# 操作手册

## 1、文件介绍

项目总共包含三个文件，分别是采集系统信息的beat文件夹，其中包含有linux和win10两个系统的系统采集beat，详情后续介绍，另一个为compliance Service文件，该文件为一个spring boot项目文件，实现对采集数据的比对和存储，以及对存储结果的分析报告，最后一个为sql文件，包含windows和linux的配置数据，即数据库中config表数据。

## 2、文件详情

### 2.1 win10-beat

#### 2.1.1 文件信息

Windows文件中包含有的文件如下图2-1所示，分别为采集Windows系统的simbeat，以及simbeat的配置文件simbeat.yml，关于beat的配置均需要在该文件中进行修改，最后是Conf.conf文件，该文件存储beat需要运行的各检查项的命令行。

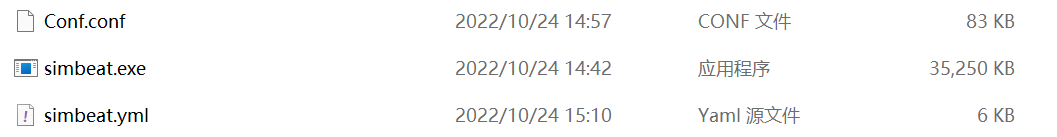


图2-1 文件截图

其中simbeat.yml文件，需要修改的字段如图2-2所示，其中period字段为beat采集一轮信息的时间间隔，图中的10s表示每10秒运行一遍beat，采集Conf.conf文件中存储的检查项的系统信息，可以根据需求进行修改。path字段存储文件中Conf.conf文件的路径，需要根据具体的路径进行修改。

对于图2-3的配置内容，配置的是beat采集的信息的发送方式以及发送的地址，beat的output方式有两种，分别是直接发给Elasticsearch以及发给Logstash，本项目采用发送给Logstash的方式。同时两种方式均需要配置发送方的ip地址，本图中地址为“192.168.1.170”，运行是可以根据存储采集信息主机的地址进行修改。

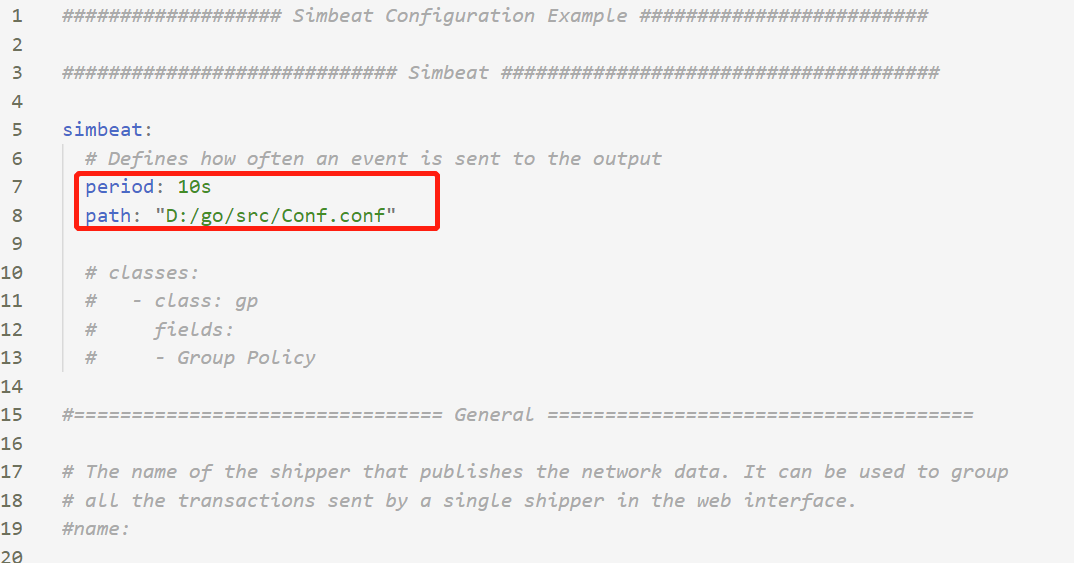


图2-2 配置文件内容

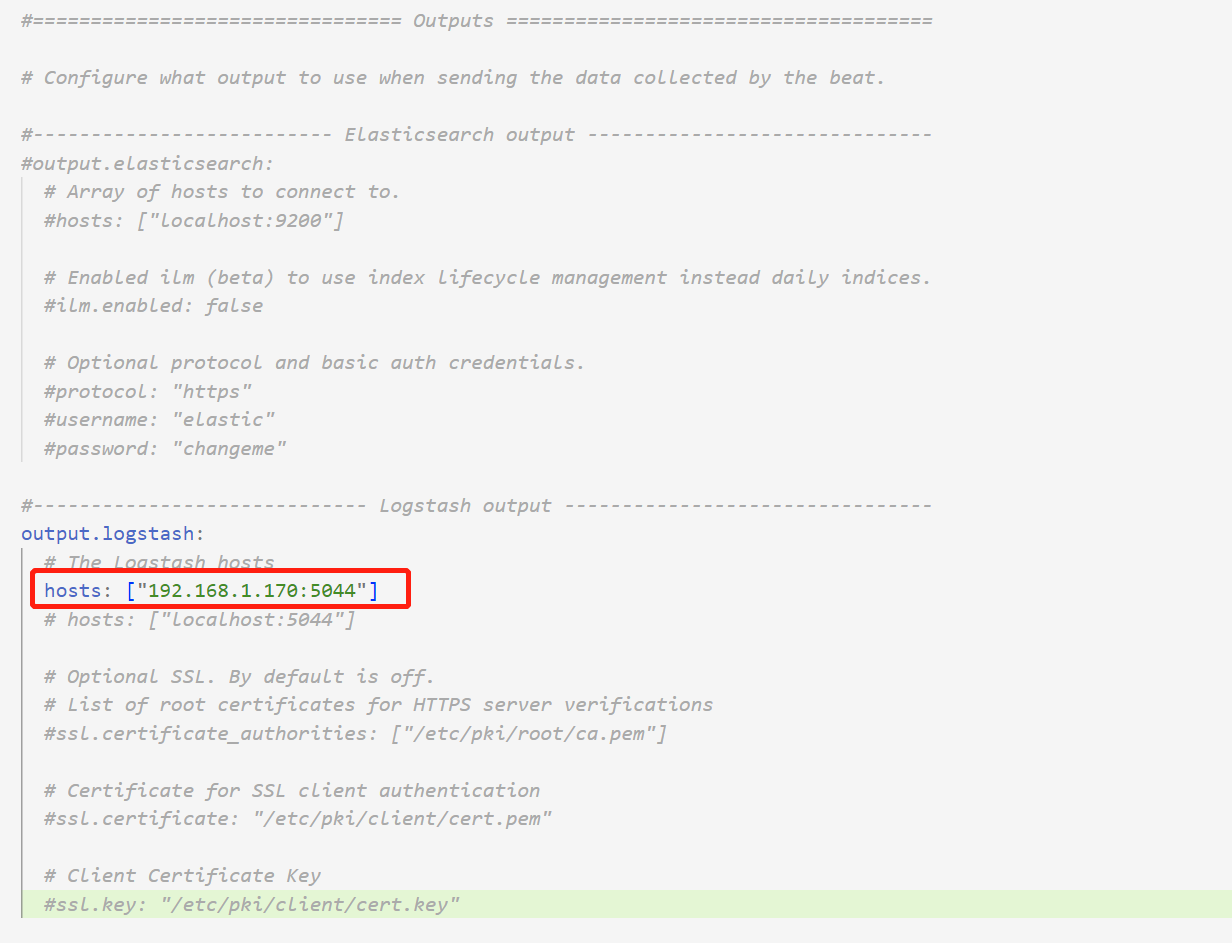


图2-3 配置文件内容

Conf.conf文件存储的是检查项的配置信息，具体如下图2-4所示，该文件一个json格式文件，每个检查项使用其规则id，里面包含有一个ruleId字段，存储检查项的规则id，param字段存储该检查项需要运行的命令行。若需要添加一个检查项，只需添加一个检查项内容，并将该检查项对应的命令行存储进去即可。

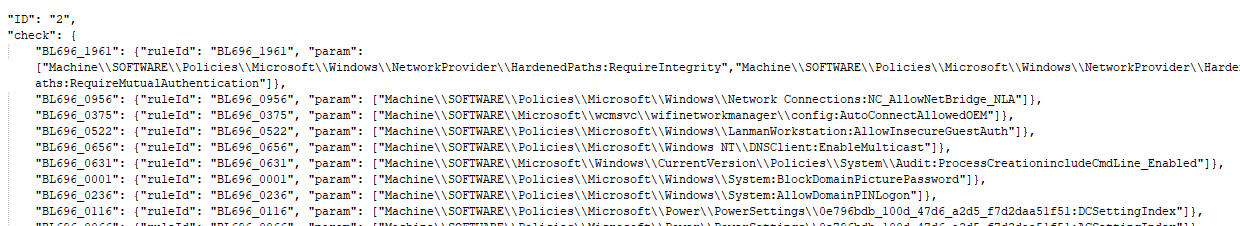


图2-4 conf文件内容

#### 2.2.2 运行方式

当设置完beat的配置信息后，运行命令“simbeat.exe -c simbeat.yml -e -d “\*””即可运行该beat文件。

### 2.2 linux-beat

#### 2.2.1 文件信息

Linux文件中包含有的文件如下图2-5所示，分别为采集Linux系统的examplebeat，以及examplebeat的配置文件examplebeat.yml，关于beat的配置均需要在该文件中进行修改，最后是linuxbeatfile文件，该文件存储beat需要运行的各检查项的命令行。

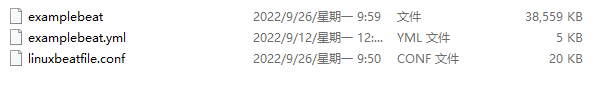


图2-5 文件截图

其中examplebeat.yml文件，需要修改的字段如图2-6所示，其中period字段为beat采集一轮信息的时间间隔，图中的1s表示即每1秒运行一遍beat，采集linuxbeatfile文件中存储的检查项的系统信息，可以根据需求进行修改。path字段，存储文件中linuxbeatfile.conf文件的路径，需要根据具体的路径进行修改。

对于图2-7的配置内容，配置的是beat采集的信息的发送方式以及发送的地址，beat的output方式有两种，分别是直接发给Elasticsearch以及发给Logstash，本项目采用发送给Logstash的方式。同时两种方式均需要配置发送方的ip地址，本图中地址为“222.20.75.121”，运行是可以根据存储采集信息主机的地址进行修改。

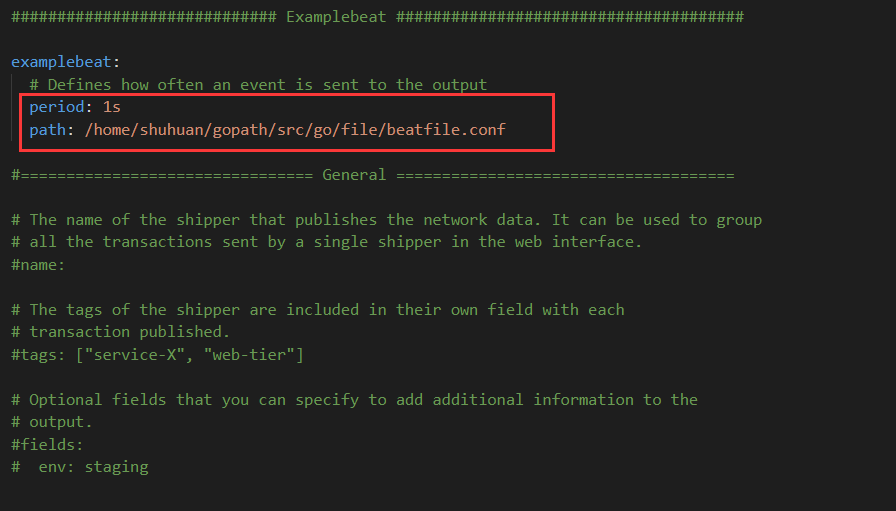


图2-6 配置文件内容

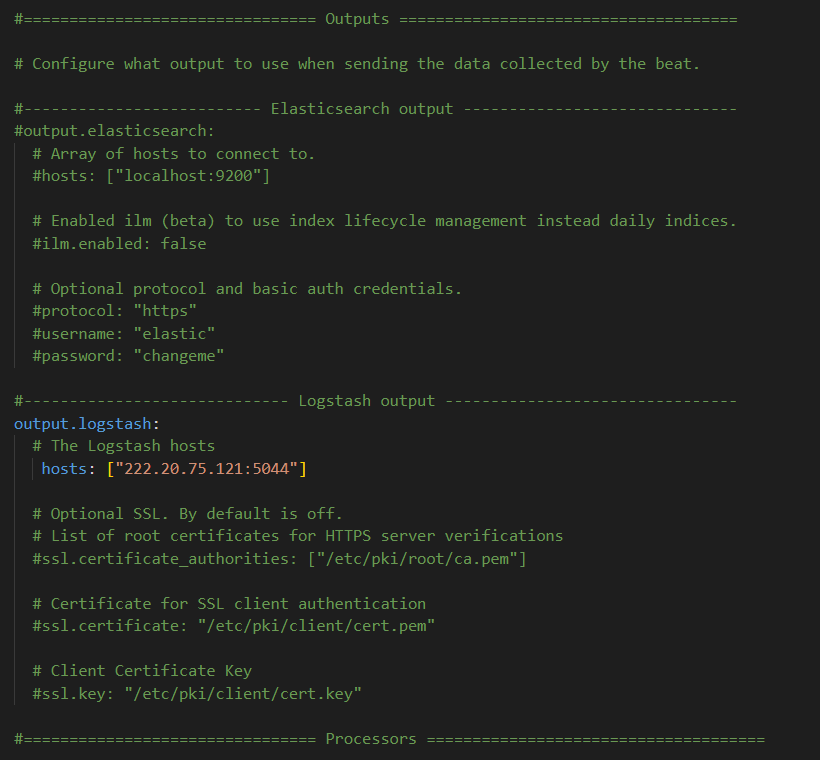


图2-7 配置文件内容

linuxbeatfile.conf文件存储的是检查项的配置信息，具体如下图2-8所示，该文件一个json格式文件，每个检查项使用其规则id，里面包含有一个ruleId字段，存储检查项的规则id，一个param字段，存储该检查项需要运行的命令行。若需要添加一个检查项，只需添加一个检查项内容，并将该检查项对应的命令行存储进去即可。

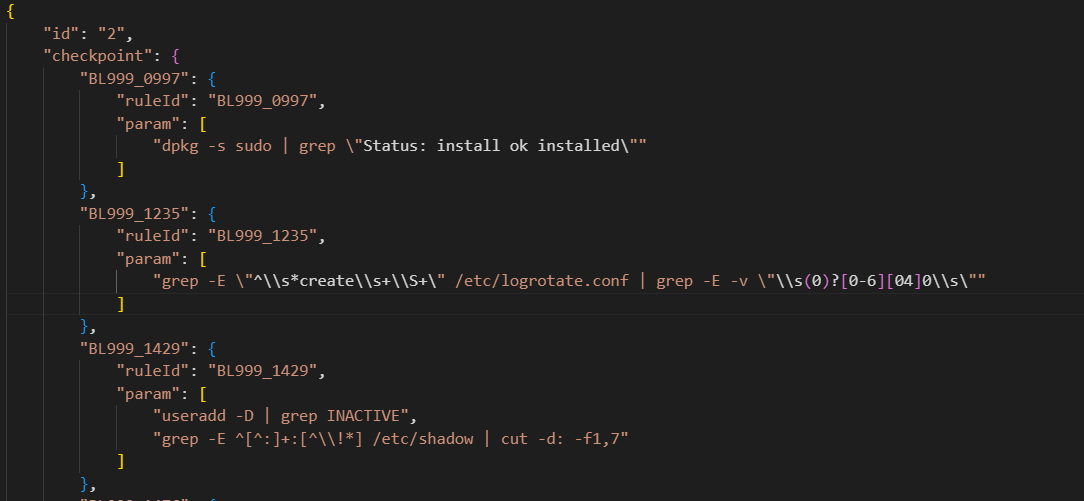


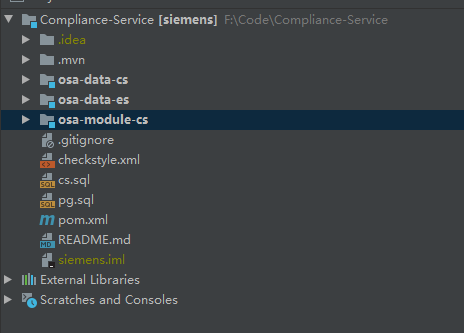
图2-8 conf文件内容

#### 2.2.2 运行方式

当设置完beat的配置信息后，运行命令“sudo ./examplebeat -e -d “\*””即可运行该beat文件。注意一定要使用sudo命令，因为有些检查项需要管理员权限才能获取到系统信息。

### 2.3 Compliance Service

该文件包含有三个spring boot模块，其中osa-data-cs模块读取数据库的信息，osa-data-es读取Elasticsearch数据库的信息，osa-module-cs模块整合上述两个模块，实现读取数据库数据和Elasticsearch数据进行数据比对和数据存储，最后并将比对结果进行统计分析的功能。



2-9 项目模块图

对于代码中需要修改的部分主要集中在module文件的配置文件部分，具体如下图所示，首先如图2-10所示，该部分配置的是数据库的信息，首先是url字段，存储的是数据库主机的ip地址，可以根据数据库的ip进行修改，然后是username字段和password字段，配置的是连接的数据库的用户名和密码，均需要根据情况进行修改配置。

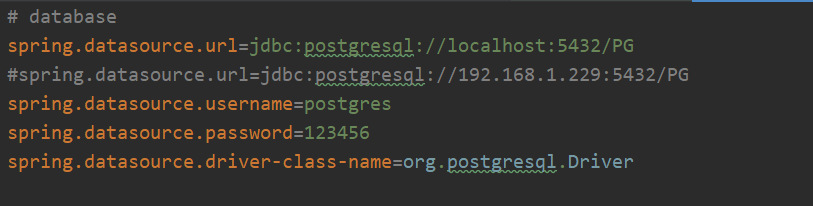


图2-10数据库部分

图2-11配置的是Elasticsearch数据库的信息，主要包括hostList字段，配置Elasticsearch所在主机的ip地址，index字段配置项目需要读取的索引的名字，这两个字段均需要根据实际情况进行修改。

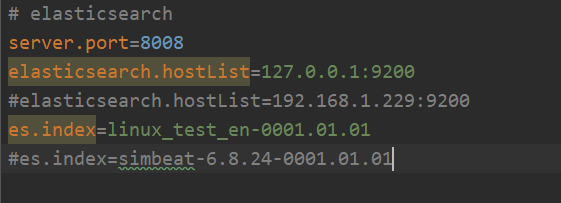


图2-11 Elasticsearch部分

图2-12配置的是结果报告的信息，包括beginTime和endTime字段，配置的是要那个时间段结果的统计报告，utc字段配置的是查看报告的人当前所在的时区，进行时区校准。然后zone字段和multiple字段规定查看报告的频度，图中为以1天为间隔查看时区是+8区的7月14号8时到7月22号8时的检测报告。

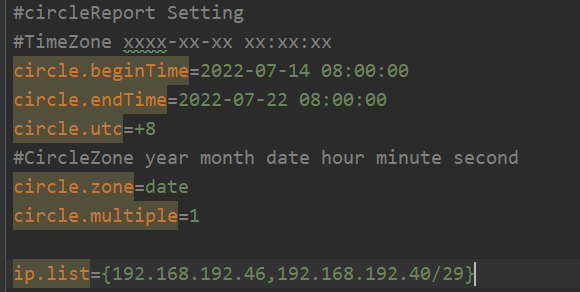


图2-12 报告时间部分

### 2.4 sql

Sql文件夹中包含有windows和linux配置文件的详细信息，也即数据库中的config表数据信息，具体文件如下图2-13所示。文件中的具体内容为一个sql语言的insert语句，插入config的数据信息。具体如图2-14所示。

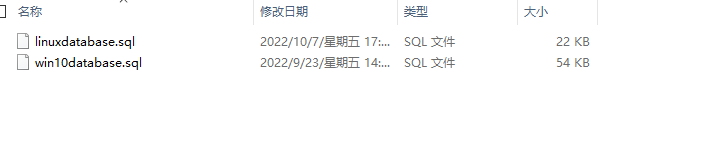


图2-13 文件截图

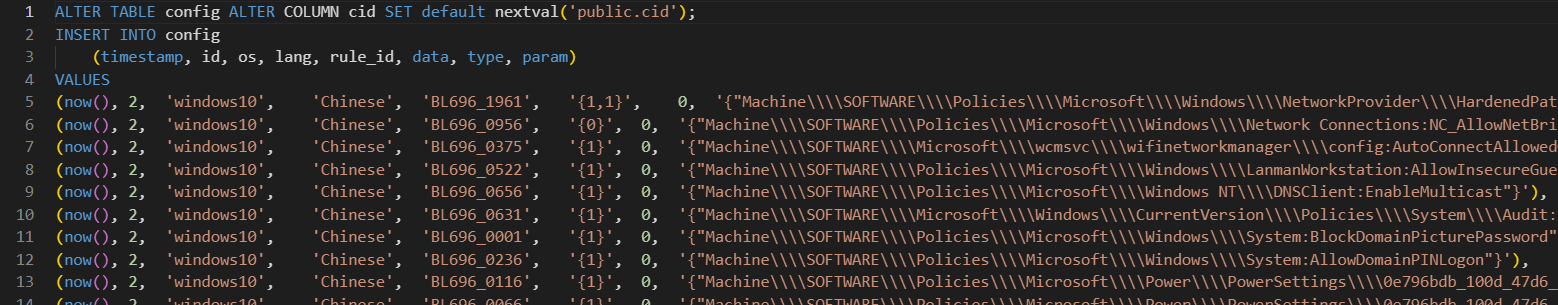


图2-14 windows文件内容