

Instalando a stack Elastic (ELK) 7.4

Importação da chave do repositório Elastic:

```
$ sudo rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch
```

Configuração do repositório:

```
$ sudo vim /etc/yum.repos.d/elasticsearch.repo

[elasticsearch]
name=Elasticsearch repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=0
autorefresh=1
type=rpm-md
```

Instalação do componente Elasticsearch

Instalação do **Elasticsearch** versão 7.4.0:

```
$ sudo yum install --enablerepo=elasticsearch elasticsearch-7.4.0-1.x86_64
```

Configuração do serviço no sistema operacional (daemon):

```
$ sudo systemctl daemon-reload
$ sudo systemctl enable elasticsearch.service
$ sudo systemctl start elasticsearch.service
```

Liberação de portas no firewall:

```
$ sudo firewall-cmd --permanent --add-port=9200/tcp
$ sudo firewall-cmd --reload
```

Teste para verificar funcionamento do elasticsearch:

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

{
  "name" : "elk-ol7",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "jugxM_UASLeLjJw0ITvZ5A",
  "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"
}
```

Configuração da licença "basic", detalhes da licenças são encontradas no site do Elastic:

```
$ sudo vim /etc/elasticsearch/elasticsearch.yml

xpack.license.self_generated.type: "basic"
transport.host: localhost
transport.tcp.port: 9300
http.port: 9200
network.host: 0.0.0.0
xpack.security.enabled: true

$ sudo systemctl restart elasticsearch.service
```

Configuração de usuários e senhas de autenticação no elasticsearch:

```
sudo /usr/share/elasticsearch/bin/elasticsearch-setup-passwords interactive
sudo systemctl restart elasticsearch.service
```

Teste de autenticação com senha certa:

```
$ curl -u elastic:senhacerta -X GET "localhost: 9200/?pretty"

{
  "name" : "elk-ol7",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "jugxM_UASLeLjJw0ITvZ5A",
  "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"
}
```

Teste de autenticação com senha errada:

```
$ curl -u elastic:senhaerrada -X GET "localhost:9200/?pretty"

{
  "error" : {
    "root_cause" : [
      {
        "type" : "security_exception",
        "reason" : "failed to authenticate user [elastic]",
        "header" : {
          "WWW-Authenticate" : "Basic realm=\"security\" charset=\"UTF-8\""
        }
      }
    ],
    "type" : "security_exception",
    "reason" : "failed to authenticate user [elastic]",
    "header" : {
      "WWW-Authenticate" : "Basic realm=\"security\" charset=\"UTF-8\""
    }
  },
  "status" : 401
}
```

Instalação do componente Kibana

Instalação do Kibana versão 7.4.0:

```
$ sudo yum install --enablerepo=elasticsearch kibana-7.4.0-1.x86_64
```

Liberação de portas no firewall:

```
$ sudo firewall-cmd --permanent --add-port=5601/tcp
$ sudo firewall-cmd --reload
```

Configuração para conectar no Elasticsearch:

```
$ sudo vim /etc/kibana/kibana.yml

server.host: "192.168.0.1"
elasticsearch.hosts: ["http://localhost:9200"]
elasticsearch.username: "kibana"
elasticsearch.password: "senha"
logging.dest: /var/log/kibana/kibana.log
```

Configuração de diretório para geração de log do Kibana:

```
$ sudo mkdir /var/log/kibana
$ sudo chown -R kibana:kibana /var/log/kibana
```

Configuração do serviço no sistema operacional (daemon):

```
$ sudo systemctl daemon-reload
$ sudo systemctl enable kibana.service
$ sudo systemctl start kibana.service
$ sudo tail -fn100 /var/log/kibana/kibana.log | grep listening
```

Teste de funcionamento do Kibana, no browser:

```
http://<ip>:5601/login
```

Revision #2

Created 16 November 2021 22:33:43

Updated 12 December 2022 23:37:00