Подключение источников событий в Логикор

Прием и обработка журналов в Логикор выполняется компонентом Saturn, внутри которого используется модифицированный инструмент Logstash для сбора, преобразования и доставки логических событий.

Логикор поддерживает несколько базовых способов подключения источников событий. В зависимости от типа источника и требований к сбору данных система может принимать журналы по сетевым протоколам, через агент или напрямую из файловой системы.

В базовой поставке Saturn предоставляет, но не ограничивается, несколькими базовыми интерфейсами для приема данных:

- **Beats** — используется для подключения журналов аудита и других источников, передающих данные через агент;
- **Syslog** — используется для подключения источников, отправляющих данные по протоколу Syslog, такие как:
  - **Linux\Unix файлы журналы** — sshd, pam, boot, auth, messages, kern и другие;
  - **Сетевое оборудование** — Palo Alto, Cisco, UserGate и другое;
  - **ПО, отправляющее записи журналов по протоколу Syslog** (или с использованием ППО rsyslog, syslog-ng, и подобных), например, веб-серверы (Apache/Nginx): /var/log/apache2/, /var/log/httpd/, /var/log/nginx/ (access.log, error.log), базы данных (MySQL/PostgreSQL): /var/log/mysql.log, /var/log/mysqld.log, /var/lib/postgres/.../pg_log, почтовые серверы: /var/log/mail.log, /var/log/exim4/, планировщик задач (cron): /var/log/cron.
- **File** — используется для чтения журналов напрямую из файловой системы.

Saturn может принимать данные в нескольких режимах:

- пассивный прием данных по протоколу Syslog;
- пересылка данных с помощью агента Winlogbeat, устанавливаемого на сервер и АРМ на базе Windows;
- активный сбор данных со стороны Saturn.

Ниже приведена сводная таблица по источникам, типам приема, документации и заметок:

	Документация	Дополнительно	Источник	Настройка	Тип сбора данных
Cisco ASA	CLI Book 1: Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide, 9.18	-	Cisco Asa		Пассивный сбор
UserGate	Экспорт журналов - UserGate :: Портал документации	-	UserGate	-	Пассивный сбор
Palo Alto	Configure Syslog Monitoring	-	Palo Alto	-	Пассивный сбор
Cisco Prime	Logging Syslog Messages - Cisco	-	Cisco Prime	-	Пассивный сбор
Cisco ISE	Configure External Syslog Server on ISE	-	Cisco ISE	-	Пассивный сбор
Checkpoint	Working with Syslog Servers	Работает только через SmartConsole	Checkpoint	-	Пассивный сбор
Windows	-	Необходимо развернуть и настроить WEC и через GPO раскатить политику WE (Forwarding)	Windows	Настройка аудита	Агентский сбор
Linux Based OS (Ubuntu/Debian/Astra) & App	Журналы работы системных служб - Справочный центр - Справочный центр Astra Linux	-	Linux Based OS (Ubuntu /Debian/Astra)	-	Пассивный сбор
Cisco Stealthwatch / Cisco SecureNetworkAnalytics	-	-	Cisco Stealthwatch / Cisco SecureNetwork Analytics	-	Пассивный сбор

ID статьи: 1622
Последнее обновление: 28 апр., 2026
Обновлено от: Михалева А.
Ревизия: 5
База знаний Логикор -> Документация -> Система хранения и обработки данных «Логикор». Версия 2.7.0 -> Логикор. Руководство разработчика -> Подключение источников событий в Логикор -> Подключение источников событий в Логикор
https://docs.axel.pro/entry/1622/