Log Analyzes 说明文档

01. 功能概述

用来读取软件中的日记信息，用来整理和提取日记中的信息，并输出到指定位置，方便对日记进行分析

02. 使用方法

将日记内容输出到 MySQL 数据库

bin\IDOL-Query.py -f logfile -t tablename [-d dbname | -P 3306 | .....]

将日记内容输出到 csv 文件

bin\CBK-Agent-Summary.py -f logfile -out csv

将日记内容分析并生成分析结果

bin\MSSQL-ErrorLog.py -f logfile -out report [-detail on]

03. 定制方法

编写启动程序：

参照 **doc/example_bin.txt** 模板添加 bin 目录下的启动程序，主要修改 **main** 函数的 p2 和 p3 里面的内容

p2 是日记分析模块

p3 是输出端方法

编写分析模块：

参照 **doc/example_mod_analysis.txt** 添加日记分析模块

模块定义的时候需要定义 2 个变量，分别是 2 个消息队列（queue）

第一个 queue 是从启动程序获取日记信息

第二个 queue 是将分析的结果放到队列中，并且由下一个进程来处理

如果想要输出端为 Report 模式，请参考“**根据输出端编写其余代码**” 其中的内容

可以参考 **mod.SQLDB** 模块中的方法，该模块会加载一个规则文件

规则文件：**mod/rules/Rules_MSSQL.py**

根据输出端编写其余代码：

To MySQL

由于输出到 MySQL 需要创建数据表，所以需要在 **mod.tools.TemplateMySQL** 类中添加一个创建表的模板

只接收字典类型的数据

To CSV

由于输出到 CSV 时需要创建 headers 信息，所以需要在 **mod.tools.TemplateCSV** 类中添加一个 headers 的模板

只接收字典类型的数据

To Report

只接收字典类型的数据

字典中必须包含如下 key：

type：值可以为 CPU、Memory、Disk、Network、Permission、Security、EventID、Others

name：用作标识

info：问题原因

keyword：作为匹配此条规则的关键字

solution：解决思路

输出结果为 html 文件

04. 授权模式

GNU General Public License v3.0