Case 1:

index="\_internal" source="\*metrics.log" group="per\_host\_thruput" | where series == "nbnvmw1app1"

假定搜索近期5分钟数据，符合条件有20个事件。

index="\_internal" source="\*metrics.log" group="per\_host\_thruput" | where series == "nbnvmw1app1"

| stats sum(kb) as TotalKb

则返回这20个事件中kb的总和。统计后只有一个结果。

index="\_internal" source="\*metrics.log" group="per\_host\_thruput" | where series == "nbnvmw1app1"

| stats sum(kb) as TotalKb by \_time

在计算总和的时候以时间分组，由于每个事件的时间是不一样的，每个事件的时间都成为一个组。所以统计结果为20个数据，并且每个数据并没有计算总和，因为在每个事件（每个组中）只有一个数据。

index="\_internal" source="\*metrics.log" group="per\_host\_thruput" | where series == "nbnvmw1app1" | bin

span=1m | stats sum(kb) as TotalKb by \_time

在计算总和的时候以时间分组，并且我们规定以1分钟分割时间。所以过去5分钟将称为5组，统计结果为5个数据，每个数据为1分钟内kb的总和。

Case2:

addcoltotals指令用于在搜索出来的结果后新增一行。该新增一行的域的值为其他事件行所对应域的总和。



P.s对比之下addtotals为每一个事件增加多一个域，值为该行事件中所有域的总和。