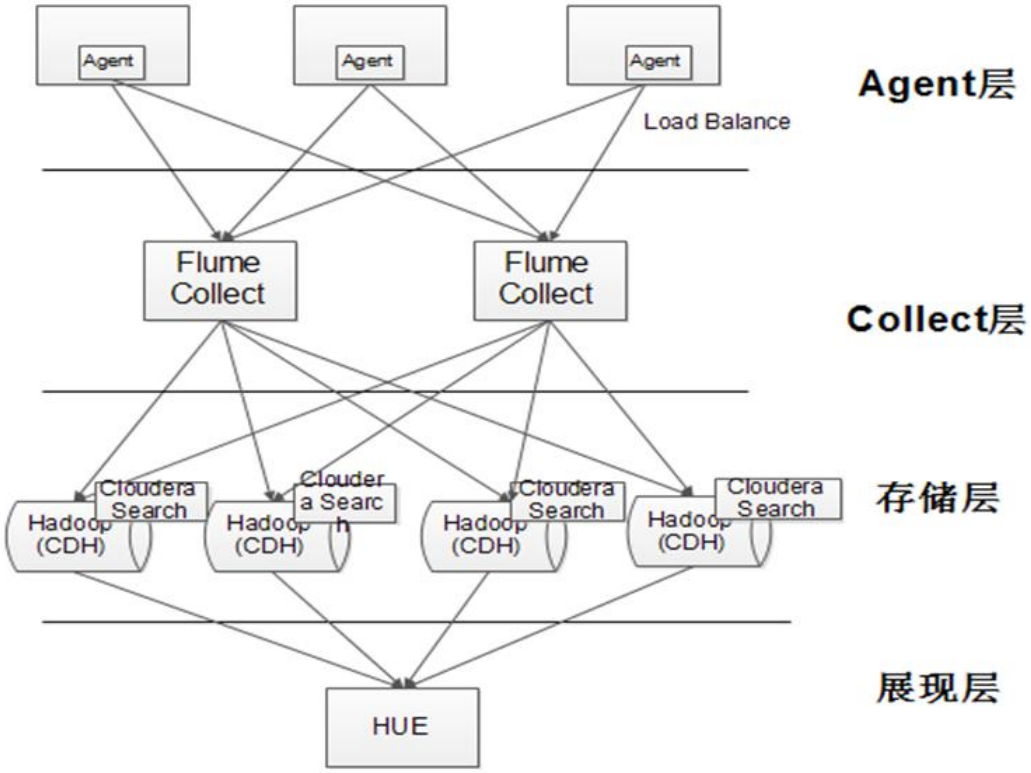
利用 flume 做日志的管理

---2018 年 8 月 29 日_厦门国际银行_ 王淇霖

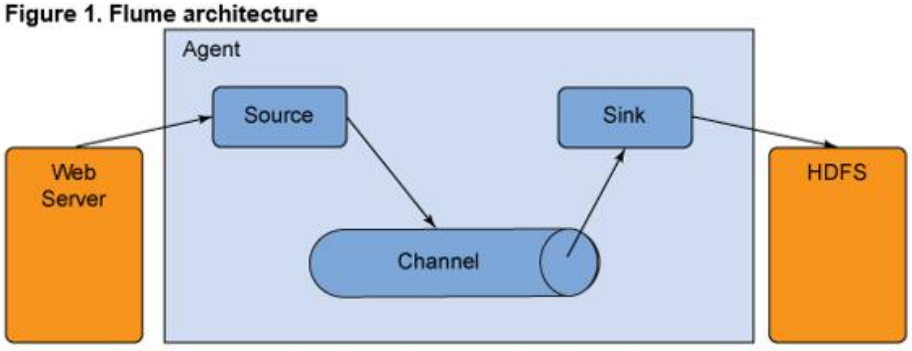
我们对日志的管理，主要是用于满足监管要求的归档要求.所以一开始我们要的是解决存储归档的问题。.最开始选择了商业 arcsight，但是发现数据量大后，查询超时.后来我们选择了 flume 来采集系统的日志，用 hdfs 来存储归档数据.



一开始上线是这样的架构,这个架构我分别描述一下,

agent 使用的是 flume 进行采集，用 tail -F 的方式 flume 的架构如下：

Figure 1. Flume architecture



Source:完成对日志数据的收集。
Channel:主要提供一个队列的功能，对source提供中的数据进行简单的缓存。
Sink:取出Channel中的数据，进行相应的存储文件系统，数据库

ExecSource，SpoolSource

Channel有多种方式：有MemoryChannel,JDBC Channel, FileChannel。
MemoryChannel可以实现高速的吞吐，但是无法保证数据的完整性。
FileChannel保证数据的完整性与一致性。

采集的时候加上一些标签

Flume agent负责采集日志，本项目中选择的采集方式是 tail -F 的方式读取卡系统日志。
Flume收集的日志格式为 headers+body，其中body的内容为flume采集的日志信息。
可以对headers添加interceptors（可以理解为标签），用于后续对日志进行分类，
日志收集项目主要使用以下3类标签：

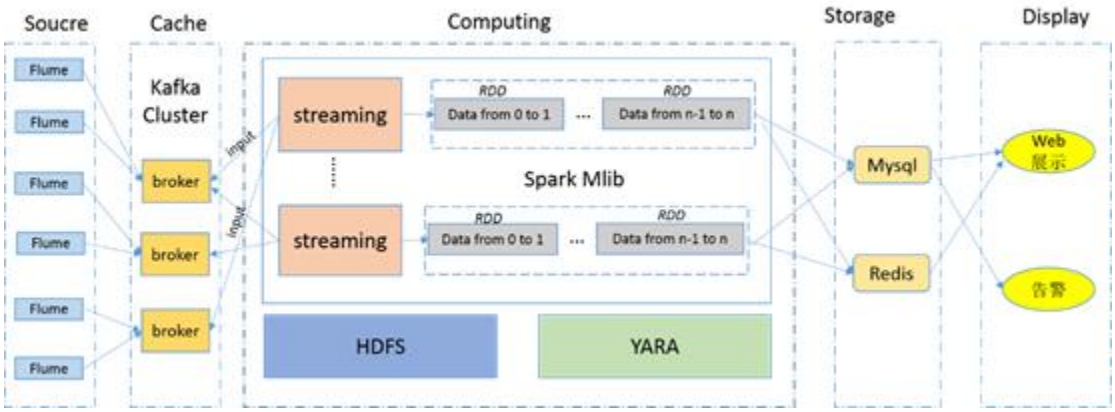
标签类型	用途	示例
host	采集IP地址	10.10.56.75
timestamp	采集时间	unixTimeInMillis
static	采集日志名（自定义）	CommH_56.75

例如日志采集后head添加的内容：

```
Flume event: [Event headers = {timestamp=1430279997080, IC=CommATMP_56.75, hostname=10.10.56.75}, body.length = 79 ]
```

collector 其实也是用了 flume 来中转。存储层：solr 用 morphlines 来分流。区别日志的来源，最后落入 solr 中。前台使用 hue 来做检索。主要的模式 flume+collector(flume)+morphlines+solrcloud+hue。hadoop 那套用的是 cloudera CDH 的解决方案

这是之前最开始的模式。后来我们发现其实开发人员更喜欢原生态的日志。不喜欢用检索。所以我们优化了一下。现在固定采集的模式是：flume +kafka +hdfs ，用 hdfs 的的 nfs gateway 模式挂载目录，使用 samba 做权限管理。开放给开发查看日志。后面运维对日志的一些处理上，需要做一些分析，我们自己开始做日志、指标数据的一下流失分析处理，用的是 spark 的 streaming 来做的。



大致的结果如上。做做系统健康的一些分析。现在在尝试做一写指标的预测，后面又效果可以分享给大家。

分享结束了！

Ask：你们监控的是什么的日志？

An：应用系统日志，日志种类很多，现在最多就是应用日志。操作系统、应用日志、数据库日志。网络日志，安全日志，都有接。

Ask：数据库的话您那边一般采集什么日志。或者说您的日志源，一般是怎么选择的

An：oralce 的 alert 日志，mysql 的 binlog，oracle 上 oswatch 的数据也接过来。日志的选择没什么固定的，一方面满足监控需求，另一方面看是否要做分析。如果要做分析，就取消来，比如 mysql 的慢查询取下来。flume+kafka 的采集还是比较靠谱的，后面落入 hdfs、solr 或者是 es 都是看我们这分析的需求。

Ask：那您那边非结构化数据是否会转为结构化数据

An：也有，我之前那张图就有做，直接写代码按要的信息截断。比如有分析网银系统的日志，他的日志都是|分隔符的。Morphlines，这个你可以去看看，也有用这个去截取过日志。