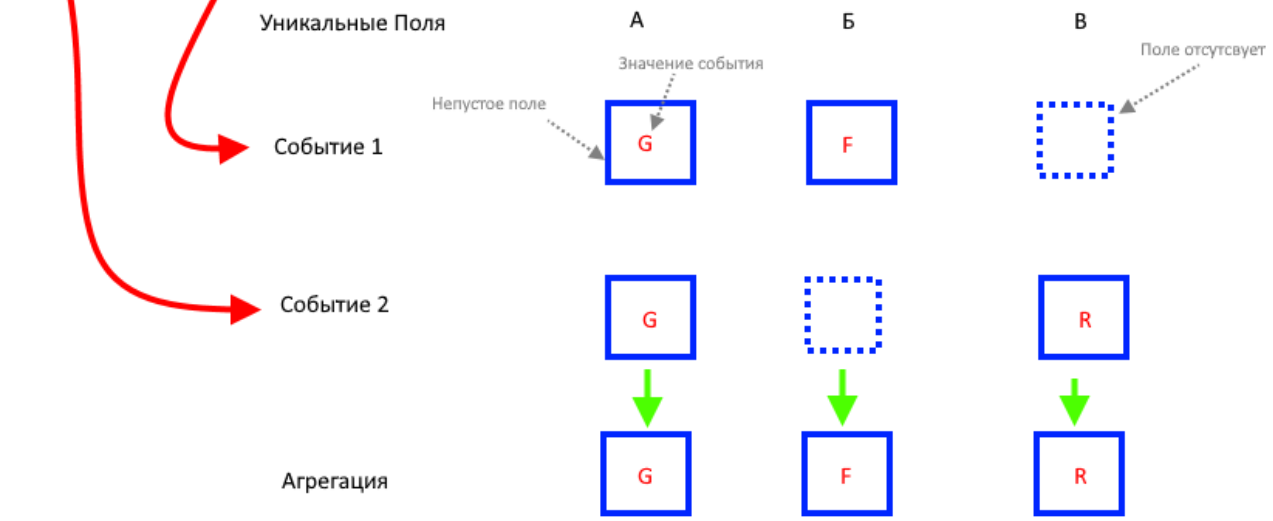
Принцип работы правила агрегации (схематично)

??????? ?????????? ??????? ?????? ????????? ?? ??????? ??????? ?????? ?? ?? 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

??? ??????? ????????? ??????? ? ????, ??????? ??????? ?? ???????????, ?.? ????????? ????????????? (?? ????? ??????? ????? ?????? ?? ? ??? ??????????????????, ??? ?? ????). ??? ???? ????? ????????? ??????????? ? 1 ????? ?????????? ? ?????????? ?????????? ?? 1 ???? ??????? ?????????? ??????? ????????? (workers) = 1. ?? ?????? ?? ????????? ???

Revision #6
Created 2024-02-05 08:42:58 UTC by Boris Rzr
Updated 2024-10-21 08:41:47 UTC by Boris Rzr