1. 提供LOG规范（统一格式）：命名、格式、内容、字段顺序

“log.pptx”里面有个session log例子，可以参考

1. 命名包括log名，比如RT\_FLOW\_SESSION\_CLOSE

字段名，比如reason，source-address，source-port

这里第一是保证有意义，第二是要统一，第三是名字尽量短

1. 格式，不是必须定义为字符串的就定义为其他，比如source-address="124.193.37.100" source-port="31006"，source-address可以定义为4个uint32，source-port可以定义为1个uint16
2. 内容，首先是能唯一确定一个事件的，或者事件的关键属性需要包含在log里，其次是客户需求。比如session log:

reason="Some reason" source-address="124.193.37.100" source-port="31006" destination-address="124.193.37.200" destination-port="32768" connection-tag="0" service-name="Medium" nat-source-address="124.193.37.100" nat-source-port="31006" nat-destination-address="124.193.37.200" nat-destination-port="32768" nat-connection-tag="0" src-nat-rule-type="Fake src nat type" src-nat-rule-name="Fake src nat rule" dst-nat-rule-type="Fake dst nat type" dst-nat-rule-name="Fake dst nat rule" protocol-id="17" policy-name="session\_policy4" source-zone-name="source\_zone4" destination-zone-name="Fake dst zone" session-id-32="1" packets-from-client="4294967295" bytes-from-client="1073741824" packets-from-server="4294967294" bytes-from-server="1073741824" elapsed-time="4294967291" application="junos:SSL" nested-application="junos:SSL" username="user4" roles="Fake UAC roles" packet-incoming-interface="source\_interface4" encrypted="Fake encrypt" application-category="Infrastructure" application-sub-category="Encryption" application-risk="4" application-characteristics="application-character4" secure-web-proxy-session-type="client-proxy" peer-session-id="3735928575" peer-source-address="124.193.37.100" peer-source-port="31006" peer-destination-address="124.193.37.200" peer-destination-port="32768" hostname="Fake host" src-vrf-grp="Fake src vrf group" dst-vrf-grp="Fake dst vrf group" tunnel-inspection="Fake tunnel inspection" tunnel-inspection-policy-set="root"

红色字体是session log的关键属性，剩下的基本都是客户要求加上的

1. 字段顺序，关键属性放在前面，因为log是有可能被截断的，首先要保证关键部分
2. 提供每种日志类型数据库的表设计

这个是要根据需求而定的，

1. SQLite读取数据库全部数据，是通过一次性SELECT全部数据？ 还是会按照时间分段读取，每次读取一部分数据（例如有时间索引）？

都可以，可以指定时间段(比如2021-06-16T，或者显示条目

1. 共享内存环形缓冲区是一种日志类型使用一个环，还是所有日志类型都共用一个环？

目前用的是一个队列，有过计划是要根据不同log或优先级别使用不同队列的。