链滴

Elasticsearch 权限控制插件 search-guard-2 安装

作者：kouzhuong

原文链接：https://ld246.com/article/1472803335867

来源网站：链滴

<h2>介绍</h2>
elasticsearch 权限控制的插件是有几个的，如官网提供的shield, http-basic 插，本文将要使用的search-guard-2插件等。除此之外，也可以通过应用自行控制，当然相应的功夫就下得多了。
本文介绍使用 search-guard, 相比shield来说，该插件大部分功能是免费使用的，当然功能上还是能很好的满足需求的。
<h2>安装</h2>
要使用search-guard-2插件，同时还需要安装 search-guard-ssh 插件，具体安装步骤如下：
1. 安装 search-guard-ssh 插件
<pre class="brush: java; light: true">bin/plugin install -b com.floragunn/search-guard-ssl/2.3.
.15</pre>
2. 下载 search-guard-ssl 源码(https://github.com/floagunncom/search-guard-ssl), 执行example-pki-scripts/example.sh(如果是windows环境可以考虑使用Cygwin运行)生成密钥库文件。
生成密钥库需要用到openssl，如果未安装，请先进行安装（）</
>
如果要使用其它的参数来生成密钥库文件，请按自己的需要修改各sh文件中的内容。
3. 成功生成密钥文件后，拷贝truststore.jks文件到elasticsearch-home/config/ 目录下，同时将 node-*-keystore.jks 分别拷贝到各个es节点上，放于config目下
4. 接着在config/elasticsearch.yml文件中 配置 search-guad-ssl 相关内容（注意修改其中不同的数据）
<pre class="brush: java; light: true">searchguard.ssl.transport.keystore_filepath: node-0-keys
ore.jks
searchguard.ssl.transport.keystore_password: changeit
searchguard.ssl.transport.truststore_filepath: truststore.jks
searchguard.ssl.transport.truststore_password: changeit
searchguard.ssl.transport.enforce_hostname_verification: false</pre>
5. 如果需要使用https进行访问，继续添加如下配置
<pre class="brush: java; light: true">searchguard.ssl.http.enabled: true
searchguard.ssl.http.keystore_filepath: node-0-keystore.jks
searchguard.ssl.http.keystore_password: changeit
searchguard.ssl.http.truststore_filepath: truststore.jks
searchguard.ssl.http.truststore_password: changeit</pre>
6. 添加 example-pki-scripts/ca/root-ca.crt 证书到系统中，此时启动elasticsearch, 便只能通过https://localhost:9200/访问成功了。下面即可始安装配置search-guard-2了。
7. 安装插件 search-guard-2
<pre class="brush: java; light: true">bin/plugin.bat install -b com.floragunn/search-guard-2/2
3.4.5</pre>
8. 配置config/elasticsearch.yml ，在其中加
<pre class="brush: java; light: true">searchguard.authcz.admin_dn:
  - "CN=kirk, OU=client, O=client, L=Test, C=DE"
searchguard.audit.type: internal_elasticsearch</pre>
其中，admin_dn的值需要根据前面密钥库文生成的时候使用的相关信息进行相应修改。同时拷贝kirk-keystore.jks到config目录（为了方便，与它的jks放到一起）
9. 启动elasticsearch , 然后在 linux上行下面的命令（ 默认密码 changeit, 默认集群名 elasticsearch，所以如果未进行修改，下面命令中

应参数可以去掉）
<pre class="brush: java; light: true">$ plugins/search-guard-2/tools/sgadmin.sh \
  -cd plugins/search-guard-2/sgconfig/ \
  -ks config/kirk-keystore.jks \
  -ts config/truststore.jks \
  -kspass changeit \
  -tspass changeit \
  -cn crimson-search-cluster \
  -nhnv</pre>
若是在windows上，则首先在 plugins/search-guard-2/tools/sgadmin.sh所在目录生成创建 sgadmin.bat文件，在其中添加如下内：
<pre class="brush: java; light: true">@echo off
setlocal
set DIR=%~dp0
java %JAVA_OPTS% -cp "%DIR%..\..\search-guard-ssl*;%DIR%..*;%DIR%..\..\..\lib*" com.floragunn.searchguard.tools.SearchGuardAdmin %*
endlocal</pre>
然后执行指令：
<pre class="brush: java; light: true">plugins\search-guard-2\tools\sgadmin.bat
   -cd plugins\search-guard-2\sgconfig\
   -ks config\kirk-keystore.jks
   -ts config\truststore.jks
   -kspass changeit
   -tspass changeit
   -cn crimson-search-cluster
   -nhnv</pre>
通过上述操作会将权限信息添加到集群索引中。此时访问https://localhost:9200/ 将会要求输入用户名密码，此处是[kirk(pwd: kirk)], 输入并确认，即可获取到当前信息
登录成功后 可以尝试访问 https://localhost:9200/_search 将会提示无权限。这里需要到 sgconfig\目录下相应文件中添加权限才行，
这里就不赘述了，可以到官网了解（https://github.com/floragunncom/search-guard/tree/v2.3.4.5）
<h2 class="brush: java; light: true">安装过程中的问题</h2>
1. 安装了search-guard-ssl 和 serch-guard-2后，并更新了相应的elasticsearch.yml配置，当访问的时候，提示：Search Guard not initialized (SG11)
解决办法：这是因为未始化search guard 权限配置信息的原因，执行上述步骤9即可。
2. 在执行步骤9的时候，示
<pre class="brush: java; light: true">FAIL: Expected 5 config types for node nYEdPSM4Tj2xR2TbtPk9A but got only []
Done with failures</pre>
解决办法：此问题在windows上LZ没有遇到，但是在linux环境上遇到了，具体什么原因没有找到，解读源码的时候，发现主要是在行com.floragunn.searchguard.tools.SearchGuardAdmin类中的下面的代码的时候，遇到 请求超的原因
<pre class="brush: java; light: true">ConfigUpdateResponse cur = tc.execute(ConfigUpdateAction.INSTANCE, new ConfigUpdateRequest(new String[]{"config","roles","rolesmapping","internalusers","actiongroups"})).actionGet();   </pre>
至于如何解决该问题，暂时还没找到办法。如果有谁知道的话，还请不吝赐教！
<span style="color: #ff0000;"

更新：
<span style="color: #008000;"
2016-09-03:
<span style="color: #008000;"
可以考虑在windows环境上部署一个与linux上的elasticsearch一样的服务，然后通过windows上的
务执行步骤9的操作，相应的数据会写入到集群中的。
2016-09-06:
经过5天的反复调试（真是浪费时
了），最终确认到问题所在：应该是系统资源不足的原因。因为用的虚拟机，开始分配的是1个cpu+
G内存，每次调试到 类 <a class="header" href="eclipse-javadoc:%E2%98%82=elasticsea
ch/src%5C/main%5C/java%3Corg">org.<a class="header" href="eclipse-javadoc:%E2%
8%82=elasticsearch/src%5C/main%5C/java%3Corg.elasticsearch">elasticsearch.<a class
"header" href="eclipse-javadoc:%E2%98%82=elasticsearch/src%5C/main%5C/java%3Corg.ela
ticsearch.transport">transport.TransportService 中
private void sendLocalRequest(
ong requestId, final String action, final TransportRequest request) 方法内，将任务添加到线程
中后
<pre class="brush: java; light: true">   final String executor = reg.getExecutor();
        if (ThreadPool.Names.SAME.equals(executor)) {
            //noinspection unchecked
            reg.processMessageReceived(request, channel);
        } else {
            threadPool.executor(executor).execute(new AbstractRunnable() {
                @Override
                protected void doRun() throws Exception {
                    //noinspection unchecked
                    reg.processMessageReceived(request, channel);
                }

                @Override
                public boolean isForceExecution() {
                    return reg.isForceExecution();
                }

                @Override
                public void onFailure(Throwable e) {
                    try {
                        channel.sendResponse(e);
                    } catch (Throwable e1) {
                        logger.warn("failed to notify channel of error message for action [" + action + "
", e1);
                        logger.warn("actual exception", e);
                    }
                }
            });</pre>

即上面else块内，然后任务就卡
不被调用了，但windows上是可以正常调用的。
所以猜想可能是资源不足的问题
于是尝试添加了一个核心，再调试，发现就可以正常处理了。

