Обработка многострочных событий на примере AuditD в KUMA

?????????? ?????? ????????? multiline auditd - ????? ????????????? "auditd", ??????? ???????? ? KUMA 3.2: https://support.kaspersky.com/help/KUMA/3.2/ru-RU/220739.htm ????????? ???? ?????? ???????? wa ? ???????? ????????? ????????????? ??????? ?? ??????? AuditD ? ????? ???? ????????? ?? ?????? ????????? ? ??????? ?????????? ???????.

Введение

? ?????? ?????? ????? ?????????? ??????? (**workaround**) ????????? ????????????? ??????? ?? ??????? ??????? AuditD.

1) ?????? ????? ???????, ???????? ??? ????????? ????? ????????? ??? 2 ??????? (?? 2 ?????). ??? ??? ? ????? ??????, ????? ? ????????????? ??????? 2 ? ????? ??????? ?????????? ????? EPS ?? ??????????.

2) ????? ?? ????????????? ?????????? ???????? ??????? (**Raw**), ??? ????????????? ???????? ????? ??????? ????? ????? ??????? ????????????? ????????, ??????? ????? ?? ??? ????????

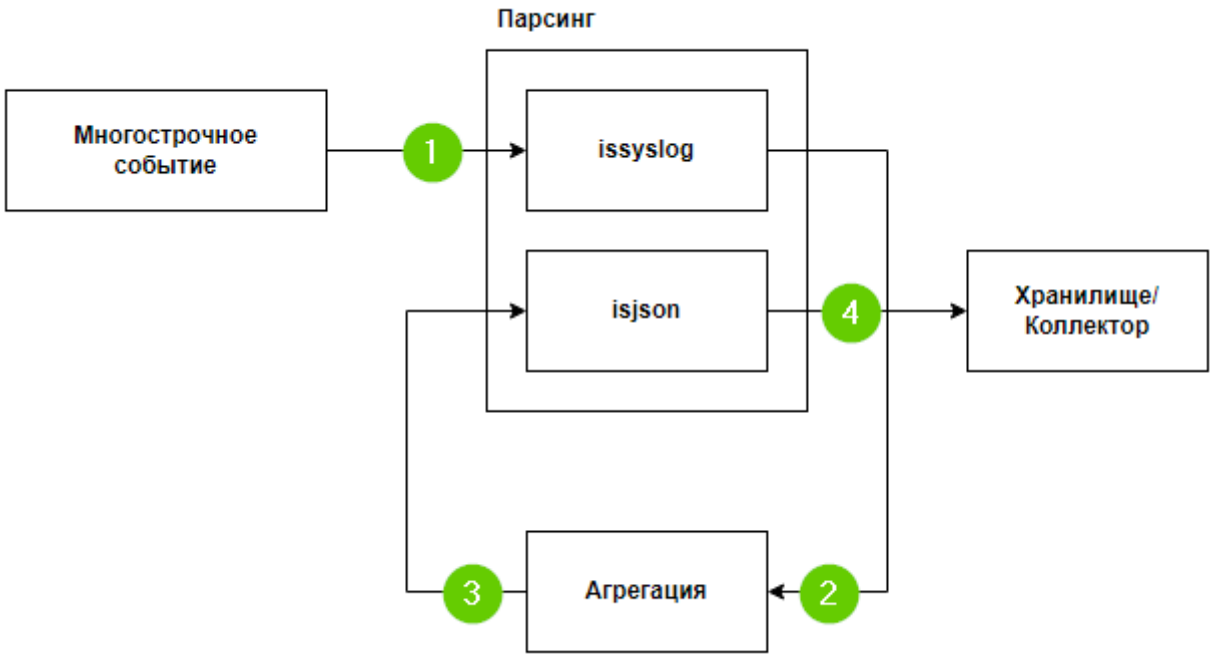
3) ????? ???????, ????????????? ??????? ??????????? ? ???? ???? (? ??????? ????? ??? **Extra** и **Message**). ????????????? ??????????? ????????????? ?????????? ??????????????.

?????????? ?????? ? ?????? ?????? ?? ????????, ?? ??? ????? ??????????? ?? ??????.

??? ??? ???????? ?????? ?????????, ?????? ????????????? ????????? ?????? ?????? ??? ???? .

Принцип работы

???? ???????????? ????? ?????? ??????? ????????????? ???????.



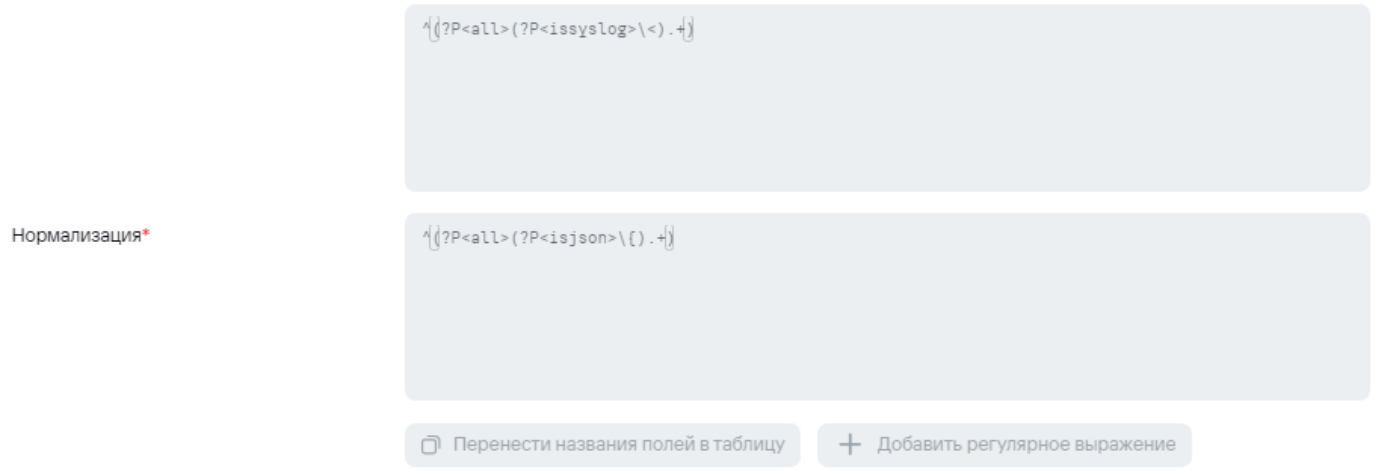
???????? ???? ??????????? ? ???, ????? ?? ?????????? ????????????? ??? ??????? ?????? ????????????? ??????? ? ????. ??? ???????? ?????????? ??? ????????? ???????? ? ???? ???? ? ????? ????????? ????? ????????????? ??????? ??????? ?? ???? ?????????? ??? ???????????.

Алгоритм работы на примере Auditd

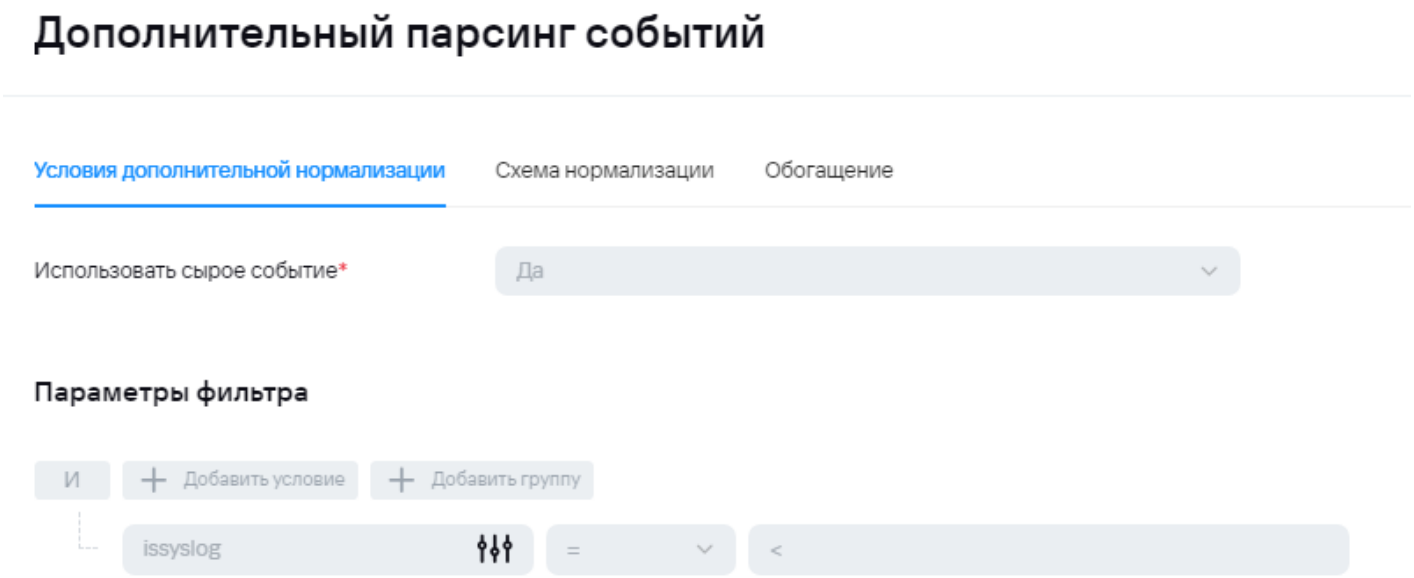
1) ?? ?????? ???? ? ????????? ????????? ???????, ??? ?????????? ????????, ??? ?? ????????? syslog ??? json, ? ???????? ??????????????????, ??????????????, ??????????? ???????? ??????? ?????????.

? ????? ????, ???????? ????? ???? ?????. ???????? ???? - ????????? ?? ??????? ???????????? ???????? ??????? ?? ????????? ?? ????????????? ???????.

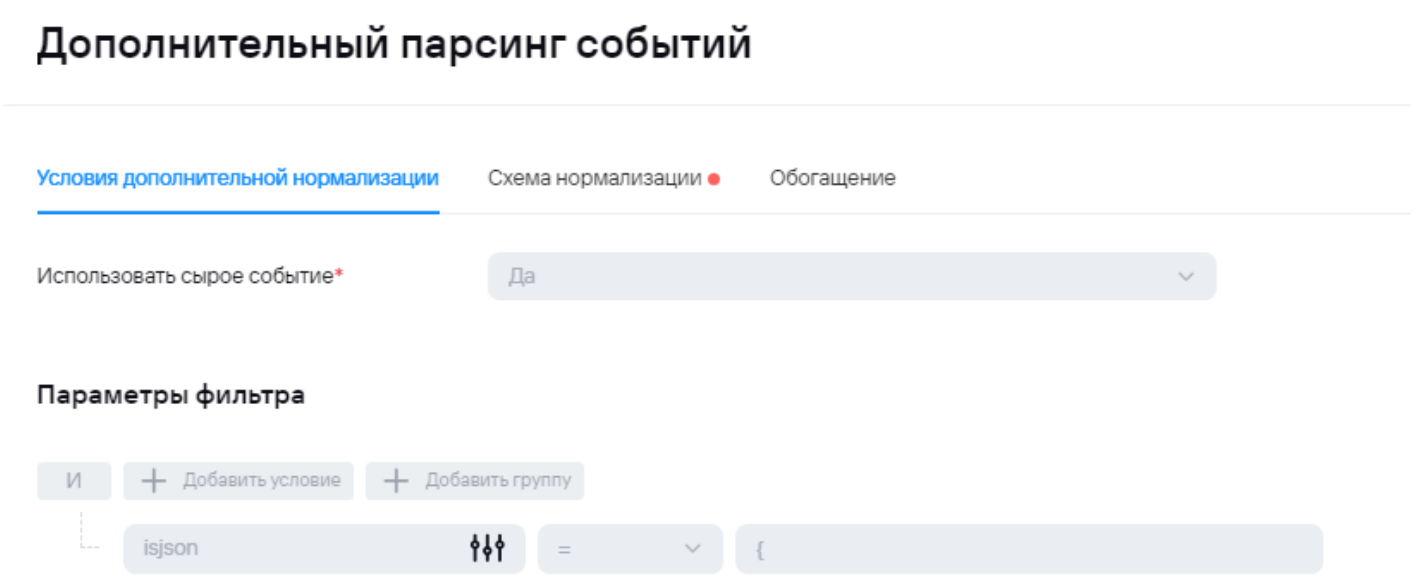
?????? ????????????.


^(?P<all>(?P<issyslog>\<).+)
Нормализация*
^(?P<all>(?P<isjson>\{).+)
Перенести названия полей в таблицу
Добавить регулярное выражение

?????? ??????? ??? ???????? ??????? ? ??????????????????, ???? ??????? ????????.

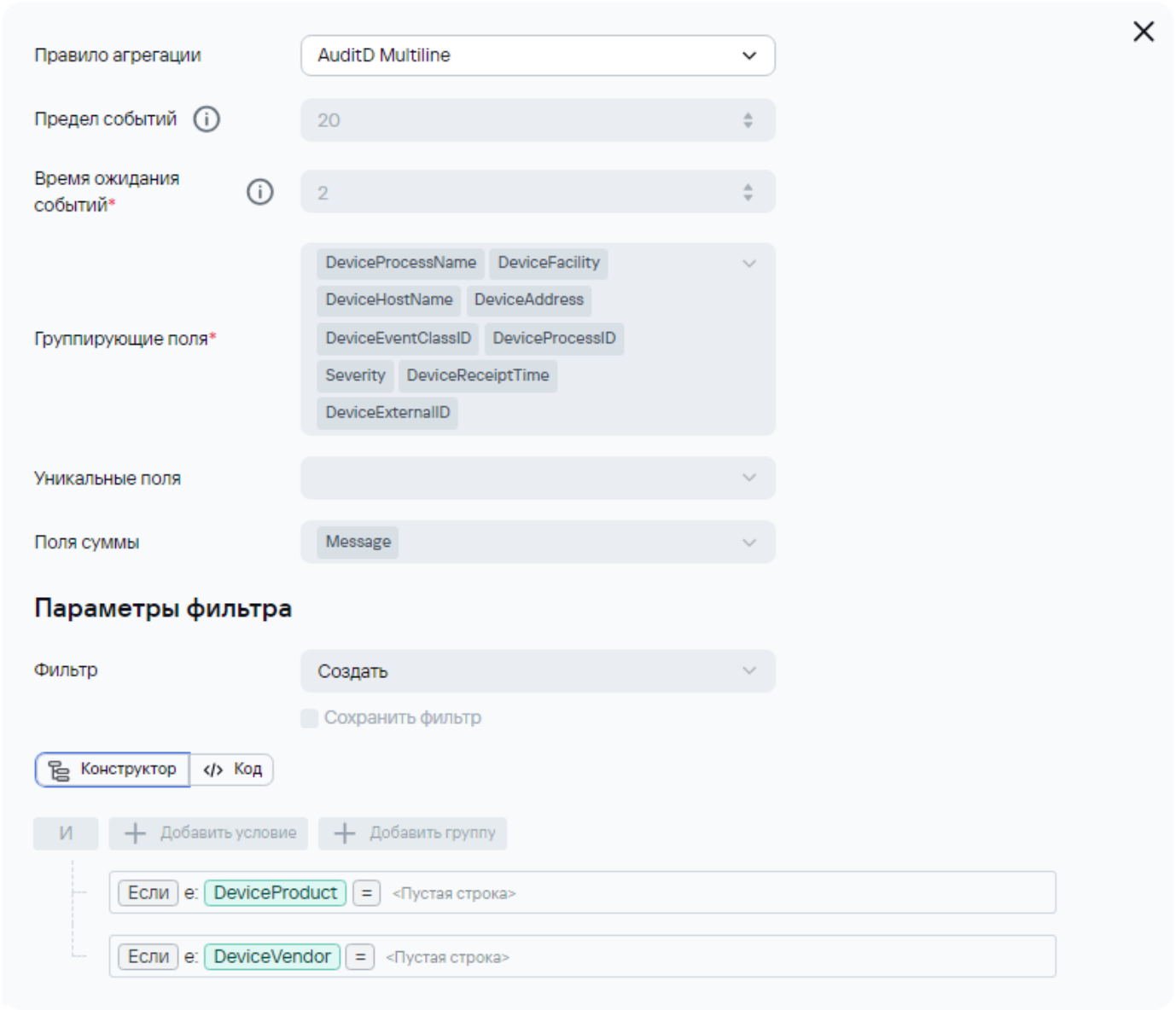

Дополнительный парсинг событий
Условия дополнительной нормализации
Схема нормализации
Обогащение
Использовать сырое событие*
Да
Параметры фильтра
И
Добавить условие
Добавить группу
issyslog
=
<

?????? ??????? ??? ???????? ??????? ? ??????????????????, ???? ??????? ?????????????.



2) ? ?????? ???????? syslog'? ?? ????? ???????????? ?? ????? ?????????? ?????????? ?????? **DeviceProduct** ? **DeviceVendor,** ??????? ?? ????? ????? ???????? ? ??????? ??? ?????????. ???? ???????? ?????? ??? ????????? ??????? AuditD:

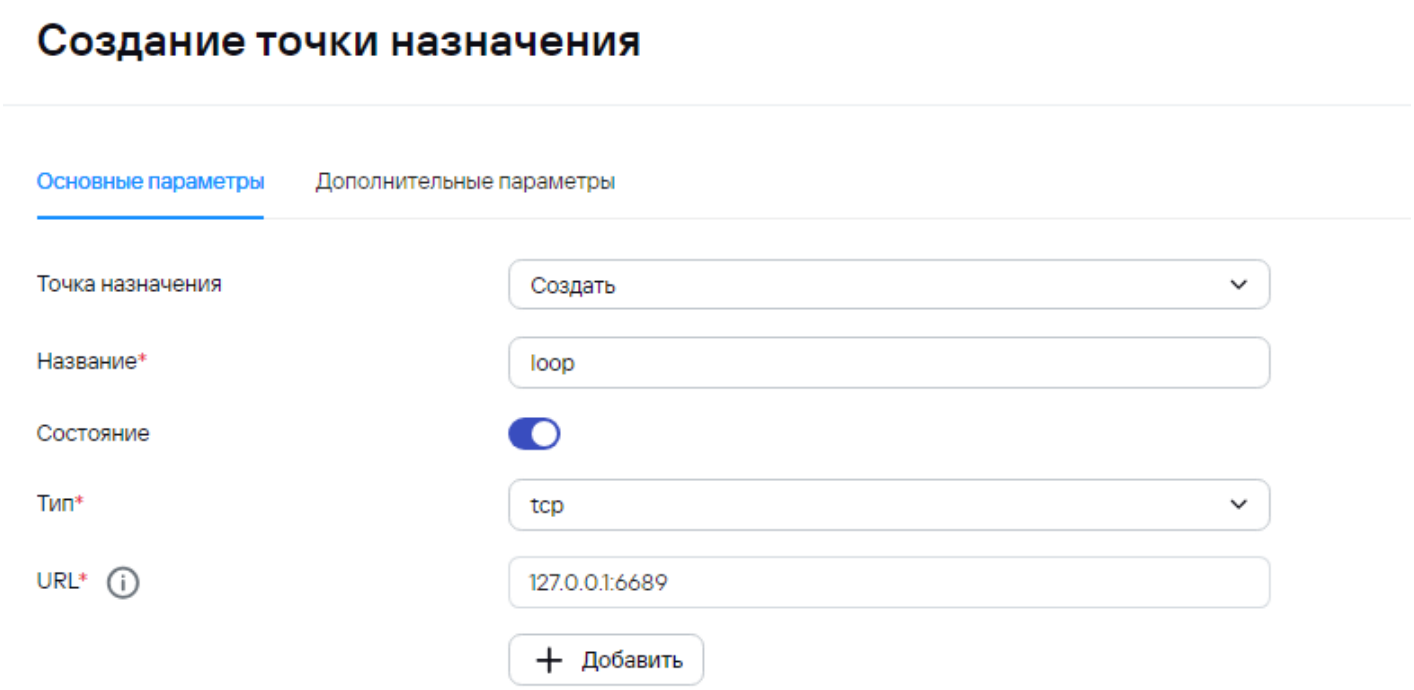
????? ????? ???????? ????? ???? ?????. ???????? ???? - ??? ??????? ????????? ?????? ???????? ?????? ???????? ???????. ????????? ??? ??????? ????????? ?????? ???? ????????? ??? ???????, ???????? ? ????????? ?????? ???. ????? ? ???? ????? ?????? ???? ??????? ?? ????, ? ??????? ?? ????? ???????? ??????? ???????? ??????.



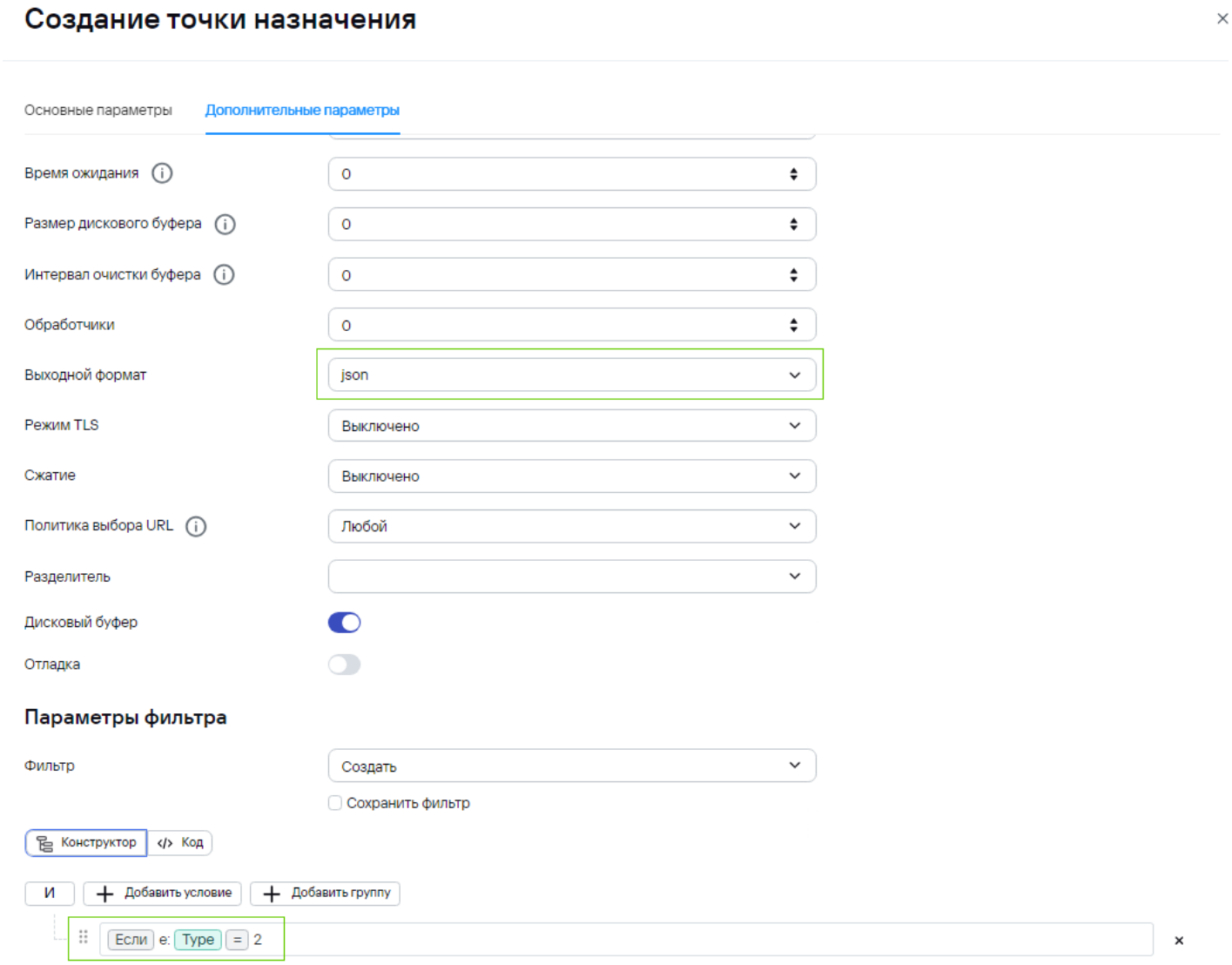
3) ?? ????? ????????????? ???? ??? ????? ??????????: 1. **Storage for AuditD** - ????????? ? **loop** - ???????????? ??????? ??????? ? ????????? (??? ? ????). ?? ????? ????? ????? ?????????? ???????? ???? ??????? **loop** - ??? *Type=2* (????????????? ???????) ? **Storage for AuditD** ??? *Type=1* (??????? ???????). ???????? ????????, ??? ??? ???????? ????? **loop,** ????? ????? ??????? ???????? ?????? **json**:

> ???????? ???? - ????????????? ????? ?????????? ?? ???? ???????. ??????? ?? ???? ?????????? ?????? ?????????? ????????????? ???????, ? ? ????????? ?????? ??????????? ?????? ???????? ??????????? ???????.

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

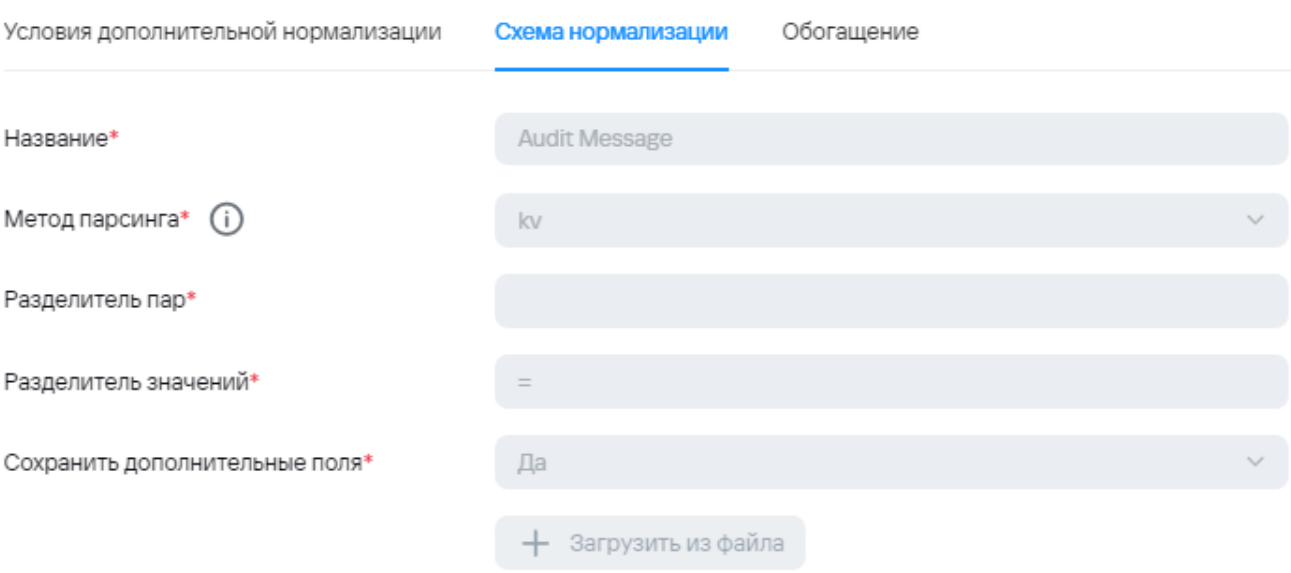

Создание точки назначения
Основные параметры
Дополнительные параметры
Точка назначения
Создать
Название*
loop
Состояние
Тип*
tcp
URL*
127.0.0.1:6689
Добавить

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



4) ????? ???????? ??????????????? ??????? ?? ???? ???? ?? ??????????, ????????? ???????? json, ??? ??? ?????????? ??????????, ? ????? ????? ?????????? ?? Message ? Extra. ??? ??????? ??? ?? ????? ????????? ????????????? ??-?? ???? ????? ???????? ? ?????? ????? ??????????.

? ????? ??????, ????, ? ??????? ?????????? ?????????? ?? ?????????? ??????? ????? ???? ?????. ????? ????? ????????? ??????????? ????????? ????? ?????.



Заключение

????? ??????????? ???? ????????? ????????? ? ?????????????? ???????????? ???????, ? ??????? ???? ????? ???????????? (id, timestamp ??? ????????? ????? ?????), ?? ???????? ????? ????????? ????????? ?????????????? ??????? ??????????? ??????? ? ??????????????.

?????, ??? ???????? ???????????????? ? ???????????? ????? ???????????? 2 ????????? ?????? ??????:

- ?????? ????????? ?????????? ???????, ????????? ??? ???????? ?????????? ? ???? ??? ????????? ????? KUMA ? ?????????? ?? ???? ??????? ?????????? ??? ???????? ? ?????????/???????????.
- ?????? ????????? ?????? ?????????? ?????????????? ??????? ?? ??????? ? ?????????? ?????????????? ??????? ? ?????????/???????????.

Полезные ссылки

1. ?????? ????????????? ? ??????? ????????? ?? ???????: https://github.com/KUMA-Community/kuma_auditd_multiline_wa/

2. ??????? ?????? ?????? ????????? (???????????): https://kb.kuma-community.ru/books/sozdanie-parserov-v-kuma-cookbook/page/princip-raboty-pravila-agregacii-sxematicno

Revision #17
Created 2024-05-24 08:39:06 UTC by lithium
Updated 2024-07-07 08:29:35 UTC by Koala