哈喽，亲爱的即友：

你能点进来，说明你有日志采集需求的，目前日志的版本管理，让我有些忐忑凌乱，为了日志世界的和平，请阅读一下我们的约定C:\Users\515203\AppData\Local\Temp\1510127839(1).png…

一：须知：

今后日志抽取相关将有git进行管理，大家请下拉最新的giveu-shop dev分支，在文件ELK日志采集规约中，日志原则上只保留两个线上版本的日志，每次新上线版本，需要抽取新版本的日志，请务必要查看历史版本的服务是否停用，如果停用，请在Excel表格中注明，以便停止抽取日志服务的进程。

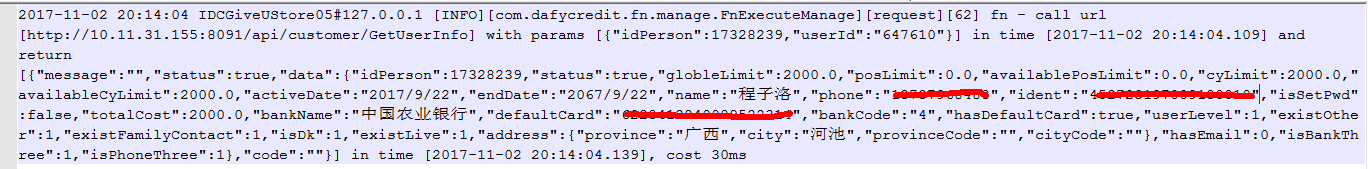
二：日志规则：

每条日志格式规则必须一样，每条日志最好含有日志打印时间、机器名、接口名、入参、出参、入参时间、出参时间、接口处理的总时间（这里指以后新增的日志）…

三：日志规范：访问接口url、入参、入参时间、出参、出参时间、访问接口的耗时。

log.info("fn - call url [{}] with params [{}] in time [{}] and return [{}] in time [{}], cost {}ms", url,json, DatetimeUtil.formatMs(start), res, DatetimeUtil.formatMs(end), end - start);

四：日志图例：



五：日志采集：

如有需要采集，请填写《ELK日志采集规约》，我需要日志服务器的IP，日志所在的目录，多条从日志服务器取出的日志（可将日志文件放入git中，例文件：fn\_log.2017-11-02-0.log ）

六：采集成功：

如果采集成功，我会及时更新《ELK日志采集规约》并口头告知相关开发人员，开发人员只需下拉git查看即可。

七：日志查看：

Kibana日志查看地址：<http://10.11.12.30:5601>

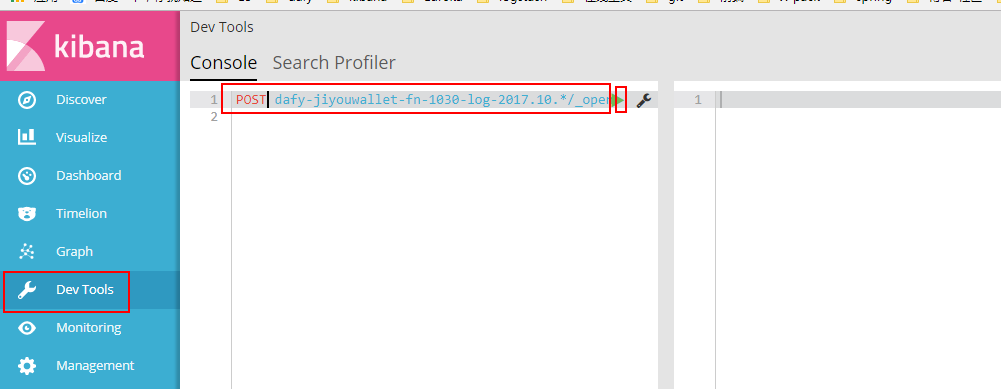
用户名/密码: elastic/changeme

**注意：**

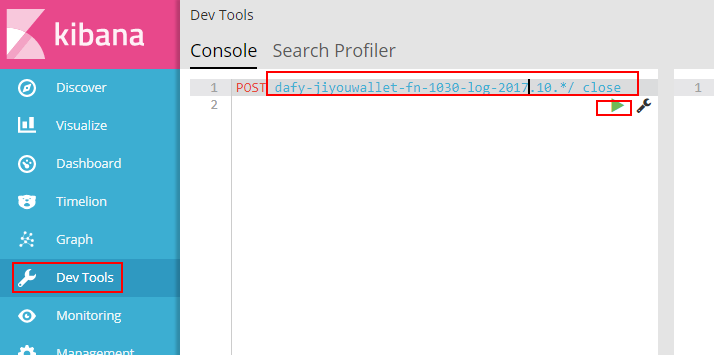
今后日志每个版本只保留30天的日志，30天前的日志并不会删除，只是将查询关闭，如果有查询前30天的数据，请如下进行：

以kibana查询索引dafy-jiyouwallet-fn-1030-log-\*为例， 今天是2017.11.15日，想查询2017.10.15日以前的数据：

1.打开kibana的Dev Tools,执行 POST dafy-jiyouwallet-fn-1030-log-2017.10.\*/\_open，结果为true则执行成功，由于加载需要时间，所以需要过一会才能查询。



2.查询完后请进行关闭。



有问题及时反馈给我….