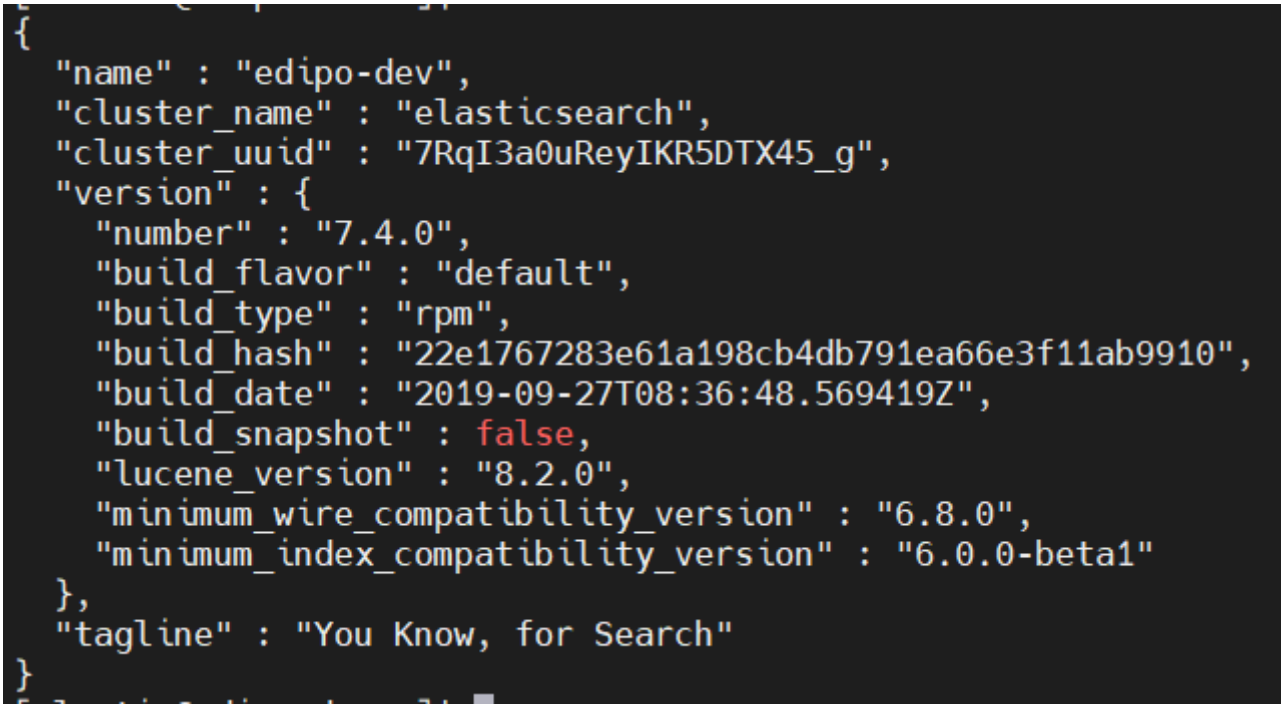
Atualização ELK em CentOS/Red Hat

Atualização ElasticSearch

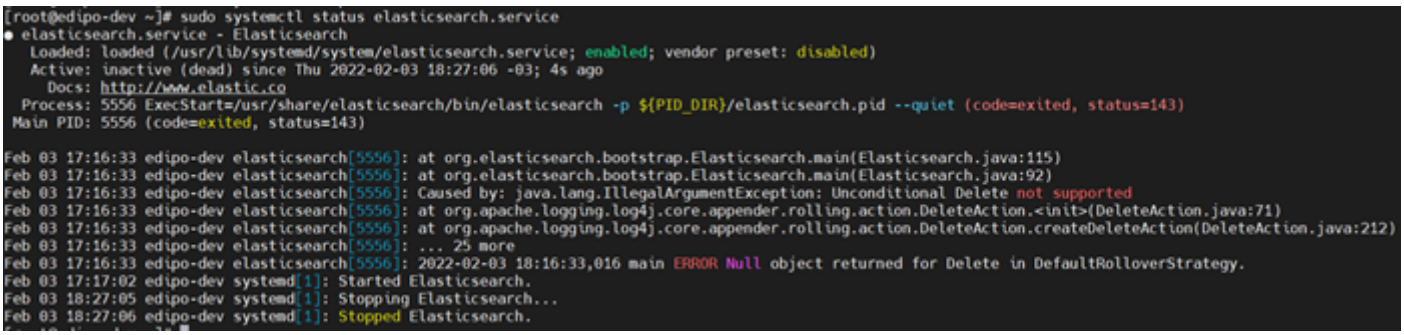
1. Efetuar login no servidor com um cliente SSH.
2. Para confirmar qual versão do ElasticSearch você possui instalada atualmente, execute o comando abaixo e em seguida verifique o campo de “number”:

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



3. Pare os serviços do ElasticSearch:

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



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: d2lzkl7pfhq30w.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: d2lzkl7pfhq30w.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 ~]#
```

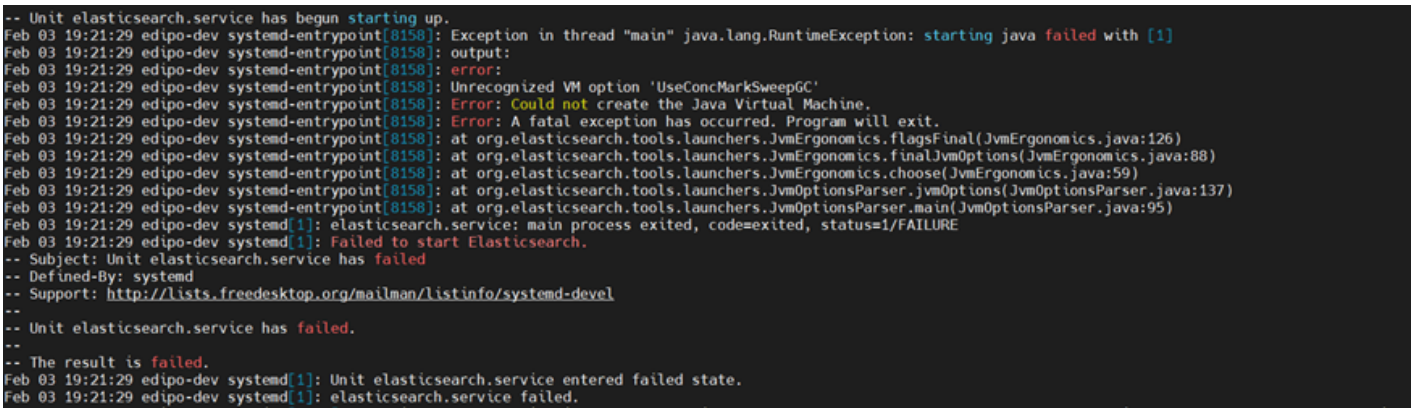
6. Após a atualização concluir, inicie os serviços do ElasticSearch:

```
$ 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:



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:

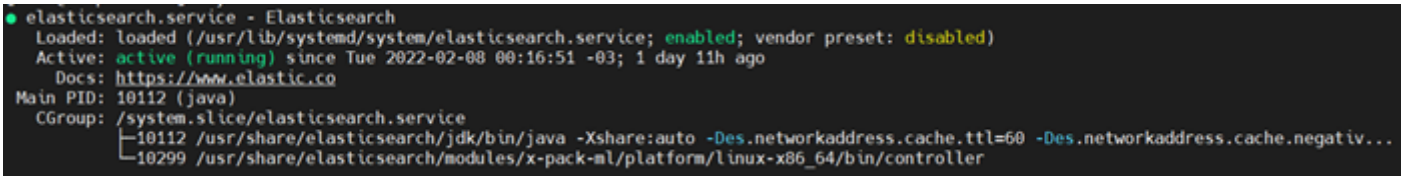
```
$ sudo systemctl daemon-reload
```

12. Tente iniciar novamente os serviços do ElasticSearch:

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

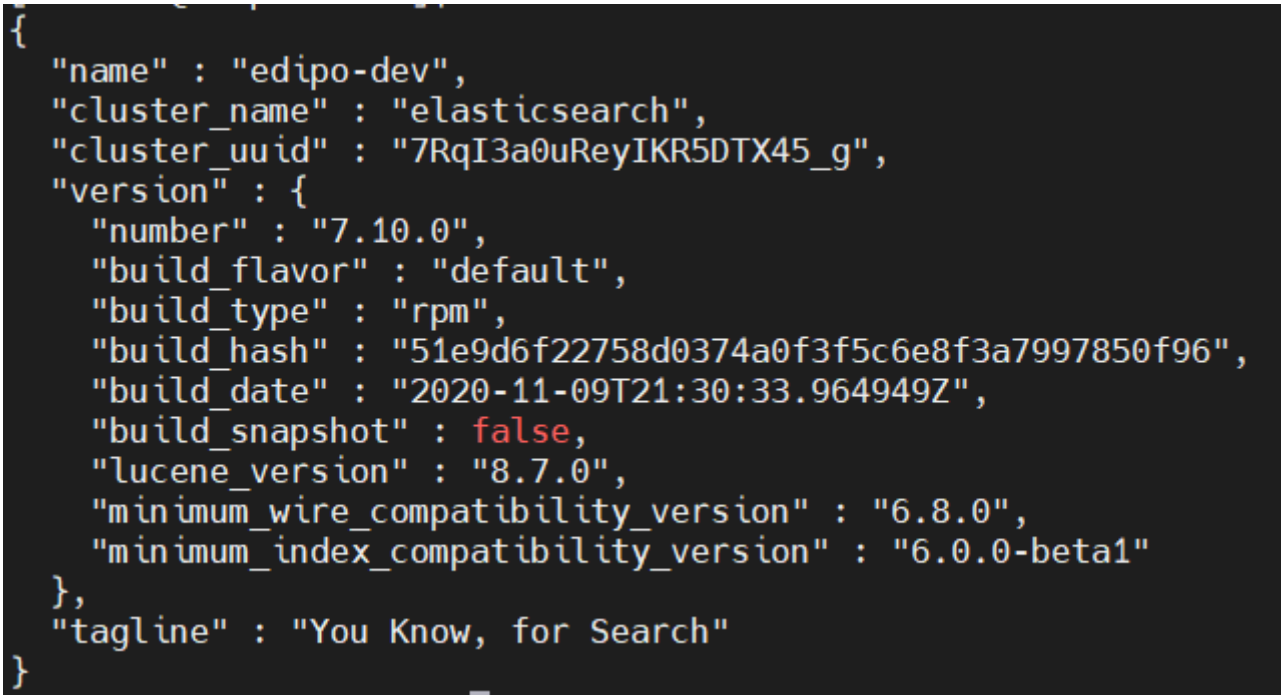
13. Verifique se a aplicação foi iniciada com sucesso:

```
$ sudo systemctl status elasticsearch.serve
```



14. Para conferir a versão do ElasticSearch, execute:

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



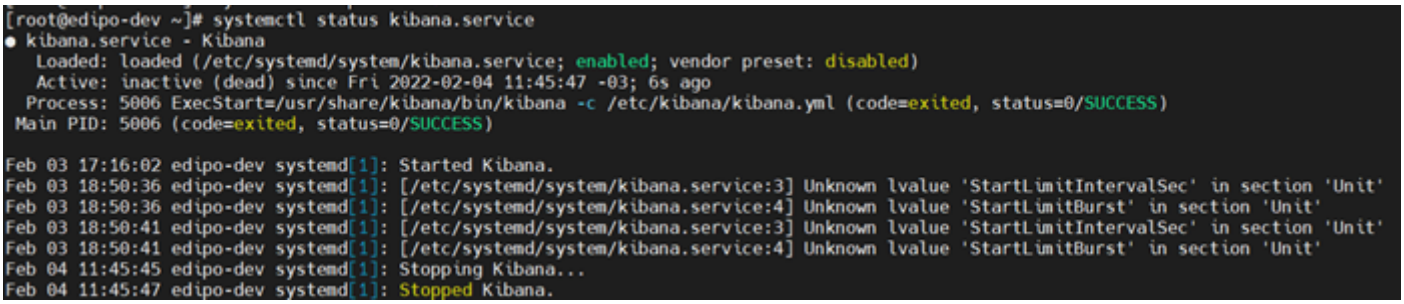
Atualização Kibana

1. Pare os serviços do Kibana:

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

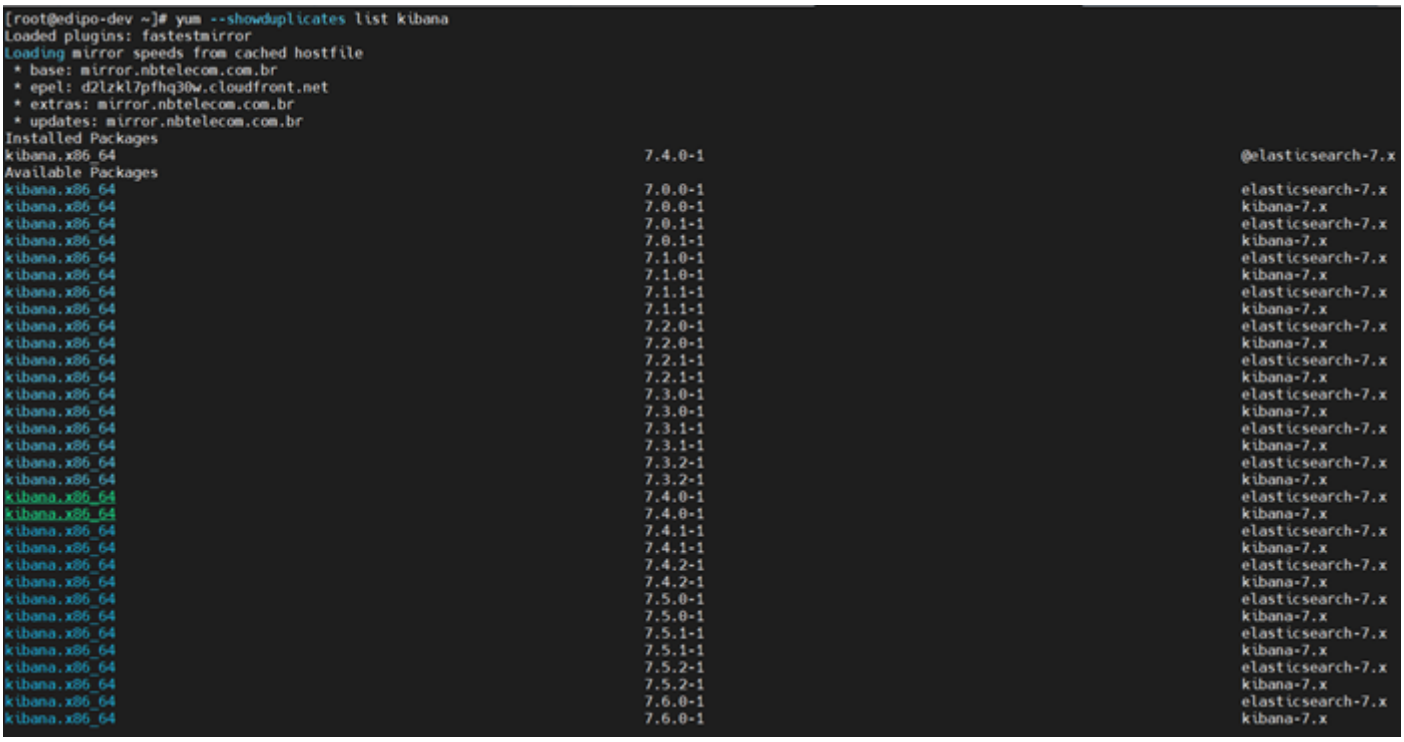
2. Confirme se os serviços foram parados:

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



3. Liste as versões disponíveis da aplicação:

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



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: d2lzkl7pfhq30w.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  ]
 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:

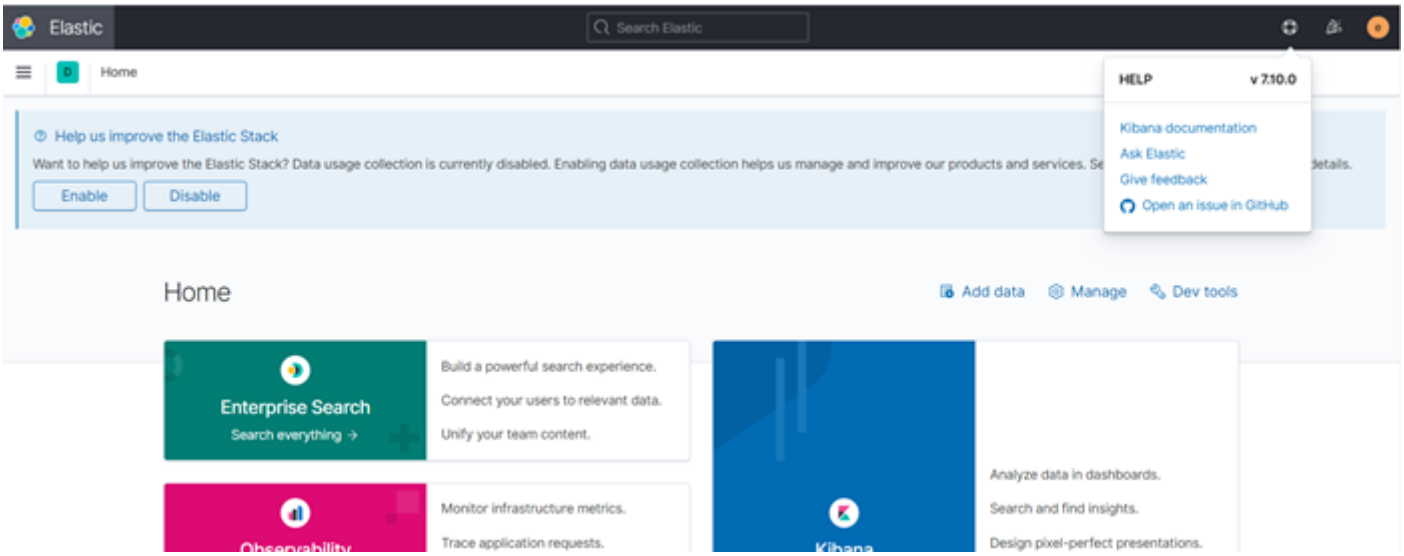
```
$ sudo systemctl start kibana.service
```

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:


Elastic
Search Elastic
Home
HELP
v 7.10.0
Kibana documentation
Ask Elastic
Give feedback
Open an issue in GitHub
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.
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.