

Table of Contents

Table of Contents	1
Сборщик логов	2
Общие сведения	3
Настройка параметров syslog-сервера	4
Настройка фильтрации syslog	5

Documentation: ☒

Product: SIEM

Version: 7.x

UserGate SIEM журналирует данные о событиях Unix-систем и других сетевых устройств, использующих стандарт syslog, с помощью [модуля log-collector](#). Эти данные содержат сведения о работе системы, ее состоянии, наличии ошибок, сбоях в работе, а также о событиях безопасности.

Модуль log-collector выполняет предварительную обработку и фильтрацию собранных данных, что позволяет UserGate SIEM использовать только необходимую информацию для обработки и [последующего анализа](#). В веб-консоли UserGate SIEM вы можете [настраивать параметры модуля log-collector](#), используемого в качестве syslog-сервера для сетевых устройств, а именно выбирать транспортный протокол (TCP или UDP) и порт подключения, а также настраивать TLS-шифрование для протокола TCP. Кроме того, вы можете [настраивать правила syslog](#) для фильтрации данных о событиях по нужным параметрам (например, по уровню важности событий).

В ходе обработки данных, полученных от модуля log-collector, UserGate SIEM записывает их в единое хранилище. Поддерживаются такие стандарты журналирования событий, как RFC 3164 и RFC 5424. Для стандарта RFC 5424 расширенные данные записываются в поле data хранилища. Вы можете просматривать все записи о событиях стандарта syslog в веб-консоли UserGate SIEM в разделе **Журналы и отчеты** → **Журналы** → **Syslog** (см. раздел «[Журнал syslog](#)»).

Настройка параметров syslog-сервера

Documentation: 

Product: SIEM

Version: 7.x

Для сбора событий стандарта syslog от сетевых устройств необходимо:

- активировать сервис **Сборщик логов** [для зон](#), в которых находятся сетевые устройства;
- настроить параметры syslog-сервера, роль которого выполняет модуль log-collector.

Чтобы настроить параметры syslog-сервера:

1. В разделе **Настройки** → **Сборщик логов** → **Syslog** нажмите **Настроить сервер**.
2. В блоке параметров **TCP** выполните следующие действия:
 - включите прием событий syslog по протоколу TCP;
 - укажите порт подключения к syslog-серверу (по умолчанию — 514);
 - укажите максимальное количество одновременных сессий между syslog-сервером и сетевыми устройствами, от которых этот сервер получает данные.

Если требуется, включите TLS-шифрование передаваемых данных. Для этого установите флажок **Безопасное соединение** и [выберите необходимые сертификаты](#). При необходимости в блоке параметров **Разрешенные соседи** вы можете указать IP-адреса и доменные имена сетевых устройств, данные о событиях которых будет разрешено передавать на syslog-сервер.

3. В блоке параметров **UDP** выполните следующие действия:
 - включите прием событий syslog по протоколу UDP;
 - укажите порт подключения к syslog-серверу (по умолчанию — 514).
4. Нажмите **Сохранить и перезапустить** для применения новых параметров к syslog-серверу.

Настройка фильтрации syslog

Documentation: 

Product: SIEM

Version: 7.x

Вы можете настроить правила syslog для фильтрации данных, которые модуль log-collector будет передавать в UserGate SIEM для дальнейшей обработки и анализа.

Правила syslog отображаются в таблице раздела **Настройки → Сборщик логов → Syslog**. Вы можете управлять правилами syslog: изменять, удалять, а также включать и отключать их. Для этого используются соответствующие кнопки в панели инструментов. Также вы можете фильтровать правила в таблице по состоянию. Так, например, можно просмотреть только правила во включенном состоянии, применив фильтр **Показать включенные**.

Порядок расположения правил syslog в таблице соответствует порядку их применения к записям журналов событий по стандарту syslog. При необходимости вы можете изменять порядок с помощью кнопок **Наверх**, **Выше**, **Ниже**, **Вниз**.

Чтобы настроить правило syslog:

1. В разделе **Настройки → Сборщик логов → Syslog** нажмите **Добавить**.
2. На вкладке **Общие** выполните следующие действия:
 - Включите правило syslog.
 - Укажите название и при необходимости описание правила syslog.
 - Выберите действие по срабатыванию правила syslog (**Разрешить** — отправлять запись в UserGate SIEM, **Запретить** — не отправлять запись в UserGate SIEM).
 - Укажите часовой пояс правила syslog относительно UTC в секундах (по умолчанию — UTC+0). Указанный часовой пояс будет использоваться для отображения времени событий в UserGate SIEM.
 - Выберите расположение правила в таблице правил syslog.
3. На соответствующих вкладках укажите необходимые параметры фильтрации записей:
 - На вкладке **Критичность** по кнопке **Добавить** выберите уровни важности событий, записи о которых следует отправлять в UserGate SIEM. При установке флажка **Инвертировать** (соответствует логическому отрицанию) выбранные уровни важности будут исключены из условий срабатывания правила syslog.
 - На вкладке **Объект** по кнопке **Добавить** выберите подсистемы, службы и сервисы, записи которых следует отправлять в UserGate SIEM. При установке флажка **Инвертировать** (соответствует логическому отрицанию) выбранные объекты будут исключены из условий срабатывания правила syslog.
 - На вкладке **Имя хоста** по кнопке **Добавить** укажите IP-адреса и доменные имена сетевых устройств, записи которых следует отправлять в UserGate SIEM.
 - На вкладке **Название приложения** укажите системные приложения, записи которых следует отправлять в UserGate SIEM. Вы можете выбрать эти приложения по кнопке **Добавить из библиотеки приложений syslog** или добавить новые приложения по кнопке **Создать и добавить новый объект**.
4. Нажмите **Сохранить**.

