

Создание запросов в KUMA (CookBook)

Этакий "CookBook" по различным интересным запросам в KUMA

- [Запросы в KUMA \(примеры\)](#)

Запросы в КУМА (примеры)

Описание функций ClickHouse для работы с запросами:

<https://clickhouse.com/docs/ru/sql-reference/functions/>

Запрос из интерфейса пробрасывается в БД с добавлением границ временного промежутка и выбранных тенантов, пример: ... AND (Timestamp >= 1715689595208 AND

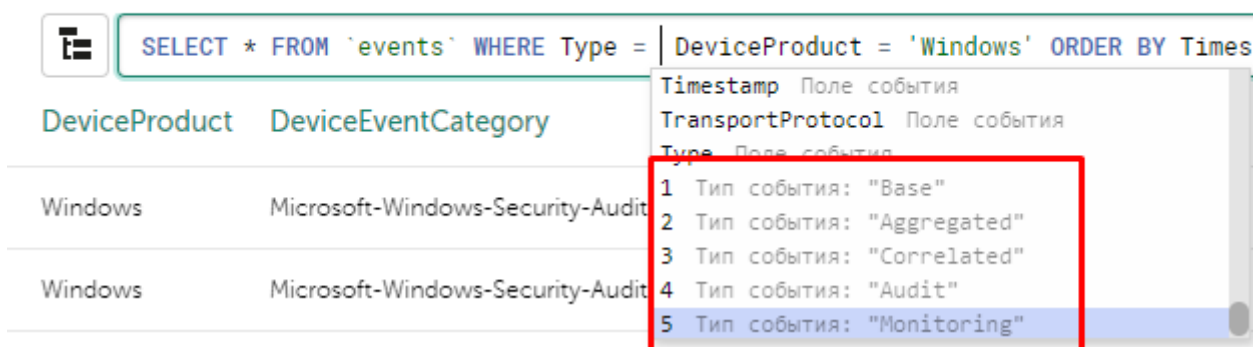
Timestamp <= 1715689895208) AND (TenantID IN ('a1fbde7a-76d3-4bbc-a769-82126b41b56f')) ORDER BY ...

https://www.youtube.com/embed/FnIT2hh_AcK?si=ktOOgrB_Q7rBL5wm

Базовые запросы

Типы событий в КУМА

События



The screenshot shows the KUMA interface with a SQL query editor and a dropdown menu for event types. The query is: `SELECT * FROM `events` WHERE Type = DeviceProduct = 'Windows' ORDER BY Times`. The dropdown menu is open, showing a list of event types: 1 Тип события: "Base", 2 Тип события: "Aggregated", 3 Тип события: "Correlated", 4 Тип события: "Audit", and 5 Тип события: "Monitoring". The first four options are highlighted with a red box, and the fifth option is highlighted with a blue box.

DeviceProduct	DeviceEventCategory
Windows	Microsoft-Windows-Security-Audit
Windows	Microsoft-Windows-Security-Audit

Подсчет событий по полю

```
SELECT count(ID) as count_num, DeviceVendor  
FROM `events`
```

GROUP BY DeviceVendor
ORDER BY count_num DESC LIMIT 250

События

Не обновлять 1д 24 часа

SELECT count(ID) as count_num, DeviceVendor FROM `events` GROUP BY DeviceVendor ORDER BY count_num DESC LIMIT 250

DeviceVendor	count_num
Unix	935809
Kaspersky	137494
Microsoft	112296

Выполнение математических операций и сравнений

```
SELECT DeviceProduct, SourceUserName, round(sum(BytesIn)/1024, 2) as KiloBytes
FROM `events`
WHERE BytesIn > '0' OR BytesOut > '0'
GROUP by SourceUserName, DeviceProduct
ORDER BY KiloBytes DESC LIMIT 250
```

Иногда бо́льшую производительность дает условие со скобками `WHERE (BytesIn > '0' OR BytesOut > '0')`

Поиск событий по подстроке (регистрозависимый) с условием И

```
SELECT *
FROM `events`
WHERE DeviceHostName like '%serv%' AND DeviceProduct = 'Windows'
ORDER BY Timestamp DESC LIMIT 250
```

События

Не обновлять 15м 15 минут

SELECT * FROM `events` WHERE DeviceHostName like '%serv%' AND DeviceProduct = 'Windows' ORDER BY Timestamp DESC LIMIT 250

DeviceProduct	DeviceHostName	SourceUserName	Timestamp ↓	TenantID	DeviceVendor	DestinationAddress	DestinationUserNa...	Name
Windows	winserv19.sales.lab		06.12.2022 10:52:20	Main	Microsoft			MALWAREPROTECTIO...
Windows	winserv19.sales.lab	winserv19\$	06.12.2022 10:51:40	Main	Microsoft		administrators	A security-enabled loc...
Windows	winserv19.sales.lab	winserv19\$	06.12.2022 10:51:40	Main	Microsoft		administrators	A security-enabled loc...

Поиск событий по подстроке (регистронезависимый)

```
SELECT *
FROM `events`
WHERE DeviceEventCategory ilike '%auditing%' AND DeviceProduct = 'Windows'
ORDER BY Timestamp DESC LIMIT 250
```

События

Не обновлять 1ч Хранилище: Exam...

SELECT * FROM `events` WHERE DeviceEventCategory ilike '%auditing%' AND DeviceProduct = 'Windows' ORDER BY Timestamp DESC LIMIT 250

DeviceProduct	DeviceEventCategory	SourceUserName	Timestamp ↓	TenantID	DeviceVendor	DestinationAddress	DestinationUserNa...	Name
Windows	Microsoft-Windows-Security Auditing	boris-test\$	06.12.2022 10:58:15	Main	Microsoft		система	An account was succe...
Windows	Microsoft-Windows-Security-Auditing	boris-test\$	06.12.2022 10:58:15	Main	Microsoft		система	An account was succe...

Поиск по исходному событию

```
SELECT *
FROM `events`
WHERE Raw ilike '%technique%'
ORDER BY Timestamp DESC LIMIT 250
```

События

Информация о событии

SELECT * FROM `events` WHERE Raw ilike '%technique%' ORDER BY Timestamp DESC LIMIT 250

TenantID	Timestamp ↓	Name	DeviceProduct	DeviceVendor	DestinationAddress
Main	30.10.2023 17:40:01	Network connection detected	Windows	Microsoft	10.68.85.130
Main	30.10.2023 17:39:59	Network connection detected	Windows	Microsoft	fe80:0:0:ddd9:f270:5...
Main	30.10.2023 17:38:47	File created	Windows	Microsoft	
Main	30.10.2023 17:38:36	Network connection detected	Windows	Microsoft	10.68.85.168
Main	30.10.2023 17:38:34	Network connection detected	Windows	Microsoft	fe80:0:0:a9c0:26b8:f0...
Main	30.10.2023 17:37:40	Network connection detected	Windows	Microsoft	10.68.85.130

Исходное событие

<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'>
<System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5778385f-c22a-43e0-bf4c-06f5698ffbd9}' /><EventID>3</EventID><Version>5</Version>
<Level>4</Level><Task>3</Task><Opcode>9</Opcode>
<Keywords>8x8000000000000000</Keywords><TimeCreated SystemTime='2023-10-30T14:39:59.5683935Z' /><EventRecordID>1056001</EventRecordID><Correlation/>
<Execution ProcessID='13572' ThreadID='13752' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Boris-Test.sales.lab</Computer>
<Security UserID='S-1-5-18' /></System><EventData><Data Name='RuleName'>technique_id=1571, technique_name=Non-Standard Port</Data>
<Data Name='UtcTime'>2023-10-30 14:36:33.425</Data><Data Name='ProcessId'>{117eae48-29b0-6362-1f00-000000000500}</Data><Data Name='ProcessId'>1400</Data></EventData></Event>

Поиск событий по нескольким значениям, вместо OR можно использовать IN

```
SELECT *
FROM `events`
```

WHERE DeviceEventClassID IN ('BROKER_USERLOGGEDOUT', 'BROKER_USERLOGGEDIN')
AND DeviceProduct = 'Horizon'
ORDER BY Timestamp DESC LIMIT 250

Events

No refresh 5m 5 minutes

SELECT * FROM `events` WHERE DeviceEventClassID IN ('BROKER_USERLOGGEDOUT', 'BROKER_USERLOGGEDIN') AND DeviceProduct = 'Horizon' ORDER BY Timestamp DESC LIMIT 250

Timestamp ↓	DeviceReceiptTime	Name	DeviceVendor	DeviceProduct	DeviceEventClassID	DestinationHostNa...	FilePath
2023-05-12 10:33:43	2023-05-12 10:33:43	Broker	VMWare	Horizon	BROKER_USERLOGGEDIN		
2023-05-12 10:33:28	2023-05-12 10:33:23	Broker	VMWare	Horizon	BROKER_USERLOGGEDIN		
2023-05-12 10:33:09	2023-05-12 10:33:04	Broker	VMWare	Horizon	BROKER_USERLOGGEDIN		
2023-05-12 10:32:54	2023-05-12 10:32:54	Broker	VMWare	Horizon	BROKER_USERLOGGEDOUT		

Поиск событий по подсети

SELECT *
FROM `events`
WHERE inSubnet(DeviceAddress, '10.68.85.70/32')
ORDER BY Timestamp DESC LIMIT 250

События

Не обновлять 15m 15 минут

SELECT * FROM `events` WHERE inSubnet(DeviceAddress, '10.68.85.70/32') ORDER BY Timestamp DESC LIMIT 250

DeviceVendor	DeviceAddress	Timestamp ↓	Name	DeviceProduct	TenantID	DestinationAddress	DestinationUserNa...
Kaspersky	10.68.85.70	02.12.2022 17:09:43	Process	EDR	Main		
Kaspersky	10.68.85.70	02.12.2022 17:09:43	Process	EDR	Main		
Kaspersky	10.68.85.70	02.12.2022 17:09:37	File change	EDR	Main		

Поиск событий по отсутствующему полю

SELECT *
FROM `events`
WHERE empty(DeviceEventClassID) AND Raw ilike '%backdoor_user%'
ORDER BY Timestamp DESC LIMIT 250

1 SELECT * FROM `events` WHERE empty(DeviceEventClassID) AND Raw.ilike('%backdoor_user%' ORDER BY Timestamp

Нажмите Ctrl + Enter, чтобы выполнить запрос

TSV

TenantID	Timestamp	DeviceHostName	DeviceEventClassID
Main	13.08.2024 11:50:39:174	ru	
Main	13.08.2024 11:50:39:174	ru	
Main	13.08.2024 11:50:33:173	ru	
Main	13.08.2024 11:50:33:173	ru	
Main	13.08.2024 11:50:33:173	ru	

Копировать

TenantID	Main
Timestamp	13.08.2024 11:50:39:174
EndTime	13.08.2024 12:20:38:000
DeviceAddress	192.168.0.178
DeviceHostName	ru
DeviceProcessID	2644130
DeviceProcessName	useradd
DeviceReceiptTime	13.08.2024 11:50:39:174
DeviceTimeZone	+03:00
DeviceVendor	Unix

Проверка работы обогащения

Обогащение событий Активами

```
SELECT *
FROM `events`
WHERE (DeviceAssetID != '' OR SourceAssetID != '' OR DestinationAssetID != '')
ORDER BY Timestamp DESC LIMIT 250
```

Обогащение событий с LDAP

```
SELECT *
FROM `events`
WHERE (SourceAccountID != '' OR DestinationAccountID != '')
ORDER BY Timestamp DESC LIMIT 250
```

Обогащение событий данными из TI

```
SELECT *
FROM `events`
WHERE NOT TI=""
```

Работа с Extra полем

Поиск событий по полю Extra содержащие ключ

```
SELECT *  
FROM `events`  
WHERE visitParamHas(Extra, 'memUsage')  
ORDER BY Timestamp DESC LIMIT 250
```

Raw	<pre>{ "cpu1": 0, "cpu2": 0, "cpu3": 0, "cpu4": 0, "diskBlock": 4096, "diskSize": 26056703, "diskUsage": 8194425, "memBlock": 65536, "memSize": 65519, "memSizeKB": 4193260, "memUsage": 61367, "sysName": "dc-01.sales.lab", "sysUpTime": 571326915 } \n</pre>
Extra	<pre>diskBlock: 4096 diskSize: 26056703 diskUsage: 8194425 memBlock: 65536 memSize: 65519 memSizeKB: 4193260 memUsage: 61367</pre>

Поиск событий по полю Extra содержащие ключ с определенным значением

```
SELECT *  
FROM `events`  
WHERE visitParamExtractString(Extra, 'memUsage') = '61367'  
ORDER BY Timestamp DESC LIMIT 250
```

```
SELECT *  
FROM `events`  
WHERE JSONExtractString(Extra, 'memUsage') = '61367'  
ORDER BY Timestamp DESC LIMIT 250
```

Type	Base
Raw	{ "cpu1":0,"cpu2":1,"cpu3":0,"cpu4":0,"diskBlock":4096,"diskSize":26056703,"diskUsage":8194425,"memBlock":65536,"memSize":65519,"memSizeKB":4193260,"memUsage":61367,"sysName":"dc-01.sales.lab","sysUpTime":571333918}\n
Extra	diskBlock: 4096 diskSize: 26056703 diskUsage: 8194425 memBlock: 65536 memSize: 65519 memSizeKB: 4193260 memUsage: 61367

Поиск событий по полю Extra НЕ содержащие ключ с определенным значением

```
SELECT *  
FROM `events`  
WHERE visitParamHas(Extra, 'memUsage')  
AND NOT visitParamExtractString(Extra, 'memUsage') = '61367'  
ORDER BY Timestamp DESC LIMIT 250
```


Type	Base
Raw	<pre>{ "cpu1": 1, "cpu2": 1, "cpu3": 1, "cpu4": 0, "diskBlock": 4096, "diskSize": 26056703, "diskUsage": 8194885, "memBlock": 65536, "memSize": 65519, "memSizeKB": 4193260, "memUsage": 61693, "sysName": "dc-01.sales.lab", "sysUpTime": 571362433 }</pre>
Extra	<pre>diskBlock: 4096 diskSize: 26056703 diskUsage: 8194885 memBlock: 65536 memSize: 65519 memSizeKB: 4193260 memUsage: 61693</pre>

Работа со временем

Timestamp по умолчанию в формате epoch time числа с миллисекундами (UnixTimestamp)

Список тайм зон: https://en.wikipedia.org/wiki/List_of_tz_database_time_zones

События				Не обновлять	1d 24 часа	Хранилище: Exam	...
<pre>SELECT Timestamp, DeviceProduct, Name, Message FROM `events` WHERE DeviceProduct = 'EDR' ORDER BY Timestamp DESC LIMIT 250</pre>							
1670227006886	DeviceProduct	Name	Message				
05.12.2022 10:56:46	EDR	Connection	Network connection from 10.68.85.145 to 10.68.85.135:5983				
05.12.2022 10:56:46	EDR	Process	Process C:\Windows\System32\wormgr.exe on				
05.12.2022 10:56:43	EDR	Connection	Network connection from 10.68.85.130 to 10.68.65.50:3128				

Задание таймзоны

```
SELECT Timestamp, fromUnixTimestamp64Milli(Timestamp, 'Europe/Moscow') as NormTime,
DeviceProduct, Name, Message
FROM `events`
WHERE DeviceProduct = 'EDR'
ORDER BY Timestamp DESC LIMIT 250
```

События				
<div>Не обновлять 24 часа Хранилище: [Екст...]</div> <div>SELECT Timestamp, fromUnixTimestamp64Milli(Timestamp, 'Europe/Moscow') as NormTime, DeviceProduct, Name, Message FROM `events` WHERE DeviceProduct = 'EDR' ORDER BY Timestamp DESC LIMIT 250</div>				
NormTime	Timestamp ↓	DeviceProduct	Name	Message
2022-12-05 10:59:58 917	05.12.2022 10:59:58	EDR	Connection	Network connection from 10.68.85.137 to 184.51.233.240:80
2022-12-05 10:59:58 917	05.12.2022 10:59:58	EDR	Process	Process C:\Windows\SysWOW64\chcp.com on
2022-12-05 10:59:58 917	05.12.2022 10:59:58	EDR	Script run via shell	Script event_script_bat_KSC.bat was run from command shell on

Указание своего формата времени

```
SELECT Timestamp, formatDateTime(fromUnixTimestamp64Milli(Timestamp), '%d-%m-%Y %H:%i:%S') as NormTime, DeviceProduct, Name, Message FROM `events` WHERE DeviceProduct = 'EDR' ORDER BY Timestamp DESC LIMIT 250
```

События				
<div>Не обновлять 24 часа Хранилище: [Екст...]</div> <div>SELECT Timestamp, formatDateTime(fromUnixTimestamp64Milli(Timestamp), '%d-%m-%Y %H:%M:%S') as NormTime, DeviceProduct, Name, Message FROM `events` WHERE DeviceProduct = 'EDR' ORDER BY Timestamp DESC LIMIT 250</div>				
NormTime	Timestamp ↓	DeviceProduct	Name	Message
05-12-2022 08:05:59	05.12.2022 11:05:59	EDR	Process	Process C:\Windows\System32\rundll32.exe on
05-12-2022 08:05:59	05.12.2022 11:05:59	EDR	Registry change	Registry value \REGISTRY\USER\S-1-5-21-781213047-594974509-2262175553-1766_Classes(Local Settings\Software)\Mic...
05-12-2022 08:05:59	05.12.2022 11:05:59	EDR	Registry change	Registry value \REGISTRY\USER\S-1-5-21-781213047-594974509-2262175553-1766(SOFTWARE\Microsoft\Windows\Cur...

Свой формат времени с таймзоной

```
SELECT Timestamp, formatDateTime(fromUnixTimestamp64Milli(Timestamp), '%d-%m-%Y %H:%i:%S', 'Europe/Moscow') as NormTime, DeviceProduct, Name, Message FROM `events` WHERE DeviceProduct = 'EDR' ORDER BY Timestamp DESC LIMIT 250
```

События				
<div>Не обновлять 24 часа Хранилище: [Екст...]</div> <div>SELECT Timestamp, formatDateTime(fromUnixTimestamp64Milli(Timestamp), '%d-%m-%Y %H:%M:%S', 'Europe/Moscow') as NormTime, DeviceProduct, Name, Message FROM `events` WHERE DeviceProduct = 'EDR' ORDER BY Timestamp DESC LIMIT 250</div>				
NormTime	Timestamp ↓	DeviceProduct	Name	Message
05-12-2022 11:08:01	05.12.2022 11:08:01	EDR	Connection	Network connection from 10.68.85.11 to 10.68.85.2-49668
05-12-2022 11:07:58	05.12.2022 11:07:58	EDR	Process	Process C:\Users\irodonov\AppData\Local\Microsoft\OneDrive\19.043.0304.0013_2\FileCoAuth.exe on
05-12-2022 11:07:37	05.12.2022 11:07:37	EDR	Process	Process C:\Windows\SysWOW64\wbem\WmiPrivSE.exe on

События в "рабочее время" с 9 до 18

```
SELECT Timestamp,
formatDateTime(fromUnixTimestamp64Milli(Timestamp), '%d-%m-%Y %H:%i:%S', 'Europe/Moscow') as
NormTime,
DeviceProduct, Name, Message
FROM `events`
WHERE DeviceProduct = 'EDR' AND toHour(fromUnixTimestamp64Milli(Timestamp, 'Europe/Moscow')) >= 9
AND toHour(fromUnixTimestamp64Milli(Timestamp, 'Europe/Moscow')) < 18
ORDER BY Timestamp ASC LIMIT 250
```

События

Не обновлять 12 02.12.2022 00:00:00 - 03:12:00 Хранилище: Exam...

SELECT Timestamp, formatDateTime(fromUnixTimestamp64Milli(Timestamp), '%d-%m-%Y %H:%i:%S', 'Europe/Moscow') as NormTime, DeviceProduct, Name, Message FROM `events` WHERE DeviceProduct = 'EDR' AND toHour(fromUnixTimestamp64Milli(Timestamp, 'Europe/Moscow')) >= 9 AND toHour(fromUnixTimestamp64Milli(Timestamp, 'Europe/Moscow')) < 18 ORDER BY Timestamp ASC LIMIT 250

Всего: 25 118

NormTime	Timestamp ↑	DeviceProduct	Name	Message
02-12-2022 09:00:00	02.12.2022 09:00:00	EDR	Process	Process C:\Windows\SysWOW64\chcp.com on
02-12-2022 09:00:01	02.12.2022 09:00:01	EDR	Process	Process C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center\kserver.exe on

Подсчет события по фильтру за период вчерашнего дня с 00 до 04 часов с группировкой по SourceAddress

```
SELECT count(ID) as Count_Num, SourceAddress, groupArray(fromUnixTimestamp64Milli(Timestamp)) as
time_stm
FROM `events`
WHERE DeviceEventClassID = '4624' AND DeviceProduct = 'Windows'
AND Timestamp >= toUnixTimestamp(toStartOfDay((now() - INTERVAL 1 DAY)))*1000
AND Timestamp <= toUnixTimestamp(toStartOfDay((now() - INTERVAL 1 DAY)) + INTERVAL 4 HOUR)*1000
GROUP BY SourceAddress LIMIT 250
```

События


Не обновлять 15 01.05.2023 00:00:00 - 16:05:00 Хранилище: OOT...

SELECT count(ID) as Count_Num, SourceAddress, groupArray(fromUnixTimestamp64Milli(Timestamp)) as time_stm FROM `events` WHERE DeviceEventClassID = '4624' AND DeviceProduct = 'Windows' AND Timestamp >= toUnixTimestamp(toStartOfDay((now() - INTERVAL 1 DAY)))*1000 AND Timestamp <= toUnixTimestamp(toStartOfDay((now() - INTERVAL 1 DAY)) + INTERVAL 4 HOUR)*1000 GROUP BY SourceAddress LIMIT 250

Count_Num	SourceAddress	time_stm
202		[2023-05-14 00:01:08.729;2023-05-14 00:01:23.750;2023-05-14 00:02:50.996;2023-05-14 00:02:50.997;2023-05-14 00:02:50.997;2023-05-14 00:03:19.100;2023-05-14 00:07:04.727;2023-05-14 00:07:36.786;2023-05-14 00:...
89	10.68.85.64	[2023-05-14 00:01:08.728;2023-05-14 00:01:08.728;2023-05-14 00:01:08.728;2023-05-14 00:01:08.729;2023-05-14 00:01:34.772;2023-05-14 00:07:02.726;2023-05-14 00:07:02.726;2023-05-14 00:07:02.727;2023-05-14 00:...
24	10.68.85.124	[2023-05-14 00:06:38.670;2023-05-14 00:21:38.550;2023-05-14 00:36:38.820;2023-05-14 00:51:39.021;2023-05-14 01:06:39.167;2023-05-14 01:21:39.306;2023-05-14 01:35:19.546;2023-05-14 01:35:19.546;2023-05-14 01:...
45	10.68.85.150	[2023-05-14 00:11:15.271;2023-05-14 00:26:15.180;2023-05-14 00:27:23.386;2023-05-14 00:41:14.534;2023-05-14 00:56:14.665;2023-05-14 01:02:01.414;2023-05-14 01:02:01.414;2023-05-14 01:02:01.414;2023-05-14 01:...

Подсчет уникальных адресов посетителей kb.kuma-community.ru

```
SELECT count(DISTINCT SourceAddress) as uniqSrcIP
FROM `events`
WHERE Code = '200' AND DeviceCustomString2 != '-' AND DestinationServiceName = 'apache_access'
AND DeviceCustomString3 = 'GET' AND DestinationHostName = 'kb'
AND not inSubnet(SourceAddress, '91.103.66.0/24')
```

 `SELECT count(DISTINCT SourceAddress) as uniqSrcIP FROM `events` WHERE Code = '200' AND DeviceCustomString2 != '-' AND DestinationServiceName = 'apache_access' AND DeviceCustomString3 = 'GET' AND DestinationHostName = 'kb' AND not inSubnet(SourceAddress, '91.103.66.0/24')`

uniqSrcIP DeviceCustomStri... SourceAddress

16

Можно использовать аналогичную более быструю функцию:

```
SELECT uniq(SourceAddress) as uniqSrcIP
FROM `events`
WHERE Code = '200' AND DeviceCustomString2 != '-' AND DestinationServiceName = 'apache_access'
AND DeviceCustomString3 = 'GET' AND DestinationHostName = 'kb'
AND not inSubnet(SourceAddress, '91.103.66.0/24')
```

Подсчет уникальных адресов посетителей kb.kuma-community.ru по дням

```
SELECT count(DISTINCT SourceAddress) as `metric`,
formatDateTime(fromUnixTimestamp64Milli(Timestamp), '%d-%m-%Y', 'Europe/Moscow') as value
FROM `events`
WHERE Code = '200' AND DeviceCustomString2 != '-' AND DestinationServiceName = 'apache_access'
AND DeviceCustomString3 = 'GET' AND DestinationHostName = 'kb'
AND not inSubnet(SourceAddress, '91.103.66.0/24')
GROUP BY value
```

Events

No refresh

11d 2023-10-22 00:00:00 - 2023...

Storage: IOTB| St...

SELECT count(DISTINCT SourceAddress) as 'metric', formatDate(fromUnixTimestamp64Milli(Timestamp), '%d-%m-%Y', 'Europe/Moscow') as value FROM 'events' WHERE Code = '200' AND DeviceCustomString2 != '-' AND DestinationServiceName = 'apache_access' AND DeviceCustomString3 = 'GET' AND DestinationHostName = 'kb' AND not inSubnet(SourceAddress, '91.103.66.0/24') GROUP BY value

metric	value
147	26-10-2023
140	27-10-2023
115	24-10-2023
103	25-10-2023
120	31-10-2023
166	30-10-2023
39	28-10-2023
33	29-10-2023
145	23-10-2023
22	22-10-2023
115	01-11-2023

Подсчет среднего количества переданных байт посетителей kb.kuma-community.ru по источнику IP с 00:00 по 08:00

```
SELECT avg(toInt32(BytesOut)), SourceAddress
FROM `events`
WHERE BytesOut!= 0 AND Timestamp >= toUnixTimestamp(toStartOfDay((now() - INTERVAL 1 DAY)))*1000
AND Timestamp <= toUnixTimestamp(toStartOfDay((now() - INTERVAL 1 DAY)) + INTERVAL 8 HOUR)*1000
GROUP BY SourceAddress DESC LIMIT 250
```

Events

No refresh

2d 2023-11-22 00:00:00 - 2023-...

Storage: STOR

SELECT avg(toInt32(BytesOut)), SourceAddress FROM 'events' WHERE BytesOut!= 0 AND Timestamp >= toUnixTimestamp(toStartOfDay((now() - INTERVAL 1 DAY)))*1000 AND Timestamp <= toUnixTimestamp(toStartOfDay((now() - INTERVAL 1 DAY)) + INTERVAL 8 HOUR)*1000 GROUP BY SourceAddress DESC LIMIT 250

avg(toInt32(BytesOut))	SourceAddress
126	::1
14365.5	207...53
9499.666666666666	185...3.50
58497.565217391304	89.1...42
43983.75	46.1...148
91397.61538461539	176...33
5874	213...3.221

Отображение количества переданных и принятых байт по внутренним адресам более 1 Гб

```
SELECT StartTime , EndTime , SourceAddress AS `SOURCE ADDRESS`, DestinationPort AS `TO PORT`,
ApplicationProtocol AS `APPLICATION`, DeviceCustomString1 AS `RULE`, formatReadableSize(BytesIn) AS
`SENT`, formatReadableSize(BytesOut) AS `RECEIVED`, formatReadableSize(FlexNumber1) AS `TOTAL`
FROM `events`
WHERE FlexNumber1 > 1000000000
GROUP BY StartTime, EndTime, SourceAddress, DestinationPort, ApplicationProtocol, DeviceCustomString1,
BytesIn, BytesOut, FlexNumber1
ORDER BY `EndTime` DESC LIMIT 250
```

Большие выгрузки за день >

Download

CSV

1d

StartTime	EndTime	SOURCE ADDRESS	TO PORT	APPLICATION	RULE	SENT	RECEIVED	TOTAL
2024-06-25 09:14:54	2024-06-25 20:15:00	192.168.1.1	3389	ms-rdp	Any	30.68 MiB	1.08 GiB	1.11 GiB
2024-06-25 16:02:48	2024-06-25 16:04:30	192.168.1.1	5434	postgres	Any	108.90 MiB	4.76 GiB	4.87 GiB

Экстра запросы

Склейка по времени подключений пользователей с одного адреса и на один VPN сервер

```
SELECT SourceUserName, SourceAddress, SourceHostName, groupArray(FlexString1) as time
FROM `events`
WHERE SourceProcessName = 'Create session'
GROUP BY SourceUserName, SourceAddress, SourceHostName LIMIT 10
```

Events

No refresh

2d 2022-12-05 00:00:00 - 2022...

SELECT SourceUserName, SourceAddress, SourceHostName, groupArray(FlexString1) as time FROM `events` where SourceProcessName = 'Create session' GROUP BY SourceUserName, SourceAddress, SourceHostName LIMIT 10

SourceAddress	SourceHostName	SourceUserName	time
21.187	SSLVPN-CL02-02	ko	06:46:57,14:28:02,11:19:19
85	SSLVPN-CL02-01	on	06:50:49
19	SSLVPN-CL02-01	m	05:00:47,05:02:07
21	SSLVPN-CL02-01	an	15:50:38,18:42:09,12:08:12

Склейка различных адресов подключений от одного пользователя на VPN сервере

Оператор HAVING доступен с версии KUMA 3.0

```
SELECT uniq(SourceAddress) as "Количество уникальных адресов", DestinationUserName as "Имя пользователя", groupUniqArray(SourceAddress) as "Список адресов"
FROM `events`
WHERE DeviceProduct = 'Ngate' AND Name = 'Create session'
GROUP BY "Имя пользователя"
HAVING "Количество уникальных адресов" > 1
ORDER BY "Количество уникальных адресов" DESC
LIMIT 10
```

Количество уникальных адресов	Имя пользователя	Список адресов
5	SKAYA	21.187, 85, 19, 21
5	OV	80.23, 95.24, 46.138
4	CHIK	95.24, 46.138, 21.187, 85
4	IV	80.23, 95.24, 46.138, 21.187
3	EV	31.17, 176.5, 176.5
3	EV	176.5, 176.5, 95.24
3	HVALOV	95.24, 46.138, 21.187
3	R	46.138, 21.187, 85

Обрезка доменов до второго уровня и условие с несколькими запросами

```
SELECT count(ID) as cnt, cutToFirstSignificantSubdomain(DestinationHostName) as dstH
FROM `events`
WHERE DeviceCustomString1 = 'Q' AND DestinationProcessName = 'DNS'
AND DeviceCustomString5 IN ('A', 'AAAA', 'HTTPS')
GROUP BY dstH
ORDER BY cnt DESC LIMIT 50
```

Events No refresh 1d 2022-12-15 12:31:15 - 2022-1... Storage: (OOTB) Storage ...

SQL

SELECT count(ID) as cnt, cutToFirstSignificantSubdomain(DestinationHostName) as dstH FROM `events` WHERE DeviceCustomString1 = 'Q' AND DestinationProcessName = 'DNS' AND DeviceCustomString5 IN ('A', 'AAAA', 'HTTPS') GROUP BY dstH ORDER BY cnt DESC LIMIT 50

Q

📊

📄

cnt	dstH
272038	OCAL
244771	gov.ru
229016	mail.ru
205223	skysever.com.br

Группировка событий по категории из TI (Regex)

```
SELECT count(ID) as cnt, extract(TI, '^.+category\\\\"\\:([^\"]+).+') as category
FROM `events`
WHERE TI != ''
GROUP BY category
ORDER BY cnt DESC
```

Events No refresh 15m 15 minutes ...

SQL

SELECT count(ID) as cnt, extract(TI, '^.+category\\\\"\\:([^\"]+).+') as category FROM `events` WHERE TI != '' GROUP BY category ORDER BY cnt DESC

Q

📊

📄

cnt	category
39	botnet_cnc
8	proxy
2	tor_node

Найти и вывести все базовые события конкретного корреляционного события по его ID

```
SELECT *
FROM `events`
WHERE ID IN (
  SELECT arrayJoin(splitByChar(',', replaceRegexpAll(JSON_QUERY(BaseEvents, '$[*].ID'), '\\[|\\]|' , ''))) as TestID
FROM `events`
WHERE (Type = 3) AND (ID = '25e4eae3-ad6d-4114-b99e-019de3574d16')
)
```

Events >

Alert investigation: [Test] Old bases

Related to alert No refresh 129d 2

SELECT * FROM `events` ORDER BY Timestamp DESC LIMIT 250

Use of SQL functions is limited when in drilldown mode. For details see [Online Help](#).

Link to alert	Timestamp ↓	Name	DestinationAddress	DestinationHostNa...	Message	ID
Linked	2023-02-06 17:15:21	[Test] Old bases	10.32.49.142	kasperskypc.	Базы данных хоста не ...	6fecc2c7-6104-4fad-b6fd-cba05281f470
Linked	2023-02-06 17:15:17		10.32.49.142	kasperskypc.		bc409f2c-6b68-46ad-9f24-44cc64388751
Linked	2023-02-06 10:40:57	[Test] Old bases	10.32.55.67	kasperskypc.	Базы данных хоста не ...	a9ea885b-4712-43d6-ab00-e6159a8ef025
Linked	2023-02-06 10:40:56		10.32.55.67	kasperskypc.		4e7ff3cd-145e-4896-b099-f16d01b1e280

Запросы к системным таблицам

У ClickHouse есть системные таблицы (<https://clickhouse.com/docs/en/operations/system-tables>).

Одна из них - query_log (https://clickhouse.com/docs/en/operations/system-tables/query_log), содержит интересную информацию о запросах.

Чтобы обратиться к данным таблицами можно использовать клиент ClickHouse, который располагается по пути `/opt/kaspersky/kuma/clickhouse/bin/client.sh`

Можно заходить в консоль ClickHouse с помощью данного клиента, а также выполнять запросы через аргументы клиента, а также формировать запросы с помощью curl. В примерах ниже будет рассмотрен именно первый способ.

Вывод запросов с сортировкой по длительности

В примере ниже представлен запрос с сортировкой по длительности выполнения запросов за конкретный день

```
SELECT *  
FROM system.query_log  
WHERE query_kind = 'Select' AND current_database = 'kuma' AND event_date = '2024-01-22'  
AND query_duration_ms != 0  
ORDER BY query_duration_ms DESC LIMIT 10
```

Вывод запросов, завершившихся ошибкой

```
SELECT *  
FROM system.query_log  
WHERE type = 'ExceptionWhileProcessing' AND current_database = 'kuma'  
LIMIT 10
```
