Search-guard 在 Elasticsearch 2.3 上的运用

<u>笑然</u> / 2016-11-23 06:00:00 / 浏览数 4983 <u>安全工具</u> 工具 顶(0) 踩(0)

uni3orns

■■■■https://sec.xiaomi.com/article/16

背景

Elasticsearch是一个基于Lucene构建的开源,分布式,RESTful搜索引擎,大量使用于各种场景,随着不断的发展,不可避免的会产生安全问题,一些危害比较大的漏洞比如C 经过es1代到2代产品的过度,目前主流的方案就只有官方的shield以及开源search-guard,然而我厂比较扣。

search-guard

search-guard 更新到2.x后跟 shield 配置上很相似,相比1.x的版本逻辑上更加松散。

searchquard 优点有:

- 节点之间通过 SSL/TLS 传输
- 支持 JDK SSL 和 Open SSL
- 支持热载入,不需要重启服务
- 支持 kibana4 及 logstash 的配置
- 可以控制不同的用户访问不同的权限
- 配置简单

安装

安装search-guard-ssl

sudo bin/plugin install -b com.floragunn/search-guard-ssl/2.3.3.11

安装search-guard-2

sudo bin/plugin install -b com.floragunn/search-guard-2/2.3.3.0-rc1

证书

根据自身情况修改官方脚本生成admin证书、node证书、根证书,将 node 证书和根证书放在 elasticsearch 配置文件目录下,同时将admin证书和根证书放到search-guard 配置文件目录下(tips:证书需要统一生成)

配置 elasticsearch 支持 ssl

elasticsearch.yml增加以下配置:

重启 elasticsearch

注意:任何修改elasticsearch.yml的操作都需要重启elasticsearch才能生效

配置文件介绍

searchguard 主要有5个配置文件在 plugins/search-guard-2/sgconfig 下:

sg_config.yml:

主配置文件不需要做改动

sg_internal_users.yml:

本地用户文件,定义用户密码以及对应的权限。例如:对于 ELK 我们需要一个 kibana 登录用户和一个 logstash 用户:

密码可用plugins/search-guard-2/tools/hash.sh生成

sg_roles.yml:

权限配置文件,这里提供 kibana4 和 logstash 的权限样例

sg_roles_mapping.yml:

定义用户的映射关系,添加 kibana 及 logstash 用户对应的映射:

sg_action_groups.yml:
定义权限
加载配置并启用
如修改了searchguard,则需要重新加载配置执行
注意:search-guard配置的相关改动不需要重启elasticsearch,相关的配置实际上存储在searchguard 的indice下了
此文章基于以下软件版本,不同版本可能略有差异: elasticsearch 2.3.3 search-guard 2.3.3 RC1
点击收藏 0 关注 1 <u>L一篇:挖掘PHP禁用函数绕过利用姿势</u> 下一篇:【原创】bashshell实现自动 1. 0 条回复 • 动动手指,沙发就是你的了!
<u>登录</u> 后跟帖
先知社区
<u>现在登录</u>
热门节点
社区小黑板
目录
RSS <u>关于社区</u> 友情链接 社区小黑板