Как избирательно удалить события из очередей ТМ

InfoWatch Traffic Monitor knowledge base

Exported on 11/12/2020

1 Table of Contents

TM-6.7, TM-6.9

2 Вопрос:

Возникла ситуация, когда сотрудник отправил на внешний жёсткий диск всё содержимое своего компьютера, поставив под угрозу переполнения раздел /opt на сервере перехвата. Нужно удалить из очереди /opt/iw/tm5/queue/db только объекты копирования на внешние носители, не затронув объекты с других каналов перехвата.

3 Ответ:

Можно воспользоваться такой однострочной командой (в неё добавлены переводы строк, экранированные обратной косой чертой, для читаемости):

```
find /opt/iw/tm5/queue/db -type f -name '*.xml' -exec \
grep -l '<object_type_code>190D004827DB11E287B1F0DB6088709B00000000</object_type_code>' {} + | \
sed -e 'p;s/xml$/dat/' | \
xargs -n 10000 -P0 -r rm
```

Регулярное выражение для grep позволяет уточнить условие поиска ещё дальше, например, указать конкретного сотрудника и т. п.

Параметры xargs:
"-P0" указывает на то, что удаление будет производиться насколько возможно большим количеством параллельных процессов,
"-n 10000" указывает, что каждой команде rm будет передано 10000 имён файлов,
"-r" указывает, что при пустом списке команды выполняться не будут.