

Instalando o ELK

Os procedimentos de instalação do Elasticsearch (ELK) devem ser executados apenas se não tenha optado pela utilização da VM disponibilizada, onde esta já vem com o Elasticsearch instalado.

i. Obtenha os arquivos Debian Package através do site oficial:

ElasticSearch: <https://www.elastic.co/pt/downloads/past-releases/elasticsearch-7-4-0>

O cURL é um pacote de suporte à validação. Link para download:

http://archive.ubuntu.com/ubuntu/pool/main/c/curl/curl_7.47.0-1ubuntu2.14_amd64.deb

ii. Coloque os arquivos no servidor.

iii. Configure o IP estático:

```
$ sudo vi /etc/network/interfaces

auto ens160
iface ens160 inet static
address 192.168.0.130
netmask 255.255.255.0
network 192.168.0.0
broadcast 192.168.0.255
gateway 192.168.0.1
dns-nameservers 192.168.0.10
```

iv. Instale o ElasticSearch com o comando

```
$ sudo dpkg -i elasticsearch-7.4.0-amd64.deb
```

v. Atualize o systemd para que o ElasticSearch fique como serviço:

```
$ sudo update-rc.d elasticsearch defaults 95 10
$ sudo /bin/systemctl daemon-reload
$ sudo /bin/systemctl enable elasticsearch.service
```

vi. Edite a configuração do Elasticsearch:

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

Colocando esse trecho no final do arquivo:

```
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
```

Este trecho é responsável por liberar as requisições remotas, habilitar o módulo de segurança e a licença basic.

vii. Inicie o serviço Elasticsearch

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

viii. Crie as senhas dos usuários com o comando:

```
$ sudo /usr/share/elasticsearch/bin/elasticsearch-setup-passwords interactive
```

ix. Liberar porta no firewall UFW

```
$ sudo ufw allow 9200
```

x. Reinicie a aplicação

```
$ sudo systemctl restart elasticsearch.service
```

xi. Faça o teste passando o usuário “elastic” com a senha cadastrada:

```
$ curl -u elastic:senha http://127.0.0.1:9200
```

O retorno deve ser:

```
{
  "name" : "ubuntuELK",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "k-uVHExsQt-9ntsSDhpxAQ",
  "version" : {
```

```
"number" : "7.4.0",
"build_flavor" : "default",
"build_type" : "deb",
"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"
}
```

Revision #1

Created 25 October 2021 19:28:24

Updated 25 October 2021 19:41:02