08 00:16:51 -03; 1 day 11h ago
     Docs: https://www.elastic.co
    Main PID: 10112 (java)
    CGroup: /system.slice/elasticsearch.service
            └─10112 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative...
            └─10299 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller
```

14. Para conferir a versão do ElasticSearch, execute:

```
$ curl -X GET "localhost:9200?pretty"
```

```
{
  "name" : "edipo-dev",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "7RqI3a0uReyIKR5DTX45_g",
  "version" : {
    "number" : "7.10.0",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "51e9d6f22758d0374a0f3f5c6e8f3a7997850f96",
    "build_date" : "2020-11-09T21:30:33.964949Z",
    "build_snapshot" : false,
    "lucene_version" : "8.7.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Atualização Kibana

1. Pare os serviços do Kibana:

```
$ sudo systemctl stop kibana.service
```

2. Confirme se os serviços foram parados:

```
$ sudo systemctl status kibana.service
```

```
[root@edipo-dev ~]# systemctl status kibana.service
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: disabled)
   Active: inactive (dead) since Fri 2022-02-04 11:45:47 -03; 6s ago
     Process: 5006 ExecStart=/usr/share/kibana/bin/kibana -c /etc/kibana/kibana.yml (code=exited, status=0/SUCCESS)
    Main PID: 5006 (code=exited, status=0/SUCCESS)

Feb 03 17:16:02 edipo-dev systemd[1]: Started Kibana.
Feb 03 18:50:36 edipo-dev systemd[1]: [/etc/systemd/system/kibana.service:3] Unknown lvalue 'StartLimitIntervalSec' in section 'Unit'
Feb 03 18:50:36 edipo-dev systemd[1]: [/etc/systemd/system/kibana.service:4] Unknown lvalue 'StartLimitBurst' in section 'Unit'
Feb 03 18:50:41 edipo-dev systemd[1]: [/etc/systemd/system/kibana.service:3] Unknown lvalue 'StartLimitIntervalSec' in section 'Unit'
Feb 03 18:50:41 edipo-dev systemd[1]: [/etc/systemd/system/kibana.service:4] Unknown lvalue 'StartLimitBurst' in section 'Unit'
Feb 04 11:45:45 edipo-dev systemd[1]: Stopping Kibana...
Feb 04 11:45:47 edipo-dev systemd[1]: Stopped Kibana.
```

3. Liste as versões disponíveis da aplicação:

```
$ yum --showduplicates list kibana
```

```
[root@edipo-dev ~]# yum --showduplicates list kibana
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.nbtelecom.com.br
 * epel: d2l2kl7pfhq30w.cloudfront.net
 * extras: mirror.nbtelecom.com.br
 * updates: mirror.nbtelecom.com.br
Installed Packages
kibana.x86_64                                7.4.0-1                                     @elasticsearch-7.x
Available Packages
kibana.x86_64                                7.0.0-1                                     elasticsearch-7.x
kibana.x86_64                                7.0.0-1                                     kibana-7.x
kibana.x86_64                                7.0.1-1                                     elasticsearch-7.x
kibana.x86_64                                7.0.1-1                                     kibana-7.x
kibana.x86_64                                7.1.0-1                                     elasticsearch-7.x
kibana.x86_64                                7.1.0-1                                     kibana-7.x
kibana.x86_64                                7.1.1-1                                     elasticsearch-7.x
kibana.x86_64                                7.1.1-1                                     kibana-7.x
kibana.x86_64                                7.1.1-1                                     kibana-7.x
kibana.x86_64                                7.2.0-1                                     elasticsearch-7.x
kibana.x86_64                                7.2.0-1                                     kibana-7.x
kibana.x86_64                                7.2.1-1                                     elasticsearch-7.x
kibana.x86_64                                7.2.1-1                                     kibana-7.x
kibana.x86_64                                7.3.0-1                                     elasticsearch-7.x
kibana.x86_64                                7.3.0-1                                     kibana-7.x
kibana.x86_64                                7.3.1-1                                     elasticsearch-7.x
kibana.x86_64                                7.3.1-1                                     kibana-7.x
kibana.x86_64                                7.3.2-1                                     elasticsearch-7.x
kibana.x86_64                                7.3.2-1                                     kibana-7.x
kibana.x86_64                                7.4.0-1                                     elasticsearch-7.x
kibana.x86_64                                7.4.0-1                                     kibana-7.x
kibana.x86_64                                7.4.1-1                                     elasticsearch-7.x
kibana.x86_64                                7.4.1-1                                     kibana-7.x
kibana.x86_64                                7.4.2-1                                     elasticsearch-7.x
kibana.x86_64                                7.4.2-1                                     kibana-7.x
kibana.x86_64                                7.5.0-1                                     elasticsearch-7.x
kibana.x86_64                                7.5.0-1                                     kibana-7.x
kibana.x86_64                                7.5.1-1                                     elasticsearch-7.x
kibana.x86_64                                7.5.1-1                                     kibana-7.x
kibana.x86_64                                7.5.2-1                                     elasticsearch-7.x
kibana.x86_64                                7.5.2-1                                     kibana-7.x
kibana.x86_64                                7.6.0-1                                     elasticsearch-7.x
kibana.x86_64                                7.6.0-1                                     kibana-7.x
```

4. Selecionando a versão 7.10.0 do Kibana:


```
$ sudo yum install kibana-7.10.0-1.x86_64
```

```
[root@edipo-dev ~]# sudo yum install kibana-7.10.0-1.x86_64
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
epel/x86_64/metalink | 45 kB 00:00:00
 * base: mirror.nbtelecom.com.br
 * epel: d2lzk17pfhq30w.cloudfront.net
 * extras: mirror.nbtelecom.com.br
 * updates: mirror.nbtelecom.com.br
base | 3.6 kB 00:00:00
elasticsearch-7.x | 1.3 kB 00:00:00
epel | 4.7 kB 00:00:00
extras | 2.9 kB 00:00:00
kibana-7.x | 1.3 kB 00:00:00
nodesource | 2.5 kB 00:00:00
updates | 2.9 kB 00:00:00
(1/2): epel/x86_64/updateinfo | 1.0 MB 00:00:00
(2/2): epel/x86_64/primary_db | 7.0 MB 00:00:00
Resolving Dependencies
--> Running transaction check
---> Package kibana.x86_64 0:7.4.0-1 will be updated
---> Package kibana.x86_64 0:7.10.0-1 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package Arch Version Repository Size
=====
Updating:
kibana x86_64 7.10.0-1 elasticsearch-7.x 245 M
Transaction Summary
=====
Upgrade 1 Package

Total download size: 245 M
Is this ok [y/d/N]: y
Downloading packages:
Delta RPMs disabled because /usr/bin/applydeltarpm not installed.
kibana-7.10.0-x86_64.rpm | 245 MB 00:00:38
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Updating : kibana-7.10.0-1.x86_64 1/2
warning: /etc/kibana/kibana.yml created as /etc/kibana/kibana.yml.rpmnew
Stopping kibana service...Stopping kibana (via systemctl): [ OK ]
  Cleanup : kibana-7.4.0-1.x86_64 2/2
  Verifying : kibana-7.10.0-1.x86_64 1/2
  Verifying : kibana-7.4.0-1.x86_64 2/2

Updated:
kibana.x86_64 0:7.10.0-1

Complete!
```

5. Após a atualização finalizar, recarregue os serviços:

```
$ sudo systemctl daemon-reload
```

6. Inicie os serviços do Kibana:


```
$ sudo systemctl start kibana.service
```

7. Verifique se os serviços foram iniciados com sucesso:

```
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2022-02-09 16:38:39 -03; 8s ago
     Main PID: 43125 (node)
        Tasks: 11 (limit: 4612)
       Memory: 198.5M
      CGroup: /system.slice/kibana.service
              └─43125 /usr/share/kibana/bin/./node/bin/node /usr/share/kibana/bin/./src/cli/dist

Feb 09 16:38:39 templetelk systemd[1]: Started Kibana.
```

8. Acesse a aplicação e faça login para confirmar o sucesso da atualização:

 Help us improve the Elastic Stack

Want to help us improve the Elastic Stack? Data usage collection is currently disabled. Enabling data usage collection helps us manage and improve our products and services. See details.

Enable

Disable

Home

 Add data

 Manage

 Dev tools




Enterprise Search
Search everything →

Build a powerful search experience.

Connect your users to relevant data.


Unify your team content.



Observability

Monitor infrastructure metrics.

Trace application requests.



Kibana

Analyze data in dashboards.

Search and find insights.

Design pixel-perfect presentations.