

Suricata

Для настройки парсера Suricata перейдите в раздел **Конфигурация → Интеграция → Парсеры Syslog → Новый парсер Syslog** и выберите значение **Suricata** в выпадающем списке.

Новый парсер Syslog Suricata ✕

1

Имя

Требуется указать имя.

2

Статус

Включено

3

Канал уведомления

Требуется канал уведомления.

4

Лимит скорости передачи

0

секунд

Создать

Сбросить

Отмена

На открывшейся странице вы можете выполнить следующие настройки:

- 1. **Имя** — имя парсера, которое будет отображаться в таблице;
 - 2. **Статус** — при активации данного параметра парсер будет принимать и обрабатывать сообщения Syslog;
 - 3. **Канал уведомлений** — абсолютный путь до ранее созданного канала уведомлений;
 - 4. **Лимит скорости передачи** — ограничение скорости передачи.
- Для того чтобы добавить новый парсер, заполните параметры конфигурации и нажмите **Создать**. Чтобы сбросить введенные параметры на стандартные значения, нажмите **Сбросить**. Для возвращения на предыдущую страницу без сохранения выполненных на странице действий нажмите **Отменить**.