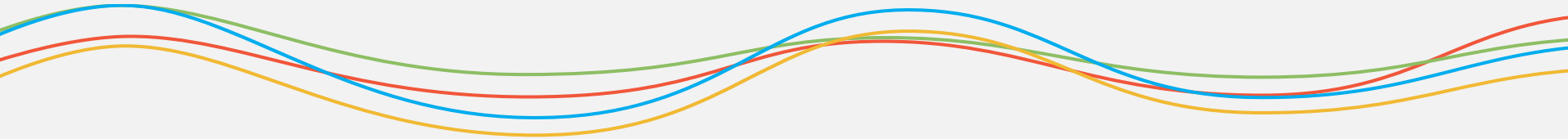
APMCon

访问日志的大数据分析应用

黄慧攀@UPYUN



简单的一条日志

APMCon

124.172.138.41 - - [15/Aug/2016:10:06:54 +0800] "GET http://img10.cn.gcimg.net/v1/pro/508987/T1e6VTByV41RCvBVdK.jpg-normalone HTTP/1.1" 200 44171 "http://product.gongchang.com/c306/CNC1078587746.html" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C; .NET4.0E)" "image/jpeg" normal 138cc1dac7755416b0f8b551a08a8e7e 0.018 "max-age=607177" "U/200, G/200" "HIT" "" "192.168.54.196:8100" "200" "0.018" "44171" 216061 scdn 607177 "T.086.M.2, T.086.M.1, V.cache_img_88, S.mix-gd-can-010, T.2424.H.1, V.mix-gd-can-011, T.54196.H.1, M.ctn-gd-fuo2-196" 0.018 0.000 "-"

格式化

APMCon

{
124.172.138.41
-
-
[15/Aug/2016:10:06:54 +0800]
"GET http://img10.cn.gcimg.net/v1/pro/508987/T1e6VTByV41RCvBVdK.jpg-normalone HTTP/1.1”
200
44171
http://product.gongchang.com/c306/CNC1078587746.html
"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C; .NET4.0E)”
"image/jpeg”
Normal
138cc1dac7755416b0f8b551a08a8e7e
0.018
"max-age=607177" "U/200, G/200" "HIT" "" "192.168.54.196:8100" "200" "0.018" "44171" 216061 scdn 607177 "T.086.M.2, T.086.M.1, V.cache_img_88, S.mix-gd-can-010, T.2424.H.1, V.mix-gd-can-011, T.54196.H.1, M.ctn-gd-fuo2-196" 0.018 0.000 "-”
}

需提炼的数据

APMCon

{

客户端IP	归属地、ISP
请求地址	客户、域名
请求类型	GET、POST、HTTP、HTTPS…
返回状态码	200、404、…
服务器输出字节数	网站平均资源大小，各文件大小的分布比例
Content-Type	资源类型
请求耗时	平均速度、平均下载耗时、平均速度分布、耗时分布
Referer //ToC	引用来源
节点IP	归属地、节点
回源IP	
源站耗时 //CDN	源站平均速度、耗时
中转节点	
中转返回信息	状态码、速度…
源站返回信息	状态码、速度…
…	

}

有多少数据

APMCon

150多个节点，3000多台服务器

每服务器日均产生 5GB 压缩日志、1亿多条日志

合共2000多亿条日志

如何处理？

APMCon

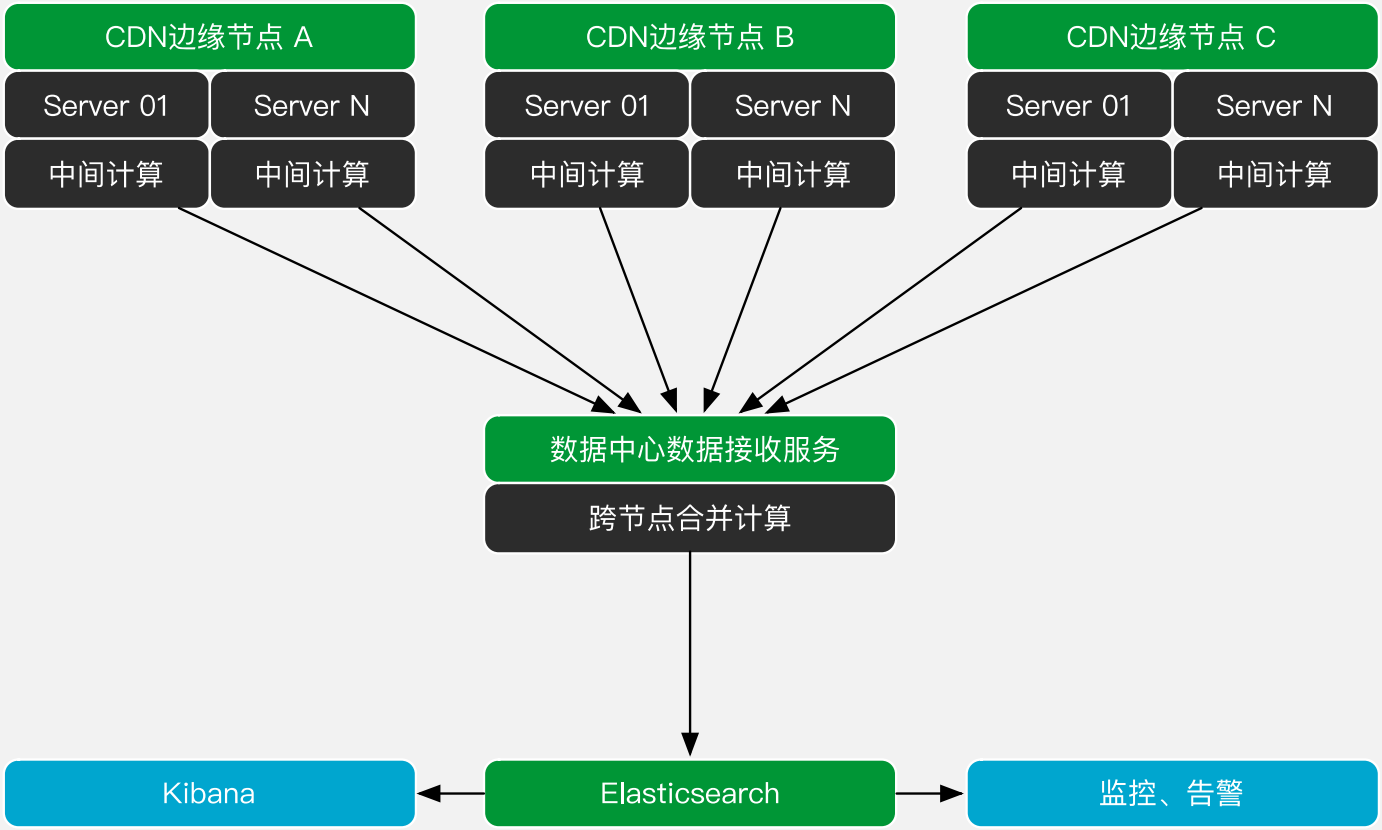
- 50台高性能大存储容量的服务器组成集群，以处理原始日志格式
  （仅能存储2天历史数据）
- 4台高性能服务器组成日志下载处理集群，以提供简化的标准日志供客户下载
  （最大延迟1小时，可下载上1小时的日志；最大延迟8小时可查看昨日的统计分析）
- 1台普通服务器，接收所有节点的二次处理后数据，输出节点质量报告
  （可存储1个月历史数据）
- 1台普通服务器，接收所有节点的二次处理后数据，输入到 ES，输出多纬度分析数据

ELK, But Not only ELK

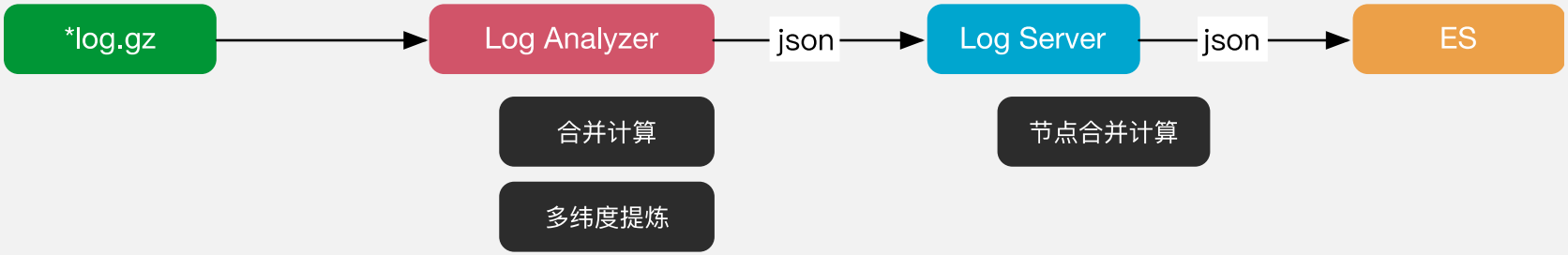
它只是个存储的容器和展现数据的方案，并不是全部

又拍云ELK方案

APMCon



又拍云ELK方案


*log.gz
Log Analyzer
json
Log Server
json
ES
合并计算
多纬度提炼
节点合并计算

解决ELK的性能问题

APMCon

纯裸日志数据存入集群的性能低、服务器资源占用高

我们需要对日志进行预先合并计算后再存入ELK

记录数量压缩1000倍！！！

提炼数据价值

原始日志只是一些基础信息，需要做二次提炼这些信息价值

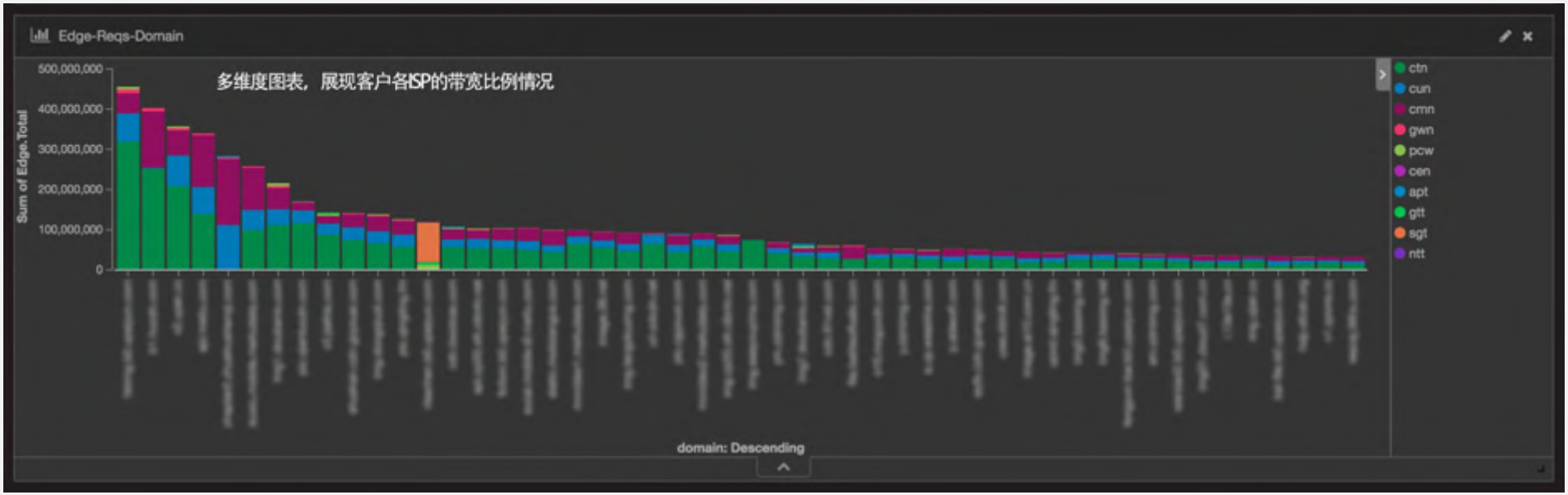
IP归属地、CDN服务节点信息、服务状态、缓存命中率、路由状态、客户对应关系 ...

一条简单的日志经过价值提炼后...

全网汇总信息

可以随时查看到全网汇总数据，如带宽总量

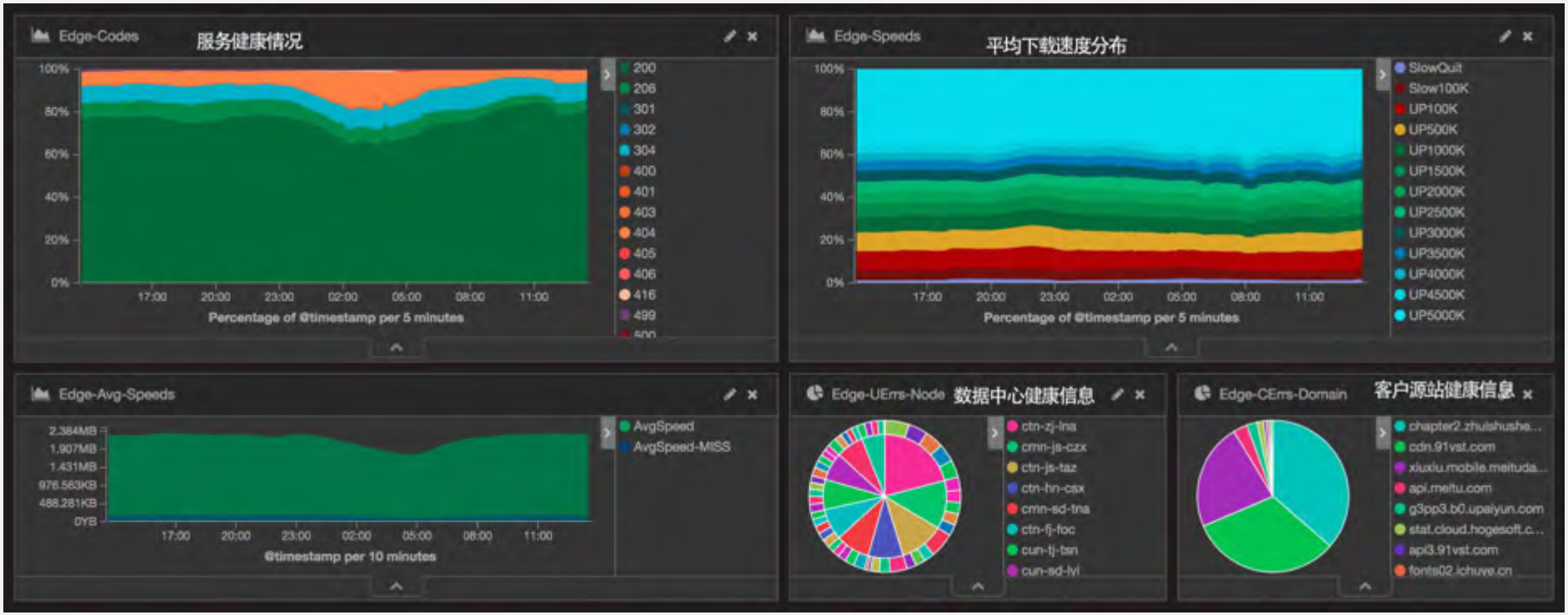
客户使用情况



实时查看平台上的大客户分布情况，和客户的网络覆盖信息。

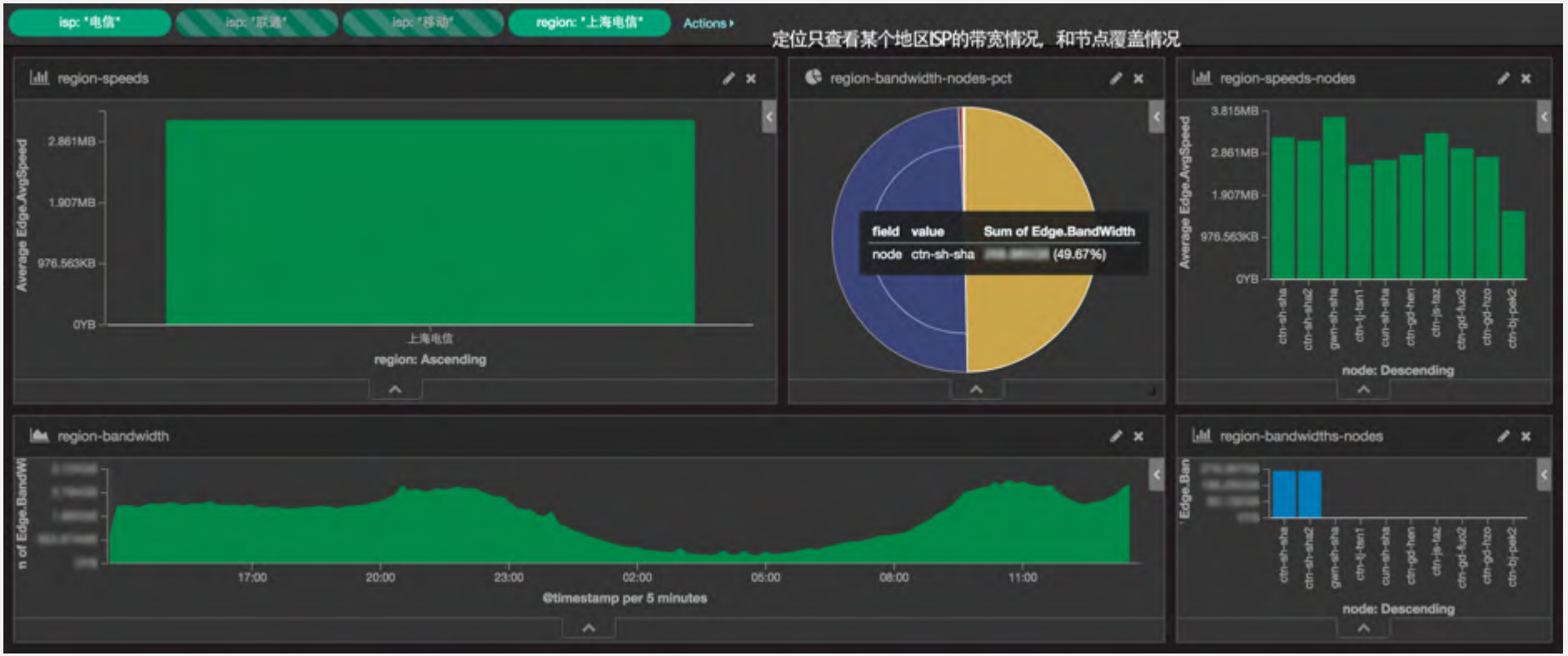
服务健康监控

APMCon



可从平台上及时发现到客户的健康信息是否有异常，以便可快速处理。
并可通过访问域名过滤，查看到某个客户的服务质量，初步定位问题

业务数据分析



还可以根据客户端的地域和网络查看CDN的服务情况，如使用哪些节点覆盖，每个节点覆盖的比例如何这个地区的使用带宽和平均下载速度。以供我们做平台性能优化之用

难点

APMCon

- 虽然有边缘3000多台服务器独立自主做初步的日志处理，但就是因为是在业务服务器上做的处理，必须把资源占用降到最低，否则会影响正常业务。所以我们采用了C/gzlib来做流式计算
- 而在接收服务器端的合并处理，使用共享内存来做数据统计，避免使用 Redis ，这个性能无法达到性能要求
- 程序化自动删除历史数据，这个很重要！！！否则磁盘会爆

谢谢 ;)