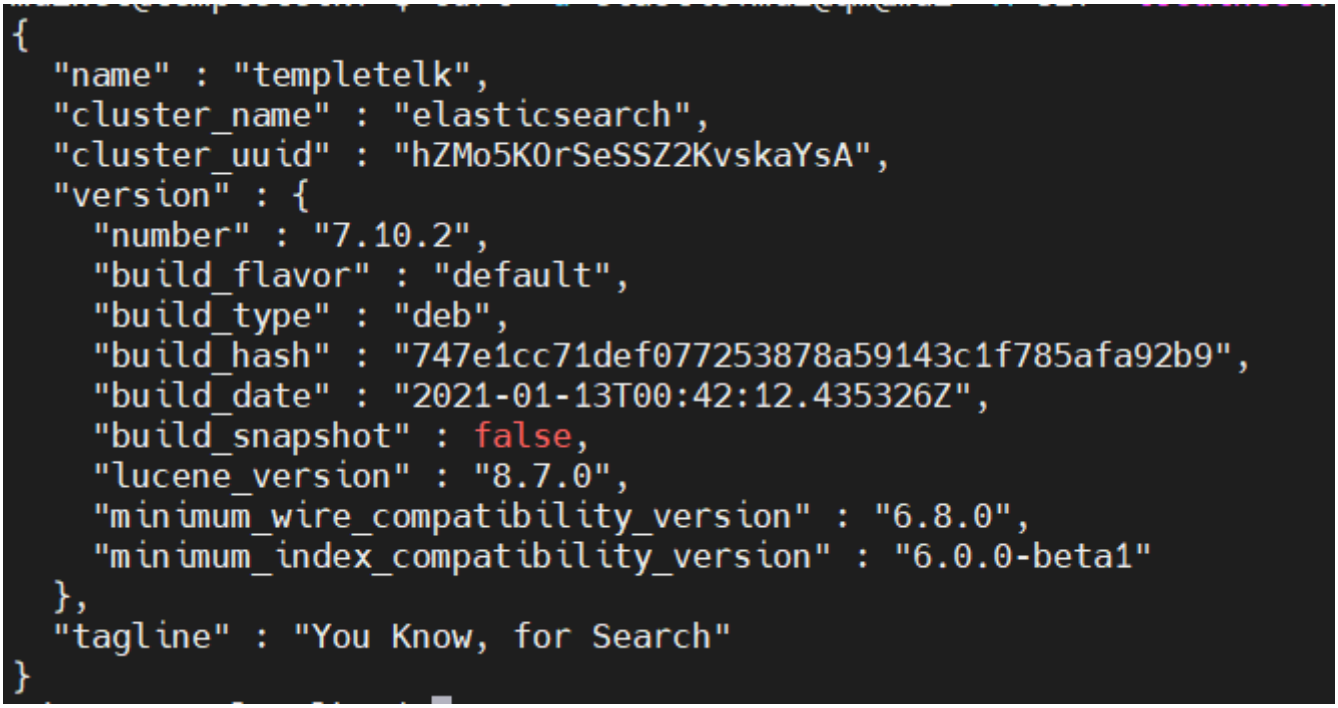
Upgrade OpenSearch - Redhat/CentOs

Antes de iniciar a ação, é importante lembrar que o servidor que deseja atualizar deve estar na versão 7.10.2 do ElasticSearch.

Para conferir a versão do seu ElasticSearch, faça login no servidor usando um cliente SSH execute o comando abaixo:

```
curl -u elastic:senha* -X GET "localhost:9200?pretty"
```



Se o seu servidor estiver em uma versão inferior a 7.10.2, siga os passos abaixo. Caso esteja na versão 7.10.2, siga para o próximo passo.

**O campo de senha deve ser preenchido com a senha configurada em sua aplicação atualmente.*

Atualizando o ELK para a versão 7.10.2:

Importante: Se o seu servidor estiver na versão 7.4 ou em alguma versão anterior a versão 7.10, clique aqui para acessar o tutorial a ser utilizado antes de realizar esse upgrade.

1. Efetuar login no servidor com um cliente SSH.

2. Pare os serviços do ElasticSearch:

```
systemctl stop elasticsearch.service
```

3. Liste as versões disponíveis da aplicação:

```
yum –showduplicates list elasticsearch
```

4. Selecione a versão 7.10.2 do ElasticSearch:

```
sudo yum install elasticsearch-7.10.2-1.x86_64
```

5. Recarregue os serviços:

```
systemctl daemon-reload
```

6. Inicie os serviços do ElasticSearch:

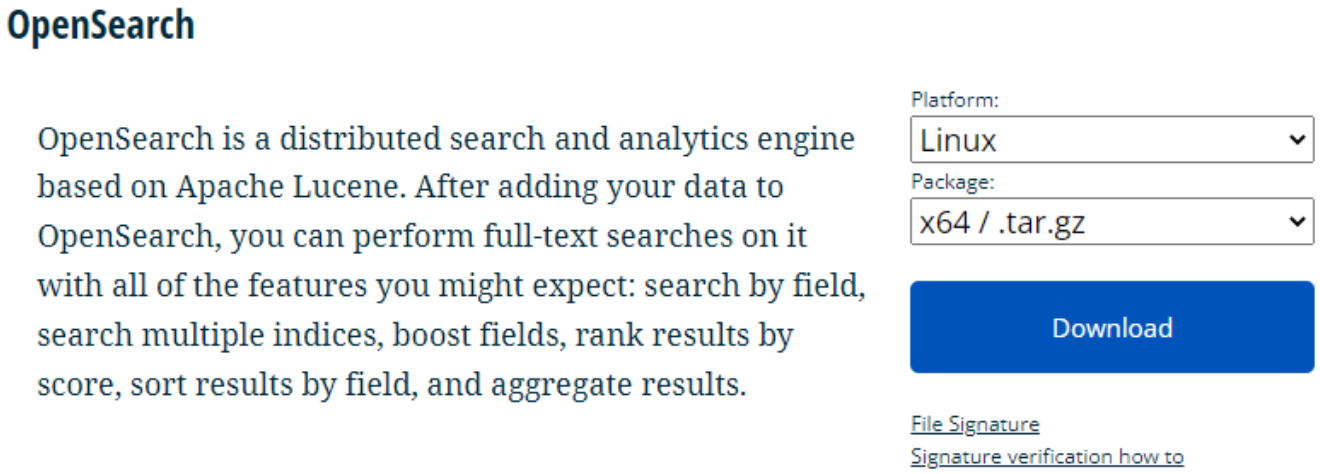
```
sudo systemctl start elasticsearch.service
```

7. Confira se a versão foi atualizada:

```
curl -u elastic:senhacorreta* -X GET "localhost:9200/?pretty"
```

Upgrade para o OpenSearch

1. Acesse https://opensearch.org/downloads.html, efetuar o download da versão 1.3.1 do OpenSearch no formato tar.gz.



Atenção: Neste tutorial o "x.x.x" referente a versão deverá ser substituído pelo número da versão que estiver disponível quando você fizer o download.

2. Efetue login no servidor com um cliente SSH.

3. Importe o arquivo baixado para o diretório /tmp.

4. Acessar o diretório /tmp

```
cd /tmp
```

5. Extrair o arquivo do OpenSearch:

```
tar -zxf opensearch-x.x.x-linux-x64.tar.gz
```

6. Renomeie e mova a pasta do OpenSearch para o diretório /etc/ ou para o diretório que desejar mantê-lo:

```
cd /tmp
sudo mv opensearch-x.x.x/ opensearch/
sudo cp -r opensearch/ /etc/
```

7. Após realizar a cópia dos arquivos, os arquivos da pasta /tmp podem ser removidos:

```
cd /tmp
rm -rf opensearch-x.x.x/
```

8. Digite o comando abaixo para listar os aliases do seu cluster:

```
curl -X GET -u elastic:senhacorreta* "localhost:9200/_cat/aliases"
```

```
.kibana                  .kibana_2                          - - - -
.kibana-event-log-7.10.2 .kibana-event-log-7.10.2-000001 - - - true
.kibana_task_manager     .kibana_task_manager_2             - - - -
.security                .security-7                        - - - -
ilm-history-3            ilm-history-3-000001               - - - true
```

9. Remova todos aliases que possuem “kibana” em seu nome já que a partir de agora não utilizaremos mais o Kibana e isso pode causar erros na hora de iniciar a nova aplicação.

```
curl -u elastic:senhacorreta* -X DELETE "localhost:9200/.kibana_*?pretty"
```

```
{
  "acknowledged" : true
}
```

10. Desative a replicação para impedir que o Elasticsearch OSS replique enquanto você realiza o upgrade:

```
curl -u elastic:senhacorreta* -X PUT "localhost:9200/_cluster/settings?pretty" -H 'Content-
Type: application/json' -d'
{
"persistent": {
"cluster.routing.allocation.enable": "primaries"
}
}
'
```

```
> {
>   "persistent": {
>     "cluster.routing.allocation.enable": "primaries"
>   }
> }
> '
{
  "acknowledged" : true,
  "persistent" : {
    "cluster" : {
      "routing" : {
        "allocation" : {
          "enable" : "primaries"
        }
      }
    }
  },
  "transient" : { }
}
```

11. Defina as seguintes variáveis de ambiente:

ES_HOME: Caminho de onde está a instalação do ElasticSearch atualmente.

```
export ES_HOME=/usr/share/elasticsearch/
```

```
md2net@templetelk:/etc$ export ES_HOME=/usr/share/elasticsearch/
md2net@templetelk:/etc$ echo $ES_HOME
/usr/share/elasticsearch/
```

ES_PATH_CONF: Caminho de onde está presente as configurações do ElasticSearch atualmente.

```
export ES_PATH_CONF=/etc/elasticsearch/
```

```
md2net@templetelk:/etc$ export ES_PATH_CONF=/etc/elasticsearch/
md2net@templetelk:/etc$ echo $ES_PATH_CONF
/etc/elasticsearch/
```

OPENSEARCH_HOME: Caminho de onde será feita a instalação do OpenSearch.

```
export OPENSEARCH_HOME=/etc/opensearch/
```

```
md2net@templetelk:/etc$ export OPENSEARCH_HOME=/etc/opensearch/
md2net@templetelk:/etc$ echo $OPENSEARCH_HOME
/etc/opensearch/
```

OPENSEARCH_PATH_CONF: Caminho de onde será armazenada as configurações do OpenSearch.

```
export OPENSEARCH_PATH_CONF=/etc/opensearch/config
```

```
md2net@templetelk:~$ export OPENSEARCH_PATH_CONF=/etc/opensearch/config
md2net@templetelk:~$ echo $OPENSEARCH_PATH_CONF
/etc/opensearch/config
```

12. Acesse o diretório do OpenSearch:

```
cd /etc/opensearch/
```

13. Execute o comando para começar o upgrade da aplicação:

```
sudo ./bin/opensearch-upgrade
```

Se caso ao executar o comando acima você receber uma mensagem “Unable to detect installed elasticsearch version”, execute os passos abaixo:

1. Acesse novamente o arquivo de configuração do ElasticSearch:

```
cd /etc/elasticsearch
```

2. Entre no arquivo de configuração do ElasticSearch:

```
sudo vim elasticsearch.yml
```

3. Procure pela linha abaixo e comente-a no arquivo. Para comentar, basta inserir um “#” antes dela:

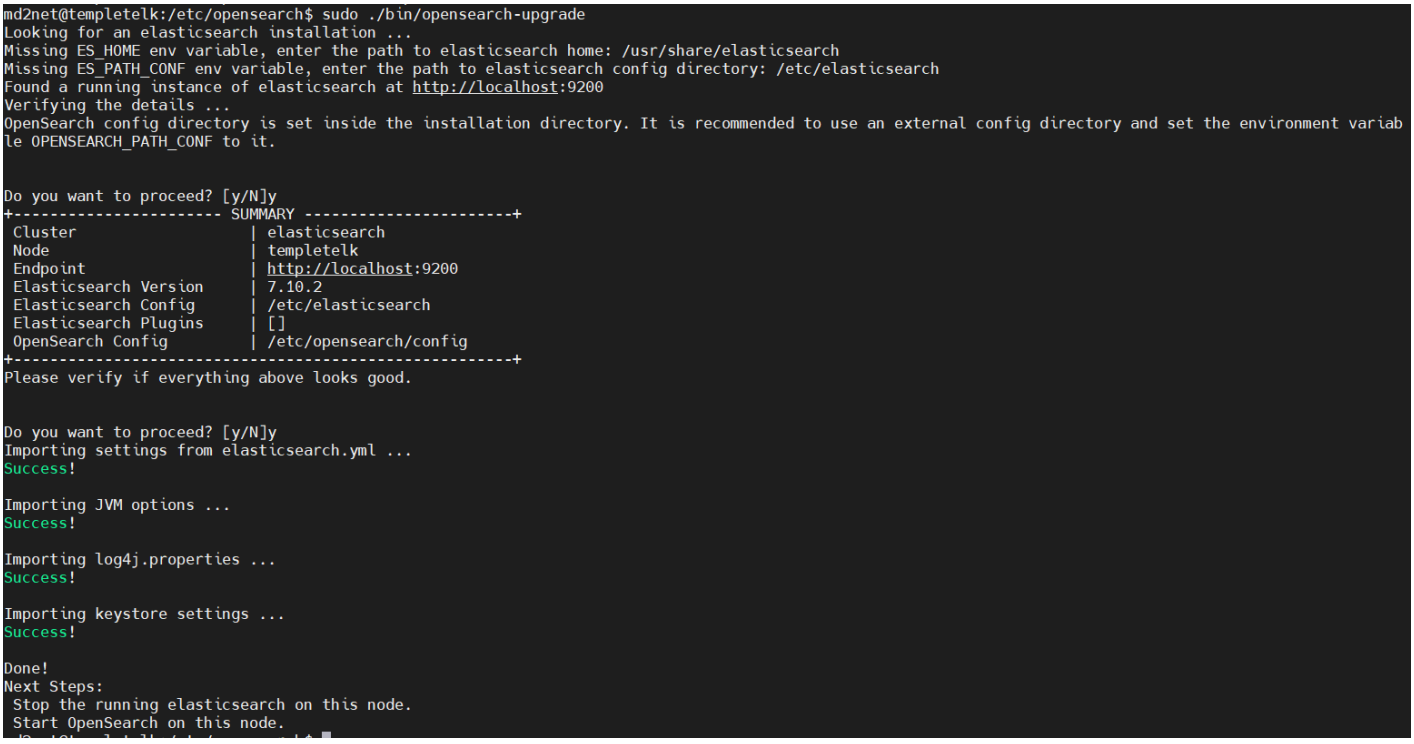
```
# xpack.security.enabled:  true
```

4. Salve o arquivo
- Aperte ESC.
- Digite “wq!” e pressione enter.

5. Reinicie os serviços do ElasticSearch e tente novamente.

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

14. Upgrade concluído:



15. Pare os serviços do ElasticSearch:

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

Instalando os plugins de segurança do OpenSearch:

1. Acesse a pasta das ferramentas de segurança dos plugins do OpenSearch:

```
cd /etc/opensearch/plugins/opensearch-security/tools
```

2. Verifique se o script “install_demo_configuration.sh” é um arquivo executável:

```
md2net@templetelk:/etc/opensearch/plugins/opensearch-security/tools$ ll
total 52
drwxr-xr-x 2 md2net md2net  4096 Mar 30 20:49 ./
drwxr-xr-x 4 md2net md2net  4096 Mar 30 20:49 ../
-rw-r--r-- 1 md2net md2net   227 Mar 30 21:09 audit_config_migrater.bat
-rw-r--r-- 1 md2net md2net   868 Mar 30 21:09 audit_config_migrater.sh
-rw-r--r-- 1 md2net md2net   219 Mar 30 21:09 hash.bat
-rw-r--r-- 1 md2net md2net   854 Mar 30 21:09 hash.sh
-rw-r--r-- 1 md2net md2net 19698 Mar 30 21:09 install_demo_configuration.sh
-rw-r--r-- 1 md2net md2net   291 Mar 30 21:09 securityadmin.bat
-rw-r--r-- 1 md2net md2net   897 Mar 30 21:09 securityadmin.sh
```

Como podemos ver na imagem acima, atualmente o script não está no modo executável.

3. Caso não seja, execute o comando abaixo e em seguida o script ficará com uma cor diferente e um asterisco ao final dele:

```
sudo chmod +x install_demo_configuration.sh
```

```
md2net@templetelk:/etc/opensearch/plugins/opensearch-security/tools$ chmod +x install_demo_configuration.sh
md2net@templetelk:/etc/opensearch/plugins/opensearch-security/tools$ ll
total 52
drwxr-xr-x 2 md2net md2net  4096 Mar 30 20:49 ./
drwxr-xr-x 4 md2net md2net  4096 Mar 30 20:49 ../
-rw-r--r-- 1 md2net md2net   227 Mar 30 21:09 audit_config_migrater.bat
-rw-r--r-- 1 md2net md2net   868 Mar 30 21:09 audit_config_migrater.sh
-rw-r--r-- 1 md2net md2net   219 Mar 30 21:09 hash.bat
-rw-r--r-- 1 md2net md2net   854 Mar 30 21:09 hash.sh
-rwxr-xr-x 1 md2net md2net 19698 Mar 30 21:09 install_demo_configuration.sh*
-rw-r--r-- 1 md2net md2net   291 Mar 30 21:09 securityadmin.bat
-rw-r--r-- 1 md2net md2net   897 Mar 30 21:09 securityadmin.sh
```

4. Execute o script para iniciar a instalação das configurações de segurança do OpenSearch:

```
sudo ./install_demo_configuration.sh
```

```
md2net@templetelk:/etc/opensearch/plugins/opensearch-security/tools$ ./install_demo_configuration.sh
OpenSearch Security Demo Installer
 ** Warning: Do not use on production or public reachable systems **
Install demo certificates? [y/N] y
Initialize Security Modules? [y/N] y
Cluster mode requires maybe additional setup of:
  - Virtual memory (vm.max_map_count)

Enable cluster mode? [y/N] y
Basedir: /etc/opensearch
OpenSearch install type: .tar.gz on DISTRIB_ID=Ubuntu
OpenSearch config dir: /etc/opensearch/config
OpenSearch config file: /etc/opensearch/config/opensearch.yml
OpenSearch bin dir: /etc/opensearch/bin
OpenSearch plugins dir: /etc/opensearch/plugins
OpenSearch lib dir: /etc/opensearch/lib
Detected OpenSearch Version: x-content-1.2.4
Detected OpenSearch Security Version: 1.2.4.0

### Success
### Execute this script now on all your nodes and then start all nodes
### OpenSearch Security will be automatically initialized.
### If you like to change the runtime configuration
### change the files in ../securityconfig and execute:
"/etc/opensearch/plugins/opensearch-security/tools/securityadmin.sh" -cd "/etc/opensearch/plugins/opensearch-security/securityconfig" -icl -key "/etc/open
search/config/kirk-key.pem" -cert "/etc/opensearch/config/kirk.pem" -cacert "/etc/opensearch/config/root-ca.pem" -nhnv
### or run ./securityadmin_demo.sh
### To use the Security Plugin ConfigurationGUI
### To access your secured cluster open https://<hostname>:<HTTP port> and log in with admin/admin.
### (Ignore the SSL certificate warning because we installed self-signed demo certificates)
```

5. Inicie os serviços do OpenSearch:

```
cd /etc/opensearch
./bin/opensearch -d
```

6. Se a mensagem de erro abaixo relacionada a licença que era utilizada no ElasticSearch for mostrada:

```
md2net@templetelk:/etc/opensearch$ ./bin/opensearch -d
md2net@templetelk:/etc/opensearch$ uncaught exception in thread [main]
java.lang.IllegalArgumentException: unknown setting [xpack.license.self_generated.type] please check that any required plugins are installed, or check the
 breaking changes documentation for removed settings
        at org.opensearch.common.settings.AbstractScopedSettings.validate(AbstractScopedSettings.java:589)
        at org.opensearch.common.settings.AbstractScopedSettings.validate(AbstractScopedSettings.java:530)
        at org.opensearch.common.settings.AbstractScopedSettings.validate(AbstractScopedSettings.java:500)
        at org.opensearch.common.settings.AbstractScopedSettings.validate(AbstractScopedSettings.java:470)
        at org.opensearch.common.settings.SettingsModule.<init>(SettingsModule.java:161)
        at org.opensearch.node.Node.<init>(Node.java:463)
        at org.opensearch.node.Node.<init>(Node.java:319)
        at org.opensearch.bootstrap.Bootstrap$5.<init>(Bootstrap.java:242)
        at org.opensearch.bootstrap.Bootstrap.setup(Bootstrap.java:242)
        at org.opensearch.bootstrap.Bootstrap.init(Bootstrap.java:412)
        at org.opensearch.bootstrap.OpenSearch.init(OpenSearch.java:178)
        at org.opensearch.bootstrap.OpenSearch.execute(OpenSearch.java:169)
        at org.opensearch.cli.EnvironmentAwareCommand.execute(EnvironmentAwareCommand.java:100)
        at org.opensearch.cli.Command.mainWithoutErrorHandling(Command.java:138)
        at org.opensearch.cli.Command.main(Command.java:101)
        at org.opensearch.bootstrap.OpenSearch.main(OpenSearch.java:135)
        at org.opensearch.bootstrap.OpenSearch.main(OpenSearch.java:101)
For complete error details, refer to the log at /var/log/elasticsearch/opensearch.log
```

Acesse o diretório do OpenSearch:

```
cd /etc/opensearch/config
```

Abra o arquivo de configuração:

```
vim opensearch.yml
```

E comente a linha abaixo:

```
# xpack.license.self_generated.type: "basic"
```

```
# Please consult the documentation for further information:
# https://www.opensearch.org
#

---
http.port: "9200"
network.host: "0.0.0.0"
path.data: "/var/lib/elasticsearch"
path.logs: "/var/log/elasticsearch"
path.repo:
- "/backup"
transport.host: "localhost"
transport.tcp.port: "9300"
#xpack.license.self_generated.type: "basic"

######## Start OpenSearch Security Demo Configuration ########
# WARNING: revise all the lines below before you go into production
plugins.security.ssl.transport.pemcert_filepath: esnode.pem
plugins.security.ssl.transport.pemkey_filepath: esnode-key.pem
plugins.security.ssl.transport.pemtrustedcas_filepath: root-ca.pem
plugins.security.ssl.transport.enforce_hostname_verification: false
plugins.security.ssl.http.enabled: true
plugins.security.ssl.http.pemcert_filepath: esnode.pem
plugins.security.ssl.http.pemkey_filepath: esnode-key.pem
plugins.security.ssl.http.pemtrustedcas_filepath: root-ca.pem
plugins.security.allow_unsafe_democertificates: true
plugins.security.allow_default_init_securityindex: true
plugins.security.authcz.admin_dn:
  - CN=kirk,OU=client,O=client,L=test, C=de

plugins.security.audit.type: internal_opensearch
plugins.security.enable_snapshot_restore_privilege: true
plugins.security.check_snapshot_restore_write_privileges: true
plugins.security.restapi.roles_enabled: ["all_access", "security_rest_api_access"]
plugins.security.system_indices.enabled: true
plugins.security.system_indices.indices: [".opendistro-alerting-config", ".opendistro-alerting-alert*", ".opendistro-anomaly-results*", ".opendistro-anomaly-detector*", ".opendistro-anomaly-checkpoints", ".opendistro-anomaly-detection-state", ".opendistro-reports-*", ".opendistro-notifications-*", ".opendistro-notebooks", ".opensearch-observability", ".opendistro-asynchronous-search-response*", ".replication-metadata-store"]
node.max_local_storage_nodes: 3
######## End OpenSearch Security Demo Configuration ########
"config/opensearch.yml" 43L, 2252C                                                    43,1          Bot
```

Salve, feche o arquivo e tente iniciar a aplicação novamente.

Para salvar aperte ESC, digite “wq!” e em seguida aperte enter.

7. Se ao iniciar os serviços for exibida mensagens de erro relacionado a falta de permissão para acessar arquivos do ElasticSearch, como a mensagem abaixo:

```
Mar 31 16:41:55 templetelk opensearch[67617]: Caused by: java.nio.file.AccessDeniedException: /var/log/elasticsearch
Mar 31 16:41:55 templetelk opensearch[67617]:         at sun.nio.fs.UnixException.translateToIOException(UnixException.java:90) ~[?:?]
Mar 31 16:41:55 templetelk opensearch[67617]:         at sun.nio.fs.UnixException.rethrowAsIOException(UnixException.java:106) ~[?:?]
Mar 31 16:41:55 templetelk opensearch[67617]:         at sun.nio.fs.UnixException.rethrowAsIOException(UnixException.java:111) ~[?:?]
Mar 31 16:41:55 templetelk opensearch[67617]:         at sun.nio.fs.UnixFileSystemProvider.checkAccess(UnixFileSystemProvider.java:312) ~[?:?]
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.Security.ensureDirectoryExists(Security.java:420) ~[opensearch-1.2.4.ja>
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.FilePermissionUtils.addDirectoryPath(FilePermissionUtils.java:88) ~[ope>
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.Security.addFilePermissions(Security.java:320) ~[opensearch-1.2.4.jar:1>
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.Security.createPermissions(Security.java:274) ~[opensearch-1.2.4.jar:1.>
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.Security.configure(Security.java:137) ~[opensearch-1.2.4.jar:1.2.4]
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.Bootstrap.setup(Bootstrap.java:237) ~[opensearch-1.2.4.jar:1.2.4]
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.Bootstrap.init(Bootstrap.java:412) ~[opensearch-1.2.4.jar:1.2.4]
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.OpenSearch.init(OpenSearch.java:178) ~[opensearch-1.2.4.jar:1.2.4]
Mar 31 16:41:55 templetelk opensearch[67617]:         ... 6 more
Mar 31 16:41:55 templetelk opensearch[67617]: uncaught exception in thread [main]
Mar 31 16:41:55 templetelk opensearch[67617]: java.lang.IllegalStateException: Unable to access 'path.logs' (/var/log/elasticsearch)
Mar 31 16:41:55 templetelk opensearch[67617]: Likely root cause: java.nio.file.AccessDeniedException: /var/log/elasticsearch
Mar 31 16:41:55 templetelk opensearch[67617]:         at java.base/sun.nio.fs.UnixException.translateToIOException(UnixException.java:90)
Mar 31 16:41:55 templetelk opensearch[67617]:         at java.base/sun.nio.fs.UnixException.rethrowAsIOException(UnixException.java:106)
Mar 31 16:41:55 templetelk opensearch[67617]:         at java.base/sun.nio.fs.UnixException.rethrowAsIOException(UnixException.java:111)
Mar 31 16:41:55 templetelk opensearch[67617]:         at java.base/sun.nio.fs.UnixFileSystemProvider.checkAccess(UnixFileSystemProvider.java:312)
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.Security.ensureDirectoryExists(Security.java:420)
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.FilePermissionUtils.addDirectoryPath(FilePermissionUtils.java:88)
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.Security.addFilePermissions(Security.java:320)
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.Security.createPermissions(Security.java:274)
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.Security.configure(Security.java:137)
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.Bootstrap.setup(Bootstrap.java:237)
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.Bootstrap.init(Bootstrap.java:412)
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.OpenSearch.init(OpenSearch.java:178)
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.OpenSearch.execute(OpenSearch.java:169)
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.cli.EnvironmentAwareCommand.execute(EnvironmentAwareCommand.java:100)
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.cli.Command.mainWithoutErrorHandling(Command.java:138)
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.cli.Command.main(Command.java:101)
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.OpenSearch.main(OpenSearch.java:135)
Mar 31 16:41:55 templetelk opensearch[67617]:         at org.opensearch.bootstrap.OpenSearch.main(OpenSearch.java:101)
Mar 31 16:41:55 templetelk opensearch[67617]: For complete error details, refer to the log at /var/log/elasticsearch/opensearch.log
```

Acesse os diretórios e altere as permissões das pastas do ElasticSearch:

```
cd /var/lib
sudo chown -R seuusuario:seugrupo elasticsearch/
```

```
cd /var/log
sudo chown -R seuusuario:seugrupo elasticsearch/
```

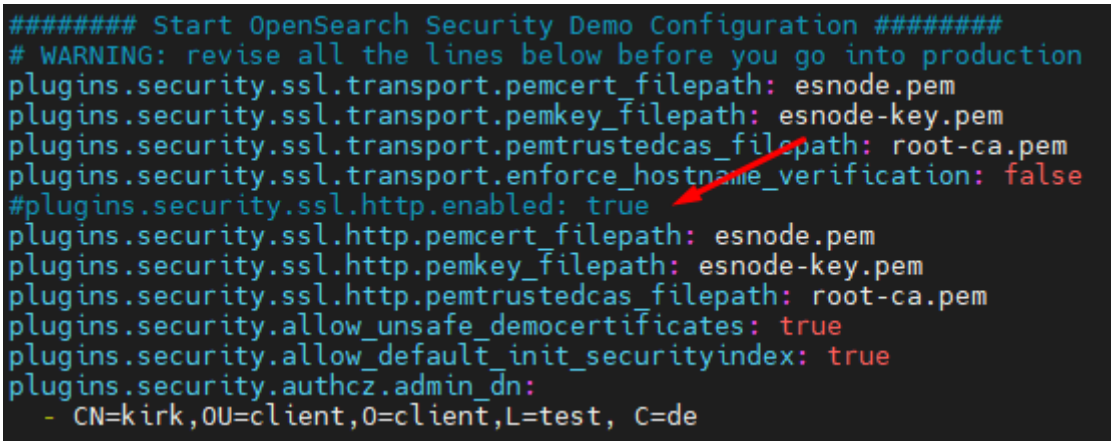
E tente novamente iniciar os serviços.

Caso seja exibida novamente a mensagem relacionado a falta de permissão, acesse o diretório exibido no erro e altere as suas permissões como demonstrado no passo acima.

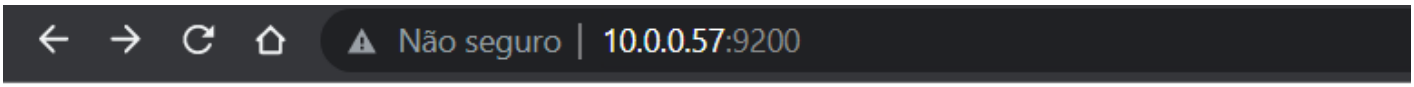
Obs: Após a atualização, a aplicação estará alocada no URL começado com https://, caso deseje alterar para o URL iniciado com http://, acesse o arquivo opensearch.yml

```
vim /etc/opensearch/config/opensearch.yml
```

Comente a linha: “plugins.security.ssl.http.enabled: true”



Acesse o OpenSearch pelo navegador com o usuário e senha “admin”:




```
{
  "name" : "templetelk",
  "cluster_name" : "opensearch",
  "cluster_uuid" : "hZMo5KOrSeSSZ2KvskaYsA",
  "version" : {
    "distribution" : "opensearch",
    "number" : "1.2.4",
    "build_type" : "tar",
    "build_hash" : "e505b10357c03ae8d26d675172402f2f2144ef0f",
    "build_date" : "2022-01-14T03:38:06.881862Z",
    "build_snapshot" : false,
    "lucene_version" : "8.10.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
```


8. Reative a replicação:

```
curl -u elastic:senhacorreta* -X PUT "localhost:9200/_cluster/settings?pretty" -H 'Content-
Type: application/json' -d'
{
"persistent": {
"cluster.routing.allocation.enable": "all"
}
}
'
```

Obs: *Todos os campos onde é mostrado “senhacorreta” deve ser preenchido com a senha configurada em seu servidor.

Criando o service do OpenSearch para facilitar a inicialização dos serviços:

1. Crie um arquivo chamado opensearch.service:

```
sudo vi /etc/systemd/system/opensearch.service
```

2. Edite o arquivo inserindo as informações abaixo (perceba que será necessário inserir o usuário de seu servidor no campo “user”):

```
[Unit]
```

```
Description=OpenSearch

[Service]
Type=simple
User=*insira aqui o usuário do seu servidor*
ExecStart=/etc/opensearch/bin/opensearch
Restart=on-failure
RestartSec=3
StartLimitBurst=3
StartLimitInterval=60
WorkingDirectory=/

[Install]
WantedBy=multi-user.target
```

3. Salve o arquivo.

Aperte ESC, digite “wq!” e aperte enter.

4. Execute-o:

```
systemctl start opensearch.service
```

5. Verifique o status para confirmar que ele foi iniciado corretamente:

```
systemctl status opensearch.service
```

Alterando a senha de acesso ao OpenSearch

Ao realizar o upgrade do ElasticSearch para o OpenSearch, a ferramenta automaticamente alterna o usuário e a senha de acesso da aplicação para “admin”. Segue abaixo um tutorial de como alterar esta senha.

1. Acesse o diretório onde se encontram as ferramentas de segurança da aplicação:

```
cd /etc/opensearch/plugins/opensearch-security/tools
```

2. Verifique se o script hash.sh está executável (caracteriza-se pela cor diferente do branco):

```
[md2net@edipo-dev tools]$ ll
total 48
-rw-r--r--. 1 md2net md2net   443 Apr  1 19:42 audit_config_migrater.bat
-rw-r--r--. 1 md2net md2net  1059 Apr  1 19:42 audit_config_migrater.sh
-rw-r--r--. 1 md2net md2net   443 Apr  1 19:42 hash.bat
-rw-r--r--. 1 md2net md2net  1046 Apr  1 19:42 hash.sh
-rwxr-xr-x. 1 md2net md2net 19739 Apr  1 19:42 install_demo_configuration.sh
-rw-r--r--. 1 md2net md2net   515 Apr  1 19:42 securityadmin.bat
-rwxr-xr-x. 1 md2net md2net   285 Apr  4 23:24 securityadmin_demo.sh
-rwxr-xr-x. 1 md2net md2net  1088 Apr  1 19:42 securityadmin.sh
```

3. Caso não esteja, execute o comando abaixo:

```
chmod +x hash.sh
```

4. Execute o script:

```
./hash.sh
```

5. Após executar, será perguntado qual senha deseja colocar em sua aplicação, digite a senha desejada, aperte enter e então aparecerá sua senha criptografa.

6. Copie a senha gerada.

7. Acesse o arquivo internal_users.yml

```
cd /etc/opensearch/plugins/opensearch-security/securityconfig
```

8. Entre no arquivo:

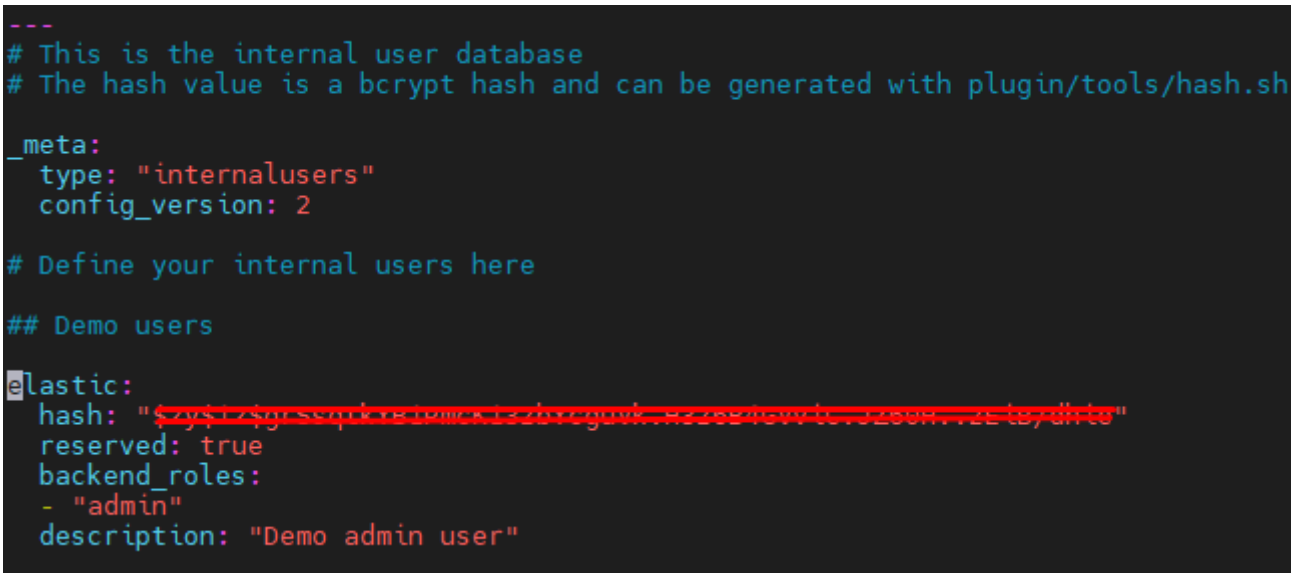
```
vim internal_users.yml
```

```
---
# This is the internal user database
# The hash value is a bcrypt hash and can be generated with plugin/tools/hash.sh

_meta:
  type: "internalusers"
  config_version: 2

# Define your internal users here

## Demo users

admin:
  hash: "[redacted]"
  reserved: true
  backend_roles:
  - "admin"
  description: "Demo admin user"
```

O primeiro campo de usuário “admin” é o usuário principal configurado atualmente. No campo de

“hash” você irá colar a senha que você copiou no passo anterior e caso deseje, também pode alterar o “admin” por algum usuário desejado.

No nosso caso, alteramos o usuário para “elastic” que é o que costumamos utilizar.



9. Acesse novamente o diretório dos scripts de segurança:

```
cd /etc/opensearch/plugins/opensearch-security/tools
```

10. Execute o comando abaixo para fazer backup da sua configuração atual antes de fazer as alterações:

```
./securityadmin.sh -backup my-backup-directory \
-icl \
-nhnv \
-cacert ../../../config/root-ca.pem \
-cert ../../../config/kirk.pem \
-key ../../../config/kirk-key.pem
```

11. Execute o comando abaixo para salvar as alterações de usuário e senha.

```
./securityadmin.sh -f ../securityconfig/internal_users.yml \
-t internalusers \
-icl \
-nhnv \
-cacert ../../../config/root-ca.pem \
-cert ../../../config/kirk.pem \
-key ../../../config/kirk-key.pem
```

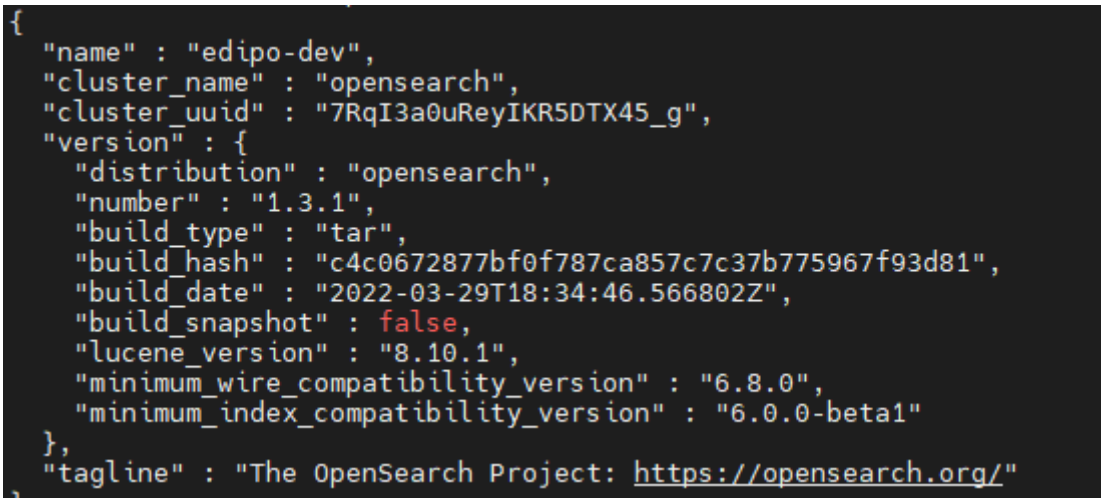
12. Reinicie os serviços do Opensearch:

```
sudo systemctl restart opensearch.service
```

13. Teste a conexão com o novo usuário e senha:

```
curl -u usuario:senhacorreta* -X GET "localhost:9200?pretty"
```

O comando deve exibir uma resposta parecida com esta:



Desativando os serviços do ElasticSearch para não iniciarem mais junto com o servidor:

```
sudo systemctl disable elasticsearch.service
```

Ativando os serviços do OpenSearch e OpenSearch Dashboards para iniciarem junto com o servidor:

```
sudo systemctl enable opensearch.service
```

Revision #7
Created 21 April 2022 00:03:56
Updated 12 December 2022 21:10:44