

KSC MS SQL

✓ **Рекомендуется** - Рекомендуемый способ сбора для этого источника событий

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

Официальная документация по данному разделу приведена в Онлайн-справке на продукт: <https://support.kaspersky.com/KUMA/2.1/ru-RU/245386.htm>

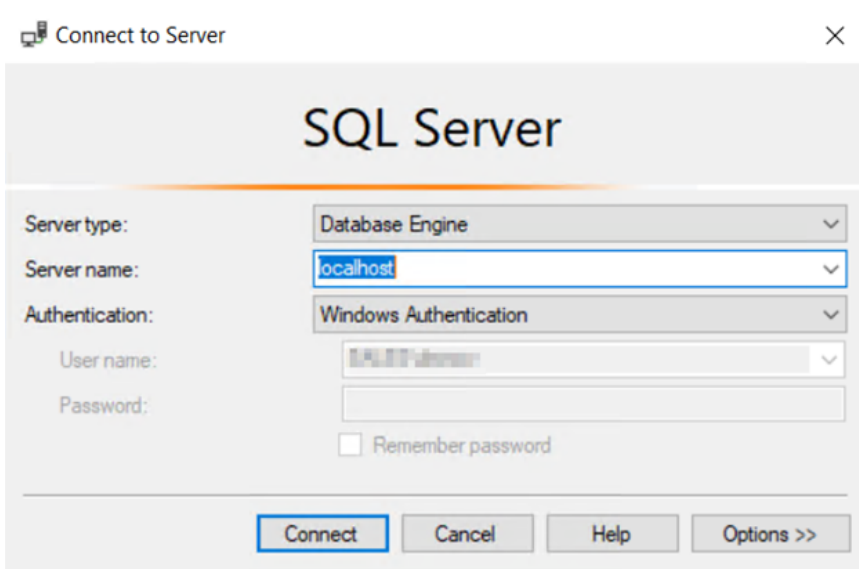
SQL Server должен поддерживать TLS 1.2 - дополнительную информацию можно изучить тут: <https://support.microsoft.com/en-us/help/3135244/tls-1-2-support-for-microsoft-sql-server>

<https://www.youtube.com/embed/pTv5ALONDQw?si=Mzunu5F7gghO4NWQ>

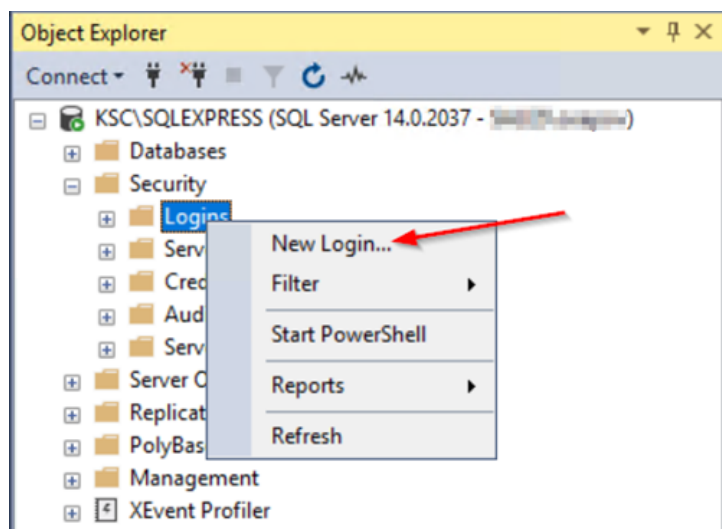
Настройка БД MS SQL

Для сбора событий из БД MS SQL необходимо создать учетную запись с соответствующими правами. Для этого выполните следующие действия:

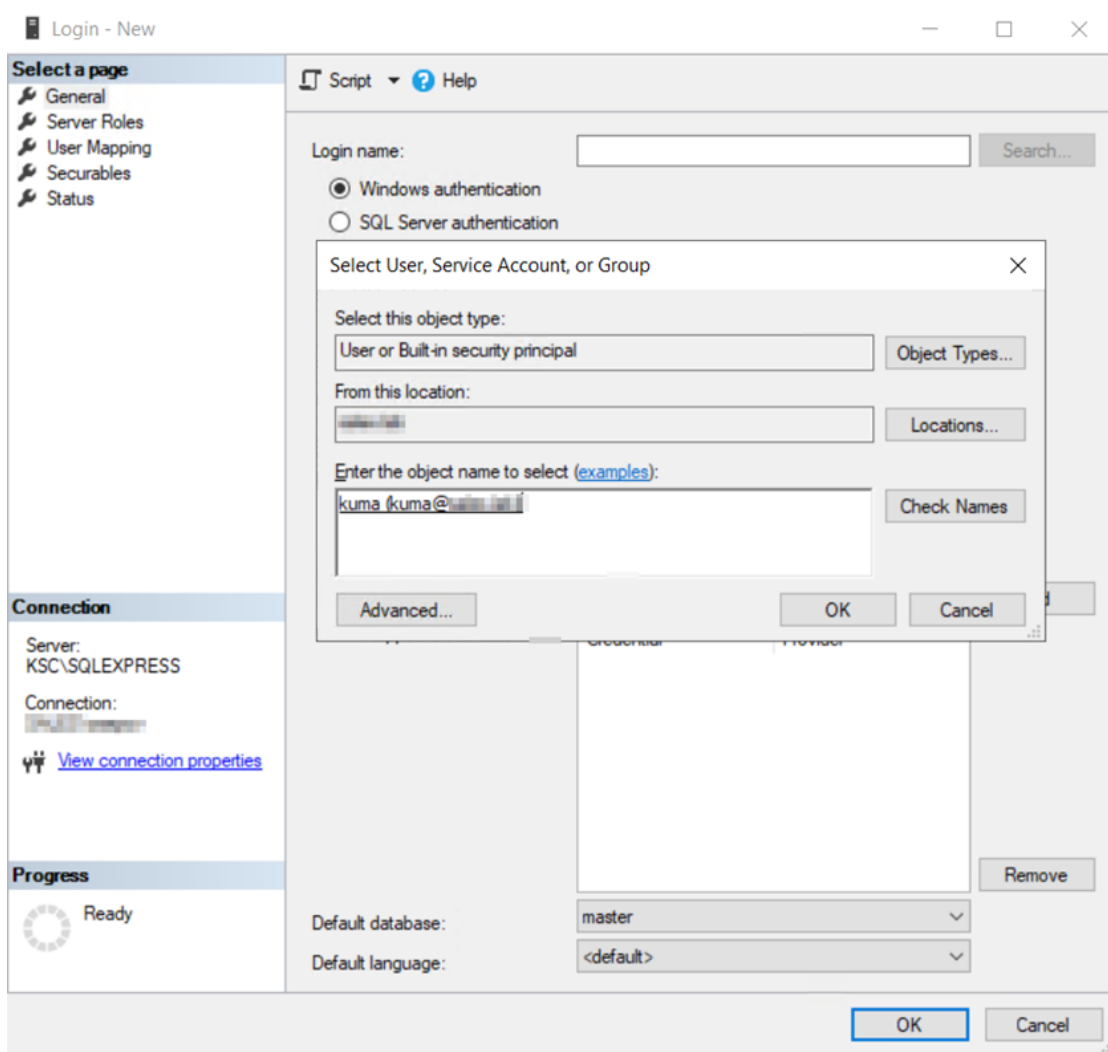
1. Перейдите на сервер, где установлена БД MS SQL для KSC. С помощью Microsoft SQL Server Management Studio подключитесь к БД из-под учетной записи, обладающей правами администратора в БД.



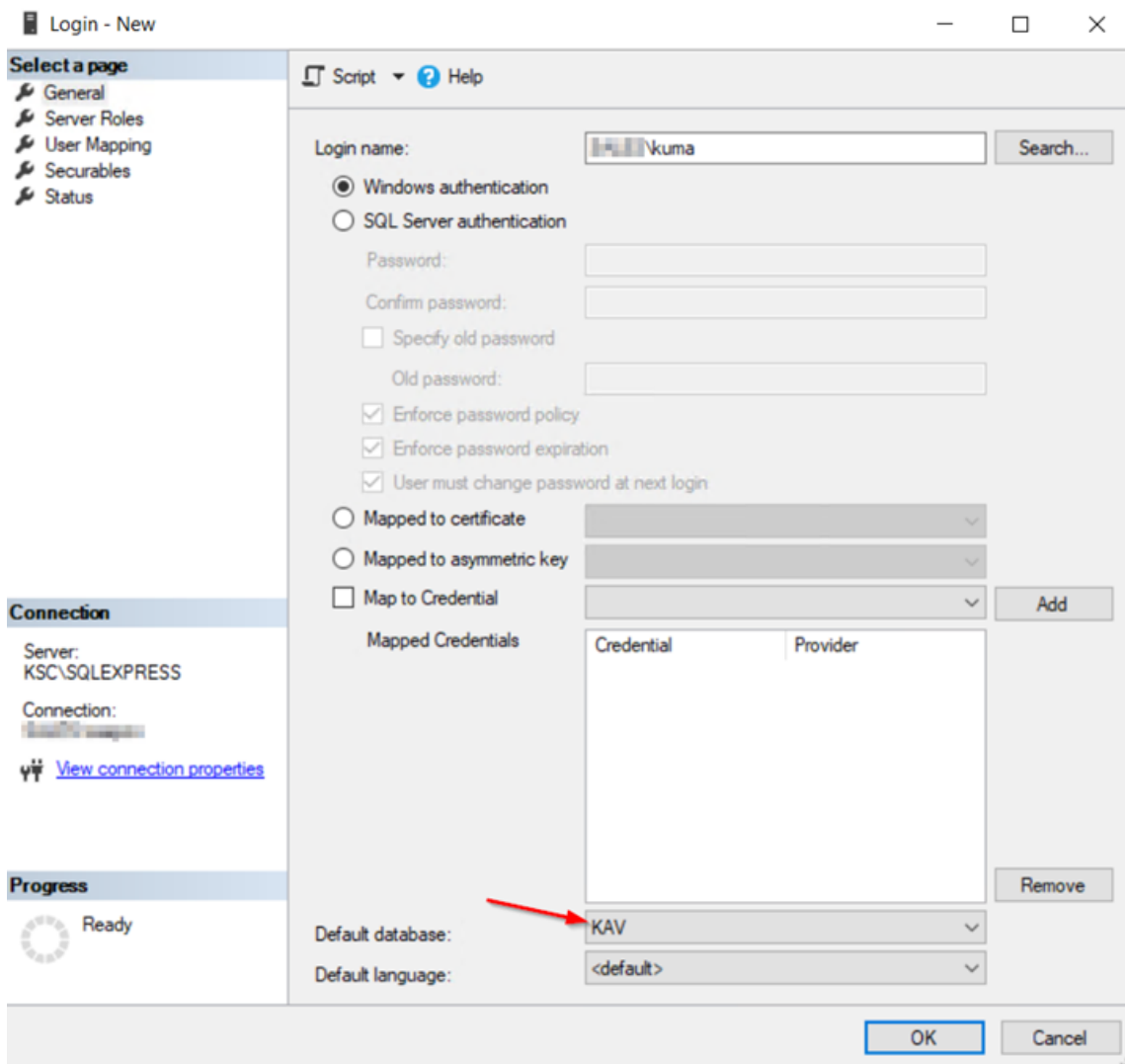
2. Перейдите в соответствующий экземпляр БД MS SQL на вкладку Security и для вкладки Logins выберите New Login...



3. Добавьте учетную запись пользователя, с помощью которой будет осуществляться доступ к БД KSC



4. Установите для учетной записи БД KSC в качестве БД по умолчанию (по умолчанию в KSC используется БД KAV).



5. Настройте учетной записи права db_datareader и public для БД KSC в соответствии с изображением ниже.

Login - New

Select a page

General

Server Roles


User Mapping


Securables

Status


Connection

Server:
KSC\SQLEXPRESS

Connection:




 [View connection properties](#)

Progress

 Ready

Script ? Help

Users mapped to this login:

Map	Database	User	Default Schema
<input checked="" type="checkbox"/>	KAV	 kuma	
<input type="checkbox"/>	master		
<input type="checkbox"/>	model		
<input type="checkbox"/>	msdb		
<input type="checkbox"/>	tempdb		

☐ Guest account enabled for: KAV

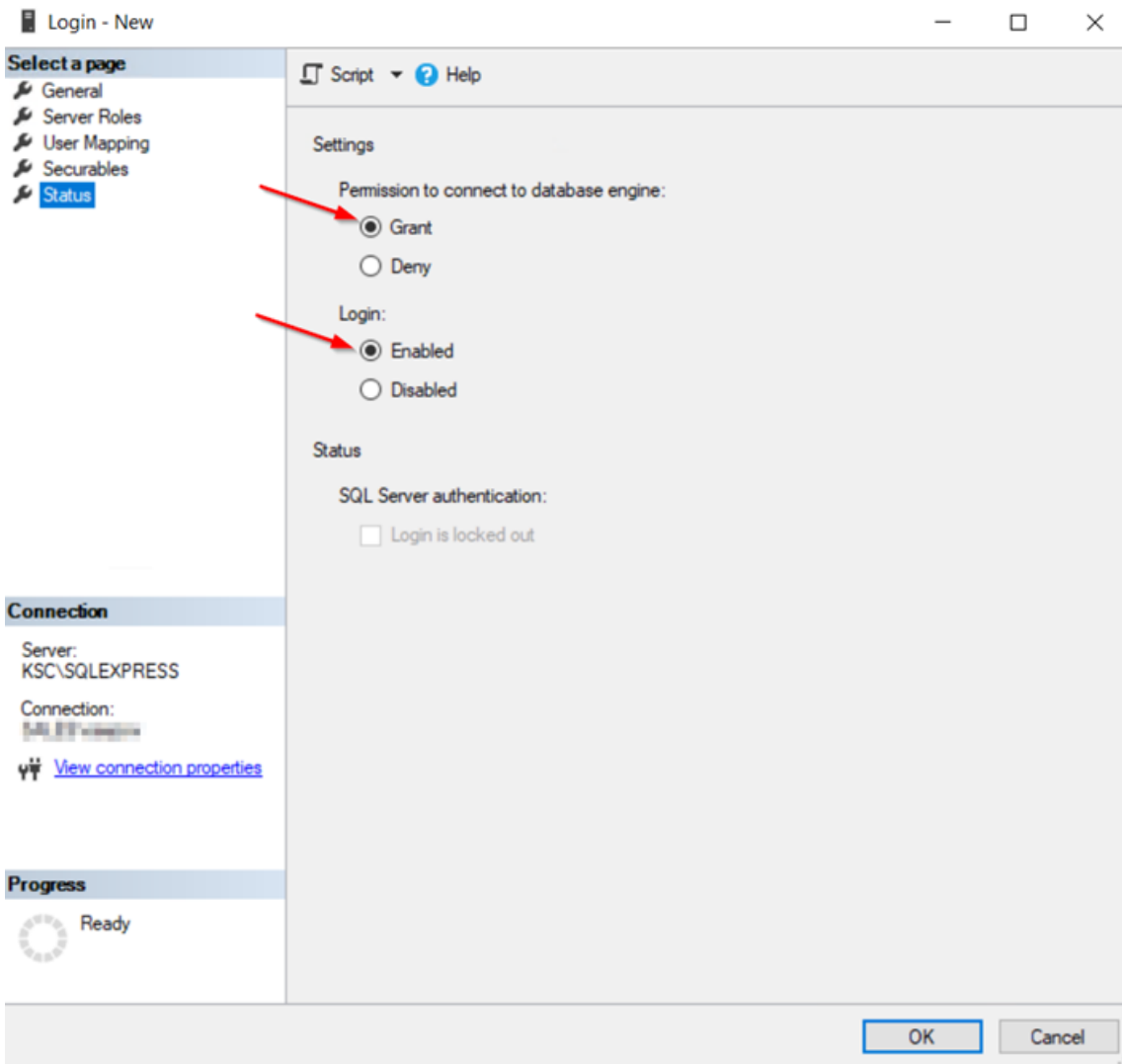
Database role membership for: KAV

<input type="checkbox"/>	db_accessadmin
<input type="checkbox"/>	db_backupoperator
<input checked="" type="checkbox"/>	db_datareader
<input type="checkbox"/>	db_datawriter
<input type="checkbox"/>	db_ddladmin
<input type="checkbox"/>	db_denydatareader
<input type="checkbox"/>	db_denydatawriter
<input type="checkbox"/>	db_owner
<input type="checkbox"/>	db_securityadmin
<input checked="" type="checkbox"/>	public

OK

Cancel

6. Убедитесь, что созданной учетной записи разрешено подключение к БД.



Для проверки прав созданной учетной записи можно запустить Microsoft SQL Management Studio от имени созданного пользователя (с зажатым Shift нажать ПКМ и выбрать Запуск от имени другого пользователя). Затем перейти в любую таблицу БД KSC и сделать выборку по этой таблице.

Настройка SQL Server Browser

Для подключения к серверу MS SQL для сбора событий необходимо настроить соответствующую службу и разрешить входящие подключения. Для этого выполните следующие действия:

1. Откройте оснастку SQL Server Configuration Manager. Запустите службу SQL Server Browser и задайте автоматический запуск службы.

SQL Server Configuration Manager

File Action View Help

SQL Server Configuration Manager (Local)

- SQL Server Services
 - SQL Server Network Configuration (32bit)
 - SQL Native Client 11.0 Configuration (32b
 - SQL Server Network Configuration
 - Protocols for SQLEXPRESS
 - SQL Native Client 11.0 Configuration

Name	State	Start Mode	Log On As	Process ID	Service Type
SQL Server (SQLE...	Running	Automatic	NT Service\MSSQL\$...	4404	SQL Server
SQL Server Agent ...	Stopped	Automatic	NT AUTHORITY\NET...	0	SQL Agent
SQL Server Browser	Running	Automatic	NT AUTHORITY\LOC...	3728	

SQL Server Browser Properties

Log On Service Advanced

Log on as:

☒ Built-in account:
Local Service

☐ This account:
Account Name: Browse
Password:
Confirm password:

Service status: Running

Start Stop Pause Restart

OK Cancel Apply Help

SQL Server Browser Properties

Log On Service Advanced

General

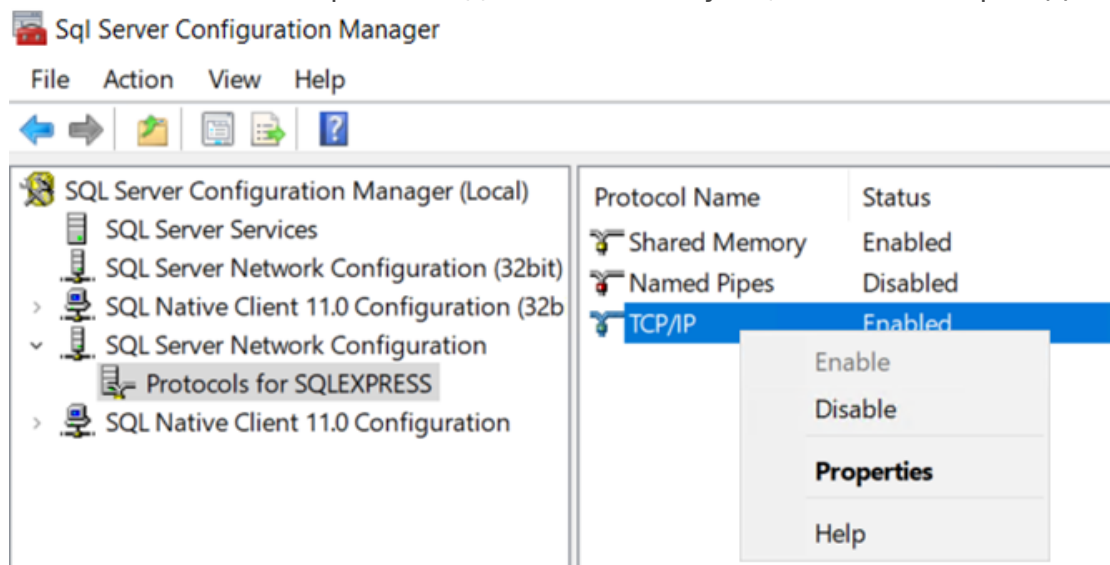
Binary Path	"C:\Program Files (x86)\Microsoft SQL
Error Control	1
Exit Code	0
Host Name	KSC
Name	SQL Server Browser
Process ID	3728
SQL Service Type	
Start Mode	Automatic
State	Running

Start Mode

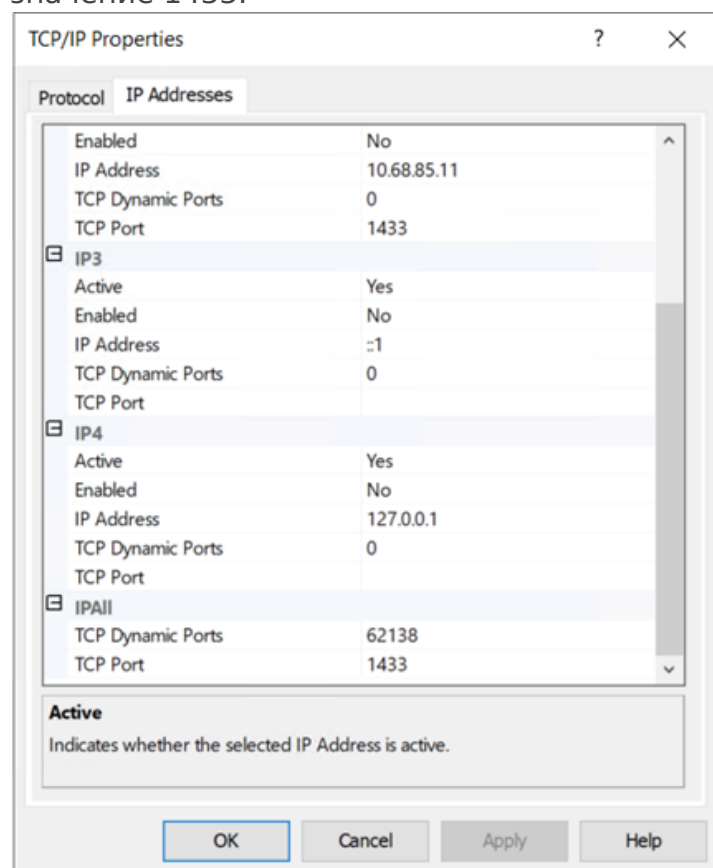
The start mode of this service.

OK Cancel Apply Help

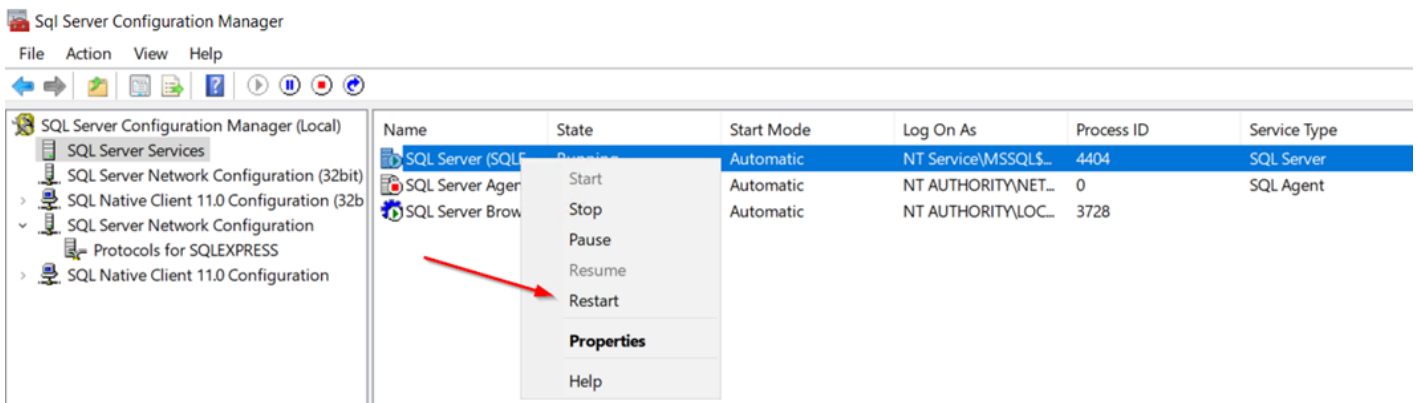
2. Включите TCP/IP протокол для соответствующего экземпляра БД.



3. В свойствах протокола, на вкладке IP Addresses для поля IPALL в TCP Port укажите значение 1433.



4. Перезапустите службу экземпляра SQL сервера.



5. Разрешите на сервере входящие подключения по порту 1433. Это можно сделать в оснастке Брандмауэр защитника Windows в режиме повышенной безопасности.

Inbound Rules										
Name	G.	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port
Allow inbound MSSQL Connection		All	Yes	Allow	No	Any	Any	Any	TCP	1433

Создание секрета KUMA

Для подключения к БД MS SQL со стороны KUMA необходимо создать строку подключения. Для этого выполните следующие действия:

1. В веб-интерфейсе KUMA перейдите на вкладку **Ресурсы → Секреты** и нажмите на кнопку **Добавить секрет**.
2. Укажите **Имя** секрета, выберите **Тенант**, к которому будет относиться создаваемый секрет.
3. Задайте секрету тип **urls** и в поле **URL** укажите строку вида:
sqlserver://[<domain>%5C]<username>:<password>@<server>:1433/KAV

Примеры

sqlserver://test.local%5Cuser:password123!@10.0.0.1:1433/KAV

sqlserver://user:password123!@server.demo.lab:1433/KAV

%5C – используется для разделения домена и пользователя и представляет собой знак \ в URL-формате.

Если в пароле пользователя используются спецсимволы их также необходимо перевести в URL формат в соответствии с таблицей ниже.

!	#	\$	%	&	'	()	*	+
%21	%23	%24	%25	%26	%27	%28	%29	%2A	%2B

,	/	:	;	=	?	@	[]	\
%2C	Encode to URL-encoded format Simply enter your data then push the encode button.								%5C

Можно и [r.org/](#)

Encode to URL-encoded format

To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Destination character set.

LF (Unix) Destination newline separator.

☐ Encode each line separately (useful for when you have multiple entries).

☐ Split lines into 76 character wide chunks (useful for MIME).

☒ Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character set).

> ENCODE < Encodes your data into the area below.

P%40%24%24w0d

пример:

4. Сохраните созданный секрет.

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

Настройка коннектора

1. Для подключения к БД MS SQL необходимо настроить коннектор. Для этого выполните следующие действия
2. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы → Коннекторы**.
3. В списке коннекторов справа найдите коннектор **[OOTB] KSC SQL** и откройте его для редактирования.

Что делать, если ресурс не доступен для редактирования

Начиная с версии KUMA 2.1 OOTB ресурсы недоступны для редактирования. В таком случае необходимо скопировать OOTB-ресурс и произвести редактирование в копии этого ресурса.

Важно! При копировании OOTB ресурса, копируется и становится доступным для редактирования только сам ресурс. Связанные ресурсы нужно копировать и привязывать отдельно.

4. На вкладке **Основные параметры** в выпадающих списках **URL** выберите секрет, созданный для подключения к БД MS SQL.

5. Нажмите **Сохранить**.

Настройка коллектора

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Коллекторы**.

2. В списке коллекторов найдите коллектор с нормализатором **[OOTB] KSC from SQL** и откройте его для редактирования.

Что делать, если ресурс не доступен для редактирования

Начиная с версии KUMA 2.1 OOTB ресурсы недоступны для редактирования. В таком случае необходимо скопировать OOTB-ресурс и произвести редактирование в копии этого ресурса.

Важно! При копировании OOTB ресурса, копируется и становится доступным для редактирования только сам ресурс. Связанные ресурсы нужно копировать и привязывать отдельно.

3. На шаге **Транспорт** выберите коннектор **[OOTB] KSC SQL**

4. На шаге Парсинг событий проверьте, что выбран нормализатор **[OOTB] KSC from SQL**.

6. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:

- **Хранилище.** Для отправки обработанных событий в хранилище.
- **Коррелятор.** Для отправки обработанных событий в коррелятор.

Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

7. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

8. Скопируйте появившуюся команду для установки коллектора KUMA.

Альтернативный вариант создания коллектора

В случае, если предполагается использование коробочных ресурсов без изменений:

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы → Секреты**
2. Откройте на редактирование секрет **[OOTB] KSC MSSQL connection**
3. Задайте в секрете строку подключения в соответствии с разделом "**Создание секрета KUMA**"
4. Сохраните созданный секрет с помощью кнопки "**Сохранить**"
5. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы → Коллекторы**.
6. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:
 - **Хранилище.** Для отправки обработанных событий в хранилище.
 - **Коррелятор.** Для отправки обработанных событий в коррелятор.

Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

7. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

8. Скопируйте появившуюся команду для установки коллектора KUMA.

Revision #21

Created 9 August 2023 11:04:03 by Admin

Updated 19 September 2024 10:10:52 by Boris RZR