触发原理：

目前机器学习有8种报警，每种报警都有对应的mysql表。

拿”异常设备 - 访问文件统计”报警举例，前14天如果有访问文件，每天都会在对应的表里面生成一条记录（如果当天没有访问文件则当天没有记录，以此类推需要生成14条记录），生成第15条记录时时，会用当天的实际值跟前14条算出来的基线进行比较（通过机器学习算法计算），如果大于该值，则触发报警，若小于该值则不触发报警，报警会在第二天0点0分触发，依次类推，第16条的基线会包括第15条的值。

手动触发流程：

拿”异常设备 - 访问文件统计”报警举例，在该表中插入14条基础数据（第14天的forecast,ucl,,err\_var需要有值并且比较小），插入第15条记录，多次上传下载业务文件，进ADdocker 在/opt/HolonetAnalytics/detection/目录下执行该条命令 python detector.py 1 '2021-01-26 23:59:59'（日期为第15条记录的日期）。

完成后需要删除user\_story\_anomalies对应的报警记录以及redis里第二个库中的记录，否则下次手动触发时不能生成

插入数据语句：

insert into device\_file\_counter\_forecasts(point, x\_axis, domain\_id, device\_id, forecast, actual, err\_var, created\_at, updated\_at) value  
 (1600099200,'2021-09-15',1,'00:e0:70:b5:75:ba','1','200','13.1','2021-09-17 00:00:00','2021-09-17 00:00:00');

