Пассивный сбор данных

В данной статье описана организация пассивного сбора данных по протоколу Syslog.

Общие шаги

1. Определите IP адрес точки назначения — это может быть балансировщик, VIP или сам компонент Saturn в случае инсталляции типа AIO.
2. Определите порт назначения — по умолчанию используется порт 5140.

Настройка отправки данных от устройств, поддерживающих пассивный сбор данных

1. Используя ссылки на инструкции, настройте оборудование на отправку данных по протоколу Syslog, используя ip \ port, определенный ранее.

Настройка хостов Linux

1. Воспользуйтесь инструкцией ОС семейства Unix: настройка источника · MaxPatrol SIEM · Справочный портал.
2. При недоступности инструкции выполните шаги для настройки auditd.

Шаги для настройки auditd

Установка и обновление службы auditd

Служба **auditd** необходима для аудита и журналирования событий безопасности в системе. Требуется версия **2.6 или новее**.

Шаг 1. Проверьте текущую версию. Выполните команду:

auditctl -v

- Если вывод содержит строку вида **auditctl version 2.8.2** — служба установлена. Сравните версию с требуемой (≥2.6).
- Если команда завершается ошибкой (**command not found** и т.п.) — служба не установлена.

Шаг 2. Установка (если служба отсутствует). Выберите команду в зависимости от вашей ОС:

ОС	Команда
ALT Linux	sudo apt-get install -y audit
Astra Linux, Debian, Ubuntu	sudo apt-get install -y auditd audispd-plugins
CentOS, Oracle Linux, RHEL	sudo yum install -y audit
Rocky Linux / AlmaLinux (dnf)	sudo dnf install -y audit
SUSE Linux Enterprise Server	sudo zypper install -y audit

Рекомендуется также установить **audispd-plugins** (для Debian/Ubuntu) — они расширяют функциональность аудита.

Шаг 3. Выполните обновление, если установленная версия ниже 2.6:

1. Сделайте резервную копию конфигурации:

   sudo cp -r /etc/audit /etc/audit.bak

2. Обновите пакеты системы:
   - Debian/Ubuntu/Astra:

     sudo apt update && sudo apt upgrade auditd

   - RHEL/CentOS/Oracle:

     sudo yum update audit
     # или для новых версий:
     sudo dnf upgrade audit

   - ALT Linux:

     sudo apt-get update && sudo apt-get upgrade audit

   - SLES:

     sudo zypper refresh && sudo zypper update audit

     Если в репозиториях ОС нет версии ≥2.6 (например, в старых LTS-выпусках), может потребоваться:

     - обновление ОС до поддерживаемой версии;
     - подключение дополнительных репозиториев (например, EPEL для RHEL);
     - компиляция из исходников (только при наличии экспертизы и одобрения ИБ-политики).
3. Перезапустите службу после обновления:

   sudo systemctl restart auditd
   sudo systemctl enable auditd # для того чтобы служба запускалась при старте

Шаг 4. Проверьте результат:

auditctl -v
systemctl status auditd

Убедитесь, что версия ≥2.6 и статус службы — **active (running)**.

Настройка адресации и формата событий

Чтобы корректно настроить адресацию и формат событий для интеграции с MaxPatrol SIEM, выполните следующие действия:

Шаг 1. Выполните настройку имени узла и файла /etc/hosts:

1. Откройте файл:

   sudo nano /etc/hosts

2. Если имя узла указано как localhost, измените его с помощью команды:

   sudo hostnamectl set-hostname <Новое_имя_узла>

   (замените <Новое_имя_узла> на желаемое имя хоста)
3. Убедитесь, что в файле **/etc/hosts** отсутствуют записи, связывающие ваше новое имя узла или FQDN с локальными адресами (127.0.0.1, 127.0.1.1, ::1). Пример некорректной строки:

   127.0.1.1 myhost.localdomain myhost

   Такую строку следует удалить.
4. Добавьте запись, сопоставляющую реальный IP-адрес узла с его именем:

   <IP-адрес_узла_источника> <Имя_узла_источника>

   Например:

   192.168.10.25 audit-srv-01

5. Сохраните файл и закройте редактор.

Шаг 2. Настройка конфигурации auditd

1. Откройте файл конфигурации **auditd**:
2. Укажите следующие параметры в соответствии с рекомендациями для MaxPatrol SIEM. Пример корректного фрагмента файла:

```
# Формат журналируемых событий
log_format = ENRICHED

# Формат отображения имён пользователей и групп
name_format = NUMERIC

# Гарантированная доставка событий без потерь
disp_qos = lossless

# Отключите запись локальных журналов, если используется MaxPatrol SIEM
# (актуально для высоконагруженных систем)
write_logs = no
```

Параметр write_logs = no рекомендуется использовать только при централизованной отправке событий чтобы избежать избыточной нагрузки на диск.

3. Сохраните изменения и закройте редактор.

Шаг 3. Перезапуск службы **auditd**:

1. Примените изменения, перезапустив службу **auditd**:

   sudo systemctl restart auditd

2. Убедитесь, что служба запущена:

   sudo systemctl status auditd

Результат: Адресация и формат событий успешно настроены для корректной работы.

Настройка правил журналирования

Для того чтобы настроить правила журналирования выполните следующие шаги.

Шаг 1. В каталоге **/etc/audit/rules.d** для всех файлов с расширением **rules** измените расширение на любое другое.

Шаг 2. Создайте файл **/etc/audit/rules.d/00-siem.rules**. Вы можете скачать архив с файлом правил журналирования из хранилища файлов.

Шаг 3. Скопируйте в файл строки с правилами журналирования.
Вместо переменной **<UID_MIN>** введите системное значение, указанное в файле **/etc/login.defs** в параметре **UID_MIN**.

Шаг 4. Если требуется исключить события определенного приложения, после строки **# exclude bins** добавьте правило:

-a never,exit -F arch=b64 -S capset,setxattr,lsetxattr,fsetxattr,settimeofday,adjtimex,clock_settime,socket,connect,accept4,accept,listen,execve,execveat,ptrace,setuid,setgid,setreuid,setregid -F exe=<Путь к исполн

Шаг 5. Сохраните файл.

Шаг 6. Примените правила журналирования:

auditctl -R /etc/audit/rules.d/00-siem.rules

Шаг 7. Перезапустите службу **auditd**.

Правила журналирования настроены.

Отключение сокета аудита systemd

Сокет **systemd-journald-audit.socket** автоматически перехватывает события ядра **audit** и передаёт их в журнал **systemd** (journald). Это может привести к дублированию событий или конфликту с настройками **auditd**, особенно при использовании MaxPatrol SIEM. Поэтому рекомендуется отключить этот сокет, если вы используете **auditd + audispd** для отправки событий в SIEM.

Сокет systemd-journald-audit.socket присутствует не во всех дистрибутивах. Он характерен для систем на базе **systemd ≥ 235**, включая:

- **RHEL / CentOS / Oracle Linux 8+**
- **Ubuntu 20.04+**
- **Debian 11+**
- **SLES 15+**
- **Astra Linux SE 1.7+ и выше**

В **ALT Linux**, **RHEL 7**, **CentOS 7** и других системах с более старыми версиями systemd этот сокет отсутствует, и отключать его не нужно.

Выполните следующие шаги:

Шаг 1. Проверьте наличие и статус сокета. Выполните команду:

systemctl is-active systemd-journald-audit.socket

- Если вывод: **inactive** или **unknown** — сокет неактивен или отсутствует. Отключение не требуется.
- Если вывод: **active** — сокет активен и требует отключения.

Также можно проверить его существование:

systemctl status systemd-journald-audit.socket

Если система сообщает Unit systemd-journald-audit.socket could not be found, — сокет не поддерживается вашим дистрибутивом.

Шаг 2. Отключите сокета (только если он активен). Выполните последовательно следующие команды:

```
sudo systemctl stop systemd-journald-audit.socket
sudo systemctl disable systemd-journald-audit.socket
sudo systemctl mask systemd-journald-audit.socket
```

Команда **mask** гарантирует, что сокет не будет запущен автоматически ни вручную, ни по зависимостям.

Проверьте результат:

systemctl is-active systemd-journald-audit.socket

Ожидаемый вывод: inactive или unknown.

Шаг 3. Перезапуск journald (опционально). Чтобы убедиться, что изменения вступили в силу, перезапустите службу журналирования:

sudo systemctl restart systemd-journald

Примечание: перезапуск journald безопасен и не приводит к потере журналов в большинстве современных систем.

Отключение сокета **systemd-journald-audit.socket** необходимо только в дистрибутивах, где он присутствует и активен, чтобы избежать конфликта между **auditd** и **systemd-journald**. В остальных случаях данная операция не требуется.

Перед отключением всегда проверяйте статус сокета — это сэкономит время и предотвратит ненужные действия на системах, где он не используется.

Проверка настройки службы auditd

Необходимо убедиться, что служба **auditd** корректно настроена для работы, использует правильный IP-адрес источника, применяет только необходимые правила аудита и не дублирует журналы при централизованной отправке событий.

Шаг 1. Проверка статуса службы **auditd**. Выполните команду:

sudo systemctl status auditd

Вместо устаревшей команды service auditd status рекомендуется использовать systemctl, так как большинство современных дистрибутивов (RHEL 7+, Ubuntu 16.04+, Debian 8+, Astra Linux, SLES 12+) используют systemd.

Ожидаемый результат: Строка Active: active (running).

Если служба **не запущена**:

- Убедитесь, что пакет **auditd** установлен.
- При необходимости переустановите его:
  - **RHEL/CentOS/Oracle Linux:** sudo yum reinstall audit audit-libs;
  - **Debian/Ubuntu/Astra Linux:** sudo apt install --reinstall auditd audispd-plugins;
  - **SLES:** sudo zypper install --force audit.

Шаг 2. Проверьте внешний IP-адрес источника. Выполните:

hostname -I

Используйте hostname -I (заглавная «i»), а не hostname -i — она выводит **все IPv4 и IPv6 адреса** , привязанные к интерфейсам, и работает надежнее.

Если вывод содержит только 127.0.0.1 или неправильный IP, проверьте:

- настройки сети (ip a, /etc/netplan/, /etc/network/interfaces, nmcli и т.д.);
- запись в /etc/hosts — убедитесь, что имя хоста сопоставлено с реальным IP, а не с 127.0.1.1 или 127.0.0.1.

Определение используемой на источнике службы журналирования

Шаг 1. Чтобы определить используемую на источнике службу журналирования,
выполните команду:

- если установлена ОС Astra Linux, Debian или Ubuntu:

  dpkg --list | grep syslog

- если ALT Linux, CentOS, Oracle Linux или Red Hat Enterprise Linux:

  rpm -qa *syslog*

- если SUSE Linux Enterprise Server:

  zypper search *syslog* --installed-only | grep 'i |'

На экране появится название используемой службы.

Настройка используемой службы

Для корректной передачи событий аудита необходимо настроить соответствующий Syslog-сервис в зависимости от используемой системы: **rsyslog**, **syslog-ng** или классический **syslogd**. Также требуется настроить модуль **audispd** для преобразования событий **audit** в формат **Syslog**.

Настройка службы rsyslog

Шаг 1. Создайте файл правил:

1. Создайте файл **/etc/rsyslog.d/10-siem.conf**:

   sudo nano /etc/rsyslog.d/10-siem.conf

2. Вставьте один из шаблонов в зависимости от протокола:
   - ### для отправки по UDP (порт 514):

     ```
     # Отправка событий audit через UDP
     if ($syslogfacility-text == "local6" or $syslogpriority-text == "info") and not re_match($syslogfacility-text,"(mail|lpr|news|uucp|cron)") then {
        action(
           type="omfwd"
           name="pt_linux_audit"
           protocol="udp"
           target="<IP-адрес_MP_10_Agent>"
           port="514"
           action.repeatedmsgcontainsoriginalmsg="off"
        )
     }

     # Отключить дублирование в /var/log/messages (для высоконагруженных систем)
     :programname, contains, "audisp" stop
     ```

   - ### для отправки по TCP (порт 1468):

     ```
     # Отправка событий audit в MP 10 Agent через TCP
     if ($syslogfacility-text == "local6" or $syslogpriority-text == "info") and not re_match($syslogfacility-text,"(mail|lpr|news|uucp|cron)") then {
        action(
           type="omfwd"
           name="pt_linux_audit"
           protocol="tcp"
           target="<IP-адрес_logiq>"
           port="1468"
           action.repeatedmsgcontainsoriginalmsg="off"
           action.resumeRetryCount="-1"
           queue.type="LinkedList"
           queue.filename="syslog_queue"
           queue.saveOnShutdown="on"
           queue.maxDiskSpace="1024m"
           queue.timeoutEnqueue="0"
        )
     }

     # Отключить дублирование в /var/log/messages (для высоконагруженных систем)
     :programname, contains, "audisp" stop
     ```

3. Замените **<IP-адрес_MP_10_Agent>** на реальный IP-адрес узла с Логикор.
4. Сохраните файл.

Шаг 2. Подключите конфигурацию в rsyslog:

1. Откройте основной конфигурационный файл:

   sudo nano /etc/rsyslog.conf

2. Убедитесь, что присутствует одна из следующих строк (раскомментируйте или добавьте):

   $IncludeConfig /etc/rsyslog.d/*.conf

   или (для новых версий rsyslog):

   include(file="/etc/rsyslog.d/*.conf" mode="optional")

Шаг 3. Настройте ограничении скорости (при необходимости):

1. Если используется **imjournal**:
   - для старого синтаксиса:

     ```
     $ModLoad imjournal
     $imjournalRatelimitBurst 20000
     $imjournalRatelimitInterval 15
     ```

- для нового синтаксиса:

  module(load="imjournal" Ratelimit.Burst="20000" Ratelimit.Interval="15")

2. Если используется **imuxsock**:
   - для старого синтаксиса:

     $ModLoad imuxsock
     $SystemLogRateLimitBurst 20000
     $SystemLogRateLimitInterval 15

   - для нового синтаксиса:

     module(load="imuxsock" SysSock.RateLimit.Burst="20000" SysSock.RateLimit.Interval="15")

Шаг 4. Проверка и перезапуск:

1. Проверьте конфигурацию:

   sudo rsyslogd -f /etc/rsyslog.conf -N 1

2. Если ошибок нет — перезапустите службу:

   sudo systemctl restart rsyslog

Настройка службы syslog-ng

Шаг 1. Определение источника.

1. Откройте основной файл конфигурации:

   sudo nano /etc/syslog-ng/syslog-ng.conf

2. Найдите блок вида:

   source s_sys { system(); };

3. Запомните имя источника (**s_sys** в примере).

Шаг 2. Создание файла правил:

1. Создайте файл:

   sudo nano /etc/syslog-ng/10-siem.conf

2. Используйте:
   - для UDP (порт 514):

     ```
     filter pt_siem_filter {
         (facility(local6) or priority(info)) and not facility(mail, lpr, news, uucp, cron);
     };

     destination logiq_udp {
         udp("<IP-адрес_logiq>" port(514));
     };

     log {
         source(s_sys);  # ← замените на ваше имя источника
         filter(pt_siem_filter);
         destination(loqiq_udp);
     };
     ```

   - для TCP (порт 1468):

     ```
     filter pt_siem_filter {
         (facility(local6) or priority(info)) and not facility(mail, lpr, news, uucp, cron);
     };

     destination logiq_tcp {
         tcp("<IP-адрес_logiq>" port(1468) log-fifo-size(1000));
     };

     log {
         source(s_sys);  # ← замените на ваше имя источника
         filter(pt_siem_filter);
         destination(logiq_tcp);
         flags(flow-control);
     };
     ```

Не забудьте заменить **s_sys** на реальное имя источника и **<IP-адрес_MP_10_Agent>** на актуальный IP.

Шаг 3. Подключение файла и фильтрация:

1. В основном файле **/etc/syslog-ng/syslog-ng.conf** добавьте:

   @include "10-siem.conf"

2. Также обновите фильтры, чтобы исключить события **audit** из локальных журналов:

   ```
   filter f_audit { program("audit") or program("audispd"); };

   filter f_messages {
       level(info,notice,warn) and
       not facility(auth,authpriv,cron,daemon,mail,news) and
       not filter(f_audit);
   };

   filter f_syslog3 {
       not facility(auth, authpriv, mail) and
       not filter(f_debug) and
       not filter(f_audit);
   };
   ```

Шаг 4. Проверка и перезапуск:

1. Проверьте конфигурацию:

   sudo syslog-ng --syntax-only

2. Если ошибок нет — перезапустите службу:

   sudo systemctl restart syslog-ng

Настройка классического syslogd

Эта служба устарела и редко используется в современных дистрибутивах.

1. Откройте файл:

   sudo nano /etc/syslog.conf

2. Добавьте в начало:
   - **для UDP:**

     *.info;mail.none;lpr.none;news.none;uucp.none;cron.none @<IP-адрес_logiq>:514

   - **для TCP:**

*.info;mail.none;lpr.none;news.none;uucp.none;cron.none @@<IP-адрес_logiq>:1468

3. Перезапустите службу:

   sudo systemctl restart syslog

Настройка отправки событий через audispd

События **audit** по умолчанию не попадают в syslog. Чтобы это исправить, используйте плагин **audispd-syslog**.

Шаг 1. Установите пакет:

- **Debian/Ubuntu/Astra Linux:** sudo apt-get install audispd-plugins;
- **RHEL/CentOS/Oracle Linux:** sudo yum install audispd-plugins;
- **SLES:** sudo zypper install audispd-plugins;
- **ALT Linux:** пакет уже включен.

Шаг 2. Настройте плагин. Файл зависит от версии **auditd**:

- **auditd ≥ 3.0**: /etc/audit/plugins.d/syslog.conf;
- **auditd < 3.0**: /etc/audisp/plugins.d/syslog.conf.

1. Откройте нужный файл:

   sudo nano /etc/audit/plugins.d/syslog.conf

2. Убедитесь, что содержимое выглядит так:

   ```
   active = yes
   direction = out
   path = builtin_syslog
   type = always
   args = LOG_LOCAL6
   format = string
   ```

Ключевой параметр — **args = LOG_LOCAL6**, он определяет **facility** для Syslog.

Шаг 3. Перезапуск **auditd:**

sudo systemctl restart auditd

События аудита теперь корректно передаются через выбранный Syslog-сервис.

ID статьи: 1558
Последнее обновление: 1 апр., 2026
Обновлено от: Михалева А.
Ревизия: 25
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 -> Пассивный сбор данных
https://docs.axel.pro/entry/1558/