Elasticsearch 7版本部署

安装部署

安装包如下：

elasticsearch-7.16.2-linux-x86_64.tar.gz

kibana-7.16.2-linux-x86_64.tar.gz

所有节点重复下列操作：

0. 创建elasticsearch用户和组

```
groupadd elasticsearch
useradd elasticsearch -g elasticsearch
```

1. 解压安装包，创建数据和日志目录，赋权

```
tar -xzvf /home/elasticsearch/elasticsearch-7.16.2-linux-x86_64.tar.gz

tar -xzvf /home/elasticsearch/kibana-7.16.2-linux-x86_64.tar.gz

mkdir -p /u01/elasticsearch/data
mkdir -p /u01/elasticsearch/logs
chown elasticsearch:elasticsearch -R /u01/elasticsearch
chown elasticsearch:elasticsearch -R /home/elasticsearch/
```

2. 修改系统配置

```
#修改系统控制参数，调整虚拟机map最大值
echo 'vm.max_map_count=655300' >> /etc/sysctl.conf
#令其生效
sysctl -p
```

3. 修改配置文件

elasticsearch.yml

```
#Path setting
path:
  data: /u01/elasticsearch/data
  logs: /u01/elasticsearch/logs
```

```
#Cluster name
cluster.name: fraudCluster
#Node Name
node.name: fraud46
#Network Host
network.host: 10.150.19.46
#discovery and cluster formation settings
discovery.seed_hosts:
   - fraud47:19300
   - fraud48:19300
   - fraud46:19300
#初次生成集群需要配置，重启后删除
cluster.initial_master_nodes:
   - fraud46
   - fraud47
   - fraud48

#http端口
http.port: 19200
#tcp端口
transport.port: 19300

#禁止下载地理图示信息 （开启需外网）
ingest.geoip.downloader.enabled: false


#安全配置开启（以下配置需要开启安全配置才需要放开）！！！！！！！
xpack.security.enabled: true

#节点间ssl加密通信
#xpack.security.transport.ssl.enabled: true
#xpack.security.transport.ssl.verification_mode: certificate
#xpack.security.transport.ssl.client_authentication: required
#xpack.security.transport.ssl.keystore.path: elastic-certificates.p12
#xpack.security.transport.ssl.truststore.path: elastic-certificates.p12
#客户端和ES集群https加密
#xpack.security.http.ssl.enabled: true
#xpack.security.http.ssl.keystore.path: /home/elasticsearch/config/http.p12(要输
入绝对路径)
```

jvm.options

es内嵌的jvm通常已经设置好了jvm参数。大部分情况无需修改。

生产情况堆内存调整为32G

-Xms32700m
-Xmx32700m

4. 修改kibana配置

kibana.yml

```
server.port: 15601
server.host: "fraud47"
elasticsearch.hosts: ["http://fraud47:19200"]
```

开启安全配置

如果当前集群内正有ES和kibana实例在跑，先停止

1. 开启最小安全配置

为内置设置用户名密码

此操作只能在一个集群内设置一次

1. 在无密码情况下启动ES集群

```
#使用内嵌jdk
export JAVA_HOME=""
./elasticsearch -d -p pid
```

2. 设置密码（集群内任意节点）

开启另一个终端窗口

如果想要生成随机密码

```
./bin/elasticsearch-setup-passwords auto
```

如果想要使用自定义密码

```
./bin/elasticsearch-setup-passwords interactive
```

如图：

```
[root@h1 bin]# sh elasticsearch-setup-passwords interactive
warning: usage of JAVA_HOME is deprecated, use ES_JAVA_HOME
Future versions of Elasticsearch will require Java 11; your Java version from
1.8.0_191/jre] does not meet this requirement. Consider switching to a distri
csearch with a bundled JDK. If you are already using a distribution with a bu
e the JAVA_HOME environment variable is not set.
Initiating the setup of passwords for reserved users elastic,apm_system,kiban
logstash_system,beats_system,remote_monitoring_user.
You will be prompted to enter passwords as the process progresses.
Please confirm that you would like to continue [y/N]y


Enter password for [elastic]:
Reenter password for [elastic]:
Enter password for [apm_system]:
Reenter password for [apm_system]:
Enter password for [kibana_system]:
Reenter password for [kibana_system]:
Enter password for [logstash_system]:
Reenter password for [logstash_system]:
Enter password for [beats_system]:
Reenter password for [beats_system]:
Enter password for [remote_monitoring_user]:
Reenter password for [remote_monitoring_user]:
Changed password for user [apm_system]
Changed password for user [kibana_system]
Changed password for user [kibana]
Changed password for user [logstash_system]
Changed password for user [beats_system]
Changed password for user [remote_monitoring_user]
Changed password for user [elastic]
[root@h1 bin]#
```

保存刚刚设置的密码，用curl命令测试下

```
curl -u elastic:密码 -XGET 192.168.14.226:19200/_cluster/health?pretty
```

为kibana设置密码

1. kibana.yml配置中添加

```
elasticsearch.username: "kibana_system"
```

2. 使用命令创建kibana用户的密钥库

```
./bin/kibana-keystore create
```

3. 将kibana_system用户的密码添加到密钥库

```
./bin/kibana-keystore add elasticsearch.password
```

4. 重启kibana
5. 用elastic用户登录kibana，密码和刚才生成的密码一致

2. 开启节点间TLS（基础安全级别）

在任一节点执行以下步骤：

1. 生成CA证书

```
./bin/elasticsearch-certutil ca
```

输入命令后，默认会在ES的安装目录生成一个CA证书

`elastic-stack-ca.p12`

mm：yhsj@gs2022

2. 生成节点的认证和私钥

```
./bin/elasticsearch-certutil cert --ca elastic-stack-ca.p12
```

指定由刚才生成的CA，颁发证书。默认生成私钥文件名是：

`elastic-certificates.p12`

mm：yhsj@gs2022

将生成的私钥 `elastic-certificates.p12` **拷贝到所有节点**ES安装目录下的config目录中

在每个节点执行以下步骤

1. 修改elasticsearch.yml配置

增加如下配置

```
#节点间ssl加密通信
xpack.security.transport.ssl.enabled: true
xpack.security.transport.ssl.verification_mode: certificate
xpack.security.transport.ssl.client_authentication: required
xpack.security.transport.ssl.keystore.path: elastic-certificates.p12
xpack.security.transport.ssl.truststore.path: elastic-certificates.p12
```

2. 在es的keystore中保存刚才输入的节点私钥的密码

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.keystore.secure_password
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.truststore.secure_password
```

mm：yhsj@gs2022

密码就是刚才CA的密码

3. 重启节点

3. 开启ES集群HTTPS访问

在任一节点执行如下命令

生成Certificate Signing Request (CSR)

1. 执行命令，为ES集群生成一个CSR证书

```
./bin/elasticsearch-certutil http
```

- When asked if you want to generate a CSR, enter `n`.
- When asked if you want to use an existing CA, enter `y`.
- Enter the path to your CA. This is the absolute path to the `elastic-stack-ca.p12` file that you generated for your cluster.
- Enter the password for your CA.
- Enter an expiration value for your certificate. You can enter the validity period in years, months, or days. For example, enter `90D` for 90 days.
- When asked if you want to generate one certificate per node, enter `y`.
- Each certificate will have its own private key, and will be issued for a specific hostname or IP address.
- When prompted, enter the name of the first node in your cluster. Use the same node name that you used when generating node certificates.
- Enter all hostnames used to connect to your first node. These hostnames will be added as DNS names in the Subject Alternative Name (SAN) field in your certificate.
- List every hostname and variant used to connect to your cluster over HTTPS.
- Enter the IP addresses that clients can use to connect to your node.

2. 完成上面操作后，会生成一个zip压缩文件，包含所需的私钥

`elasticsearch-ssl-http.zip`

目录结构如下

```
/elasticsearch
|_ README.txt
|_ http.p12
|_ sample-elasticsearch.yml
```

```
/kibana
|_ README.txt
|_ elasticsearch-ca.pem
|_ sample-kibana.yml
```

3. 将其中的/elasticsearch/http.p12拷贝至每一个节点的config目录下

在每个节点执行如下步骤

1. 修改elasticsearch.yml配置

增加如下配置

```
#客户端和ES集群https加密
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.keystore.path: /home/elasticsearch/config/http.p12(要输入绝对路径)
```

2. 在keyStore中保存私钥的密码

```
./bin/elasticsearch-keystore add
xpack.security.http.ssl.keystore.secure_password
```

3. 重启ES节点

为kibana访问ES配置HTTPS

在生成CSR的步骤中生成Certificate Signing Request (CSR)，生成的elasticsearch-ssl-http.zip文件中，kibana目录下有一个 `elasticsearch-ca.pem` 文件。我们通过配置该文件，使kibana信任ES的CA。

1. 将 `elasticsearch-ca.pem` 拷贝至kibana的config目录下；
2. 在 `kibana.yml` 中添加、修改配置

```
elasticsearch.ssl.certificateAuthorities: /home/elasticsearch/kibana-7.16.2-linux-x86_64/config/elasticsearch-ca.pem
#将该配置协议修改为HTTPS
elasticsearch.hosts: https://192.168.14.226:19200
```

3. 重启kibana。