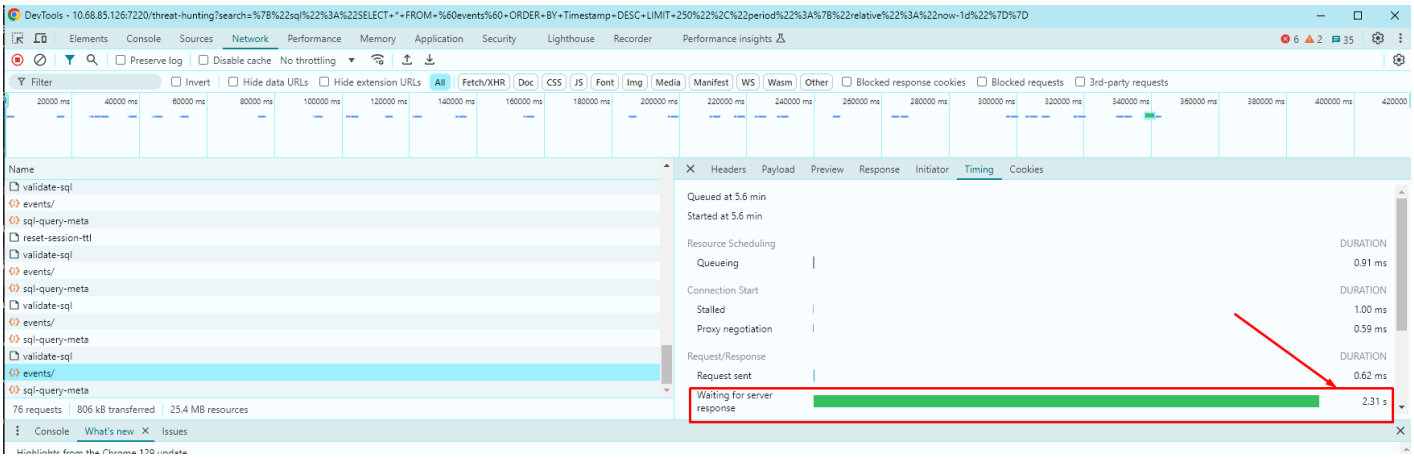
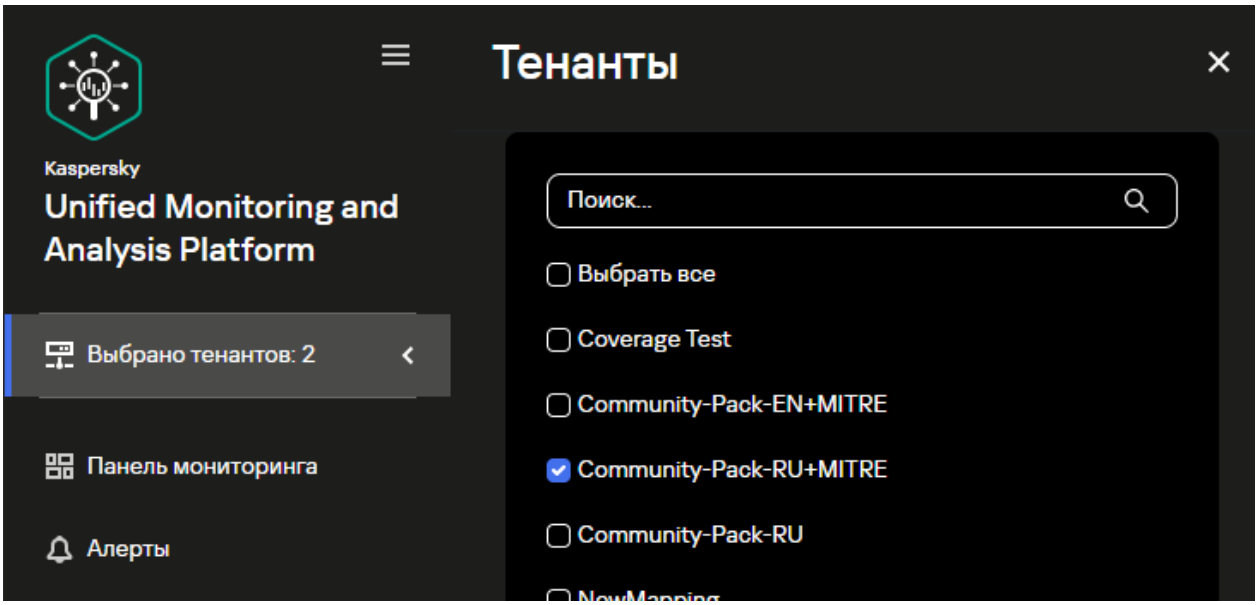
Создание оптимизированных запросов

Длительность выполнения запроса можно посмотреть при нажатии F12 (режим разработчика) в браузере Chrome после нажатия кнопки поиска:



При создании запросов всегда явно выбирайте необходимый тенант с нужными событиями:



Если известны конкретные поля для поиска, то можно использовать более глубокий поиск по событиям. Старайтесть **НЕ** использовать поиск по всем полям:

```
SELECT *
```

При поисках не увеличивайте LIMIT по умолчанию более чем 10000, все данные по поиску буферизируются в браузере.

Примеры оптимизации поисковых запросов

Пример 1:

```
SELECT SourceAddress, DestinationUserName, DeviceEventClassID
FROM `events`
WHERE DeviceProduct = 'Windows'
AND NOT endsWith(SourceUserName,'$') AND SourceUserName != 'vasya'
AND (startsWith(SourceUserName,'adm-') OR startsWith(DestinationUserName, 'adm_'))
AND NOT inSubnet(SourceAddress, '10.10.10.150/24') AND NOT inSubnet(SourceAddress, '192.168.20.180/16')
GROUP BY SourceAddress, DestinationUserName, eviceEventClassID
```

Оптимизированный запрос:

```
SELECT SourceAddress, DestinationUserName, DeviceEventClassID
FROM `events`
WHERE DeviceProduct = 'Windows'
AND SourceUserName NOT LIKE '%$' AND SourceUserName != 'vasya'
AND (SourceUserName LIKE 'adm-%' OR DestinationUserName LIKE 'adm_%')
AND NOT inSubnet(SourceAddress, '10.10.10.150/24') AND NOT inSubnet(SourceAddress, '192.168.20.180/16')
GROUP BY SourceAddress, DestinationUserName, eviceEventClassID
```

Или можно таже попробовать отказаться от функции inSubnet:

```
SELECT SourceAddress, DestinationUserName, DeviceEventClassID
FROM `events`
WHERE DeviceProduct = 'Windows'
AND SourceUserName NOT LIKE '%$' AND SourceUserName != 'vasya'
AND (SourceUserName LIKE 'adm-%' OR DestinationUserName LIKE 'adm_%')
AND NOT (SourceAddress LIKE '10.10.10.%' OR SourceAddress LIKE '192.168.%.%')
GROUP BY SourceAddress, DestinationUserName, eviceEventClassID
```

Принцип:

- Уменьшение количества условий: Объединяйте условия, где это возможно, чтобы сократить количество операций.
- Использование подзапросов или CTE: Если набор данных большой, рассмотрите возможность использования подзапросов или общих табличных выражений (CTE), чтобы разбить запрос на более мелкие, более управляемые части.
- Избегание функций в предложении WHERE: Такие функции, как endsWith, startsWith и inSubnet, могут быть узкими местами производительности. Если возможно, попробуйте переписать условия исравнить скорость выполнения.

Revision #3
Created 30 September 2024 12:49:00 by Boris Rzr
Updated 1 October 2024 14:24:49 by Boris Rzr