

KSC MariaDB

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и НЕ является официальной рекомендацией вендора.

Настройка MariaDB

В **MariaDB** настройки на сервере базы данных можно выполнять несколькими способами: через консоль (SSH, терминал ОС) или с помощью графических интерфейсов, таких как **phpMyAdmin** или **MySQL Workbench**

В данной статье сервер БД MariaDB работает под управлением ОС Ubuntu 22.04.5, а все настройки выполняются **в консоли**.

Для удобства в базе данных MariaDB Kaspersky Security Center предусмотрен набор публичных представлений. Таким образом можно создавать запросы непосредственно к публичным представлениям и извлекать из них данные о событиях. "Коробочный" коннектор KUMA **[OOTB] KSC MySQL** содержит уже готовые запросы к публичным представлениям **v_akpub_ev_event** и **v_akpub_host**.

Для обеспечения корректной работы MariaDB с Kaspersky Security Center рекомендуется использовать версии MariaDB начиная с 10.5.17 или более новые.

Проверка имени БД KSC

Чтобы проверить имя базы данных KSC можно воспользоваться следующей статьей:

Просмотр имени базы данных Kaspersky Security Center Linux - (KSC Linux) -

<https://support.kaspersky.ru/ksc-linux/15.1/228689>

Альтернативным вариантом является проверка имени БД в консоли сервера, на котором установлена БД KSC:

- Подключитесь к серверу базы данных

```
mariadb -h localhost -u admin -p
```

где, вместо `admin` задайте логин своего пользователя MariaDB

- Запустите интерактивный терминал MariaDB и выведите список баз данных сервера

```
SHOW DATABASES;
```

```
MariaDB [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| KAV      |
| information_schema |
| mysql    |
| performance_schema |
| sys      |
+-----+
5 rows in set (0.001 sec)
```

Создание роли БД и предоставление прав

- Подключитесь к серверу базы данных

```
mariadb -h localhost -u admin -p
```

- Создайте роль пользователя для сбора событий, в данном примере - `kuma_siem`

```
CREATE USER kuma_siem IDENTIFIED BY 'password';
```

- Предоставьте права роли KUMA к публичным представлениям:

```
GRANT SELECT ON `KAV`.`v_akpub_hst_prdstate` TO `kuma_siem`@`%`;
GRANT SELECT ON `KAV`.`v_akpub_ev_event` TO `kuma_siem`@`%`;
GRANT SELECT ON `KAV`.`v_akpub_host_status` TO `kuma_siem`@`%`;
GRANT SELECT ON `KAV`.`v_akpub_virus_activity` TO `kuma_siem`@`%`;
GRANT SELECT ON `KAV`.`v_akpub_host` TO `kuma_siem`@`%`;
```

Права предоставляются в виде:

```
GRANT SELECT ON `название базы данных`.`таблица` TO `имя пользователя БД`@`хост с
которого идет подключение`;
# % - все хосты
```

- Проверьте права пользователя

```
SHOW GRANTS FOR 'kuma_siem'@`%`;
```

```
+-----+
| Grants for kuma_siem@% |
+-----+
| GRANT USAGE ON *.* TO `kuma_siem`@`%` IDENTIFIED BY PASSWORD '*6F8F4246640BC81D824AE210AEEBE2AB20D5A7BB' |
| GRANT SELECT ON `KAV`.`v_akpub_hst_prdstate` TO `kuma_siem`@`%` |
| GRANT SELECT ON `KAV`.`v_akpub_ev_event` TO `kuma_siem`@`%` |
| GRANT SELECT ON `KAV`.`v_akpub_host_status` TO `kuma_siem`@`%` |
| GRANT SELECT ON `KAV`.`v_akpub_virus_activity` TO `kuma_siem`@`%` |
| GRANT SELECT ON `KAV`.`v_akpub_host` TO `kuma_siem`@`%` |
+-----+
```

При необходимости разрешите входящие соединения на порт БД MariaDB (по умолчанию, TCP/3306) в параметрах локального FW, а также в настройках конфигурационного файла `my.cnf`

Создание секрета KUMA

1. В веб-интерфейсе KUMA перейдите на вкладку **Ресурсы** → **Секреты** → **Добавить**

2. Создайте секрет MariaDB, В появившемся окне задайте

- URL (формат URL можно взять из **Описания** к секрету). В поле URL укажите:
 - Имя ранее созданной роли (в нашем примере это **kuma_siem**) и ее пароль;
 - Протокол подключения
 - IP-адрес или FQDN сервера БД ;
 - Порт подключения (по умолчанию `3306`)
 - Наименование БД KSC (по умолчанию `KAV`). См. **Проверка имени БД KSC**).

```
mysql://<имя пользователя БД>:<Пароль>@<протокол подключения>(<IP-адрес или FQDN сервера БД>:<порт>)/<имя Базы данных>
```

Например: `mysql://kuma_siem:password@tcp(10.10.10.10:3306)/KAV`

Если в пароле используются спецсимволы необходимо перевести данные спецсимволы в URL формат в соответствии с таблицей ниже.

Примеры

```
mysql://kuma:p%40ssword123%2@tcp(ip:port)/KAV
```

!	#	\$	%	&	'	()	*	+
%21	%23	%24	%25	%26	%27	%28	%29	%2A	%2B
,	/	:	;	=	?	@	[]	\
%2C	%2F	%3A	%3B	%3D	%3F	%40	%5B	%5D	%5C

Можно использовать следующий ресурс для преобразования <https://www.urlencoder.org/>

3. Нажмите **Сохранить**

Обратите внимание, после сохранения секрета поле URL будет пустым во избежание утечки чувствительной информации.

Настройка коннектора

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Коннекторы**
2. В списке коннекторов найдите коннектор **[OOTB] KSC MySQL**, отметьте его галочкой и нажмите **Дублировать**
3. В появившемся окне задайте:
 - Название коннектора
 - На вкладке **Основные параметры** в разделе **Соединение** в выпадающих списках URL выберите секрет, созданный ранее для подключения к БД MariaDB KSC

Обратите внимание, что в коннекторе используется несколько запросов! URL подключения необходимо заменить для **ВСЕХ** запросов.

4. В запросе смените название БД (`ksc_srv`) на имя БД KSC, в нашем случае `KAV` (по умолчанию)

Редактирование коннектора

Основные параметры

Дополнительные параметры

Столбец идентификатора*

infoUpdate

Начальное значение
идентификатора*

2023-01-01T00:00:00.000

Запрос ⓘ

```
....CAST(serv.nIp·%·256·AS·CHAR)·AS·kscIP,␣  
....(serv.wstrDnsName+'·'+serv.wstrDnsDomain)·as·kscHost␣  
.....␣  
FROM KAV.v_akpub_host as host␣  
....Inner·Join·KAV.v_akpub_hst_pidstate as state on state  
  .nHost = host.nId␣  
....Inner·Join·KAV.v_akpub_host_status as status on state  
  .nHost = status.nId␣  
....Inner·Join·KAV.v_akpub_host as serv on serv.nId = 1␣  
WHERE␣  
....state.tmAvbasesDate is NOT NULL␣  
....AND·host.tmLastNagentConnected >= TIMESTAMPADD(hour, -4  
  , NOW(3))␣  
....OR·host.tmLastInfoUpdate >= ?␣  
ORDER BY host.tmLastInfoUpdate
```

Интервал запросов, сек.

0

Редактирование коннектора

Основные параметры

Дополнительные параметры

Тип* ⓘ

sql

Запрос по умолчанию*

```
.....ELSE·ev.tmRegistrationTime␣  
.....END␣  
.....AS·virusTime,␣  
....virus.wstrObject·As·filePath,␣  
....virus.wstrVirusName·as·virusName,␣  
....virus.result_ev·as·result␣  
FROM KAV.v_akpub_ev_event as ev␣  
....LEFT·JOIN·KAV.v_akpub_host as hs ON ev.nHostId =  
  hs.nId␣  
.....INNER·JOIN·KAV.v_akpub_host as serv ON serv.nId =  
  1␣  
....Left·Join·KAV.v_akpub_virus_activity as virus on  
  ev.nId = virus.nEventVirus␣  
WHERE·ev.nId > ?␣  
ORDER BY ev.nId
```

Обратите внимание, что в коннекторе используется несколько запросов! Название БД необходимо заменить для **ВСЕХ** запросов.

Настройка коллектора

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** и нажмите **Подключить источник**
2. В появившемся окне задайте **Название коллектора** и **Тенант**
3. На шаге **Транспорт** выберите ранее созданный коннектор
4. На шаге **Парсинг событий** выберите сдублированный нормализатор **[OOTB] KSC from SQL**.
5. На шаге **Маршрутизация** задайте следующие точки назначения:
 - **Хранилище**. Для отправки обработанных событий в хранилище.
 - **Коррелятор**. Для отправки обработанных событий в коррелятор.
6. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.
7. Скопируйте появившуюся команду и выполните установку сервиса коллектора.

Проверка поступления событий KSC в KUMA

Для проверки, что экспорт событий из БД KSC успешно настроен, перейдите в **Ресурсы -> Активные сервисы ->** выберите ранее созданный коллектор **KSC PostgreSQL** и нажмите **Перейти к событиям**

В открывшемся окне **События** убедитесь, что присутствуют события KSC.

События



SELECT * FROM `events` WHERE ServiceID = '08d27e3e-6b3c-4445-b505-bf481045dd6d' ORDER BY Timestamp DESC LIMIT 250

TenantID	Timestamp ↓	Name	DeviceProduct	DeviceVendor	DeviceEventCategory
Main	09.01.2024 13:23:47	Application_Control	KSC	Kaspersky	Запуск приложения заблокирован в тестовом режиме
Main	09.01.2024 13:23:47	Application_Control	KSC	Kaspersky	Запуск приложения заблокирован в тестовом режиме
Main	09.01.2024 13:23:07	Application_Control	KSC	Kaspersky	Запуск приложения заблокирован в тестовом режиме
Main	09.01.2024 13:23:07	Application_Control	KSC	Kaspersky	Запуск приложения заблокирован в тестовом режиме

Полезные ссылки

Настройка сервера MariaDB x64 для работы с Kaspersky Security Center Linux - <https://support.kaspersky.ru/ksc-linux/15/210277>

Коннекторы типа sql в kuma - <https://support.kaspersky.ru/kuma/3.2/220746>

Revision #11
Created 26 November 2024 08:29:07 by Kortik
Updated 26 November 2024 13:00:06 by Boris RZR