**########**需求解析

table

a(time) b(user) c(app) d(traffic)

1

2

1.按流量排序

SELECT a as time, b as user, c as app, d as traffic FROM $log ORDER BY traffic;

2.按用户流量排名，选择前5应用

SELECT a AS time, b AS user, c AS app, SUM(d) AS trfsum

FROM $log

WHERE app IN

(SELECT b AS user, c AS app, SUM(d) AS trfsum

FROM $log

WHERE user IN

(SELECT b AS user, SUM(d) AS trfsum

FROM $log

GROUP BY user

ORDER BY trfsum

LIMIT 0,5

)

GROUP BY app

ORDER BY trfsum

)

AND user IN

(SELECT b AS user, SUM(d) AS trfsum

FROM $log

GROUP BY user

ORDER BY trfsum

LIMIT 0,5

)

GROUP BY user

ORDER BY trfsum

1.求某个用户总流量

2.按照用户总流量排名

**########**

最终APP排序效果图

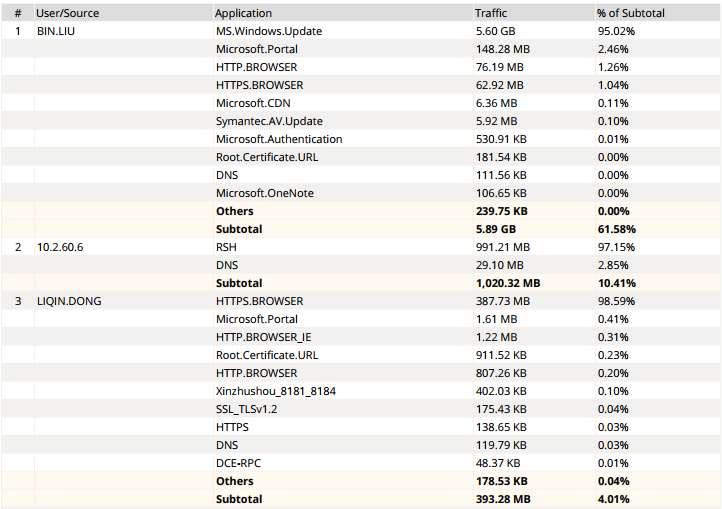
图1.根据流量选择Top30用户，再根据每用户选择对应应用Top10及流量统计。

图2.根据Filter，选择某个对应用户的详细会话，按每会话流量排序

**########**ASB\_Suzhou\_Dataset---图1

select coalesce(nullifna(`user`),ipstr(`srcip`)) as user\_src,app,sum(rcvdbyte + sentbyte) as traffic from $log where $filter and app is not null group by user\_src,app having sum(sentbyte+rcvdbyte)>0 order by traffic desc

图表调用dig挖掘

**########**

**########**ASB\_Suzhou\_Single\_User\_Details---图2

select from\_dtime(dtime) as Begin,duration as "duration(s)",User\_src,IP\_src,Destination,app,Traffic from **###**(select dtime,duration,coalesce(nullifna(`user`),ipstr(`srcip`)) as User\_src,ipstr(`srcip`) as IP\_src,coalesce(hostname,ipstr(`dstip`)) as Destination,app,sum(sentbyte+rcvdbyte) as Traffic from $log where $filter and logid\_to\_int(logid) not in (4,7,14) and action in ('accept','close','timeout') group by dtime,duration,User\_src,srcip,Destination,app order by sum(sentbyte+rcvdbyte) desc)**###** t group by Begin,duration,User\_src,IP\_src,Destination,app,Traffic order by Traffic desc

图表调用简单，不做排序，流量显示为KB/MB/GB，其他不用变更

**########**20171227新需求，整体报告按照URL排序，用户详细报告中dst显示website名称，而不是IP地址

web-Top-User-Visted-Websites-by-Bandwidth

select website, catdesc, sum(bandwidth) as bandwidth from ###(select hostname as website, catdesc, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-traffic where $filter and hostname is not null and logid\_to\_int(logid) not in (4, 7, 14) and (countweb>0 or ((logver is null or logver<52) and (hostname is not null or utmevent in ('webfilter', 'banned-word', 'web-content', 'command-block', 'script-filter')))) group by hostname, catdesc having sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0))>0 order by bandwidth desc)### t group by website, catdesc order by bandwidth desc

1 参考上面的数据集，写调用url的数据

select hostname from $log-traffic where (hostname is not null or utmevent in ('webfilter', 'banned-word', 'web-content', 'command-block', 'script-filter')) group by hostname, catdesc having sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0))>0 order by bandwidth desc)### t group by website, catdesc order by bandwidth desc

2 最后发现问题，对比第一条FAZ自带数据集，其日志表是 $log-traffic，我之前用的是 $log，导致无法看到hostname信息，调用$log-traffic之后，就能看到数据了。

select coalesce(nullifna(`user`),ipstr(`srcip`)) as user\_src,hostname,sum(rcvdbyte + sentbyte) as traffic from $log-traffic where $filter and app is not null group by user\_src,hostname having sum(sentbyte+rcvdbyte)>0 and (hostname is not null or utmevent in ('webfilter', 'banned-word', 'web-content', 'command-block', 'script-filter')) order by traffic desc

3 select user\_src,website,traffic from ###(select coalesce(nullifna(`user`),ipstr(`srcip`)) as user\_src,hostname as website,sum(rcvdbyte + sentbyte) as traffic from $log-traffic where $filter and ipstr(`srcip`)!='10.2.62.11' and hostname is not null and logid\_to\_int(logid) not in (4, 7, 14) and (countweb>0 or ((logver is null or logver<52) and (hostname is not null or utmevent in ('webfilter', 'banned-word', 'web-content', 'command-block', 'script-filter')))) group by user\_src, website having sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0))>0 order by traffic desc)### t

group by user\_src,website,traffic order by traffic desc

4 调用上一条生成的数据，生成报告后数据量很少，猜测由于钻取数据会调用元数据库，如果在写数据集的时候，采用了临时表的形式，最终的数据就不能直接获取了。

select coalesce(nullifna(`user`),ipstr(`srcip`)) as user\_src,hostname as website,sum(rcvdbyte + sentbyte) as traffic from $log-traffic where $filter and ipstr(`srcip`)!='10.2.62.11' and hostname is not null and logid\_to\_int(logid) not in (4, 7, 14) and (countweb>0 or ((logver is null or logver<52) and (hostname is not null or utmevent in ('webfilter', 'banned-word', 'web-content', 'command-block', 'script-filter')))) group by user\_src, website having sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0))>0 order by traffic desc

这条数据集，产生的数据比上一条多，但是还是很少。统计出来的是按照每条会话的流量计。总和加起来只有600KB左右。

5

select `user`,rcvdbyte,sentbyte,app,hostname from $log-traffic where (app='HTTPS.BROWSER' or app='HTTP.BROWSER' or app='HTTP' or app='HTTPS') and `user`='QIAN.XU' order by rcvdbyte desc

6.日志类型选择“网页过滤”

select coalesce(nullifna(`user`),ipstr(`srcip`)) as user\_src,hostname,sum(rcvdbyte + sentbyte) as traffic from $log where $filter and hostname is not null group by user\_src, hostname having sum(sentbyte+rcvdbyte)>0 order by traffic d

7 从网站上面看到的，统计出URL的访问次数和流量

select sum(minutes) as CountTimeStamps, user\_src, catdesc, hostname as website, status, sum(bandwidth) as bandwidth from ###(select count(dtime) as minutes, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as user\_src, catdesc, hostname, cast(utmaction as text) as status, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-traffic where $filter and hostname is not null and logid\_to\_int(logid) not in (4, 7, 14) and (countweb>0 or ((logver is null or logver<52) and (hostname is not null or utmevent in ('webfilter', 'banned-word','web-content', 'command-block', 'script-filter')))) group by user\_src, catdesc, hostname, utmaction)### t group by user\_src, catdesc, website, status having sum(minutes) > 1 order by catdesc, CountTimeStamps DESC

8最后参照PostgreSQL的JOIN写法，拉取两个日志类型的字段进行对比，找出可以作为同一会话的参数，进行INNER JOIN选取数据

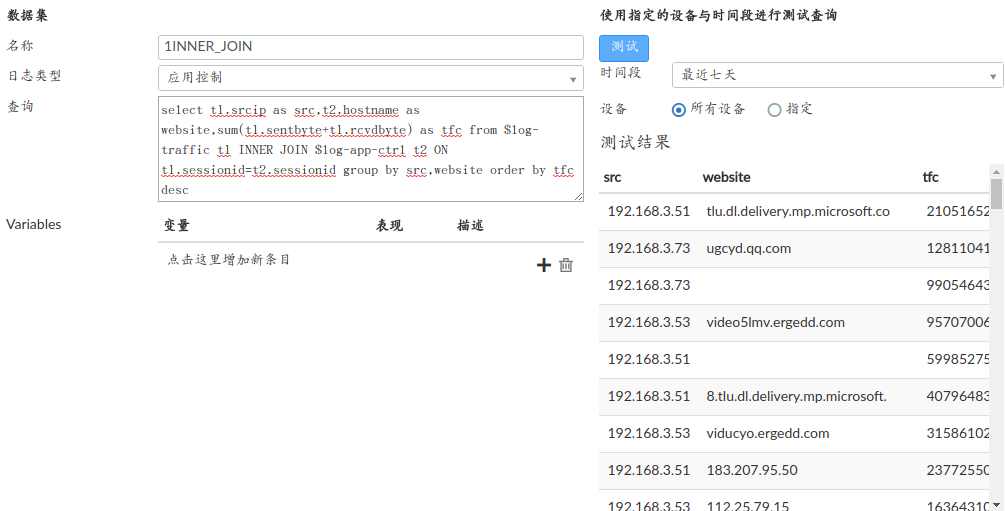
a.select \* from $log-traffic

b.select \* from $log-app-ctrl

**找出可以作为同一个会话身份的字段，不是之前猜测的logid，而是sessionid**

**最终数据集，以及效果如下**

select t1.srcip as src,t2.hostname as website,sum(t1.sentbyte+t1.rcvdbyte) as tfc from $log-traffic t1 INNER JOIN $log-app-ctrl t2 ON t1.sessionid=t2.sessionid group by src,website order by tfc

**问题：调用该数据集生成宏/图表及报告的时候，会报错“生成报告失败”**

**#########**

**########**以下是一开始的时候，手动写的按照用户排名的select语句，仅做参考

select

from\_itime(itime) as timestamp,

coalesce(nullifna(`user`),nullifna(`unauthuser`),ipstr(`srcip`)) as user\_src,

sum(coalesce(`rcvdbyte`,0)+coalesce(`sentbyte`,0)) as bandwidth,

(select app from $log where coalesce(nullifna(`user`),nullifna(`unauthuser`),ipstr(`srcip`))=user\_src group by app order by sum(coalesce(`rcvdbyte`,0)+coalesce(`sentbyte`,0)) desc limit 1 offset 0) as app01,

(select sum(coalesce(`rcvdbyte`,0)+coalesce(`sentbyte`,0)) from $log where coalesce(nullifna(`user`),nullifna(`unauthuser`),ipst(`srcip`))=user\_src group by app order by sum(coalesce(`rcvdbyte`,0)+coalesce(`sentbyte`,0)) desc limit 1 offset 0) as bandwidth01,

(select sum(coalesce(`rcvdbyte`,0)) from $log where coalesce(nullifna(`user`),nullifna(`unauthuser`),ipstr(`srcip`))=user\_src group by app order by sum(coalesce(`rcvdbyte`,0)+coalesce(`sentbyte`,0)) desc limit 1 offset 0) as inbound01,

(select sum(coalesce(`sentbyte`,0)) from $log where coalesce(nullifna(`user`),nullifna(`unauthuser`),ipstr(`srcip`))=user\_src group by app order by sum(coalesce(`rcvdbyte`,0)+coalesce(`sentbyte`,0)) desc limit 1 offset 0) as outbound01

(......此处省略app02,bandwidth02,inbound02,outbound02----05,总共五个排名)

from $log

group by user\_src order by bandwidth desc

**########**系统自带数据集汇总

1.选择排名中的前几 limit offset:

select \* from $log limit 5 offset 0;

select \* from $log limit 0,5;

2.排序，DESC逆向由大到小或者从后往前，ASC顺序有小到大或者从前往后:

select \* from $log order by xx DESC;

3.

!Traffic-Top10-App\_Of\_First\_User

select app, sum(rcvdbyte + sentbyte) as bandwidth

from $log

where (`user`=(

select coalesce(nullifna(`user`), ipstr(`srcip`)) as user\_src

from $log where $filter

group by user\_src having sum(sentbyte+rcvdbyte)>0

order by sum(rcvdbyte + sentbyte) desc limit 1 offset 1))

and $filter and app is not null

group by app having sum(sentbyte+rcvdbyte)>0

order by bandwidth desc

**####**

!将应用选中为app1,2,3,4,5的方式，数值存放在列，而不是放在行

select

from\_itime(itime) as timestamp,coalesce(nullifna(`user`),nullifna(`unauthuser`),ipstr(`srcip`)) as user\_src,sum(coalesce(`rcvdbyte`,0)+coalesce(`sentbyte`,0)) as bandwidth,

(select app from $log where coalesce(nullifna(`user`),nullifna(`unauthuser`),ipstr(`srcip`))=user\_src group by app order by sum(coalesce(`rcvdbyte`,0)+coalesce(`sentbyte`,0)) desc limit 1 offset 0) as app01,

(select sum(coalesce(`rcvdbyte`,0)+coalesce(`sentbyte`,0)) from $log where coalesce(nullifna(`user`),nullifna(`unauthuser`),ipst(`srcip`))=user\_src group by app order by sum(coalesce(`rcvdbyte`,0)+coalesce(`sentbyte`,0)) desc limit 1 offset 0) as bandwidth01,

(select sum(coalesce(`rcvdbyte`,0)) from $log where coalesce(nullifna(`user`),nullifna(`unauthuser`),ipstr(`srcip`))=user\_src group by app order by sum(coalesce(`rcvdbyte`,0)+coalesce(`sentbyte`,0)) desc limit 1 offset 0) as inbound01,

(select sum(coalesce(`sentbyte`,0)) from $log where coalesce(nullifna(`user`),nullifna(`unauthuser`),ipstr(`srcip`))=user\_src group by app order by sum(coalesce(`rcvdbyte`,0)+coalesce(`sentbyte`,0)) desc limit 1 offset 0) as outbound01

from $log group by user\_src order by bandwidth desc limit 5 offset 0

**####**

select

from\_itime(itime) as timestamp,coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as user\_src,(select app from $log where user=user\_src group by user order by sum(rcvdbyte+sentbyte) limit 1 offset 0) AS app1,coalesce(root\_domain(hostname), ipstr(dstip)) as destination,sum(coalesce(`sentbyte`, 0)+coalesce(`rcvdbyte`, 0)) as bandwidth,cast(policyid as text) as polid

from $log

where $filter

and logid\_to\_int(logid) not in (4, 7, 14)

and action in ('accept', 'close', 'timeout')

group by timestamp, user\_src, app, destination, polid

order by bandwidth desc LIMIT 5 OFFSET 0

**####**

!ASB\_app\_by\_bandwidth\_with\_user\_dsip\_and\_timestamp

select from\_itime(itime) as timestamp, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as user\_src, app, coalesce(root\_domain(hostname), ipstr(dstip)) as destination, sum(coalesce(`sentbyte`, 0)+coalesce(`rcvdbyte`, 0)) as bandwidth,cast(policyid as text) as polid from $log where $filter and logid\_to\_int(logid) not in (4, 7, 14) and action in ('accept', 'close', 'timeout') group by timestamp, user\_src, appcat, app, destination, polid having bandwidth>0 order by bandwidth desc

**####**

!Top-Users-By-Bandwidth

select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as user\_src,

srcip, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth,

sum(coalesce(rcvdbyte, 0)) as traffic\_in,

sum(coalesce(sentbyte, 0)) as traffic\_out

from $log

where $filter

and logid\_to\_int(logid) not in (4, 7, 14)

and srcip is not null

group by user\_src, srcip having sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0))>0

order by bandwidth desc

**####**

!Traffic-top-10-application-of-NO.1-user

select app, sum(rcvd + sent) as bandwidth

from $log

where (`user`=(select coalesce(nullifna(`user`), `src`) as user\_src

from $log

where $filter group by user\_src having sum(sent+rcvd)>0

order by sum(rcvd + sent) desc limit 1 offset 0

)

)

and $filter

and app is not null

group by app having sum(sent+rcvd)>0

order by bandwidth desc