es 7.17.4 x-pack 认证镜像

测试镜像版本：192.168.251.78/edoc2v5/elasticsearch:v7.17.4.1-0711

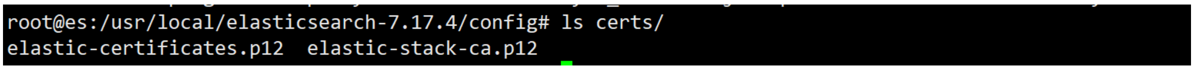
此版本单机和集群已经进行测试可以运行及生成相关认证用户。

主要变更

1. elasticsearch.yml 添加了 xpack相关安全配置，集群之间开启了ssl连接（开启xpack后集群必须要开启ssl）

```
xpack.security.enabled: true
xpack.security.authc.accept_default_password: true
xpack.security.transport.ssl.enabled: true
xpack.security.transport.ssl.verification_mode: certificate
xpack.security.transport.ssl.keystore.path: certs/elastic-certificates.p12
xpack.security.transport.ssl.truststore.path: certs/elastic-certificates.p12
```

2. config目录下添加了 certs目录，配置了默认的证书：



```
root@es:/usr/local/elasticsearch-7.17.4/config# ls certs/
elastic-certificates.p12  elastic-stack-ca.p12
```

3. 启动流程变更，elasticsearch-start.sh脚本开启子shell 初始化认证用户

```
.................

{
    if [ $(hostname) == "es" ];then
        if [ -f "/esdata/.espass.enc" ];then
            echo "elastic auth user already init.."
        else
            while true;do
                status=$(curl -sIL -w "%{http_code}\n" -o /dev/null es:9200)
                if [ "$status" == "401" ];then
                    yes y | ./bin/elasticsearch-setup-passwords auto >
/esdata/.espass
                    espass=$(cat /esdata/.espass | awk '/elastic =/{print
$NF}')
                    curl -u elastic:"${espass}" -H "Content-Type:
application/json" -XPUT http://es:9200/_security/role/edoc2Role -d '
                    {
                        "indices": [
                            {
                              "names": [
                                "*"
                              ],
                              "privileges": [
                                "all"
                              ]
                            }
                          ]
                    }'
                    curl -u elastic:"${espass}" -H "Content-Type:
application/json" -XPOST http://es:9200/_security/user/edoc2 -d '
                    {
                      "password" : "1qaz2WSX",
                      "roles" : ["edoc2Role","elastic_admin"]
                    }'

                    openssl enc -e -aes256 -pbkdf2 -in /esdata/.espass -out
/esdata/.espass.enc -a -pass pass:edoc2@edoc2
                    rm -f /esdata/.espass
                    break
                fi
                echo "elasticsearch No startup completed, wite for 5s.. "
                sleep 5
            done
        fi
    fi
} &

su elasticsearch -c "./bin/elasticsearch"
```

1） 后台启动子shell 等待 es启动完成

2）判断启动节点hostname是否为es，其作为初始化认证用户节点

3）初始化后的集群，会在es数据目录生成 /esdata/.espass.enc es默认系统用户的加密文件，判断此文件是否存在决定是否进行认证用户的初始化

4）通过请求es状态码 返回401 判断，es是否启动完成，启动完成则进行相应初始化

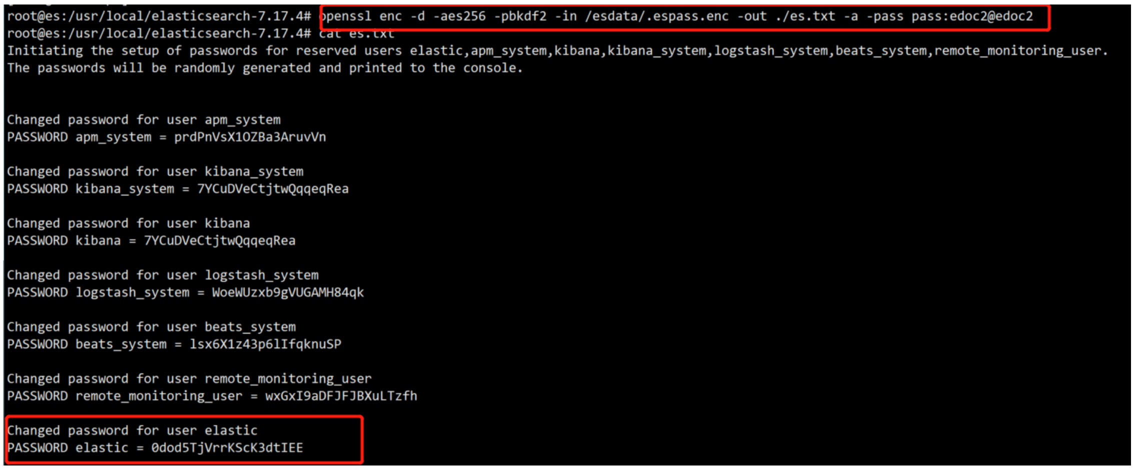
5）调用 elasticsearch-setup-passwords 自动生成随机密码，并获取elastic管理员密码

6）使用elastic管理用户创建 edoc2Role，创建edoc2用户绑定到edoc2Role，并设置其密码为 1qaz2WSX

7）对生成的随机明文密码 /esdata/.espass 文件进行对称加密，加密密码为 edoc2@edoc2 ，并删除明文密码

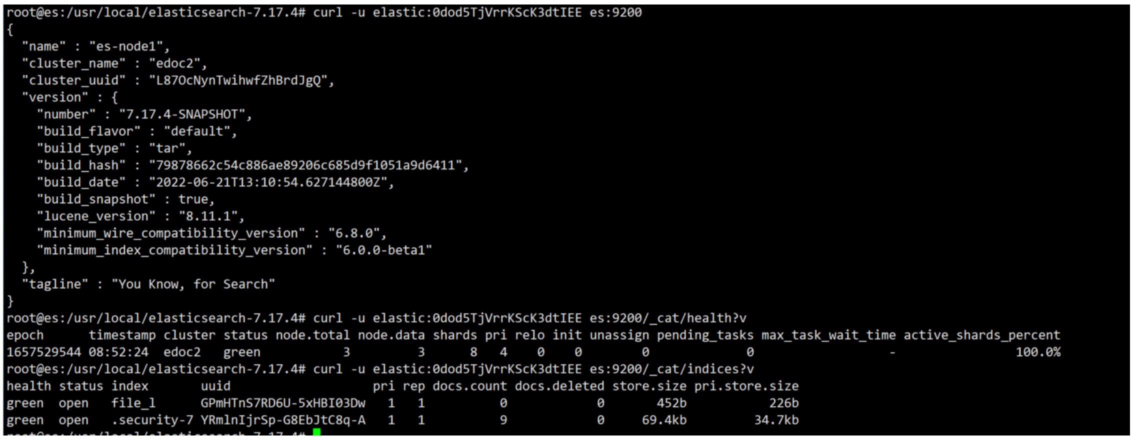
3. 管理员密码获取

```
openssl enc -d -aes256 -pbkdf2 -in /esdata/.espass.enc -out ./es.txt -a -
pass pass:edoc2@edoc2
```



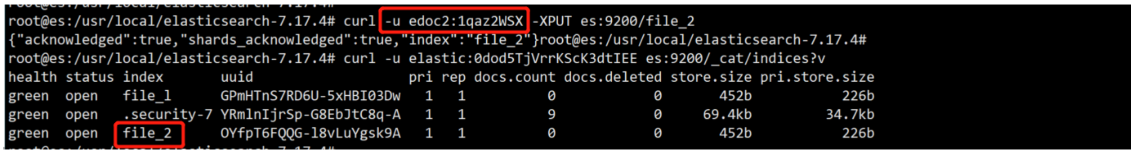
```
root@es:/usr/local/elasticsearch-7.17.4# openssl enc -d -aes256 -pbkdf2 -in /esdata/.espass.enc -out ./es.txt -a -pass pass:edoc2@edoc2
root@es:/usr/local/elasticsearch-7.17.4# cat es.txt
Initiating the setup of passwords for reserved users elastic,apm_system,kibana,kibana_system,logstash_system,beats_system,remote_monitoring_user.
The passwords will be randomly generated and printed to the console.


Changed password for user apm_system
PASSWORD apm_system = prdPnVsX1OZBa3AruvVn

Changed password for user kibana_system
PASSWORD kibana_system = 7YCuDVeCtjtwQqqeqRea

Changed password for user kibana
PASSWORD kibana = 7YCuDVeCtjtwQqqeqRea

Changed password for user logstash_system
PASSWORD logstash_system = WoeWUzxb9gVUGAMH84qk

Changed password for user beats_system
PASSWORD beats_system = lsx6X1z43p6lIfqknuSP

Changed password for user remote_monitoring_user
PASSWORD remote_monitoring_user = wxGxI9aDFJFJBXuLTzfh

Changed password for user elastic
PASSWORD elastic = 0dod5TjVrrKScK3dtIEE
```

4. 查看集群状态信息需要有管理员权限

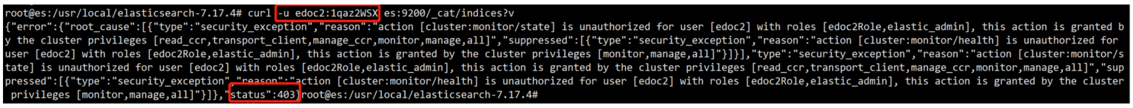


```
root@es:/usr/local/elasticsearch-7.17.4# curl -u elastic:0dod5TjVrrKScK3dtIEE es:9200
{
  "name" : "es-node1",
  "cluster_name" : "edoc2",
  "cluster_uuid" : "L87OcNynTwihwfZhBrdJgQ",
  "version" : {
    "number" : "7.17.4-SNAPSHOT",
    "build_flavor" : "default",
    "build_type" : "tar",
    "build_hash" : "79878662c54c886ae89206c685d9f1051a9d6411",
    "build_date" : "2022-06-21T13:10:54.627144800Z",
    "build_snapshot" : true,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
root@es:/usr/local/elasticsearch-7.17.4# curl -u elastic:0dod5TjVrrKScK3dtIEE es:9200/_cat/health?v
epoch      timestamp cluster status node.total node.data shards pri relo init unassign pending_tasks max_task_wait_time active_shards_percent
1657529544 08:52:24  edoc2   green           3         3      8   4    0    0        0             0                  -                100.0%
root@es:/usr/local/elasticsearch-7.17.4# curl -u elastic:0dod5TjVrrKScK3dtIEE es:9200/_cat/indices?v
health status index       uuid                   pri rep docs.count docs.deleted store.size pri.store.size
green  open   file_1      GPmHTnS7RD6U-5xHBI03Dw   1   1          0            0       452b           226b
green  open   .security-7 YRmlnIjrSp-G8EbJtC8q-A   1   1          9            0     69.4kb         34.7kb
```

5. 应用用户 edoc2赋予的索引操作相关的所有权限



```
root@es:/usr/local/elasticsearch-7.17.4# curl -u edoc2:1qaz2WSX -XPUT es:9200/file_2
{"acknowledged":true,"shards_acknowledged":true,"index":"file_2"}root@es:/usr/local/elasticsearch-7.17.4#
root@es:/usr/local/elasticsearch-7.17.4# curl -u elastic:0dod5TjVrrKScK3dtIEE es:9200/_cat/indices?v
health status index       uuid                   pri rep docs.count docs.deleted store.size pri.store.size
green  open   file_1      GPmHTnS7RD6U-5xHBI03Dw   1   1          0            0       452b           226b
green  open   .security-7 YRmlnIjrSp-G8EbJtC8q-A   1   1          9            0     69.4kb         34.7kb
green  open   file_2      OYfpT6FQQG-l8vLuYgsk9A   1   1          0            0       452b           226b
```



```
root@es:/usr/local/elasticsearch-7.17.4# curl -u edoc2:1qaz2WSX es:9200/_cat/indices?v
{"error":{"root_cause":[{"type":"security_exception","reason":"action [cluster:monitor/state] is unauthorized for user [edoc2] with roles [edoc2Role,elastic_admin], this action is granted b
y the cluster privileges [read_ccr,transport_client,manage_ccr,monitor,manage,all]","suppressed":[{"type":"security_exception","reason":"action [cluster:monitor/health] is unauthorized for
user [edoc2] with roles [edoc2Role,elastic_admin], this action is granted by the cluster privileges [monitor,manage,all]"}]}],"type":"security_exception","reason":"action [cluster:monitor/s
tate] is unauthorized for user [edoc2] with roles [edoc2Role,elastic_admin], this action is granted by the cluster privileges [read_ccr,transport_client,manage_ccr,monitor,manage,all]","sup
pressed":[{"type":"security_exception","reason":"action [cluster:monitor/health] is unauthorized for user [edoc2] with roles [edoc2Role,elastic_admin], this action is granted by the cluster
 privileges [monitor,manage,all]"}]},"status":403}root@es:/usr/local/elasticsearch-7.17.4#
```

6. es_single_backup.sh 单机备份脚本适配支持es认证