Агентский сбор данных

В данной статье описана установка и настройка Winlogbeat для отправки логов в Логикор.

Общие сведения

Winlogbeat — это агент, предназначенный для сбора событий из журнала событий Windows (Event Log) и их пересылки в централизованную систему анализа, в данном случае — в Логикор.
Данный документ описывает полный процесс установки, настройки и запуска Winlogbeat без обращения к внешним ресурсам, включая работу с учетными записями с ограниченными правами и интеграцию с Windows Event Collector (WEC).

Поддерживаемые версии Windows

Winlogbeat официально поддерживается на следующих актуальных и распространённых версиях Windows:

- Windows 10 (версии 1809 и новее);
- Windows 11;
- Windows Server 2016;
- Windows Server 2019;
- Windows Server 2022.

Убедитесь, что на целевой системе установлены последние обновления ОС и .NET Framework 4.7.2 или выше (для корректной работы PowerShell-скриптов).

Подготовка к установке

Получение дистрибутива

Используется предварительно подготовленный архив:

logiq_winlogbeat_9.0.1.zip — содержит Winlogbeat версии 9.0.1 с типовой конфигурацией для отправки данных в Логикор.

Распаковка

1. Скопируйте архив **logiq_winlogbeat_9.0.1.zip** на целевой хост.
2. Распакуйте его в папку: **C:\Program Files**.
3. После распаковки вы получите папку вида **winlogbeat-9.0.1-windows-x86_64**.
4. Переименуйте ее в **Winlogbeat**, чтобы путь стал: **C:\Program Files\Winlogbeat**.

Настройка конфигурации

1. Удалите файл **winlogbeat.yml** если он присутствует.
2. Скопируйте в папку **C:\Program Files\Winlogbeat** файл конфигурации: **logiq_winlogbeat_conf.yaml**.
3. Откройте **logiq_winlogbeat_conf.yaml** в текстовом редакторе (например, Notepad++ или VS Code).
4. Найдите строку, содержащую адрес назначения, например:
   output.logstash:
   hosts: ["192.168.1.100:5044"]
   Замените IP-адрес **(192.168.1.100)** на IP-адрес коллектора или балансировщика Логикор в вашем окружении.
5. Сохраните файл.

Файл **logiq_winlogbeat_conf.yaml** уже содержит рекомендованные источники событий (Security, System, Application и др.), фильтрацию и форматирование под Логикор.

Установка как службы (стандартный способ — от администратора)

Этот способ требует прав локального администратора.

Выполните следующие шаги:

1. Откройте PowerShell от имени администратора. Нажмите ПКМ на **значок PowerShell → Запуск от имени администратора**.
2. Перейдите в папку Winlogbeat:

   cd "C:\Program Files\Winlogbeat"

3. Разблокируйте скрипты (если появляется предупреждение о безопасности):

   Unblock-File .\install-service-winlogbeat.ps1

4. Установите службу:

   .\install-service-winlogbeat.ps1

5. Запустите службу:

   Start-Service winlogbeat

6. Проверьте статус:

   Get-Service winlogbeat

Запуск от пользовательской учетной записи

Многие пользователи спрашивают: можно ли запускать Winlogbeat без прав администратора?
Ответ: частично — да, но с ограничениями.

Возможности и ограничения:

- Чтение большинства журналов событий (Application, System) доступно даже пользователям из группы Users;
- Журнал Security требует членства в группе Event Log Readers (или выше);
- Установка как службы Windows невозможна без прав администратора;
- Однако Winlogbeat можно запускать вручную (в режиме foreground) из командной строки или PowerShell.

Ручной запуск (без установки службы)

1. Убедитесь, что пользователь состоит в группе Event Log Reader:
   - Откройте **Управление компьютером → Локальные пользователи и группы → Группы → Event Log Readers** .
   - Добавьте туда свою учетную запись.
2. Перейдите в папку Winlogbeat:
   - **cd "C:\Program Files\Winlogbeat"**.
3. Запустите Winlogbeat напрямую:
   - **.\winlogbeat.exe -c logiq_winlogbeat_conf.yaml -e**.
   - Флаг **-e** выводит логи в консоль (удобно для отладки).
   - Без **-e** логи пишутся в **winlogbeat.log** (по умолчанию в той же папке).

При ручном запуске Winlogbeat не будет автоматически перезапускаться после перезагрузки. Для автозапуска можно использовать:

- Планировщик заданий (Task Scheduler);
- Скрипт в автозагрузке пользователя.

Автозапуск через Планировщик заданий (без прав администратора)

1. Откройте **Планировщик заданий**.
2. Создайте новую задачу:
   - **Триггер**: «При входе пользователя»;
   - **Действие**: запуск программы;
   - **Программа**: **C:\Program Files\Winlogbeat\winlogbeat.exe**;
   - **Аргументы**: **-c "C:\Program Files\Winlogbeat\logiq_winlogbeat_conf.yaml"**.
     Убедитесь, что галочка **«Выполнять только при входе в систему»** включена.
3. Сохраните задачу.

Это позволяет запускать Winlogbeat при каждом входе пользователя без прав администратора.

Запуск Winlogbeat от учетной записи с ограниченными правами

Хотя по умолчанию служба Winlogbeat работает от системной учетной записи **Local System**, ее можно настроить на запуск от локальной учетной записи без прав администратора. Это соответствует принципам минимальных привилегий и часто требуется в корпоративных средах.

Учетная запись должна быть локальной (не доменной, если не настроены дополнительные политики) и иметь два обязательных разрешения:

- Право **Вход в качестве службы** (Log on as a service);
- Членство в группе **Event Log Readers**.

Подготовка учетной записи

1. Создайте или выберите локального пользователя (например, winlogbeat-user), не входящего в группу администраторов.
2. Добавьте пользователя в группу **Event Log Readers**.
3. Назначьте право **Вход в качестве службы**.

Настройка службы Winlogbeat

1. Убедитесь, что служба уже установлена.
2. Откройте консоль служб.

3. Найдите службу **winlogbeat**, откройте **Свойства → Вход в систему** (Log On).
4. Выберите **«Эта учетная запись»** → укажите имя пользователя (например, .\\winlogbeat-user) и введите пароль.
5. Нажмите **Применить → OK**.
6. Перезапустите службу.

Проверка

- Убедитесь, что служба запущена.
- Проверьте логи на ошибки доступа.
- Если видите ошибки вида **Access denied to Security log** , убедитесь, что пользователь действительно в группе **Event Log Readers**.

Особенности при сборе событий с WEC (Windows Event Collector)

Если события собираются не напрямую с локального хоста, а через централизованный сервер WEC (Forwarded Events), то:

- Winlogbeat должен быть установлен на сервере WEC, а не на конечных хостах.
- В конфигурации **logiq_winlogbeat_conf.yaml** нужно указать чтение из журнала ForwardedEvents:

```
winlogbeat.event_logs:
  - name: ForwardedEvents
    ignore_older: 72h
```

- Учетная запись, от которой запущен Winlogbeat, должна иметь права на чтение ForwardedEvents (обычно достаточно членства в Event Log Readers на сервере WEC).
- Не требуется установка Winlogbeat на каждый клиентский хост — только на WEC-сервер.

Проверка работоспособности

1. Убедитесь, что служба запущена:

   ```
   Get-Service winlogbeat
   ```

2. Проверьте логи:

   ```
   Get-Content .\winlogbeat.log -Tail 20
   ```

3. Убедитесь, что события поступают в Логикор (через интерфейс Логикор или Kibana).

Устранение типичных проблем

1. **«Access denied» при чтении Security.**
   Добавьте пользователя в группу **Event Log Readers.**
2. **Служба не запускается.**
   Проверьте синтаксис YAML-файла (отступы, кавычки).
3. **Нет событий в Логикор.**
   Проверьте сетевую доступность коллектора, порт 5044, firewall.
4. **Ошибка выполнения .ps1.**
   Выполните **Unblock-File** перед запуском.

ID статьи: 1559
Последнее обновление: 31 мар., 2026
Обновлено от: Михалева А.
Ревизия: 8
База знаний Логикор -> Документация -> Система хранения и обработки данных «Логикор». Версия 2.5.0 -> Логикор. Руководство разработчика -> Подключение источников событий в Логикор -> Тип сбора данных -> Агентский сбор данных
https://docs.axel.pro/entry/1559/