

Запросы в KUMA (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

Время в событиях

Если в событии присутствует информация о таймзоне (deviceTimeZone) или корректно парсится timestamp события в нормализаторе, где получаем $\pm hh:mm$ и маппится это значение в поле DeviceTimeZone - событие поступает в KUMA со значением этой таймзоны

Если в событии нет deviceTimeZone или время из события не содержит таймзону, которую можно распарсить, то для такого события устанавливается таймзона сервера на котором установлен коллектор.


Таймзону еще можно поправить следующим образом:

- создать правило обогащения типа таймзона и скорректировать временную зону;
- в поисковый запрос добавить константу с таймзоной (пример, `SELECT '+0300' as deviceTimeZone`), можно так же указать таймзону формата `+03:00` или `+03`.

Базовые запросы (поиск событий)

Типы событий в KUMA

События

 <code>SELECT * FROM `events` WHERE Type = DeviceProduct = 'Windows' ORDER BY Times</code>	
DeviceProduct	DeviceEventCategory
Windows	Microsoft-Windows-Security-Audit
Windows	Microsoft-Windows-Security-Audit



Timestamp Поле события
TransportProtocol Поле события
Type Поле события

- 1 Тип события: "Base"
- 2 Тип события: "Aggregated"
- 3 Тип события: "Correlated"
- 4 Тип события: "Audit"
- 5 Тип события: "Monitoring"

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  24 часа

 <code>SELECT count(ID) as count_num, DeviceVendor FROM `events` GROUP BY DeviceVendor ORDER BY count_num DESC LIMIT 250</code>	
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 БОльшую производительность дает условие со скобками WHERE (BytesIn > '0' OR BytesOut > '0')

По подстроке (регистрозависимый) с условием И

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

События

Не обновлять1515 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...

По подстроке (регистроНЕзависимый)

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

События

Не обновлять11 часХранилище: [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...

По исходному / сырому 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						Исходное событие	
TenantID	Timestamp ↓	Name	DeviceProduct	DeviceVendor	DestinationAddress	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-86f5698ffbd9}' /><EventID>3</EventID><Version>5</Version><Level>4</Level><Task>3</Task><Opcode>8</Opcode><Keywords>8x8000000000000000</Keywords><TimeCreated SystemTime='2023-10-30T14:39:59.560393Z' /><EventRecordID>1056001</EventRecordID><Correlation><Execution ProcessID='13572' ThreadID='13752' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Boris-Test.sales.lab</Computer><Security UserID='0x0000000000000000' /></System><EventData><Data Name='RuleName'>technique_id:T1571, technique_name:Non-Standard Port</Data><Data Name='UtcTime'>2023-10-30 14:36:33.425</Data><Data Name='ProcessGuid'>{117eae48-29b0-6362-1f00-00000000500}</Data><Data Name='ProcessId'>1400</Data></EventData></Event>	
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:dd9f270:5...		
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:a9c0:26b8f0...		
Main	30.10.2023 17:38:40	Network connection detected	Windows	Microsoft	10.68.85.70		

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			

По подсети

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

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		

Внешние IPv4 адреса

```
SELECT count(ID) as count, DestinationAddress
FROM `events`
WHERE NOT empty(DestinationAddress) AND NOT (inSubnet(DestinationAddress, '10.0.0.0/8') OR
inSubnet(DestinationAddress, '172.16.0.0/12') OR inSubnet(DestinationAddress, '192.168.0.0/16') OR
inSubnet(DestinationAddress, '127.0.0.0/8'))
AND NOT isIPv6String(DestinationAddress)
GROUP BY DestinationAddress
ORDER BY count DESC LIMIT 250
```

```
1 SELECT count(ID) as count, DestinationAddress FROM `events` WHERE NOT empty(DestinationAddress) AND NOT (inSubnet(DestinationAddress, '10.0.0.0/8') OR inSubnet(DestinationAddress, '172.16.0.0/12') OR inSubnet
(DestinationAddress, '192.168.0.0/16') OR inSubnet(DestinationAddress, '127.0.0.0/8')) AND NOT isIPv6String(DestinationAddress) GROUP BY DestinationAddress ORDER BY count DESC LIMIT 250
```

Нажмите Ctrl + Enter, чтобы выполнить запрос

TSV

Поиск по полям группы...

DestinationAddress: 185.199.110.133
count: 810
DestinationAddress: 185.199.108.133
count: 809
DestinationAddress: 185.199.109.133

TSV

Поиск по локальным событиям...

TenantID	Timestamp	Name	DeviceProduct	DeviceVendor
Main	19.12.2024 10:54:31.284		audit	Unix
Main	19.12.2024 10:54:30.284		audit	Unix
Main	19.12.2024 10:54:29.282		audit	Unix

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 Row 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

По регулярному выражению

SELECT *
FROM `events`
WHERE match(DestinationUserName, '^\\w+\\-\\d\\\$\\\$')
ORDER BY Timestamp DESC LIMIT 250

События

Не обновлять

1д Последние 24ч

1 SELECT * FROM `events` WHERE match(DestinationUserName, '^\\w+\\-\\d\\\$\\\$') ORDER BY Timestamp DESC LIMIT 250

Нажмите Ctrl + Enter, чтобы выполнить запрос

TSV

Timestamp	Name	DeviceProduct	DeviceVendor	DestinationUserName	DeviceEventClassID
23.10.2024 16:24:31:736	An account was successfully logged on.	Windows	Microsoft	pc-2\$	4624
23.10.2024 16:24:31:736	An account was logged off.	Windows	Microsoft	pc-2\$	4634
23.10.2024 16:24:28:735	An account was successfully logged on.	Windows	Microsoft	pc-5\$	4624
23.10.2024 16:24:28:735	An account was logged off.	Windows	Microsoft	pc-5\$	4634
23.10.2024 16:23:53:578	An account was successfully logged on.	Windows	Microsoft	pc-4\$	4624

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=""  
ORDER BY Timestamp DESC LIMIT 250
```

Работа с Extra полем

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>

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	<pre>{ "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</pre>
Extra	<pre>diskBlock: 4096 diskSize: 26056703 diskUsage: 8194425 memBlock: 65536 memSize: 65519 memSizeKB: 4193260 memUsage: 61367</pre>

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	{ "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}
Extra	diskBlock: 4096 diskSize: 26056703 diskUsage: 8194885 memBlock: 65536 memSize: 65519 memSizeKB: 4193260 memUsage: 61693

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 24 часа Хранилище: [Екст...]

SELECT Timestamp, DeviceProduct, Name, Message FROM `events` WHERE DeviceProduct = 'EDR' ORDER BY Timestamp DESC LIMIT 250

	DeviceProduct	Name	Message
1670227006986	EDR	Connection	Network connection from 10.68.85.145 to 10.68.85.135.5985
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

Не обновлять 24 часа Хранилище: [Exam...]

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

Не обновлять 24 часа Хранилище: [Exam...]

NormTime	Timestamp ↓	DeviceProduct	Name	Message
05-12-2022 08:05:59	05.12.2022 11:05:59	EDR	Process	Process C:\Windows\System32\cmd.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					Не обновлять	1d 24 часа	Хранилище: [Exam...]	...
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					🔍	📊	📄	
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	1d 02.12.2022 00:00:00 - 03.12...	Хранилище: [Exam...]	...
SELECT Timestamp, formatDateTime(fromUnixTimestamp64Milli(Timestamp), '%d-%m-%Y %H:%M:%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\klserver.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

15a 01.05.2023 00:00:00 - 16.05...

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', 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

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 посетителями 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
```

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	207.172.153
9499.666666666666	185.199.13.50
58497.565217391304	89.148.142
43983.75	46.101.148
91397.61538461539	176.16.133
5874	213.141.13.221

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 >

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
213.187.187.187	SSLVPN-CL02-02	korotkov	06:46:57,14:28:02,11:19:19
81.187.187.187	SSLVPN-CL02-01	korotkov	06:50:49
193.187.187.187	SSLVPN-CL02-01	korotkov	05:00:47,05:02:07
213.187.187.187	SSLVPN-CL02-01	korotkov	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	2 ██████████ 50
5	██████████ OV	80 ██████████ 27
4	██████████	95 ██████████ 115
4	██████████ NCHIK	80.23 ██████████ 0
3	██████████ V	31.1 ██████████ 94
3	██████████ EV	176.5 ██████████ 27
3	██████████	176.5 ██████████ 65
3	██████████ HVALOV	95.2 ██████████ 32
3	██████████ ?	46.138 ██████████ 58

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	Id	2022-12-15 12:31:15 - 2022-1...	Storage: [OOTB] Storage	...
<pre>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</pre>						
cnt	dstH					
272038	██████████ OCAL					
244771	██████████ gov.ru					
229016	mail.ru					
205223	skysever.com.br					

Обрезка доменов до второго уровня и исключение IP адресов с помощью регулярного выражения


```
SELECT count(ID) as `metric`, cutToFirstSignificantSubdomain(RequestUrl) as `value`,  
match(`value`, '^\([a-zA-Z0-9-]+\.[a-zA-Z]{2,}\$') AS is_valid_domain  
FROM `events`  
WHERE DeviceProduct = 'UTM' AND FlexString2 = 'Instant Messaging' AND Type != 3 AND is_valid_domain = 1  
GROUP BY `value` ORDER BY `metric` DESC LIMIT 250
```

Группы (6)

Карточки Таблица <<

TSV

Поиск по полям группы... 🔍

metric	value	is_valid_domain
107	whatsapp.net	1
68	telegram.org	1
14	whatsapp.com	1
10	jivo.ru	1
1	t.me	1
1	telegram.me	1

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

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

cnt	category
39	botnet_cnc
8	proxy
2	ip_node

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.		4e7f3cd-145e-4896-b099-f16d01b1e280

Дерево процесса

```
SELECT
  b.DeviceHostName AS HostName,
  b.SourceAccountID AS AccountID,
  b.SourceUserName AS UserName,
  a.DeviceCustomString3 AS GrandParentProcessID,
  a.SourceProcessName AS GrandParentProcessName,
  a.DeviceCustomString5 AS ParentProcessID,
  a.DestinationProcessName AS ParentProcessName,
  b.DeviceCustomString5 AS ProcessID,
  b.DestinationProcessName AS ProcessName,
  concat(a.SourceProcessName, ' -> ', a.DestinationProcessName, ' -> ', b.DestinationProcessName) AS
ProcessTree
FROM `events` AS a
INNER JOIN
```

```
(
  SELECT *
  FROM `events`
  WHERE DeviceEventClassID='4688'
) AS b
ON a.DeviceCustomString5 = b.DeviceCustomString3
WHERE DeviceEventClassID='4688'
```

GrandParentProcessID	0x374
GrandParentProcessName	C:\Windows\System32\svchost.exe
HostName	pc-5.demo.lab
ParentProcessID	0x2d94
ParentProcessName	C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.17763.164_none_7e114a3d4d0589d4\TiWorker.exe
ProcessID	0x1160
ProcessName	C:\Windows\System32\conhost.exe
ProcessTree	C:\Windows\System32\svchost.exe -> C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.17763.164_none_7e114a3d4d0589d4\TiWorker.exe -> C:\Windows\System32\conhost.exe
UserName	john

Среднее время сессии Windows пользователей за 24 часа

Рассматривается запрос на основе событий Windows по пользователям (DestinationUserName) событиям входа (EventID 4624) и выхода (EventID 4634) с расчетом среднего времени сессии пользователя за последние 24 часа

```
SELECT
  login_events.DestinationUserName AS destination_user_name,
  round(AVG(logout_events.logout_time - login_events.login_time)/1000) AS avg_time_diff_s,
  COUNT(DISTINCT login_events.login_time) AS total_logins,
  COUNT(DISTINCT logout_events.logout_time) AS total_logouts,
  concat(
    toString(floor(avg_time_diff_s / 86400)), ' days, ',
    toString(floor((avg_time_diff_s % 86400) / 3600)), ' hours, ',
    toString(floor((avg_time_diff_s % 3600) / 60)), ' minutes, ',
    toString(avg_time_diff_s % 60), ' seconds'
```

```

        ) AS human_readable_diff
FROM
    (SELECT
        DestinationUserName,
        toUnixTimestamp(EndTime) AS login_time,
        FlexString1 AS logon_id
    FROM `events`
    WHERE DeviceEventClassID = '4624'
    AND EndTime >= now('Europe/Moscow') - INTERVAL 24 HOUR
    AND DestinationUserName NOT LIKE '%$%') AS login_events
INNER JOIN
    (SELECT
        DestinationUserName,
        toUnixTimestamp(EndTime) AS logout_time,
        FlexString1 AS logon_id
    FROM `events`
    WHERE DeviceEventClassID = '4634'
    AND EndTime >= now('Europe/Moscow') - INTERVAL 24 HOUR
    AND DestinationUserName NOT LIKE '%$%') AS logout_events

    ON login_events.DestinationUserName = logout_events.DestinationUserName
    AND logout_events.logon_id = login_events.logon_id

WHERE logout_events.logout_time >= login_events.login_time
GROUP BY login_events.DestinationUserName
ORDER BY avg_time_diff_s DESC
LIMIT 100

```

Несмотря на ошибку запрос выполняется корректно:

```
28 ....AND EndTime>=now()-INTERVAL 24 HOUR
29 ....AND DestinationUserName NOT LIKE '%$%' ) AS Logout_events
30 #
31 ....ON login_events.DestinationUserName = logout_events.DestinationUserName
32 ....AND logout_events.login_id = login_events.login_id
33 #
34 WHERE logout_events.logout_time >= login_events.login_time
35 GROUP BY login_events.DestinationUserName
36 ORDER BY avg_time_diff_s DESC
37 LIMIT 100
```

Code: 47. DB-Exception: Missing columns: 'avg_time_diff_s' 'Timestamp' while processing query
Нажмите Ctrl + Enter, чтобы выполнить запрос

Вернуться к исходному запросу

Выполнить запрос

Группы (16)

TSV

Поиск по полям группы...

destination_user_name	avg_time_diff_s	total_logins	total_logouts	human_readable_diff
osepov	35102	1	1	0 days, 9 hours, 45 minutes, 2 seconds
sedn	24	70	70	0 days, 0 hours, 0 minutes, 24 seconds
pavlenko	22	73	73	0 days, 0 hours, 0 minutes, 22 seconds
gruzinov	21	215	212	0 days, 0 hours, 0 minutes, 21 seconds
zhukovsky	20	77	77	0 days, 0 hours, 0 minutes, 20 seconds

События группы

Поиск по локальным событиям...

Timestamp

DeviceEventClass

Выполните запрос...

Частота и отношение неуспешных входов к успешным в Windows

```
SELECT
count(CASE WHEN DeviceEventClassID = '4625' THEN 1 END) as `Failed logins`,
count(CASE WHEN DeviceEventClassID = '4624' THEN 1 END) as `Success logins`,
`Failed logins` / `Success logins` as `Ratio`
FROM 'events'
HAVING `Ratio` > 0.03
```

Или

```
SELECT countIf(DeviceEventClassID = '4625') as F, countIf(DeviceEventClassID = '4624') as S
FROM 'events'
LIMIT 250
```

```
1 SELECT count(CASE WHEN DeviceEventClassID = '4625' THEN 1 END) as 'Failed logins', count(CASE WHEN DeviceEventClassID = '4624' THEN 1 END) as 'Success logins', 'Failed logins' / 'Success logins' as 'Ratio'
2 FROM 'events'
3 HAVING 'Ratio' > 0.03
```

Нажмите Ctrl + Enter, чтобы выполнить запрос

Выполнить запрос

Результаты запроса

TSV

Failed logins	Success logins	Ratio
24	545	0.044036697247706424

Работа с кастомными полями (SA. NA.)

Вхождение элемента по полю

Поиск происходит по точному совпадению с элементом

```
SELECT *
FROM `events`
WHERE has(SA.user_groups, 'system:serviceaccounts')
ORDER BY Timestamp DESC LIMIT 250
```

События

Не обновлять

1д Послед

1 SELECT * FROM `events` WHERE has(SA.user_groups, 'system:serviceaccounts') ORDER BY Timestamp DESC LIMIT 250

Нажмите Ctrl + Enter, чтобы выполнить запрос

TSV

DeviceProduct	DeviceCustomString1	SA.user_groups
Kubernetes	ord.projectcalico.org/v1	system:serviceaccounts,system:serviceaccounts:kube-system,system:authenticated
Kubernetes	/	system:serviceaccounts,system:serviceaccounts:kube-system,system:authenticated
Kubernetes	ord.projectcalico.org/v1	system:serviceaccounts,system:serviceaccounts:kube-system,system:authenticated
Kubernetes	/	system:serviceaccounts,system:serviceaccounts:kube-system,system:authenticated
Kubernetes	ord.projectcalico.org/v1	system:serviceaccounts,system:serviceaccounts:kube-system,system:authenticated

Вхождение по подстроке элемента по полю (где более 2 значений в массиве)

Счет в массиве начинается с нуля

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

WHERE length(arrayFilter(x -> x LIKE '%serviceaccounts%', SA.user_groups)) > 1
ORDER BY Timestamp DESC LIMIT 250

События

Не обновлять

1д Последние 24ч

1 SELECT * FROM `events` WHERE length(arrayFilter(x -> x LIKE '%serviceaccounts%', SA.user_groups)) > 1 ORDER BY Timestamp DESC LIMIT 250

Нажмите Ctrl + Enter, чтобы выполнить запрос

TSV

DeviceProduct	DeviceCustomString1	SA.user_groups
Kubernetes	ord.projectcalico.org/v1	system:serviceaccounts,system:serviceaccounts:kube-system,system:authenticated
Kubernetes	ord.projectcalico.org/v1	system:serviceaccounts,system:serviceaccounts:kube-system,system:authenticated
Kubernetes	/	system:serviceaccounts,system:serviceaccounts:kube-system,system:authenticated
Kubernetes	ord.projectcalico.org/v1	system:serviceaccounts,system:serviceaccounts:kube-system,system:authenticated
Kubernetes	ord.projectcalico.org/v1	system:serviceaccounts,system:serviceaccounts:kube-system,system:authenticated

Revision #38
Created 10 August 2023 11:21:22 by Boris RZR
Updated 31 March 2025 14:11:09 by Boris RZR