

1С

- 1С:Предприятие (новые версии)
- Пересылка многострочных XML-файлов 1С с помощью Linux-агента
- 1С Битрикс (Bitrix) интеграция с KUMA

1С:Предприятие (новые версии)

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

Инструкция на примере версии 8.3

Настройки на стороне 1С

Конфигурация 1С выполняется от учетной записи, с правами локального администратора Windows.

Выгрузка журнала регистрации информационной базы в локальную папку (JSON)

1. Запустите **1С:Предприятие**.
2. Выберите в списке информационную базу и нажмите кнопку 1С:Предприятие, затем введите данные учетной записи администратора и нажмите кнопку **Войти**.
3. В левой части окна нажмите **НСИ и администрирование**.
4. Откройте вкладку **Печатные формы, отчеты и обработки**.
5. Если не установлен флажок **Дополнительные отчеты и обработки**, установите его.
6. Откройте вкладку **Дополнительные отчеты и обработки**.
7. В панели инструментов вкладки нажмите кнопку **Добавить из файла**, затем в окне проводника **Выберите файл внешнего отчета или обработки**. Скачать архив [registration_log_json_upload.zip](#) со сценарием для внешней обработки.
8. Выберите файл и нажмите кнопку **Открыть**. Откроется вкладка дополнительная обработка (создание).

9. В панели инструментов вкладки **нажмите Значок сохранить**.
10. На вкладке **Команды** выберите строку **Выгрузка журнала регистрации в формате JSON**.
11. Нажмите кнопку **Выполнить**. Откроется вкладка Выгрузка журнала регистрации в формате JSON.
12. В поле директория для хранения файлов введите путь для сохранения файлов журнала регистрации, например `C:\1C_Журнал`.
13. В поле **Интервал выгрузки в минутах** введите количество минут, за которые события журнала регистрации будут выгружаться в отдельный файл, рекомендуется `15` минут.
14. В поле **Дата выгрузки** выберите дату, с которой начнется выгрузка журнала регистрации.
15. Нажмите кнопку **Сохранить настройки** и подтвердите сохранение.
16. Закройте вкладку Выгрузка журнала регистрации в формате JSON.
17. На вкладке **Команды** в строке **Выгрузка журнала регистрации в формате JSON** установите **флажок**. Откроется окно **Расписание**.
18. Выберите вкладку **Дневное** и в поле **Повторять через** введите `900` (количество секунд в 15 минутах). Время начала и окончания оставьте без изменений (пустым). Нажмите кнопку **ОК**.
19. На вкладке **Команды** в строке **Удаление старых файлов** установите **флажок**. Откроется окно **Расписание**.
20. Выберите вкладку **Общие** и в поле **Повторять каждые** введите `1`. Нажмите кнопку **ОК**.
21. Нажмите кнопку **Записать и закрыть**.

Должно получиться следующее:

← → ☆ **Выгрузка журнала регистрации в формате JSON (Дополнительная обработка)**

Записать и закрыть Обновить из файла... Сохранить как...

Наименование: Режим работы: Не безопасный ?

Публикация: Используется Режим отладки Отключена

Команды (3) Дополнительная информация

Размещение: [Не определено](#)

▶ Выполнить

Наименование	Быстрый доступ		Расписание
Выгрузка журнала регистрации в формате JSON	Нет	<input checked="" type="checkbox"/>	с 24 ноября 2023 г. каждый день; каждые 900 секунд
Удаление старых файлов	Нет	<input checked="" type="checkbox"/>	с 28 ноября 2023 г. каждый день; один раз в день

Настройка журналирования событий технологического журнала

Чтобы настроить журналирование событий технологического журнала на сервере «1С:Предприятия»:

1. Создайте конфигурационный файл `logcfg.xml`. Если вы используете Windows — в папке `<Папка установки "1С:Предприятия">\bin\conf`.
2. Добавьте в файл служебные строки:
3.

```
<?xml version="1.0" encoding="UTF-8"?>
<config xmlns="http://v8.1c.ru/v8/tech-log">
</config>
```
4. Добавьте в файл в элемент `<config>` строки с указанием пути для сохранения файлов журнала и времени хранения событий (в часах). Если вы используете Windows, укажите путь к общей папке:
5.

```
<log location="<Путь к общей папке>" history="168">
<property name="all"></property>
</log>
```
6. Добавьте в файл в элемент `<log>` строки с фильтрами событий из подпунктов ниже, затем **Сохраните** конфигурационный файл.
7. Настройте общий доступ к папкам с файлами журналов (сетевую файловую шару).

Фильтры по типам событий

- Успешная или неуспешная авторизация через толстый клиент, конфигуратор или COM-соединение

```
<event>
  <eq property="name" value="CALL"/>
  <eq property="MName" value="authenticateServer"/>
</event>
```

- Успешная авторизация через толстый клиент

```
<event>
  <eq property="name" value="SCALL"/>
  <eq property="MName" value="setSessionData"/>
  <eq property="t:applicationName" value="1CV8C"/>
</event>
```

- Ошибка авторизации через тонкий клиент

```
<event>
  <eq property="name" value="EXCP"/>
  <eq property="t:applicationName" value="1CV8C"/>
  <like property="Descr" value="%VResourceInfoBaseServerImpl.cpp%"/>
</event>
```

- Ошибка авторизации через веб-клиент

```
<event>
  <eq property="name" value="EXCP"/>
  <eq property="t:applicationName" value="WebServerExtension"/>
  <like property="Descr" value="%VResourceInfoBaseServerImpl.cpp%"/>
</event>
```

- Успешная авторизация через веб-клиент

```
<event>
  <eq property="name" value="SCALL"/>
  <eq property="t:applicationName" value="WebServerExtension"/>
  <eq property="MName" value="setSessionData"/>
  <ne property="Usr" value="DefUser"/>
</event>
```

- Успешно установлено соединение с сервером «1С:предприятия»

```
<event>
  <eq property="name" value="CONN"/>
  <like property="Txt" value="Accepted%"/>
</event>
```

- Подключение к дизайнеру заблокировано другим пользователем

```
<event>
  <eq property="name" value="CALL"/>
  <eq property="MName" value="lockConfig"/>
</event>
```

- Просмотр списка пользователей, подключенных к серверу «1С:Предприятия»

```
<event>
  <eq property="name" value="CALL"/>
```

```
<eq property="MName" value="activeUsers"/>
</event>
```

- Просмотр пользователем параметров информационной базы

```
<event>
  <ea property="name" value="CALL"/>
  <eq property="MName" value="readInfoBaseAdmParams"/>
  <ne property="Usr" value=""/>
</event>
```

Пример конфигурационного файла logcfg.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<config
  xmlns="http://v8.1c.ru/v8/tech-log">
  <log location="<Путь к файлам журнала>" history="168">
    <event>
      <eq property="name" value="CALL"/>
      <eq property="MName" value="authenticateServer"/>
    </event>
    <event>
      <eq property="name" value="SCALL"/>
      <eq property="MName" value="setSessionData"/>
      <eq property="t:applicationName" value="1CV8C"/>
    </event>
    <event>
      <eq property="name" value="EXCP"/>
      <eq property="t:applicationName" value="1CV8C"/>
      <like property="Descr" value="%VResourceInfoBaseServerImpl.cpp%"/>
    </event>
    <event>
      <eq property="name" value="EXCP"/>
      <eq property="t:applicationName" value="WebServerExtension"/>
      <like property="Descr" value="%VResourceInfoBaseServerImpl.cpp%"/>
    </event>
    <event>
      <eq property="name" value="SCALL"/>
      <eq property="t:applicationName" value="WebServerExtension"/>
    </event>
  </log>
</config>
```

```

    <eq property="MName" value="setSessionData"/>
    <ne property="Usr" value="DefUser"/>
  </event>
</event>
  <eq property="name" value="CONN"/>
  <like property="Txt" value="Accepted%"/>
</event>
</event>
  <eq property="name" value="CALL"/>
  <eq property="MName" value="lockConfig"/>
</event>
</event>
  <eq property="name" value="CALL"/>
  <eq property="MName" value="activeUsers"/>
</event>
</event>
  <ea property="name" value="CALL"/>
  <eq property="MName" value="readInfoBaseAdmParams"/>
  <ne property="Usr" value=""/>
</event>
<property name="all"></property>
</log>
</config>

```

Монтирование папки к KUMA

Монтирование папки с журналом можно сделать по аналогии с [этой](#) инструкцией.

Пересылка многострочных XML-файлов 1С с помощью Linux-агента

Зачастую создание файловых информационных ресурсов на хостах компании недопустимо с точки зрения действующих требований департамента информационной безопасности. В связи с этим использование стандартного коллектора 1с-xml с возможностью вычитки события через примонтированную к серверу коллектора шару реализовать невозможно.

1. Настройка коллектора и агента KUMA для нормализации многострочных XML-файлов 1С

Конфигурация коллектора

Название поля	Значение поля	Описание
Collector name	[xml][1C] - Multiline	Название коллектора
Transport → Kind	tcp	Тип
Transport → URL	:5180	Локальный порт, который слушает коллектор
Event parsing → Name	[OOTB] 1C EventJournal Normalizer	Нормализатор для многострочных XML-файлов 1С

Конфигурация агента

Название поля	Значение поля	Описание
Agent name	[xml][1C] - Multiline	Название агента
Config → Connector → Name	local - 1C-XML	Название коннектора
Config → Connector → Kind	1c-xml	Тип
Config → Connector → URL	/opt/1c	Директория xml-файлов 1С

Config→ Destinations → Name	1C-XML	Название точки назначения
Config→ Destinations → Kind	tcp	Тип
Config→ Destinations → URL	<KUMA-FQDN>:5180	Сервер и порт коллектора для приема журналов 1C

Base settings

Config #1

+

Connector:

Basic settings

Advanced settings

Create new

*Name

local - 1C-XML

*Kind

1c-xml

?

*URL

/opt/1c

?

Destinations:

Basic settings

Advanced settings

Create new

*Name

1C-XML

☐ Disabled

*Kind

tcp

?

*URL

<KUMA-FQDN>:5180

2. Установка Linux-агента на хост для сбора XML-журналов 1C

Для разового запуска Агента воспользуйтесь следующей командой:

```
sudo /opt/kaspersky/kuma/kuma agent --core https://<KUMA-FQDN>:7210 --id <ID> --wd /opt/kaspersky/agent/<ID>
```

Для автоматизации процесса сбора событий установите агент в качестве службы. Также можно воспользоваться утилитой **supervisor**. Для этого создайте конфигурационный файл (например, 1c.conf) в директории `/etc/supervisor/conf.d/` со следующими настройками:

```
[program:agent_5f45aee7-655c-4014-aacd-07e4548de8ae]
command=sudo /opt/kaspersky/kuma/kuma agent --core https://<KUMA-FQDN>:7210 --id <ID> --wd /opt/kaspersky/agent/<ID>
autostart=true
autorestart=true
```

Для применения конфигурации перезагрузите службу:

```
sudo systemctl restart supervisor
```

Для просмотра статуса и наличия ошибок воспользуйтесь следующей командой:

```
sudo supervisorctl status
```

3. Проверка получения событий

В веб-интерфейсе KUMA выберите коллектор и перейдите к событиям (Resources → Collector → Go to events). На основном экране появятся нормализованные события 1С, полученные с Linux-агента.

SELECT * FROM `events` WHERE ServiceID = <ID> ORDER BY Timestamp DESC LIMIT 250

TenantID	Timestamp ↓	Name	DeviceProduct	DeviceVendor
Main	2023-08-23 19:23:11	Данные. Изменен...	Журнал событий	1C
Main	2023-08-23 19:23:11	Фоновое задание...	Журнал событий	1C
Main	2023-08-23 19:23:11	Сеанс. Начало	Журнал событий	1C
Main	2023-08-23 19:23:11	Фоновое задание...	Журнал событий	1C
Main	2023-08-23 19:23:11	Сеанс. Начало	Журнал событий	1C

1С Битрикс (Bitrix) интеграция с KUMA

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

Настройки на стороне 1С

Создание пользователя для чтения логов

1) Подключитесь к машине на которой установлен 1С:Управление сайтом и запустите консоль mysql под рутом (по умолчанию не требует пароля).

```
mysql -u root
```

Если вы не знаете пароль, то его возможно восстановить, но это рекомендуется сначала делать на **тестовом стенде**: <https://dev.1c-bitrix.ru/community/forums/messages/forum32/topic63387/message727606/#message727606>

2) В БД необходимо создать нового пользователя с правами на чтение журнала событий, вместо **10.10.10.10** укажите **IP KUMA**.

```
CREATE USER 'kuma'@'10.10.10.10' IDENTIFIED BY 'password';  
GRANT SELECT ON sitemanager.b_event_log TO 'kuma'@'10.10.10.10';  
FLUSH PRIVILEGES;
```

Настройки на стороне KUMA

1) <https://box.kaspersky.com/f/622c0730465643948c20/> Импортируйте ресурс (пароль q123123Q!):

2) Измените секрет для подключения (**Ресурсы** -> **Секреты** -> **1С: Управление сайтом**), если используются спец символы, то пароль можно будет использовать следующий ресурс для преобразования <https://www.urlencoder.org/>

mysql://kuma:password@tcp(10.10.10.11:3306)/sitemanager

5) При создании коллектора выберите коннектор и парсер - 1С:Управление сайтом, затем укажите точки назначения и создайте сервис.