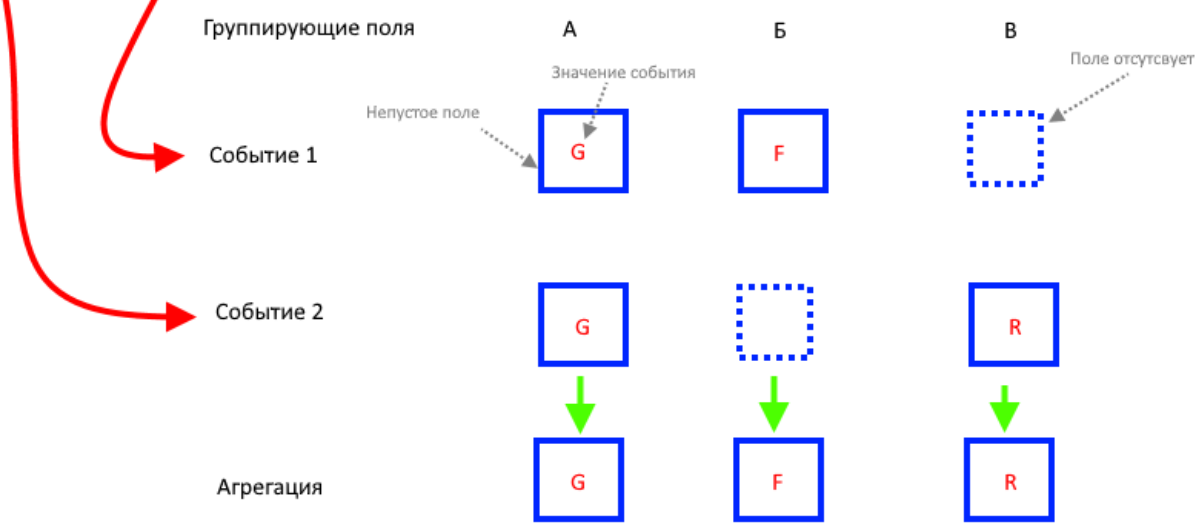
Принцип работы правила агрегации (схематично)

Отразим схематично принцип работы агрегации на примере событий аудита от ОС Linux:

```
time->Thu Aug 12 20:35:45 2021
type=PROCTITLE msg=audit(1628789745.294:566): proctitle=2F7573722F7362696E2F6:
type=PATH msg=audit(1628789745.294:566): item=0 name="/usr/share/zoneinfo/Afr:
type=CWD msg=audit(1628789745.294:566): cwd="/var/www/html"
type=SYSCALL msg=audit(1628789745.294:566): arch=c000003e syscall=257 success:
```



Надо раскидать нужные поля в парсинге, как в PATH, так и в SYSCALL (эти типы событий наиболее полезно объединить), чтобы по принципу тетриса получить одно полное агрегационное событие

> При склейке множества событий в одно, порядок событий не сохраняется, т.к о бработка многопоточная (на выход события могут прийти не в той последовательности, как на вход). Для того чтобы обработка происходила в 1 поток необходимо в настройках коллектора на 1 шаге указать количество рабочих процессов (workers) = 1. см пример со склейктой тут

Revision #5
Created 5 February 2024 08:42:58 by Boris Rzr

Updated 12 July 2024 12:59:20 by Boris Rzr