# 资产统计（变化资产、闲置资产、退网资产）

### 1. 简介

主要是通过对1）T\_HISTORY\_MODELRULES历史表相关数据、2)ES数据进行处理。

### 2. svn目录

1）代码路径：

a. 变化资产

<http://10.130.10.38:9999/svn/bdtsgz/branches/BDSSA/DataMining/Traffic_2.0a/src/main/scala/AssetStatistics/SubClass/changeAsset.scala>

b. 闲置资产

<http://10.130.10.38:9999/svn/bdtsgz/branches/BDSSA/DataMining/Traffic_2.0a/src/main/scala/AssetStatistics/SubClass/idleAsset.scala>

c. 退网资产

<http://10.130.10.38:9999/svn/bdtsgz/branches/BDSSA/DataMining/Traffic_2.0a/src/main/scala/AssetStatistics/SubClass/outAsset.scala>

2）配置文件路径：

<http://10.130.10.38:9999/svn/bdtsgz/branches/BDSSA/DataMining/Traffic_2.0a/conf/asset_statistics.properties>

账号：yt；密码：123456；（失效的话请用，账号：wzd, 密码：132456）

### 3. 开发环境

语言：Spark(Maven工程)、Scala、linux/window环境即可。

window下环境配置spark.master.url = local

linux下环境配置spark.master.url = spark://ip:7077

### 4. 模块运行

主要是运行” …/scala/AssetStatistics/**assetStatistics.scala**”进行调度的，

每天运行一次（时间设置为00:30）

### 5. 存在问题和注意事项

Q1: Traffic\_2.0a/… /scala/AssetStatistics/**assetStatistics.scala运行之前，必须先运行**[http://10.130.10.38:9999/svn/bdtsgz/branches/BDSSA/DataMining/Traffic\_rebuild/src/main/scala/jobFiveMinute/subJob/netflowProcess/](http://10.130.10.38:9999/svn/bdtsgz/branches/BDSSA/DataMining/Traffic_rebuild/src/main/scala/jobFiveMinute/subJob/netflowProcess/ntProcessMain.scala) ，因为相关历史数据需要靠它来生成。

Q2: **变化资产**主要是通过ES的事件表event\_yyyyMMdd (event\_rule\_name（端口异常(destip)、异常流量(destip))这2个维度进行整合判断的。

Q3: **退网资产**主要是通过对前30天的历史数据生成基线来预测的。

历史数据保存至T\_HISTORY\_MODELRULES

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | TYPE | TYPERESULT | IDENTITYRESULT | STANDBY01 | STANDBY02 |
| 唯一标识 | 退网资产 | 访问host的日期（格式为yyyymmdd） | history\_asset | 入库时间（long类型然后存string） | 当天的所有网元ip（用#合并） |

Q4: **闲置资产**主要是通过对一天中T\_HISTORY\_MODELRULES（type=’异常流量‘ and standby03=’tcp’）的相关数据作聚合来判断的。

Q5: **变化资产、退网资产、闲置资产**最终的结果保存至T\_SIEM\_DEV\_FIND。

|  |  |  |
| --- | --- | --- |
| 字段 | 类型 | 解释说明 |
| recordid | varchar(64) | 唯一标识 |
| ip | varchar(25) | 异常ip |
| isnew | int4(32) | null |
| flg | int4(32) | "flg" IS '0是新发现，1为拒绝入网，2入网,3退网资产,4变化资产,5闲置资产' |
| storagetime | timestamp(6) | 入库时间 |
| protocol | varchar(255) | null |
| port | varchar(255) | null |
| srcip | varchar(25) | null |
| dstip | varchar(25) | null |
| packagenum | varchar(25) | null |