

Настройка отправки журналов с устройства UserGate

В данной статье описано, как настроить отправку журналов с UserGate.

Общие сведения

Функция экспортирования журналов событий UserGate позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM (Security information and event management).

UserGate поддерживает выгрузку следующих журналов:

- журнал событий;
- журнал веб-доступа;
- журнал COB;
- журнал трафика;
- журнал инспектирования SSH;
- журнал DNS;
- журнал почтового трафика;
- журнал UserID.

Поддерживается отправка журналов на серверы SSH (SFTP), FTP и Syslog. Отправка на серверы SSH и FTP проводится по указанному в конфигурации расписанию. Отправка на серверы Syslog происходит сразу же при добавлении записи в журнал.

Настройка отправки журналов

Для отправки журналов необходимо создать конфигурации экспорта журналов в разделе **Экспорт журналов**.

Если в настройках указан **Log Analyzer**, то обработка и экспорт журналов, создание отчетов и обработка других статистических данных производятся сервером LogAn.

При создании конфигурации требуется указать следующие параметры:

Наименование	Описание
Название правила	Название правила экспорта журналов
Описание	Опциональное поле для описания правила
Параметры разового экспорта	Выбор диапазона экспорта журналов. Опция доступна в версии ПО 7.2.0 и выше
Журналы для экспорта	<p>Выбор файлов журналов, которые необходимо экспортировать:</p> <ul style="list-style-type: none">• журнал событий;• журнал веб-доступа;• журнал COB;• журнал трафика;• журнал инспектирования SSH;• журнал DNS;• журнал почтового трафика;• журнал UserID. <p>Для каждого из журналов возможно указать синтаксис выгрузки:</p> <ul style="list-style-type: none">• CEF — Common Event Format (ArcSight);• CEF Compact;• JSON — JSON format;• @CEE: JSON — CEE Log Syntax (CLS) Encoding JSON. <p>Обратитесь к документации на используемую у вас систему SIEM для выбора необходимого формата выгрузки журналов</p>
Тип сервера	SSH (SFTP), FTP, Syslog
Адрес сервера	IP-адрес или доменное имя сервера
Транспорт	Только для типа серверов Syslog — TCP или UDP
Порт	Порт сервера, на который следует отправлять данные

Наименование	Описание
Протокол	Только для типа серверов Syslog — RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM
Критичность	<p>Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения:</p> <ul style="list-style-type: none"> • Тревога: состояние, требующее незамедлительного вмешательства. • Критическая: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе. • Ошибки: в системе возникли ошибки. • Предупреждения: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия. • Уведомительная: события, которые относятся к необычному поведению системы, но не являются ошибками. • Информативная: информационные сообщения.
Facility	<p>Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения:</p> <ul style="list-style-type: none"> • Сообщения пользовательские; • Системный сервис; • Безопасность/авторизация; • Аудит; • Тревога; • Local 0; • Local 1; • Local 2; • Local 3; • Local 4; • Local 5; • Local 6; • Local 7.
Имя хоста	Только для типа серверов Syslog. Уникальное имя хоста, идентифицирующее сервер, отправляющий данные на сервер syslog, в формате Fully Qualified Domain Name (FQDN)
App-Name	Только для типа серверов Syslog. Уникальное имя приложения, которое отправляет данные на сервер syslog
Логин	Имя учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog
Пароль	Пароль учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog
Путь на сервере	Каталог на сервере для копирования файлов журналов. Не применяется к методу отправки Syslog

Наименование	Описание
Расписание	<p>Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты:</p> <ul style="list-style-type: none"> • Ежедневно; • Еженедельно; • Ежемесячно; • Каждые ... часов; • Каждые ... минут; • Задать вручную. <p>При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом:</p> <ul style="list-style-type: none"> • Звездочка (*) — обозначает весь диапазон (от первого до последнего); • Дефис (-) — обозначает диапазон чисел. Например, 5-7 будет означать 5, 6 и 7; • Списки — это числа (или диапазоны), разделенные запятыми. Например, 1,5,10,11 или 1-11,19-23; • Звездочка или диапазон с шагом — используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, 2-10/2" будет значить 2,4,6,8,10, а выражение */2 в поле часы будет означать каждые два часа.
Управление журналами	<p>Управление временными файлами журналов, подготавливаемых для отправки на удаленные серверы ssh и ftp.</p> <p>При отправке журналов на сервера ssh и ftp UserGate сохраняет данные для отправки во временные файлы. По указанному расписанию все созданные для отправки файлы копируются на удаленный сервер, при этом файлы не очищаются и не удаляются. Данная настройка позволяет указать период ротации временных файлов (в днях) или удалить любой из временных файлов вручную. Ротация файлов происходит один раз в сутки.</p> <p>Всего хранятся N архивов журналов за предыдущие дни (по количеству дней ротации) и один журнал за текущий день.</p>

ID статьи: 1624

Последнее обновление: 28 апр., 2026

Обновлено от: Михалева А.

Ревизия: 1

База знаний Логикор -> Документация -> Система хранения и обработки данных «Логикор». Версия 2.7.0 -> Логикор.

Руководство разработчика -> Подключение источников событий в Логикор -> Настройка источников -> Настройка отправки журналов с устройства UserGate

<https://docs.axel.pro/entry/1624/>