

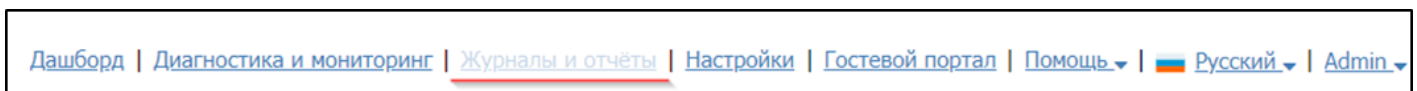
Usergate

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

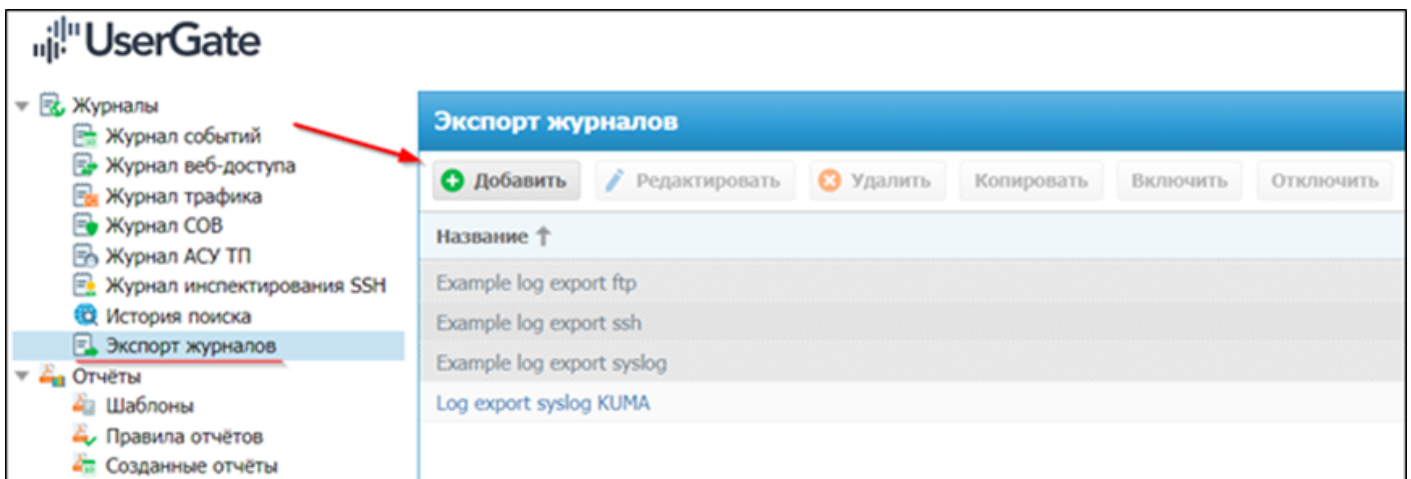
Настройка Usergate

Для настройки отправки событий с Usergate в KUMA выполните следующие действия:

1. В веб-интерфейсе Usergate перейдите на вкладку **Журналы и отчеты**.



2. Выберите **Экспорт журналов** и нажмите кнопку **Добавить**.



3. На вкладке **Общие** поставьте галочку напротив параметра **Включено** и задайте имя правилу экспорта журналов.

The screenshot shows a window titled "Свойства правила экспорта журналов" (Properties of log export rule). It has five tabs: "Общие" (General), "Удалённый сервер" (Remote server), "Журналы для экспорта" (Logs for export), "Расписание" (Schedule), and "Управление журналами" (Log management). The "Удалённый сервер" tab is active. It contains the following fields:

- "Включено:" (Enabled): A checkbox that is checked.
- "Название:" (Name): A text field containing "Log export syslog KUMA".
- "Описание:" (Description): An empty text area.

At the bottom right, there are three buttons: "Проверить соединение" (Check connection), "Сохранить" (Save), and "Отмена" (Cancel).

4. На вкладке **Удаленный сервер** задайте следующие настройки:

- **Тип сервера** - **Syslog**
- **Адрес** - коллектора KUMA
- **Порт** - порт коллектора KUMA
- **Транспорт** - **UDP** или **TCP** (настройка должна совпадать с настройками коллектора KUMA).
- **Протокол** - **Syslog (RFC 5424)**.
- **Критичность** и **Объект** выберите в соответствии с потребностями в логировании.

В поле **Имя хоста** по умолчанию указано имя хоста Usergate с символом @. Замените символ «@» на символ «.» для корректной нормализации событий Usergate на стороне KUMA.

Свойства правила экспорта журналов

Общие

Удалённый сервер

Журналы для экспорта

Расписание

Управление журналами

Тип сервера:

Syslog

Адрес сервера:

10.68.85.125

Порт:

5155

Транспорт:

UDP

Протокол:

Syslog (RFC 5424)

Критичность:

Информативная

Объект:

Сообщения пользовательские

Имя хоста:

utmcore.icastasinspe

Название приложения:

utm-loganalyzer

Проверить соединение

Сохранить

Отмена

5. На вкладке **Журналы для экспорта** поставьте галочки напротив **Журналов**, которые необходимо экспортировать в KUMA. Для каждого экспортируемого журнала выберите **Формат CEF**.

6. Сохраните внесенные изменения.

Настройка KUMA

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий Usergate.

1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками на стороне Usergate.

2. На шаге **Парсинг** событий выберите нормализатор **[OOTB] Syslog-CEF**.

3. 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.

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

5. Скопируйте появившуюся команду для установки коллектора KUMA.

Полезные ссылки

Экспорт журналов (документация UserGate): https://docs.usergate.com/eksport-zhurnalov_178.html

Revision #4

Created 11 August 2023 12:45:19 by Koala

Updated 7 July 2024 08:50:59 by Koala