



Руководство по настройке источников

Оглавление

Информация по релизам	6
О релизе № 36 от 03.09.2025	6
О релизе № 35 от 20.08.2025	7
О релизе № 34 от 06.08.2025	8
О релизе № 33 от 23.07.2025	10
О релизе № 32 от 09.07.2025	12
О релизе № 31 от 24.06.2025	16
О релизе № 30 от 11.06.2025	18
О релизе № 29 от 04.06.2025	20
О релизе № 28 от 28.05.2025	20
О релизе № 27 от 14.05.2025	23
О релизе № 26 от 30.04.2025	25
О релизе № 25 от 17.04.2025	28
О релизе № 24 от 02.04.2025	30
О релизе № 23 от 18.03.2025	31
О релизе № 22 от 04.03.2025	32
Поддерживаемые источники событий	35
С-Терра	49
Шлюз 4.3	49
Перечень правил детектирования	55
Карта покрытия тактик и техник матрицы MITRE ATT&CK правилами детектирования	56
Графики покрытия тактик матрицы MITRE ATT&CK правилами детектирования	57
1С	58
Битрикс24	58
1С:Предприятие Журнал регистрации	61
1С:Предприятие Технологический журнал	68
Ansible	74
AWX	74
Tower	76
Apache	79
Apache Cassandra	79
Apache HTTP Server	82
Bind DNS	87
Cisco	92
Cisco ASA	92
Cisco Firepower 6	94
Citrix	99
Netscaler	99
XenApp	102

Eltex	106
ESR	106
MES	109
Fortinet	113
Fortigate	113
FreeIPA	116
Гарда	119
Гарда DBF	119
Гарда DLP	123
Гарда NDR	131
Гарда WAF	136
Hewlett Packard Enterprise	143
ArubaOS CX	143
Huawei	145
USG	145
Kaspersky	148
Kaspersky Security Center	148
Сбор событий в формате CEF	148
Сбор событий из СУБД MSSQL	150
Сбор событий из СУБД MySQL (Maria DB)	155
Сбор событий из СУБД PostgreSQL	158
Kaspersky Web Traffic Security	161
Kubernetes (K8s)	167
Linux	173
Linux Auditd	173
Системные журналы Linux	177
Microsoft	182
ADDS	182
ADWS	185
IIS	187
SQL Server	189
Windows Sysmon	200
MikroTik	208
RouterOS	208
Nextcloud	214
Nginx	217
OpenBao	220
OpenVPN	223
Oracle	226
MySQL	226
PostgreSQL	231
Positive Technologies	234

Application Firewall v3	234
Application Firewall v4	238
Network Attack Discovery	242
Sandbox	245
R-Vision	248
R-Vision TDP	248
R-Vision TIP	251
Универсальный коннектор CEF	253
Redis Enterprise	258
SberTech (СберTex)	261
Pangolin SE	261
Solar (Солар)	265
Solar Dozor	265
Squid	268
Usergate (Entensys)	271
Usergate UTM	271
VMware	273
ESXi	273
Horizon	277
vCenter	279
Zabbix	283
ИнфоTeKC	290
ViPNet Coordinator 4	290
ViPNet IDS NS	293
ViPNet TIAS	296
Код Безопасности	301
Secret Net LSP	301
Secret Net Studio	305
Континент 4	312
Конфидент	316
Dallas Lock Сервер Безопасности 8.0	316
Сбор событий в формате CEF	316
Сбор событий из СУБД MS SQL	318
Dallas Lock ЕЦУ	334
Сбор событий в формате CEF	335
Сбор событий из СУБД PostgreSQL	338
C-Terra	342
Шлюз 4.3	342

Настоящее руководство содержит рекомендации по подключению элементов IT-инфраструктуры организации к системе R-Vision Security Information and Event Management (далее – "R-Vision SIEM" или "система") для организации сбора событий с различных источников.

Документ включает инструкции по интеграции, настройке и проверке источников событий, а также описывает требования к их конфигурации. Руководство предназначено для специалистов, выполняющих внедрение и настройку R-Vision SIEM в организации.

Информация по релизам

Настройка источников событий в системе R-Vision SIEM обеспечивает сбор и обработку данных для мониторинга и анализа информационной безопасности.

Мы регулярно разрабатываем правила нормализации и корреляции для новых систем. Подробнее с ними можно ознакомиться в наших релизах.



Если у вас есть вопросы по поддерживаемым источникам или запрос на поддержку нового источника, вы можете обратиться в [R-Vision SIEM Community](#).

2025

- [О релизе № 36 от 03.09.2025](#)
- [О релизе № 35 от 20.08.2025](#)
- [О релизе № 34 от 06.08.2025](#)
- [О релизе № 33 от 23.07.2025](#)
- [О релизе № 32 от 09.07.2025](#)
- [О релизе № 31 от 24.06.2025](#)
- [О релизе № 30 от 11.06.2025](#)
- [О релизе № 29 от 04.06.2025](#)
- [О релизе № 28 от 28.05.2025](#)
- [О релизе № 27 от 14.05.2025](#)
- [О релизе № 26 от 30.04.2025](#)
- [О релизе № 25 от 17.04.2025](#)
- [О релизе № 24 от 02.04.2025](#)
- [О релизе № 23 от 18.03.2025](#)
- [О релизе № 22 от 04.03.2025](#)

О релизе № 36 от 03.09.2025

Мы постоянно работаем над расширением экспертизы и ее улучшением для R-Vision SIEM.

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии 2.3.0 и выше.

Кратко о релизе

- Добавили проверку новых индикаторов компрометации ФСТЭК России от 21.08.2025 и от 27.08.2025.
- Скорректировали фильтры в двух правилах детектирования.
- Добавили рекомендации по Incident Response в правила детектирования, которые относятся к

базовому рубрикатору, для источников Windows, Linux, KSC и KSMG.

Правила детектирования

Улучшения и исправления

- **Общее:**
 - Таблица IoC: добавлены новые индикаторы компрометации ФСТЭК России от 21.08.2025 и от 27.08.2025.
- **Microsoft Windows:**
 - Закрепление через Shim: исправлена опечатка в фильтре.
 - В правила добавлены рекомендации по Incident Response.
- **Linux:**
 - Создание интерактивной оболочки через GTFOBins: исключение FP для run-parts.
 - В правила добавлены рекомендации по Incident Response.
- **KSC:**
 - В правила добавлены рекомендации по Incident Response.
- **KSMG:**
 - В правила добавлены рекомендации по Incident Response.

О релизе № 35 от 20.08.2025

Мы постоянно работаем над расширением экспертизы и ее улучшением для R-Vision SIEM.

Кратко о релизе

- Разработали одно новое правило нормализации для источника UserGate MTA.
- Добавили нормализацию для частных событий в правилах Cisco ASA, Cisco IOS, HPE ArubaOS-CX и R-Vision TDP.
- Разработали одно новое правило детектирования для источника VMware vCenter и ESXi.
- Добавили проверку новых индикаторов компрометации ФСТЭК России от 08.08.2025.
- Скорректировали фильтры и провели рефакторинг в ряде правил детектирования.

Правила нормализации

Новые правила

- UserGate MTA: покрытие нормализацией нового источника.

Улучшения и исправления

- Cisco ASA: добавлена обработка события типа ICMP flood.
- Cisco IOS: добавлена обработка множества частных событий.

- HPE ArubaOS-CX: добавлена обработка множества частных событий.
- VMware vCenter и ESXi: выполнена оптимизация элементов кода правила.
- R-Vision TDP: добавлена обработка множества частных событий.

Правила детектирования

Новые правила

- **VMware vCenter и ESXi:**
 - Вызов и выполнение Guest API в гостевой ОС.

Улучшения и исправления

- **Общее:**
 - Таблица IoC: добавлены новые индикаторы компрометации ФСТЭК России от 08.08.2025.
- **Microsoft Windows:**
 - Интерактивный вход под сервисной учетной записью: добавлен активный список для сервисных учетных записей.
 - Создание дампа NTDS.dit: скорректировано описание.
- **Linux:**
 - Разведка установленного ПО в Linux: рефакторинг правила.
- **Atlassian Confluence:**
 - Эксплуатация уязвимости в Confluence — CVE-2023-22518: исправлена тактика в тегах.
- **VMware vCenter и ESXi:**
 - Клонирование нескольких критичных виртуальных машин: доработан data_source.
- **KSC:**
 - Устройство давно не подключалось к серверу KSC: дополнено описание.
- **Eltex vESR:**
 - Успешный подбор пароля к маршрутизатору Eltex vESR: доработан фильтр.
 - Подбор пароля к маршрутизатору Eltex vESR: доработан фильтр.
 - Подбор пароля к маршрутизатору Eltex vESR методом Password Spraying: доработан фильтр.
 - Вход привилегированного пользователя на маршрутизатор Eltex vESR с неизвестного хоста: доработан фильтр.

О релизе № 34 от 06.08.2025

Мы постоянно работаем над расширением экспертизы и ее улучшениям для R-Vision SIEM.

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии 2.3.0 и выше.

Кратко о релизе

- Добавили проверку новых индикаторов компрометации ФСТЭК России от 31.07.2025.
- Скорректировали фильтры и провели рефакторинг в ряде правил детектирования.
- Поддержали нормализацию событий от нового источника: Multifactor - Система многофакторной аутентификации и контроля доступа для любого удалённого подключения
- Внесли исправления и улучшения в правила нормализации

Правила нормализации

Новые правила

- **Multifactor** - Добавлено правило нормализации

Улучшения и исправления

- **Checkpoint NGFW** - исправлен багом с некорректным типом поля deviceTranslatedAddress
- **Xello Deception** - добавлена обработка отрицательных значений
- **MS Windows Security** - актуализирована версия правила
- **MS Windows Security** - внесено исправление в маппинг поля shost события EventId 4768
- **Eltex ESR** - переработка правила под актуальный формат событий источника
- **VMware vCenter** - Добавлена нормализация новых типов событий (управление ролями пользователей)

Правила детектирования

Новые правила

- **Windows:**
 - Создание дампа NTDS.dit
- **KSC:**
 - Устройство давно не подключалось к серверу KSC
- **Linux:**
 - Использование chisel для туннелирования трафика

Улучшения и исправления

- **Общее:**
 - Таблица IoC: добавлены новые индикаторы ФСТЭК России от 31.07.2025.
- **Microsoft Windows:**
 - Добавление файла в директорию расширения браузера: расширен фильтр.
 - Изменение пароля через утилиту mimikatz: добавлен общий фильтр.
 - Использование вредоносных утилит: скорректирован фильтр событий 4103, 4104.

- Порт RDP по умолчанию изменен на нестандартный: скорректирован фильтр.
- Зафиксировано использование WinApi через PowerShell: исправлен блок формирования событий.
- Перечисление учетных записей в домене методом перебора: добавлена проверка принадлежности к контроллерам домена в фильтре, переписано в декларативный формат.
- Изменение критичных параметров сервиса: скорректирован фильтр.
- **Linux:**
 - Использование сетевых утилит Linux для сканирования сети: добавлен общий фильтр.
 - Изменение критичных файлов конфигурации интерактивной оболочки: скорректирован фильтр, добавлено исключение.
 - Использование хакерской утилиты в Linux: добавлен общий фильтр.
- **Atlassian Confluence:**
 - Выполнение OGNL инъекции через Java-выражения в Confluence: исправлен общий фильтр
- **KSC:**
 - Не было удалено обнаруженное средствами AB3 ВПО: убран compact в on_correlate и скорректирован фильтр.

О релизе № 33 от 23.07.2025

Мы постоянно работаем над расширением экспертизы и ее улучшениям для R-Vision SIEM.

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии 2.3.0 и выше.

Кратко о релизе

- Внесли исправления и улучшения в правила нормализации.
- Разработали одно новое правило детектирования для источника VMware ESXi.
- Добавили проверку новых индикаторов компрометации ФСТЭК России от 09.07.2025.
- Скорректировали фильтры и провели рефакторинг в ряде правил детектирования.
- Удалили правило детектирования "Изменение сервисов Linux".

Правила нормализации

Улучшения и исправления

- Xello Deception: добавлена обработка отрицательных значений.
- Security Account Logon: сделан инкремент версии правила.
- Windows Security: скорректировано событие с EventID 4768 (удален shost).

Правила детектирования

Новые правила

- **VMware vCenter и ESXi:**

- Лишение пользователя доступа к ESXi.

Улучшения и исправления

- **Общее:**

- Таблица IoC: добавлены новые индикаторы ФСТЭК России от 09.07.2025.

- **Microsoft Windows:**

- Отключение или модификация Windows Defender: расширен фильтр.
- Отключение ETW провайдера PowerShell: скорректирован фильтр.
- Вход под несуществующим пользователем: добавлен троттлинг.
- Запуск скрипта из временной директории: проведена оптимизация, добавлены исключения.
- Обнаружение стеганографии в Windows: скорректирован data_source.
- Туннелирование с использованием ngrok: скорректирован data_source.
- Удалена глобальная группа с включенной безопасностью: исправлен фильтр.
- Сброс пароля от учетной записи через утилиту mimikatz: добавлен общий фильтр.
- Отключение снапшотов томов: переработана логика правила.
- Защита от записи для хранилища отключена: переработана логика правила.

- **Linux:**

- Изменение критичных файлов Linux: скорректированы теги.
- Добавление/удаление модулей ядра Linux: добавлен общий фильтр.
- Загрузка файла с помощью утилит GTFOBins: добавлена проверка в фильтре.
- Изменение tmp файлов логирования Linux: обновлен фильтр для снижения FP.
- Разведка локальных УЗ в Linux: рефакторинг правила.

- **VMware vCenter и ESXi:**

- Использование утилит ESXi через CLI: расширен фильтр.

- **KSC:**

- Удалено обнаруженное средствами АВЗ ВПО: расширен фильтр.
- Зафиксированы устаревшие базы антивирусного ПО Kaspersky: рефакторинг правила.
- Отключение компонентов защиты продуктов Kaspersky: рефакторинг правила.
- Отключение продукта Kaspersky в результате выполнения задачи: рефакторинг правила.
- Множество хостов заражены одним типом ВПО: перенесено в декларативный формат.
- Множественное срабатывание вердиктов средств АВЗ на одном хосте: перенос в декларативный формат.

- **PostgreSQL:**

- Разведка структуры базы данных PostgreSQL: рефакторинг правила.
- Изменение файла конфигурации базы данных PostgreSQL: рефакторинг правила.

- **JetBrains TeamCity:**

- Скорректировано заполнение поля **data_source** в связи со сменой формата.

- **Atlassian Confluence:**

- Скорректировано заполнение поля **data_source** в связи со сменой формата.

Удаленные правила

- **Linux:**

- Изменение сервисов Linux: логика правила покрывается правилом "Изменение критичных файлов Linux" с помощью событий Auditd по модификации файлов по путям **/etc/systemd** и **/usr/lib/systemd**.

О релизе № 32 от 09.07.2025

Мы постоянно работаем над расширением экспертизы и ее улучшением для R-Vision SIEM.

Кратко о релизе

- Поддержали правилами нормализации новый источник РЕД АДМ (Система централизованного управления ИТ-инфраструктурой от РЕД ОС).
- Доработали правило для Check Point Gaia в части поддержки событий в формате CEF.
- Внесли исправления и улучшения в правила нормализации.
- Разработали семь новых правил детектирования для Microsoft Windows, Linux, MS SQL, VMware vCenter и ESXi. В частности:
 - Покрыли новые техники MITRE ATT&CK сокрытия артефактов Bind Mounts и Extended Attributes:
 - Extended Attributes — это метаданные, которые можно связать с файлами и директориями в файловых системах. Они позволяют пользователям хранить дополнительную информацию о файле, выходящую за рамки стандартных атрибутов, таких как размер файла, временные метки и разрешения. Ранее было замечено, что APT Lazarus использовала технику Extended Attributes для размещения полезной нагрузки в легитимных файлах.
 - Bind Mounts — это метод сокрытия артефактов, который позволяет атакующим скрывать свою активность от системных утилит, создавая ложное представление о выполняющихся процессах. Bind Mounts сопоставляет каталог или файл из одного места файловой системы в другое, аналогично ярлыкам в Windows.
 - Разработали правило детектирования одной из популярных утилит LaZagne, которая также была замечена в различных АРТ-атаках. Данная утилита предназначена для извлечения учетных данных из программного обеспечения на локальном компьютере.
- Добавили проверку новых индикаторов компрометации ФСТЭК России от 26.06.2025 и 03.07.2025.

- Перешли к использованию активного списка для правил, использовавших таблицу обогащения known_DC. Переход с таблицы обогащения на активные списки позволит упростить поддержание актуального списка известных контроллеров домена и обеспечит возможность добавления записей через интерактивный интерфейс. Для корректного перехода требуется перенести всю информацию из таблиц обогащения known_DC в активный лист known_dc, а также заполнить активный лист known_dc_ip известными IP-адресами контроллеров домена для корректной работы правил.
- Провели рефакторинг правил детектирования для Microsoft Windows.
- Внесли многие другие улучшения.

Правила нормализации

Новые правила

- РЕД АДМ: добавлено правило нормализации.

Улучшения и исправления

- Check Point: добавлена обработка событий в формате CEF.
- Linux auth/secure: изменены поля **.cat** и **.act** события типа auth.
- Linux Auditd: скорректировано заполнение поля **outcome** для нескольких событий.
- VMware vCenter и ESXi: добавлена нормализация новых типов событий.

Правила детектирования

Новые правила

- **Microsoft Windows:**
 - Эксплуатация утилиты LaZagne.
 - Эксфильтрация данных через finger.exe.
- **Linux:**
 - Злоупотребление расширенными атрибутами.
 - Аномальное bind-монтирование.
- **MS SQL:**
 - Выгрузка ключа шифрования или сертификата MS SQL.
- **VMware vCenter и ESXi:**
 - Изменение меток времени через touch.
 - Маскировка через переименование/подмену index.html.

Улучшения и исправления

- **Общее:**
 - Таблица IoC: добавлены новые индикаторы ФСТЭК России от 26.06.2025 и 03.07.2025.

• Microsoft Windows:

- Обнаружение HTML/SVG Smuggling в Windows: добавлено обнаружение SVG Smuggling.
- Запуск подозрительного CAB-файла через msdt.exe: расширен фильтр.
- Выполнение команд в системе от редактора кода VS Code: добавлены исключения.
- Вход на устройство под разными учетными записями: перенесено в декларативный формат.
- Удаленное выполнение команд с помощью SMBExec: переведено в декларативный формат.
- Вход под несуществующим пользователем: проведена оптимизация правила.
- Утечка NTLM через library-ms (CVE-2025-24071): таблицы обогащения заменены на активный список.
- Атака DCShadow: таблицы обогащения заменены на активный список.
- Вход на несколько узлов под одной учетной записью: таблицы обогащения заменены на активный список.
- Изменение SPN учетной записи: таблицы обогащения заменены на активный список.
- Компрометация через KrbRelayUp: таблицы обогащения заменены на активный список.
- Использование хакерской утилиты Nishang: добавлены теги.
- Обнаружение стеганографии в Windows: добавлены теги.
- Сжатие дампов-файлов средствами 7Zip: рефакторинг правила.
- Сжатие дампов-файлов средствами WinRAR: рефакторинг правила.
- Использование Replace.exe: рефакторинг правила.
- Получение информации о службе RDP через sc.exe: рефакторинг правила.
- Попытка дампа процесса LSASS с помощью утилиты HandleKatz: рефакторинг правила.
- Атака типа AS-REP Roasting: рефакторинг правила.
- Захват учетных данных с помощью Rpsping.exe: рефакторинг правила.
- Подозрительный снимок базы данных Active Directory средствами ADExplorer: рефакторинг правила.
- Поиск процессов с уязвимыми модулями: рефакторинг правила.
- Подозрительная DDL загружена средствами CertOC.exe: рефакторинг правила.
- Скачивание файлов с IP-адреса через CertOC.exe: рефакторинг правила.
- Установка root-сертификата средствами CertMgr.exe: рефакторинг правила.
- Необычное выполнение приложений через AtBroker.exe: рефакторинг правила.
- Скачивание файлов через IMEWDBLD.exe: рефакторинг правила.
- Новый сертификат root был установлен средствами Certutil.exe: рефакторинг правила.
- Дамп памяти процесса средствами Dotnet-Dump: рефакторинг правила.
- Попытка дампа оперативной памяти с помощью RdrLeakDiag.exe: рефакторинг правила.
- Скачивание файла средствами MpCmpRun.exe: рефакторинг правила.
- Скачивание файлов через msedge_proxu.exe: рефакторинг правила.

- Скачивание файлов через PresentationHost.exe: рефакторинг правила.
- Скачивание файла средствами ProtocolHandler: рефакторинг правила.
- Скачивание файлов через Squirrel.exe: рефакторинг правила.
- Скачивание файлов средствами MS-AppInstaller: рефакторинг правила.
- Подозрительное выполнение Regasm/Regsvcs с нестандартным расширением: рефакторинг правила.
- Дамп памяти ядра через LiveKD: рефакторинг правила.
- Закрепление через ключ реестра ReflectDebugger утилиты WerFault: рефакторинг правила.
- Подозрительный агент обновления Windows: рефакторинг правила.
- Выполнение Sysinternals PsSuspend: рефакторинг правила.
- PowerShell инициировал сетевое подключение: рефакторинг правила.
- Изменение пароля пользователя или хоста с помощью Ksetup.exe: рефакторинг правила.
- Добавление потенциально подозрительного источника загрузки в Winget: рефакторинг правила.
- Извлечение CAB-файлов через Wusa.exe: рефакторинг правила.
- Создание Self Extracting Package в подозрительном месте: рефакторинг правила.
- Экспорт структуры AD через csvde.exe: рефакторинг правила.
- Запуск файла из корзины: рефакторинг правила.
- Изменение атрибутов групповой политики: рефакторинг правила.

- **Linux:**

- Злоупотребление сырыми сокетами: добавлены поля в корреляционное событие.
- Чтение памяти процессов на Linux: добавлены теги.
- Изменение TMP-файлов логирования Linux: добавлены поля в корреляционное событие.
- Большое количество подозрительных команд: перенос в декларативный формат.
- Загрузка файла с помощью утилит GTF0Bins: добавлены поля в корреляционное событие.

- **KSC:**

- Перемещение устройства в группу администрирования на сервере KSC: корректировка корреляционной карточки.

- **VMware vCenter и ESXi:**

- Доступ к критичным файлам на сервере vCenter: добавлены теги техник MITRE ATT&CK для ESXi.

- **Cisco IOS:**

- Скорректировано заполнение поля **data_source** в связи со сменой формата.

- **Cisco ASA:**

- Скорректировано заполнение поля **data_source** в связи со сменой формата.

- **Secret Net Studio:**

- Скорректировано заполнение поля **data_source** в связи со сменой формата.

О релизе № 31 от 24.06.2025

Мы постоянно работаем над расширением экспертизы и ее улучшениям для R-Vision SIEM.

Кратко о релизе

- Добавили проверку новых индикаторов компрометации ФСТЭК России от 11.06.2025 и 19.06.2025.
- Перенесли часть правил детектирования из императивного в декларативный формат.
- Провели корректировку правил детектирования для снижения ложноположительных срабатываний и поддержания работоспособности правил в условиях изменившейся нормализации.
- Проведен рефакторинг правил детектирования на основе Sysmon-журнала.

Правила нормализации

Новые правила

- Kaspersky EDR: добавлено правило нормализации.
- macOS R-Point: покрыта нормализация событий нового агента R-Vision EVO для macOS.

Улучшения и исправления

- Linux Auditd: исправлено поле **outcome**.

Правила детектирования

Улучшения и исправления

- **Общее:**
 - Таблица IoC: добавлены новые индикаторы ФСТЭК РОССИИ от 11.06.2025 и 19.06.2025.
- **Microsoft Windows:**
 - Подозрительная модификация ключей реестра COM/WMI: расширен фильтр.
 - Несистемный процесс повысил привилегии до системных (CreateProcessWithToken): правило перенесено в декларативный формат.
 - Вход с разных хостов на один хост под одной учетной записью: правило перенесено в декларативный формат, предусмотрен список исключений.
 - Удаленный запуск процесса с помощью WMI: правило перенесено в декларативный формат.
 - Создание и удаление учетной записи в течении одной минуты: правило перенесено в декларативный формат.
 - Множественные неудачные попытки аутентификации учетной записи: правило перенесено в декларативный формат.

- Атака Password Spraying: правило перенесено в декларативный формат.
- Обход UAC с помощью реестра: усовершенствована логика правила.
- Создание сетевого подключения процессом Winlogon: рефакторинг правила.
- Подозрительный доступ к памяти процесса LSASS: рефакторинг правила.
- Кража токена через именованные каналы: рефакторинг правила.
- Кража токена доступа из системного процесса: рефакторинг правила.
- Дамп LSASS с помощью Python-утилит: рефакторинг правила.
- Создание токена и имперсонация учетной записи: скорректирован фильтр.
- Запуск множества подозрительных команд: скорректирован фильтр.
- Использование утилиты Smbtakeover: корректировка под изменения в нормализации.
- Отключение ETW провайдера PowerShell: скорректирован фильтр.
- Изменения в планировщике задач: замена таблицы обогащения на активный список.
- Зафиксирована подгрузка подозрительного пакета процессом LSA: скорректирован фильтр.
- Удаление временных RDP файлов в Windows: скорректирован фильтр.
- Отключение или модификация Windows Defender: корректировка в соответствии с измененной нормализацией.
- Отключение ETW провайдера Windows Defender: корректировка в соответствии с измененной нормализацией.
- Ослабление защиты или мониторинга системы: корректировка в соответствии с измененной нормализацией.
- Зафиксировано изучение общих сетевых ресурсов: корректировка в соответствии с измененной нормализацией.
- Подключение к SMB папке по протоколу QUIC: корректировка в соответствии с измененной нормализацией.
- Отключение службы Windows EventLog: корректировка в соответствии с измененной нормализацией.
- Перечисление ключей реестра для разведки: корректировка в соответствии с измененной нормализацией.
- Изучение конфигурации локальной системы: корректировка в соответствии с измененной нормализацией.
- Получение учетных данных из реестра: корректировка в соответствии с измененной нормализацией.
- Очистка истории команда PowerShell в Windows: корректировка в соответствии с измененной нормализацией.
- Изменение политик Windows Defender Firewall: корректировка в соответствии с измененной нормализацией.
- Отключение ETW провайдера .NET: корректировка в соответствии с измененной нормализацией.
- Отключение логирования событий IIS: корректировка в соответствии с измененной нормализацией.

нормализацией.

- Запуск PowerShell окна в скрытом режиме: корректировка в соответствии с измененной нормализацией.
- Сбор информации о сетевых подключениях: корректировка в соответствии с измененной нормализацией.
- Зафиксировано изучение системного времени: корректировка в соответствии с измененной нормализацией.
- Использование вредоносных утилит: корректировка в соответствии с измененной нормализацией.
- Уничтожение информации на диске в Windows: корректировка в соответствии с измененной нормализацией.
- Зафиксировано добавление исполняемого файла к профилю PowerShell: корректировка в соответствии с измененной нормализацией.

- **Linux:**

- Изменение задач cron: добавлено исключение пакетных менеджеров.
- Изменение критичных файлов Linux: добавлена проверка процесса для уменьшения ложноположительных сработок.
- Изменение критичных файлов конфигурации интерактивной оболочки: рефакторинг правила.

- **OpenVPN:**

- Множество неуспешных HTTP-запросов к OpenVPN AS: исправлена обработка ошибок.
- Аномальный HTTP-запрос к webUI Access Server: исправлена обработка ошибок.

- **Kaspersky Secure Mail Gateway:**

- Получение спам-письма: скорректированы техники.
- Вредоносная ссылка в письме: скорректированы техники.
- Получение массовой рассылки писем: скорректированы техники.
- Вредоносное вложение в письме: скорректированы техники.
- Проверка подлинности отправителя сообщений: скорректированы техники.
- Шифрованное вложение в письме: скорректированы техники.

О релизе № 30 от 11.06.2025

Мы постоянно работаем над расширением экспертизы и ее улучшением для R-Vision SIEM.

Кратко о релизе

- Добавили проверку новых индикаторов компрометации ФСТЭК от 06.06.2025.
- Выпустили базовый набор правил детектирования для MySQL.
- Расширили покрытие Kubernetes и MS SQL.
- Включили в пакет экспертизы схемы типовых дашбордов.

- Внесли улучшения и исправления в правила нормализации для ранее поддерживаемых источников.

Правила нормализации

Новые правила

Дашборды: в релиз включены дашборды, доступные для импорта из пака экспертизы.

Улучшения и исправления

- Linux и Windows: внесены небольшие исправления в правила.
- Cisco IOS XE: доработана нормализация событий, исправлен маппинг полей.
- Microsoft SQL Server: добавлена обработка новых типов событий Backup Service Master Key.
- OpenVPN: добавлена обработка новых типов событий.

Правила детектирования

Новые правила

- **Kubernetes:**
 - Назначение сервисного аккаунта контейнеру в kube-system.
 - Создание контейнера с Linux Capabilities.
 - Создание привилегированного пода k8s.
- **MS SQL:**
 - Поиск резервных копий базы данных.
 - Использование хранимых процедур sp_proxу и sp_grant_proxу.
- **VMware vCenter и ESXi:**
 - Доступ к критичным файлам на сервере ESXi.
 - Удаление или отключение логирования команд.
- **MySQL:**
 - Создание резервной копии MySQL.
 - Изменение пароля учетной записи MySQL.
 - Просмотр пользовательских данных MySQL.
 - Получение списка подключений к MySQL.
 - Остановка сессии пользователя в MySQL.
 - Удаление базы данных в MySQL.
 - Назначение прав администратора MySQL.
 - Массовое удаление таблиц MySQL.
 - Получение информации о версии MySQL.
 - Изменение\удаление таблицы аудита MySQL.

Улучшения и исправления

- **Общее:**
 - Таблица IoC: добавлены новые индикаторы от ФСТЭК.
- **Kubernetes:**
 - Создание сервисного аккаунта k8s: скорректированы техники.
- **MySQL:**
 - Корректировка поля datasource: исправлено для источника MySQL.
 - Список критичных сервисов Linux систем: добавлен сервис MySQL.
 - Изменение критичных файлов Linux: добавлен файл конфигурации MySQL.
- **MS SQL:**
 - Вход привилегированного пользователя в Microsoft SQL Server: исправлена опечатка.

О релизе № 29 от 04.06.2025

Мы постоянно работаем над расширением экспертизы и ее улучшением для R-Vision SIEM.

Кратко о релизе

Внесли исправления в правила нормализации для обеспечения совместимости пака экспертизы с SIEM версии 2.3.0 и выше.

Правила нормализации

Улучшения и исправления

- Windows, Linux Audit, Jira: исправлены правила нормализации для обеспечения совместимости с SIEM версии 2.3.0.
- Microsoft ADDS: исправлено поле dproduct.
- Check Point: внесены небольшие исправления и улучшения.
- Windows Sysmon: исправлен вызов глобальной функции в правиле.

О релизе № 28 от 28.05.2025

Мы постоянно работаем над расширением экспертизы и ее улучшением для R-Vision SIEM.

Кратко о релизе

- Выпустили новое правило детектирования по распространению и проверке индикаторов компрометации от ФСТЭК.
- Провели корректировку правил детектирования для снижения ложноположительных срабатываний и поддержания работоспособности правил в условиях изменившейся нормализации.
- Внесли улучшения и исправления в правила нормализации для ранее поддерживаемых источников.

Правила нормализации

Улучшения и исправления

- VMware ESXi: доработано правило, внесены исправления в нормализацию событий.
- Huawei USG: внесены исправления в таблицу обогащения событий Huawei USG.
- Check Point: добавлены поля status и deviceTranslatedAddress.
- Linux Auth, R-Point, Auditd: изменено поле act для событий USER_LOGIN.
- Linux Auditd: добавлено условие обработки spid и dpid.
- Windows Security: адаптированы правила для работы с агентом R-Vision Endpoint.
- VMware vCenter: изменена логика парсинга событий журнала vpxd.

Правила детектирования

Новые правила

- Вышло универсальное правило для проверки индикаторов компрометации, предоставленных ФСТЭК.
 - Обнаружен индикатор компрометации.

Улучшения и исправления

- **Microsoft Windows:**
 - Добавление пользователя в критичные локальные группы: скорректировано в соответствии с измененной нормализацией.
 - Попытка дампа процесса LSASS с помощью утилиты ProcDump: скорректирован фильтр для снижения ложноположительных срабатываний.
 - Использование вредоносных утилит: скорректирован фильтр для снижения ложноположительных срабатываний.
 - Запуск файла без расширения: добавлена фильтрация по журналу событий.
 - Установка ПО для удаленного доступа: добавлен новый тег.
 - Удаленное подключение к узлу через туннелирование в VSCode: добавлен новый тег.
 - Возможность использования обфускации PowerShell: добавлен новый тег.
 - Запуск интерпретатора командной строки от WinRAR: добавлен новый тег.
 - Добавление файла в директорию расширения браузера: добавлен новый тег.
 - Добавление расширения в браузер средством CLI: добавлен новый тег.
 - Выполнение команд в системе от редактора кода VSCode: добавлен новый тег.
 - Атака Bad USB Windows: добавлен новый тег.
 - Добавление пользователя в критичные доменные группы: в список критичных добавлена группа ESX Admins.
 - Возможность использования WinAPI через PowerShell: проведен рефакторинг правила.

- **Linux:**

- Создание/изменение правила nf_tables: добавлено исключение для системного пользователя.
- Загрузка кода в процесс Linux: изменен фильтр для снижения ложноположительных срабатываний.
- Успешный подбор пароля на хосте Linux: добавлена группировка по cat.
- Подбор пароля на хосте Linux: скорректировано правило в соответствии с обновленной нормализацией.
- Подбор пароля пользователя Linux: скорректировано правило в соответствии с обновленной нормализацией.
- Успешный подбор пароля пользователя Linux: скорректировано правило в соответствии с обновленной нормализацией.
- Изменение сервисов Linux: добавлен новый тег.
- Добавление файла в расширения браузера Linux: добавлен новый тег.
- Добавление расширения в браузер через CLI Linux: добавлен новый тег.
- Загрузка файла с помощью утилит GTF0Bins: обновлена логика правила.

- **KSC:**

- Отключение задачи средств AV-защиты Kaspersky: исключены обновления.
- Подключение недоверенного устройства: добавлен новый тег.

- **FreeIPA:**

- Добавление HBAC-правила через FreeIPA: проведен рефакторинг правила.

- **VMware vCenter и ESXi:**

- Использование утилит ESXi через CLI: дополнен фильтр проверки esxcli.
- Использование find в ESXi: добавлены теги техник MITRE для ESXi.
- Эксплуатация уязвимости CVE-2021-21972 на сервере vCenter: добавлены теги техник MITRE для ESXi.
- Обнаружение уязвимой конфигурации ESXi: добавлены теги техник MITRE для ESXi.
- Доступ к критичным файлам на сервере vCenter: добавлены теги техник MITRE для ESXi.
- Эксплуатация уязвимости CVE-2021-22005 на сервере vCenter: добавлены теги техник MITRE для ESXi.
- Создание ssh-туннелей на ESXi: добавлены теги техник MITRE для ESXi.
- Обнаружение атаки Password Spraying: добавлены теги техник MITRE для ESXi.
- Выгрузка нескольких файлов с критичной виртуальной машины: скорректировано в соответствии с измененной нормализацией.
- Выгрузка файла с критичной виртуальной машины: скорректировано в соответствии с измененной нормализацией.
- Изменение конфигурации критичной виртуальной машины: скорректировано в соответствии с измененной нормализацией.

- Изменение конфигурации нескольких критичных виртуальных машин: скорректировано в соответствии с измененной нормализацией.
- Изменение аудита виртуальной инфраструктуры: скорректировано в соответствии с измененной нормализацией.
- Удаление критичной виртуальной машины: скорректировано в соответствии с измененной нормализацией.
- Клонирование критичной виртуальной машины: скорректировано в соответствии с измененной нормализацией.
- Клонирование нескольких критичных виртуальных машин: скорректировано в соответствии с измененной нормализацией.
- Отключение критичной виртуальной машины: скорректировано в соответствии с измененной нормализацией.
- Отключение нескольких критичных виртуальных машин: скорректировано в соответствии с измененной нормализацией.
- Создание множества виртуальных машин: скорректировано в соответствии с измененной нормализацией.
- Удаление нескольких критичных виртуальных машин: скорректировано в соответствии с измененной нормализацией.

• Гарда WAF:

- Множественная атака на веб-приложение Гарда WAF: скорректировано в соответствии с измененной нормализацией.
- Множественные атаки на веб-приложение Гарда WAF: скорректировано в соответствии с измененной нормализацией.
- Атака на веб-приложение Гарда WAF: скорректировано в соответствии с измененной нормализацией.
- Подбор пароля пользователя к Гарда WAF: скорректировано в соответствии с измененной нормализацией.
- Успешный подбор пароля к Гарда WAF: скорректировано в соответствии с измененной нормализацией.

О релизе № 27 от 14.05.2025

Мы постоянно работаем над расширением и улучшением экспертизы для R-Vision SIEM.

Кратко о релизе

- В рамках данного релиза были внесены изменения в правила нормализации для обеспечения совместимости пака с R-Vision SIEM версии 2.3.0. Обновления включают исправление типов данных и глобальных функций, а также улучшение и исправление правил для ранее поддерживаемых источников.
- Разработали 31 новое правило детектирования для Microsoft Windows, Oracle DB, MS SQL, BIND, Garda WAF и VMware vCenter и ESXi. В частности:

- покрыли использование утилиты для создания туннелей из интернета в локальную сеть LocaltoNet. Данная утилита активно используется атакующими. Например, APT Morlock компрометировали IT-подрядчиков для последующего проникновения к жертве, используя LocaltoNet в качестве закрепления.
- покрыли уязвимость CVE-2025-24071, которая связана с механизмом обработки файлов в Windows Explorer. Это позволяет получить хэш NTLMv2 учетной записи в результате некорректной обработки файлов .library-ms.
- реализовали новые правила для детектирования злоупотребления ssh.exe, например, создания туннелей, кражи NTLM-хэша, выполнения команд без явного подключения к удаленному серверу. Известно, что группировка ToddyCat использовала ssh.exe в качестве инструмента для туннелирования трафика.

Правила нормализации

Улучшения и исправления

- UserGate: исправлена нормализация событий NAT.
- MikroTik: добавлена поддержка новых типов событий.
- Garda WAF: исправлено значение поля outcome для события блокировки пользователя.
- Passbolt: убраны отладочные поля test, добавлено приведение к типу.
- Linux Auth: обновлена обработка событий ошибок.
- Глобальные функции: исправлена проблема совместимости с SIEM 2.3.0.
- Atlassian Jira: обновлены правила нормализации для совместимости с SIEM 2.3.0.
- Windows Security: обновлены правила нормализации для совместимости с SIEM 2.3.0.
- Linux Audit: обновлены правила нормализации для совместимости с SIEM 2.3.0.
- Linux Rpoint: исправлен путь журналов для совместимости с новым агентом.

Правила детектирования

Новые правила

- **Microsoft Windows:**
 - Запуск ssh.exe с подозрительными параметрами.
 - Создание обратного туннеля через ssh.exe.
 - Использование ssh.exe для кражи NTLM-хэша.
 - Подозрительные DNS-запросы к LocaltoNet домену.
 - Обход UAC через COM-объекты.
 - Обнаружение эксплуатации DDE через Office.
 - Изменение доверительных отношений между доменами.
 - Прямой доступ к диску через PowerShell.
 - Сжатие файлов средствами PowerShell.

- Использование средств виртуализации.
- Утечка NTLM через library-ms (CVE-2025-24071).

- **Oracle DB:**

- Поиск информации о конфигурации OracleDB.
- Поиск информации о структуре в OracleDB.
- Вход привилегированного пользователя в СУБД Oracle.
- Успешный подбор пароля к СУБД Oracle.
- Получение информации о пользователях СУБД Oracle.
- Манипуляция с учетными данными СУБД Oracle.
- Подбор пароля к СУБД Oracle.
- Атака Password Spraying на OracleDB.
- Экспорт базы данных Oracle.

- **MS SQL:**

- Попытка подключения к СУБД через DAC.
- Попытка получить состояние службы Windows.
- Попытка изменить состояние службы Windows.
- Запись ключа реестра средствами MS SQL.
- Чтение ключа реестра средствами MS SQL.
- Отправка результатов SQL-запроса почтой.
- Использование процедур для локального выполнения кода.

- **BIND:**

- Обнаружение DNS-запроса к домену LocaltoNet.

- **Garda WAF:**

- Массовое удаление УЗ Garda WAF.
- Изменение настроек защиты подключенного сервера.

- **VMware vCenter и ESXi:**

- Использование chmod в ESXi через CLI.

Улучшения и исправления

- **Linux:**

- Размещение архивов в сетевой папке Linux: обновлено поле data_source, скорректирован фильтр.

О релизе № 26 от 30.04.2025

Мы постоянно работаем над расширением и улучшением экспертизы для R-Vision SIEM.

Кратко о релизе

В части правил детектирования провели рефакторинг, скорректировали фильтры и исключения для уменьшения ложно-положительных срабатываний, перевели правила для KSC на новый формат data_source.

Разработали правила нормализации для нового источника: Huawei USG. Внесли исправления и улучшения в существующие правила нормализации.

Правила нормализации

Новые правила

- Huawei USG: покрытие нового источника.

Улучшения и исправления

- Redis: исправлено наименование правила.
- Garda WAF: исправлено наименование вендора в поле dvendor.
- Garda DBF: исправлено наименование вендора в поле dvendor.
- Garda DLP: исправлено наименование вендора в поле dvendor.
- Garda NDR: исправлено наименование вендора в поле dvendor.
- ViPNet IDS: исправлено заполнение поля severity.
- Microsoft Windows Security: внесены небольшие исправления в правило.
- KSC: исправлено заполнение полей duser, suser с двумя и более пользователями в событиях KES.
- Bitrix24: внесены небольшие исправления.
- Aurora Center: исправлено заполнение поля outcome.
- Auditd: добавлено декодирование полей dproc, fname при записи значений в HEX-формате.

Правила детектирования

Новые правила

- **Microsoft Windows**

Улучшения и исправления

- **Microsoft Windows:**
 - Структура AD была экспортирована средствами Ldifde.exe: рефакторинг правила.
 - Манипулирование запланированными задачами через реестр: рефакторинг правила.
 - Включение или отключение учетной записи: рефакторинг правила.
 - Включение переменных среды COR Profiler: рефакторинг правила.
 - Запуск файла без расширения: корректировка фильтра.
 - Вход под учетной записью администратора: добавлен активный список.

- Возможно успешный подбор пароля пользователя: перенос в декларативный формат.
- Вход на несколько узлов под одной учетной записью: перенос в декларативный формат.

• **Linux:**

- Изменение файлов в домашнем каталоге другим пользователем: скорректирован фильтр.
- Модификация файлов MOTD в Linux: добавление исключений.
- Изменение критичных файлов конфигурации интерактивной оболочки: добавление исключений.
- Закрепление при помощи утилиты Trap: рефакторинг правила.
- Остановка критичных сервисов в Linux: рефакторинг правила.
- Разведка доменных УЗ в Linux: рефакторинг правила.
- Изменение tmp файлов логирования Linux: добавление исключений.
- Загрузка файла сервисной учетной записью: корректировка фильтра.
- Отключение или модификация Syslog Linux: корректировка фильтра.
- Копирование стандартных исполняемых файлов (маскарадинг утилит): добавление исключений.
- Чтение файлов с пользовательскими учетными данными: добавление исключений.
- Обнаружена команда reverse/bind shell: корректировка фильтра.
- Успешный подбор пароля пользователя Linux: правило совместимо с secure журналом.
- Подбор пароля пользователя Linux: правило совместимо с secure журналом.
- Успешный подбор пароля на хосте Linux: правило совместимо с secure журналом.
- Подбор пароля на хосте Linux: правило совместимо с secure журналом.
- Создание и удаление учетной записи в короткий период времени: правило совместимо с secure журналом.
- Создание пользователя или группы: правило совместимо с secure журналом.

• **KSC:**

- Общее: новый формат datasource для всех правил KSC.
- Зафиксирован переход по опасной ссылке: добавлен троттлинг.

• **FreeIPA:**

- Изменение оболочки входа средствами FreeIPA: рефакторинг правила.
- Подбор пароля пользователя FreeIPA: рефакторинг правила.

• **VMware vCenter и ESXi:**

- Эксплуатация уязвимости CVE-2021-21972 на сервере vCenter: актуализирован data_source.

Удаленные правила

• **Linux:**

- Дамп учетных записей Linux: логика правила покрывается правилом "Чтение файлов с пользовательскими учетными данными".

О релизе № 25 от 17.04.2025

Мы постоянно работаем над расширением и улучшением экспертизы для R-Vision SIEM.

Кратко о релизе

- Разработали 31 новое правило детектирования для Microsoft Windows, Linux, Garda WAF, MS SQL, VMware vCenter and ESXi.
- В 133 правилах детектирования для Windows убрано множественное экранирование. Теперь информация в правилах лучше воспринимается, а правила становятся совместимы с различными сборщиками и транспортом событий в SIEM.
- В существующих правилах для VMware vCenter поддержали VMware ESXi.
- Разработали правила нормализации для двух новых источников: Microsoft ADDS, Garda DLP
- Внесли исправления и улучшения для существующих правил нормализации

Правила нормализации

Новые правила

- **Microsoft ADDS**
- **Нормализация Garda DLP**

Улучшения и исправления

- **Microsoft Security и System** - Убрано некорректное экранирование символа "\" в событиях
- **Garda WAF** - Скорректирована запись наименования роли в поля события
- **Garda Monitor** - Внесены небольшие исправления
- **Linux Auditd** - Добавлено поле ses в sourceSessionId
- **PT ISIM** - Расширен перечень обрабатываемых типов событий
- **Контент 4** - Исправлены типы данных для корректной записи в поля нормализованного события
- **WinLogBeat** - Убрано некорректное экранирование символа "\" в событиях
- **1C** - Внесены небольшие исправления
- **KSC** - Исправлено заполнение поля .user в событиях редактирования групп

Правила детектирования

Новые правила

- **Microsoft Windows:**
 - Добавление файла в директорию расширения браузера
 - Добавление расширения в браузер средством CLI
- **Linux:**

- Добавление расширения в браузер средством CLI Linux
- Добавление файла в расширения браузера Linux

- **Garda WAF:**

- Добавление пользователю критичной роли Garda WAF
- Множественные атаки на веб-приложение Garda WAF
- Атака на веб-приложение Garda WAF
- Множественная атака на веб-приложение Garda WAF
- Отключение или изменение паттерна Garda WAF
- Подбор пароля пользователя к Garda WAF
- Успешный подбор пароля к Garda WAF
- Атака Password Spraying к Garda WAF

- **MS SQL:**

- Создание резервных копий MSSQL средствами PowerShell
- Включение небезопасных параметров в конфигурации MSSQL
- Отключение политики входа пользователей MS SQL
- Установка небезопасного свойства MS SQL
- Попытка включить смешанную аутентификацию MS SQL
- Получение информации об алгоритме шифрования БД
- Получение информации о пользователях ОС
- Доступ к локальной файловой системе MSSQL
- Поиск пользователей с административными правами в MSSQL
- Получение информации о пользователях MSSQL
- Получение информации о версии MSSQL
- Получение информации о привилегиях пользователя MSSQL
- Получение хеша пароля пользователей MSSQL

- **VMware vCenter и ESXi:**

- Обнаружение уязвимой конфигурации ESXi
- Использование утилит ESXi через CLI
- Использование find в ESXi
- Создание ssh-туннелей на ESXi
- Остановка критичного сервиса ESXi

- **Kaspersky Endpoint Security:**

- Подключение недоверенного устройства

Улучшения и исправления

- **Microsoft Windows:**

- В 133 правилах детектирования для Windows убрано множественное экранирование.

- **VMware vCenter and ESXi:**

- Клонирование нескольких критичных виртуальных машин - актуализирован data_source.
- Клонирование критичной виртуальной машины - актуализирован data_source.
- Эксплуатация уязвимости CVE-2021-22005 на сервере vCenter - актуализирован data_source.
- Доступ к критичным файлам на сервере vCenter - актуализирован data_source.
- Изменена конфигурация критичной виртуальной машины - поддержан ESXi.
- Выгрузка нескольких файлов с критичной виртуальной машины - поддержан ESXi.
- Изменена конфигурация нескольких критичных виртуальных машин - поддержан ESXi.
- Выгрузка файла с критичной виртуальной машины - поддержан ESXi.
- Обнаружена атака Password Spraying - поддержан ESXi.
- Возможно успешный подбор пароля пользователя на VMware - поддержан ESXi.
- Множественные неуспешные попытки аутентификации пользователя - поддержан ESXi.
- Вход под привилегированной учетной записью с неизвестного хоста - поддержан ESXi.
- Изменение аудита виртуальной инфраструктуры - актуализирован data_source.
- Отключено несколько критичных виртуальных машин - поддержан ESXi.
- Отключена критичная виртуальная машина - поддержали ESXi.
- Удалено несколько критичных виртуальных машин - поддержан ESXi.
- Удалена критичная виртуальная машина - shost заменен на dhost.
- Создание множества виртуальных машин - shost заменен на dhost.

О релизе № 24 от 02.04.2025

Мы постоянно работаем над расширением экспертизы и ее улучшениям для R-Vision SIEM.

Кратко о релизе

- В правилах детектирования брутфорса и манипуляции с пользователями на Linux поддержали журналы auth.log и Auditd.
- Правила Windows перевели на новый формат data_source.
- Разработали правила нормализации для двух новых источников: Континент 4, Linux auth.log.
- Внесли улучшения для уже существующих правил нормализации и детектирования.

Правила нормализации

Новые источники

- **Континент 4:** нормализация событий из БД (PgSQL).
- **Linux:** покрытие журнала auth.log.

Улучшения и исправления

- **Garda WAF:** добавлена обработка событий ролей.
- **PTAFv3:** исправлен маппинг поля request.
- **Windows Sysmon:** оптимизирован фильтр событий.
- **PT Sandbox:** оптимизирован парсинг событий с учетом формата.
- **Garda Monitor:** добавлена нормализация событий из системных журналов.

Правила детектирования

Улучшения и исправления

- **Microsoft Windows:**
 - Скорректировано заполнение поля **data_source** в связи со сменой формата.
- **Linux:**
 - Создание пользователя или группы — поддерживаны auth.log и auditd.
 - Создание и удаление учетных записей в короткий период времени — поддерживаны auth.log и auditd.
 - Успешный подбор пароля на хосте Linux — поддерживаны auth.log и auditd.
 - Подбор пароля на хосте Linux — поддерживаны auth.log и auditd.
 - Успешный подбор пароля пользователя Linux — поддерживаны auth.log и auditd.
 - Подбор пароля пользователя Linux — поддерживаны auth.log и auditd.

О релизе № 23 от 18.03.2025

Мы постоянно работаем над расширением экспертизы и ее улучшениям для R-Vision SIEM.

Кратко о релизе

- Разработали правила нормализации для 2 новых источников: NextCloud, Kaspersky CyberTrace.
- Разработали 14 правил детектирования для KSMG, OpenVPN.
- Внесли улучшения для уже существующих правил нормализации и детектирования.

Правила нормализации

Новые источники

- NextCloud
- Kaspersky CyberTrace

Улучшения и исправления

- Linux Auditd

- Kaspersky Security Center (KSC)
- Kaspersky Secure Mail Gateway (KSMG)
- Garda WAF - Добавлено поле
- OpenVPN

Правила детектирования

Новые правила

- **Kaspersky Secure Mail Gateway (KSMG):**
 - Вредоносное вложение в письме
 - Вредоносная ссылка в письме
 - Проверка подлинности отправителей сообщений
 - Получение массовой рассылки писем
 - Получение спам-письма
 - Шифрованное вложение в письме
- **OpenVPN:**
 - Подключение OpenVPN за пределами России
 - Подбор пароля в веб-консоль OpenVPN AS
 - Успешный подбор пароля клиента OpenVPN
 - Подбор пароля клиента OpenVPN
 - Множество неуспешных HTTP-запросов к OpenVPN AS
 - Доступ к файлу с ключами и сертификатами OpenVPN
 - Изменение конфигурации OpenVPN
 - Аномальный HTTP-запрос к webUI

Улучшения и исправления

- **Microsoft Windows:**
 - Использование утилит для создания снимков экрана - уменьшение количества ложноположительных срабатываний.
- **KSC:**
 - Повторное заражение хоста одним вирусом - переведено в декларативный формат

О релизе № 22 от 04.03.2025

Мы постоянно работаем над расширением экспертизы и ее улучшениям для R-Vision SIEM.

Кратко о релизе

- Разработали правила нормализации для 2 новых источников: OpenVPN Access Server, Microsoft

AD DS.

- Разработали 15 правил детектирования для Kubernetes, Microsoft SQL Server, 7-Zip, JetBrains TeamCity, Microsoft Windows (выявление способов повышения привилегий).
- Внесли улучшения для уже существующих правил нормализации и детектирования.

Правила нормализации

Новые источники

- OpenVPN Access Server
- Microsoft AD DS

Улучшения и исправления

- R-Point
- CyberPeak
- Linux Auditd
- Garda WAF
- Garda Monitor
- Bitrix24
- Microsoft Sysmon
- Microsoft Windows Powershell
- OracleDB
- Kaspersky Security Center (KSC)
- Kaspersky Secure Mail Gateway (KSMG)

Правила детектирования

Новые правила

- **Microsoft Windows:**
 - Удаленное выполнение команд с помощью PsExec
 - Эксплуатация Mark-of-the-Web bypass
 - Изменение SID-History
 - Запуск процесса от другого пользователя
 - Подмена PID родительского процесса
- **JetBrains TeamCity:**
 - Эксплуатация CVE-2023-42793 в JetBrains TeamCity
- **Linux:**
 - Отключение мандатного контроля целостности
- **Microsoft SQL Server:**

- Изменение пароля привилегированной УЗ MS SQL Server
- Назначена роль администратора пользователю MS SQL Server
- Удаление базы данных в MS SQL Server
- Удаление нескольких таблиц в MS SQL Server
- Создание резервной копии БД MS SQL Server
- Получение информации об аудите MS SQL Server
- Изменение аудита базы данных MS SQL Server

- **Kubernetes:**

- Запуск интерактивной оболочки в контейнере

Улучшения и исправления

- **Общее:**

- Скорректировано заполнение поля **data_source** в связи со сменой формата.

- **Microsoft Windows:**

- Чтение Ticket CCACHE файла - оптимизация правила
- Успешный подбор пароля пользователя FreeIPA - оптимизация правила
- Закрепление через Shim - уменьшение количества ложноположительных срабатываний.
- Поиск данных в сетевых папках Windows - уменьшение количества ложноположительных срабатываний.
- Доступ к чувствительному сетевому диску Windows - уменьшение количества ложноположительных срабатываний.
- Запуск файла без расширения - уменьшение количества ложноположительных срабатываний.
- Журнал событий Windows был очищен - скорректировано уведомление.
- Отключение или модификация Windows Audit Log Policy - оптимизация правила.

- **KSC:**

- Повторное заражение хоста одним вирусом - переведено в декларативный формат

Поддерживаемые источники событий

Данная таблица содержит список информационных систем, из которых в SIEM поступают события. Для указанных источников разработаны правила нормализации.

Вендор	Продукт	Версия	Класс	Тип подключения	ID правила нормализации	Комментарий
R-Vision	Universal CEF	-	-	Syslog	RV-N-18	Правило нормализации для сбора и обработки событий в формате ArcSight CEF. Используется для всех источников перечня с типом подключения "Universal CEF".
1C	Битрикс24	24	Application	DB(MySQL)	RV-N-3	
1C	Предприятие	8.3	ERP	Агент R-Vision Endpoint Скрипт	RV-N-1 RV-N-2	
АйТи Бастион	СКДПУ НТ Мониторинг и аналитика	-	PAM	Universal CEF	RV-N-18	
Астра	ALD Pro	2.0.0	LDAP	Syslog	RV-N-38 RV-N-39 RV-N-40 RV-N-41	
Астра	Astra Linux	1.7	OS	Агент R-Vision Endpoint	RV-N-57	
Атом Безопасность	StaffCop	5.5	DLP	Syslog CEF	RV-N-118	

Вендор	Продукт	Версия	Класс	Тип подключения	ID правила нормализации	Комментарий
Гарда	Гарда Монитор (NDR)	4	NDR	Syslog CEF	RV-N-163	
Гарда	Гарда DBF	5	DBF	Syslog CEF	RV-N-138	
Гарда	Гарда DLP	1.0	DLP	Syslog	RV-N-171	
Гарда	Гарда WAF	2.4	WAF	DB (PostgreSQL)	RV-N-144	
ИнфоТеКс	ViPNet IDS NS	3.10	IDS	Syslog CEF	RV-N-145	
ИнфоТеКс	ViPNet TIAS	3.10	TI (IDS Center)	Syslog CEF	RV-N-146	
Конфидент	Dallas Lock ЕЦУ	2	AM	Syslog DB (PostgreSQL)	RV-N-133 RV-N-135	
Конфидент	Dallas Lock СБ	8 10	AM	Syslog DB (MSSQL)	RV-N-134 RV-N-135	
Открытая Мобильная Платформа	Аврора Центр	5	Application	DB(PostgreSQL)	RV-N-162	
Ред Софт	RedOS	7	OS	Агент R-Vision Endpoint	RV-N-57	
Сайберпик	Спектр	3.5		Syslog CEF	RV-N-141	
Солар	Solar Dozor	7 8	DLP	Syslog	RV-N-113	
Солар	Solar inRights	3	IDM	Syslog	RV-N-114	
Солар	Solar webProxy	4.1	DLP	Syslog	RV-N-115 RV-N-116	
AhnLabs	Absolute Data and Device Security (DDS)	-	DLP	Universal CEF	RV-N-18	
AhnLabs	AhnLab Malware Defense System (MDS)	-	Sandbox	Universal CEF	RV-N-18	
Altex Soft	RedCheck Scanner	2.9	VM	Syslog	RV-N-104	

Вендор	Продукт	Версия	Класс	Тип подключения	ID правила нормализации	Комментарий
Apache	Cassandra	4.1	DB	Syslog	RV-N-6	
Apache	HTTP-server	2	Web	Агент R-Vision Endpoint Syslog	RV-N-7 RV-N-8	
Apple	MacOS	10 11	OS	Агент R-Vision Endpoint	RV-N-9 RV-N-174	
Atlassian	Confluence	8	Business	Syslog	RV-N-10 RV-N-11	
Atlassian	Jira	9 10	Business	Syslog	RV-N-12 RV-N-13	
Avigilon	Avigilon Access Control Manager (ACM)	-	ACM	Universal CEF	RV-N-18	
AVSoft	Athena	1.4	Sandbox	Syslog	RV-N-4	
Ayehu	Ayehu eyeShare	-	ITSM	Universal CEF	RV-N-18	
Barracuda	Barracuda Networks NG Firewall	-	NGFW	Universal CEF	RV-N-18	
BeyondTrust	BeyondTrust BeyondInsight	-	PAM	Universal CEF	RV-N-18	
BeyondTrust	BeyondTrust Privilege Management Console	-	PAM	Universal CEF	RV-N-18	
BIND	BIND DNS	9.9	Application	Syslog	RV-N-14 RV-N-15 RV-N-16 RV-N-17 RV-N-142	
Bloombase	Bloombase StoreSafe	-	Application	Universal CEF	RV-N-18	

Вендор	Продукт	Версия	Класс	Тип подключения	ID правила нормализации	Комментарий
BMC	BMC CorreLog	-	SIEM	Universal CEF	RV-N-18	
Bricata	Bricata ProAccel	-	IPS	Universal CEF	RV-N-18	
Brinqa Risk	Brinqa Risk Analytics	-	ROC (Risk Operation Center)	Universal CEF	RV-N-18	
Broadcom	Broadcom Symantec Advanced Threat Protection (ATP)	-	TP	Universal CEF	RV-N-18	
Broadcom	Broadcom Symantec Endpoint Protection Mobile	-	AV	Universal CEF	RV-N-18	
Broadcom	Broadcom Symantec Threat Hunting Center	-	TH	Universal CEF	RV-N-18	
Canonical	Ubuntu	1804 2004 2204 2404	OS	Агент R-Vision Endpoint	RV-N-57	
Check Point	Firewall	R80+	NGFW	Syslog CEF	RV-N-19	
Check Point	Gaia	R80+	OS	Syslog	RV-N-20	
Cisco	ASA	8.4 9	FW	Syslog	RV-N-22	
Cisco	IOS	12 13 14 15	Network	Syslog	RV-N-24	
Cisco	IOS XE	17	Network	Syslog	RV-N-25	
Cisco	IOS XR	24	Network	Syslog	RV-N-26	

Вендор	Продукт	Версия	Класс	Тип подключения	ID правила нормализации	Комментарий
Cisco	Nexus	10.1	Network	Syslog	RV-N-27	
Cisco	Secure Email Gateway (SEG)	-	GW	Universal CEF	RV-N-18	
Cisco	Secure Firewall Management Center	-	MC	Universal CEF	RV-N-18	
Cisco	FirePower	6 7	IPS	Syslog	RV-N-23	
Cisco	IPFIX	v10	Network	Netflow	RV-N-87	
Cisco	Netflow v5	v5	Network	Netflow	RV-N-86	
Cisco	Netflow v9	v9	Network	Netflow	RV-N-88	
Citrix	NetScaler	13 14	Gateway	Syslog	RV-N-28	
Citrix	Virtual App and Desktops (VAD)	7	VDI	Syslog	RV-N-29 RV-N-30	
Citrix	XenApp	7	HV	DB(MSSQL)	RV-N-127	
Claroty	Claroty Continuous Threat Detection	-	TP	Universal CEF	RV-N-18	
ClickHouse	ClickHouse	23 24 25	DB	DB(ClickHouse)	RV-N-31	
CloudPassage	CloudPassage Halo	-	TP	Universal CEF	RV-N-18	
Corvil	Corvil Network Analytics	-	Application	Universal CEF	RV-N-18	
Cribl	Cribl Stream	-	Application	Universal CEF	RV-N-18	
CrowdStrike	Falcon Host	-	SOC Application	Universal CEF	RV-N-18	
CyberArk	CyberArk Privileged Threat Analytics (PTA)	-	TP	Universal CEF	RV-N-18	

Вендор	Продукт	Версия	Класс	Тип подключения	ID правила нормализации	Комментарий
Debian	Debian	10 11 12	OS	Агент R-Vision Endpoint	RV-N-57	
DeepInstinct	DeepInstinct	-	VM	Universal CEF	RV-N-18	
Delinea	Delinea Secret Server	-	Vault	Universal CEF	RV-N-18	
Digital Guardian	Digital Guardian Endpoint Threat Detection	-	TD	Universal CEF	RV-N-18	
DistKontrol	DistKontrolUSB	5	SW	Syslog	RV-N-32	
Dragos	Dragos Platform	-	TD	Universal CEF	RV-N-18	
Eclectiq	Eclectiq Intelligence Center	-	TD	Universal CEF	RV-N-18	
Edge Technologies	Edge Technologies AppBoard and enPortal	-	Application	Universal CEF	RV-N-18	
Eltex	ESR	1.18	GW	Syslog	RV-N-33	
Eltex	MES	1.28	SW	Syslog	RV-N-34	
Eltex	vESR	1.18	GW	Syslog	RV-N-33	
ESET	ESET Protect	-	AV	Universal CEF	RV-N-18	
F5	Big-IP Advanced Firewall Manager (AFM)	-	FW Manager	Universal CEF	RV-N-18	
FFR yara	FFRI	-	AV	Universal CEF	RV-N-18	
FireEye	FireEye CM Series	-	CMS	Universal CEF	RV-N-18	
FireEye	FireEye Malware Protection System	-	AV	Universal CEF	RV-N-18	

Вендор	Продукт	Версия	Класс	Тип подключения	ID правила нормализации	Комментарий
Forcepoint	Forcepoint NGFW	-	NGFW	Universal CEF	RV-N-18	
Forcepoint	Forcepoint SMC	-	SMC	Universal CEF	RV-N-18	
Fortinet	Fortigate	6.4 7.2 7.4	NGFW	Syslog	RV-N-37	
Fortinet	Fortinet FortiSOAR	-	SOAR	Universal CEF	RV-N-18	
FreelIPA	FreelIPA	3 4	Application	Syslog	RV-N-38 RV-N-39 RV-N-40 RV-N-41	
Gigamon	Gigamon GigaVUE	-	Application	Universal CEF	RV-N-18	
Gitlab	Gitlab	17 18	Application	Syslog	RV-N-42	
HAProxy	HAProxy	2.4	Application	Syslog	RV-N-44	
Hewlett Packard Enterprise	Aruba ClearPass	-	Application	Universal CEF	RV-N-18	
Hewlett Packard Enterprise	ArubaOS-CX	-	Switch	Syslog	RV-N-43	
Hewlett Packard Enterprise	ProCurve	-	SW	Syslog	RV-N-132	
Huawei	USG	5	NGFW	Syslog	RV-N-172	
IBM	IBM InfoSphere Guardium	-	Application	Universal CEF	RV-N-18	
Illumio	Illumio Policy Compute Engine (PCE)	-	Application	Universal CEF	RV-N-18	

Вендор	Продукт	Версия	Класс	Тип подключения	ID правила нормализации	Комментарий
Imperva	Imperva Incapsula	-	AntiDDoS	Universal CEF	RV-N-18	
Imperva	Imperva SecureSphere	-	SecurityPlatform	Universal CEF	RV-N-18	
Infotecs	ViPNet Coordinator	4	NGFW	Syslog	RV-N-46	
InfoWatch	Traffic Monitor	3	DLP	DB	RV-N-45	
Intralinks	Intralinks VIA	-	Application	Universal CEF	RV-N-18	
JetBrains	TeamCity	2023	Application	Syslog	RV-N-47	
		2024			RV-N-48	
					RV-N-136	
Juniper	JunOS	21	NGFW	Syslog	RV-N-49	
		23				
Kaspersky	Kaspersky Anti Targeted Attack (KATA)	7	Sandbox	Syslog	RV-N-50	
Kaspersky	Kaspersky CyberTrace	5	AV	Syslog	RV-N-166	
Kaspersky	Kaspersky Secure Mail Gateway	2.1	AV	Syslog CEF	RV-N-18	
Kaspersky	Kaspersky Security Center	14	AV	DB MS SQL	RV-N-51	
				DB MySQL (MariaDB)	RV-N-130	
				DB PostgreSQL		
				Syslog CEF		
Kaspersky	Kaspersky Web Traffic Security	6.1	AV	Syslog	RV-N-52	
Kubernetes	Kubernetes	1.18	Application	Vector	RV-N-53	
					RV-N-54	

Вендор	Продукт	Версия	Класс	Тип подключения	ID правила нормализации	Комментарий
Lieberman	Lieberman Application ERPM	-	Vault	Universal CEF	RV-N-18	
Lighttpd	Lighttpd	2.4	Web	Syslog	RV-N-160 RV-N-161	
Mattermost	Mattermost	9	Application	Syslog	RV-N-129	
Microsoft	Active Directory Domain Services	2008—2022	Application	Агент R-Vision Endpoint	RV-N-147	
Microsoft	Active Directory Web Services	2008—2022	Application	Агент R-Vision Endpoint	RV-N-58	
Microsoft	DHCP Server	2008—2022	Application	Агент R-Vision Endpoint	RV-N-59	
Microsoft	DNS Server	2008—2022	Application	Агент R-Vision Endpoint	RV-N-60 RV-N-61 RV-N-62	
Microsoft	Exchange	2019	Application	Агент R-Vision Endpoint	RV-N-63	
Microsoft	Microsoft IIS	2008—2022	WEB	Агент R-Vision Endpoint	RV-N-64	
Microsoft	Microsoft WMI	-	OS	WMI	RV-N-126	
Microsoft	SQL Server	2008—2022	DB	DB Агент R-Vision Endpoint	RV-N-69 RV-N-70	
Microsoft	System Center Configuration Manager	-	Application	Агент R-Vision Endpoint	RV-N-65 RV-N-66 RV-N-67	
Microsoft	System Center Operations Manager	-	Application	Агент R-Vision Endpoint	RV-N-68	
Microsoft	Terminal Services	-	Application	Агент R-Vision Endpoint	RV-N-78	

Вендор	Продукт	Версия	Класс	Тип подключения	ID правила нормализации	Комментарий
Microsoft	Windows AppLocker	-	OS	Агент R-Vision Endpoint	RV-N-72	
Microsoft	Windows Bits	-	OS	Агент R-Vision Endpoint	RV-N-73	
Microsoft	Windows PowerShell	-	OS	Агент R-Vision Endpoint	RV-N-74	
Microsoft	Windows Security	-	OS	Агент R-Vision Endpoint	RV-N-157	
Microsoft	Windows Sysmon	-	OS	Агент R-Vision Endpoint	RV-N-76	
Microsoft	Windows TaskScheduler	-	OS	Агент R-Vision Endpoint	RV-N-77	
Microsoft	Windows Terminal Service Gateway	-	Application	Агент R-Vision Endpoint	RV-N-79	
Microsoft	Windows WinRM	-	OS	Агент R-Vision Endpoint	RV-N-71	
Mikrotik	Router OS	6 7	SW/Router/FW	Syslog	RV-N-80	
MongoDB	MongoDB	7 8	DB	Syslog	RV-N-81	
Netgate	pfSense	2.7 2.8	Application	Syslog	RV-N-164	
NetIQ	NetIQ Identity Manager	-	IM	Universal CEF	RV-N-18	
NetScout	NetScout Systems nGenius Performance Manager	-	Application	Universal CEF	RV-N-18	
Netskope	Cloud Access Security Broker	-	Application	Universal CEF	RV-N-18	
Netwrix	Netwrix Auditor	-	Application	Universal CEF	RV-N-18	

Вендор	Продукт	Версия	Класс	Тип подключения	ID правила нормализации	Комментарий
Nextcloud	Nextcloud	26	Application	Syslog	RV-N-167	
		27				
		28				
		29				
Nexthink	Nexthink Engine	-	Application	Universal CEF	RV-N-18	
Nginx	Nginx	1.26	Web	Агент R-Vision Endpoint	RV-N-84	
		1.27		Syslog	RV-N-85	
		1.28			RV-N-139	
NIKSUN	NIKSUN NetDetector	-	Application	Universal CEF	RV-N-18	
One Identity	One Identity Privileged Session Management	-	PAM	Universal CEF	RV-N-18	
OpenBao	OpenBao	2.1	Application	Syslog	RV-N-89	
OpenVPN	OpenVPN	2.4	VPN	Syslog	RV-N-90	
		2.6			RV-N-91	
OpenVPN	OpenVPN Access Server	2	Application	Syslog	RV-N-165	
Oracle	MySQL	8	DB	Syslog	RV-N-82	
				DB(MySQL)	RV-N-83	
Oracle	OracleDB	21	DB	Syslog	RV-N-92	
Orion Soft	zVirt (oVirt)	4	Virtualization	DB (PostgreSQL)	RV-N-158	
PagerDuty	PagerDuty	-	Application	Universal CEF	RV-N-18	
Palo Alto	Palo Alto Cortex Data Lake	-	Application	Universal CEF	RV-N-18	
Palo Alto	Palo Alto Networks PANOS	-	Application	Universal CEF	RV-N-18	
Passbolt	Passbolt	4	Vault	Syslog	RV-N-93	

Вендор	Продукт	Версия	Класс	Тип подключения	ID правила нормализации	Комментарий
Passwork	Passwork	-	Vault	Syslog CEF	RV-N-94	
Penta Security	WAPPLES	-	WAF	Universal CEF	RV-N-18	
Positive Technologies	Application Firewall	3	WAF	Syslog	RV-N-95 RV-N-96	
Positive Technologies	Application Firewall	4	WAF	Syslog	RV-N-97	
Positive Technologies	Industrial Security Incident Manager	5	NTA (в сегмент АСУ ТП)	Syslog	RV-N-159	
Positive Technologies	Network Attack Discovery	-	NTA	Syslog	RV-N-128	
Positive Technologies	Sandbox	4	Sandbox	Syslog	RV-N-98	
PostgreSQL	PostgreSQL	14 17	DB	Syslog	RV-N-100	
Progress	Kemp LoadMaster	-	Application	Universal CEF	RV-N-18	
Proofpoint	Proofpoint Insider Threat Management	-	TD	Universal CEF	RV-N-18	
Proxmox	Proxmox Virtual Environment	8	HV	Syslog	RV-N-101	
R-Vision	R-Vision SOAR	-	IM	Syslog	RV-N-131	
R-Vision	R-Vision TDP	-	TDP	Syslog	RV-N-102	
R-Vision	R-Vision TIP	-	TIP	Syslog CEF	RV-N-103	
Recorded Future	Threat Intelligence Platform	-	TIP	Universal CEF	RV-N-18	
Red Hat	Ansible Tower	v3	Application	Syslog	RV-N-5	
Red Hat	AWX	24	Application	Syslog	RV-N-5	

Вендор	Продукт	Версия	Класс	Тип подключения	ID правила нормализации	Комментарий
Linux	Linux Auditd	-	OS	Агент R-Vision Endpoint Syslog	RV-N-55 RV-N-56 RV-ET-2 RV-A-1	
Red Hat	Red Hat Enterprise Linux	7 8 9	OS	Агент R-Vision Endpoint	RV-N-57	
Redis	Redis Enterprise DB	7.2	DB	Syslog	RV-N-105	
ReversingLabs	ReversingLabs N1000 Appliance	-	Application	Universal CEF	RV-N-18	
Rocky Foundation	Rocky Linux	8 9 10	OS	Агент R-Vision Endpoint	RV-N-57	
S-Terra	S-Terra Gate	4.3	VPN	Syslog	RV-N-106	
SailPoint	SailPoint IdentityIQ	-	IDM	Universal CEF	RV-N-18	
SberTech	Platform V Pangolin SE	6	DB	Syslog	RV-N-107	
Searchinform	Searchinform DLP	-	DLP	Universal CEF	RV-N-18	
Security Code	Континент	4	NGFW	Syslog	RV-N-112	
Security Code	SecretNet Studio	8	ACM	DB (MSSQL)	RV-N-109 RV-N-110	
Security Code	SecretNet Studio LSP	1.12	ACM	Syslog	RV-N-108	
SentinelOne	SentinelOne	-	EDR	Universal CEF	RV-N-18	
Squid	Squid	6 7	Proxy	Syslog	RV-N-117	

Вендор	Продукт	Версия	Класс	Тип подключения	ID правила нормализации	Комментарий
Suricata	Suricata	7 8	Application	Syslog	RV-N-140	
ThreatConnect	Threat Intelligence Platform	-	TIP	Universal CEF	RV-N-18	
ThreatQuotient	ThreatQuotient	-	Application	Universal CEF	RV-N-18	
TrapX	DeceptionGrid	-	Deception	Universal CEF	RV-N-18	
Trend Micro	Trend Micro Control Manager	-	Application	Universal CEF	RV-N-18	
Trend Micro	Trend Micro Deep Security	-	Application	Universal CEF	RV-N-18	
Trend Micro	Trend Micro NGFW	-	NGFW	Universal CEF	RV-N-18	
Trustwave	Application Security DbProtect	-	WAF	Universal CEF	RV-N-18	
Usergate	Usergate NGFW	6	NGFW	Syslog	RV-N-35	
Usergate	Usergate UTM	6	UTM	Syslog	RV-N-36	
Varonis	DatAdvantage	-	Data Protection	Universal CEF	RV-N-18	
Veeam	Veeam Backup	11	Backup	Агент R-Vision Endpoint	RV-N-122	
Veriato	Veriato 360	-	UEBA	Universal CEF	RV-N-18	
VMware	VMware Carbon Black EDR	-	EDR	Universal CEF	RV-N-18	
VMware	VMware ESXi	6 7	HV	Syslog	RV-N-119	
VMware	VMware Horizon	7.8	HV	Syslog	RV-N-120	
VMware	VMware vCenter	6 7	HV	Syslog	RV-N-121	

Вендор	Продукт	Версия	Класс	Тип подключения	ID правила нормализации	Комментарий
Vormetric	Vormetric Data Security Manager	-	SMC	Universal CEF	RV-N-18	
Votiro	Votiro Disarmer for Windows	-	Application	Universal CEF	RV-N-18	
Webroot	Webroot BrightCloud	-	Application	Universal CEF	RV-N-18	
Xello	Xello Deception	5.5	Honeypot	Syslog CEF	RV-N-143	
Zabbix	Zabbix	6 7	Application	DB (PostgreSQL)	RV-N-124	
Zeek	Traffic Parcer	4	Application	Syslog	RV-N-125	
Zettaset	BDEncrypt	-	DBF	Universal CEF	RV-N-18	
Zscaler	Zscaler Nanolog Streaming Service (NSS)	-	Application	Universal CEF	RV-N-18	

С-Терра

Данный раздел содержит список систем для настройки от компании С-Терра:

- [Шлюз 4.3](#)

Шлюз 4.3

Данное руководство описывает процесс настройки отправки событий логирования в R-Vision SIEM, а также получения событий аудита С-Терра Шлюз 4.3.

- [Настройка С-Терра Шлюз 4.3](#)
 - [Настройка службы rsyslog](#)
- [Настройка в R-Vision SIEM](#)
- [Типы обрабатываемых событий](#)
- [Таблицы маппинга](#)

Настройка С-Терра Шлюз 4.3

Для настройки отправки событий логирования в SIEM выполните следующие шаги:

1. Откройте Cisco-like консоль источника.

2. Перейдите в режим администрирования:

```
enable
```

3. Перейдите в режим конфигурации:

```
configure terminal
```

4. Включите логирование и установите уровень логирования:

```
logging on  
logging trap debugging
```

5. Настройте службу отправки. Для этого выполните следующие команды в командной строке источника:

```
log_mgr set-syslog -y enable -a <siem-collector-ip> -f local7  
log_mgr set -l debug
```

Здесь **<siem-collector-ip>** — IP-адрес коллектора SIEM.

6. Установите подготовленные (изначально имеющиеся в источнике) конфигурационные файлы логирования:

```
log_mgr set -e /opt/VPNagent/etc/msg_grpCERTS.ini -f  
log_mgr set -e /opt/VPNagent/etc/msg_grpKERNEL.ini -f  
log_mgr set -e /opt/VPNagent/etc/msg_grpLDAP.ini -f  
log_mgr set -e /opt/VPNagent/etc/msg_grpPOLICY.ini -f  
log_mgr set -e /opt/VPNagent/etc/msg_grpSYSTEM.ini -f
```

Настройка службы rsyslog

1. Откройте файл **/etc/rsyslog.conf**.
2. Добавьте в файл следующую строку:

```
local7.* @<siem-collector-ip><port>
```

Здесь:

- **<siem-collector-ip>** — IP-адрес коллектора SIEM, указанный при [настройке источника](#).
- **<port>** — порт точки входа Syslog на конвейере SIEM — любой свободный порт в диапазоне 30000–32767.

3. Перезапустите службу **rsyslog** с помощью команды:

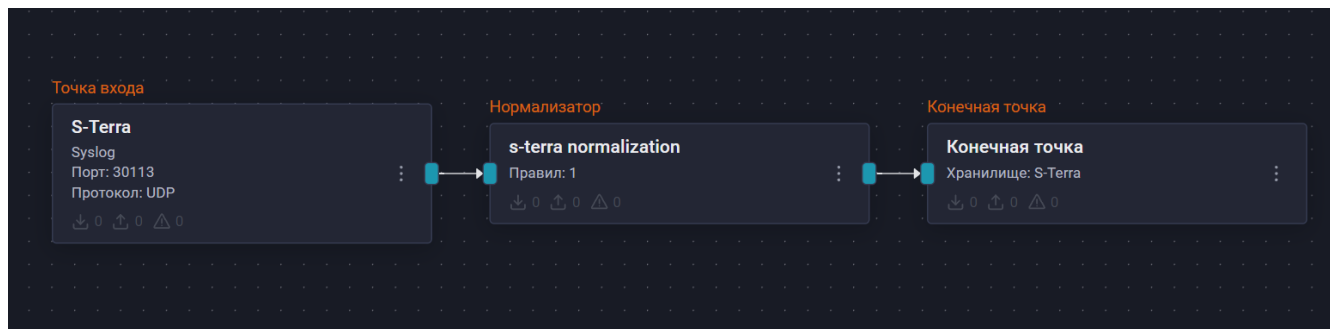
```
systemctl restart rsyslog.service
```

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Syslog**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [службы rsyslog](#).
 - Протокол: выберите вариант **UDP**.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **S-Terra Gate ST 4.3** (идентификатор правила: **RV-N-106**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события С-Терра Шлюз 4.3.

Найти события С-Терра Шлюз 4.3 в хранилище можно по следующему фильтру:

```
dproduct = "s-terra gate st"
```



Добавить фильтр

☐ Инvertировать (NOT)

Поле

dproduct

Оператор

=

Значение

s-terra gate st

☐ Настроить заголовок

Отменить

Добавить

Типы обрабатываемых событий

События из С-Терра Шлюз 4.3 во внешние системы передаются в формате RFC. Подробная информация о событиях представлена в документе [РЛКЕ.00027-01 92 016 "РУКОВОДСТВО АДМИНИСТРАТОРА ПРОТОКОЛИРОВАНИЕ СОБЫТИЙ"](#) от 10.09.2021.

Таблицы маппинга

Таблица 1. Общий маппинг

Поле модели событий	Значение
dvendor	s-terra
dproduct	s-terra gate st
dversion	4.3
dvchost	raw.hostname
dvc	raw.hostname
msg	Приводится к виду user-like на основе других полей
rt	raw.timestamp
severity	raw.severity
externalId	raw.message.code
facility	raw.facility
destinationServiceName	raw.message.appname

Таблица 2. Login in cisco-like

Поле модели событий	Значение
name	Cisco-like console started
outcome	success
act	login

Поле модели событий	Значение
suser	account name

Таблица 3. Logout

Поле модели событий	Значение
name	Cisco-like console exited
outcome	success
act	logout
suser	account name

Таблица 4. Use command interpreter

Поле модели событий	Значение
outcome	success/failure
act	input command
suser	account name
cmd	raw.message.command

Таблица 5. User created/removed/password changed/privilege changed

Поле модели событий	Значение
name	User created/removed/password changed/privilege changed
act	user created/removed/password changed/privilege changed
duser	Учетная запись, над которой выполняется операция
suser	Учетная запись, выполняющая операцию

Таблица 6. Enable mode

Поле модели событий	Значение
name	User privilege changed
outcome	success
act	enable mode

Таблица 7. Start IKE session

Поле модели событий	Значение
name	Start IKE session
dst	raw.message.peer.address
dpt	raw.message.peer.port
targetSessionId	raw.message.sessionId

Таблица 8. IPSec connection established

Поле модели событий	Значение
name	IPSec connection established
dst	raw.message.peer.address
dpt	raw.message.peer.port
cs1	raw.message.traffic selector.src subnet
cs1Label	src tunnel subnet
cs2	raw.message.traffic selector.dst subnet
cs2Label	dst tunnel subnet
cs3	raw.message.connection num
cs3Label	connection num

Таблица 9. IPSec connection closed

Поле модели событий	Значение
name	IPSec connection closed
cs3	raw.message.connection num
cs3Label	connection num
bytesIn	raw.message.bytes received
bytesOut	raw.message.bytes sent

Таблица 10. ISAKMP connection established

Поле модели событий	Значение
name	ISAKMP connection established
dst	raw.message.peer.address
dpt	raw.message.peer.port
cs3	raw.message.connection num
cs3Label	connection num

Таблица 11. ISAKMP connection closed

Поле модели событий	Значение
name	ISAKMP connection closed
cs3	raw.message.connection num
cs3Label	connection num
bytesIn	raw.message.bytes received
bytesOut	raw.message.bytes sent

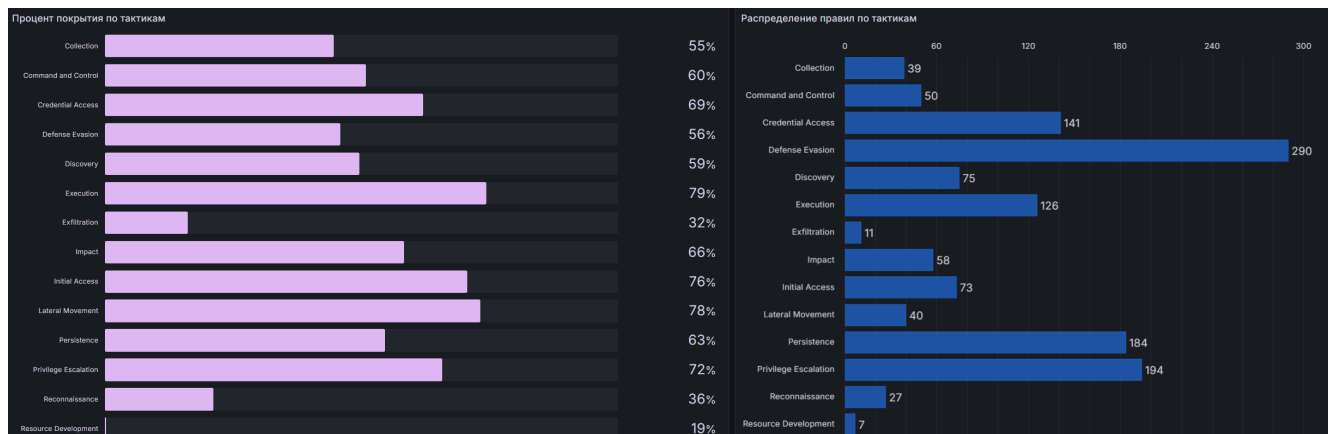
Перечень правил детектирования

Данная таблица содержит список разработанных правил детектирования. Для каждого правила указано, к какой информационной системе оно относится, а также какие тактики и техники MITRE ATT&CK оно затрагивает.

Карта покрытия тактик и техник матрицы MITRE ATT&CK правилами детектирования

[illegible]

Графики покрытия тактик матрицы MITRE ATT&CK правилами детектирования



1С

Данный раздел содержит список систем для настройки от компании "1С":

- [Битрикс24](#)
- [1С:Предприятие Журнал регистрации](#)
- [1С:Предприятие Технологический журнал](#)

Битрикс24

Данная инструкция описывает настройку сбора событий на сервере Битрикс24 и последующей отправки в R-Vision SIEM:

- [Предварительные требования](#)
- [Настройка в Битрикс24](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Предварительные требования

- Сетевой доступ к БД Битрикс24.
- Учетная запись в СУБД с правами на чтение таблицы **b_event_log**.

Настройка в Битрикс24

Настроить, какие события будут записываться в журнал и сколько по времени они будут храниться, можно в разделе: **Настройки** → **Настройки продукта** → **Настройки модулей** → **Главный модуль** → **Журнал событий**.



Чтобы просмотреть журнал, перейдите в раздел **Настройки** → **Инструменты** → **Журнал событий**

События журнала записываются в СУБД MySQL в таблицу **b_event_log**, которая обычно используется системой Битрикс24 для хранения событий.

▼ Перечень возможных событий в Битрикс24:

- успешный вход;
- выход из системы;
- ошибки входа;
- ошибки доступа к файлам;
- блокировка пользователя;
- регистрация нового пользователя;
- ошибки регистрации;

- запросы на смену пароля;
- смена пароля;
- редактирование пользователя;
- удаление пользователя;
- изменение групп пользователя;
- изменение политики безопасности группы;
- изменение доступа к модулю;
- изменение доступа к файлу;
- изменение уровня доступа;
- установка и удаление решений из Marketplace.

Настройка в R-Vision SIEM

Создание секрета

Добавьте секрет для подключения к базе Битрикс24 в разделе **Ресурсы** → **Секреты** со следующими параметрами:

- **Тип секрета** — Строка подключения;
- **Строка подключения** — строка вида:

```
jdbc:mysql://<address>:<port>/<database>?user=<user>&password=<password>
```

где:

- **<address>** — адрес сервера базы;
- **<port>** — порт подключения;
- **<database>** — имя базы событий аудита;
- **<user>** — логин пользователя базы;
- **<password>** — пароль пользователя базы.

Пример 1. Пример строки подключения

```
jdbc:mysql://192.0.2.70:3306/sitemanager1?user=user&password=password
```

Настройка конвейера для сбора событий аудита

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте в конвейер элемент **Точка входа** типа **Database** со следующими параметрами:
 - **Драйвер базы данных** — MySQL
 - **Адрес подключения** — выберите созданный ранее [секрет](#);

◦ SQL запрос:

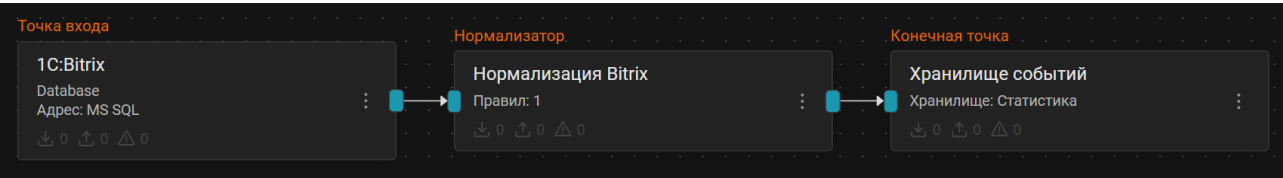
```
SELECT ID as ident,TIMESTAMP_X,SEVERITY,AUDIT_TYPE_ID,MODULE_ID,
ITEM_ID,REMOTE_ADDR,USER_AGENT,REQUEST_URI,USER_ID,DESCRIPTION,
"Bitrix24" as appname FROM <database>.b_event_log WHERE ID > ?;
```

Здесь **<database>** — имя БД событий аудита.

- Поле идентификатора — **ident** со значением **1**
- Интервал запроса — **15**

- 3. Добавьте **Нормализатор** с правилом **1С-Битрикс Битрикс 24** (идентификатор **RV-N-3**). Соедините нормализатор с точкой входа.
- 4. Добавьте элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
- 5. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера



Если настройка выполнена корректно, то в хранилище начнут поступать события источника.

Таблица маппинга

В рамках таблицы маппинга приведено сопоставление между полями в Битрикс24 и полями универсальной модели R-Vision SIEM:

Поле события	Значение поля
dvendor	"000 "1С-Битрикс""
dproduct	"Битрикс 24"
externalId	.raw.ident
severity	.raw.SEVERITY
rt	.raw.TIMESTAMP_X
cat	.raw.AUDIT_TYPE_ID
app	.raw.MODULE_ID
objName	.raw.ITEM_ID
src	.raw.REMOTE_ADDR
request	.raw.REQUEST_URI
suid	.raw.USER_ID
requestClientApplication	.raw.USER_AGENT

Поле события	Значение поля
msg	.raw.DESRIPTION

1С:Предприятие Журнал регистрации

Данное руководство описывает процесс настройки сбора событий журнала регистрации на сервере 1С:Предприятия и их последующей отправки в R-Vision SIEM.

- [Настройка 1С:Предприятие Журнал регистрации](#)
 - [Настройка подсистемы журналирования](#)
- [Настройка в R-Vision Endpoint](#)
- [Настройка в R-Vision SIEM](#)
- [Типы обрабатываемых событий](#)
- [Таблица маппинга](#)



Действия описаны на примере конфигурации "Зарплата и управление персоналом 3.1". В других конфигурациях названия и расположение элементов интерфейса могут отличаться.

Настройка 1С:Предприятие Журнал регистрации

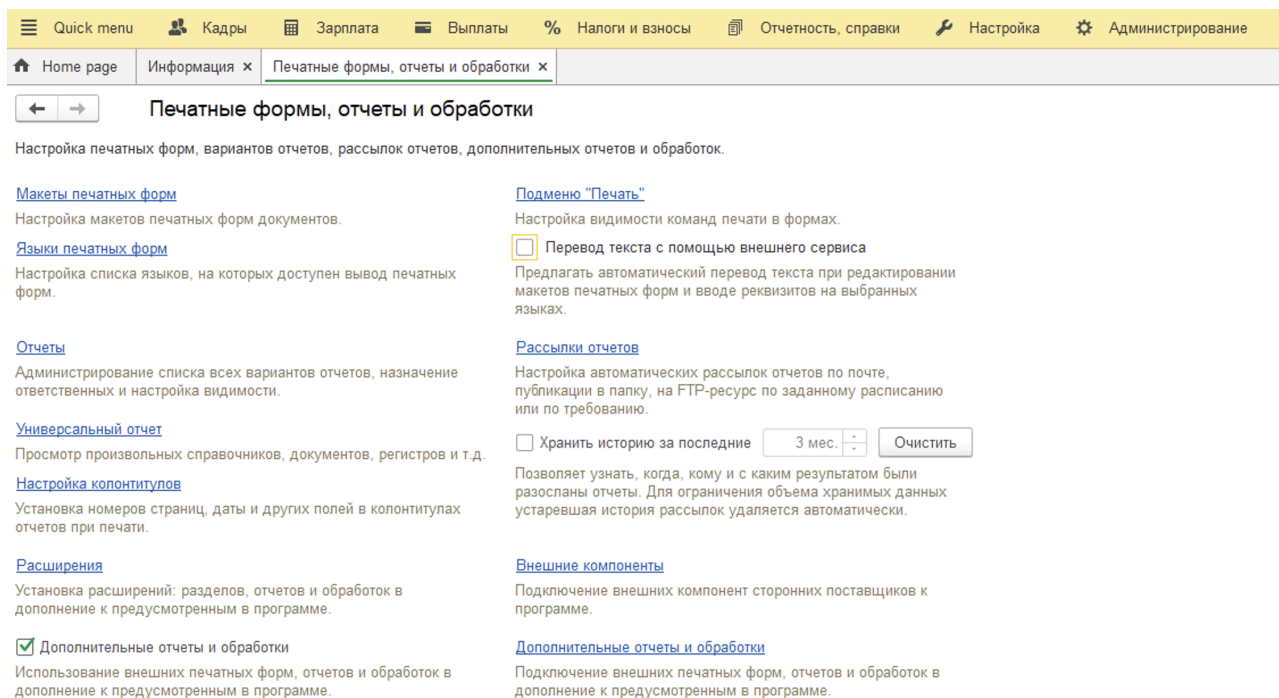
Настройка подсистемы журналирования



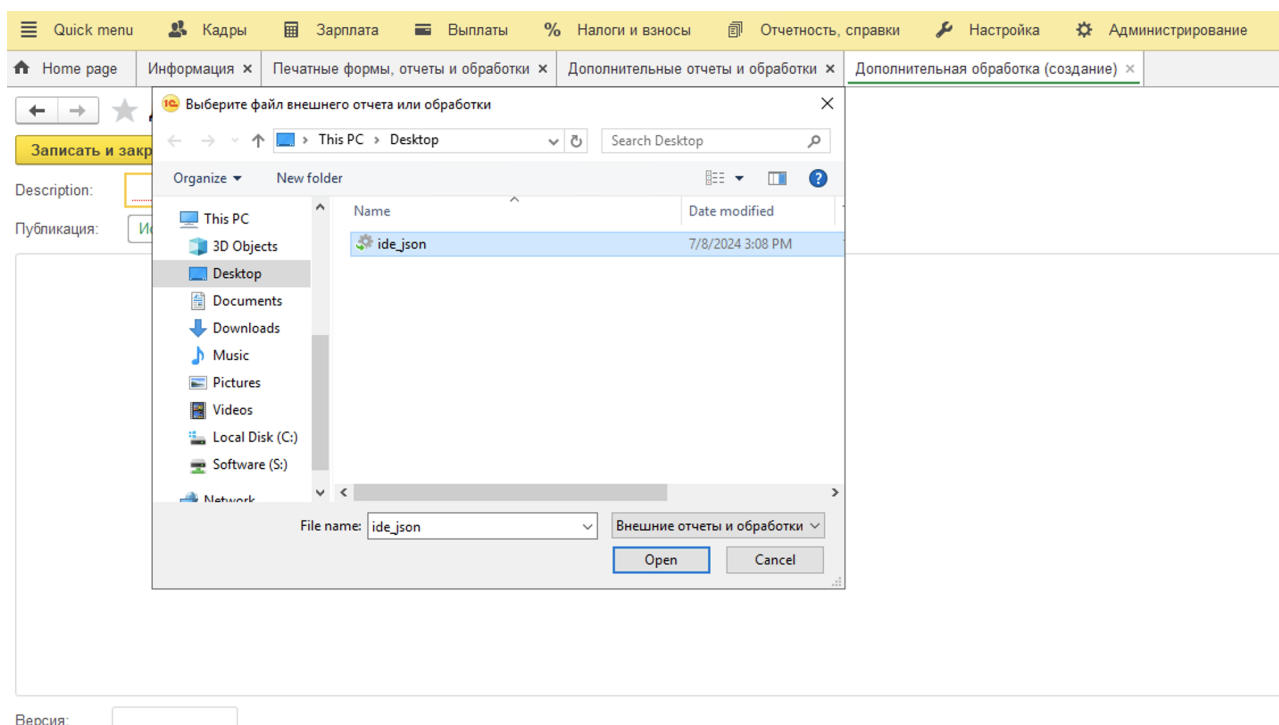
Для выгрузки журнала регистрации в информационной базе 1С:Предприятия должен быть установлен модуль **1С:Библиотека стандартных подсистем**. Кроме того, если указан часовой пояс информационной базы, он должен совпадать с часовым поясом узла, на котором установлен сервер 1С:Предприятия.

Чтобы настроить выгрузку регистрационного журнала в папку:

1. Войдите в программу 1С:Предприятие. Для этого:
 - a. Запустите 1С:Предприятие. Откроется окно **Запуск 1С:Предприятия**.
 - b. Выберите в списке информационную базу и нажмите на кнопку **1С:Предприятие**.
 - c. В открывшемся окне введите данные учетной записи администратора и нажмите на кнопку **Войти**. Откроется окно 1С:Предприятия.
2. Перейдите в раздел **Администрирование → Печатные формы, отчеты и обработки**.
3. Установите флажок **Дополнительные отчеты и обработки**.



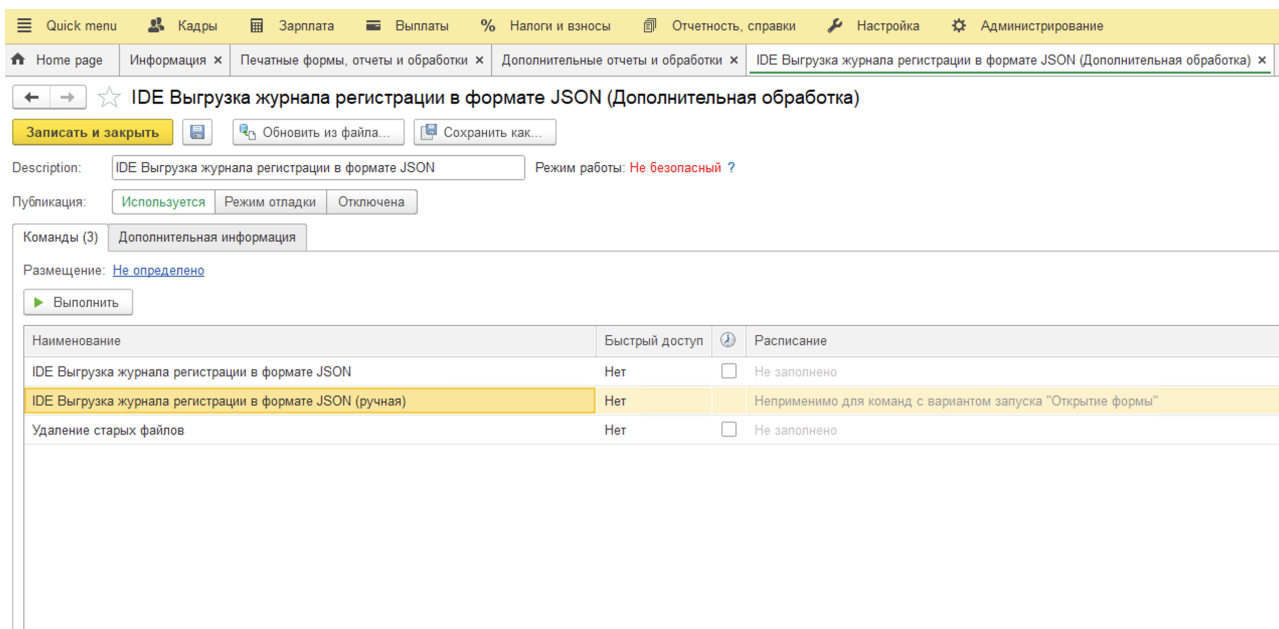
4. Перейдите в раздел **Дополнительные отчеты и обработки**.
5. На панели инструментов раздела нажмите на кнопку **Добавить из файла**. Откроется окно проводника.



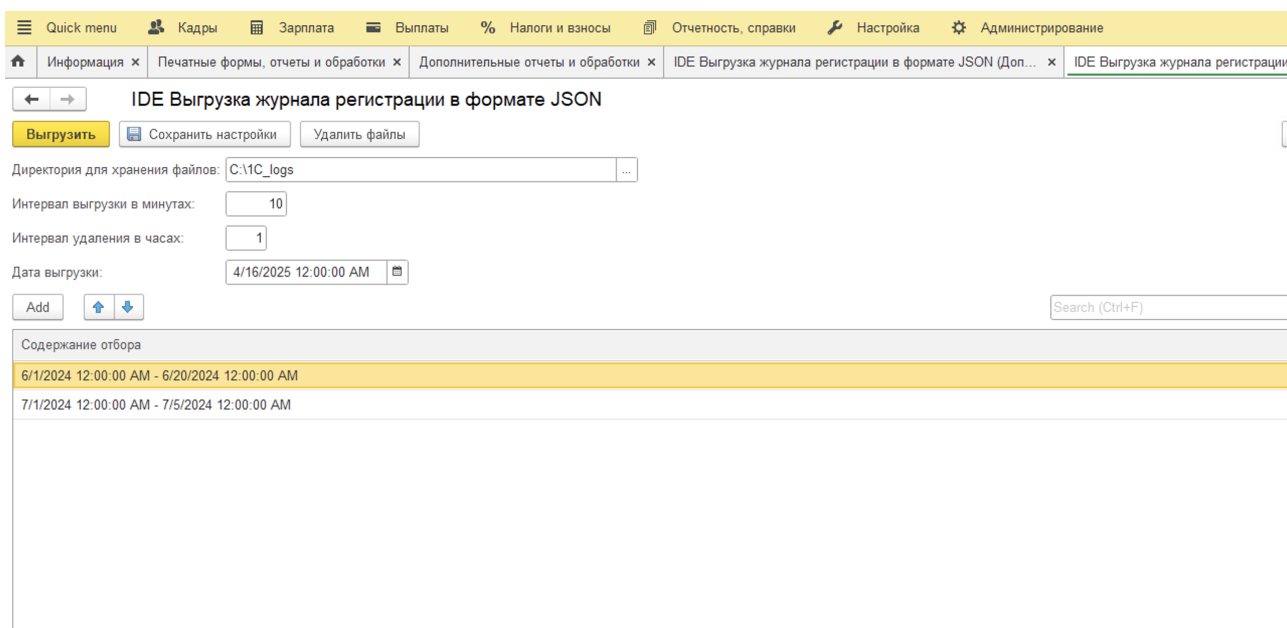
6. Выберите файл внешнего отчета или обработки и нажмите на кнопку **Open**. Откроется вкладка **IDE Выгрузка журнала регистрации в формате JSON (Дополнительная обработка)**.



Архив со сценарием обработки [представлен по ссылке](#).



7. На панели инструментов вкладки нажмите на кнопку **Сохранить**.
8. На вкладке **Команды** выберите опцию **IDE Выгрузка журнала регистрации в формате JSON (ручная)** и нажмите на кнопку **Выполнить**. Откроется вкладка **IDE Выгрузка журнала регистрации в формате JSON**.
9. Укажите настройки выгрузки:
 - **Директория для хранения файлов:** введите путь для сохранения файлов журнала регистрации, например, **C:/1C_logs/**.
 - **Интервал выгрузки в минутах:** укажите временной промежуток в минутах, в течение которого события, зафиксированные в журнале регистрации, будут сохраняться в отдельном файле, например, **10**.
 - **Интервал удаления в часах:** укажите временной промежуток в часах, через который события, зафиксированные в журнале регистрации, будут автоматически удаляться, например, **1**.
 - **Дата выгрузки:** укажите дату, с которой начнется выгрузка журнала регистрации.



10. Нажмите на кнопку **Сохранить настройки** и подтвердите сохранение.
11. Закройте вкладку **IDE Выгрузка журнала регистрации в формате JSON**.
12. Перейдите на вкладку **IDE Выгрузка журнала регистрации в формате JSON (Дополнительная обработка)**.
13. На вкладке **Команды** установите флажок **IDE Выгрузка журнала регистрации в формате JSON**. Откроется окно **Schedule**.
14. Выберите вкладку **Daily** и в поле **Repeat after** введите значение **600**.
15. Нажмите на кнопку **OK**.

Schedule

General Daily Weekly Monthly

Begin at: : : AM × Repeat after: 600 sec

End at: : : AM × Repeat after pause: 0 sec

Terminate at: : : AM × Terminate in: 0 sec

Detailed day schedule:

Add Delete More actions ▾

from April 16, 2025 every day; every 600 seconds

OK Cancel ?

16. На вкладке **Команды** установите флажок **Удаление старых файлов**. Откроется окно **Schedule**.

Информация ×
Печатные формы, отчеты и обработки ×
Дополнительные отчеты и обработки ×
IDE Выгрузка журнала регистрации в формате JSON (... ×)

← →
☆ IDE Выгрузка журнала регистрации в формате JSON (Дополнительная обработка) *

Записать и закрыть
Обновить из файла...
Сохранить как...

Description: IDE Выгрузка журнала регистрации в формате JSON
Режим работы: Не безопасный ?

Публикация:
Используется
Режим отладки
Отключена

Команды (3)
Дополнительная информация

Размещение: Не определено

▶ Выполнить

Наименование	Быстрый доступ		Расписание
IDE Выгрузка журнала регистрации в формате JSON	Нет	✓	from April 16, 2025 one day; every 600 seconds
IDE Выгрузка журнала регистрации в формате JSON (ручная)	Нет		Неприменимо для команд с вариантом запуска
Удаление старых файлов	Нет	✓	every day; once a day

17. Выберите вкладку **General** и в поле **Repeat every** введите значение **1**.

18. Нажмите на кнопку **OK**.

Schedule

General

Daily

Weekly

Monthly

Start date:

4/16/2025

×

▲

▼

End date:

/ /

×

▲

▼

Repeat every:

1

▲

▼

day(s)

from April 16, 2025 every day; every 600 seconds

OK

Cancel

?

19. Нажмите на кнопку **Записать и закрыть**.

Логирование на стороне источника настроено.

Настройка в R-Vision Endpoint

Чтобы настроить отправку событий из R-Vision Endpoint:

1. Добавьте в интерфейсе R-Vision Endpoint политику для сбора событий технологического журнала.
2. В поле **Путь** укажите путь к логам из конфигурационного файла:

Тип журнала

Путь

syslog

▼

C:\1C_logs*.json

3. Нажмите на кнопку **Сохранить и применить**.

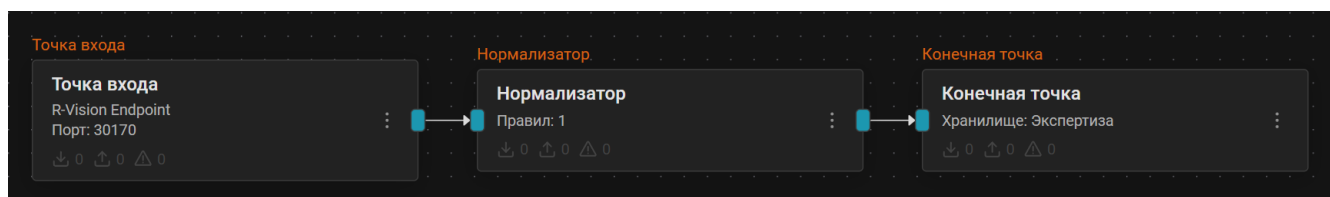
События начнут поступать в SIEM согласно конфигурации R-Vision Endpoint.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **R-Vision Endpoint**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [сервера](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом **1C-Soft 1C:Enterprise 8.3** (идентификатор правила: **RV-N-1**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

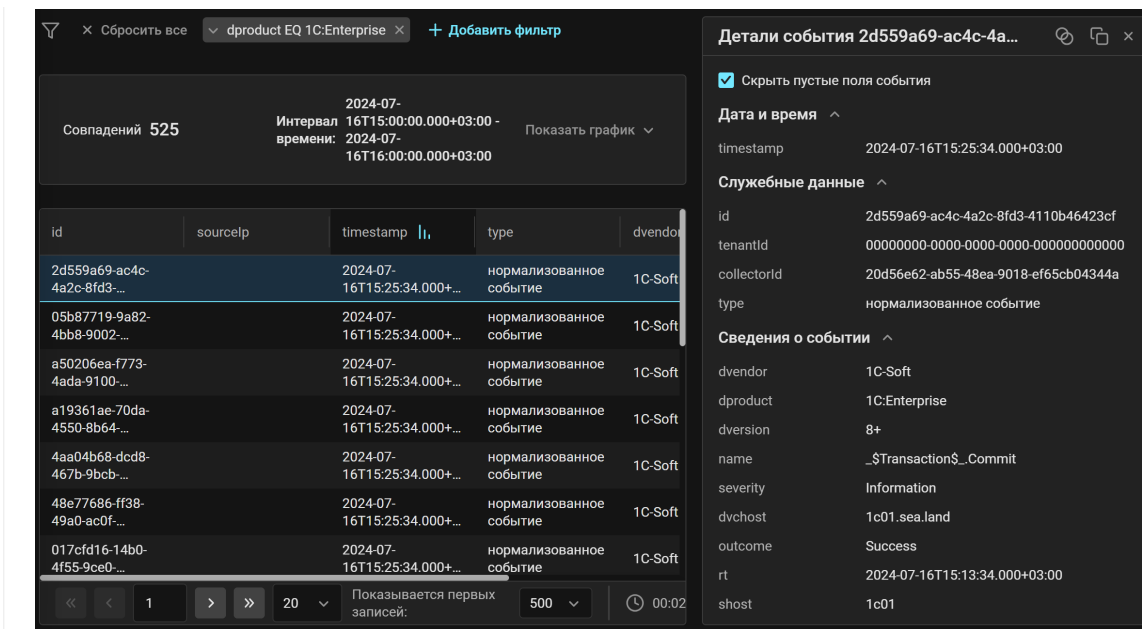


После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события 1С:Предприятия.

Найти события 1С:Предприятия в хранилище можно по следующему фильтру:

```
dproduct = "1C:Enterprise"
```





Типы обрабатываемых событий

- Успешная или неуспешная авторизация через толстый клиент, конфигуратор или COM-соединение.
- Успешная авторизация через толстый клиент.
- Ошибка авторизации через тонкий клиент.
- Ошибка авторизации через веб-клиент.
- Успешная авторизация через веб-клиент.
- Успешно установлено соединение с сервером 1C:Предприятия.
- Подключение к дизайнеру заблокировано другим пользователем.
- Просмотр списка пользователей, подключенных к серверу 1C:Предприятия.
- Просмотр пользователем параметров информационной базы.

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

1C:Предприятие Технологический журнал

Данное руководство описывает процесс настройки сбора событий технологического журнала на сервере 1C:Предприятия и их отправки в хранилище R-Vision SIEM.

- [Настройка 1C:Предприятие Технологический журнал](#)
 - [Настройка подсистемы журналирования](#)
- [Настройка в R-Vision Endpoint](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Настройка 1С:Предприятие Технологический журнал

Настройка подсистемы журналирования

Чтобы настроить логирование событий технологического журнала на сервере 1С:Предприятия, выполните следующие шаги:

1. Создайте конфигурационный файл logcfg.xml. Расположение файла зависит от ОС и архитектуры сервера:
 - В Windows создайте файл в папке `\bin\conf` внутри папки, где установлено 1С:Предприятие.
 - В ОС семейства Unix с 32-битной архитектурой создайте файл в каталоге `/opt/1C/v8.3/i386/conf`.
 - В ОС семейства Unix с 64-битной архитектурой создайте файл в каталоге `/opt/1C/v8.3/x86_64/conf`.
2. Добавьте в файл следующие строки:

```
<?xml version="1.0" encoding="UTF-8"?>
<config xmlns="http://v8.1c.ru/v8/tech-log">

</config>
```

3. Укажите внутри элемента `config` каталог для хранения файлов журнала и время хранения событий:

```
<log location="<path>" history="<time>">

  <property name="all"/>
</log>
```

Здесь:

- `<path>` — путь для хранения файлов журнала. Для Windows укажите общую папку, для ОС семейства Unix — домашний каталог пользователя, от имени которого запускается сервер 1С:Предприятия.
 - `<time>` — время хранения событий в часах. Например, для хранения событий за 7 суток укажите значение `168`.
4. Добавьте внутри элемента `log` фильтры событий:

```
<event>
  <eq property="name" value="CALL"/>
  <eq property="MName" value="authenticateServer"/>
</event>
<event>
  <eq property="name" value="SCALL"/>
  <eq property="MName" value="setSessionData"/>
```

```

    <eq property="t:applicationName" value="1CV8C"/>
</event>
<event>
    <eq property="name" value="EXCP"/>
    <eq property="t:applicationName" value="1CV8C"/>
    <like property="Descr" value="%VResourceInfoBaseServerImpl.cpp%"/>
</event>
<event>
    <eq property="name" value="EXP"/>
    <eq property="t:applicationName" value="WebServerExtension"/>
    <like property="Descr" value="%VResourceInfoBaseServerImpl.cpp%"/>
</event>
<event>
    <eq property="name" value="SCALL"/>
    <eq property="t:applicationName" value="WebServerExtension"/>
    <eq property="MName" value="setSessionData"/>
    <ne property="Usr" value="DefUser"/>
</event>
<event>
    <eq property="name" value="CONN"/>
    <like property="Txt" value="Accepted%"/>
</event>
<event>
    <eq property="name" value="CALL"/>
    <eq property="MName" value="lockConfig"/>
</event>
<event>
    <eq property="name" value="CALL"/>
    <eq property="MName" value="activeUsers"/>
</event>
<event>
    <eq property="name" value="CALL"/>
    <eq property="MName" value="readInfoBaseAdmParams"/>
    <ne property="Usr" value=""/>
</event>

```

5. Сохраните конфигурационный файл.

Логирование событий технологического журнала настроено.

▼ Пример конфигурационного файла для ОС Windows

```

<?xml version="1.0" encoding="UTF-8"?>
<config xmlns="http://v8.1c.ru/v8/tech-log">
  <log location="C:\v8\logs" history="168">
    <event>
      <eq property="name" value="CALL"/>
      <eq property="MName" value="authenticateServer"/>
    </event>
    <event>
      <eq property="name" value="SCALL"/>

```

```

    <eq property="MName" value="setSessionData"/>
    <eq property="t:applicationName" value="1CV8C"/>
</event>
<event>
    <eq property="name" value="EXCP"/>
    <eq property="t:applicationName" value="1CV8C"/>
    <like property="Descr" value="%VResourceInfoBaseServerImpl.cpp%"/>
</event>
<event>
    <eq property="name" value="EXP"/>
    <eq property="t:applicationName" value="WebServerExtension"/>
    <like property="Descr" value="%VResourceInfoBaseServerImpl.cpp%"/>
</event>
<event>
    <eq property="name" value="SCALL"/>
    <eq property="t:applicationName" value="WebServerExtension"/>
    <eq property="MName" value="setSessionData"/>
    <ne property="Usr" value="DefUser"/>
</event>
<event>
    <eq property="name" value="CONN"/>
    <like property="Txt" value="Accepted%"/>
</event>
<event>
    <eq property="name" value="CALL"/>
    <eq property="MName" value="lockConfig"/>
</event>
<event>
    <eq property="name" value="CALL"/>
    <eq property="MName" value="activeUsers"/>
</event>
<event>
    <eq property="name" value="CALL"/>
    <eq property="MName" value="readInfoBaseAdmParams"/>
    <ne property="Usr" value=""/>
</event>
<property name="all"/>
</log>
</config>

```

Этот файл создает технологический журнал в папке **C:\v8\logs** с хранением событий в течение 7 суток.

Настройка в R-Vision Endpoint

Чтобы настроить отправку событий из R-Vision Endpoint:

1. Добавьте в интерфейсе R-Vision Endpoint политику для сбора событий технологического журнала.
2. В поле **Путь** укажите путь к логам из конфигурационного файла.

3. Нажмите на кнопку **Сохранить и применить**.

События начнут поступать в SIEM согласно конфигурации R-Vision Endpoint.

Настройка в R-Vision SIEM

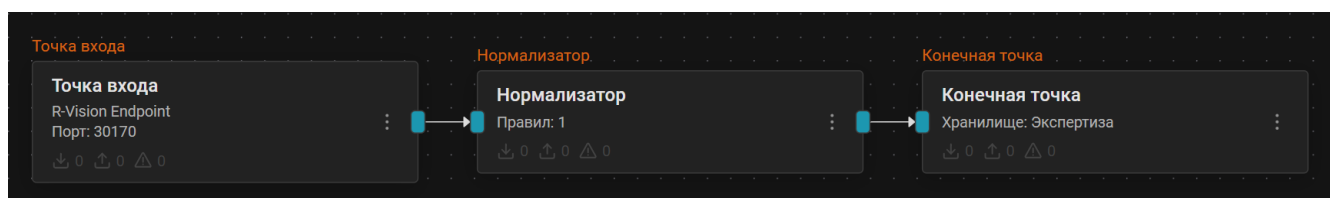


Если у вас уже настроен конвейер для сбора событий журнала регистрации, выполните только пункты **3** и **7** данной инструкции.

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **R-Vision Endpoint**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [сервера](#).
3. Добавьте на конвейер **Нормализатор** с правилом **1C-Soft 1C:Enterprise 8.3** (идентификатор правила: **RV-N-2**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события 1С:Предприятия.

Найти события 1С:Предприятия в хранилище можно по следующему фильтру:

```
dproduct = "1C:Enterprise"
```



Сбросить все

dproduct EQ 1C:Enterprise

+ Добавить фильтр

Совпадений 525

Интервал времени: 2024-07-16T15:00:00.000+03:00 - 2024-07-16T16:00:00.000+03:00

Показать график

id	sourceIp	timestamp	type	dvendor
2d559a69-ac4c-4a2c-8fd3-...		2024-07-16T15:25:34.000+...	нормализованное событие	1C-Soft
05b87719-9a82-4bb8-9002-...		2024-07-16T15:25:34.000+...	нормализованное событие	1C-Soft
a50206ea-f773-4ada-9100-...		2024-07-16T15:25:34.000+...	нормализованное событие	1C-Soft
a19361ae-70da-4550-8b64-...		2024-07-16T15:25:34.000+...	нормализованное событие	1C-Soft
4aa04b68-dcd8-467b-9bcb-...		2024-07-16T15:25:34.000+...	нормализованное событие	1C-Soft
48e77686-ff38-49a0-ac0f-...		2024-07-16T15:25:34.000+...	нормализованное событие	1C-Soft
017cfd16-14b0-4f55-9ce0-...		2024-07-16T15:25:34.000+...	нормализованное событие	1C-Soft

<<

<

1

>

>>

20

Показывается первых 500 записей:

00:02

Детали события 2d559a69-ac4c-4a...

☒ Скрыть пустые поля события

Дата и время

timestamp2024-07-16T15:25:34.000+03:00

Служебные данные

id2d559a69-ac4c-4a2c-8fd3-4110b46423cf

tenantId00000000-0000-0000-0000-000000000000

collectorId20d56e62-ab55-48ea-9018-ef65cb04344a

typenормализованное событие

Сведения о событии

dvendor1C-Soft

dproduct1C:Enterprise

dversion8+

name_.\$Transaction\$.Commit

severityInformation

dvchost1c01.sea.land

outcomeSuccess

rt2024-07-16T15:13:34.000+03:00

shost1c01

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Ansible

Данный раздел содержит список систем управления сервисом Ansible.

- [AWX](#)
- [Tower](#)

AWX

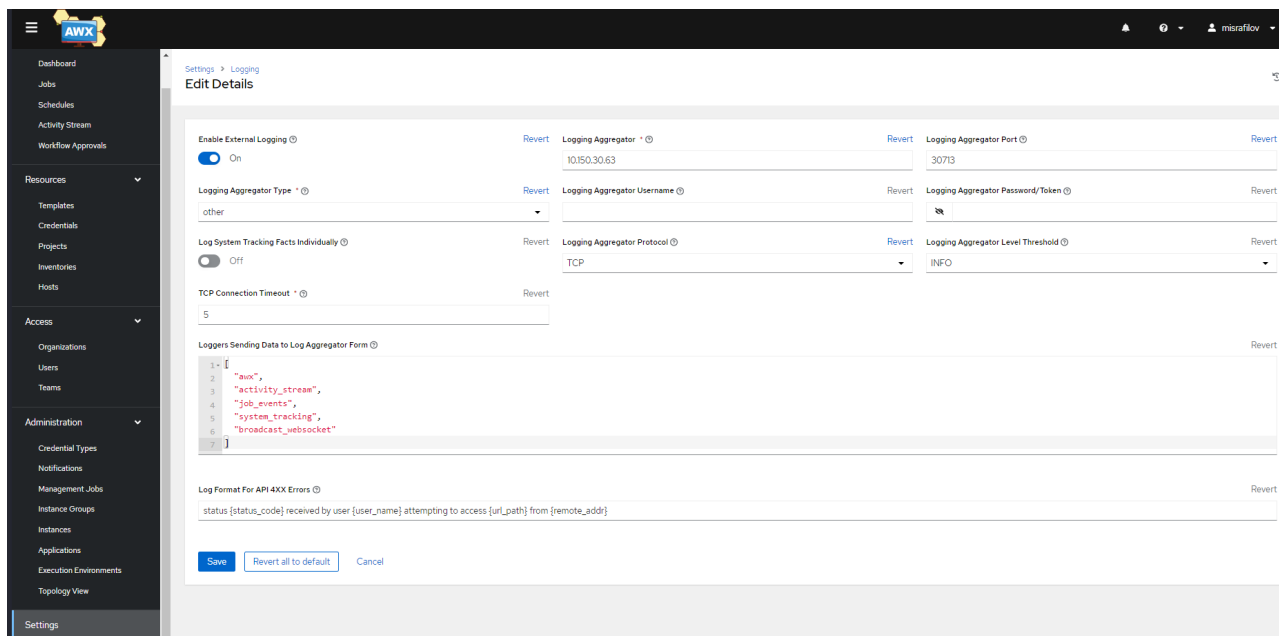
Данное руководство описывает процесс настройки сбора и отправки событий AWX в R-Vision SIEM.

- [Настройка AWX](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Настройка AWX

Чтобы настроить AWX, выполните следующие шаги:

1. Войдите в веб-интерфейс Ansible AWX.
2. Перейдите в раздел **Settings** → **Logging** → **Edit Details**.
3. Задайте следующие параметры:
 - Enable External Logging: переведите переключатель в активное положение.
 - Logging Aggregator Type: выберите из выпадающего списка вариант **Other**.
 - Logging Aggregator: введите IP-адрес коллектора SIEM.
 - Logging Aggregator Protocol: выберите из выпадающего списка вариант **TCP** или **UDP**. Выбор протокола зависит от требований к надежности и безопасности Syslog-сообщений.
 - Logging Aggregator Port: введите порт точки входа типа Syslog.
4. Остальные параметры оставьте без изменений.
5. Сохраните настройки, нажав на кнопку **Save**.



Настройка в R-Vision SIEM

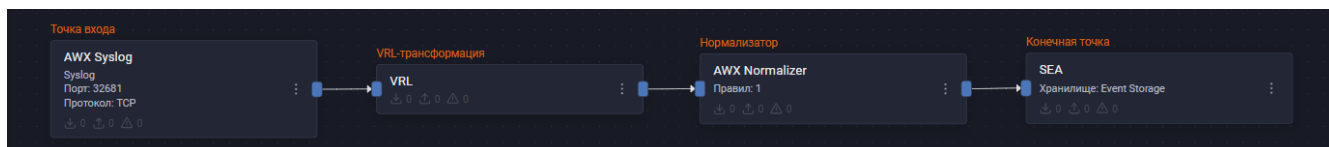
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. Перейдите в раздел **Ресурсы** → **Коллекторы** и создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Syslog**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [AWX](#).
 - Протокол: выберите вариант в соответствии с настройками на стороне [AWX](#).
3. Добавьте на конвейер элемент **VRL-трансформация** со следующим кодом:

```
.dproduct = "AWX"
```

4. Соедините добавленную точку входа и VRL-трансформацию.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Ansible AWX** (идентификатор правила: **RV-N-5**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события Ansible AWX.

Найти события Ansible AWX в хранилище можно по следующему фильтру:

```
dproduct = "AWX"
```



Изменить фильтр

☐ Инvertировать (NOT)

Поле

dproduct

Оператор

=

Значение

AWX

☐ Настроить заголовок

Отменить

Сохранить

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Tower

- [Настройка Tower](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Данное руководство описывает процесс настройки сбора и отправки событий Tower в R-Vision SIEM.

Настройка Tower

Чтобы настроить Tower, выполните следующие шаги:

1. Войдите в веб-интерфейс Ansible AWX.
2. Перейдите в раздел **Settings** → **Logging** → **Edit Details**.
3. Задайте следующие параметры:
 - Enable External Logging: переведите переключатель в активное положение.

- Logging Aggregator Type: выберите из выпадающего списка вариант **Other**.
 - Logging Aggregator: введите IP-адрес коллектора SIEM.
 - Logging Aggregator Protocol: выберите из выпадающего списка вариант **TCP** или **UDP**. Выбор протокола зависит от требований к надежности и безопасности Syslog-сообщений.
 - Logging Aggregator Port: введите порт точки входа типа Syslog.
- Остальные параметры оставьте без изменений.
 - Сохраните настройки, нажав на кнопку **Save**.

The screenshot shows the 'Edit Details' page for the 'Logging' settings in AWX. The left sidebar contains navigation links like Dashboard, Jobs, Schedules, Activity Stream, Workflow Approvals, Resources, Access, Organizations, Users, Teams, Administration, and Settings. The main content area is titled 'Settings > Logging Edit Details'. It features several configuration fields with 'Revert' buttons. The 'Enable External Logging' toggle is turned 'On'. The 'Logging Aggregator' is set to '10.150.30.63' and the 'Logging Aggregator Port' is '30713'. The 'Logging Aggregator Type' is set to 'other'. The 'Logging Aggregator Protocol' is set to 'TCP'. The 'Logging Aggregator Level Threshold' is set to 'INFO'. The 'Log System Tracking Facts Individually' toggle is turned 'Off'. The 'TCP Connection Timeout' is set to '5'. The 'Loggers Sending Data to Log Aggregator Form' is a JSON array: `[\"awx\", \"activity_stream\", \"job_events\", \"system_tracking\", \"broadcast_websocket\"]`. The 'Log Format For API 4XX Errors' is a text field with the value: `status [status_code] received by user [user_name] attempting to access [url_path] from [remote_addr]`. At the bottom, there are 'Save', 'Revert all to default', and 'Cancel' buttons.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

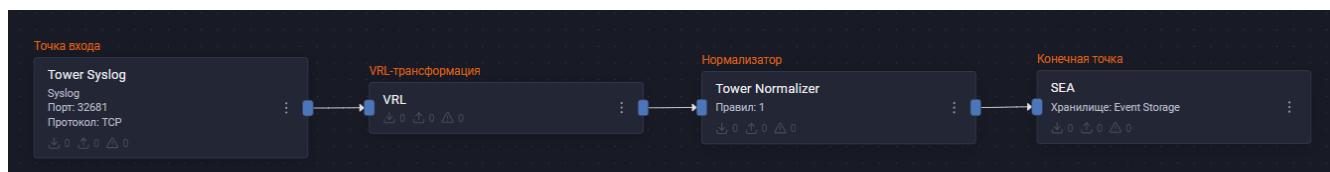
- Перейдите в раздел **Ресурсы** → **Коллекторы** и создайте новый конвейер в коллекторе.
- Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Syslog**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [Tower](#).
 - Протокол: выберите вариант в соответствии с настройками на стороне [Tower](#).
- Добавьте на конвейер элемент **VRL-трансформация** со следующим кодом:

```
.dproduct = "AWX"
```

- Соедините добавленную точку входа и VRL-трансформацию.
- Добавьте на конвейер элемент **Нормализатор** с правилом **Ansible AWX** (идентификатор правила: **RV-N-5**).
- Соедините нормализатор с VRL-трансформацией.

- Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
- Соедините конечную точку с нормализатором.
- Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события Ansible Tower.

Найти события Ansible Tower в хранилище можно по следующему фильтру:

```
dproduct = "AWX"
```



Изменить фильтр

☐ Инvertировать (NOT)

Поле

dproduct

Оператор

=

Значение

AWX

☐ Настроить заголовок

Отменить

Сохранить

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Apache

Данный раздел содержит список систем для настройки сбора событий, распространяемых под эгидой **Apache Software Foundation**:

- [Apache Cassandra](#)
- [Apache HTTP Server](#)

Apache Cassandra

Данное руководство описывает процесс настройки сбора и отправки событий СУБД Apache Cassandra в R-Vision SIEM.

Настройка сбора событий на стороне источника

Для настройки журналирования событий Apache Cassandra выполните следующие шаги:

1. Убедитесь, что на сервере, где установлена Apache Cassandra, доступно не менее 5 ГБ дискового пространства.
2. Подключитесь к серверу Apache Cassandra под учетной записью с правами администратора.
3. Перед внесением изменений создайте резервные копии следующих конфигурационных файлов:
 - `/etc/cassandra/cassandra.yaml` или `/etc/alternatives/cassandra/cassandra.yaml`;
 - `/etc/cassandra/logback.xml` или `/etc/alternatives/cassandra/logback.xml`.
4. Убедитесь, что параметры конфигурационного файла `cassandra.yaml` имеют следующие значения, и при необходимости измените их:
 - в секции `audit_logging_options: enabled = true`;
 - в секции `logger: class_name = FileAuditLogger`.
5. В конфигурационный файл `logback.xml` добавьте следующий фрагмент:

```
<appender name="AUDIT" class="ch.qos.logback.core.rolling.RollingFileAppender">
  <file>${cassandra.logdir}/audit/audit.log</file>
  <rollingPolicy
class="ch.qos.logback.core.rolling.SizeAndTimeBasedRollingPolicy">
    <!-- rollover daily -->
    <fileNamePattern>${cassandra.logdir}/audit/audit.log.%d{yyyy-MM-dd}.%i.zip</fileNamePattern>
    <!-- each file should be at most 50MB, keep 30 days worth of history, but
at most 5GB -->
    <maxFileSize>50MB</maxFileSize>
    <maxHistory>30</maxHistory>
    <totalSizeCap>5GB</totalSizeCap>
  </rollingPolicy>
  <encoder>
    <pattern>%-5level [%thread] %date{ISO8601} %F:%L - %msg%n</pattern>
  </encoder>
```

```
</appender>
<!-- Audit Logging additivity to redirect audit logging events to audit/audit.log
-->
<logger name="org.apache.cassandra.audit" additivity="false" level="INFO">
    <appender-ref ref="AUDIT"/>
</logger>
```

6. Сохраните изменения в конфигурационном файле.
7. Перезапустите службу Apache Cassandra с помощью следующих команд:

```
sudo systemctl stop cassandra.service
sudo systemctl start cassandra.service
```

8. После перезапуска проверьте статус Apache Cassandra с помощью следующей команды:

```
sudo systemctl status cassandra.service
```

Убедитесь, что вывод команды содержит следующее сообщение:

```
Active: active (running)
```

Настройка передачи событий Apache Cassandra завершена. Передаваемые события будут сохраняться в файле `/var/log/cassandra/audit/audit.log`.

Настройка службы rsyslog

1. Создайте файл конфигурации rsyslog:

```
sudo nano /etc/rsyslog.d/01-cassandra.conf
```

2. Добавьте в созданный файл следующее правило:

```
module(load="imfile" PollingInterval="10")

input(type="imfile"
      File="/var/log/cassandra/audit/audit.log"
      startmsg.regex="INFO "
      readTimeout="1"
      escapeLF="off"
      Tag="cassandra-audit")

if $syslogtag contains 'cassandra' then {
    action(type="omfwd" target="<target>" port="<port>" protocol="<protocol>")
    stop
}
```

```
}
```

Здесь:

- **<target>** — IP-адрес или полное доменное имя (FQDN) централизованного syslog-сервера, с которого будет осуществляться отправка сообщений в SIEM.
- **<port>**:
 - либо порт точки входа Syslog в конвейере SIEM — любой свободный порт больше 30000;
 - либо порт сервера rsyslog — **514**.
- **<protocol>** — **tcp** или **udp**.

Настройка syslog-сервера

Для настройки syslog-сервера выполните следующие шаги:

1. Откройте конфигурационный файл rsyslog (**/etc/rsyslog.conf** или **/etc/rsyslog.d/**).
2. Добавьте следующее правило:

```
if $syslogtag contains 'cassandra' then {  
    action(type="omfwd" Target="<target>" Port="<port>" Protocol="tcp")  
    stop  
}
```

Здесь:

- **<target>** — IP-адрес или полное доменное имя (FQDN) централизованного syslog-сервера, с которого будет осуществляться отправка сообщений в SIEM.
 - **<port>** — порт точки входа Syslog в конвейере SIEM — любой свободный порт больше 30000.
3. Перезапустите rsyslog для применения изменений:

```
sudo systemctl restart rsyslog
```

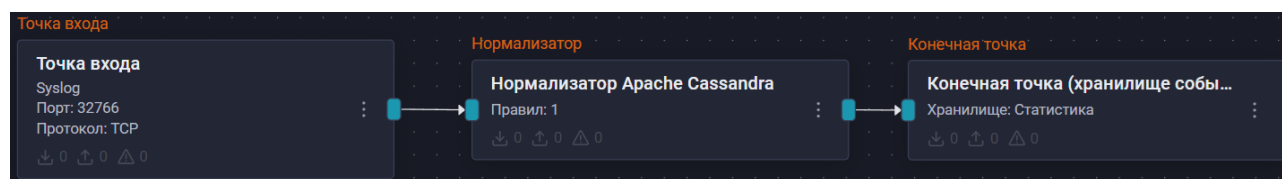
Настройка интеграции с R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте в конвейер элемент **Точка входа** со следующими параметрами:
 - a. **Тип точки входа** — Syslog;
 - b. **Порт точки входа** — в соответствии с настройками на стороне [syslog-сервера](#);
 - c. **Протокол** — TCP.
3. Соедините с точкой входа **Нормализатор** с добавленным правилом нормализации с ID **RV-N-6**.

4. Соедините с нормализатором конечную точку типа **Хранилище событий**.
5. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера



Список типов событий

Список типов событий аудита Apache Cassandra доступен в [официальной документации](#).

Apache HTTP Server

Данное руководство описывает процесс настройки сбора и отправки событий Apache HTTP Server в R-Vision SIEM.

- [Настройка Apache HTTP Server](#)
 - [Описание подсистемы журналирования Apache HTTP Server](#)
 - [Настройка журналирования Apache HTTP Server](#)
 - [Отправка событий Apache HTTP Server](#)
 - [Настройка отправки событий на сервер syslog](#)
 - [Настройка отправки событий в SIEM](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Настройка Apache HTTP Server

Описание подсистемы журналирования Apache HTTP Server

Журналирование событий службы Apache HTTP Server по умолчанию ведется в одной из следующих директорий:

- `/var/log/apache;`
- `/var/log/httpd.`

Запись событий осуществляется следующим образом:

1. В файл `error.log` собираются обращения хостов сети к ресурсам.
2. В файл `access.log` записываются события с ошибками в работе службы веб-сервера.

Настройка журналирования Apache HTTP Server

Для корректного отображения в R-Vision SIEM событий журнала `access` настройте на сервере Apache

формат сообщений согласно следующим рекомендациям:

1. В файле `apache.conf` или `httpd.conf` найдите строку, задающую формат логов, и замените ее на следующий вариант:

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
```



Для сервиса Apache Tomcat необходимо изменить формат лога в файле `server.xml`:

```
%a %{jira.request.id}r %{jira.request.username}r %t &quot;%m %U%q  
%H&quot;; %s %b %D &quot;%{Referer}i&quot;; &quot;%{User-Agent}i&quot;;
```

2. Перезапустите службу Apache HTTP Server с помощью команды:

```
systemctl restart httpd
```

Отправка событий Apache HTTP Server

Настройка отправки событий на сервер syslog

События службы Apache HTTP Server отправляются на централизованный сервер syslog. Затем происходит отправка событий в SIEM.

Чтобы настроить отставку событий службы Apache HTTP Server, выполните следующие шаги:

1. Откройте конфигурационный файл rsyslog: `/etc/rsyslog.conf` или `/etc/rsyslog.d/`.
2. Добавьте в файл следующие правила:

```
module(load="imfile")  
  
input(  
    type="imfile"  
    File="/var/log/httpd/access_log"  
    Tag="Apache_Access"  
    Severity="info"  
    Facility="local4"  
)  
  
input(  
    type="imfile"  
    File="/var/log/httpd/error_log"  
    Tag="Apache_Error"  
    Severity="info"  
    Facility="local4"  
)
```

```
if $syslogtag == 'Apache_Access' or $syslogtag == 'Apache_Error' then {
    action(
        type="omfwd"
        Target="<target>"
        Port="<port>"
        Protocol="udp"
    )
    stop
}
```

Здесь:

- **<target>** — IP-адрес или полное доменное имя (FQDN) сервера syslog.
- **<port>** — порт **514** или любой другой порт, настроенный для приема.

3. Чтобы изменения вступили в силу, перезапустите rsyslog с помощью команды:

```
sudo systemctl restart rsyslog
```

Настройка отправки событий в SIEM

Настройте отправку логов с сервера syslog в SIEM:

1. Откройте конфигурационный файл rsyslog: **/etc/rsyslog.conf** или **/etc/rsyslog.d/**.
2. Добавьте в файл следующее правило:

```
if $syslogtag == 'Apache' then {
    action(type="omfwd" target="target" port="port" protocol="tcp")
    stop
}
```

Здесь:

- **<target>** — IP-адрес или полное доменное имя (FQDN) узла кластера Kubernetes, на котором запущен коллектор SIEM.
- **<port>** — порт точки входа Syslog: значение в диапазоне 30000–32767.

3. Чтобы изменения вступили в силу, перезапустите rsyslog с помощью команды:

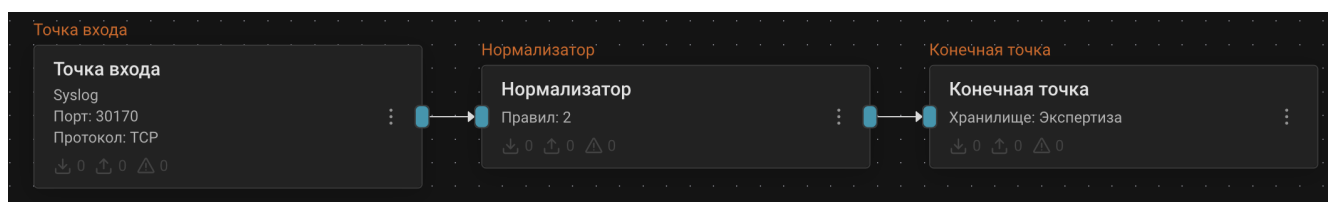
```
sudo systemctl restart rsyslog
```

Настройка в R-Vision SIEM

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:

- Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Syslog**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [Apache HTTP Server](#).
 - Протокол: выберите вариант в соответствии с настройками на стороне [Apache HTTP Server](#).
- Добавьте на конвейер элемент **Нормализатор** с правилами **Apache HTTP-server** (идентификатор правила: **RV-N-7**) и **Apache HTTP-server** (идентификатор правила: **RV-N-8**).
 - Соедините нормализатор с точкой входа.
 - Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
 - Соедините конечную точку с нормализатором.
 - Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события Apache HTTP Server.

Найти события Apache HTTP Server в хранилище можно по следующему фильтру:

`dproduct = "Apache"`



Совпадений 8

Интервал: 2025-05-06T09:51:41.099+03:00 - 2025-05-06T09:56:41.099+03:00

Показать график

timestamp	dvendor	dproduct
2025-05-06T09:56:30.000+03:00	Apache	Apache
2025-05-06T09:56:28.000+03:00	Apache	Apache
2025-05-06T09:56:26.000+03:00	Apache	Apache
2025-05-06T09:56:24.000+03:00	Apache	Apache
2025-05-06T09:56:22.000+03:00	Apache	Apache
2025-05-06T09:56:20.000+03:00	Apache	Apache

Показывается первых 50 записей.

Детали события 854f72fa-04d7-4b4...

☒ Скрыть пустые поля события

Дата и время

timestamp: 2025-05-06T09:56:30.000+03:00

Служебные данные

id: 854f72fa-04d7-4b44-81a8-a80c9827245f

tenantid: 00000000-0000-0000-0000-000000000000

collectorid: a7fdf468-2c31-4e48-91a2-68559ad42d21

type: нормализованное событие

Сведения о событии

dvendor: Apache

dproduct: Apache

dversion: 2+

severity: info

cat: Access Log

dvchost: jira01

externalid: 200

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по](#)

ссылке.

Bind DNS

Данное руководство описывает процесс настройки сбора и отправки событий Bind DNS в R-Vision SIEM.

- [Настройка Bind DNS](#)
 - [Настройка журналирования Bind DNS](#)
 - [Отправка событий Bind DNS](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Настройка Bind DNS

В настоящем руководстве рассматривается передача событий с помощью службы syslog-ng. Предполагается, что syslog-ng на станции с ОС Linux уже установлен.

Настройка журналирования Bind DNS

Для настройки журналирования Bind DNS выполните следующие действия:

1. Добавьте в файл `/etc/bind/named.conf` следующую строку:

```
include "/etc/bind/named.conf.local";
```

2. Добавьте в файл `/etc/bind/named.conf.local` следующие строки:

```
logging {
    channel default_channel {
        file "/var/log/named/default.log";
        print-time yes;
        print-category yes;
        print-severity yes;
        severity dynamic;
    };
    channel general_channel {
        file "/var/log/named/general.log";
        print-time yes;
        print-category yes;
        print-severity yes;
        severity dynamic;
    };
    channel notify_channel {
        file "/var/log/named/notify.log";
        print-time yes;
        print-category yes;
        print-severity yes;
    };
}
```

```

        severity dynamic;
    };
    channel network_channel {
        file "/var/log/named/network.log";
        print-time yes;
        print-category yes;
        print-severity yes;
        severity dynamic;
    };
    channel queries_channel {
        file "/var/log/named/queries.log";
        print-time yes;
        print-category yes;
        print-severity yes;
        severity dynamic;
    };
    channel query-errors_channel {
        file "/var/log/named/query-errors.log";
        print-time yes;
        print-category yes;
        print-severity yes;
        severity dynamic;
    };
    channel lame-servers_channel {
        file "/var/log/named/lame-servers.log";
        print-time yes;
        print-category yes;
        print-severity yes;
        severity dynamic;
    };
    category default { default_channel; };
    category general { general_channel; };
    category notify { notify_channel; };
    category network { network_channel; };
    category queries { queries_channel; };
    category query-errors { query-errors_channel; };
    category lame-servers { lame-servers_channel; };
};

```

3. Перезапустите сервис bind9-pkcs11 с помощью команды:

```
# systemctl restart bind9-pkcs11.service
```

Журналирование Bind DNS настроено.

Отправка событий Bind DNS

Для настройки передачи событий из файлов Bind DNS выполните следующие действия:

1. Создайте файл `/etc/syslog-ng/conf.d/binddns-siem.conf` со следующим содержимым:

```
source binddns {
    file("/var/log/bind/default.log" flags(no-parse) log_prefix("BIND-DNS-
default: "));
    file("/var/log/bind/general.log" flags(no-parse) log_prefix("BIND-DNS-
general: "));
    file("/var/log/bind/queries.log" flags(no-parse) log_prefix("BIND-DNS-
queries: "));
    file("/var/log/bind/query-errors.log" flags(no-parse) log_prefix("BIND-DNS-
query-errors: "));
    # в случае необходимости, остальные файлы можно добавить по аналогии
};

destination siem {
    udp("<target>" port(<port>)); # указать IP и порт точки входа SIEM
};

log {
    source(binddns); destination(siem);
};
```

Здесь:

- `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- `<port>` — порт точки входа Syslog на конвейере SIEM.

2. Перезапустите сервис `syslog-ng` с помощью команды:

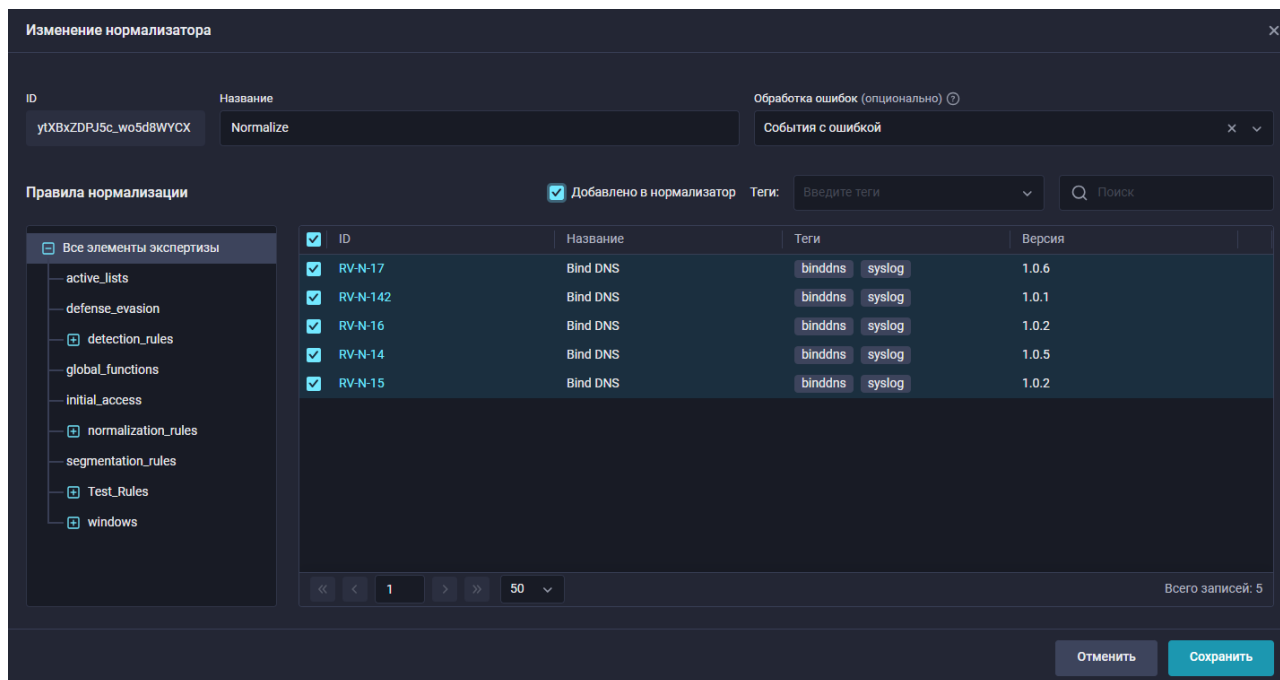
```
# systemctl restart syslog-ng
```

Отправка событий Bind DNS настроена.

Настройка в R-Vision SIEM

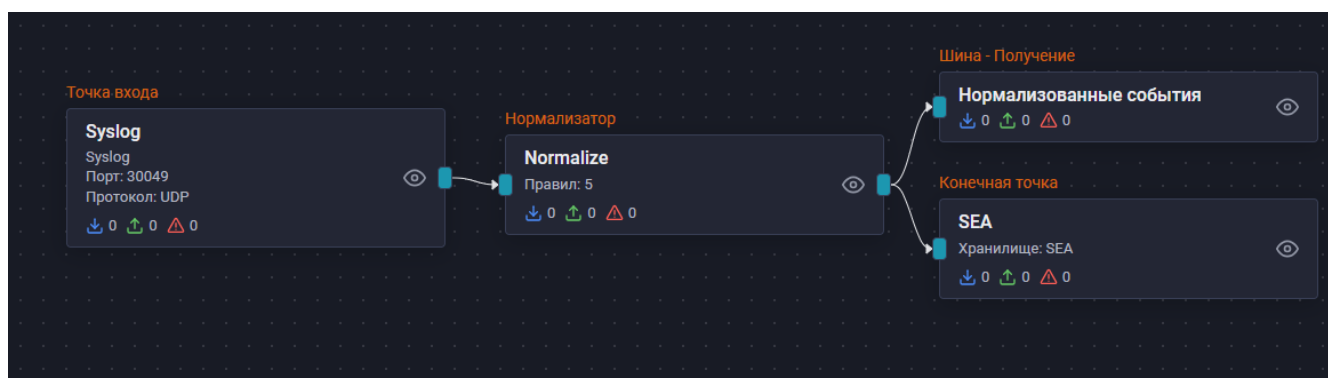
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Syslog**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [Bind DNS](#).
 - Протокол: выберите вариант в соответствии с настройками на стороне [Bind DNS](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилами **Bind DNS** (идентификаторы правил: **RV-N-14, RV-N-15, RV-N-16, RV-N-17, RV-N-142**).



4. Соедините точку входа с нормализатором.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. При необходимости добавьте на конвейер элемент **Шина**, настроенный на получение. Он используется для проброса событий между конвейерами.
7. Соедините конечную точку и шину с нормализатором.
8. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события Bind DNS.



Найти события Bind DNS в хранилище можно по следующему фильтру:

```
dproduct = "BIND"
```

Добавить фильтр

☐ Инвертировать (NOT)

Поле

Оператор

Значение

dpproduct

=

BIND

☐ Настроить заголовок

Отменить

Добавить

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

91

Cisco

Данный раздел содержит список систем для настройки от компании Cisco:

- [Cisco ASA](#)
- [Cisco Firepower 6](#)

Cisco ASA

Данное руководство описывает процесс настройки отправки событий межсетевого экрана Cisco ASA в R-Vision SIEM.

- [Настройка Cisco ASA](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Настройка Cisco ASA

Настройте передачу событий по **syslog**. Для этого в режиме конфигурации терминала выполните следующие действия:

1. Включите логирование командой:

```
ciscoasa(config)# logging enable
```

2. Укажите интерфейс, адрес коллектора SIEM, протокол и порт:

```
ciscoasa(config)# logging host <iface> <target> <protocol> /<port>
```

Здесь:

- **<iface>** — интерфейс, через который будут отправляться события.
- **<target>** — IP-адрес коллектора SIEM.
- **<port>** — порт точки входа Syslog в конвейере SIEM.
- **<protocol>** — сетевой протокол: **tcp** или **udp**.

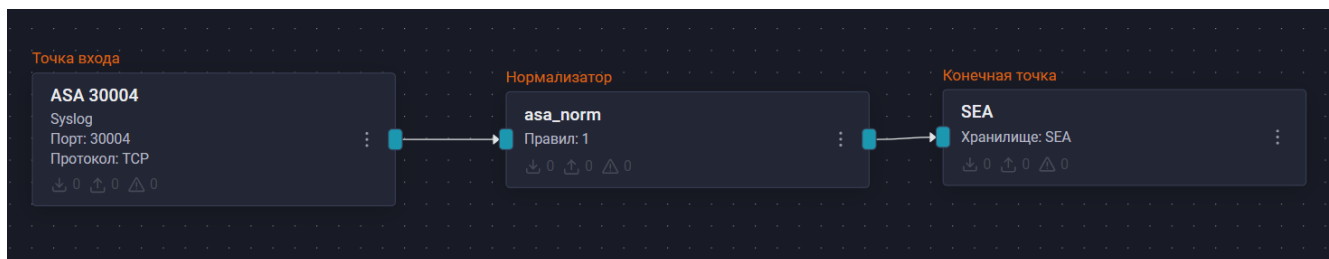
Настройка в R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие действия:

1. В интерфейсе R-Vision SIEM перейдите в раздел **Ресурсы** → **Коллекторы** и откройте карточку коллектора.
2. На вкладке **Обогащение** добавьте таблицу **ASA_events_et** обогащения коллектора.
3. В том же коллекторе создайте новый конвейер.

- Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Syslog;
 - Порт точки входа и протокол: в соответствии с настройками на стороне [Cisco ASA](#).
- Добавьте на конвейер элемент **Нормализатор** с правилом Cisco ASA (Идентификатор правила: RV-N-22). Соедините нормализатор с точкой входа.
- Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
- Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



Если настройка выполнена корректно, после [настройки передачи событий](#) в хранилище начнут поступать события Cisco ASA.

Найти события Cisco ASA в хранилище можно по следующему фильтру:

`dproduct = "ASA"`



События Хранилище событий: **SEA**

Введите запрос и наж... Последний период 24 часа Поиск

Сбросить все dvendor EQ Cisco externalid EQ 113015 + Добавить фильтр

Совпадений 1 Интервал 2024-08-25T16:10:19.812+03:00 - времени: 2024-08-26T16:10:19.812+03:00 Показать график

id	sourceip	timestamp	type	dvendor
e81c4a1d-72f0-46d0-bffd...		2024-08-26T11:28:13.000+...	нормализованное событие	Cisco

Детали события e81c4a1d-72f0-46d...

dproduct	ASA
severity	Informational
cat	AAA user authentication
deviceFacility	local4
dvchost	eveasa
externalid	113015
msg	AAA user authentication Rejected : reason = Invalid password : local database : user = admin : user IP = 172.17.1.3
outcome	failure
reason	Invalid password
rt	2024-08-26T11:28:11.000+03:00
src	172.17.1.3
user	admin
cs1	A request for authentication to the user database for a user associated with an IPsec or WebVPN connection has been rejected. The username is hidden when invalid or unknown, but appears when valid or the no logging hide username command has been configured.

Показывается первых записей: 500 00:01.028

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Cisco Firepower 6

Данное руководство описывает процесс настройки сбора и отправки событий модульной платформы безопасности Cisco Firepower в R-Vision SIEM.

- [Настройка Cisco Firepower](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Настройка Cisco Firepower

Устройства Firepower поддерживают возможность передачи событий с помощью службы **syslog**.

В экосистему Firepower входят следующие устройства:

- Firepower Management Center (Firepower MC) — узел централизованного управления устройствами Firepower.
- Firepower Next Generation IPS (Firepower NGIPS) — узел, исполняющий функции IPS.
- Firepower Threat Defense (Firepower FTD) — узел, предотвращающий вторжения. Выполняет функции контроля и видимости приложений (Application Visibility and Controls, AVC), фильтрации URL, идентификации и аутентификации пользователей, а также защиты от вредоносных программ.
- Cisco Adaptive Security Appliance (ASA) — межсетевой экран, выполняющий функции узлов, перечисленных выше (кроме MC). Также может выступать в качестве модулей для ASA. Инструкция по настройке Cisco ASA [представлена по ссылке](#).

Алгоритмы подключения устройств через Firepower MC:

- [Настройка Firepower MC](#)
- [Настройка Firepower NGIPS](#)
- [Настройка Firepower FTD](#)

Настройка Firepower MC

Для настройки Firepower MC выполните следующие действия:

1. Войдите в веб-интерфейс Cisco Firepower MC.
2. Нажмите на кнопку  и перейдите на вкладку **configuration**.
3. На вкладке **Audit Log** заполните поля:
 - **Send Audit Log to Syslog** — установите значение **Enabled**.
 - **Hosts (Up to 5)** — введите адрес коллектора SIEM.
 - **Facility** — выберите категорию для событий, поступающих с устройства.
 - **Severity** — выберите уровень событий для отправки в SIEM.
 - **Tag** — введите Cisco MC.

Для полей **Send Audit Log to HTTP Server** и **URL to Post Audit** заполнение не требуется.

Рекомендуем предварительно проверить соединение, нажав на кнопку **Test Syslog Server**.

The screenshot shows the 'Audit Log' configuration interface. On the left is a dark sidebar with a menu. The 'Audit Log' option is highlighted. The main panel has a light gray background. At the top right of the main panel is a blue 'Save' button. The configuration fields are as follows:

- Send Audit Log to Syslog:** A dropdown menu set to 'Enabled'.
- Hosts (Up to 5):** A text input field containing '10.150.49.240'.
- Facility:** A dropdown menu set to 'LOCAL7'.
- Severity:** A dropdown menu set to 'DEBUG'.
- Tag (optional):** A text input field containing 'Cisco MC'.
- Send Audit Log to HTTP Server:** A dropdown menu set to 'Disabled'.
- URL to Post Audit:** An empty text input field.

At the bottom right of the main panel is a blue button labeled 'Test Syslog Server'.

4. Нажмите на кнопку **Save**.

Настройка Firepower NGIPS

Для настройки Firepower NGIPS выполните следующие действия:

1. Перейдите в раздел **Devices** → **Platform Settings**.
2. Если для платформы еще не создана политика, создайте ее. Для этого:
 - a. Нажмите на кнопку **New Policy**.
 - b. Выберите **тип платформы** — Firepower Settings.
 - c. В появившейся форме заполните поля и выберите устройства Firepower NGIPS, с которых планируете передавать события в SIEM.
3. Перейдите на страницу настройки политики, нажав на кнопку .
4. Перейдите в раздел **Audit Log**.
5. Заполните поля по аналогии с Firepower MC, заменив значение поля **Tag** на **Cisco NGIPS**.
6. Нажмите на кнопку **Save**.

Настройка Firepower FTD

Для настройки Firepower FTD выполните следующие действия:

1. Перейдите в раздел **Devices** → **Platform Settings**.
2. Если для платформы еще не создана политика, создайте ее. Для этого:
 - a. Нажмите на кнопку **New Policy**.
 - b. Выберите **тип платформы** — Threat Defense Settings.
 - c. В появившейся форме заполните **поля** и выберите **устройства** Firepower FTD, с которых

планируете передавать события в SIEM.

3. Перейдите на страницу настройки политики, нажав на кнопку .
4. Перейдите в раздел **Syslog**.
5. На вкладке **Logging Setup** установите флажки рядом со следующими опциями:
 - Enable Logging
 - Enable Logging on the failover standby unit
 - Send debug messages as syslogs
6. На вкладке Logging Destinations создайте точку отправки. Для этого выполните следующие действия:
 1. Нажмите на кнопку **Add** и выберите следующие пункты:
 - Logging Destination — Syslog Servers.
 - Event Class - Filter on Severity и выберите уровень логирования.
 2. Нажмите кнопку **OK**.

Edit Logging Filter ?

Logging Destination

Syslog Servers ▼

Event Class

Filter on Severity ▼

informational ▼

+ Add

Event Class	Syslog Severity	
No records to display		

Cancel

OK

7. На вкладке **Syslog Settings** настройте следующие поля:
 - **Facility** — выберите категорию для событий, поступающих с устройства;
 - **Enable Timestamp on Syslog Messages** — включите;
 - **Timestamp Format** — выберите формат RFC 5424;
 - **Enable Syslog Device ID** — включите;
 - **Host Name** — выберите имя хоста.
8. На вкладке **Syslog Servers** создайте точку отправки. Для этого выполните следующие действия:
 - а. Нажмите на кнопку **Add** и заполните поля:

- **IP Address** — выберите объект-хост, в котором указан IP-адрес коллектора или нажмите на **+**, чтобы создать объект типа **host**;
- **Protocol** — протокол, настроенный на точке сбора коллектора SIEM;
- **Port** — порт, слушаемый коллектором;
- **Reachable By** — варианты управления сервером (выберите Device Management Interface).

Edit Syslog Server

IP Address*

MySyslog

+

Protocol

☒ TCP
 ☐ UDP

Port

514

(514 or 1025-65535)

Log Messages in Cisco EMBLEM format(UDP only)

☐

Enable secure syslog.

☐

Reachable By:

☒ Device Management Interface (Applicable on FTD v6.3.0 and above)
 ☐ Security Zones or Named Interface

Available Zones

Q Search

External

Internal

Add

Selected Zones/Interfaces

Interface Name

Add

Cancel

OK

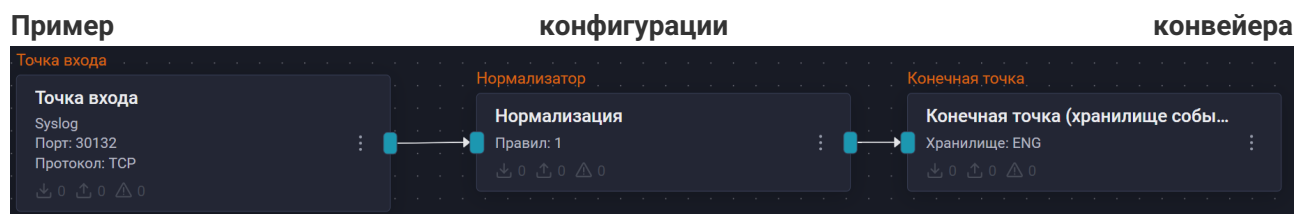
9. Нажмите на кнопку **Save**. После настройки политик перейдите на вкладку **Deploy** → **Deployment**, выберите все устройства и нажмите на кнопку **Deploy**.

Настройка в R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:

- a. **Тип точки входа** — Syslog;
- b. **Порт точки входа** и **Протокол** — в соответствии с настройками на стороне syslog-сервера.
3. Добавьте на конвейер элемент **Нормализатор** с соответствующим правилом (id:RV-N-23). Соедините нормализатор с точкой входа.
4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
5. Сохраните и установите конфигурацию конвейера.



Информацию о событиях Firepower можно посмотреть в [официальной документации Cisco](#).

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Citrix

Данный раздел содержит список систем для настройки от компании Citrix:

- [Netscaler](#)
- [XenApp](#)

Netscaler

Данное руководство содержит инструкции по настройке Citrix, который позволяет использовать ресурсы серверов и сети и повышать скорость доставки веб-приложений.

Настройка источника событий

Citrix CTX120609 обеспечивает синхронизацию и настройку системных журналов NetScaler с помощью Newsyslog. По умолчанию Citrix ADC хранит несколько системных журналов на локальном устройстве.



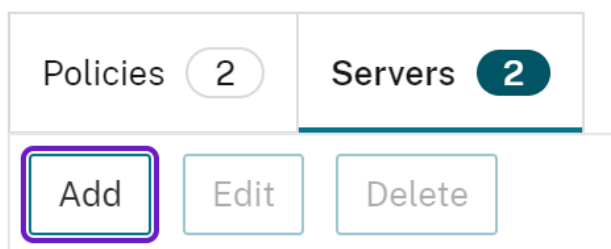
Краткое описание типов событий, регистрируемых в каждом из журналов, представлено в [документации Citrix](#).

Рассмотрим настройку на примере журнала аудита **User Configurable Log Messages**.

Чтобы создать политику для отправки записи системного журнала на внешний сервер syslog:

1. В интерфейсе NetScaler перейдите в раздел **System** → **Auditing** → **Syslog**.
2. Перейдите на вкладку **Servers** и нажмите на кнопку **Add**.

Syslog Auditing



3. Укажите данные сервера:

- **Name** — имя сервера (например, syslog).
- В выпадающем списке **Server Type** выберите Server IP и в поле **IP Address** укажите IP-адрес сервера.

Либо в выпадающем списке **Server Type** выберите Server Domain Name и в поле **Server Domain Name** введите полное доменное имя сервера.

- **Port** — 514.

4. В блоке **Log Levels** укажите параметры логирования:

- Выберите нужный уровень логирования.
- В выпадающем списке **Date Format** выберите формат даты.
- Установите флажок **User Configurable Log Messages**.

Log Levels

☐ ALL
 ☐ NONE
 ☒ CUSTOM
 ?

☒ EMERGENCY
 ☒ ALERT
 ☒ CRITICAL
 ☒ ERROR
 ☒ WARNING
 ☒ NOTICE
 ☒ INFORMATIONAL
 ☐ DEBUG

Log Facility*

LOCAL0

▼

Date Format*

YYYYMMDD

▼

?

Time Zone

☒ GMT
 ☐ Local

☐ TCP Logging
 ☐ ACL Logging
 ☒ User Configurable Log Messages ?
☐ AppFlow Logging
 ☐ Large Scale NAT Logging
 ☐ ALG messages Logging
 ☐ Subscriber Logging
 ☐ DNS
 ☐ SSL Interception
 ☐ URL Filtering
 ☐ Content Inspection Logging

- Нажмите на кнопку **Create**.
- Перейдите во вкладку **Policies** и нажмите на кнопку **Add**.

Syslog Auditing

Policies 2

Servers 2

Add

Edit

Delete

Select Action ▼

- Укажите параметры политики:
 - **Name** — имя политики (например, syslog);
 - **Expression Type** — выберите **Advanced Policy**
 - **Server** — выберите созданный ранее сервер.
- Нажмите на кнопку **Create**.
- На вкладке **Policies** выберите в раскрывающемся списке **Select Action** пункт **Advanced Policy Global Bindings**. Нажмите на кнопку **Add Binding**.
- Укажите параметры привязки политики:
 - **Select Policy** — название ранее созданной политики;
 - **Priority** — 100 или меньше;

- **Global Bind Type** — SYSTEM_GLOBAL.

Нажмите на кнопку **Bind**.

Настройка логирования и отправки логов на сервер syslog завершена.



Настройка логирования подробно описана в [документации Citrix](#).

Настройка сервера syslog

Для настройки сервера syslog выполните следующие шаги:

1. Откройте конфигурационный файл rsyslog (`/etc/rsyslog.conf` или `/etc/rsyslog.d/`).
2. Добавьте следующее правило обработки:

```
# Укажите IP-адрес Citrix NetScaler
if $fromhost-ip=='192.0.2.0' then {
# Укажите адрес и порт SIEM
  action(type="omfwd" target="siem.sea.land" port="30000" protocol="tcp")
  stop
}
```

3. Перезапустите rsyslog, чтобы изменения вступили в силу:

```
sudo systemctl restart rsyslog
```

Настройка конвейера для сбора событий аудита

Для интеграции источника с R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - a. **Тип точки входа** — Syslog;
 - b. **Порт точки входа** и **Протокол** — в соответствии с настройками на стороне [сервера syslog](#).
3. Добавьте на конвейер элемент **VRL-трансформация** со следующим кодом:

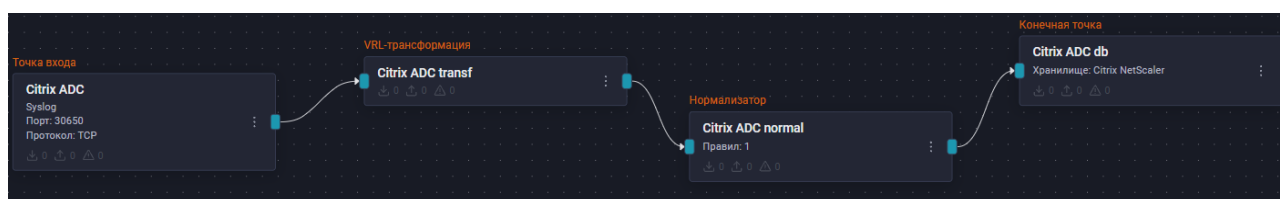
```
.dproduct="Citrix Net Scaler"
```

Соедините VRL-трансформацию с точкой входа.

4. Добавьте на конвейер **Нормализатор** с правилом **Citrix NetScaler**. Соедините нормализатор с VRL-трансформацией.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.

6. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера



Если настройка выполнена корректно, в хранилище начнут поступать события Citrix NetScaler.

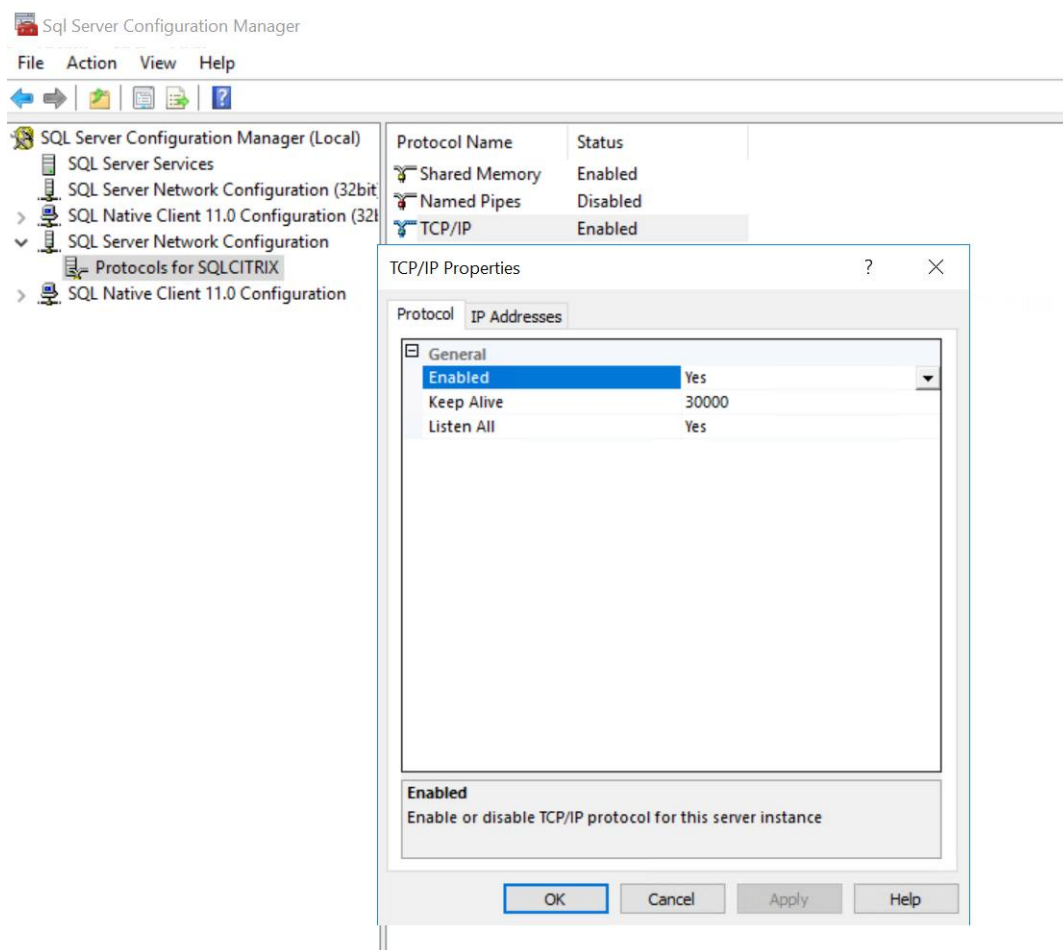
XenApp

XenApp — это программное обеспечение для виртуализации и доставки приложений с удаленного сервера на локальные устройства через тонкий клиент. XenApp позволяет запускать приложения для Windows на компьютерах и мобильных устройствах под управлением других операционных систем. Сами приложения находятся на выделенном сервере или в облаке.

Настройка источника событий

1. Создайте учетную запись в СУБД MS SQL. Для этого:
 - a. Подключитесь к СУБД посредством SQL Server Management Studio под доменной учетной записью.
 - b. Вызовите контекстное меню для **security/logins** и выберите опцию **New login**.
 - c. Укажите параметры сервисной учетной записи:
 - **Имя для входа;**
 - Выберите опцию **Проверка подлинности SQL Server;**
 - **Пароль;**
 - **База данных по умолчанию** — название экземпляра БД, используемой XenApp.
2. Перейдите в настройки **SQL Server Configuration Manager** и убедитесь, что TCP/IP включен в конфигурации сети **SQL Server**. Для этого перейдите в раздел **SQL Server Network Configuration** → **Protocols for SQLCITRIX**.

Появится окно с настройкой TCP/IP, где в параметре **Enabled** должно быть указано **Yes**.



Настройка интеграции с R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - a. **Тип точки входа** — Database;
 - b. **Драйвер базы данных** — необходимый для **MSSQL**
 - c. **Адрес подключения** — укажите заранее созданный секрет.
 - d. **SQL-запрос** — введите следующий:

```
SELECT LowEv.Uid as uid
      ,LowEv.Text as msg
      ,HighEv.Text as HighEventText
      ,LowEv.AdminMachineIP as src
      ,LowEv.AdminId as AdminUid
      ,AdminAccountName as suser
      ,(DATEADD(hour,DATEDIFF(hour,GETUTCDATE()),GETDATE()),LowEv.EndTime)) AS
endtime
      ,LowEv.Source as appname
      ,LowEv.SourceSdk as appnameSDK
      ,LowEv.HighLevelOperationUid as HighLevelOperationUid
      ,(DATEADD(hour,DATEDIFF(hour,GETUTCDATE()),GETDATE()),LowEv.StartTime)) AS
```

```

starttime
,LowEv.IsSuccessful as status
FROM
<database>.ConfigLoggingSchema.LowLevelOperationView as LowEv
LEFT JOIN <database>.ConfigLoggingSchema.Users as XenAppUsers ON LowEv.AdminId =
XenAppUsers.Id
LEFT JOIN <database>.ConfigLoggingSchema.HighLevelOperationView AS HighEv ON
LowEv.HighLevelOperationUid = HighEv.Uid WHERE
(DateAdd(hour,DATEDIFF(hour,GETUTCDATE()),GETDATE()),(DateAdd(hour,DATEDIFF(hour,
GETUTCDATE()),GETDATE()),LowEv.StartTime)) ) >= DateAdd(Minute, -1, GetDate()))

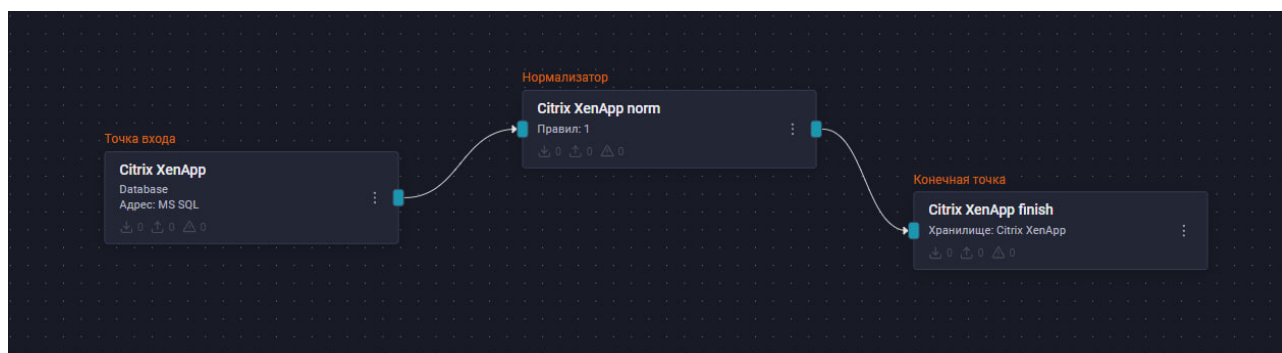
```

Здесь **<database>** — название экземпляра БД, используемой XenApp.

е. **Интервал запроса** — 60 секунд.

- Добавьте на конвейер **Нормализатор** с правилом **Citrix XenApp 7.x** (идентификатор **RV-N-127**). Соедините нормализатор с точкой входа.
- Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
- Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера



Таблицы маппинга

Таблица 12. Общий маппинг

Поле модели событий	Значение
act	raw.msg[0]
cat	raw.appnameSDK
dvendor	"Citrix"
dproduct	"XenApp"
dversion	"7.x"
destinationServiceName	raw.appname
externalId	raw.uid
suser	raw.suser
suid	raw.AdminUid

Поле модели событий	Значение
startTime	raw.starttime
endTime	raw.endtime
outcome	"success" или "failure" (зависит от успешности/ не успешности выполняемого действия)
src	raw.src
name	raw.HighEventText

Таблица 13. Конкретные действия

Поле модели событий	Добавление или удаление пользователя с машины	Изменение логирования	Запрос аналитики из БД	Добавление нового объекта в XenApp
msg	Сообщение, приведенное к человекочитаемому виду + objName + suser	Сообщение, приведенное к человекочитаемому виду + suser	Сообщение, приведенное к человекочитаемому виду + suser	Сообщение, приведенное к человекочитаемому виду + suser + objType+ objName.
objType	Извлекается из raw.msg	"Configure"	"Data"	Извлекается из raw.msg
objName	Извлекается из raw.msg	"Logging"		Извлекается из raw.msg
dntdom	Извлекается из raw.msg			
dhost	Извлекается из raw.msg			

Данное руководство описывает процесс настройки сбора и отправки событий физических и виртуальных маршрутизаторов семейства Eltex ESR в R-Vision SIEM.

Настройка сбора событий на стороне источника

Настройка физического маршрутизатора

1. Установите и подключите устройство согласно официальной документации. Подключите его питание и интерфейс управления.
2. Выполните первое подключение к устройству через консольный порт и войдите в систему. Данные для входа по умолчанию: логин — **admin**, пароль — **password**.
3. Перейдите в раздел [Конфигурация логирования](#).

Настройка виртуального маршрутизатора Eltex vESR

1. Получите файл виртуальной машины, который распространяется производителем оборудования.
2. Загрузите полученный файл на ваш гипервизор. Требования к виртуальной машине:
 - 1 ядро CPU;
 - 4 ГБ ОЗУ;
 - 8 ГБ на жестком диске;
 - сетевой интерфейс.
3. Запустите виртуальную машину. Первичная загрузка может длиться около 15 минут.
4. Войдите в виртуальную машину. Данные для входа по умолчанию: логин — **admin**, пароль — **password**.
5. Перейдите в раздел [Конфигурация логирования](#).

Конфигурация логирования

1. Перейдите в меню конфигурации с помощью команды:

```
configure
```

2. Настройте сбор логов с необходимых журналов, выполнив для каждого из них команду:

```
logging <journal-name>
```

Здесь:

- **<journal-name>** — имя журнала.



Список поддерживаемых журналов приведен для физического маршрутизатора Eltex ESR-200 и виртуального маршрутизатора Eltex vESR 0.18.4. Список поддерживаемых журналов для других моделей и версий смотрите в документации производителя.

Поддерживаются следующие журналы:

- **aaa** — журнал авторизации и аутентификации;
- **acl** — журнал работы со списками контроля доступа;
- **firewall** — журнал параметров файрвола;
- **ips** — журнал IP-адресов;
- **login** — журнал параметров логина;
- **nat** — журнал NAT;
- **service** — журнал сервисных параметров;
- **syslog** — журнал параметров syslog;
- **userinfo** — журнал изменений в профиле пользователя.

3. Настройте отправку логов в syslog-коллектор с помощью команды:

```
syslog host <hostname>
```

Здесь:

- **<hostname>** — имя вашего хоста в системе Eltex.

4. Перейдите в меню настройки вашего хоста. Для отправки логов укажите следующие параметры конфигурации:

- **remote-address** — адрес syslog-коллектора. Поддерживаются IPv4 и IPv6 адреса.
- **port** — порт прослушивания syslog-коллектора.
- **severity** — начиная с какого уровня логирования, события будут передаваться в SIEM. Доступные уровни логирования:
 - **emerg** — критическая ситуация;
 - **alert** — небезопасные действия;
 - **crit** — проверка состояния;
 - **error** — ошибка;
 - **warning** — вывод предупреждений;
 - **notice** — события в рамках ожидаемого поведения;
 - **info** — статистика;
 - **debug** — отладка поступающих сообщений;
 - **none** — события не передаются.
- **transport** — протокол передачи данных: **udp** или **tcp**.

Пример общей настройки параметров:

```
remote-address 192.168.0.1
port 30104
severity info
transport udp
```

5. Выйдите в основное меню настройки с помощью команды:

```
exit
```

Команду необходимо ввести два раза.

6. Примените изменения и запишите их в память устройства с помощью команд:

```
commit
confirm
```

7. Сохраните конфигурацию с помощью команды:

```
save
```

Настройка интеграции с R-Vision SIEM

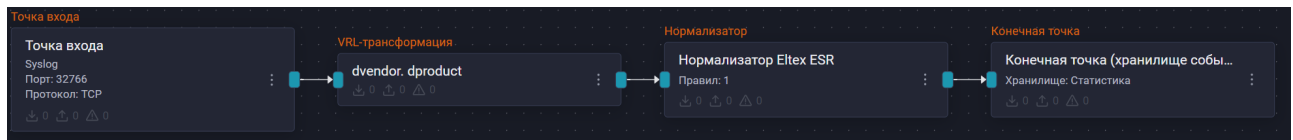
Для интеграции источника с R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте в конвейер элемент **Точка входа** со следующими параметрами:
 - a. **Тип точки входа** — Syslog;
 - b. **Порт точки входа** и **Протокол** — в соответствии с настройками на стороне [Eltex ESR](#).
3. Добавьте VRL-трансформацию:

```
.dvendor = "EltexESR"
.dproduct = "ESR"
```

4. Соедините с VRL-трансформацией **Нормализатор** с добавленным правилом нормализации с ID **RV-N-33**.
5. Соедините с нормализатором конечную точку типа **Хранилище событий**.
6. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера



MES

В этом руководстве описано, как настроить отправку логов с коммутаторов Eltex MES в систему R-Vision SIEM.

Настройка оборудования

1. Подключитесь к устройству через консольный порт.
2. Войдите в систему. Данные для входа по умолчанию:
 - логин — **admin**;
 - пароль — **admin**.
3. Перейдите в меню конфигурации с помощью команды:

```
configure
```

4. Включите типы сообщений, которые будут регистрироваться, командой **logging**. Доступно включение следующих типов:
 - **logging on** — все доступные типы логирования;
 - **aaa logging login** — события аутентификации, авторизации и учета (AAA);
 - **logging events link-status** — изменения состояний интерфейсов;
 - **logging events spanning-tree port-state-change** — изменения статуса интерфейсов в STP;
 - **logging events spanning-tree topology-change** — изменения топологии в STP;
 - **logging events spanning-tree root-bridge-change** — смена root bridge;
 - **logging events ddm threshold** — изменения параметров SFP с DDM;
 - **logging cli-commands** — команды, введенные в командной строке;
 - **file-system logging <copy | delete-rename>** — события файловой системы, где:
 - **copy** — копирование файлов;
 - **delete-rename** — удаление и переименование файлов.
 - **management logging deny** — события запрета доступа к управлению коммутатором;
 - **logging service cpu-rate limits <traffic>** — ограничения скорости входящих кадров для определенного типа трафика, где **<traffic>** — один из типов http, telnet, ssh, snmp, ip, link-local, arp, switch-mode, arp inspection, stp-bpdu, other-bpdu, dhcp snooping, dhcpv6 snooping, igmp-snooping, mld-snooping, sflow, log deny-aces, vrrp.

Чтобы отключить какой-либо тип логирования, используйте ключевое слово **no**, например:

```
no logging cli-commands
```

5. Настройте параметры логирования командой **logging**:

- **logging aggregation on** — группировать сообщения;
- **logging origin-id <id>** — использовать указанный идентификатор хоста в сообщениях syslog, где <id> — строка, имя хоста, IPv4 или IPv6-адрес;
- **logging source-interface <interface>** — использовать IP-адрес указанного интерфейса в качестве источника в IP-пакетах протокола syslog;
- **logging source-interface-ipv6 <interface>** — использовать IPv6-адрес указанного интерфейса в качестве источника в IP-пакетах протокола syslog;

Чтобы посмотреть данные логирования, запустите в основном интерфейсе Eltex MES следующую команду:

```
show logging
```

Пример результатов команды **show logging**

```
MSR#sh logging
Logging is enabled.
Origin id: hostname
Console Logging: Level info. Console Messages: 149 Dropped.
Buffer Logging: Level info. Buffer Messages: 451 Logged, 451 Displayed, 1000 Max.
File Logging: Level error. File Messages: 165 Logged, 289 Dropped.
SysLog server 172.30.0.30 Port: 514. Logging: info. Messages format: default. Messages
: 0 Dropped.
3 messages were not logged

Application filtering control
Application          Event                      Status
-----
AAA                  Login                      Enabled
File system          Copy                       Enabled
File system          Delete-Rename             Enabled
Management ACL       Deny                     Enabled
```

6. Включите отправку логов на удаленный сервер syslog с помощью команды **logging host**:

```
logging host <target> port <port> transport <protocol> severity
<level> facility <facility>
```

Здесь:

- **<target>** — IP-адрес или сетевое имя сервера;
- **<port>** — номер порта для передачи сообщений по протоколу syslog;
- **<protocol>** — **udp** или **tcp**.
- **<level>** — уровень важности, начиная с которого сообщения будут передаваться на сервер syslog. Существуют следующие уровни, в порядке возрастания важности:

- debugging — отладочные.
 - informational — информационные;
 - notifications — уведомления;
 - warnings — предупреждения;
 - errors — ошибки;
 - critical — критические ошибки;
 - alerts — сигналы тревоги;
 - emergencies — чрезвычайные сообщения;
- **<facility>** — категория сообщений вида **localN**, где N — цифра от 0 до 7.

▼ *Пример использования команды*

```
logging host 203.0.113.30 port 30150 facility local7 severity informational
```

При использовании данной команды все сообщения, кроме отладочных, будут направляться по протоколу UDP на порт 30150.

Чтобы отменить логирование на указанный адрес, используйте ключевое слово **no**, например:

```
no logging host 203.0.113.30
```

Чтобы просмотреть текущую логирования, запустите в основном интерфейсе Eltex MES следующую команду:

```
show syslog-servers
```

Результат выполнения команды:

```
MSR#show syslog-servers
```

```
Source IPv4 interface:
```

```
Source IPv6 interface:
```

```
Device Configuration
```

```
-----
```

IP address	Port	Facility	Severity	Description
203.0.113.30	30150	local7	info	

Сохранить конфигурацию с помощью команды:

+

Настройка интеграции с R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - a. **Тип точки входа** — Syslog;
 - b. **Порт точки входа** и **Протокол** — в соответствии с настройками на стороне [Eltex MES](#).
3. Добавьте на конвейер элемент **VRL-трансформация** со следующим кодом:

```
.dproduct = "EltexMES"
```

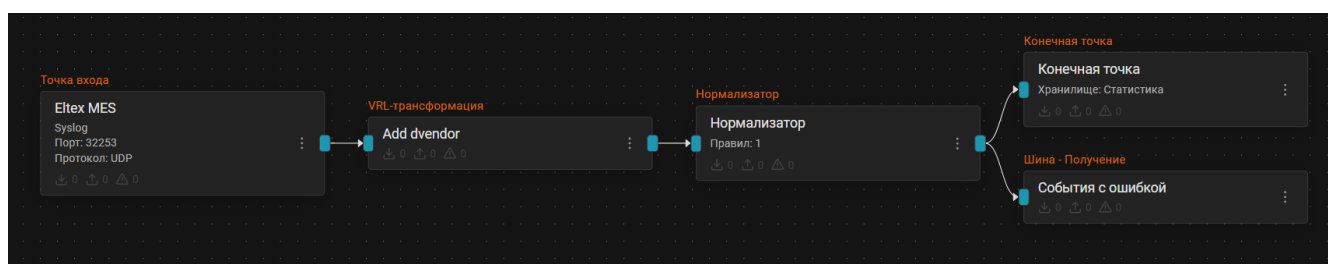
Соедините VRL-трансформацию с точкой входа.

4. Добавьте на конвейер **Нормализатор** с правилом **Нормализация событий источника Eltex MSR** (идентификатор **RV-N-34**). Соедините нормализатор с VRL-трансформацией.
5. Добавьте на конвейер элемент для отправки событий:
 - Чтобы сохранять нормализованные события в хранилище, добавьте элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
 - Чтобы отправлять события на другой конвейер для дальнейшей обработки, добавьте в коллектор шину, затем добавьте на конвейер соединение с этой шиной в режиме **Получение**.

На другом конвейере добавьте соединение с этой шиной в режиме **Отправка**.

6. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера



После установки конфигурации вы должны входящие события Eltex MES будут поступать на конвейер.

Fortinet

Данный раздел содержит список систем для настройки от компании Fortinet:

- [Fortigate](#)

Fortigate

Данное руководство содержит инструкцию по настройке сбора событий Fortigate на стороне источника и настройки сбора событий источника на стороне SIEM.

Настройка Fortigate

Журналирование событий источника условно делится на 2 категории:

- **Журнал событий** — хранит события системы, пользователей, конечных точек, события высокой доступности и другие.
- **Журнал трафика** — хранит разрешенный трафик, запрещенный трафик, исходящий трафик.

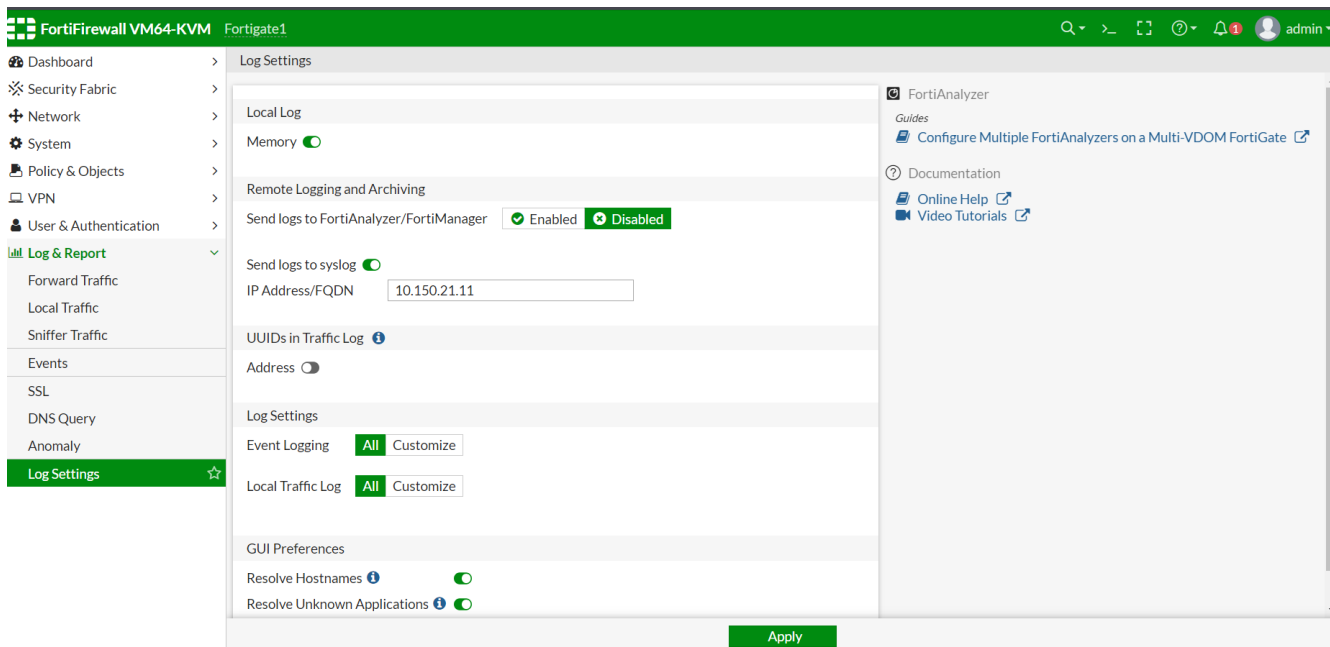
Отправка сообщений журналов .log осуществляется посредством syslog.

Настройка может производиться через [GUI](#) или через [CLI](#).

Настройка отправки событий через GUI

Для настройки отправки логов через GUI выполните следующие действия:

1. Авторизируйтесь в веб-панели управления Fortigate.
2. Перейдите в раздел **Log Settings**.
3. Укажите адрес сервера Syslog.
4. Установите переключатель **Event Logging** в положение **All**.
5. Установите переключатель **Local Traffic Log** в положение **All**.
6. Нажмите **Apply** для применения настроек.



Настройка отправки событий через CLI

Для настройки отправки логов через CLI выполните следующие действия:

1. Подключитесь к устройству Fortigate через CLI.
2. Перейдите в режим конфигурации syslog с помощью команды:

```
config log syslogd setting
```

3. Проверьте текущие настройки с помощью команды:

```
get
```

Убедитесь, что параметры настроены правильно. Например, **status: enable**, **server: <syslog-server-ip>**, **port: 514**.

4. Измените режим отправки логов на надёжный (**reliable**) с помощью команды:

```
set mode reliable
```

После изменения режима порт автоматически сбрасывается на значение по умолчанию (514).

5. Установите порт отправки логов, например, 31 121:

```
set port 31121
```

6. Убедитесь, что изменения применены, с помощью команды:

```
get
```

Проверьте, что параметры обновлены:

```
mode          : reliable
port          : 31121
```

7. Завершите настройку с помощью команды:

```
end
```

Настройка в R-Vision SIEM

Для настройки получения события источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Syslog.
 - Порт точки входа: любой в диапазоне 30 000—32 000.
 - Протокол: TCP.
3. Добавьте на конвейер элемент **Нормализатор** с правилом "RV-N-37". Соедините нормализатор с точкой входа.
4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
5. Сохраните и установите конфигурацию конвейера.

Если настройка выполнена корректно, в хранилище начнут поступать события журналов.

Для поиска полученных событий сделайте следующее:

1. Перейдите в меню "Поиск"
2. В качестве фильтра установите выражение `dvendor = "Fortinet" && dproduct = "Fortigate"`
[fortinet fortigate v6 search data]

Таблица маппинга

Таблица соответствия полей события [представлена по ссылке](#).

FreeIPA

Данное руководство описывает процесс настройки сбора и отправки событий FreeIPA в R-Vision SIEM.

Настройка FreeIPA

Описание подсистемы журналирования FreeIPA

FreeIPA — это открытое программное обеспечение, предоставляющее специализированную службу каталогов для операционных систем на базе Linux. Оно предназначено для создания централизованной среды управления аутентификацией, авторизацией и учетными записями пользователей.

Продукт FreeIPA регистрирует события следующих служб:

- 389 DS;
- KRB5KDC;
- HTTPD.

Отправка событий FreeIPA

В настоящем руководстве рассматривается передача событий с помощью службы rsyslog. Предполагается, что rsyslog на станции с ОС Linux уже установлен.

Для настройки источника выполните следующие действия:

1. Настройте передачу событий из файлов. Для этого создайте файл конфигурации **/etc/rsyslog.d/01-freeipa.conf** со следующим содержимым:

```
module(load="imfile" mode="inotify")
input(
    type="imfile"
    File="/var/log/dirsrv/slapd-<DOMAIN>/access"
    Tag="FreeIPA-389DS-access"
    Severity="info"
    Facility="local4"
)
input(
    type="imfile"
    File="/var/log/dirsrv/slapd-<DOMAIN>/audit"
    Tag="FreeIPA-389DS-audit"
    Severity="info"
    Facility="local4"
)
input(
    type="imfile"
    File="/var/log/dirsrv/slapd-<DOMAIN>/errors"
```



```

    Tag="FreeIPA-389DS-errors"
    Severity="info"
    Facility="local4"
)

input(
    type="imfile"
    File="/var/log/httpd/error_log"
    Tag="FreeIPA-HTTPD-error_log"
    Severity="info"
    Facility="local4"
)

input(
    type="imfile"
    File="var/log/krb5kdc.log"
    Tag="FreeIPA-KDC-krb5kdc_log"
    Severity="info"
    Facility="local4"
)

if $syslogtag contains 'FreeIPA' then {
    action(type="omfwd" Target="<target>" Port="<port>" Protocol="<protocol>")
    stop
}

```

Здесь:

- **<target>** — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- **<port>** — порт точки входа Syslog в конвейере SIEM.
- **<protocol>** — сетевой протокол: **tcp** или **udp**.
- **<DOMAIN>** — доменное имя.

2. Перезапустите службу `rsyslog.service` с помощью команды:

```
systemctl restart rsyslog.service
```



Для дистрибутивов на основе Debian журнал ошибок Apache по умолчанию располагается по пути `/var/log/apache2/error.log`.



Чтобы корректно разбирать даты в журнале `krb5kdc.log` на системах с дистрибутивами на основе Debian, установите значение системной локали в файле `/etc/default/locale` на `en_US`.

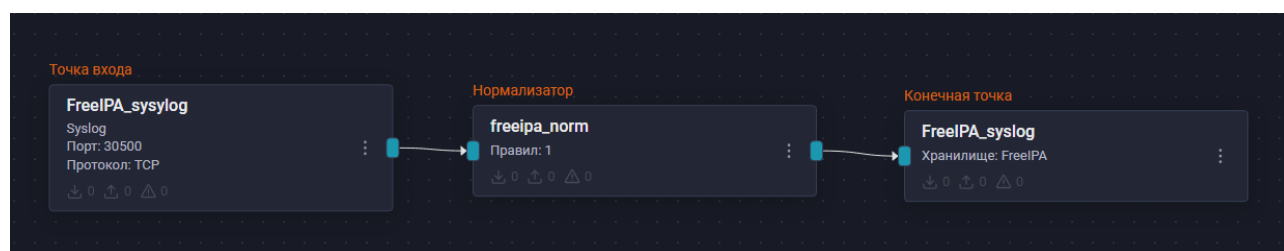
Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие

шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Syslog.
 - Порт точки входа и протокол: в соответствии с настройками на стороне [FreeIPA](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилами FreeIPA и ALDPro (идентификаторы правил: RV-N-38, RV-N-39, RV-N-40, RV-N-41). Соедините нормализатор с точкой входа.
4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
5. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события FreeIPA.



Найти события FreeIPA в хранилище можно по следующему фильтру:

```
.dproduct = "FreeIPA"
```

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Гарда

Данный раздел содержит список систем для настройки от компании Гарда:

- [Гарда DBF](#)
- [Гарда DLP](#)
- [Гарда NDR](#)
- [Гарда WAF](#)

Гарда DBF

Данное руководство описывает процесс настройки сбора и отправки событий комплекса Гарда DBF в R-Vision SIEM.

Настройка Гарда DBF



Система позволяет отправлять события безопасности во внешние системы посредством syslog. Для настройки передачи система требует ввести шаблон сообщения syslog. В рамках инструкции подготовлены шаблоны для передачи событий.

Для настройки передачи событий syslog на Гарда DBF:

1. Войдите в консоль администратора **Гарда DBF**.
2. Перейдите на вкладку **Настройки** → **Системные настройки** → **Экспорт в SIEM**.
3. Настройте [экспорт данных по политикам](#).
4. Настройте [экспорт журналов](#).
5. Настройте [экспорт аномалий](#).

Настройка экспорта данных по политикам

1. В разделе **Политики** создайте шаблон экспорта данных по политике в SIEM. Для этого нажмите на кнопку **Добавить новый шаблон (+)**.
2. Заполните поля:
 - **Название:** укажите название шаблона политики.
 - **IP-адрес/Доменное имя:** укажите IP-адрес коллектора SIEM.
 - **Порт:** укажите порт, который настроен в SIEM для приема событий источника.
 - **Протокол:** выберите протокол, настроенный в SIEM.
 - **Формат:** выберите формат CEF.
 - **Формат сообщения:**

```
dst=$GardaDB.peer_ip;src=$GardaDB.uni_ip;dpt=$GardaDB.peer_port;spt=$GardaDB.uni_port;cs1=$GardaDB.time;cs1Label=Время;cs2=$GardaDB.sql_text;cs2Label=Запрос;cs3
```

```
=${GardaDB.sql_var};cs3Label=Переменные;cs4=${GardaDB.sql_response};cs4Label=Ответ;cs5=${GardaDB.sql_objects};cs5Label=Таблицы;cs6=${GardaDB.sql_users};cs6Label=Пользователи;cs7=${GardaDB.sql_columns};cs7Label=Поля;cs8=${GardaDB.req_size};cs8Label=РазмерЗапроса;cs9=${GardaDB.resp_size};cs9Label=РазмерОтвета;cs10=${GardaDB.resp_line_count};cs10Label=СтрокВОтвете;cs11=${GardaDB.continuanse};cs11Label=Продолжительность;cs12=${GardaDB.sql_error};cs12Label=ТекстОшибки;cs13=${GardaDB.db_name};cs13Label=ИмяБД;cs14=${GardaDB.sql_db_name};cs14Label=ЭкземплярБД;cs15=${GardaDB.policy_name};cs15Label=Политика;cs16=${GardaDB.sniffer_name};cs16Label=Анализатор;cs17=${GardaDB.db_login};cs17Label=ЛогинБД;cs18=${GardaDB.os_login};cs18Label=ЛогинОС;cs19=${GardaDB.sql_program};cs19Label=ИмяПрограммы;cs20=${GardaDB.sql_machine};cs20Label=ИмяКомпьютера;cs21=${GardaDB.sql_auth};cs21Label=Аутентификация;cs22=${GardaDB.ldap_name};cs22Label=ФИО;cs23=${GardaDB.ldap_dep};cs23Label=Подразделение;cs24=${GardaDB.ldap_pos};cs24Label=Должность;cs25=${GardaDB.ldap_email};cs25Label=Email;cs26=${GardaDB.add_field_1};cs26Label=Доп1;cs27=${GardaDB.add_field_2};cs27Label=Доп2;cs28=${GardaDB.add_field_3};cs28Label=Доп3;cs29=${GardaDB.add_field_4};cs29Label=Доп4;cs30=${GardaDB.add_field_5};cs30Label=Доп5;cs31=${GardaDB.profilng_details};cs32=https://127.0.0.1/#/Search/SearchById/${GardaDB.object_id_for_url};cs32Label=Ссылка;cs33=${GardaDB.agent_guid};cs33Label=Guid_Агента;
```

3. Нажмите на кнопку **Применить**.

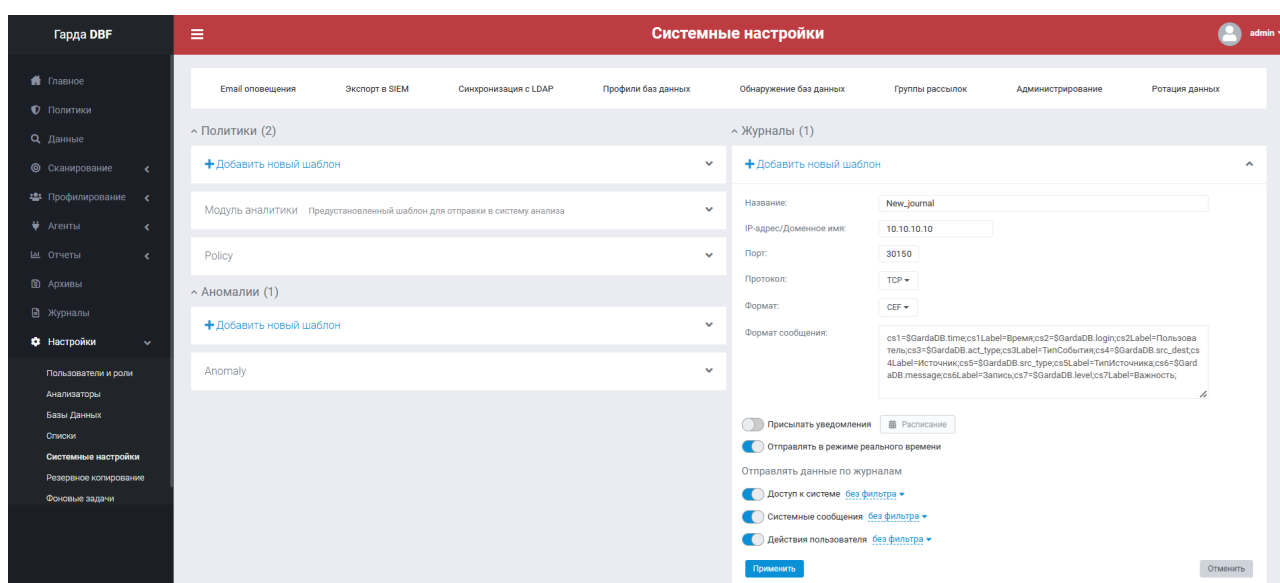
Настройка экспорта журналов

1. В разделе **Журналы** создайте шаблон экспорта из журналов в SIEM. Для этого нажмите на кнопку **Добавить новый шаблон** (+).
2. Заполните поля:
 - **Название:** укажите название шаблона журнала.
 - **IP-адрес/Доменное имя:** укажите IP-адрес коллектора SIEM.
 - **Порт:** укажите порт, который настроен в SIEM для приема событий источника.
 - **Протокол:** выберите протокол, настроенный в SIEM.
 - **Формат:** выберите формат CEF.

- **Формат сообщения:**

```
cs1=$GardaDB.time;cs1Label=Время;cs2=$GardaDB.login;cs2Label=Пользователь;cs3=$GardaDB.act_type;cs3Label=ТипСобытия;cs4=$GardaDB.src_dest;cs4Label=Источник;cs5=$GardaDB.src_type;cs5Label=ТипИсточника;cs6=$GardaDB.message;cs6Label=Запись;cs7=$GardaDB.level;cs7Label=Важность;
```

3. Установите переключатель **Отправлять в режиме реального времени** в активное положение.
4. Установите переключатель **Доступ к системе** в активное положение.
5. Установите переключатель **Системные сообщения** в активное положение.
6. Установите переключатель **Действия пользователя** в активное положение.
7. Нажмите на кнопку **Применить**.



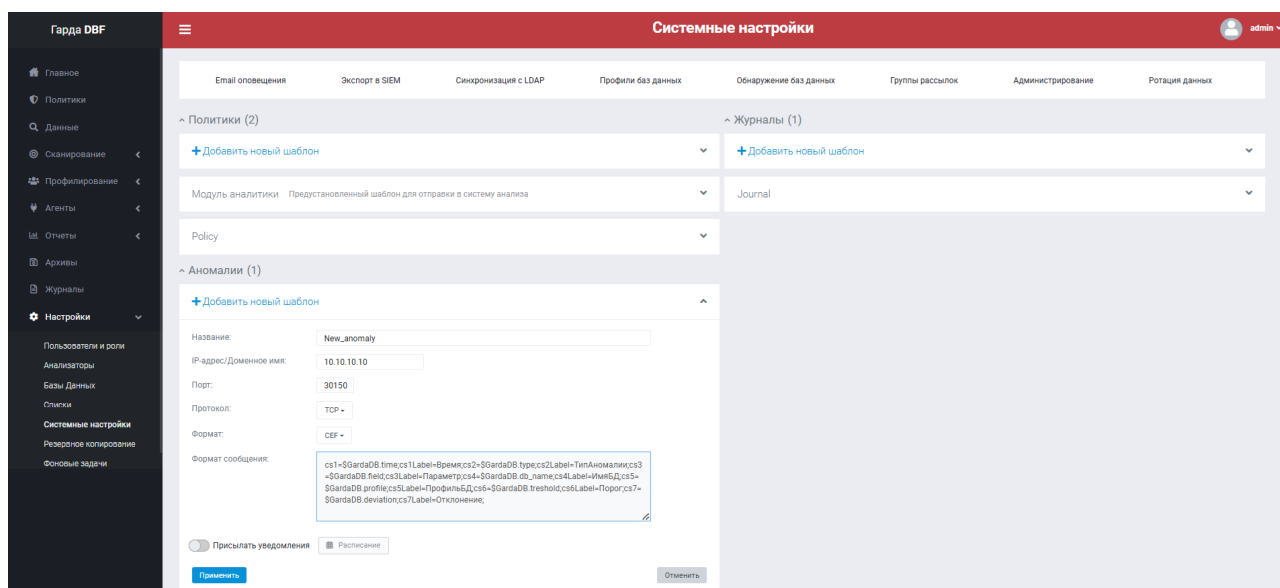
Настройка экспорта аномалий

1. В разделе **Аномалии** создайте шаблон экспорта аномалий в SIEM. Для этого нажмите на кнопку **Добавить новый шаблон (+)**.
2. Заполните поля:
 - **Название:** укажите название шаблона аномалий.
 - **IP-адрес/Доменное имя:** укажите IP-адрес коллектора SIEM.
 - **Порт:** укажите порт, который настроен в SIEM для приема событий источника.
 - **Протокол:** выберите протокол, настроенный в SIEM.
 - **Формат:** выберите формат CEF.
 - **Формат сообщения:**

```
cs1=$GardaDB.time;cs1Label=Время;cs2=$GardaDB.type;cs2Label=ТипАномалии;cs3=$GardaDB.field;cs3Label=Параметр;cs4=$GardaDB.db_name;cs4Label=ИмяБД;cs5=$GardaDB.profile;cs5Label=ПрофильБД;cs6=$GardaDB.threshold;cs6Label=Порог;cs7=$GardaDB.deviation;cs7Label=Отклонение;
```

```
tion;cs7Label=0отклонение;
```

3. Нажмите на кнопку **Применить**.



Настройка Гарда DBF завершена.

Настройка R-Vision SIEM

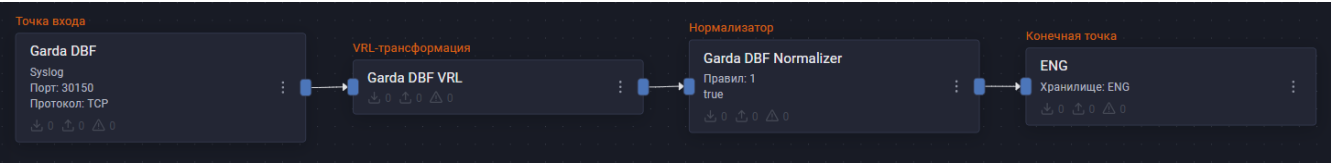
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Syslog**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [Гарда DBF](#).
 - Протокол: выберите вариант в соответствии с настройками на стороне [Гарда DBF](#).
3. Добавьте VRL-трансформацию:

```
.dproduct = "Garda DBF"
```

4. Соедините добавленную точку входа и VRL-трансформацию.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Garda Database Firewall** (идентификатор правила: **RV-N-138**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события Гарда DBF.

Найти события Гарда DBF в хранилище можно по следующему фильтру:

```
dproduct = "Garda DBF"
```



Совпадений 28. Интервал времени: 2024-12-06T20:26:05.766+03:00 - 2024-12-06T20:31:05.766+03:00. Показать график

id	sourceip	timestamp	type	dvendor	dproduct
56d9bda-0a93-46bb-a4a1-b48b7e65c2a5	10.150.15.230	2024-12-06T20:30:00.000+03:00	нормализованное событие	Гарда	Garda DBF
4b18dd0a-c505-479c-98eb-25322ab17441	10.150.15.230	2024-12-06T20:30:00.000+03:00	нормализованное событие	Гарда	Garda DBF
72466f4f-48de-4b05-8e56-81ad03cc8fa7		2024-12-06T20:30:00.000+03:00	нормализованное событие	Гарда	Garda DBF
837e64e9-ed0a-4213-a9f1-b315243431e6		2024-12-06T20:30:00.000+03:00	нормализованное событие	Гарда	Garda DBF
46b2600d-ca4a-407d-bfab-06c43911be2c		2024-12-06T20:30:00.000+03:00	нормализованное событие	Гарда	Garda DBF
944ba174-7811-45fd-b39f-5a671719678d		2024-12-06T20:30:00.000+03:00	нормализованное событие	Гарда	Garda DBF
190e993b-accb-453d-83de-ad9ee4b10322		2024-12-06T20:30:00.000+03:00	нормализованное событие	Гарда	Garda DBF
edcc0389-5aa2-45d3-b068-3cb4cddac419		2024-12-06T20:29:30.000+03:00	нормализованное событие	Гарда	Garda DBF
f57155e1-4e92-4e10-993a-8c4d8e9f6d1		2024-12-06T20:29:30.000+03:00	нормализованное событие	Гарда	Garda DBF
2b2b013-467c-423f-ba9c-612b237f0ec2		2024-12-06T20:29:30.000+03:00	нормализованное событие	Гарда	Garda DBF
f64ec071-45b9-4622-acd3-6c3cabae1ec2		2024-12-06T20:29:00.000+03:00	нормализованное событие	Гарда	Garda DBF
1e3ea860-2a0b-4708-8b32-		2024-12-	нормализованное событие	Гарда	Garda DBF

Детали события 4b18dd0a-c505-479c-98eb-25322ab17441

☒ Скрыть пустые поля события

Дата и время

timestamp 2024-12-06T20:30:00.000+03:00

Служебные данные

id 4b18dd0a-c505-479c-98eb-25322ab17441
sourceip 10.150.15.230
tenantid 00000000-0000-0000-0000-000000000000
collectorid a7df468-2dc31-4e48-91a2-68559ad42621
type нормализованное событие

Сведения о событии

dvendor Гарда
dproduct Garda DBF
dversion 1.0.0-0
deviceEventClassId 100
severity Warning
deviceFacility local4
dvchost grd03
msg Трафик на БД "Garda_DBF" отсутствует больше 0 часов
outcome Success
rt 2024-12-06T20:30:37.000+03:00
objType TaskExecutor

Исходное событие

Гарда DLP

Данное руководство описывает процесс настройки сбора и отправки событий комплекса Гарда DLP в R-Vision SIEM.

Настройка Гарда DLP



Система позволяет отправлять события безопасности во внешние системы посредством syslog. Для настройки передачи система требует ввести шаблон сообщения syslog. В рамках инструкции подготовлены шаблоны для передачи событий, генерируемых профилями безопасности по умолчанию.

Для настройки передачи событий syslog на Гарда DLP:

1. Войдите в консоль администратора Гарда DLP.
2. Перейдите на вкладку **Настройки** → **Экспорт в SIEM**.
3. Создайте шаблоны экспорта в SIEM под каждый профиль по умолчанию. Для этого нажмите на кнопку **Добавить новый шаблон экспорта в SIEM**.
4. Заполните поля:

- Общие поля для всех профилей:
 - **IP-адрес** -ш укажите IP-адрес коллектора SIEM.
 - **Порт** — укажите порт, который настроен в SIEM для приема событий с источника.
 - **Протокол** — выберите протокол, настроенный в SIEM.
 - **Формат** — выберите формат CEF.
- Форматы сообщений для каждого профиля:
 - ПДН в почте, мессенджерах, загрузка на сайты:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop
uni_email=$Garda.uni_email peer_email=$Garda.peer_email
have_attach=$Garda.have_attach url=$Garda.url
content_type=$Garda.content_type http_type=$Garda.http_type size=$Garda.size
web_obj_id=$Garda.web_obj_id web_parent_id=$Garda.web_parent_id
web_object_type=$Garda.web_object_type result_code=$Garda.result_code
referer=$Garda.referer content_encoding=$Garda.content_encoding
web_uni_id=$Garda.web_uni_id web_peer_id=$Garda.web_peer_id
web_source_id=$Garda.web_source_id protocol=$Garda.protocol
proto_descr=$Garda.proto_descr channel=$Garda.channel
uni_ident=$Garda.uni_ident peer_ident=$Garda.peer_ident
subject=$Garda.subject login=$Garda.login chat_id=$Garda.chat_id
send_time=$Garda.send_time mail_partid=$Garda.mail_partid
mail_flags=$Garda.mail_flags uni_is_server=$Garda.uni_is_server
uni_is_sender=$Garda.uni_is_sender blocking_action=$Garda.blocking_action
cat="ПДН_в_почте,_мессенджерах,_загрузка_на_сайты"
uni_phone=$Garda.uni_phone peer_phone=$Garda.peer_phone
account=$Garda.account user_action=$Garda.user_action
type_action=$Garda.type_action prop_text_part=$Garda.prop_text_part
```

- Использование подозрительного ПО:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop
process_name=$Garda.process_name process_id=$Garda.process_id
action_type=$Garda.action_type user_action=$Garda.user_action
device_name=$Garda.device_name serial_id=$Garda.serial_id
protocol=$Garda.protocol proto_descr=$Garda.proto_descr
channel=$Garda.channel uni_is_server=$Garda.uni_is_server
uni_is_sender=$Garda.uni_is_sender blocking_action=$Garda.blocking_action
cat="Использование_подозрительного_ПО"
```


- Документы и архивы с паролем:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop
uni_email=$Garda.uni_email peer_email=$Garda.peer_email
have_attach=$Garda.have_attach path=$Garda.path file_size=$Garda.file_size
process_name=$Garda.process_name flags=$Garda.flags
device_name=$Garda.device_name serial_id=$Garda.serial_id url=$Garda.url
content_type=$Garda.content_type http_type=$Garda.http_type size=$Garda.size
web_obj_id=$Garda.web_obj_id web_parent_id=$Garda.web_parent_id
web_object_type=$Garda.web_object_type result_code=$Garda.result_code
referer=$Garda.referer content_encoding=$Garda.content_encoding
web_uni_id=$Garda.web_uni_id web_peer_id=$Garda.web_peer_id
web_source_id=$Garda.web_source_id protocol=$Garda.protocol
proto_descr=$Garda.proto_descr channel=$Garda.channel login=$Garda.login
chat_id=$Garda.chat_id send_time=$Garda.send_time
mail_partid=$Garda.mail_partid mail_flags=$Garda.mail_flags
uni_is_server=$Garda.uni_is_server uni_is_sender=$Garda.uni_is_sender
blocking_action=$Garda.blocking_action cat="Документы_и_архивы_с_паролем"
```

- Выгрузка БД на внешние носители:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop path=$Garda.path
file_size=$Garda.file_size process_name=$Garda.process_name
flags=$Garda.flags device_name=$Garda.device_name serial_id=$Garda.serial_id
protocol=$Garda.protocol proto_descr=$Garda.proto_descr
channel=$Garda.channel uni_is_server=$Garda.uni_is_server
uni_is_sender=$Garda.uni_is_sender blocking_action=$Garda.blocking_action
cat="Выгрузка_БД_на_внешние_носители"
```

- ПДН на внешних носителях и в печати:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop path=$Garda.path
file_size=$Garda.file_size process_name=$Garda.process_name
flags=$Garda.flags device_name=$Garda.device_name serial_id=$Garda.serial_id
protocol=$Garda.protocol proto_descr=$Garda.proto_descr
channel=$Garda.channel uni_is_server=$Garda.uni_is_server
```

```
uni_is_sender=$Garda.uni_is_sender blocking_action=$Garda.blocking_action
cat="ПДН_на_внешних_носителях_и_в_печати"
prop_text_part=$Garda.prop_text_part
```

- Блокировка фразы:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop url=$Garda.url
content_type=$Garda.content_type http_type=$Garda.http_type size=$Garda.size
process_name=$Garda.process_name web_obj_id=$Garda.web_obj_id
web_parent_id=$Garda.web_parent_id web_object_type=$Garda.web_object_type
result_code=$Garda.result_code referer=$Garda.referer
content_encoding=$Garda.content_encoding web_uni_id=$Garda.web_uni_id
web_peer_id=$Garda.web_peer_id web_source_id=$Garda.web_source_id
protocol=$Garda.protocol proto_descr=$Garda.proto_descr
channel=$Garda.channel uni_is_server=$Garda.uni_is_server
uni_is_sender=$Garda.uni_is_sender blocking_action=$Garda.blocking_action
cat="Блокировка_фразы" uni_phone=$Garda.uni_phone
peer_phone=$Garda.peer_phone account=$Garda.account
user_action=$Garda.user_action type_action=$Garda.type_action
prop_text_part=$Garda.prop_text_part
```

- Передача исполняемых файлов в почте:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop
uni_email=$Garda.uni_email peer_email=$Garda.peer_email
have_attach=$Garda.have_attach subject=$Garda.subject
content_type=$Garda.content_type size=$Garda.size send_time=$Garda.send_time
mail_partid=$Garda.mail_partid mail_flags=$Garda.mail_flags
protocol=$Garda.protocol proto_descr=$Garda.proto_descr
channel=$Garda.channel uni_is_server=$Garda.uni_is_server
uni_is_sender=$Garda.uni_is_sender blocking_action=$Garda.blocking_action
path=$Garda.path file_size=$Garda.file_size mime_type=$Garda.mime_type
hash=$Garda.hash prop_text_part=$Garda.prop_text_part
prop_guid=$Garda.prop_guid prop_blob_id=$Garda.prop_blob_id
cat="Передача_по_почте_исполняемого_файла"
```

- Кредитные карты:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
```

```
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop
uni_email=$Garda.uni_email peer_email=$Garda.peer_email
have_attach=$Garda.have_attach path=$Garda.path file_size=$Garda.file_size
process_name=$Garda.process_name flags=$Garda.flags
device_name=$Garda.device_name serial_id=$Garda.serial_id url=$Garda.url
content_type=$Garda.content_type http_type=$Garda.http_type size=$Garda.size
web_obj_id=$Garda.web_obj_id web_parent_id=$Garda.web_parent_id
web_object_type=$Garda.web_object_type result_code=$Garda.result_code
referer=$Garda.referer content_encoding=$Garda.content_encoding
web_uni_id=$Garda.web_uni_id web_peer_id=$Garda.web_peer_id
web_source_id=$Garda.web_source_id protocol=$Garda.protocol
proto_descr=$Garda.proto_descr channel=$Garda.channel
uni_ident=$Garda.uni_ident peer_ident=$Garda.peer_ident
subject=$Garda.subject login=$Garda.login chat_id=$Garda.chat_id
send_time=$Garda.send_time mail_partid=$Garda.mail_partid
mail_flags=$Garda.mail_flags uni_is_server=$Garda.uni_is_server
uni_is_sender=$Garda.uni_is_sender blocking_action=$Garda.blocking_action
cat="Кредитные карты" uni_phone=$Garda.uni_phone
peer_phone=$Garda.peer_phone account=$Garda.account
user_action=$Garda.user_action type_action=$Garda.type_action
prop_text_part=$Garda.prop_text_part
```

- Использование удаленного доступа:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop
process_name=$Garda.process_name process_id=$Garda.process_id
action_type=$Garda.action_type user_action=$Garda.user_action
device_name=$Garda.device_name serial_id=$Garda.serial_id
protocol=$Garda.protocol proto_descr=$Garda.proto_descr
channel=$Garda.channel uni_is_server=$Garda.uni_is_server
uni_is_sender=$Garda.uni_is_sender blocking_action=$Garda.blocking_action
cat="Использование программы удаленного доступа"
```

- Конфиденциальная информация:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop
uni_email=$Garda.uni_email peer_email=$Garda.peer_email
have_attach=$Garda.have_attach path=$Garda.path file_size=$Garda.file_size
process_name=$Garda.process_name flags=$Garda.flags
```

```
device_name=$Garda.device_name serial_id=$Garda.serial_id url=$Garda.url  
content_type=$Garda.content_type http_type=$Garda.http_type size=$Garda.size  
web_obj_id=$Garda.web_obj_id web_parent_id=$Garda.web_parent_id  
web_object_type=$Garda.web_object_type result_code=$Garda.result_code  
referer=$Garda.referer content_encoding=$Garda.content_encoding  
web_uni_id=$Garda.web_uni_id web_peer_id=$Garda.web_peer_id  
web_source_id=$Garda.web_source_id protocol=$Garda.protocol  
proto_descr=$Garda.proto_descr channel=$Garda.channel  
uni_ident=$Garda.uni_ident peer_ident=$Garda.peer_ident  
subject=$Garda.subject login=$Garda.login chat_id=$Garda.chat_id  
send_time=$Garda.send_time mail_partid=$Garda.mail_partid  
mail_flags=$Garda.mail_flags uni_is_server=$Garda.uni_is_server  
uni_is_sender=$Garda.uni_is_sender blocking_action=$Garda.blocking_action  
cat="Конфиденциальная информация" uni_phone=$Garda.uni_phone  
peer_phone=$Garda.peer_phone account=$Garda.account  
user_action=$Garda.user_action type_action=$Garda.type_action  
prop_text_part=$Garda.prop_text_part
```

В результате получится 10 шаблонов:

Экспорт в SIEM

Администратор ...

🏠

🛡️

👥

📁

🔍

📊

☰

📄

⚙️

^ ПДН в почте, мессенджерах, загрузка на сайты 10.150.30.88:30194 [Удалить](#)

^ Использование подозрительного ПО 10.150.30.88:30194 [Удалить](#)

^ Документы и архивы с паролем 10.150.30.88:30194 [Удалить](#)

^ Выгрузка БД на внешние носители 10.150.30.88:30194 [Удалить](#)

^ ПДН на внешних носителях и в печати 10.150.30.88:30194 [Удалить](#)

^ Блокировка фразы 10.150.30.88:30194 [Удалить](#)

^ Передача исполняемых файлов в почте 10.150.30.88:30194 [Удалить](#)

^ Кредитные карты 10.150.30.88:30194 [Удалить](#)

^ Использование удаленного доступа 10.150.30.88:30194 [Удалить](#)

^ Конфиденциальная информация 10.150.30.88:30194 [Удалить](#)

[+ Добавить новый шаблон экспорта в SIEM](#)

5. Перейдите на вкладку **Политики**.

6. Выберите одну из политик по умолчанию.

7. В открывшемся меню включите функцию **Загружать данные в SIEM систему, используя шаблон** и выберите шаблон одноименный политике.

Выгрузка БД на внешние носители

Название:

Описание:

Изменение только создателем
 Администратор комплекса

Права доступа:

Каналы передачи данных:

Контролировать:

- ☒ Фразы
- ☒ Персональные данные
- ☒ Документы

☐ Включить поиск по точному совпадению

Сотрудники:

Словари:

Дополнительные параметры:

☐ Учитывать накопленные данные
 При первом запуске политики будет выполнен поиск в ранее накопленных данных

☐ Включить оповещения по Email, используя следующие списки:

☒ Загружать данные в SIEM систему, используя шаблон:

☐ ПДН в почте, мессенджерах, загрузка на сайты
☐ Использование подозрительного ПО
☐ Документы и архивы с паролем
☒ Выгрузка БД на внешние носители
☐ ПДН на внешних носителях и в печати
☐ Блокировка фразы
☐ Передача исполняемых файлов в почте
☐ Кредитные карты

8. Повторите последний шаг для оставшихся политик.

Настройка Гарда DLP завершена.

Настройка R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - a. Тип точки входа: Syslog.
 - b. Порт точки входа: в соответствии с настройками на стороне [Гарда DLP](#).
 - c. Протокол: TCP или UDP.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **RV-N-171**. Соедините нормализатор с точкой входа.
4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
5. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

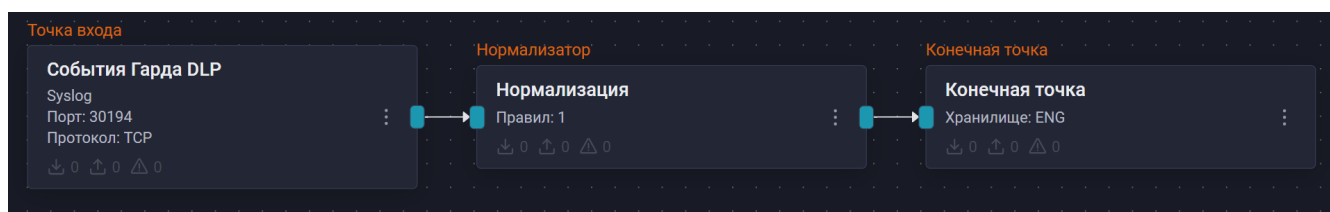


Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Гарда NDR

Данное руководство описывает процесс настройки сбора и отправки событий средства сетевого обнаружения и реагирования Гарда NDR в R-Vision SIEM.

Настройка Гарда NDR

Описание подсистемы журналирования

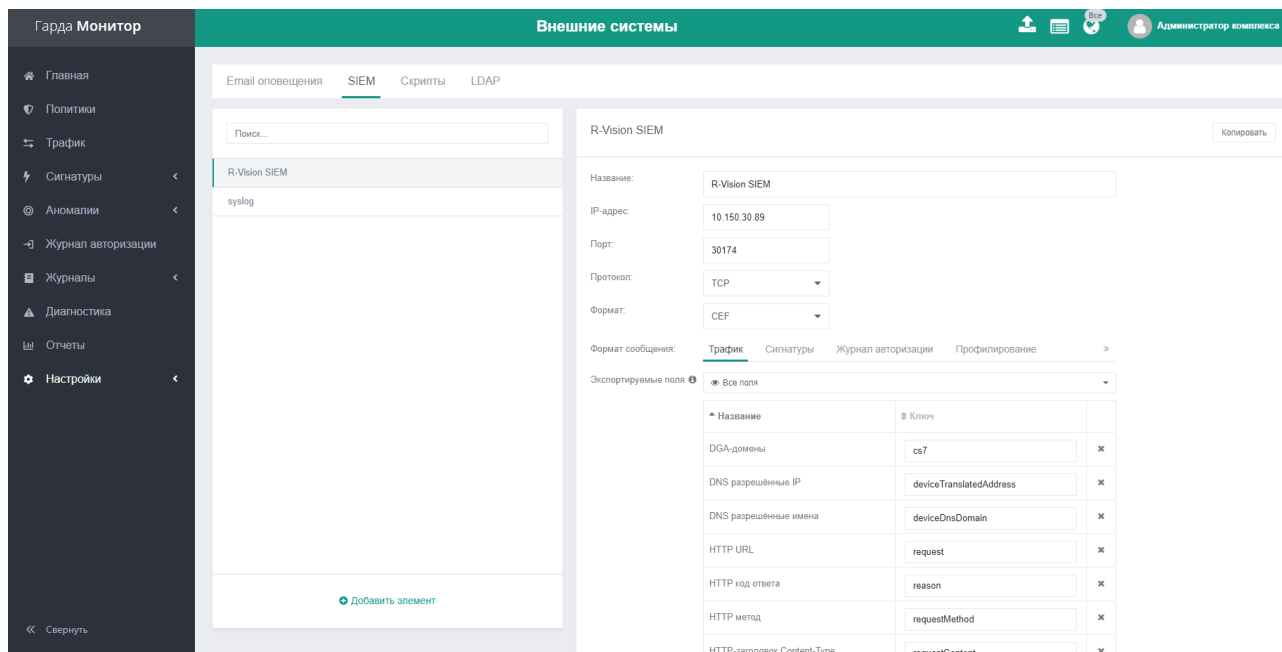
Гарда NDR позволяет передавать события, регистрируемые в рамках политик, по Syslog в формате CEF. Данные журналов действий пользователей и системных событий пишутся в СУБД ClickHouse.

Отправка событий Гарда NDR

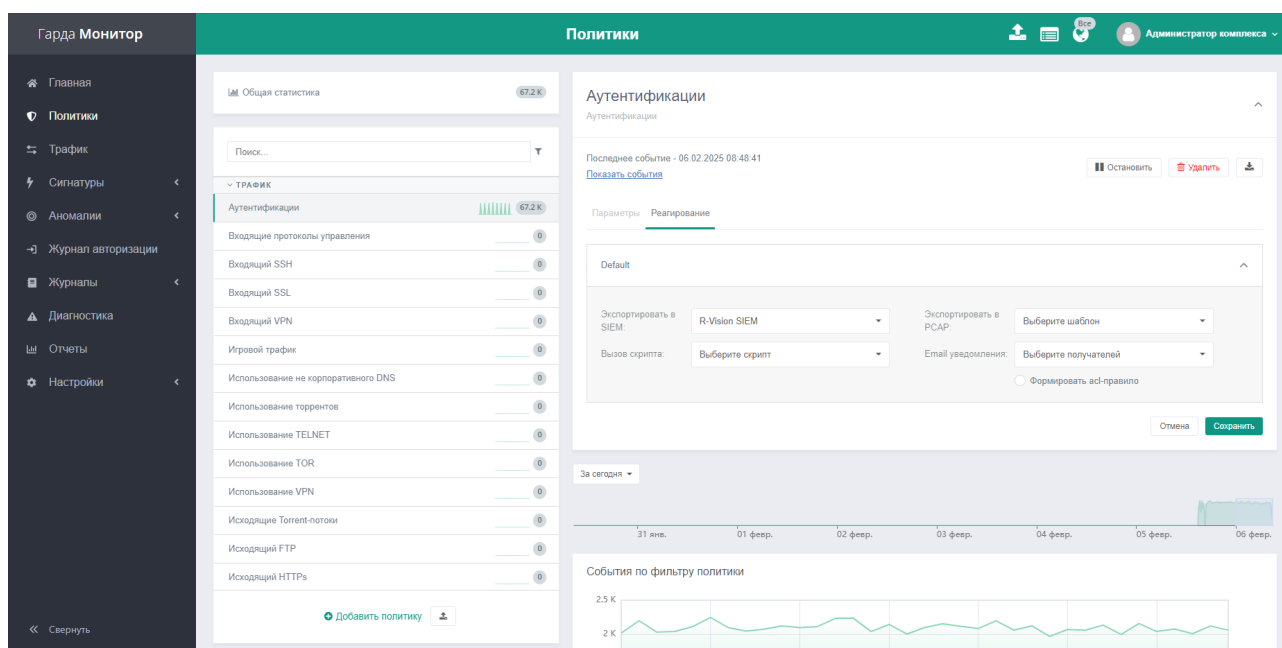
Настройка логирования для политики сбора трафика

Чтобы настроить экспорт событий Гарда NDR, выполните следующие шаги:

1. На панели администрирования **Гарда NDR** перейдите в раздел **Настройки** → **Внешние системы** → **SIEM**.
2. Нажмите на кнопку **Добавить элемент** (+).
3. Заполните поля **Название**, **IP-адрес**, **Порт** и **Протокол**, указав в них данные [точки входа из конвейера SIEM](#).
4. Сохраните изменения.



5. Перейдите в раздел **Политики**.
6. Выберите политику, события которой нужно пересылать в R-Vision SIEM.
7. Перейдите на вкладку **Реагирование** и раскройте настройки.
8. В поле **Экспортировать в SIEM** выберите из выпадающего списка созданный ранее профиль.



9. Настройка экспорта событий политики в R-Vision SIEM завершена.
10. Повторите шаги 6—8 для каждой политики.

Настройка ClickHouse для сбора событий журналов действий пользователей и системных событий

Чтобы настроить ClickHouse для передачи событий журналов, выполните следующие шаги:

1. На сервере ClickHouse откройте файл `/etc/clickhouse-server/users.xml`.
2. Задайте пароль пользователю `readonly` в теге `<password>`.

3. В теге `<ip>` укажите адреса коллекторов R-Vision SIEM или целую подсеть, откуда пользователю будет разрешено подключаться к СУБД.

Пример конфигурации:

```
<readonly>
  <password>readonly</password>
  <networks incl="networks" replace="replace">
    <ip>::1</ip>
    <ip>127.0.0.1</ip>
    <ip>10.150.0.0/16</ip>
  </networks>
  <profile>readonly</profile>
  <quota>default</quota>
</readonly>
```

4. В конфигурационном файле `/etc/clickhouse-server/config.xml` раскомментируйте блок:

```
<http_port>8123</http_port>
```

5. Перезапустите сервер ClickHouse:

```
systemctl restart clickhouse-server
```

6. Подготовка ClickHouse для передачи событий журналов в R-Vision SIEM завершена.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:

- a. Перейдите в раздел **Ресурсы** → **Секреты**.
- b. Нажмите на кнопку **Создать** (+).
- c. В раскрывшемся окне создания секрета заполните поля:
 - Название: введите название секрета.
 - Описание (опционально): опишите, для чего будет использоваться секрет.
 - Тип секрета: выберите вариант **Строка подключения**.
 - Строка подключения: введите строку вида:

```
jdbc:clickhouse://10.150.20.49:8123/default?user=readonly&password=readonly&compress=0
```

- d. Нажмите на кнопку **Создать**.
2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
3. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название **Garda NDR Traffic**.
 - Тип точки входа: выберите вариант **Syslog**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [Гарда NDR](#).
 - Протокол: выберите вариант в соответствии с настройками на стороне [Гарда NDR](#).
4. Добавьте VRL-трансформацию:

```
.dvendor = "Garda Technologies"
.dproduct = "Garda NDR"
.cat = "Traffic event"
```

5. Соедините добавленную точку входа и VRL-трансформацию.
6. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название **Garda NDR User Actions**.
 - Тип точки входа: выберите вариант **Database**.
 - Драйвер базы данных: выберите вариант **ClickHouse**.

- Адрес подключения: выберите секрет, созданный ранее.
- SQL-запрос: введите запрос вида:

```
SELECT *, toUnixTimestamp(TimeReal) AS rt FROM monitor.logging_user_actions
WHERE rt > ? ORDER BY rt ASC;
```

- Поле идентификатора: введите ключ **rt** со значением **1**.
- Интервал запроса, секунд: введите значение **15**.

7. Добавьте VRL-трансформацию:

```
.dvendor = "Garda Technologies"
.dproduct = "Garda NDR"
.cat = "User action"
```

8. Соедините добавленную точку входа и VRL-трансформацию.

9. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:

- Название: введите название **Garda NDR System Messages**.
- Тип точки входа: выберите вариант **Database**.
- Драйвер базы данных: выберите вариант **ClickHouse**.
- Адрес подключения: выберите секрет, созданный ранее.
- SQL-запрос: введите запрос вида:

```
SELECT *, toUnixTimestamp(TimeReal) AS rt FROM monitor.logging_system_messages
WHERE rt > ? ORDER BY rt ASC;
```

- Поле идентификатора: введите ключ **rt** со значением **1**.
- Интервал запроса, секунд: введите значение **15**.

10. Добавьте VRL-трансформацию:

```
.dvendor = "Garda Technologies"
.dproduct = "Garda NDR"
.cat = "System message"
```

11. Соедините добавленную точку входа и VRL-трансформацию.

12. Добавьте на конвейер элемент **Нормализатор** с правилами **Garda NDR Syslog** (идентификатор правила: **RV-N-163**) и **Garda NDR DB** (идентификатор правила: **RV-N-168**).

13. Соедините нормализатор с тремя добавленными VRL-трансформациями.

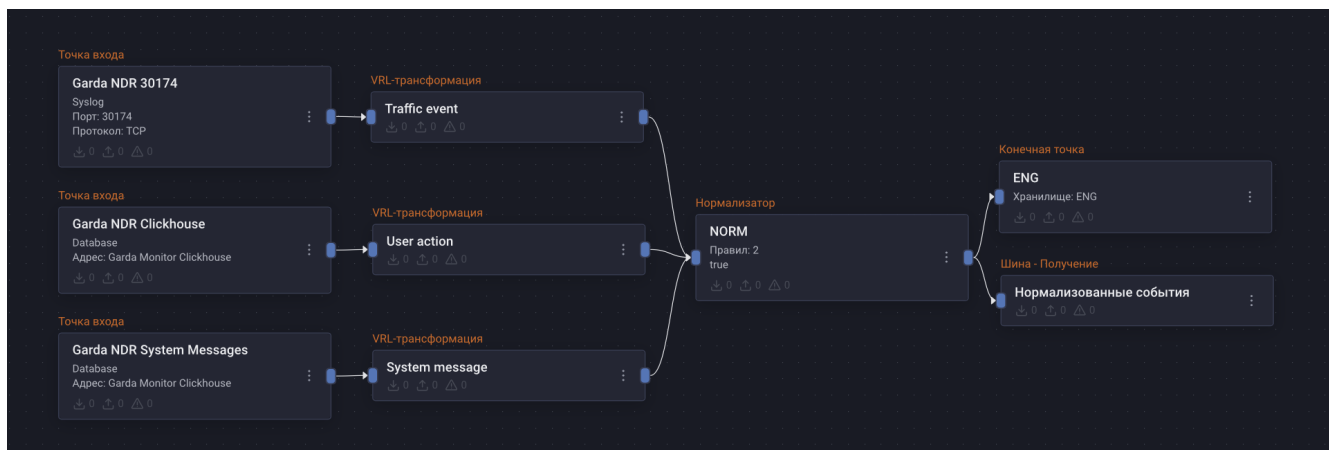
14. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.

15. Добавьте на конвейер элемент **Шина**, настроенный на получение.

16. Соедините конечную точку и шину с нормализатором.

17. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события Гарда NDR.

Найти события Гарда NDR в хранилище можно по следующему фильтру:

```
dproduct = "Garda NDR"
```



Изменить фильтр

☐ Инvertировать (NOT)

Поле

dproduct

Оператор

=

Значение

Garda NDR

☐ Настроить заголовок

Отменить

Сохранить

Гарда WAF

Данное руководство описывает процесс настройки сбора и отправки событий программного комплекса Гарда WAF в R-Vision SIEM.

Об источнике

Гарда WAF — это комплексное решение класса WAAP (Web Application and API Protection), которое включает расширенные инструменты для защиты веб-приложений и API от атак и уязвимостей, выявляет аномалии и угрозы нулевого дня.

Настройка Гарда WAF

Предварительные требования

- Сетевой доступ к БД Гарда WAF.
- Учетная запись в СУБД с правами на чтение БД Гарда WAF (Сбор событий из БД).

Настройки СУБД PostgreSQL

События Гарда WAF записываются в базу данных **waf** СУБД PostgreSQL. Для настройки сбора логов из базы данных необходимо к ней подключиться. Чтобы подключиться к БД, используйте специально созданную сервисную учетную запись (далее — УЗ).

Создание учетной записи в СУБД PostgreSQL

Чтобы создать сервисную УЗ, подключитесь к СУБД с правами администратора. Для этого выполните следующие действия на сервере с установленной СУБД:

1. Выполните следующую команду из-под пользователя postgres:

```
sudo -u postgres psql
```

2. Создайте сервисную учетную запись, выполнив следующие команды:

```
CREATE USER "gwaf_reader";  
ALTER ROLE gwaf_reader WITH PASSWORD 'password';
```

3. Выдайте права на чтение БД:

```
GRANT SELECT ON ALL TABLES IN SCHEMA public TO gwaf_reader;
```

Настройка в R-Vision SIEM

Для сбора событий SIEM необходимо создать конвейер с двумя точками входа — отдельно запрашиваются события аудита и событий безопасности.

Для подключения базы данных PostgreSQL в качестве источника событий в SIEM настройте следующий конвейер:

1. Добавьте на конвейер первую точку входа со следующими параметрами:
 - Тип точки входа: Database.
 - SQL-запрос:

```
SELECT  
    ilr.id AS ilr_id,  
    ilr.chain_id,
```

```

    ilr.accuracy,
    ilr.intervention_hostname,
    ilr.matched_data,
    ilr.maturity,
    ilr.message,
    ilr.passive,
    ilr.ref,
    ilr.rev,
    ilr.rule_id,
    ilr.severity,
    ilr.uri AS ilr_uri,
    ilr.ver,
    ilt.tags,
    icr.cluster_id,
    icr.cluster_name,
    icr.instance_id,
    icr.timestamp as timestamp,
    icr.worker_process_id,
    icr.worker_thread_id,
    icr.client_address,
    icr.hostname AS icr_hostname,
    icr.request_id,
    icr.request_id_hash,
    icr.server_id,
    icr.is_blocked,
    icr.status_code,
    icr.max_severity,
    icr.min_severity,
    icr.user_agent,
    icr.is_passive,
    rlr.uri AS request_uri,
    rlr.method as method,
    inet_server_addr() AS dvc,
    'Garda WAF' as product
FROM public.intervention_log_record ilr
LEFT JOIN
(
    SELECT
        log_id,
        string_agg(name, ', ') AS tags
    FROM
        public.intervention_log_record_tag
    GROUP BY
        log_id
) ilt ON ilr.id = ilt.log_id
JOIN
    public.interventions_chain_record icr ON ilr.chain_id = icr.id
LEFT JOIN
    public.request_log_record rlr ON icr.request_id = rlr.request_id
WHERE icr.timestamp > CAST(? AS BIGINT)
ORDER BY

```

```
icr.timestamp;
```

- База данных: PostgreSQL.
- Интервал запроса: 20.
- Поле идентификатора:
 - Ключ: **timestamp**.
 - Значение: **1742380463**.
- Строка подключения в секрете:

```
jdbc:postgresql://DBSERVER:5432/waf?user=gwaf_reader&password=password
```

Здесь:

- **DBSERVER** — FQDN или IP-адрес сервера СУБД.
- **5432** -- порт подключения.

2. Добавьте на конвейер вторую точку входа со следующими параметрами:

- Тип точки входа: Database.
- SQL-запрос:

```
SELECT
    ae.event_id as event_id,
    ae.cluster_id,
    ae.server_index,
    ae.timestamp,
    ae.username,
    ae.event_type,
    ae.entity_type,
    ae.event,
    ae.service_name,
    ae.cluster_name,
    ae.ip_address,
    scah.allowed_hostnames as server_name,
    inet_server_addr() AS dvc,
    'Garda WAF' as product,
    'Audit' as type_event
FROM public.audit_event ae
LEFT JOIN public.server_configuration_allowed_hostnames scah
    ON ae.server_index = scah.server_configuration_id
WHERE ae.event_id > CAST(? AS BIGINT)
ORDER BY ae.event_id ASC LIMIT 10000;
```

- База данных: PostgreSQL.
- Интервал запроса: 60.

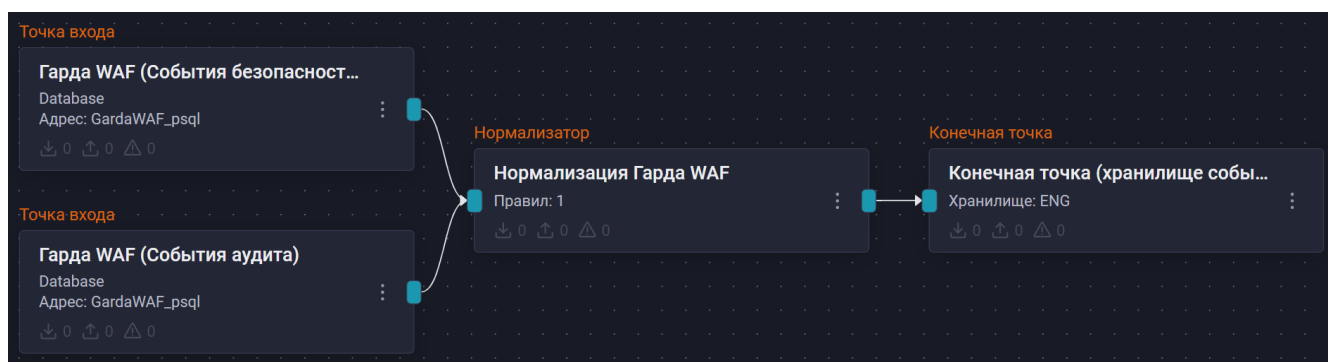
- Поле идентификатора:
 - Ключ: **event_id**.
 - Значение: **1**.
- Строка подключения в секрете:

```
jdbc:postgresql://DBSERVER:5432/waf?user=gwaf_reader&password=passwd
```

Здесь:

- **DBSERVER** — FQDN или IP-адрес сервера СУБД.
 - **5432** -- порт подключения.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **RV-N-144**. Соедините нормализатор с точками входа.
 4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
 5. Установите конфигурацию конвейера.

Пример конфигурации конвейера:



Если настройка выполнена корректно, в хранилище начнут поступать события из PostgreSQL.



Найти события из PostgreSQL в хранилище можно по следующему фильтру:

```
dproduct = Garda WAF
```


Настройка секрета database в R-Vision SIEM

Чтобы создать секрет подключения к СУБД:

- В интерфейсе R-Vision SIEM перейдите в раздел **Ресурсы** → **Секреты**.
- Нажмите на кнопку **Создать**.
- В открывшемся окне заполните поля:
 - Название** — введите название секрета.
 - Описание** (опционально) — введите назначение секрета.
 - Тип секрета** — выберите вариант **Строка подключения**.
 - Строка подключения** — укажите данные для подключения к СУБД.
- Нажмите на кнопку **Создать**.

Создание секрета

×

Название

Garda WAF (PSQL)

Описание (опционально)

Секрет подключения к СУБД Garda WAF

Тип секрета

Строка подключения

Строка подключения

jdbc:postgresql://DBSERVER:5432/DBNAME?
user=gwaf_reader&password=P@ssw0rd

Отменить

Создать

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Hewlett Packard Enterprise

Данный раздел содержит список систем для настройки от компании Hewlett Packard Enterprise:

- [ArubaOS CX](#)

ArubaOS CX

Данное руководство описывает процесс отправки событий сетевого коммутатора ArubaOS-CX в R-Vision SIEM.

Настройка ArubaOS CX

Настройте отправку событий на сетевом коммутаторе, последовательно выполнив команды:

```
# conf
# logging <target> <protocol> <port>
# write memory
```

Здесь:

- **<target>** — IP-адрес коллектора SIEM.
- **<port>** — порт точки входа Syslog в конвейере SIEM.
- **<protocol>** — сетевой протокол: **tcp** или **udp**.

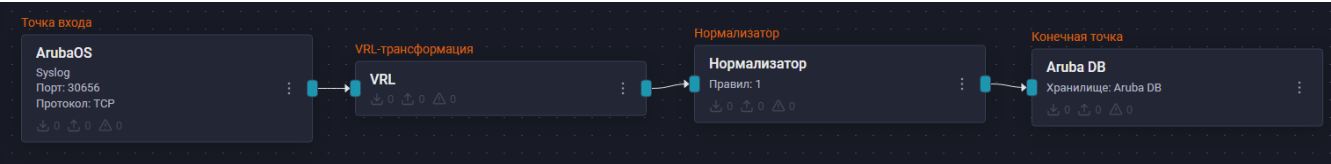
Настройка интеграции с R-Vision SIEM

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Syslog.
 - Порт точки входа и протокол: в соответствии с настройками на стороне [источника](#).
3. Добавьте VRL-трансформацию:

```
.dproduct = "ArubaOS-CX"
```

4. Соедините добавленную точку входа и VRL-трансформацию.
5. Добавьте на конвейер элемент **Нормализатор** с правилом HPE ArubaOS-CX 10.04+ (Идентификатор правила: RV-N-43).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события ArubaOS CX.

Найти события ArubaOS CX в хранилище можно по следующему фильтру:

```
dproduct = "ArubaOS-CX"
```



Совпадений 5

Интервал времени: 2024-07-05T11:14:19.609+03:00 - 2024-07-05T11:29:19.609+03:00

id	sourceip	timestamp	type	dvendor
717b8978-5313-4dbd-8b71-...		2024-07-05T11:24:09.000+...	нормализованное событие	HPE
669866ad-1b9a-4148-bdbd-...		2024-07-05T11:23:51.000+...	нормализованное событие	HPE
72806391-594b-41dc-866d-...		2024-07-05T11:23:51.000+...	нормализованное событие	HPE
2f80ac58-6f89-4faf-a740-d6c0fb83922d		2024-07-05T11:20:21.000+...	нормализованное событие	HPE
f73b78b8-289f-45a1-8cb6-...		2024-07-05T11:16:32.000+...	нормализованное событие	HPE

Показывается первых 500 записей

Детали события 717b8978-5313-4dbd-8b71-83f6d0d08850

☒ Скрыть пустые поля события

Дата и время

timestamp 2024-07-05T11:24:09.000+03:00

Служебные данные

id 717b8978-5313-4dbd-8b71-83f6d0d08850

tenantId 00000000-0000-0000-0000-000000000000

collectorId 29d2deeb-8354-4baa-89aa-997e52edbdde

type нормализованное событие

Сведения о событии

dvendor HPE

dproduct ArubaOS-CX

dversion 10.04+

name LACP event

severity Information

cat LACP

externalId 1306

msg LACP mode set to passive for LAG 5

outcome Success

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Huawei

Данный раздел содержит список систем для настройки от компании Huawei.

- [USG](#)

USG

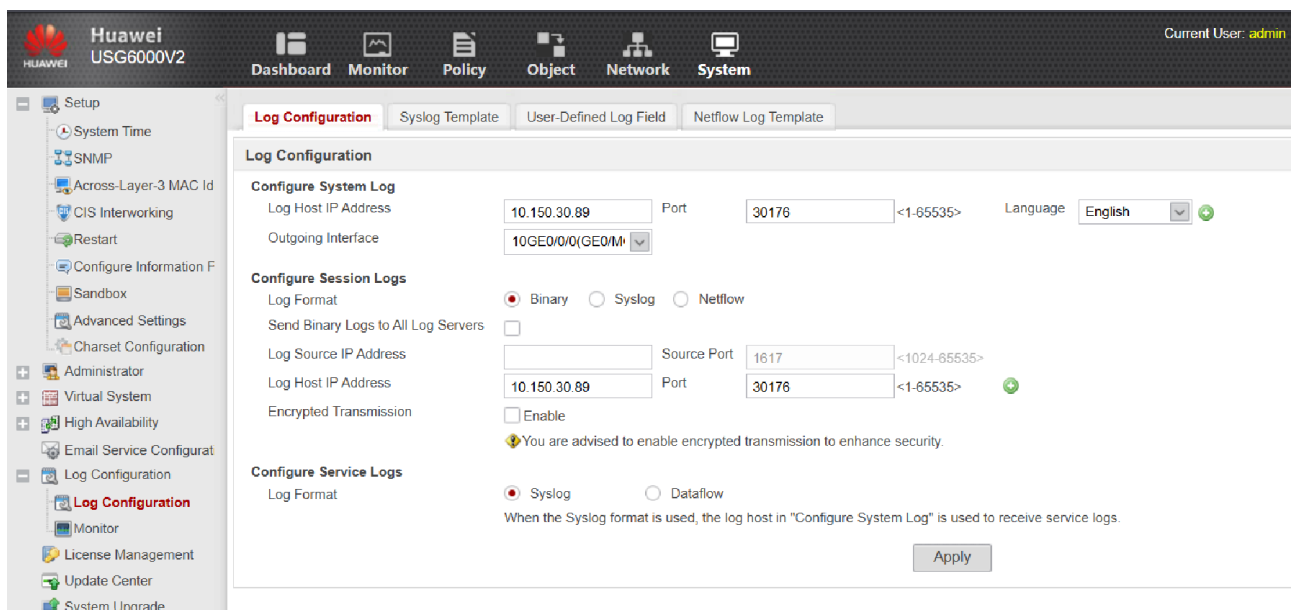
Данное руководство описывает процесс настройки сбора и отправки событий межсетевого экрана Huawei USG в R-Vision SIEM.

- [Настройка Huawei USG](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Настройка Huawei USG

В настоящем руководстве рассматривается передача событий с помощью syslog.

1. Откройте веб-интерфейс Huawei USG.
2. На панели администрирования устройства перейдите на вкладку **System** → **Log Configuration**.
3. Укажите адрес коллектора и [UDP порт точки входа конвейера SIEM](#).



4. Выберите из выпадающего списка **Outgoing Interface** исходящий интерфейс.
5. Примените конфигурацию, нажав на кнопку **Apply**.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

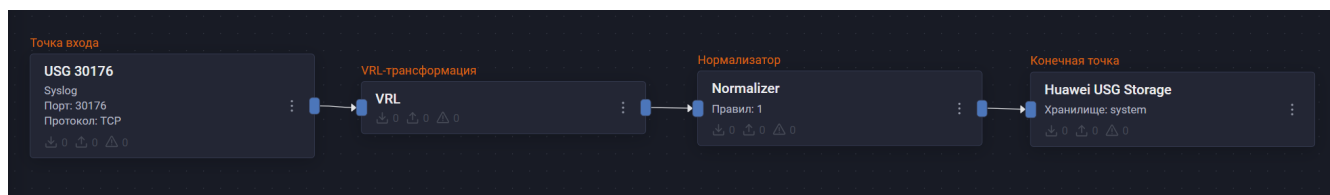
1. Перейдите в раздел **Ресурсы** → **Коллекторы** и создайте новый конвейер в коллекторе.

- Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Syslog.
 - Порт точки входа и протокол: в соответствии с настройками на стороне [Huawei USG](#).
- Добавьте VRL-трансформацию:

```
.dvendor = "Huawei"
.dproduct = "USG"
```

- Добавьте на конвейер элемент **Нормализатор** с правилом Huawei USG (идентификатор правила: RV-N-172). Соедините нормализатор с VRL-трансформацией.
- Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
- Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события Huawei USG.

Найти события Huawei USG в хранилище можно по следующему фильтру:

```
dproduct = "USG"
```



Добавить фильтр

☐ Инvertировать (NOT)

Поле

dproduct

Оператор

=

Значение

USG

☐ Настроить заголовок

Отменить

Добавить

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по](#)

ссылке.

Данный раздел содержит список систем для настройки от компании Kaspersky:

- [Kaspersky Security Center](#)

Kaspersky Security Center

Данный раздел содержит список инструкций по настройке источника Kaspersky Security Center:

- [Сбор событий из СУБД MSSQL](#)
- [Сбор событий из СУБД PostgreSQL](#)
- [Сбор событий из СУБД MySQL \(Maria DB\)](#)
- [Сбор событий в формате CEF](#)

Сбор событий в формате CEF

Предварительные требования

- Лицензии: Kaspersky Endpoint Security (расширенная) или Kaspersky Symphony (сбор событий в формате CEF)

Настройка Security Center

Для пересылки событий, зарегистрированных Kaspersky Security Center, в R-Vision SIEM в формате CEF выполните следующие действия:

1. Откройте консоль управления KSC и выберите сервер администрирования.
2. Из выпадающего списка **Настроить параметры уведомлений и экспорта событий** выберите **Настроить экспорт в SIEM-систему**.

The screenshot shows the Kaspersky Security Center (KSC) console. The left sidebar contains navigation options: 'Server Administration KSC02', 'Managed Devices', 'Device Selections', 'Unmanaged Devices', 'Policies', 'Tasks', 'Licenses', 'Kaspersky Labs', and 'Additional'. The main window displays the 'Events' tab for the server 'KSC02 (SEA/misrafilov)'. The 'Events' tab is selected, and the 'Last Events' view is active. The table shows a list of events with columns: 'Время' (Time), 'Устройство' (Device), 'Событие' (Event), 'Описание' (Description), 'Группа' (Group), 'Программа' (Program), and 'Номер версии' (Version). The 'Events' tab is selected, and the 'Last Events' view is active. There are buttons for 'Запустить выборку' (Run Selection), 'Свойства выборки' (Custom Selection), 'Создать выборку' (Create Selection), and 'Импорт/Экспорт' (Import/Export). A search bar is also present.

3. В раскрывшемся окне укажите следующие параметры:
 - SIEM-система: ArcSight (CEF-формат).
 - Адрес сервера SIEM-системы: Адрес коллектора
 - Порт сервера: Порт точки входа в конвейере.
4. Сохраните изменения, нажав **ОК**.

Свойства: События

Разделы

- Уведомление
- Экспорт событий**

Экспорт событий

☒ Автоматически экспортировать события в базу SIEM-системы

SIEM-система:
ArcSight (CEF-формат)

Адрес сервера SIEM-системы: 10.150.30.89

Порт сервера SIEM-системы: 30108

Протокол: TCP/IP

Максимальный размер сообщения в байтах: 2048

Параметры...

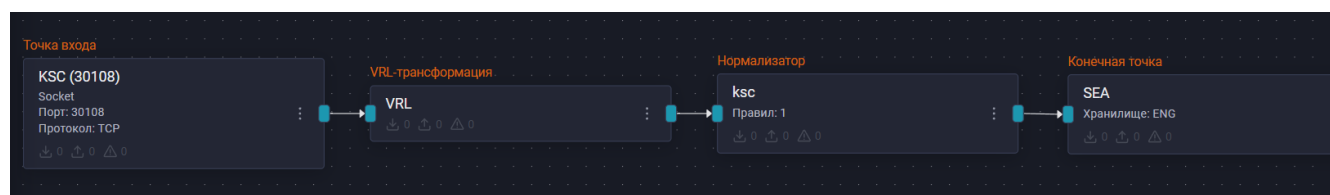
Чтобы экспортировать имеющиеся события, начиная с указанной даты, нажмите на кнопку "Экспортировать архив".

Экспортировать архив...

[Справка](#) **ОК** Отмена Применить

Настройка в R-Vision SIEM

Общий вид рабочего конвейера для обеспечения получения и отображения событий:



Для сбора событий KSC в формате CEF настройте следующий конвейер:

1. Добавьте точку входа со следующими параметрами:
 - Тип точки входа: Socket.
 - Название: произвольное, понятное.
 - Порт точки входа: произвольный больше 30000.
2. Добавьте VRL-трансформацию со следующим содержимым:

```
.dvendor = "Kaspersky"  
.dproduct = "KSC"
```

3. Добавьте нормализатор с правилом "Kaspersky Security Center CEF".
4. Добавьте конечную точку типа **Хранилище событий**.
5. Установите конфигурацию конвейера.

Если настройка выполнена корректно, в хранилище начнут поступать события KSC.

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Сбор событий из СУБД MSSQL

Предварительные требования

- Сетевая доступность между R-Vision SIEM и СУБД Kaspersky Security Center (tcp/1433).
- Учетная запись в СУБД с правами на чтение таблицы **kav.dbo.ev_event** (Сбор событий из БД).

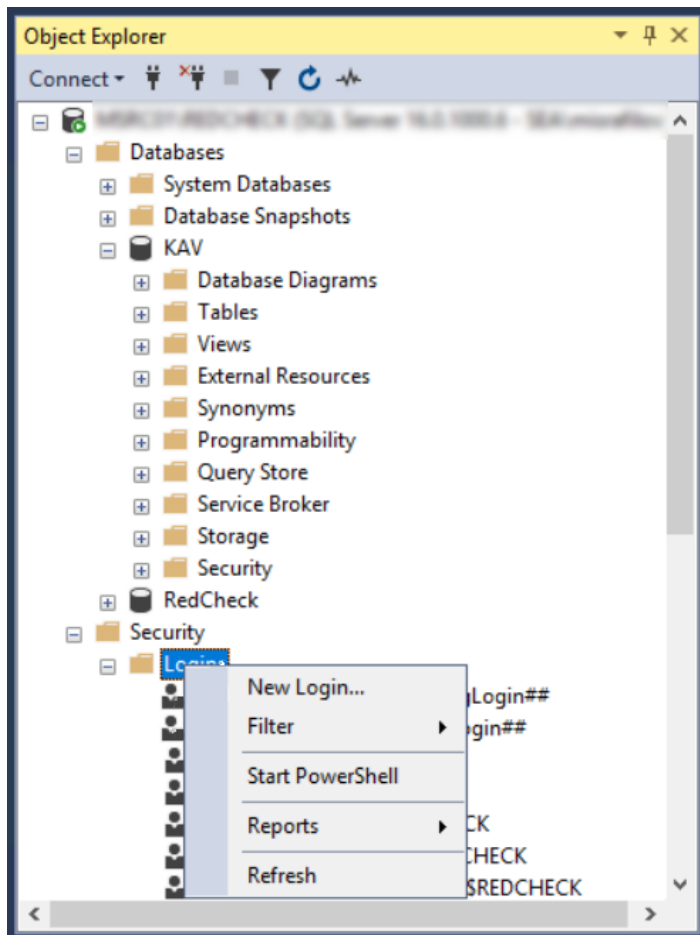
Настройка в СУБД MS SQL

События Kaspersky Security Center записываются в таблицу **ev_event** базы данных KAV СУБД MS SQL. Для настройки сбора логов из базы данных необходимо к ней подключиться. Чтобы подключиться к БД, используйте специально созданную сервисную учетную запись (далее — УЗ).

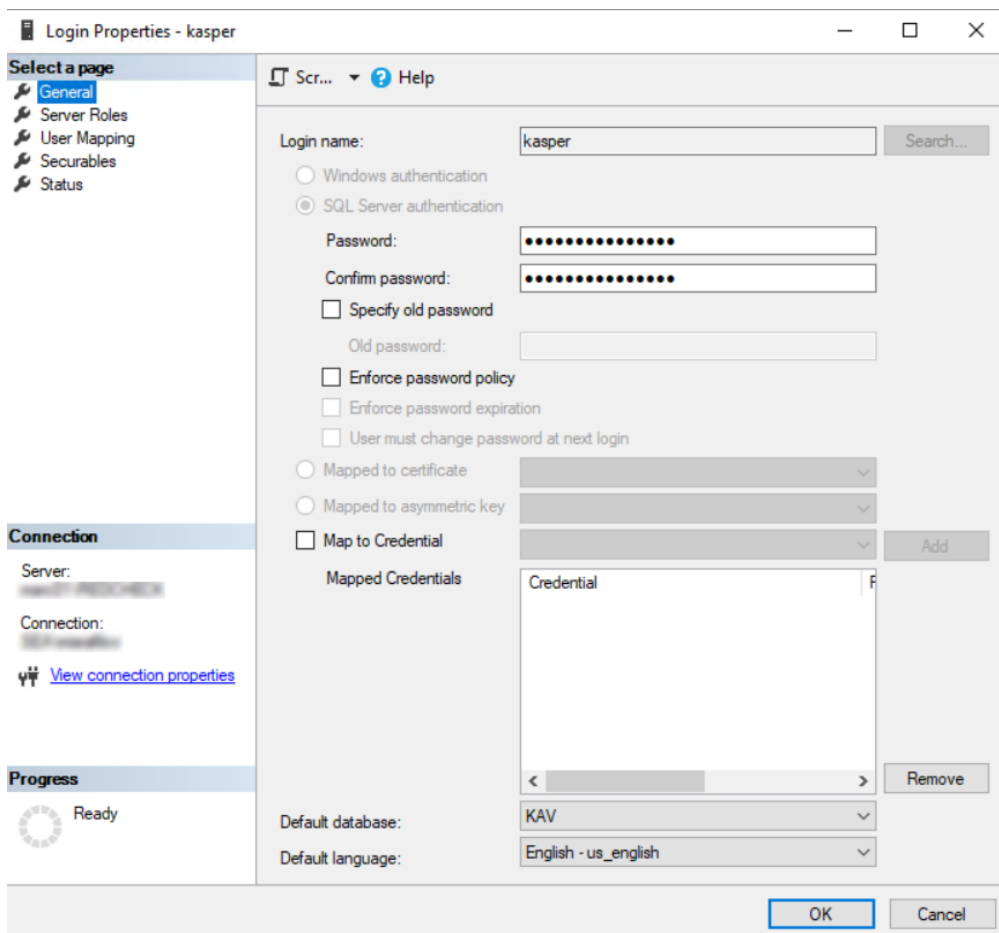
Создание учетной записи в СУБД MS SQL

Чтобы создать сервисную УЗ, подключитесь к СУБД с правами администратора. Для этого выполните следующие действия в SQL Server Management Studio:

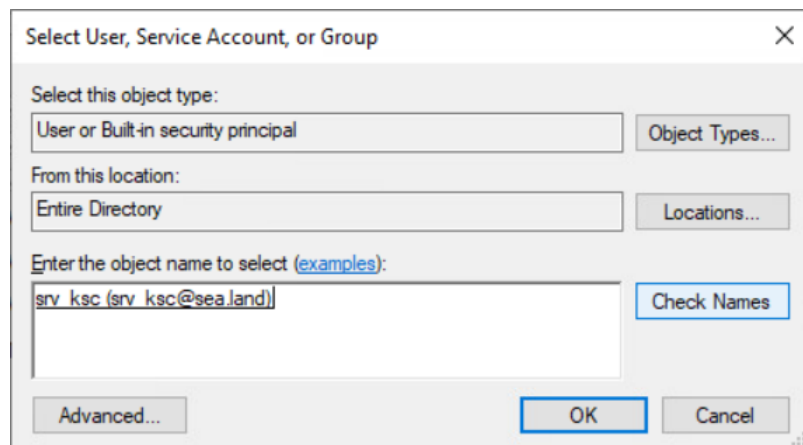
1. Выберите **New Login** в контекстном меню для **Security/Logins**.



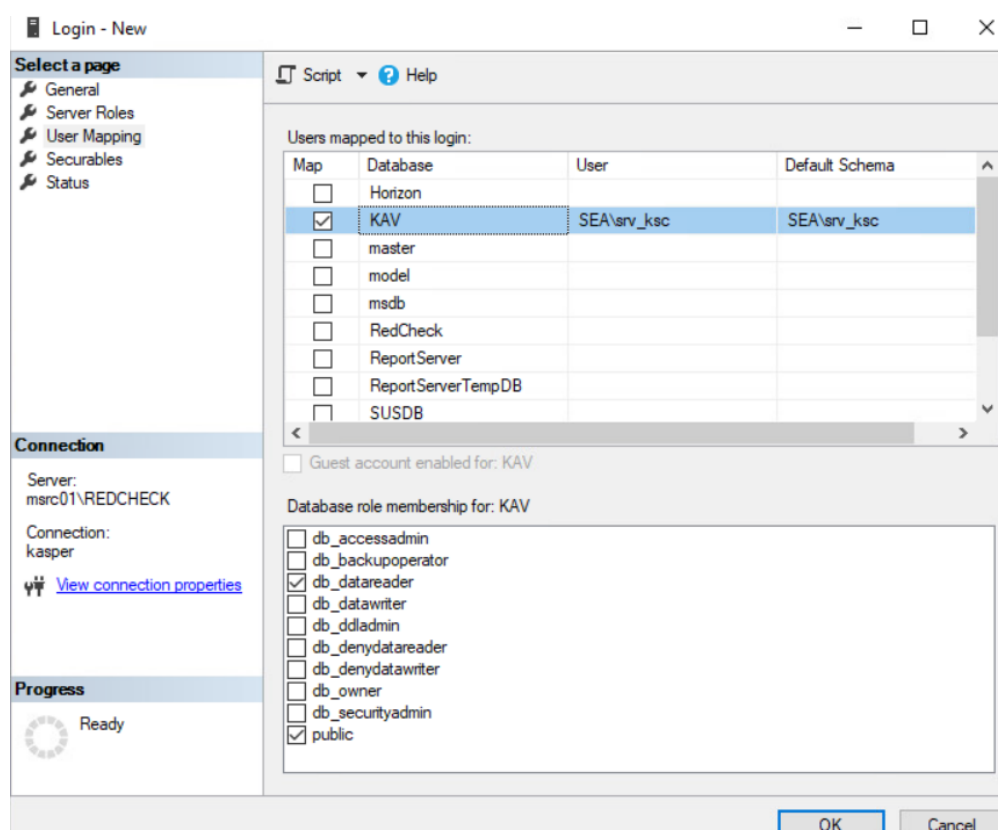
2. Создайте сервисную учетную запись.



Вместо локальной УЗ вы также можете использовать заранее созданную доменную.

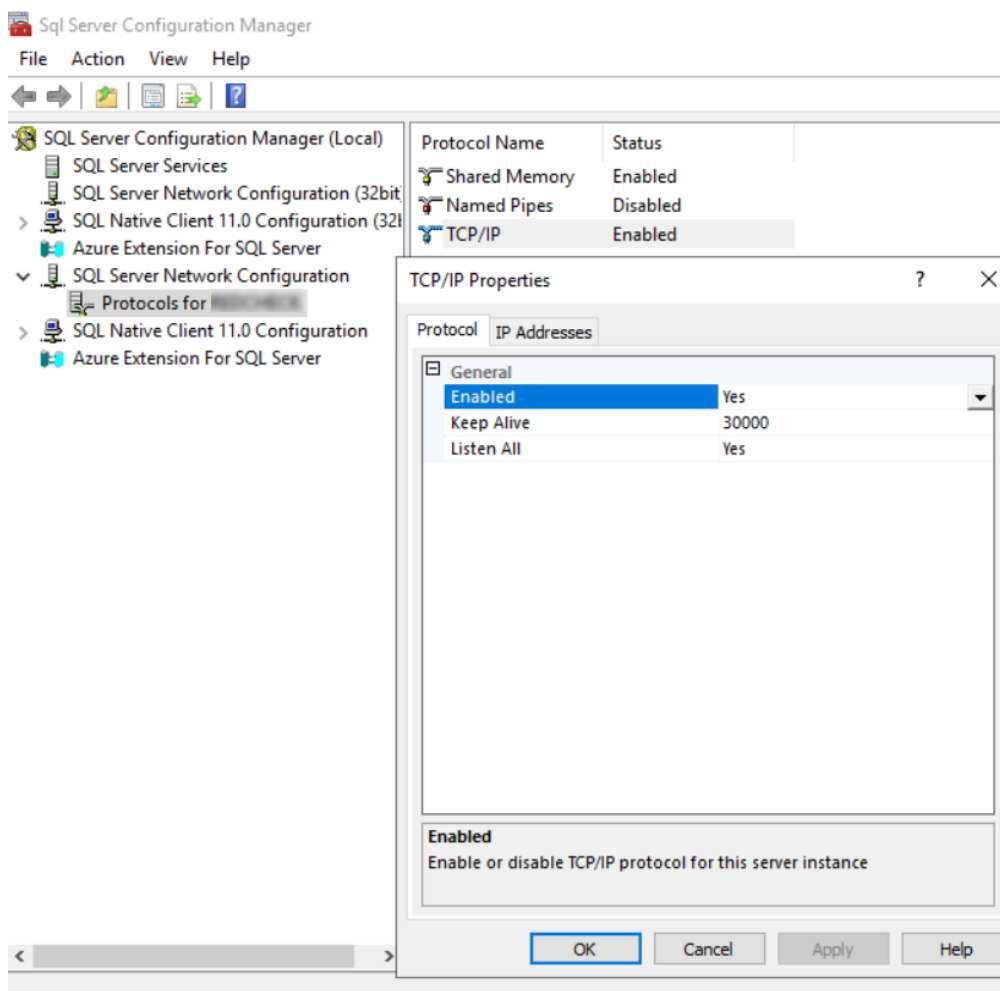


3. Предоставьте учетной записи права на чтение базы KAV.



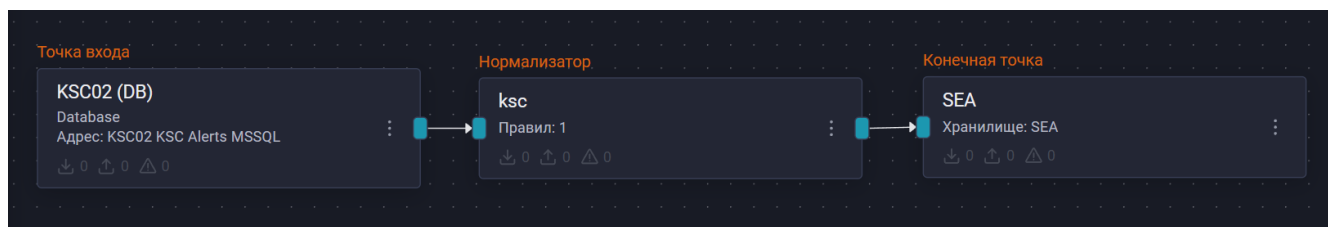
Настройка сервера MS SQL

В настройках SQL Server Configuration Manager убедитесь, что TCP/IP включен в конфигурации сети SQL Server.



Настройка в R-Vision SIEM

Общий вид рабочего конвейера для обеспечения получения и отображения событий:



Для подключения базы данных MS SQL в качестве источника событий в SIEM настройте следующий конвейер:

1. Создайте точку входа со следующими параметрами:

- Тип точки входа: Database.
- SQL-запрос:

```
SELECT
    TOP 10000 ev.event_id AS event_id
    , ev.event_type_id AS deviceEventClassId
    , ev.severity AS severity
    , ev.task_display_name AS taskDisplayName
    , ev.product_name AS product_name
```

```

, ev.product_displ_version AS product_version
, ev.event_type AS externalId
, ev.event_type_display_name AS event_subcode
, ev.descr AS msg
, CASE
    WHEN ev.rise_time is not NULL
    THEN DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.rise_time
)
    ELSE ev.rise_time END AS endTime
, CASE
    WHEN ev.registration_time is not NULL
    THEN
DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.registration_time )
    ELSE ev.registration_time END AS kscRegistrationTime
, cast(ev.par7 AS varchar(4000)) AS sourceUserName
, hs.wstrWinName AS dHost
, hs.wstrWinDomain AS strNtDom
, serv.wstrWinName AS kscName
, CAST(hs.nIp / 256 / 256 / 256 % 256 AS VARCHAR) + '.'
    + CAST(hs.nIp / 256 / 256 % 256 AS VARCHAR) + '.'
    + CAST(hs.nIp / 256 % 256 AS VARCHAR) + '.'
    + CAST(hs.nIp % 256 AS VARCHAR) AS sourceAddress
, serv.wstrWinDomain AS kscNtDomain
, CAST(serv.nIp / 256 / 256 / 256 % 256 AS VARCHAR) + '.'
    + CAST(serv.nIp / 256 / 256 % 256 AS VARCHAR) + '.'
    + CAST(serv.nIp / 256 % 256 AS VARCHAR) + '.'
    + CAST(serv.nIp % 256 AS VARCHAR) AS kscIP
, CASE
    WHEN virus.tmVirusFoundTime IS NOT NULL
    THEN
DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),virus.tmVirusFoundTime )
    ELSE ev.registration_time END AS virusTime
, virus.wstrObject AS filePath
, virus.wstrVirusName AS virusName
, virus.result_ev AS result
FROM kav.dbo.ev_event AS ev
LEFT JOIN kav.dbo.v_akpub_host AS hs
    ON ev.nHostId = hs.nId
INNER JOIN kav.dbo.v_akpub_host AS serv
    ON serv.nId = 1
LEFT JOIN kav.dbo.rpt_viract_index AS Virus
    ON ev.event_type_id = virus.nEventVirus
WHERE event_id > ?

```



При большом количестве событий в СУБД рекомендуется добавлять **TOP 10000** в начало SQL-запроса.

- База данных: MS SQL.
- Интервал запроса: 15.

- Поле идентификатора:
 - Ключ: event_id.
 - Значение: 1.
- Строка подключения в секрете:

```
jdbc:sqlserver://DBSERVER:1433;encrypt=false;databaseName=KAV;user=kasper;password=passwd
```

Строка подключения в секрете в случае использования доменной учетной записи:

```
jdbc:sqlserver://DBSERVER:1433;encrypt=false;databaseName=KAV;authenticationScheme=NTLM;integratedSecurity=true;user=svr_ksc;password=P@ssw0rd
```

Здесь:

- **DBSERVER**-- FQDN или IP-адрес сервера СУБД.
- **1433**-- порт подключения

2. Добавьте нормализатор с правилом "Kaspersky Security Center".
3. Добавьте конечную точку типа **Хранилище событий**.
4. Установите конфигурацию конвейера.

Если настройка выполнена корректно, в хранилище начнут поступать события из MS SQL.

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Сбор событий из СУБД MySQL (Maria DB)

Предварительные требования

- Сетевой доступ к БД Kaspersky Security Center.
- Учетная запись в СУБД с правами на чтение таблицы **ev_event** (Сбор событий из БД).

Настройки СУБД MySQL (MariaDB)

Создание учетной записи в СУБД MySQL (MariaDB)

Для создания сервисной УЗ подключитесь к СУБД с правами администратора. Для этого на сервере с установленной СУБД выполните следующие действия:

1. Выполните следующую команду из-под пользователя root:

```
mysql -u root -p
```

2. Создайте сервисную учетную запись, выполнив следующую команду:

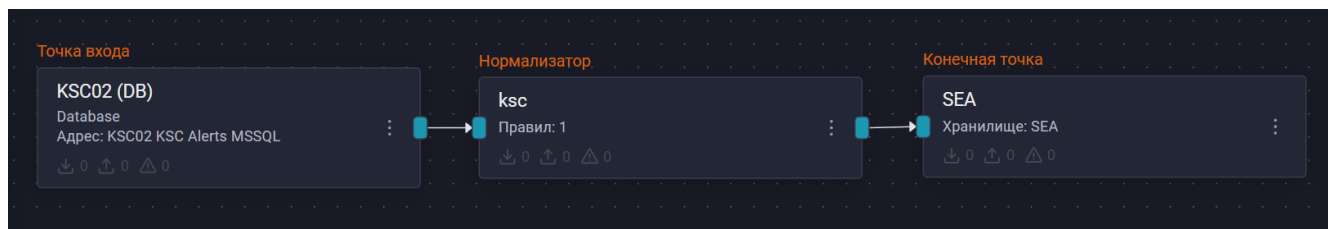
```
CREATE USER 'kasper'@'localhost' IDENTIFIED BY 'passw0rd';
```

3. Выдайте права на подключение к базе и чтение таблицы:

```
GRANT CONNECT ON DATABASE KAV to kasper;  
GRANT SELECT ON ev_event TO 'kasper'@'localhost';
```

Настройка в R-Vision SIEM

Общий вид рабочего конвейера для обеспечения получения и отображения событий:



Для подключения базы данных MySQL (MariaDB) в качестве источника событий в SIEM настройте следующий конвейер:

1. Создайте точку входа со следующими параметрами:

- Тип точки входа: Database.
- SQL-запрос:

```
SELECT  
ev.event_id AS event_id,  
    ev.event_type_id AS deviceEventClassId,  
    ev.severity AS severity,  
    ev.task_display_name AS taskDisplayName,  
    ev.product_name AS product_name,  
    ev.product_displ_version AS product_version,  
    ev.event_type AS externalId,  
    ev.event_type_display_name AS event_subcode,  
    ev.descr AS msg,  
    CASE  
        WHEN ev.rise_time IS NOT NULL THEN DATE_ADD(ev.rise_time, INTERVAL  
TIMESTAMPDIFF(HOUR, UTC_TIMESTAMP(), NOW()) HOUR)  
        ELSE ev.rise_time  
    END AS endTime,  
    CASE  
        WHEN ev.registration_time IS NOT NULL THEN
```



```

DATE_ADD(ev.registration_time, INTERVAL TIMESTAMPDIF(HOUR, UTC_TIMESTAMP(),
NOW())) HOUR)
    ELSE ev.registration_time
END AS kscRegistrationTime,
CAST(ev.par7 AS CHAR(4000)) AS sourceUserName,
hs.wstrWinName AS dHost,
hs.wstrWinDomain AS strNtDom,
serv.wstrWinName AS kscName,
CONCAT(
    FLOOR(hs.nIp / 256 / 256 / 256 % 256), '.',
    FLOOR(hs.nIp / 256 / 256 % 256), '.',
    FLOOR(hs.nIp / 256 % 256), '.',
    FLOOR(hs.nIp % 256)
) AS sourceAddress,
serv.wstrWinDomain AS kscNtDomain,
CONCAT(
    FLOOR(serv.nIp / 256 / 256 / 256 % 256), '.',
    FLOOR(serv.nIp / 256 / 256 % 256), '.',
    FLOOR(serv.nIp / 256 % 256), '.',
    FLOOR(serv.nIp % 256)
) AS kscIP,
CASE
    WHEN virus.tmVirusFoundTime IS NOT NULL THEN
DATE_ADD(virus.tmVirusFoundTime, INTERVAL TIMESTAMPDIF(HOUR, UTC_TIMESTAMP(),
NOW())) HOUR)
    ELSE ev.registration_time
END AS virusTime,
virus.wstrObject AS filePath,
virus.wstrVirusName AS virusName,
virus.result_ev AS result
FROM kav.ev_event AS ev
LEFT JOIN kav.v_akpub_host AS hs ON ev.nHostId = hs.nId
INNER JOIN kav.v_akpub_host AS serv ON serv.nId = 1
LEFT JOIN kav.rpt_viract_index AS virus ON ev.event_type_id = virus.nEventVirus
WHERE
    ev.event_id > ? ORDER BY ev.event_id ASC

```

- База данных: MySQL.
- Интервал запроса: 15.
- Поле идентификатора:
 - Ключ: event_id.
 - Значение: 1.
- Строка подключения в секрете:

```
jdbc:mysql://DBSERVER:3306/kav?user=kasper&password=passw0rd
```

Здесь:

- **DBSERVER**-- FQDN или IP-адрес сервера СУБД.
 - **3306**-- порт подключения
2. Добавьте нормализатор с правилом "Kaspersky Security Center".
 3. Добавьте конечную точку типа **Хранилище событий**.
 4. Установите конфигурацию конвейера.

Если настройка выполнена корректно, в хранилище начнут поступать события из MySQL.

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Сбор событий из СУБД PostgreSQL

Предварительные требования

- Сетевой доступ к БД Kaspersky Security Center.
- Учетная запись в СУБД с правами на чтение таблицы **ev_event** (Сбор событий из БД).

Настройки СУБД PostgreSQL

События Kaspersky Security Center записываются в таблицу **ev_event** базы данных KAV СУБД MS SQL. Для настройки сбора логов из базы данных необходимо к ней подключиться. Чтобы подключиться к БД, используйте специально созданную сервисную учетную запись (далее — УЗ).

Создание учетной записи в СУБД PostgreSQL

Чтобы создать сервисную УЗ, подключитесь к СУБД с правами администратора. Для этого выполните следующие действия на сервере с установленной СУБД:

1. Выполните следующую команду из-под пользователя postgres:

```
sudo -u postgres psql
```

2. Создайте сервисную учетную запись, выполнив следующие команды:

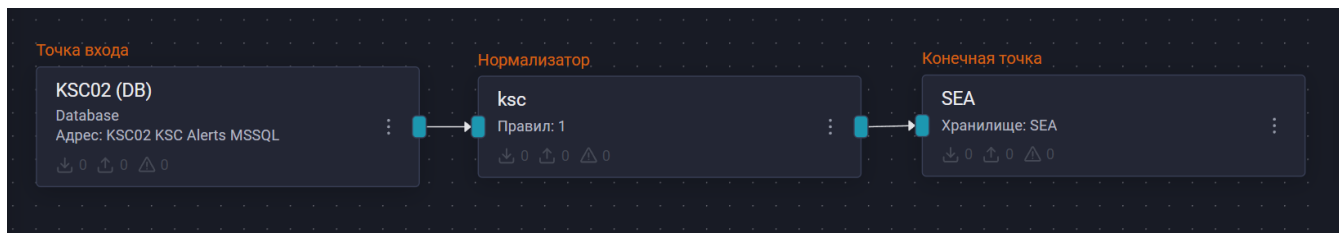
```
CREATE USER "kasper";  
ALTER ROLE kasper WITH PASSWORD 'passw0rd';
```

3. Выдайте права на подключение к базе и чтение таблицы:

```
GRANT CONNECT ON DATABASE KAV to kasper;  
GRANT SELECT ON ev_event TO kasper;
```

Настройка в R-Vision SIEM

Общий вид рабочего конвейера для обеспечения получения и отображения событий:



Для подключения базы данных PostgreSQL в качестве источника событий в SIEM настройте следующий конвейер:

1. Создайте точку входа со следующими параметрами:

- Тип точки входа: Database.
- SQL-запрос:

```
SELECT
    ev.event_id AS event_id,
    ev.event_type_id AS deviceEventClassId,
    ev.severity AS severity,
    ev.task_display_name AS taskDisplayName,
    ev.product_name AS product_name,
    ev.product_displ_version AS product_version,
    ev.event_type AS externalId,
    ev.event_type_display_name AS event_subcode,
    ev.descr AS msg,
    CASE
        WHEN ev.rise_time IS NOT NULL THEN ev.rise_time + INTERVAL '1 hour' *
(EXTRACT(EPOCH FROM (NOW() AT TIME ZONE 'UTC' - NOW())) / 3600)
        ELSE ev.rise_time
    END AS endTime,
    CASE
        WHEN ev.registration_time IS NOT NULL THEN ev.registration_time +
INTERVAL '1 hour' * (EXTRACT(EPOCH FROM (NOW() AT TIME ZONE 'UTC' - NOW())) /
3600)
        ELSE ev.registration_time
    END AS kscRegistrationTime,
    CAST(ev.par7 AS VARCHAR(4000)) AS sourceUserName,
    hs."wstrWinName" AS dHost,
    hs."wstrWinDomain" AS strNtDom,
    serv."wstrWinName" AS kscName,
    CONCAT(
        (hs."nIp" >> 24) & 255, '.',
        (hs."nIp" >> 16) & 255, '.',
        (hs."nIp" >> 8) & 255, '.',
        hs."nIp" & 255
    ) AS sourceAddress,
    serv."wstrWinDomain" AS kscNtDomain,
```

```

CONCAT(
    (serv."nIp" >> 24) & 255, '.',
    (serv."nIp" >> 16) & 255, '.',
    (serv."nIp" >> 8) & 255, '.',
    serv."nIp" & 255
) AS kscIP,
CASE
    WHEN virus."tmVirusFoundTime" IS NOT NULL THEN virus."tmVirusFoundTime"
+ INTERVAL '1 hour' * (EXTRACT(EPOCH FROM (NOW() AT TIME ZONE 'UTC' - NOW())) /
3600)
    ELSE ev.registration_time
END AS virusTime,
virus."wstrObject" AS filePath,
virus."wstrVirusName" AS virusName,
virus.result_ev AS result
FROM ev_event AS ev
LEFT JOIN v_akpub_host AS hs ON ev."nHostId" = hs."nId"
INNER JOIN v_akpub_host AS serv ON serv."nId" = 1
LEFT JOIN rpt_viract_index AS virus ON ev.event_type_id = virus."nEventVirus"
WHERE ev.event_id > CAST(? AS BIGINT)
ORDER BY ev.event_id ASC LIMIT 10000;

```

- База данных: MySQL.
- Интервал запроса: 15.
- Поле идентификатора:
 - Ключ: event_id.
 - Значение: 1.
- Строка подключения в секрете:

```
jdbc:postgresql://DBSERVER:5432/KAV?user=kasper&password=passw0rd
```

Здесь:

- **DBSERVER** — FQDN или IP-адрес сервера СУБД.
- **5432** -- порт подключения

2. Добавьте нормализатор с правилом "Kaspersky Security Center".
3. Добавьте конечную точку типа **Хранилище событий**.
4. Установите конфигурацию конвейера.

Если настройка выполнена корректно, в хранилище начнут поступать события из PostgreSQL.

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Kaspersky Web Traffic Security

Данное руководство описывает процесс настройки сбора и отправки событий Kaspersky Web Traffic Security в R-Vision SIEM.

- [Настройка Kaspersky Web Traffic Security](#)
 - [Настройка журналирования Kaspersky Web Traffic Security](#)
 - [Отправка событий Kaspersky Web Traffic Security](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)
- [Настройка SSH-доступа](#)

Настройка Kaspersky Web Traffic Security

Настройка журналирования Kaspersky Web Traffic Security

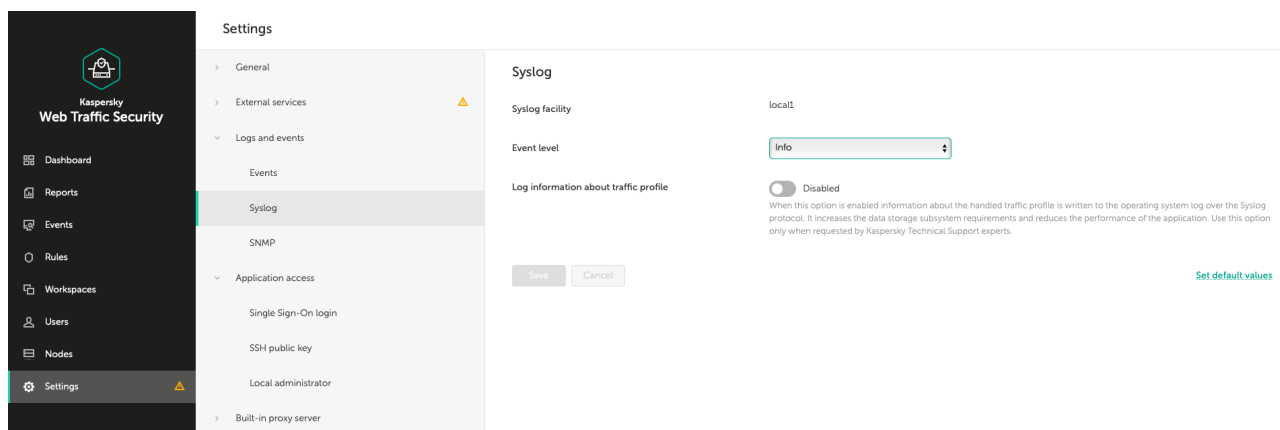
Для настройки rsyslog выполните следующие действия:

1. Подключитесь к консоли управления Kaspersky Web Traffic Security.
 - Если Kaspersky Web Traffic Security был установлен из ISO-файла, подключитесь к консоли управления Kaspersky Web Traffic Security с помощью учетной записи root по протоколу SSH.



Информацию о загрузке ключа можно найти в разделе [Настройка SSH-доступа](#).

- Если Kaspersky Web Traffic Security был установлен из RPM- или DEB-пакета, запустите командную оболочку операционной системы для выполнения команд с полномочиями суперпользователя (администратора системы).
2. Из веб-меню администратора перейдите в меню настройки syslog. Запомните или запишите значение Syslog facility, используемого основной системой. Данное значение может меняться в зависимости от инсталляции.



3. События передаются во внешнюю SIEM-систему с помощью системной службы ведения журналов rsyslog. Убедитесь, что служба установлена и запущена, с помощью команды:

```
systemctl status rsyslog
```

- Если служба установлена и запущена, ее статус будет **running**.
 - Если служба rsyslog не запущена или отсутствует, установите и активируйте службу rsyslog согласно документации вашей операционной системы.
4. Укажите адрес и порт подключения к серверу с SIEM-системой. Для этого создайте файл /etc/rsyslog.d/kwts-cef-messages.conf и добавьте в него следующие строки:

```
$ActionQueueFileName ForwardToSIEM5
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
<facility>.* @@<IP-адрес любого доступного рабочего узла SIEM>:<Номер выбранного
порта вашей точки входа>
<facility>.* stop
```

Здесь:

- **<facility>** — значение Syslog facility, которое вы посмотрели на шаге 2. По умолчанию значение Syslog facility — **local5**.
5. Перезапустите службу rsyslog с помощью команды:

```
systemctl restart rsyslog
```

Отправка событий Kaspersky Web Traffic Security

Перед включением экспорта событий в формате CEF требуется установить пакет обновления siem_logging_fixes.zip на каждом узле кластера Kaspersky Web Traffic Security. Пакет обновления предоставляется по запросу в службу технической поддержки.

Выполните следующие шаги на каждом узле кластера, события с которого требуется экспортировать в формате CEF.

1. Подключитесь к консоли управления Kaspersky Web Traffic Security.
 - Если Kaspersky Web Traffic Security был установлен из ISO-файла, подключитесь к консоли управления виртуальной машиной Kaspersky Web Traffic Security под учетной записью root, используя закрытый ключ SSH. Будет осуществлен вход в Technical Support Mode.
 - Если Kaspersky Web Traffic Security был установлен из RPM- или DEB-пакета, запустите командную оболочку операционной системы для выполнения команд с полномочиями суперпользователя (администратора системы).
2. Перейдите в каталог **/opt/kaspersky/kwts/share/templates/core_settings** и создайте резервную копию файла event_logger.json.template с помощью команды:

```
cp -p event_logger.json.template event_logger.json.template.backup
```

3. Откройте файл `event_logger.json.template` в режиме редактирования и, соблюдая синтаксис и структуру JSON-файла, в секции **siemSettings** укажите следующие значения параметров:

- **enabled: true;**
- **facility: Local5** — указанный ранее на шаге [настройки rsyslog](#);
- **logLevel: Info.**

4. В веб-интерфейсе приложения в разделе **Параметры** → **Журналы и события** внесите изменения в значение любого параметра и нажмите на кнопку **Сохранить**. Это необходимо для синхронизации параметров между узлами кластера и применения изменений, внесенных в конфигурационный файл. После этого можно вернуть исходное значение измененного параметра.

5. Убедитесь, что изменения применены, с помощью команды:

```
/opt/kaspersky/kwts/bin/kwts-control --get-settings 20 --format json | grep -A 4 siemSettings
```

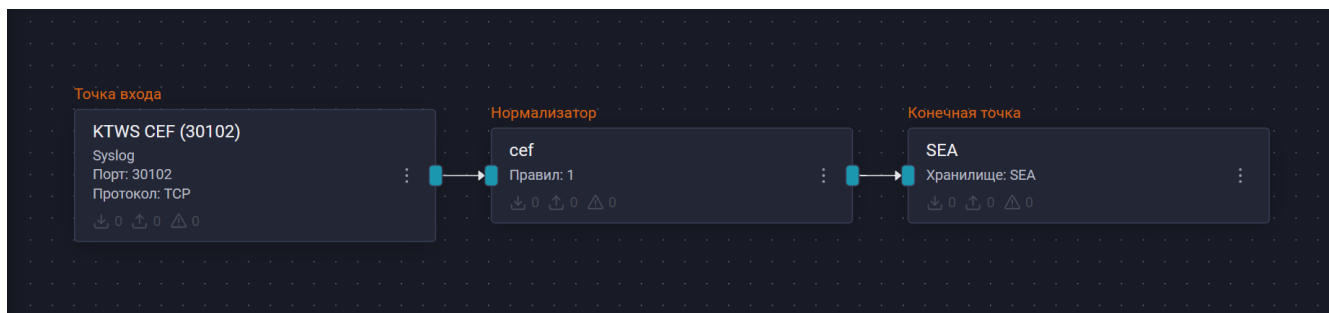
Результат выполнения команды должен содержать параметры со значениями, указанными на шаге 3.

Экспорт событий в формате CEF настроен.

Настройка в R-Vision SIEM

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Syslog**.
 - Порт точки входа: введите значение в диапазоне 30 000—32 000, указанное ранее в разделе [отправки событий Kaspersky Web Traffic Security](#).
 - Протокол: выберите вариант в соответствии с настройками на стороне [Kaspersky Web Traffic Security](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Kaspersky Web Traffic Security** (идентификатор правила: **RV-N-52**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



Если настройка выполнена корректно, после [настройки передачи событий](#) в хранилище начнут поступать события Kaspersky Web Traffic Security.

События Хранилище событий: **kaspersky_syslog** admin

↑ | 📄 | 🔍 raw like "%KWTS%" x | Последний период | 30 | - + | минут | 🔍 Поиск

+ Добавить фильтр

Совпадений 42 Интервал времени: 20.02.2024 14:57:44 - 20.02.2024 15:27:44 Показать график

id	sourceip	tenantId	art	raw	collectorId	timestamp	aggregationRu
27704f42-6425-47c7-9148-...		99311ef1-32a1-4b2d-9d38-...		{"appname": "KWTS", "facility": "local5", "h...	436e8c9e-744a-4ebd-9c96-...	20.02.2024 15:26:26	
57b816cf-9fb9-4ebb-9de0-...		99311ef1-32a1-4b2d-9d38-...		{"appname": "KWTS", "facility": "local5", "h...	436e8c9e-744a-4ebd-9c96-...	20.02.2024 15:24:30	
ac6c6dff-6b84-49a7-858a-...		99311ef1-32a1-4b2d-9d38-...		{"appname": "KWTS", "facility": "local5", "h...	436e8c9e-744a-4ebd-9c96-...	20.02.2024 15:24:30	
767e6de0-0c7f-4903-998c-...		99311ef1-32a1-4b2d-9d38-...		{"appname": "KWTS", "facility": "local5", "h...	436e8c9e-744a-4ebd-9c96-...	20.02.2024 15:24:19	
b33a7736-7ea5-430d-9869-...		99311ef1-32a1-4b2d-9d38-...		{"appname": "KWTS", "facility": "local5", "h...	436e8c9e-744a-4ebd-9c96-...	20.02.2024 15:22:31	
b01153a5-a567-4487-8205-...		99311ef1-32a1-4b2d-9d38-...		{"appname": "KWTS", "facility": "local5", "h...	436e8c9e-744a-4ebd-9c96-...	20.02.2024 15:22:19	

« < 1 > » 20 00:00.429 🔁 Автообновление 📅

Найти события Kaspersky Web Traffic Security в хранилище можно по следующему фильтру:

dproduct = "KWTS"



Добавить фильтр

☐ Инvertировать (NOT)

Поле

dproduct

Оператор

=

Значение

KWTS

☐ Настроить заголовок

Отменить

Добавить

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Настройка SSH-доступа

Настройка отправки событий осуществляется с помощью Technical Support Mode, доступ к которому можно получить только через SSH-интерфейс. Для первичного входа в SSH-интерфейс необходимо загрузить свой персональный ключ доступа SSH через интерфейс администратора.

Для загрузки ключа выполните следующие операции:

1. Войдите в веб-интерфейс Kaspersky Web Traffic Security под учетной записью Administrator. Пароль к данной учетной записи устанавливается во время установки продукта.
2. Сгенерируйте свой ключ на любой машине.

Пример 2. Пример команды для генерации ключа на Linux-машине

```
ssh-keygen -t rsa
```

3. В меню веб-интерфейса вставьте публичный ключ **<filename>.pub**.



Kaspersky
Web Traffic Security

Dashboard

Reports

Events

Rules

Workspaces

Users

Nodes

Settings

Settings

General

External services

Logs and events

Application access

SSH public key

Local administrator

Built-in proxy server

SSH public key

Add an SSH public key to get access to Technical Support Mode.

Description

main_key

SSH key

ssh-keygen -t rsa <data>|

Add

Kubernetes (K8s)

Данная инструкция описывает настройку сбора событий с узла Kubernetes и их отправки в систему R-Vision SIEM.

- [Настройка Kubernetes](#)
 - [Настройка сервиса Vector](#)
 - [Настройка KubeApi](#)
- [Настройка в R-Vision SIEM](#)

Настройка Kubernetes



Приведенные консольные команды выполняются на РЕД ОС. Если вы используете другой дистрибутив Linux, рекомендуется обратиться к официальной документации вашего дистрибутива.

Настройка сервиса Vector

Чтобы настроить сбор логов, выполните следующие шаги:

1. Подключитесь по ssh к мастер-машине вашего кластера.
2. Запросите список всех нод вашего кластера с помощью команды `kubectl get nodes`.
3. Установите на каждом узле Kubernetes сервис Vector командой:

```
sudo dnf install epel-release
sudo dnf install vector
```

4. Замените команду запуска в файле `/usr/lib/systemd/system/vector.service` на следующую:

```
[Unit]
Description=Vector
Documentation=https://vector.dev
After=network-online.target
Requires=network-online.target

[Service]
User=<user>
Group=<user>
ExecStartPre=/usr/bin/vector validate
ExecStart=/usr/bin/vector -c /etc/vector/vector.toml
ExecReload=/usr/bin/vector validate
ExecReload=/bin/kill -HUP $MAINPID
Restart=always
AmbientCapabilities=CAP_NET_BIND_SERVICE
EnvironmentFile=-/etc/default/vector
```

```
#Since systemd 229, should be in Unit but in order to support systemd <229,  
#it is also supported to have it here.  
StartLimitInterval=10  
StartLimitBurst=5  
  
[Install]  
WantedBy=multi-user.target
```

Здесь **<user>** — имя пользователя, от имени которого будет работать сервис.

Убедитесь, что учетная запись пользователя **<user>** имеет права на чтение (Read) и запись (Write) для следующих директорий:

- Конфигурационные директории: **/etc/vector/**, **/etc/kubernetes/**.
- Директории хранения файлов и логов: **/var/log/kubernetes/**.
- Директории исполняемых файлов: **/usr/sbin/**, **/usr/bin/**.

По умолчанию данные права доступны только для записи root.

5. Перезагрузите конфигурацию командой:

```
sudo systemctl daemon-reload
```

6. Создайте файл **/etc/vector/vector.toml**.

7. Добавьте в созданный файл конфигурацию следующего вида:

```
# Источник событий kubernetes-hardware  
[sources.kubernetes_logs]  
  type = "kubernetes_logs"  
  self_node_name = "<node_name>"  
  
# Источник событий kube-api  
[sources.audit_policy_log]  
  type = "file"  
  include = [ "/var/log/kubernetes/audit.log" ]  
  
# Цель для отправки логов  
[sinks.vector_siem]  
  type = "vector"  
  inputs = ["kubernetes_logs", "audit_policy_log"]  
  address = "<address>:<port>"
```

Здесь:

- **<node_name>** — имя узла Kubernetes.
- **<address>** — IP-адрес сервера SIEM.

- **<port>** — порт, на который будут отправляться события.

8. Включите новый сервис командой:

```
sudo systemctl enable vector --now
```

9. Проверьте отсутствие ошибок в сервисе Vector командой:

```
sudo systemctl status vector.service
```

10. Проверьте правильность конфигурации следующей командой:

```
vector validate
```

В случае успешного выполнения система выведет сообщение следующего вида:

```
✓ Loaded ["/etc/vector/vector.toml"]
✓ Component configuration
✓ Health check "<vector_siem>"
-----
                          Validated
```

Настройка KubeApi

Для настройки и контроля событий, собираемых сервисом Kubernetes, выполните следующие шаги:

1. Загрузите политику мониторинга kubernetes по [ссылке](#).
2. Разместите ее в директории **/etc/kubernetes/audit-policy.yaml**.
3. Откройте файл **/etc/kubernetes/manifests/kube-apiserver.yaml** для редактирования.
 - а. Добавьте в секцию **spec.containers.command** следующие строки:

```
- --audit-log-path=/var/log/kubernetes/audit.log
- --audit-policy-file=/etc/kubernetes/audit-policy.yaml
```

Конфигурационный файл примет вид:

```
spec:
  containers:
  - command:
    - kube-apiserver
    - --advertise-address=<your-master-node-ip>
    - --allow-privileged=true
    - --anonymous-auth=True
```

...

Здесь `<your-master-node-ip>` — адрес доступной мастер-ноды вашего кластера.

- b. Добавьте два дополнительных пространства в секцию `spec.containers.volumeMounts`:

```
volumeMounts:
  - mountPath: /etc/kubernetes/audit-policy.yaml
    name: audit-policy
    readOnly: true
  - mountPath: /var/log/kube-audit
    name: audit-logs
    readOnly: false
...
```

- c. Добавьте два дополнительных пространства в секцию `spec.containers.volumes`:

```
- hostPath:
  path: /etc/kubernetes/audit-policy.yaml
  type: File
  name: audit-policy
- hostPath:
  path: /var/log/kube-audit
  type: DirectoryOrCreate
  name: audit-logs
```

4. Перезагрузите сервис kubelet на вашей нодe. Для этого используйте команду:

```
systemctl restart kubelet
```



Это необязательное действие, однако kubernetes не поддерживает функции проверки конфигурации для своих kube-api подов.

5. После перезагрузки сервисов выполните команду `kubectl get nodes`. В случае успешного применения политики вы увидите список ваших нод. В случае наличия ошибок будут выведены ошибки вида `Timeout exceeded`.



При использовании версий kubernetes 1.26.3–1.28.1 необходимо, чтобы у пользователя root были следующие права:

- чтение директории `/etc/kubernetes`;
- чтение и запись в директории `/var/log/kubernetes`;
- чтение файла `/etc/kubernetes/audit-policy.yaml`.

Настройка в R-Vision SIEM

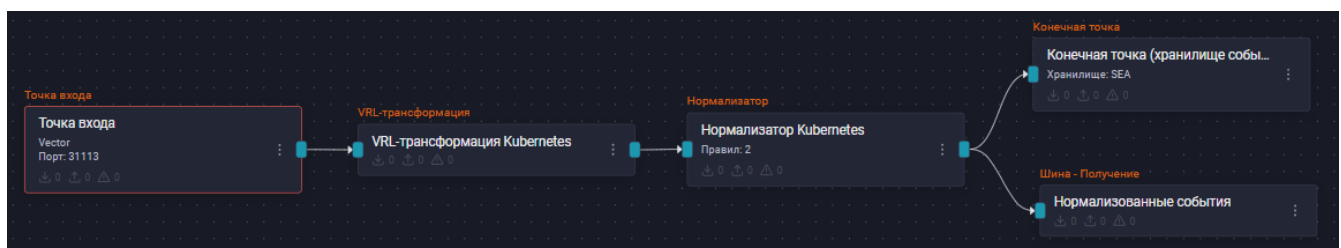
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Vector**.
 - Порт точки входа: введите значение, указанное в конфигурации [сервиса Vector](#).
3. Добавьте VRL-трансформацию:

```
.dproduct = "kubernetes"
```

4. Соедините добавленную точку входа и VRL-трансформацию.
5. Добавьте на конвейер элемент **Нормализатор** с правилами **Kubernetes** (идентификатор правила: **RV-N-53**) и **Kubernetes** (идентификатор правила: **RV-N-54**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Если необходимо отправить события на другой конвейер для дальнейшей обработки, добавьте в коллектор шину, настроенную на получение.
9. Соедините конечную точку и шину с нормализатором.
10. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события Kubernetes.



Найти события Kubernetes в хранилище можно по следующему фильтру:

```
dproduct = "Kubernetes"
```

Добавить фильтр

Инвертировать (NOT)

Поле

dproduct

Оператор

=

Значение

Kubernetes

Настроить заголовок

Отменить

Добавить

Linux

Данный раздел содержит инструкции по сбору событий из журналов Linux различными методами:

- [Linux Auditd](#)
- [Системные журналы Linux](#)

Linux Auditd

Данное руководство описывает процесс отправки событий службы Linux Auditd в R-Vision SIEM.

- [Настройка Auditd](#)
 - [Настройка журналирования Auditd](#)
 - [Отправка событий Auditd](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Настройка Auditd



В настоящем руководстве рассматривается передача событий с помощью службы rsyslog. Предполагается, что rsyslog на станции с ОС Linux уже установлен.

Настройка журналирования Auditd

Журналирование событий службы Auditd определяет, какие события будут регистрироваться в системе. Журналирование событий настраивается с помощью правил. Если у вас уже настроена служба Auditd, пропустите этот пункт и перейдите к [настройке передачи событий](#).

Для настройки журналирования Auditd выполните следующие действия:

1. Проверьте, установлена ли служба Auditd, с помощью команды:

```
auditctl -v
```

- Если служба установлена, на экране отобразится версия установленной службы, например, **auditctl version 3.0.7**.



Если версия установленной службы ниже 2.6, обновите службу согласно рекомендациям производителя ОС.

- Если служба не установлена, на экране отобразится сообщение об ошибке. В этом случае необходимо установить службу с помощью одной из следующих команд:
 - На ОС ALT Linux:

```
apt-get install -y audit audispd-plugins
```

- На ОС Astra Linux, Debian или Ubuntu:

```
apt-get install -y auditd audispd-plugins
```

- На ОС CentOS, Oracle Linux, Red Hat Enterprise Linux или РЕД ОС:

```
yum install -y audit audispd-plugins
```

- На ОС SUSE Linux Enterprise Server:

```
zypper install audit audispd-plugins
```

- На VMware Photon OS:

```
sudo dnf install -y yum  
sudo yum install audit audispd-plugins
```

- На ОС Platform V SberLinux OS Server:

```
rpm install <path_to_audit-*.x86_64.rpm>
```

Здесь `<path_to_audit-*.x86_64.rpm>` — путь к файлу `audit-*.x86_64.rpm`.

Файл `audit-*.x86_64.rpm` нужно скопировать из пакета `./sberlinux-9-for-x86_64-baseos-rpms/Packages/a/audit-*.x86_64.rpm`, который находится в архиве с установщиком Platform V SberLinux OS Server.

2. Запустите и добавьте службу Auditd в автозагрузку с помощью команды:

```
systemctl enable --now auditd.service
```

3. Настройте службу Auditd, применив рекомендованные компанией R-Vision правила Auditd. Для этого:

- а. Скачайте правила [по ссылке](#).
- б. Скопируйте файл **audit.rules** в директорию `/etc/audit/rules.d`.
- в. Перезапустите службу Auditd с помощью команды:

```
systemctl restart auditd.service
```

4. После перезапуска убедитесь, что служба запустилась корректно:

```
systemctl status auditd.service
```

5. Убедитесь в наличии событий в файле `/var/log/audit/audit.log`:

```
tail -f /var/log/audit/audit.log
```

Отправка событий Auditd

Для пересылки логов Auditd по syslog выполните следующие шаги:

1. Убедитесь, что установлен плагин `audispd`. Установка плагина осуществляется в пункте [Настройка журналирования Auditd](#).



Если установка плагина невозможна или нежелательна, можно использовать модуль `imfile rsyslog` для чтения событий из файла `audit.log`. В таком случае нужно вручную указать для параметра **syslogtag** значение **audisp-syslog**.

2. Включите передачу audit по syslog, установив в параметре **active** значение **yes**:
- для auditd версий 3.0 или выше в файле `/etc/audit/plugins.d/syslog.conf`;
 - для auditd версий ниже 3.0 в файле `/etc/audisp/plugins.d/syslog.conf`.
3. Перезапустите службу Auditd с помощью команды:

```
systemctl restart auditd.service
```

4. Создайте правило `/etc/rsyslog.d/40-auditd.conf` со следующим содержимым:

```
if $programname contains 'audisp' or $syslogtag contains 'audisp' then {
    action(type="omfwd" Target="<target>" Port="<port>" Protocol="<protocol>")
    stop
}
```

Здесь:

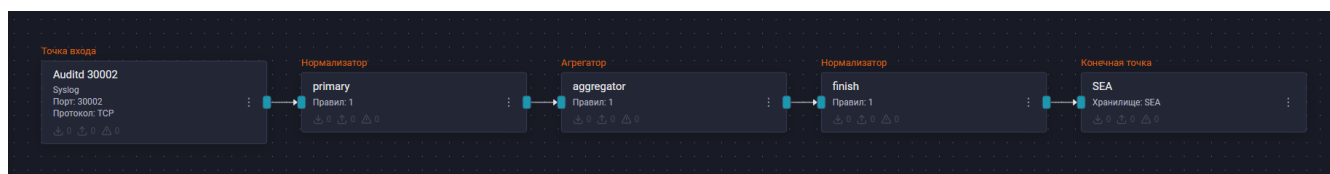
- **<target>** — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
 - **<port>** — порт точки входа Syslog на конвейере SIEM.
 - **<protocol>** — сетевой протокол: **tcp** или **udp**.
5. Перезапустите службу Rsyslog с помощью команды:

```
systemctl restart rsyslog.service
```

Настройка в R-Vision SIEM

1. В интерфейсе R-Vision SIEM в карточке коллектора перейдите на вкладку **Обогащение**.
2. Добавьте таблицу обогащения **AuditEvents_enrichment**.
3. Создайте новый конвейер в данном коллекторе.
4. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Syslog**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [Auditd](#).
 - Протокол: выберите вариант **TCP**.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Linux Auditd** (идентификатор правила: **RV-N-55**).
6. Соедините нормализатор с точкой входа.
7. Добавьте на конвейер элемент **Агрегатор** с правилом **Linux Auditd** (идентификатор правила: **RV-A-1**).
8. Соедините агрегатор с нормализатором.
9. Добавьте на конвейер элемент **Нормализатор** с правилом **Linux Auditd** (идентификатор правила: **RV-N-56**).
10. Соедините второй нормализатор с агрегатором.
11. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
12. Соедините конечную точку со вторым нормализатором.
13. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события Auditd.



Найти события источника в хранилище можно по следующему фильтру:

```
dproduct = "Auditd"
```

Поиск

Хранилище событий: SEA

↑

↺

📄

🔍

Введите запрос и нажмите кнопку Поиск

🗑

5

— +

минут

Поиск

✕ Сбросить все

▼ dproduct = Auditd

+ Добавить фильтр

Совпадений 47587

Интервал времени: 2025-04-04T09:07:47.430+03:00 - 2025-04-04T09:12:47.430+03:00

Показать график ▼

Данные

Статистика

timestamp	dvendor	dproduct	name	dvc	msg
2025-04-04T09:11:55.000+...	Linux	Auditd			Выполнена команда k3s...
2025-04-04T09:11:55.000+...	Linux	Auditd			Выполнена команда k3s...
2025-04-04T09:11:55.000+...	Linux	Auditd			Выполнена команда k3s...
2025-04-04T09:11:55.000+...	Linux	Auditd			Выполнена команда k3s...
2025-04-04T09:11:55.000+...	Linux	Auditd			Выполнена команда k3s...
2025-04-04T09:11:54.000+...	Linux	Auditd			Объектные системные...
2025-04-04T09:11:54.000+...	Linux	Auditd			Выполнена команда...
2025-04-04T09:11:54.000+...	Linux	Auditd			Объектные системные...
2025-04-04T09:11:54.000+...	Linux	Auditd			Выполнена команда...
2025-04-04T09:11:54.000+...	Linux	Auditd			Выполнена...

« < 1 > » 50

Показывается первых записей: 500

⌚ 00:04.895 ↺

● Автообновление

Детали события 649bf7c0-5405-4fa...

duid

0

dvchost

arm88

dvcpid

3595195

externalid

1730797960.048:176703328

fileid

0

filePath

/etc/resolv.conf

filePermission

r

fname

/etc/resolv.conf

msg

Выполнена команда k3s server, Тип системного вызова openat

outcome

success

rt

2024-11-05T12:12:40.000+03:00

sourceServiceName

Syslog

spid

3595195

suid

-1

suser

unset

cs2

docker

cs2Label

key

cs3

a0=ffffffffffff9c a1=c013b9fd70 a2=80000

cs3Label

syscall arguments

cs4

openat

cs4Label

SYSCALL

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Системные журналы Linux

Данное руководство описывает процесс отправки событий из журналов ОС семейства Linux в R-Vision SIEM с помощью продукта R-Vision Endpoint.

Здесь и далее под **ОС Linux** подразумевается любой современный дистрибутив операционной системы на базе ядра Linux.

- [Настройка ОС Linux](#)
 - [Установка агента](#)
 - [Настройка политики](#)
 - [Создание новой группы](#)
 - [Добавление узла в группу](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Настройка ОС Linux

Настройка сбора событий ОС Linux с помощью продукта R-Vision Endpoint включает [установку агента R-Vision Endpoint](#) на конечное устройство и [конфигурирование политики](#).

177

Установка агента



Для установки агента обратитесь к [документации продукта R-Vision Endpoint](#).

После установки агента на станцию и настройки его связи с менеджером R-Vision Endpoint в веб-интерфейсе управления менеджера R-Vision Endpoint появится информация о подключенной станции.

По умолчанию добавленный хост входит в группу **default**.

Агенты					
+ Создать группу					
☐	Имя	Статус	Группа	IP-адрес	Тех. аудит
☐	ipa01.sea.local	●	default	10.150.50.77	117 / 152 / 25
☐	ipa01.sea.local	●	default	10.150.10.110	102 / 118 / 19
☐	ki15.sea.land	●	default	172.18.0.1 172.17.0.1...	120 / 183 / 23
☐	arm31.sea.land	●	default Windows	10.150.50.20	0 / 0 / 0
☐	ki06	●	default	172.18.0.1 172.17.0.1...	114 / 163 / 49

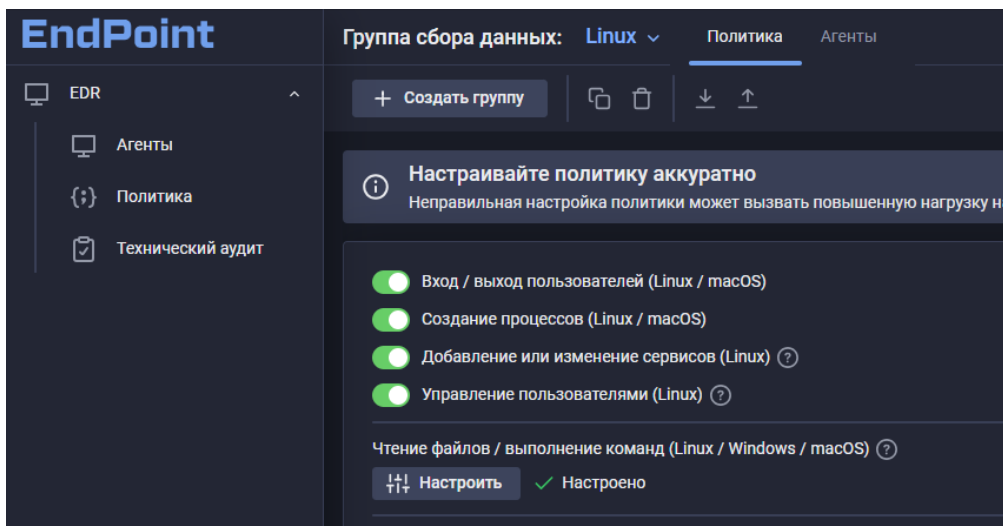
Настройка политики

Для сбора событий с узлов ОС Linux необходимо [создать новую группу](#) и [добавить в нее узел под управлением ОС Linux](#).

Создание новой группы

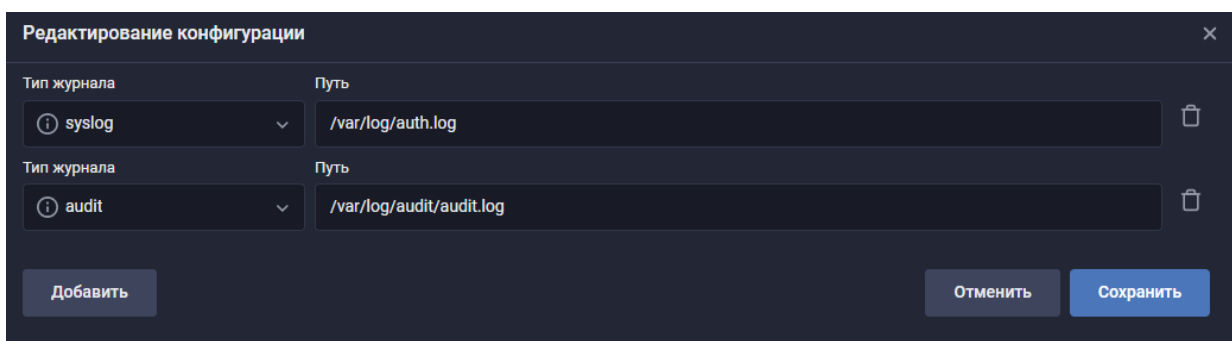
Для создания новой группы:

1. В главном меню R-Vision Endpoint перейдите в раздел **Политика**.
2. Нажмите на кнопку **Создать группу** (**+**) и введите название группы.
3. Из выпадающего списка **Группа сбора данных** выберите созданную группу.
4. Переведите следующие переключатели в активное положение:
 - **Вход/выход пользователей (Linux / macOS)**;
 - **Создание процессов (Linux / macOS)**;
 - **Добавление или изменение сервисов (Linux)**;
 - **Управление пользователями (Linux)**.



5. Если требуется подключение журналов ОС, выполните следующие действия:

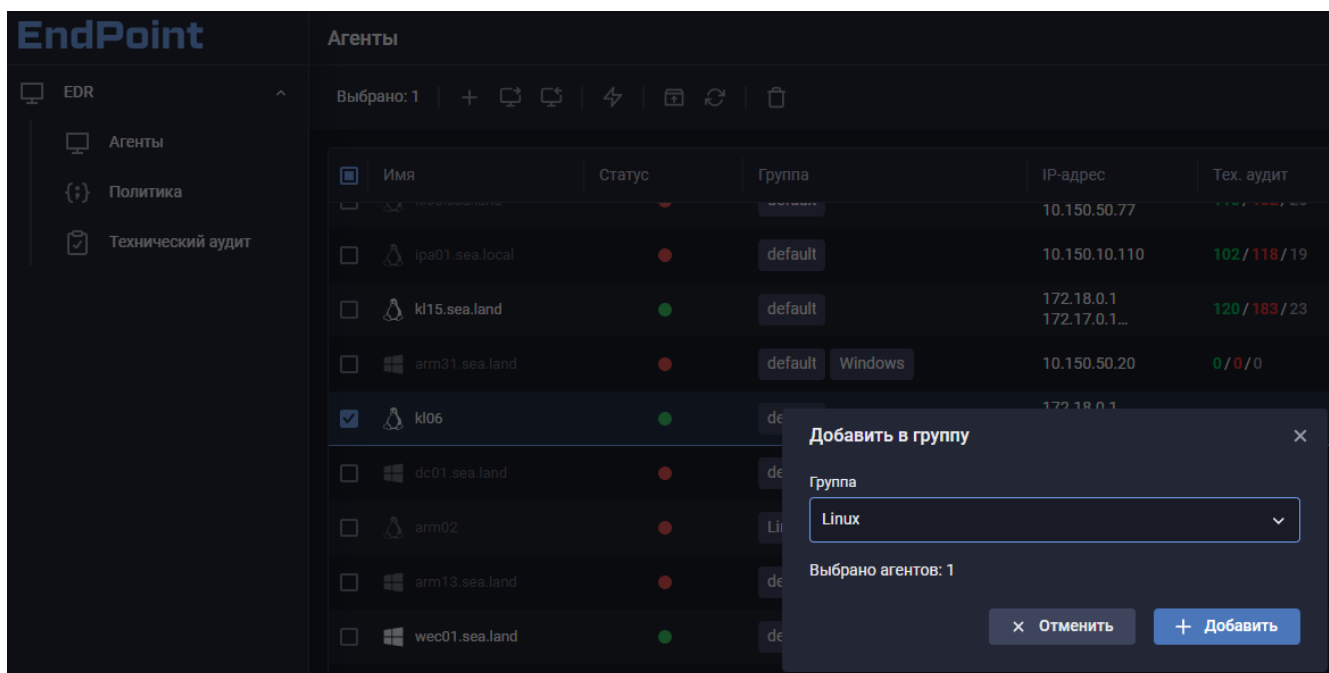
- В разделе **Чтение файлов/выполнение команд** нажмите на кнопку **Настроить**.
- Выберите из выпадающего списка тип журнала **syslog** для любых журналов, которые создает служба syslog на хосте.
- Выберите из выпадающего списка тип журнала **auditd**, если формат записей в журнале соответствует формату журнала audit.log службы Auditd.
- Нажмите на кнопку **Сохранить**.



Добавление узла в группу

Для добавления узла под управлением ОС Linux в созданную группу:

- В главном меню перейдите в раздел **Агенты**.
- Выберите нужный узел и нажмите на кнопку  на панели инструментов.
- Выберите ранее созданную группу и нажмите на кнопку **Добавить** (+).
- Дождитесь применения политики на агенте.



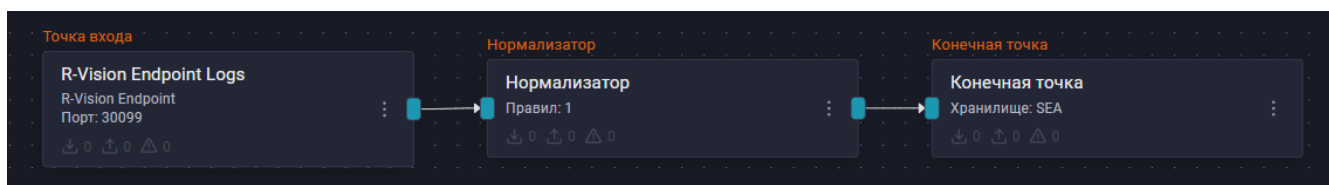
Настройка в R-Vision SIEM



Для настройки интеграции продуктов R-Vision SIEM и R-Vision Endpoint обратитесь к [документации продукта R-Vision SIEM](#).

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **R-Vision Endpoint**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [OC Linux](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Linux Rpoint** (идентификатор правила: **RV-N-57**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки политики сбора и передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события хоста под управлением OC Linux.



Найти события хоста под управлением OC Linux в хранилище можно по

следующему фильтру:

```
dvendor = "Linux"
```

Добавить фильтр

☐ Инvertировать (NOT)

Поле

dvendor

Оператор

=

Значение

Linux

☐ Настроить заголовок

Отменить

Добавить

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Microsoft

Данный раздел содержит список систем для настройки от компании Microsoft:

- [ADDS](#)
- [ADWS](#)
- [IIS](#)
- [SQL Server](#)
- [Windows Sysmon](#)

ADDS

Данное руководство описывает процесс настройки сбора и отправки событий Microsoft ADDS (Active Directory Domain Services) в R-Vision SIEM.

- [Настройка Microsoft ADDS](#)
 - [Настройка журналирования Microsoft ADDS](#)
 - [Настройка в R-Vision Endpoint](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Настройка Microsoft ADDS

В настоящем руководстве рассматривается передача событий с помощью продукта R-Vision Endpoint.

Для настройки передачи событий выполните следующие шаги:

1. [Настройка журналирования Microsoft ADDS](#)
2. [Настройка в R-Vision Endpoint](#)

Настройка журналирования Microsoft ADDS

Чтобы настроить журналирование, включите логирование событий Microsoft через редактирование реестра, для этого:

1. Используйте комбинацию клавиш WIN+R.
2. В открывшемся окне введите команду **regedit** и нажмите на кнопку **OK**.
3. В дереве навигации перейдите по пути **Computer\ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics**.
4. Укажите следующие значения для полей **15 Field Engineering, 15 LDAP Interface Events, 16 LDAP Interface Events, 8 Directory Access**:
 - Value Data: 5.
 - Base: Hexadecimal.

NetPipeActivator	10 Performance Counters	REG_DWORD	0x00000000 (0)
netprofm	11 Initialization/Termination	REG_DWORD	0x00000000 (0)
NetSetupSvc	12 Service Control	REG_DWORD	0x00000000 (0)
NetTcpActivator	13 Name Resolution	REG_DWORD	0x00000000 (0)
NetTcpPortSharing	14 Backup	REG_DWORD	0x00000000 (0)
netvsc	15 Field Engineering	REG_DWORD	0x00000005 (5)
netvscvfp	15 LDAP Interface Events	REG_DWORD	0x00000005 (5)
NgcCtnrSvc	16 LDAP Interface Events	REG_DWORD	0x00000005 (5)
NgcSvc	17 Setup	REG_DWORD	0x00000000 (0)
NlaSvc	18 Global Catalog	REG_DWORD	0x00000000 (0)
nnjwfgod	19 Inter-site Messaging	REG_DWORD	0x00000000 (0)
npcap	2 Security Events	REG_DWORD	0x00000000 (0)
npcap_wifi	20 Group Caching	REG_DWORD	0x00000000 (0)
Npfs	21 Linked-Value Replication	REG_DWORD	0x00000000 (0)
npsvctrig	22 DS RPC Client	REG_DWORD	0x00000000 (0)
nsi	23 DC RPC Server	REG_DWORD	0x00000005 (5)
nsiproxy	23 DS RPC Server	REG_DWORD	0x00000000 (0)
NTDS	24 DS Schema	REG_DWORD	0x00000000 (0)
Diagnostics	25 Transformation Engine	REG_DWORD	0x00000000 (0)
Parameters	26 Claims-Based Access Control	REG_DWORD	0x00000000 (0)
Performance	3 ExDS Interface Events	REG_DWORD	0x00000000 (0)
RID Values	4 MAPI Interface Events	REG_DWORD	0x00000000 (0)
Security	5 Replication Events	REG_DWORD	0x00000000 (0)
NtFrs	6 Garbage Collection	REG_DWORD	0x00000000 (0)
Ntfs	7 Internal Configuration	REG_DWORD	0x00000000 (0)
Null	8 Directory Access	REG_DWORD	0x00000005 (5)
nvdimm	9 Internal Processing	REG_DWORD	0x00000000 (0)
nvraid			
nvstor			

Edit DWORD (32-bit) Value [X]

Value name:
15 Field Engineering

Value data:
5

Base
☒ Hexadecimal
☐ Decimal

OK Cancel

5. Установите на узле агент R-Vision Endpoint. Инструкции по работе с агентами R-Vision Endpoint [представлены по ссылке](#).



Посмотреть логируемые события можно в **Event Viewer\Windows Logs\Applications and Services Logs\Directory Service**.

Настройка в R-Vision Endpoint

Для настройки передачи событий в R-Vision Endpoint:

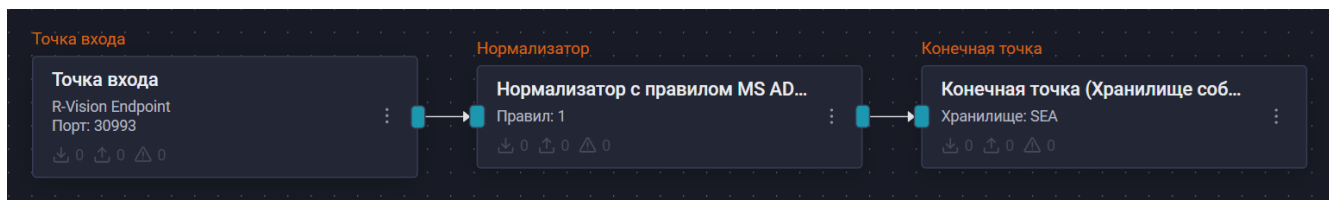
1. В веб-интерфейсе управления R-Vision Endpoint создайте группу, нажав на кнопку **Создать группу** (+) в разделе **Агенты**.
2. Введите имя группы и нажмите на кнопку **Создать** (+).
3. Добавьте **узел**, на котором установлен агент, для этого:
 - a. Перейдите в раздел **Агенты**.
 - b. Установите флажок напротив нужного вам хоста.
 - c. Нажмите на кнопку .
 - d. Выберите созданную ранее группу в выпадающем списке и нажмите на кнопку **Добавить** (+).
4. Перейдите в раздел **Политика**.
5. В секции **Чтение файлов/выполнение команд** нажмите на кнопку **Настроить** (.
6. Нажмите на кнопку **Добавить** (+).
7. В выпадающем списке **Тип журнала** выберите вариант **eventchannel**, а в поле **Путь** введите "Directory Service".
8. Нажмите на кнопку **Сохранить** () в окне редактирования конфигурации.
9. Нажмите на кнопку **Сохранить и применить** () в разделе **Политика**.
10. Дождитесь применения политики группы на узле.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **R-Vision Endpoint**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [сервера](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft AD Directory Services** (идентификатор правила: **RV-N-147**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события Microsoft ADDS.

Найти события Microsoft ADDS в хранилище можно по следующему фильтру:

```
dproduct = "Active Directory Domain Services"
```



Изменить фильтр

☐ Инвертировать (NOT)

Поле

dproduct

Оператор

=

Значение

Active Directory Domain Services

☐ Настроить заголовок

Отменить

Сохранить

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

ADWS

Данное руководство содержит инструкции по настройке подключения к системе R-Vision SIEM источника событий ADWS (Active Directory Web Services).

- [Подготовка инфраструктуры](#)
- [Настройка сбора событий источника на стороне R-Vision Endpoint](#)
- [Настройка в R-Vision SIEM](#)

Подготовка инфраструктуры



Microsoft ADWS устанавливается по умолчанию при установке роли ADDS (Active Directory Domain Services). Дополнительная настройка службы не требуется.

Установите агент R-Point на узле, работу которого требуется контролировать.

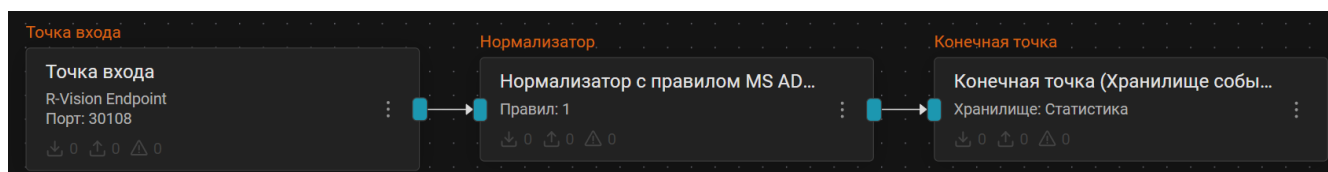
Настройка сбора событий источника на стороне R-Vision Endpoint

1. Выберите в интерфейсе R-Vision Endpoint группу установленных ранее агентов и в секции **Чтение файлов/выполнение команд** нажмите на кнопку **Добавить** (+).
2. В выпадающем списке **Тип журнала** выберите вариант **eventchannel**.
3. В поле **Путь** введите значение **ADWS**.
4. Нажмите на кнопку **Сохранить и применить**.

Настройка в R-Vision SIEM

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **R-Vision Endpoint**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне сервера.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft Active Directory Web Services** (идентификатор правила: **RV-N-58**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

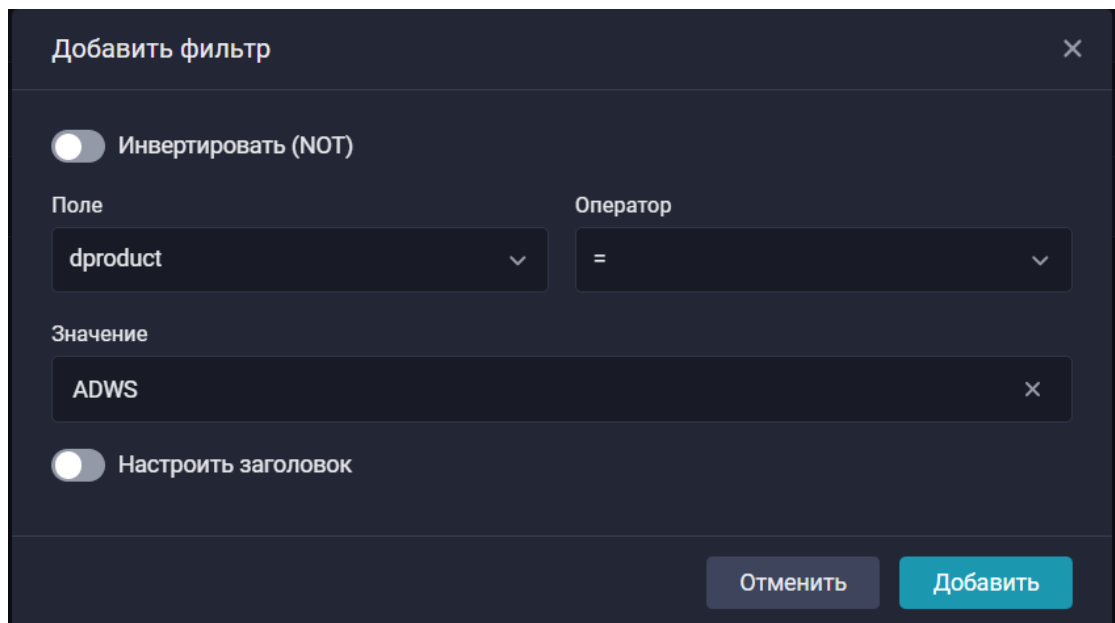


Если настройка выполнена корректно, в хранилище начнут поступать события журнала ADWS.

Найти события ADWS в хранилище можно по следующему фильтру:

```
dproduct = "ADWS"
```





IIS

Данное руководство описывает процесс настройки сбора событий Microsoft IIS (Internet Information Services) и их отправки в R-Vision SIEM.

- [Настройка Microsoft IIS](#)
 - [Настройка журналирования Microsoft IIS](#)
 - [Настройка отправки событий в R-Vision Endpoint](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Настройка Microsoft IIS

Настройка журналирования Microsoft IIS



В настоящем руководстве рассматривается передача событий с помощью продукта R-Vision Endpoint.

Включите логирование событий Microsoft через Event Viewer:

1. В дереве навигации перейдите по пути **Microsoft** → **Windows** → **IIS Logging** → **Logs**.
2. Чтобы настроить журналирование, выполните команду **Enable Log** в контекстном меню.
3. Установите на узле [агент R-Vision Endpoint](#).

Настройка отправки событий в R-Vision Endpoint

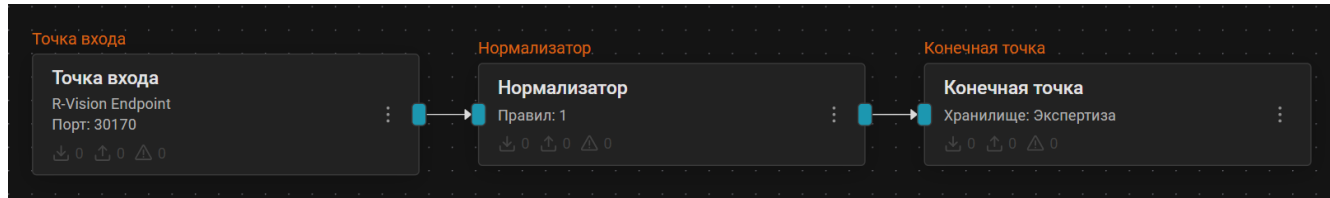
1. В веб-интерфейсе управления R-Vision Endpoint создайте группу и добавьте в нее [узел](#), на котором установлен агент.
2. В созданной группе узлов в секции **Чтение файлов/выполнение команд** нажмите на кнопку **Добавить**.

3. В выпадающем списке **Тип журнала** выберите вариант **eventchannel**.
4. В поле **Путь** введите значение **Microsoft-Windows-IIS-Logging/Logs**.
5. Нажмите на кнопку **Сохранить и применить**.
6. Дождитесь применения политики группы на узле. Сбор событий настроен.

Настройка в R-Vision SIEM

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **R-Vision Endpoint**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне сервера.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft IIS** (идентификатор правила: **RV-N-64**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события Microsoft IIS.

Найти события Microsoft IIS в хранилище можно по следующему фильтру:

```
dproduct = "Microsoft-Windows-IIS-Logging"
```



Добавить фильтр

☐ Инвертировать (NOT)

Поле: dproduct Оператор: =

Значение: Microsoft-Windows-IIS-Logging

☐ Настроить заголовок

Отменить Добавить

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

SQL Server

Данное руководство описывает процесс настройки сбора и отправки событий Microsoft SQL Server (MS SQL) в R-Vision SIEM.

- [Предварительные требования](#)
- [Настройка MS SQL](#)
 - [Описание подсистемы журналирования MS SQL](#)
 - [Создание учетной записи в СУБД MS SQL](#)
 - [Настройка аудита MS SQL](#)
 - [Настройка аудита выгрузки ключей и сертификатов MS SQL](#)
 - [Установка агента](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Предварительные требования

- Сетевая доступность сервера СУБД источника по целевому порту и протоколу для каждой ноды кластера SIEM.
- Учетная запись в СУБД с правами на чтение базы данных.

Настройка MS SQL

Описание подсистемы журналирования MS SQL

Журналирование событий источника может осуществляться двумя путями:

1. Запись в журнал событий. Например, события журналов сервера Microsoft SQL Server записываются в журнал Application.



Настройка сбора событий журнала Windows SQL Server с помощью R-Vision Endpoint включает в себя установку агента R-Vision Endpoint на конечной точке и настройку политики.

2. Отдельная настройка журналирования событий. Например, отдельно настраиваются события аудита команд SQL Server.

Создание учетной записи в СУБД MS SQL

Для отправки событий аудита команд создайте сервисную учетную запись в СУБД MS SQL и предоставьте ей права на просмотр всех сеансов на сервере:

```
GRANT VIEW SERVER STATE TO [имя пользователя];
```

Настройка аудита MS SQL

Для настройки аудита на уровне сервера выполните следующие шаги:

1. Откройте SQL Server Management Studio.
2. В боковом меню перейдите в раздел **Security**.
3. Откройте контекстное меню **Audits** и выберите вариант **New Audit...**. Будет создан новый объект аудита SQL Server.
4. Выберите действие, которое будет запущено при сбое журнала аудита:
 - продолжить;
 - остановить операции с базой данных, которые проверяются;
 - завершить работу сервера.
5. В качестве назначения аудита выберите из выпадающего списка вариант **Application Log**.

Audit Properties

Ready

Select a page

- General
- Filter

Script | Help

Audit name: Login

Queue delay (in milliseconds): 1000

On Audit Log Failure:

- ☒ Continue
- ☐ Fail operation
- ☐ Shut down server

Audit destination: Application Log

Path:

Audit File Maximum Limit:

- ☒ Maximum rollover files:
 - ☐ Unlimited
- ☐ Maximum files:
 - Number of files: 0

Maximum file size:

- 0 MB
- ☒ Unlimited
- GB
- TB

☐ Reserve disk space

Connection

MSRC01\REDCHECK

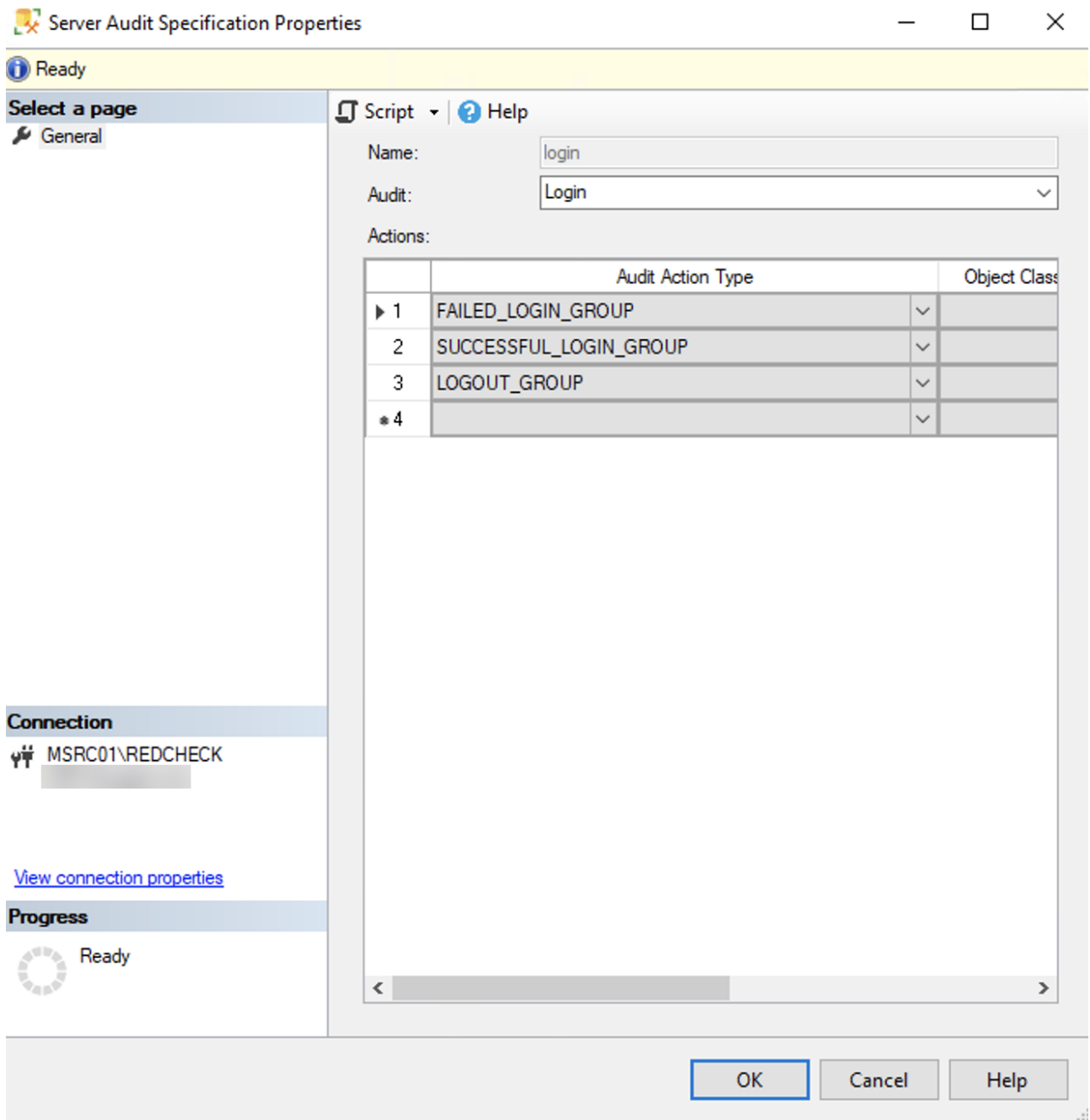
[View connection properties](#)

Progress

Ready

OK Cancel Help

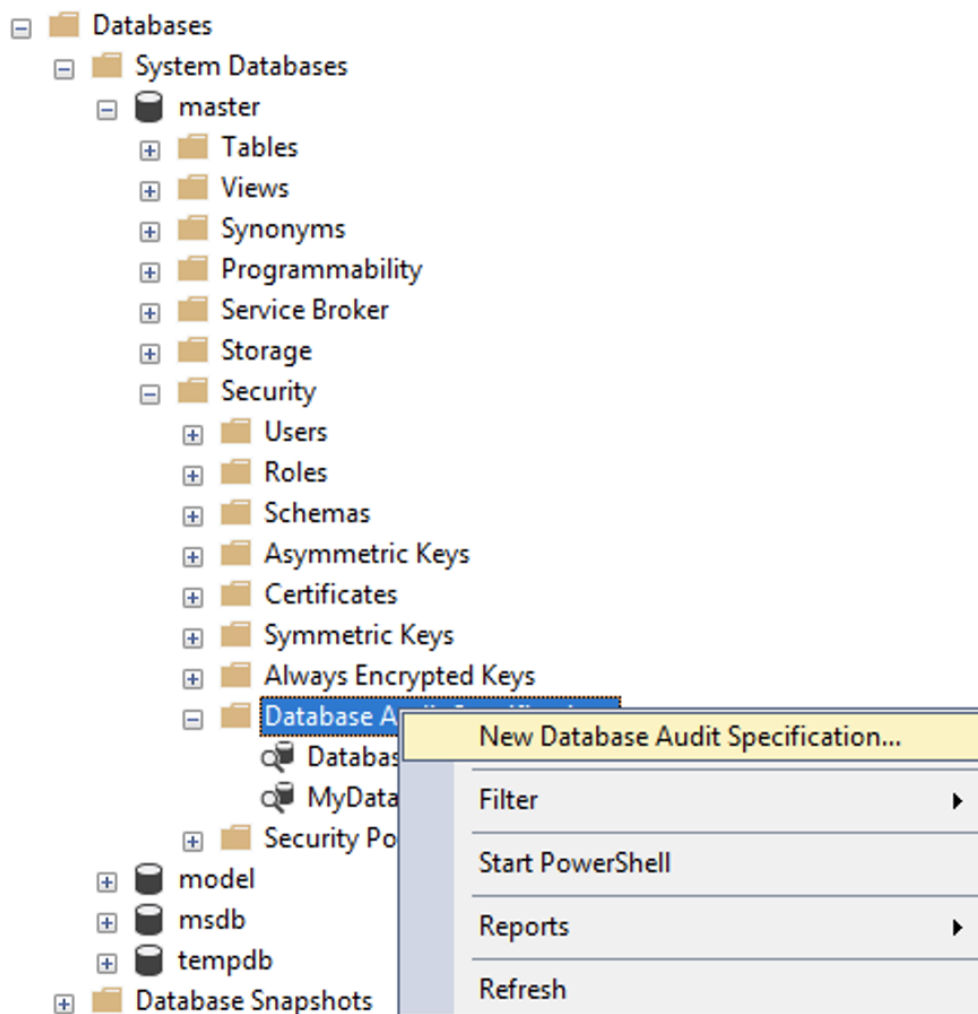
- Нажмите на кнопку **OK**.
- Откройте контекстное меню созданного аудита и выберите вариант **Enable Audit**.
- Откройте контекстное меню **Server Audit Specifications** и выберите вариант **New Server Audit Specification...**. Откроется окно настроек нового объекта спецификации аудита SQL Server.
- Введите название аудита.
- Выберите аудит, созданный на уровне сервера.
- Укажите в таблице типы событий, которые необходимо логировать.



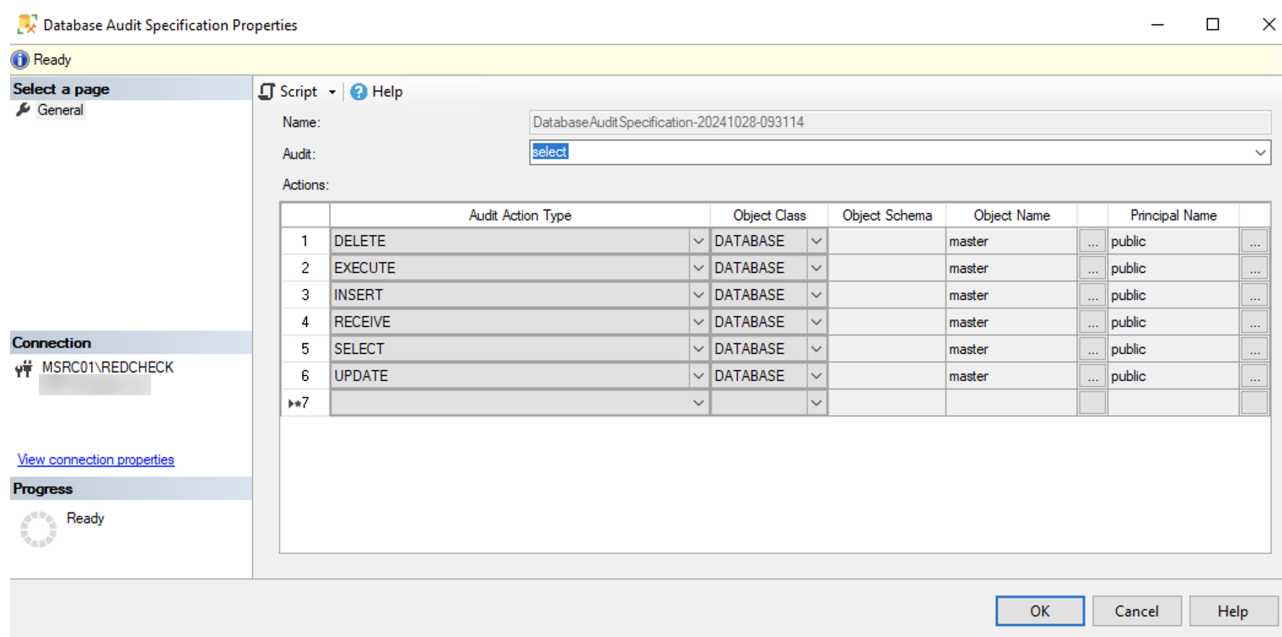
12. Нажмите на кнопку **OK**.

Для настройки аудита на уровне базы данных выполните следующие шаги:

1. Откройте SQL Server Management Studio.
2. Подключитесь к базе данных, для которой необходимо включить аудит.
3. В боковом меню перейдите в раздел **Security** выбранной базы данных.
4. Откройте контекстное меню папки **Database Audit Specifications** и выберите вариант **New Database Audit Specification....** Откроется окно настроек нового объекта аудита SQL Server.



5. Введите имя аудита.
6. Выберите аудит, созданный на уровне сервера.
7. Укажите типы событий, которые необходимо логировать.



8. Нажмите на кнопку **OK**.

Настройка аудита выгрузки ключей и сертификатов MS SQL

Для настройки аудита выгрузки ключей и сертификатов MS SQL выполните следующие шаги:

1. Откройте SQL Server Management Studio.
2. Создайте Extended Events-сессию с логированием в файл:

```
DROP EVENT SESSION IF EXISTS TrackBackupCryptoFile ON SERVER;
GO

CREATE EVENT SESSION TrackBackupCryptoFile
ON SERVER
ADD EVENT sqlserver.sql_statement_completed
(
    ACTION (
        sqlserver.sql_text,
        sqlserver.username,
        sqlserver.client_hostname,
        sqlserver.nt_username
    )
    WHERE
        sqlserver.sql_statement_completed.statement LIKE '%BACKUP%CERTIFICATE%' OR
        sqlserver.sql_statement_completed.statement LIKE
        '%BACKUP%SERVICE%MASTER%KEY%' OR
        sqlserver.sql_statement_completed.statement LIKE '%BACKUP%MASTER%KEY%' OR
        sqlserver.sql_statement_completed.statement LIKE '%BACKUP%SYMMETRIC%KEY%'
)
ADD TARGET package0.event_file
(
    SET filename = 'C:\AuditLogs\TrackBackupCrypto.xel',
    max_file_size = 10,
    max_rollover_files = 5
);
GO

ALTER EVENT SESSION TrackBackupCryptoFile ON SERVER STATE = START;
```

3. Создайте представление для просмотра событий из файла:

```
CREATE VIEW dbo.BackupCryptoAuditLogView AS
SELECT
    event_xml.value('(event/@timestamp)[1]', 'datetime') AS EventTime,
    ISNULL(event_xml.value('(event/action[@name="username"])/value)[1]',
    'nvarchar(100)'), 'N/A') AS SqlLogin,
    ISNULL(event_xml.value('(event/action[@name="client_hostname"])/value)[1]',
    'nvarchar(100)'), 'N/A') AS HostName,
    ISNULL(event_xml.value('(event/action[@name="nt_username"])/value)[1]',
    'nvarchar(100)'), 'N/A') AS WindowsUser,
    ISNULL(event_xml.value('(event/data[@name="statement"])/value)[1]',
```

```
'nvarchar(max)'), 'N/A') AS Statement,
      ISNULL(event_xml.value('(event/action[@name="sql_text"]/value)[1]',
'nvarchar(max)'), 'N/A') AS FullSQL
FROM sys.fn_xe_file_target_read_file('C:\AuditLogs\TrackBackupCrypto*.xel', NULL,
NULL, NULL) AS xelog
CROSS APPLY (SELECT CAST(xelog.event_data AS XML) AS event_xml) AS evt;
GO
```

4. Настройте автозапуск при старте SQL Server:

```
-- Создаем процедуру автозапуска
CREATE PROCEDURE StartTrackBackupCrypto
AS
BEGIN
    IF NOT EXISTS (
        SELECT * FROM sys.dm_xe_sessions WHERE name = 'TrackBackupCryptoFile'
    )
    BEGIN
        ALTER EVENT SESSION TrackBackupCryptoFile ON SERVER STATE = START;
    END
END;
GO

-- Включаем запуск при старте SQL Server
EXEC sp_procoption 'StartTrackBackupCrypto', 'startup', 'on';
```

5. Предоставьте необходимые права для просмотра представления сервисной учетной записи, созданной ранее:

```
GRANT SELECT ON dbo.BackupCryptoAuditLogView TO [имя пользователя];
EXEC sp_addrolemember 'db_datareader', [имя пользователя];
EXEC sp_addsrvrolemember 'VIEW SERVER STATE', [имя пользователя];
```

Установка агента



Для установки агента обратитесь к [документации продукта R-Vision Endpoint](#).

Установите агент на станцию и настройте его связь с менеджером R-Vision Endpoint. После этого в веб-интерфейсе управления менеджера R-Vision Endpoint появится информация о подключенном хосте.

По умолчанию добавленный хост находится в группе **default**. Добавьте его в группу, в которой настроен сбор журнала Application.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:

- a. Перейдите в разделы **Ресурсы** → **Секреты** → **Создать**:
- b. В раскрывшемся окне создания секрета заполните поля:
 - Название: введите название секрета.
 - Описание (опционально): опишите, для чего будет использоваться секрет.
 - Тип секрета: выберите вариант **Строка подключения**.
 - Строка подключения — введите строку вида:

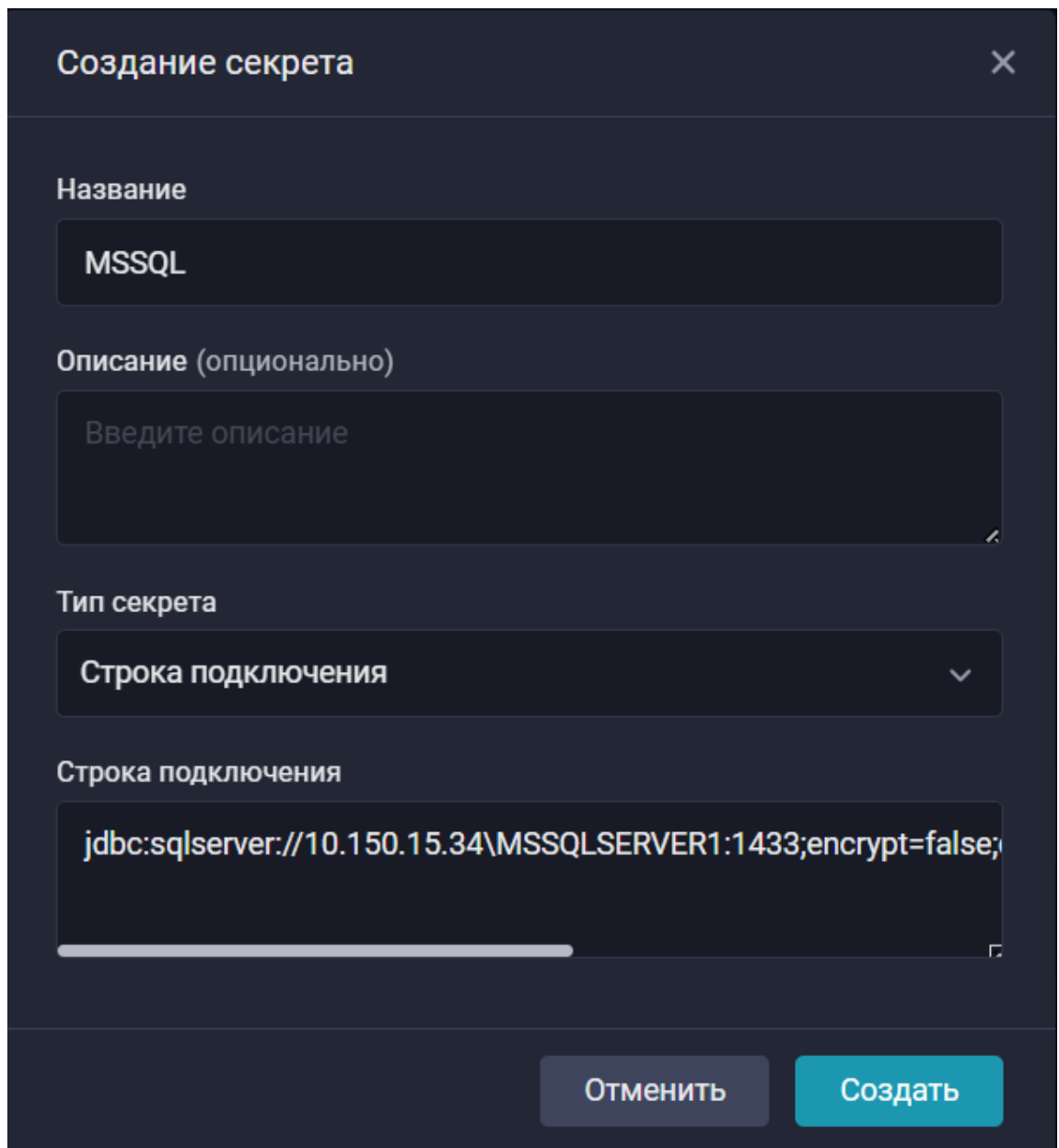
```
jdbc:sqlserver://<address>\<instance>:<port>;encrypt=false;databaseName=<database>;user=<user>&password=<password>
```

где:

- **<address>** — адрес сервера базы данных.
- **<instance>** — сущность сервера СУБД.
- **<port>** — порт подключения.
- **<database>** — имя базы событий аудита.
- **<user>** — логин пользователя базы данных.
- **<password>** — пароль пользователя базы данных.

Пример 3. Пример строки подключения

```
jdbc:sqlserver://10.150.15.34\MSSQLSERVER1:1433;encrypt=false;databaseName=master;user=user;password=P@ssw0rd
```

Создание секрета

Название

MSSQL

Описание (опционально)

Введите описание

Тип секрета

Строка подключения

Строка подключения

jdbc:sqlserver://10.150.15.34\MSSQLSERVER1:1433;encrypt=false;

Отменить Создать

с. Нажмите на кнопку **Создать**.

- В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
- Добавьте на конвейер элемент **Точка входа** для событий аудита команд MS SQL со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Database**.
 - Драйвер базы данных: выберите вариант **MS SQL**.
 - Адрес подключения: выберите секрет, созданный ранее.
 - SQL-запрос — введите запрос вида:

```
DECLARE @appname NVARCHAR(15);  
  
SET @appname = N'MSSQL';  
  
SELECT c.session_id,
```

```

@@SERVERNAME as dvchost,
s.login_name,
s.status,
st.text as query,
s.login_time,
s.program_name,
s.last_request_start_time as rt,
c.auth_scheme,
s.host_process_id,
s.nt_domain,
s.nt_user_name,
s.host_name as shost,
c.client_net_address as src,
c.client_tcp_port as spt,
c.local_net_address as dst,
c.local_tcp_port as dpt,
@appname as appname
FROM sys.dm_exec_connections c
INNER JOIN sys.dm_exec_sessions s
ON c.session_id = s.session_id
CROSS APPLY sys.dm_exec_sql_text(most_recent_sql_handle) AS st
WHERE (DATEDIFF(second,{d '1970-01-01'},
s.last_request_start_time) >= DATEDIFF(second,{d '1970-01-01'}, DATEADD(SECOND,
-15, GetDate())));

```

- Интервал запроса, секунд: введите значение **15**.
4. Добавьте на конвейер дополнительный элемент **Точка входа** для событий выгрузки ключей и сертификатов со следующими параметрами:
- Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Database**.
 - Драйвер базы данных: выберите вариант **MS SQL**.
 - Адрес подключения: выберите секрет, созданный ранее.
 - SQL-запрос — введите запрос вида:

```

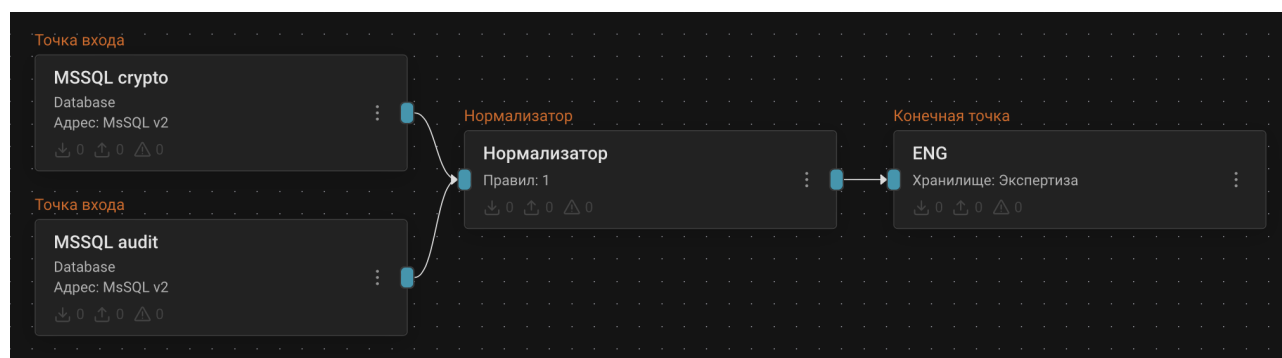
DECLARE @dproduct NVARCHAR(15);
DECLARE @appname NVARCHAR(15);
SET @dproduct = N'SQL Server Crypto';
SET @appname = N'MSSQL'

SELECT * FROM dbo.BackupCryptoAuditLogView,
@dproduct AS device_product,
@appname as appname,
@@SERVERNAME as dvchost,
WHERE EventTime > DATEADD(S, CONVERT(INT, ?)+1, '1970-01-01')
ORDER BY EventTime ASC;

```

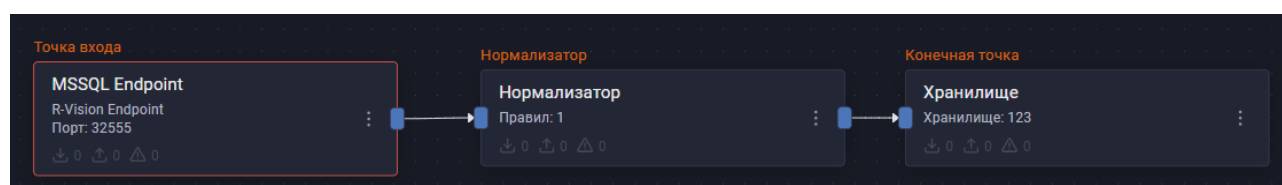
- Поле идентификатора: введите ключ **EventTime** со значением текущего времени в формате UNIX-time.
 - Интервал запроса, секунд: введите значение **15**.
- Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft SQL Server** (идентификатор правила: **RV-N-69**).
 - Соедините нормализатор с точками входа.
 - Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
 - Соедините конечную точку с нормализатором.
 - Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



- Нормализацию событий из других журналов, которые собираются через Endpoint, настройте на конвейере, отвечающем за нормализацию событий Endpoint. Для этого:
- В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
- Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **R-Vision Endpoint**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [Microsoft SQL Server](#).
- Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft SQL Server** (идентификатор правила: **RV-N-70**).
- Соедините нормализатор с точкой входа.
- Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
- Соедините конечную точку с нормализатором.
- Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события из журналов SQL Server.

Найти события источника в хранилище можно по фильтру:

```
dproduct = "SQL Server"
```



The screenshot shows the R-Vision SIEM interface. At the top, a filter bar displays 'dproduct = SQL Server' and a button to 'Добавить фильтр'. Below this, a summary bar indicates 167 matches and a time interval from 2025-05-19T13:48:35.332+03:00 to 2025-05-19T13:58:35.332+03:00. The main area contains a table of events with columns: timestamp, dvendor, dproduct, name, and dvc. The table lists several 'Выполнение SQL запроса' (SQL query execution) events from Microsoft. To the right, a 'Детали события' (Event details) panel for event ID 6d9c15f6-eece-4b9... is shown, including fields like timestamp, id, tenantid, collectorid, type, and a detailed description of the SQL query execution.

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Windows Sysmon

Данное руководство описывает процесс отправки событий из журнала Windows Sysmon в R-Vision SIEM с помощью продукта R-Vision Endpoint.

- [Настройка ОС Windows](#)
 - [Установка службы Sysmon](#)
 - [Установка агента](#)
 - [Настройка политики](#)
 - [Создание новой группы](#)
 - [Добавление узла в группу](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Настройка ОС Windows

Настройка сбора событий журнала Windows Sysmon с помощью R-Vision Endpoint включает в себя:

- [установку службы Sysmon](#);
- [установку агента R-Vision Endpoint](#) на конечную точку;
- [настройку политики](#).

Установка службы Sysmon

Для мониторинга событий с помощью сервиса Sysmon вам необходимо распространить сервис Sysmon на все машины, с которых вы планируете собирать данные. Для этого:

1. Загрузите архив с сервисом Sysmon. Последняя версия сервиса доступна на [официальном сайте Microsoft](#).
2. Загрузите политику мониторинга. Политику мониторинга можно найти по [ссылке](#).
3. Сконфигурируйте пути Sysmon в вашей операционной системе. Планируемая к использованию учетная запись должна иметь доступ к исполняемому файлу Sysmon.exe и к политике мониторинга.
4. Разместите файлы на вашем файловом сервере по планируемому пути.
5. Измените пути в следующем Powershell-скрипте. Назовите его sysmon.ps1.

```
$sysmon = C:\Windows\Sysmon64.exe -s | select-string "System Monitor v"

# Путь к ранее скачанному и распакованному приложению Sysmon, расположенному на
файловом сервере:
$sysmonsource = '\\<FS-name>\Sysmon\Sysmon64.exe'

# Путь к вашему файлу с политикой мониторинга, расположенному на файловом сервере:
$sysmonconfig = '\\<FS-name>\Sysmon\monitoring.xml'

# Строка, указывающая версию вашего ПО (опционально):
$sysmonstring = 'System Monitor <Версия Sysmon> - System activity monitor'

# Путь на вашей машине, по которому вы планируете устанавливать сервис Sysmon:
$filePath = 'C:\Sysmon\Sysmon64.exe'

IF (Test-Path $filePath) {
    IF ($sysmon.ToString() -eq $sysmonstring) {
        & $sysmonsource -c $sysmonconfig
    } ELSE {
        # Uninstall sysmon and re-install new version
        & $filePath -u
        Remove-Item -path $filePath
        & $sysmonsource -i $sysmonconfig -acceptEula
    }
} ELSE {
    & $sysmonsource -i $sysmonconfig -acceptEula
```

```
}
```

Здесь **<FS-name>** — DNS или IP-адрес вашего файлового сервера.

6. В зависимости от используемого типа авторизации и размещения машины в вашей сети, создайте дополнительную групповую или локальную политику.

- Создайте задачу по расписанию. Для этого:

- Настройте триггер:

- Выберите из выпадающего списка **Begin the task** опцию **On a schedule**.
- Задайте расписание для выполнения задачи.

Пример

расписания:

Edit Trigger [X]

Begin the task: **On a schedule**

Settings

☐ One time
☐ Daily
☒ Weekly
☐ Monthly

Start: 30.03.2023 12:35:01 ☐ Synchronize across time zones

Recur every: 1 weeks on:

☐ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday
☐ Thursday ☒ Friday ☐ Saturday

Advanced settings

☐ Delay task for up to (random delay): 1 hour

☐ Repeat task every: 1 hour for a duration of: 1 day
☐ Stop all running tasks at end of repetition duration

☐ Stop task if it runs longer than: 3 days

☐ Expire: 04.06.2026 13:34:58 ☐ Synchronize across time zones

☒ Enabled

OK Cancel

- Нажмите на кнопку **OK**.

- Настройте действие:

- Выберите из выпадающего списка **Action** опцию **Start a program**.
- В поле **Program/script** введите команду для запуска **powershell.exe**.
- В поле **Add arguments (optional)** введите значение **-executionpolicy bypass -file \\<FS-name>\Sysmon\sysmon.ps1**.

Здесь **<FS-name>** — DNS или IP-адрес вашего файлового сервера.

d. Нажмите на кнопку **OK**.

Edit Action [X]

You must specify what action this task will perform.

Action: Start a program [v]

Settings

Program/script: powershell.exe [Browse...]

Add arguments (optional): -executionpolicy bypass

Start in (optional):

[OK] [Cancel]

- В форме **Security options** установите флажок **Run with highest privileges**.

Security options

When running the task, use the following user account:

SYSTEM [Change User or Group...]

☐ Run only when user is logged on

☒ Run whether user is logged on or not

☐ Do not store password. The task will only have access to local computer resources.

☒ Run with highest privileges

☐ Hidden

Configure for: Windows Vista™, Windows Server™ 2008 [v]

[OK] [Cancel]

7. Сохраните изменения.



Для первичной синхронизации политик используйте принудительную синхронизацию с помощью команды **gpupdate /force**.

Установка агента



Для установки агента обратитесь к [документации продукта R-Vision Endpoint](#).

После установки агента на станцию и настройки его связи с менеджером R-Vision Endpoint в веб-интерфейсе управления менеджера R-Vision Endpoint появится информация о подключенной станции.

EndPoint		Агенты					
EDR		+ Создать группу					
Агенты							
{+} Политика							
Технический аудит							
		Имя	Статус	Группа	IP-адрес	Тех. аудит	ОС
		☐ arm18.sea.land	●	default Windows	10.150.50.118 192.168.56.1...	43 / 55 / 210	Microsoft Windows Server 2019 Standard...
		☐ sra01	●	default	10.150.50.90	97 / 144 / 18	Ubuntu 24.04
		☐ kl05.sea.land	●	default	172.17.0.1 10.150.50.77	118 / 182 / 26	Kali GNU/Linux 2022.3
		☐ lpa01.sea.local	●	default	10.150.10.110	102 / 118 / 19	Rocky Linux 9.4
		☐ kl15.sea.land	●	default	172.18.0.1 172.17.0.1...	120 / 183 / 23	Kali GNU/Linux 2022.3
		☐ arm31.sea.land	●	default Windows	10.150.50.20	0 / 0 / 0	Microsoft Windows 10 Enterprise 10.0
		☐ kl06	●	default Linux	172.18.0.1 172.17.0.1...	114 / 163 / 49	Kali GNU/Linux 2023.3
		☐ dc01.sea.land	●	default	10.150.48.10 10.150.49.10...	49 / 54 / 200	Microsoft Windows Server 2016 Standard...

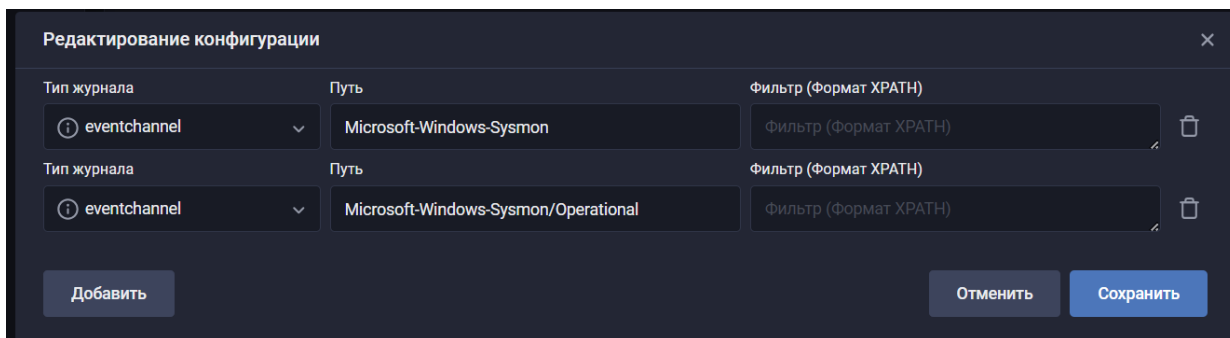
Настройка политики

Для сбора событий журнала Windows Sysmon необходимо [создать новую группу](#) и [добавить в нее узел](#).

Создание новой группы

Для создания новой группы:

1. В главном меню интерфейса R-Vision Endpoint перейдите в раздел **Политика**.
2. Нажмите на кнопку **Создать группу** (+). Откроется окно создания группы.
3. Введите название группы.
4. Выберите из выпадающего списка **Группа сбора данных** созданную группу.
5. Подключите журналы Sysmon, выполнив следующие действия:
 - a. В разделе **Чтение файлов/выполнение команд** нажмите на кнопку **Настроить**.
 - b. Выберите тип журнала **eventchannel** для журналов **Microsoft-Windows-Sysmon** и **Microsoft-Windows-Sysmon/Operational**.
 - c. Нажмите на кнопку **Сохранить**.



Добавление узла в группу

Для добавления узла в созданную группу:

1. В главном меню интерфейса R-Vision Endpoint перейдите в раздел **Агенты**.
2. Выберите нужный узел и нажмите на кнопку  на панели инструментов.
3. Выберите ранее созданную группу и нажмите на кнопку **Добавить**.
4. Дождитесь применения политики на агенте.

Настройка в R-Vision SIEM

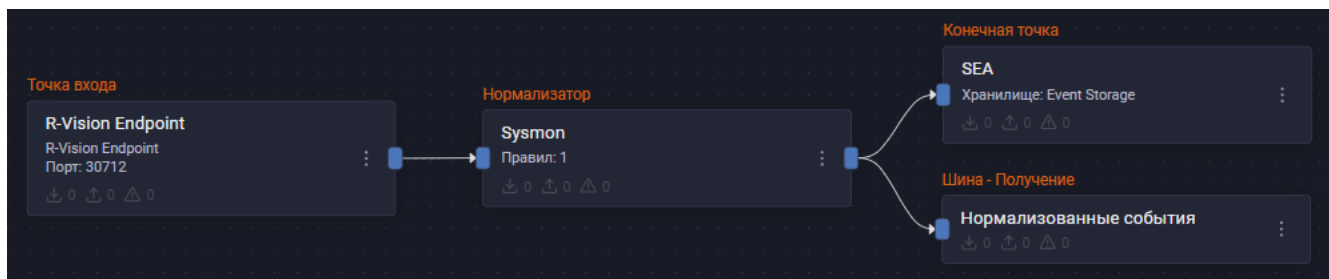


Для настройки интеграции продуктов R-Vision SIEM и R-Vision Endpoint обратитесь к [документации продукта R-Vision SIEM](#).

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **R-Vision Endpoint**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [сервера](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft Windows Sysmon** (идентификатор правила: **RV-N-76**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Добавьте на конвейер элемент **Шина**, настроенный на получение. Он передает нормализованные события для дальнейшей работы с ними.
7. Соедините конечную точку и шину с нормализатором.
8. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки политики сбора и передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события хоста из журнала Windows Sysmon.

Найти события Windows Sysmon в хранилище можно по следующему фильтру:

```
dproduct = "Microsoft-Windows-Sysmon"
```



Добавить фильтр

☐ Инвертировать (NOT)

Поле

Оператор

dproduct
=

Значение

Microsoft-Windows-Sysmon

☐ Настроить заголовок

Отменить
Добавить

Пример поиска события Sysmon с External ID 1:

Поиск
Хранилище событий: SEA
externalId = "1"
10 минут
Поиск

+ Добавить фильтр

Совпадений 8
Интервал времени: 2025-06-27T09:24:10.528+03:00 - 2025-06-27T09:34:10.528+03:00
Показать график

timestamp	dvendor	dproduct	name	dvc	msg	outcome
2025-06-27T09:31:16.000+03...	Microsoft	Microsoft-Windows-Sysmon	Process creation	(Пусто)	The process creation event provides...	success
2025-06-27T09:27:36.000+03...	Microsoft	Microsoft-Windows-Sysmon	Process creation	(Пусто)	The process creation event provides...	success
2025-06-27T09:27:36.000+03...	Microsoft	Microsoft-Windows-Sysmon	Process creation	(Пусто)	The process creation event provides...	success
2025-06-27T09:27:36.000+03...	Microsoft	Microsoft-Windows-Sysmon	Process creation	(Пусто)	The process creation event provides...	success
2025-06-27T09:27:36.000+03...	Microsoft	Microsoft-Windows-Sysmon	Process creation	(Пусто)	The process creation event provides...	success
2025-06-27T09:27:36.000+03...	Microsoft	Microsoft-Windows-Sysmon	Process creation	(Пусто)	The process creation event provides...	success
2025-06-27T09:27:36.000+03...	Microsoft	Microsoft-Windows-Sysmon	Process creation	(Пусто)	The process creation event provides...	success
2025-06-27T09:26:17.000+03...	Microsoft	Microsoft-Windows-Sysmon	Process creation	(Пусто)	The process creation event provides...	success

Детали события 7fa49199-c243-4694-8bda-bb3bfd92baad

Дата и время
timestamp 2025-06-27T09:31:16.000+03:00

Служебные данные
id 7fa49199-c243-4694-8bda-bb3bfd92baad
sourceId 10.150.50.112
tenantId 00000000-0000-0000-0000-000000000000
collectorId 6619a09e-657a-4b13-9e19-ac4942158197
type нормализованное событие

Сведения о событии
dvendor Microsoft
dproduct Microsoft-Windows-Sysmon
dversion 10.0.20348.169
name Process creation
severity INFORMATION
act Process creation
cat process-operation
destinationServiceName C:\Windows\system32\wbem\wmiprvse.exe -secured-Embedding
deviceDirection входящее соединение
dhost arm112.sea.land
dntdom NT AUTHORITY
dnid 10668

Показывается первых записей: 500
00:00.572
Автообновление

Если вам необходимо использовать Sysmon-нормализацию совместно с Windows-Security нормализацией, то правило нормализации **Microsoft Windows Sysmon** (идентификатор правила: **RV-N-76**) необходимо подключить в нормализатор **Global**.

Пример конфигурации конвейера:

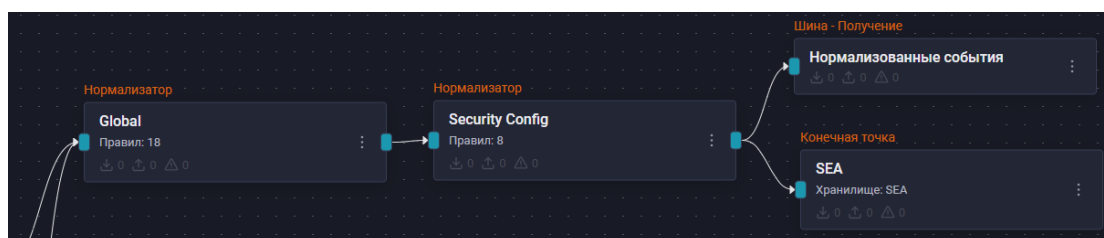


Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

MikroTik

Данный раздел содержит список систем для настройки от компании MikroTik

- [RouterOS](#)

RouterOS

Данное руководство описывает процесс настройки роутеров MikroTik с использованием RouterOS для интеграции с R-Vision SIEM.

- [Настройка MikroTik RouterOS](#)
 - [Настройка роутера MikroTik](#)
 - [Настройка через Winbox](#)
- [Настройка в R-Vision SIEM](#)

Настройка MikroTik RouterOS

Настройка роутера MikroTik

После первичной настройки RouterOS необходимо определить IP-адреса для интерфейса управления (mgmt). В данном руководстве используется интерфейс **ether1**. По умолчанию для входа используются логин **admin** и пустой пароль.

1. Просмотрите все интерфейсы с помощью команды:

```
/interface ethernet print
```

2. Найдите в списке необходимый интерфейс. Установите IP-адрес для интерфейса командой:

```
/ip address add address=192.168.1.1/24 interface=ether1
```

3. Настройте шлюз:

```
/ip route add gateway=192.168.1.254
```

4. Включите SSH-доступ. В зависимости от версии RouterOS используйте одну из следующих команд:

- ```
/ip service set ssh disabled=no
```

- ```
/ip service set ssh enabled=yes
```

5. При необходимости измените порт SSH:

```
/ip service set ssh port=2222
```



В RouterOS 7 все настройки сохраняются в постоянную память автоматически.

Настройка через Winbox

1. Скачайте официальное приложение [Winbox](#). Дальнейшая настройка производится через этот инструмент.
2. Включите необходимые сервисы в меню **IP** → **Services**:

	Name	Port	Available From	VRF	Certificate	TLS Ver...	
	api	8728		main			
	api-ssl	8729		main	none	any	
	ftp	21					
	ssh	22		main			
	telnet	23		main			
	winbox	8291		main			
	www	80		main			
X	www-ssl	443		main	none	any	

8 items

3. Создайте интерфейс сетевого моста. Рекомендуемое время агрегации — не менее 5 минут.

New Interface

General STP VLAN Status Traffic

Name:

Type:

MTU:

Actual MTU:

L2 MTU:

MAC Address:

ARP:

ARP Timeout:

Admin. MAC Address:

Ageing Time:

☐ IGMP Snooping

☐ DHCP Snooping

☒ Fast Forward

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Torch

Reset Traffic Counters

enabled running slave passthrough

4. Установите необходимые настройки VLAN и STP.
5. Настройте WAN и LAN интерфейсы, как показано на скриншоте:

Interface List

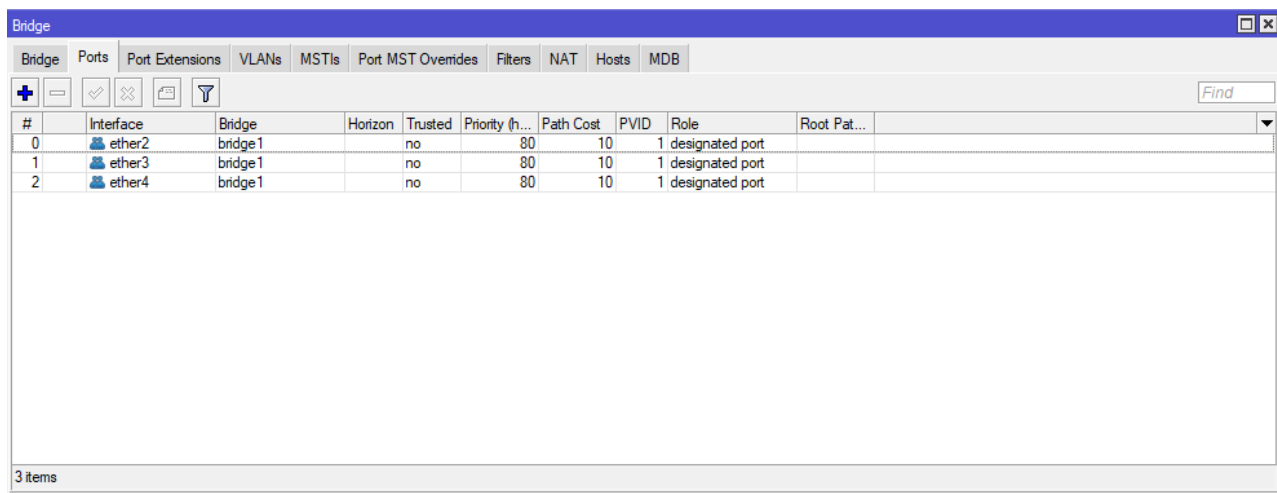
Interface Interface List Ethernet EoIP Tunnel IP Tunnel GRE Tunnel V

+ - ✓ ✗ 📁 🔍 Lists

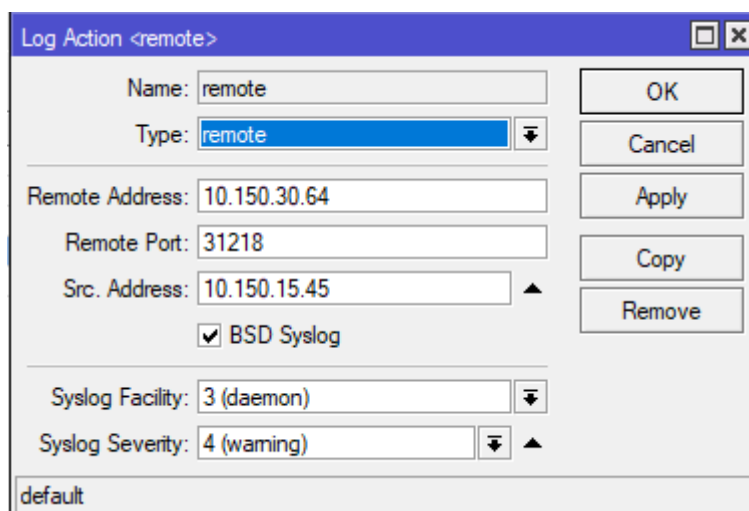
List	Interface
LAN	bridge1
WAN	ether1

2 items (1 selected)

6. Добавьте оставшиеся интерфейсы в **LAN-bridge**:



7. Перейдите в меню **System** → **Logging**.
8. Создайте новое действие в меню **Actions**. В выпадающем списке **Type** выберите вариант **remote**. Укажите адрес рабочего узла SIEM или адрес коллектора логов.



9. Настройте правила отправки логов. Выберите необходимые поля в выпадающем списке и присвойте им созданное действие (Action).

Настройка в R-Vision SIEM

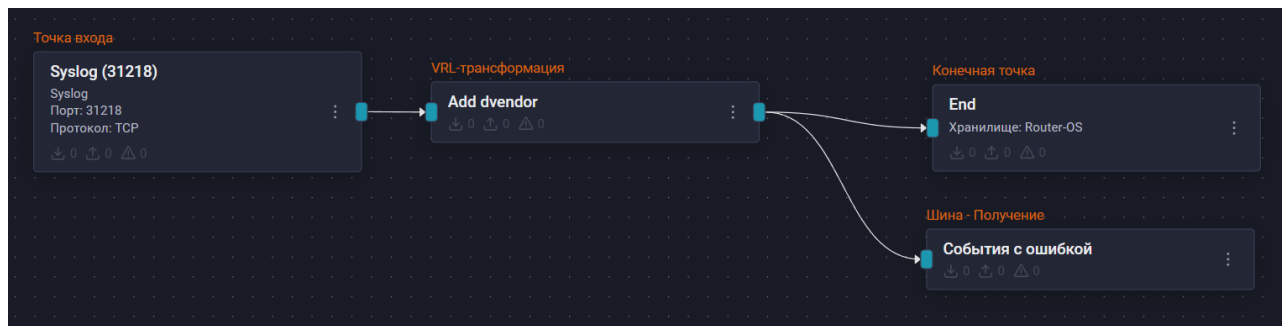
1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Syslog**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне RouterOS.
 - Протокол: выберите вариант в соответствии с настройками на стороне RouterOS.
3. Добавьте на конвейер элемент **VRL-трансформация** со следующим кодом:

```
.dvendor = "MikroTik"
```

4. Соедините добавленную точку входа и VRL-трансформацию.

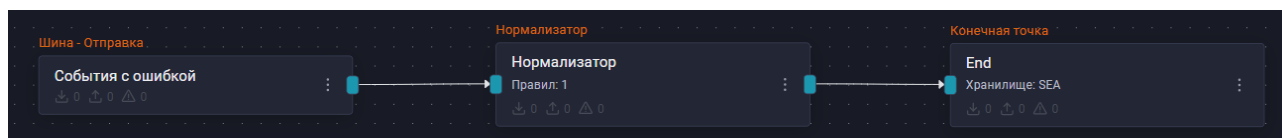
- Добавьте на конвейер элемент **Шина** с типом **Получение**.
- Соедините шину с VRL-трансформацией.
- Если нужно записывать ненормализованные события в базу данных, добавьте элемент **Конечная точка** типа **Хранилище событий** и соедините его с VRL-трансформацией.

Пример конфигурации конвейера:



- Создайте в коллекторе еще один конвейер, в котором будет происходить нормализация событий.
- Добавьте на новый конвейер элемент **Шина** со следующими параметрами:
 - Шина: выберите шину, которая получает события из предыдущего конвейера.
 - Соединение с шиной: выберите вариант **Отправка**.
- Добавьте на конвейер элемент **Нормализатор** с правилом **MikroTik RouterOS** (идентификатор правила: **RV-N-80**).
- Соедините нормализатор с шиной.
- Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
- Соедините конечную точку с нормализатором.

Пример конфигурации конвейера:



- Сохраните и установите конфигурацию конвейеров.

Все события RouterOS будут нормализовываться согласно модели события.

Найти события RouterOS в хранилище можно по следующему фильтру:

```
dproduct = "Router OS"
```



Добавить фильтр

Инвертировать (NOT)

Поле

dproduct

▼

Оператор

=

▼

Значение

Router OS

×

Настроить заголовок

Отменить

Добавить

Nextcloud

Данное руководство описывает процесс настройки сбора и отправки событий Nextcloud в R-Vision SIEM.

Настройка Nextcloud

В настоящем руководстве рассматривается передача событий с помощью службы rsyslog. Предполагается, что rsyslog на станции с ОС Linux уже установлен.



Nextcloud может быть развернут как на операционной системе, так и в docker контейнере. В обоих случаях сбор событий осуществляется из одного и того же журнала с той лишь разницей, что в случае с docker инсталляцией требуется дополнительный проброс файла журнала в корневую систему.

Для настройки источника выполните следующее:

1. Добавьте или измените в файле **\$NEXTCLOUD_HOME/config/config.php** следующие строки:

```
'logfile' => '/var/log/nextcloud/nextcloud.log',  
'loglevel' => 1,  
'log_type' => 'file',
```

Здесь:

- **logfile** — расположение файла с последующим хранением логов.
- **loglevel** — уровень логирования: 1 (**Info**).
- **log_type** — тип логирования: **file**.

2. Настройте передачу событий из файла. Для этого создайте файл **/etc/rsyslog.d/02-Nextcloud.conf** со следующим содержимым:

```
module(load="imfile" mode="inotify")  
input(  
    type="imfile"  
    File="/var/log/nextcloud/nextcloud.log"  
    Tag="Nextcloud"  
    Severity="info"  
    Facility="local5"  
)  
  
if $syslogtag == 'Nextcloud' then {  
    action(type="omfwd" Target="<target>" Port="<port>" Protocol="<protocol>")  
    stop  
}
```

Здесь:

- **<target>** — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- **<port>** — Порт точки входа Syslog в конвейере SIEM.
- **<protocol>** — Сетевой протокол: **tcp** или **udp**.

3. Перезапустите службу `rsyslog.service` с помощью команды:

```
systemctl restart rsyslog.service
```

Настройка интеграции с R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие шаги:

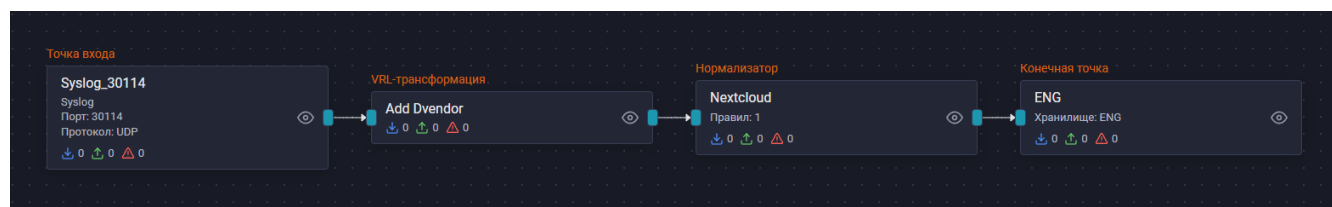
1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Syslog.
 - Порт точки входа и протокол: в соответствии с настройками на стороне [Nextcloud](#).
3. Добавьте на конвейер элемент **VRL-трансформация** со следующим содержимым:

```
.dproduct = "Nextcloud"
```

Соедините VRL-трансформацию с точкой входа.

4. Добавьте на конвейер элемент **Нормализатор** с правилом RV-N-167. Соедините нормализатор с VRL-трансформацией.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
6. Установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события Nextcloud.



Найти события Nextcloud в хранилище можно по следующему фильтру:

```
dproduct = "Nextcloud"
```

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Nginx

Данное руководство описывает процесс настройки сбора и отправки событий Nginx в R-Vision SIEM.

Настройка Nginx

В настоящем руководстве рассматривается передача событий с помощью службы rsyslog. Предполагается, что rsyslog на станции с ОС Linux уже установлен.



Журналирование событий службы Nginx по умолчанию ведется в директории **/var/log/nginx**. Дополнительных действий по настройке журналирования не требуется.

Для настройки источника выполните следующие действия:

1. Настройте передачу событий из файла. Для этого создайте файл `/etc/rsyslog.d/03-Nginx.conf` со следующим содержимым

```
$ModLoad imfile

$InputFileName /var/log/nginx/access.log
$InputFileTag nginx-access
$InputFileSeverity info
$InputFileFacility local4
$InputRunFileMonitor
$InputRunFileMonitor

$InputFileName /var/log/nginx/error.log
$InputFileTag nginx-error
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor
$InputRunFileMonitor

if $syslogtag contains 'nginx' then {
    action(type="omfwd" target="<target>" port="<port>" protocol="<protocol>")
    stop
}
```

Здесь:

- **<target>** — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- **<port>** — порт точки входа Syslog в конвейере SIEM.
- **<protocol>** — сетевой протокол: **tcp** или **udp**.

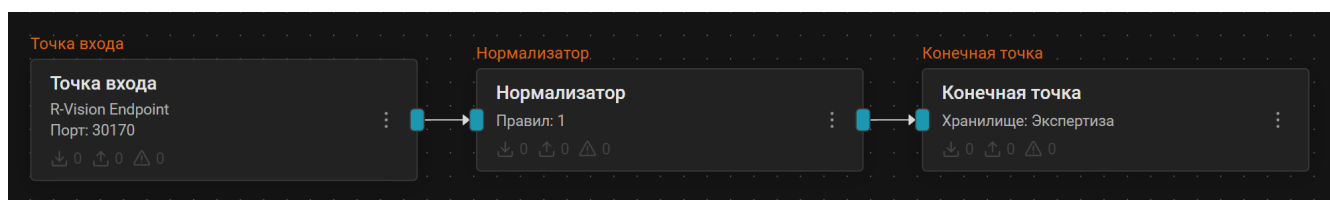
2. Перезапустите службу `rsyslog.service` с помощью команды:

```
systemctl restart rsyslog.service
```

Настройка интеграции с R-Vision SIEM

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Syslog.
 - Порт точки входа и протокол: в соответствии с настройками на стороне [источника](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом Nginx. Соедините нормализатор с точкой входа.
4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
5. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события Nginx.

Найти события Nginx в хранилище можно по следующему фильтру:

```
dproduct = "Nginx"
```

Пример настройки фильтра



Добавить фильтр ✕

☐ Инvertировать (NOT)

Поле

dproduct ▾

Оператор

= ▾

Значение

Nginx ✕

☐ Настроить заголовок

Отменить

Добавить

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

OpenBao

Данное руководство описывает процесс настройки сбора и отправки событий OpenBao в R-Vision SIEM.

- [Настройка OpenBao](#)
 - [Основная настройка](#)
 - [Альтернативная настройка](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Настройка OpenBao

Основная настройка

Чтобы настроить OpenBao:

1. Включите передачу событий в службу **syslog** с помощью команды:

```
sudo openbao audit enable -address="https://<адрес openbao>:8200" syslog  
tag="openbao"
```

Если команда выполнена успешно, в консоли появится сообщение:

```
Success! Enabled the syslog audit device at: syslog/
```

2. Создайте файл **xx-openbao.conf** в директории **/etc/rsyslog.d/** командой:

```
sudo touch /etc/rsyslog.d/xx-openbao.conf
```

где **xx** — номер файла конфигурации.

3. Добавьте в файл **xx-openbao.conf** строки:

```
if $syslogtag contains 'openbao-vault' then {  
    action(type="omfwd" Target="<Адрес коллектора SIEM>" Port="<Порт>"  
    Protocol="<tcp/udp>")  
    stop  
}
```

4. Перезапустите службу **rsyslog** с помощью команды:


```
sudo systemctl restart rsyslog.service
```

Альтернативная настройка

Если в **rsyslog** возникает ошибка, связанная с доступом к **journal**, выполните альтернативную настройку:

1. Включите передачу событий OpenBao в файл с помощью команды:

```
sudo openbao audit enable -address="https://<адрес openbao>:8200" file  
file_path="/var/log/openbao_audit.log"
```

2. Добавьте в файл конфигурации /etc/rsyslog.d/xx-openbao.conf следующие строки:

```
module(load="imfile" PollingInterval="10" mode="inotify")  
  
input(type="imfile"  
      File="/var/log/openbao_audit.log"  
      Tag="openbao"  
      Severity="info"  
      Facility="local6"  
)  
  
local6.info action(type="omfwd" Target="<Адрес коллектора SIEM>" Port="<Порт>"  
Protocol="<tcp/udp>")
```

3. Перезапустите службу **rsyslog** с помощью команды:

```
sudo systemctl restart rsyslog.service
```

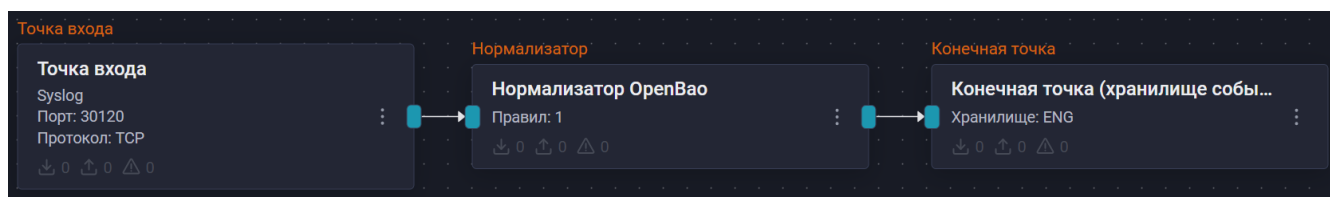
Настройка в R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие шаги:

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Ресурсы** → **Коллекторы** и создайте новый конвейер в коллекторе.
2. Добавьте в конвейер элемент **Точка входа** со следующими параметрами:
 - **Тип точки входа:** Syslog.
 - **Порт точки входа** и **протокол:** в соответствии с [настройкой OpenBao](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом OpenBao (идентификатор правила: RV-N-89). Соедините нормализатор с точкой входа.
4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.

5. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события OpenBao.

Найти события OpenBao в хранилище можно по следующему фильтру:

```
dproduct = "OpenBao"
```



timestamp	dvendor	dproduct	severity	act	rt	spt	src	cs1
2025-05-05T17:51:11.000+...	(Пусто)	OpenBao	info	Login successfull	2024-10-02T17:11:44.000+...	61190	10.150.161.10	response
2025-05-05T17:51:08.000+...	(Пусто)	OpenBao	info	Login successfull	2024-10-09T18:48:18.000+...	57216	10.150.161.10	response
2025-05-05T17:51:05.000+...	(Пусто)	OpenBao	info	Login successfull	2024-10-09T14:15:30.000+...	61620	10.150.161.10	response
2025-05-05T17:51:02.000+...	(Пусто)	OpenBao	info	Login failure	2024-10-02T16:56:13.000+...	61190	10.150.161.10	response
2025-05-05T17:50:59.000+...	(Пусто)	OpenBao	info	Login failure	2024-10-02T16:56:43.000+...	61190	10.150.161.10	response
2025-05-05T17:50:56.000+...	(Пусто)	OpenBao	info	Login failure	2024-10-02T16:56:13.000+...	61190	10.150.161.10	response
2025-05-05T17:50:53.000+...	(Пусто)	OpenBao	info	Login successfull	2024-10-09T18:48:18.000+...	57216	10.150.161.10	response

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

OpenVPN

Данное руководство описывает процесс настройки сбора событий с сервера OpenVPN и их отправки в хранилище R-Vision SIEM.

Типы собираемых событий

- Warning events
- Peer info events
- Channel events
- MULTI events
- PUSH events
- SENT CONTROL events
- Verify events
- TLS events
- Connection reset events
- Client-instance restarting events
- Peer connection initiated events
- Connection established events

Настройка источника событий



Журналирование событий сервиса OpenVPN по умолчанию ведется в директории **/var/log/openvpn**. Дополнительных действий по настройке журналирования не требуется.

События сервера OpenVPN могут отправляться на централизованный сервер syslog либо напрямую в систему SIEM. Далее рассмотрим оба варианта настройки.

Чтобы настроить отправку событий сервера OpenVPN, выполните следующие шаги:

1. Откройте конфигурационный файл rsyslog (**/etc/rsyslog.conf** или **/etc/rsyslog.d/**).
2. Добавьте следующие правила:

```
module(load="imfile" PollingInterval="10")
input(type="imfile"
      File="/var/log/openvpn/openvpn.log"
      Tag="openvpn")
input(type="imfile"
      File="/var/log/openvpn/openvpn-status.log"
      Tag="openvpn-stat")
if $syslogtag contains 'openvpn' then {
    action(type="omfwd" target="<target>" port="<port>" protocol="udp")
}
```

```
stop
}
```

Здесь:

- **<target>**: IP-адрес или полное доменное имя (FQDN) сервера syslog либо узла кластера Kubernetes, на котором запущен коллектор SIEM.
- **<port>**:
 - При отправке событий на сервер rsyslog укажите порт **514**.
 - При отправке событий на конвейер SIEM укажите порт точки входа Syslog — любой свободный порт больше 30000;

3. Перезапустите rsyslog, чтобы изменения вступили в силу:

```
sudo systemctl restart rsyslog
```

Настройка сбора событий с источника на сервере syslog

Если события сначала отправляются на сервер syslog, настройте отправку логов с сервера в SIEM:

1. Откройте конфигурационный файл rsyslog (**/etc/rsyslog.conf** или **/etc/rsyslog.d/**).
2. Добавьте следующее правило:

```
# Укажите адрес IP-адрес SIEM и порт, куда будут отправляться события
if $syslogtag contains 'openvpn' then {
    action(type="omfwd" target="192.0.2.12" port="30000" protocol="tcp")
    stop
}
```

3. Перезапустите rsyslog, чтобы изменения вступили в силу:

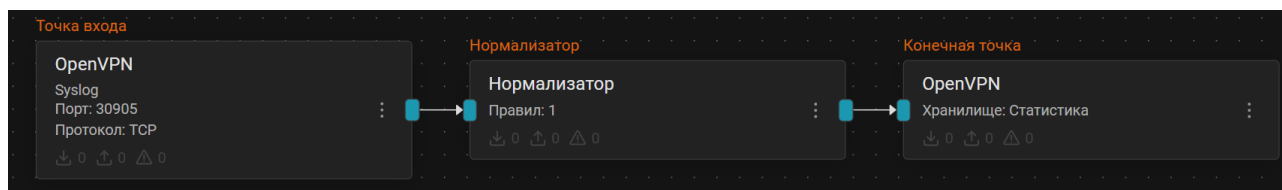
```
sudo systemctl restart rsyslog
```

Настройка интеграции с R-Vision SIEM

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте в конвейер элемент **Точка входа** типа **Syslog** со следующими параметрами:
 - **Название** — любое понятное;
 - **Тип точки входа** — Syslog;
 - **Порт точки входа** и **Протокол** — в соответствии с настройками на стороне [сервера syslog](#).
3. Добавьте **Нормализатор** с правилом **Нормализация событий OpenVPN**. Соедините нормализатор с точкой входа.

- Добавьте элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
- Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера



Если настройка выполнена корректно, то в хранилище начнут поступать события OpenVPN.

Oracle

Данный раздел содержит список систем для настройки от компании Oracle:

- [MySQL](#)

MySQL

Данное руководство описывает процесс настройки сбора и отправки событий MySQL в R-Vision SIEM.

- [Настройка MySQL](#)
 - [Установка плагина для ведения журнала аудита](#)
 - [Настройка службы rsyslog](#)
 - [Настройка syslog-сервера](#)
- [Настройка в R-Vision SIEM](#)
- [Типы обрабатываемых событий](#)

Настройка MySQL

Установка плагина для ведения журнала аудита

Для настройки аудита MySQL установите [плагин для ведения журнала аудита, разработанный компанией Percona](#). Он поддерживает полный аудит в различных форматах, таких как XML, JSON и CSV, а также регистрирует события, связанные с аутентификацией.



Плагин поддерживает только MySQL версии 8.0 и выше.

Чтобы установить плагин аудита Percona, выполните следующие действия:

1. Скачайте архив с плагином, выполнив следующую команду:

```
wget https://downloads.percona.com/downloads/Percona-Server-8.0/Percona-Server-8.0.36-28/binary/tarball/Percona-Server-8.0.36-28-Linux.x86_64.glibc2.35.tar.gz
```

2. Распакуйте архив с плагином:

```
tar -xvf Percona-Server-8.0.36-28-Linux.x86_64.glibc2.35.tar.gz --wildcards --no-anchored '*audit_log.so*'
```

3. Получите путь к директории, в которой располагаются плагины MySQL:

- а. Войдите в консоль MySQL:

```
mysql -u root -p -h localhost
```

b. Выполните следующий запрос:

```
SHOW GLOBAL VARIABLES LIKE 'plugin_dir';
```

▼ Пример вывода запроса пути к директории плагинов

```
+-----+-----+
| Variable_name | Value                |
+-----+-----+
| plugin_dir    | /usr/lib64/mysql/plugin/ |
+-----+-----+
1 row in set (0.00 sec)
```

В примере директория плагинов — `/usr/lib64/mysql/plugin/`.

4. Скопируйте плагин в директорию плагинов:

```
cp Percona-Server-8.0.36-28-Linux.x86_64.glibc2.35/lib/plugin/audit_log.so <plugin-dir>
```

Здесь:

- `<plugin-dir>` — директория плагинов, полученная на шаге 3.

5. Установите плагин:

a. Войдите в консоль MySQL:

```
mysql -u root -p -h localhost
```

b. Выполните следующий запрос:

```
INSTALL PLUGIN audit_log SONAME 'audit_log.so';
```

Если плагин установлен успешно, отобразится сообщение:

```
Query OK, 0 rows affected (0.02 sec)
```

6. Добавьте настройки плагина в раздел `_[mysqld]_` в файле `my.cnf`:

```
[mysqld]
audit_log_format = JSON
audit_log_policy = ALL
audit_log_handler = SYSLOG
```

7. Перезапустите сервер MySQL:

```
systemctl restart mysqld
```

Настройка службы rsyslog

Чтобы настроить службу rsyslog, выполните следующие действия:

1. Создайте файл конфигурации rsyslog:

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

2. Добавьте в созданный файл следующее правило:

```
if $syslogtag == 'mysqld' or $syslogtag == 'percona-audit' then {  
    action(type="omfwd" target="<target>" port="514" protocol="tcp")  
    stop  
}
```

Здесь:

- **<target>** — IP-адрес или полное доменное имя (FQDN) централизованного syslog-сервера, с которого будет осуществляться отправка сообщений в SIEM.

3. Перезапустите rsyslog для применения изменений:

```
sudo systemctl restart rsyslog
```

Настройка syslog-сервера

Для настройки syslog-сервера выполните следующие шаги:

1. Откройте конфигурационный файл rsyslog (**/etc/rsyslog.conf** или **/etc/rsyslog.d/**).
2. Добавьте в файл правило обработки CEF-сообщений:

```
if $syslogtag == 'mysqld' or $syslogtag == 'percona-audit' then {  
    action(type="omfwd" Target="<target>" Port="<port>" Protocol="tcp")  
    stop  
}
```

Здесь:

- **<target>** — IP-адрес или полное доменное имя (FQDN) централизованного syslog-сервера, с которого будет осуществляться отправка сообщений в SIEM.
- **<port>** — порт точки входа Syslog на конвейере SIEM — любой свободный порт в диапазоне

30000—32767.

3. Перезапустите rsyslog для применения изменений:

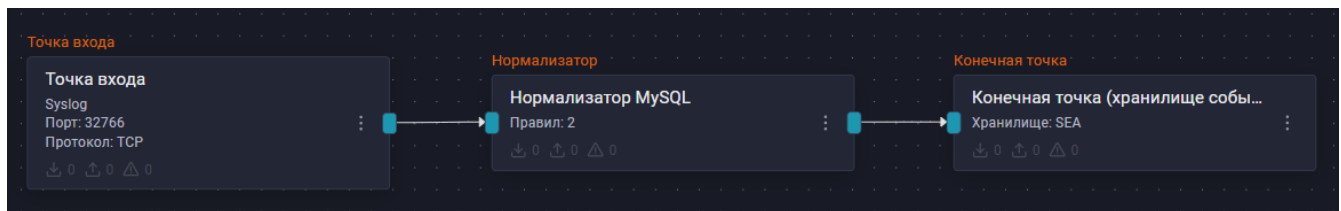
```
sudo systemctl restart rsyslog
```

Настройка в R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие шаги:

1. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Syslog**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [syslog-сервера](#).
 - Протокол: выберите вариант **TCP**.
2. Добавьте на конвейер элемент **Нормализатор** с правилами **Oracle MySQL** (идентификатор правила: **RV-N-82**) и **Oracle MySQL** (идентификатор правила: **RV-N-83**).
3. Соедините нормализатор с точкой входа.
4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
5. Соедините конечную точку с нормализатором.
6. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события MySQL.

Найти события MySQL в хранилище можно по следующему фильтру:

```
dproduct = "MySQL"
```



Добавить фильтр

☐ Инвертировать (NOT)

Поле

Оператор

Значение

dproduct

=

MySQL

☐ Настроить заголовок

Отменить

Добавить

Типы обрабатываемых событий

Событиями аудита являются выполняемые команды MySQL. С их перечнем можно ознакомиться в [официальной документации MySQL](#).

PostgreSQL

Данное руководство описывает процесс настройки сбора и отправки событий СУБД PostgreSQL в R-Vision SIEM.

Настройка PostgreSQL

В настоящем руководстве рассматривается передача событий с помощью службы rsyslog. Предполагается, что rsyslog на станции с ОС Linux уже установлен.

Настройка журналирования PostgreSQL

Для настройки источника выполните следующие действия:

1. В конфигурационном файле postgresql.conf найдите и отредактируйте параметры:

```
listen_addresses = '*'
log_destination = 'syslog'
logging_collector = on
log_min_messages = debug5
log_min_error_statement = debug5
log_checkpoints = on
log_connections = on
log_disconnections = on
log_error_verbosity = verbose
log_line_prefix = '%m [%p] %u %r '
shared_preload_libraries = 'pgaudit'
```



В поле log_line_prefix указано регулярное выражение в правиле нормализации.

2. Если требуется сбор логов аудита, установите модуль pgaudit:

- a. Выполните команду:

```
yum install -y pgaudit16_14
```

- b. От имени postgres выполните:

```
ALTER SYSTEM SET pgaudit.log='all'
```

3. Перезапустите сервис PostgreSQL командой:

```
systemctl restart postgresql-14
```

Отправка событий PostgreSQL

Чтобы настроить отправку событий PostgreSQL:

1. Создайте файл **/etc/rsyslog.d/60-postgres.conf** со следующим содержимым:

```
if $programname == 'postgres' or $syslogtag == 'postgres' then {  
    action(type="omfwd" Target="<target>" Port="<port>" Protocol="<protocol>")  
    stop  
}
```

Здесь:

- **<target>** — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- **<port>** — порт точки входа Syslog в конвейере SIEM.
- **<protocol>** — сетевой протокол: **tcp** или **udp**.

2. Перезапустите службу rsyslog.service с помощью команды:

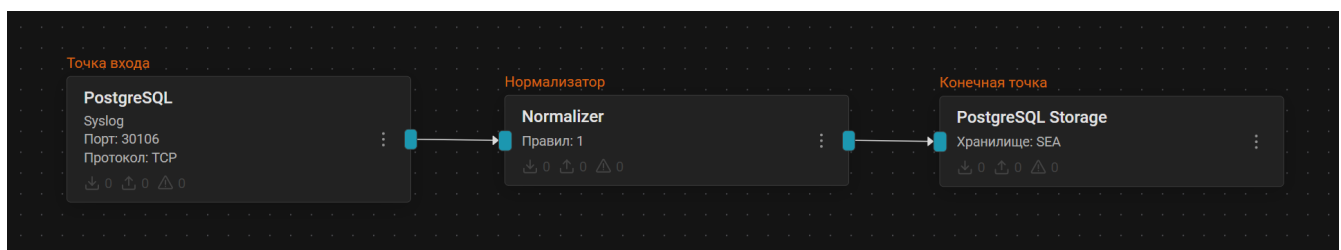
```
systemctl restart rsyslog.service
```

Настройка интеграции с R-Vision SIEM

Для настройки сбора событий от источника в R-Vision SIEM выполните следующие шаги:

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Ресурсы** → **Коллекторы** и создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Syslog.
 - Порт точки входа и протокол: в соответствии с настройками на стороне [PostgreSQL](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом PostgreSQL (идентификатор правила: RV-N-100). Соедините нормализатор с точкой входа.
4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
5. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события PostgreSQL.

Найти события PostgreSQL в хранилище можно по следующему фильтру:

```
dproduct = "PostgreSQL"
```



Поиск Хранилище событий: SEA

Введите запрос и нажмите кнопку Поиск

2025-05-21, 00:00:00 2025-05-21, 23:59:59 Поиск

Сбросить все dproduct = PostgreSQL + Добавить фильтр

Совпадений 1032827 Интервал времени: 2025-05-21T00:00:00+03:00 - 2025-05-21T23:59:59+03:00 Показать график

timestamp	dvendor	dproduct	name	dvc	msg	outcome
2025-05-21T06:35:24.000+03:00	PostgreSQL	PostgreSQL	Transaction Event	(Пусто)	00000: CommitTransaction(1)...	success
2025-05-21T06:35:24.000+03:00	PostgreSQL	PostgreSQL	Connection Event	(Пусто)	00000: connection authorized: user=svr_aws...	success
2025-05-21T06:35:24.000+03:00	PostgreSQL	PostgreSQL	Connection Event	(Пусто)	00000: connection authenticated:...	success
2025-05-21T06:35:24.000+03:00	PostgreSQL	PostgreSQL	LOCATION	(Пусто)	recv_password_packet, auth.c:763	success
2025-05-21T06:35:24.000+03:00	PostgreSQL	PostgreSQL	DEBUG	(Пусто)	00000: my backend ID is 31	success
2025-05-21T06:35:24.000+03:00	PostgreSQL	PostgreSQL	LOCATION	(Пусто)	InitPostgres, postinit.c:587	success
2025-05-21T06:35:24.000+03:00	PostgreSQL	PostgreSQL	DEBUG	(Пусто)	00000: InitPostgres	success
2025-05-21T06:35:24.000+03:00	PostgreSQL	PostgreSQL	LOCATION	(Пусто)	BackendInitialize, postmaster.c:4423	success
2025-05-21T06:35:24.000+03:00	PostgreSQL	PostgreSQL	LOG	(Пусто)	00000: duration: 0.131 ms statement: SELECT...	success
2025-05-21T06:35:24.000+03:00	PostgreSQL	PostgreSQL	Audit Event	(Пусто)	00000: AUDIT: SESSION,7,1,READ,SELEC...	success
2025-05-21T06:35:24.000+03:00	PostgreSQL	PostgreSQL	Query Event	(Пусто)	SELECT pg_advisory_unlock(-756...	success
2025-05-21T06:35:24.000+03:00	PostgreSQL	PostgreSQL	Transaction Event	(Пусто)	ShowTransactionStateRec, xact.c:5427	success
2025-05-21T06:35:24.000+03:00	PostgreSQL	PostgreSQL	LOCATION	(Пусто)	exec_simple_query, postgres.c:1308	success

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Positive Technologies

Данный раздел содержит список систем для настройки от компании Positive Technologies

- [Application Firewall v3](#)
- [Application Firewall v4](#)
- [Network Attack Discovery](#)
- [Sandbox](#)

Application Firewall v3

Данное руководство описывает процесс настройки сбора и отправки событий Positive Technologies Application Firewall 3 (PT AF 3) в R-Vision SIEM.

- [Настройка PT AF 3](#)
 - [Включение логирования системных и прикладных событий WAF](#)
 - [Включение логирования событий веб-приложений](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Настройка PT AF 3



Для источника PT AF 3 на конвейере коллектора R-SIEM **необходимо создать отдельную точку входа** с выделенным портом, в которую будут поступать только события от PT AF 3. При попадании в эту же точку входа событий от других источников работа правил нормализации будет некорректной, а ожидаемый результат на выходе непредсказуемым.

Настройка отправки событий делится на два этапа:

1. Настройка системных сообщений.
2. Настройка прикладных событий веб-приложений.

Включение логирования системных и прикладных событий WAF

Для включения логирования системных и прикладных событий в консоли WSC выполните команды:

```
syslog set uri @@<target>:<port>
syslog set criticality error
syslog set send enabled
```

Здесь:

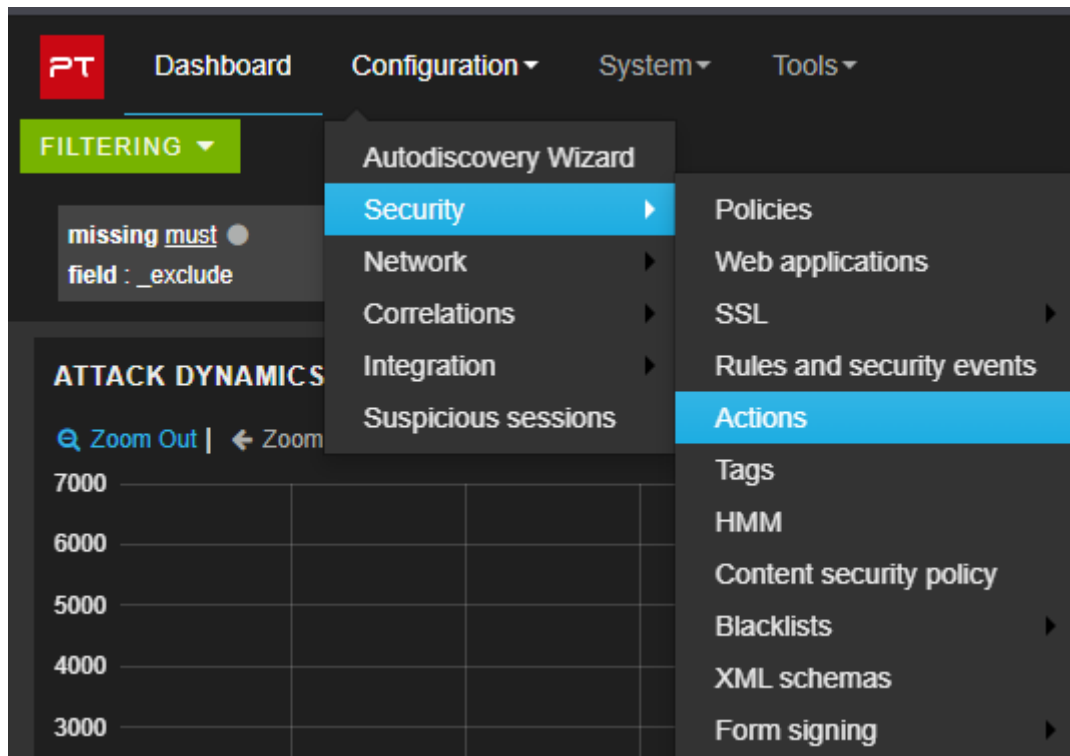
- **@@** — указатель на протокол TCP.
- **<target>** — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.

- **<port>** — порт точки входа Syslog на конвейере SIEM.

Включение логирования событий веб-приложений

На панели управления сервера PT AF 3 выполните следующие действия:

1. Перейдите в раздел **Configuration** → **Security** → **Actions**:



2. В разделе **Actions** нажмите на кнопку **Create**:

The screenshot shows the PT Configuration interface. At the top, there are tabs for Dashboard, Configuration (selected), System, and Tools. Below the tabs is a header bar with 'ACTIONS' and two buttons: 'List' and 'Create' (highlighted in blue). The main form area contains several fields:

- Name ***: A text input field.
- Type**: A dropdown menu with 'Send to syslog (attack, alert, ...)' selected.
- Object type**: A dropdown menu with 'Attacks' selected.
- Configuration**: A section containing:
 - IP address ***: A text input field.
 - Port**: A text input field with '514' entered.
 - Format**: A large text area for defining the syslog message format.
 - Escape characters**: A text input field.
 - Escape characters in matched variables**: A text input field.

At the bottom right of the Format field, there is a 'Format help' icon. At the bottom of the form, there are three buttons: 'Apply' (highlighted in green), 'Save and Add', and 'Cancel'.

3. Создайте 3 действия:

a. Действие **Attacks** со следующими параметрами:

- Name: введите значение **Send attack to syslog**.
- Type: выберите вариант **Send to syslog (attack, alert, vulnerability)**.
- Object type: выберите вариант **Attacks**.
- IP address: введите IP-адрес syslog-сервера.
- Port: укажите порт syslog-сервера.
- Format — введите строку:

```
-- Attack -- %EVENT_ID -- %EVENT_SEVERITY -- %EVENT_DESCRIPTION --
%POLICY_NAME -- %REQUEST_HOST -- %REQUEST_PATH -- %MATCHED.VALIDATOR --
%MATCHED.VARIABLE -- %MATCHED.VALUE -- %REQUEST_QUERY
```

Остальные параметры оставьте без изменений и нажмите на кнопку **Apply**.

b. Действие **Alerts** со следующими параметрами:

- Name: введите значение **Send alert to syslog**.

- Type: выберите вариант **Send to syslog (attack, alert, vulnerability)**.
- Object type: выберите вариант **Alerts**.
- IP address: введите IP-адрес syslog-сервера.
- Port: укажите порт syslog-сервера.
- Format — введите строку:

```
-- Alert -- %ALERT_SEVERITY -- %ALERT_NAME -- %ALERT_DESCRIPTION
```

Остальные параметры оставьте без изменений и нажмите на кнопку **Apply**.

с. Действие **Vulnerability** со следующими параметрами:

- Name: введите значение **Send vulnerability to syslog**.
- Type: выберите вариант **Send to syslog (attack, alert, vulnerability)**.
- Object type: выберите вариант **Vulnerabilities**.
- IP address: введите IP-адрес syslog-сервера.
- Port: укажите порт syslog-сервера.
- Format — введите строку:

```
-- Vulnerability -- %EVENT_ID -- %EVENT_SEVERITY -- %EVENT_DESCRIPTION --  
%POLICY_NAME -- %REQUEST_HOST -- %REQUEST_PATH -- %MATCHED.VALIDATOR --  
%MATCHED.VARIABLE -- %MATCHED.VALUE
```

Остальные параметры оставьте без изменений и нажмите на кнопку **Apply**.

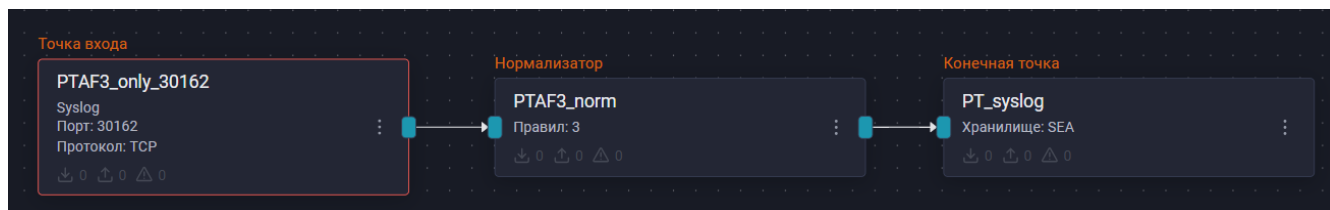
Настройка в R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие действия:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Syslog**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [PT AF 3](#).
 - Протокол: выберите вариант в соответствии с настройками на стороне [PT AF 3](#).
3. Добавьте на конвейер элемент **Нормализатор** со следующими правилами:
 - **Positive Technologies Application Firewall 3** (идентификатор правила: **RV-N-95**);
 - **Positive Technologies Application Firewall 3** (идентификатор правила: **RV-N-96**);
 - **Positive Technologies Application Firewall 3** (идентификатор правила: **RV-N-99**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.

6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события PT AF 3.

Найти события PT AF 3 в хранилище можно по следующему фильтру:

`dproduct = "Application Firewall"`



timestamp	dvendor	dproduct	name	dvc	msg
2025-04-08T14:23:57.000+...	Positive Technologies	Application Firewall	waf-sync-twisted		14:12:22+0300 [1...
2025-04-08T14:23:55.000+...	Positive Technologies	Application Firewall	wafd		ev_sender: (111: Connection...
2025-04-08T14:23:52.000+...	Positive Technologies	Application Firewall	Attack		Ha yane splunk.waf.sea.lan...
2025-04-08T14:23:49.000+...	Positive Technologies	Application Firewall	waf-nginx-error		SEVERITY EXTRACT ERROR 2024/04/1...
2025-04-08T14:23:47.000+...	Positive Technologies	Application Firewall	waf-nginx-error		SEVERITY EXTRACT ERROR 2025/04/0...
2025-04-08T14:23:47.000+...	Positive Technologies	Application Firewall	waf-nginx-error		SEVERITY EXTRACT ERROR 2025/04/0...
2025-04-08T14:23:47.000+...	Positive Technologies	Application Firewall	carbon-console		08/04/2025 14:12:13 :: Sorted...
2025-04-08T14:23:47.000+...	Positive Technologies	Application Firewall	carbon-console		08/04/2025 14:12:13 :: Queue...
2025-04-08T14:23:47.000+...	Positive Technologies	Application Firewall	carbon-console		08/04/2025 14:12:13 :: ...

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Application Firewall v4

Данное руководство описывает процесс настройки сбора и отправки событий Positive Technologies Application Firewall 4 (PT AF 4) в R-Vision SIEM.

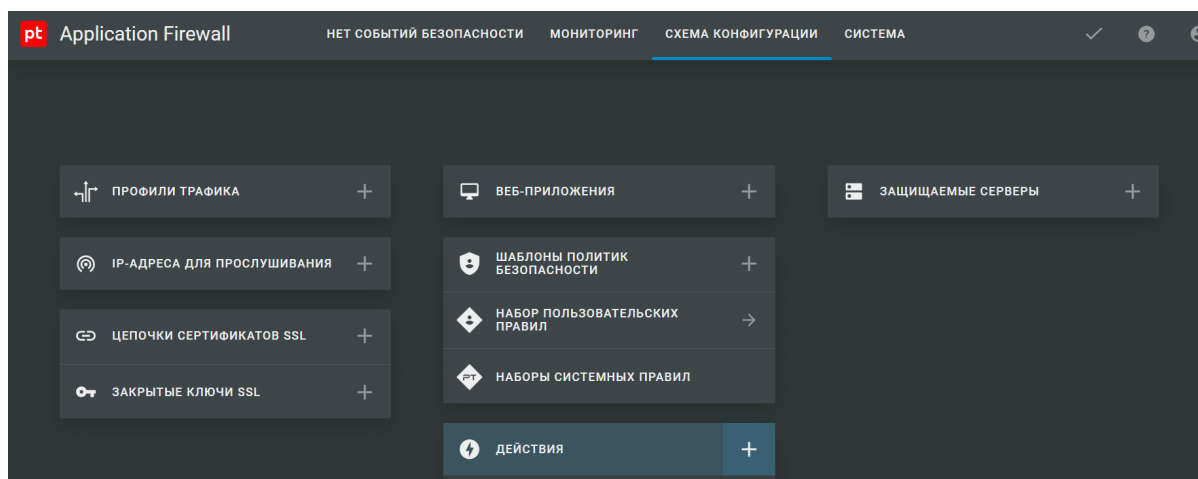
- [Настройка PT AF 4](#)
- [Настройка в R-Vision SIEM](#)

- [Таблица маппинга](#)

Настройка PT AF 4

Для настройки отправки событий на панели управления сервера PT AF 4:

1. В главном меню перейдите на вкладку **Схема конфигурации**.
2. В разделе **Действия** нажмите на кнопку **+**:



3. Создайте новое действие со следующими параметрами:
 - Название: введите значение **Send to syslog**.
 - Тип: выберите вариант **Отправлять событие на syslog-сервер**.
 - IP-адрес или имя узла: введите IP-адрес syslog-сервера.
 - Протокол: выберите вариант в соответствии с настройками [точки входа конвейера R-Vision SIEM](#).
 - Порт: введите значение в соответствии с настройками [точки входа конвейера R-Vision SIEM](#).
 - Максимальный размер: введите значение **65507**.
 - Шаблон: выберите вариант **CEF**.

Остальные параметры оставьте без изменений.

×

Новое пользовательское действие

Название

Send to syslog

Тип

☐ Добавлять IP-адрес клиента в глобальный динамический список

☐ Записывать событие в базу данных

☐ Изменять заголовки ответа

☐ Отправлять свой ответ

☒ Отправлять событие на syslog-сервер

Отправлять информацию о событии на удаленный syslog-сервер

Параметры

IP-адрес или имя узла

10.150.21.11

Протокол

☒ UDP

☐ TCP

Порт

514

Максимальный размер

65507

Не больше 65507 байт

Шаблон

CEF

Формат

RFC 5424

Содержимое

☒ Основные сведения

ID события безопасности, уровень опасности, теги, тип, время, действия, ID и название правила, ID и название веб-приложения

☒ Описание совпадений

☒ Узел обработки трафика

IP-адрес для прослушивания и порт

☒ Пользователь

Браузер, IP-адрес, порт и логин

☒ Описание события безопасности

☒ HTTP-запрос

Метод, путь и узел

>

ДОБАВИТЬ ДЕЙСТВИЕ

ОТМЕНА

4. Нажмите на кнопку **Добавить действие**

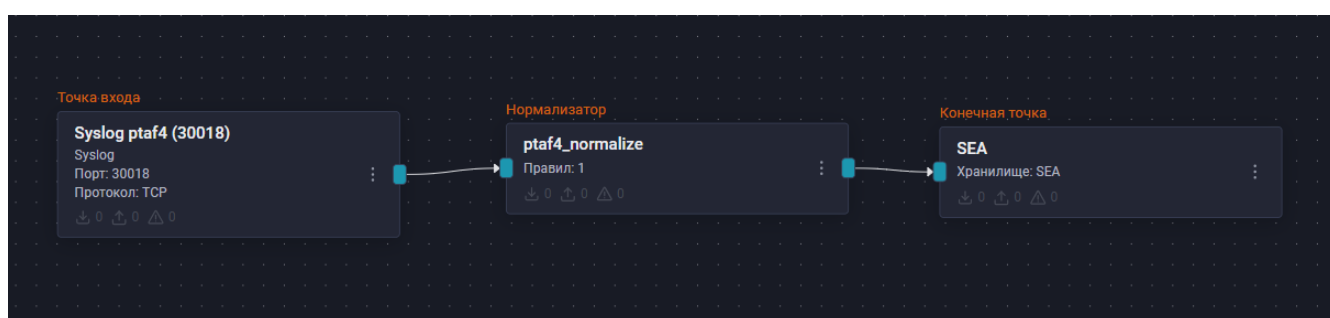
Настройка в R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие действия:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:

- Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Syslog**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [PT AF 4](#).
 - Протокол: выберите вариант в соответствии с настройками на стороне [PT AF 4](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Positive Technologies Application Firewall 4** (идентификатор правила: **RV-N-97**).
 4. Соедините нормализатор с точкой входа.
 5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
 6. Соедините конечную точку с нормализатором.
 7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события PT AF 4.

Найти события PT AF 4 в хранилище можно по следующему фильтру:

```
dproduct = "Application Firewall"
```



Добавить фильтр

☐ Инvertировать (NOT)

Поле

dproduct

Оператор

=

Значение

Application Firewall

☐ Настроить заголовок

Отменить

Добавить

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Network Attack Discovery

Данное руководство описывает процесс настройки подсистемы журналирования и отправки событий из PT Network Attack Discovery (PT NAD) в R-Vision SIEM.

- [Настройка PT NAD](#)
 - [Описание подсистемы журналирования PT NAD](#)
 - [Настройка syslog-сообщений об активностях, атаках и индикаторах компрометации](#)
 - [Настройка syslog-сообщений о результатах ретроспективного анализа и уведомлениях](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Настройка PT NAD

Описание подсистемы журналирования PT NAD

Согласно п. 10.11 руководства администратора PT Network Attack Discovery, продукт может записывать в системный журнал syslog следующие сведения:

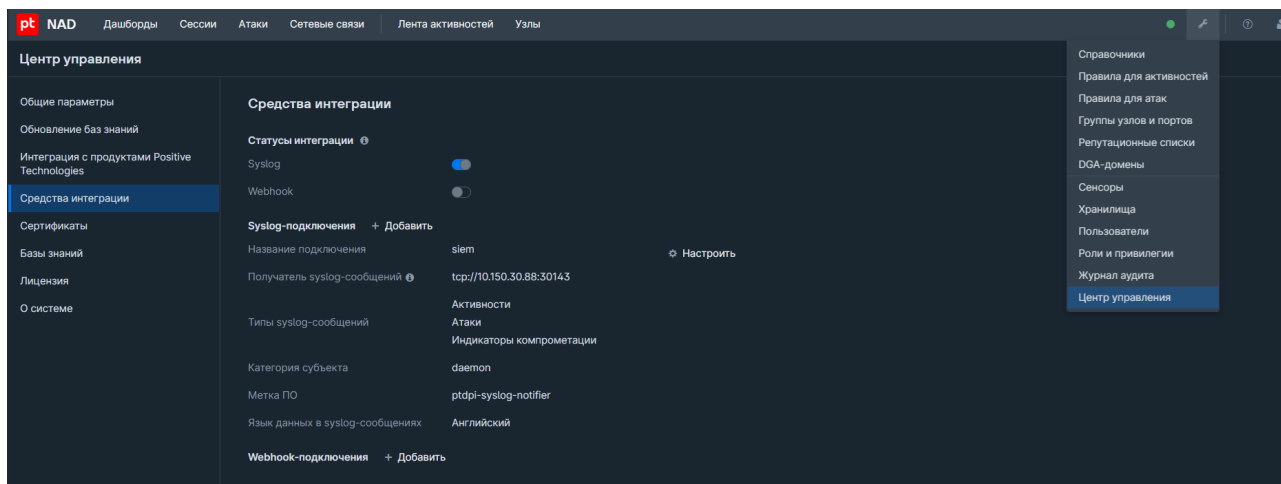
- информация об активностях;
- информация о выявленных атаках;
- информация об обнаруженных индикаторах компрометации;
- результаты ретроспективного анализа;
- уведомления о заполнении журнала аудита.

Настройка отправки событий делится на два этапа:

1. Настройка syslog-сообщений об активностях, атаках и индикаторах компрометации (п. 10.11.1 руководства администратора PT NAD).
2. Настройка syslog-сообщений о результатах ретроспективного анализа и уведомлениях о заполнении журнала аудита (п. 10.11.2 руководства администратора PT NAD).

Настройка syslog-сообщений об активностях, атаках и индикаторах компрометации

1. В веб-интерфейсе PT NAD перейдите в раздел **Центр управления** → **Средства интеграции**.



2. Переведите переключатель **Syslog** в активное положение и нажмите на кнопку **Добавить** в настройках Syslog-подключения. Откроется окно настройки подключения.

Настройка syslog-подключения

Соединение установлено

Название подключения

siem

Получатель syslog-сообщений

tcp://10.150.30.88:30143

Типы syslog-сообщений

Активности еще 1

Категория субъекта

daemon

Метка ПО

ptdpi-syslog-notifier

Язык данных в syslog-сообщениях

Английский Русский

Проверить соединение

Удалить

Сохранить

Отмена

3. В поле **Получатель syslog-сообщений** укажите протокол, адрес и порт syslog-сервера в формате **<протокол>://<адрес>:<порт>**.
4. Проверьте корректность настроек с помощью кнопки **Проверить соединение**.
5. Нажмите на кнопку **Сохранить**, чтобы применить изменения.

Настройка syslog-сообщений о результатах ретроспективного анализа и уведомлений

1. Откройте файл `/etc/rsyslog.d/45-ptdpi.conf`.
2. Раскомментируйте строку и задайте значения параметров **target**, **port** и **protocol**. Например:

```
action(type="omfwd" target="10.150.30.88" port="30143" protocol="tcp")
```

3. Сохраните изменения в файле `/etc/rsyslog.d/45-ptdpi.conf`.
4. Перезапустите службу `rsyslog` с помощью команды:

```
sudo systemctl restart rsyslog.service
```

5. Чтобы включить запись `syslog`-сообщений о ретроспективном анализе и заполнении журнала аудита, выполните следующие шаги:
 - a. Откройте файл `/opt/ptsecurity/etc/nad.settings.yaml`.
 - b. Раскомментируйте параметры `retrospective_notify_syslog` и `journal_notify_syslog`.
 - c. Установите для данных параметров значение `true`.
 - d. Перезапустите службы с помощью команд:

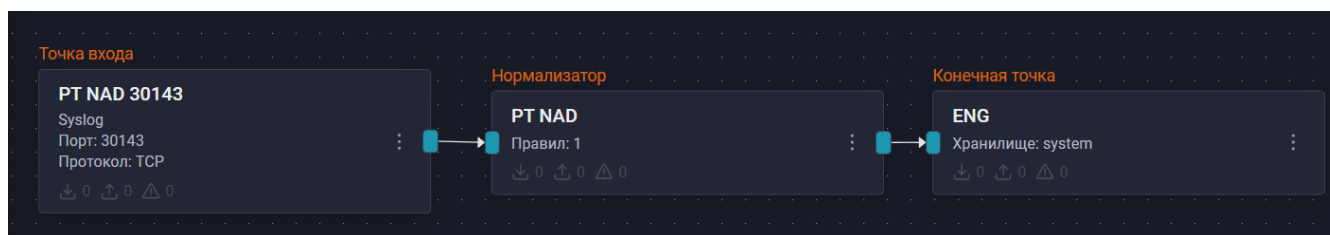
```
sudo systemctl restart nad-task-server.service
sudo systemctl restart nad-web-server.service
```

Настройка в R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Syslog**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [PT NAD](#).
 - Протокол: выберите вариант в соответствии с настройками на стороне [PT NAD](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Positive Technologies Network Attack Discovery** (идентификатор правила: **RV-N-128**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут

поступать события PT NAD.

Найти события PT NAD в хранилище можно по следующему фильтру:

dproduct = "NAD"



Добавить фильтр ×

☐ Инvertировать (NOT)

Поле

dproduct ▼

Оператор

= ▼

Значение

NAD ×

☐ Настроить заголовок

Отменить

Добавить

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Sandbox

Данное руководство описывает процесс настройки сбора и отправки событий Positive Technologies Sandbox (PT Sandbox) в R-Vision SIEM.

- [Настройка PT Sandbox](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Настройка PT Sandbox

Для настройки отправки событий PT Sandbox выполните следующие шаги:

1. В главном меню интерфейса PT Sandbox перейдите в раздел **Система** → **Основные параметры**.
2. В группе параметров **Отправка сообщений по протоколу syslog** установите верхний переключатель в активное положение, чтобы включить отправку сообщений.
3. В поле **Адрес syslog-сервера** введите IP-адрес или полное доменное имя (FQDN) коллектора R-Vision SIEM.
4. Укажите значение порта в диапазоне 30000—32767 в соответствии с настройками на [конвейере](#)

SIEM.

5. В поле **Протокол** выберите транспортный протокол **TCP**.
6. Установите переключатель **Отправлять события аудита** в активное положение.
7. Нажмите на кнопку **Сохранить**. Изменения будут применены в течение нескольких минут.

СводкаЗаданияОбъектыСредства проверкиИсточникиСистема

Основные параметрыТокены доступаОбновленияКонфигурацияЛицензия

Отправка сообщений по протоколу syslog

Сообщения о результатах проверки объектов и событиях аудита системы будут отправляться на внешний syslog-сервер. Например, вы можете отправлять такие сообщения во внешнюю SIEM-систему для последующего анализа.

☒

Адрес syslog-сервера

10.150.30.89

:

30 177

Протокол

TCPUDP

☒ Отправлять события аудита

Отправка данных в PT Threat Analyzer

Данные об обнаруженных опасных и потенциально опасных объектах будут отправляться через API в PT Threat Analyzer для создания отчетов.

☐

Уведомления об угрозах

PT Sandbox может уведомлять специалистов

☐

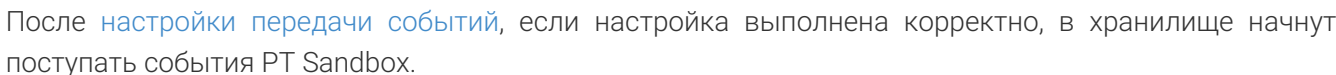
СохранитьОтмена

Настройка в R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Syslog**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [PT Sandbox](#).
 - Протокол: выберите вариант в соответствии с настройками на стороне [PT Sandbox](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Positive Technologies Sandbox** (идентификатор правила: **RV-N-98**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.

Пример конфигурации конвейера:



```
dproduct = "Sandbox"
```

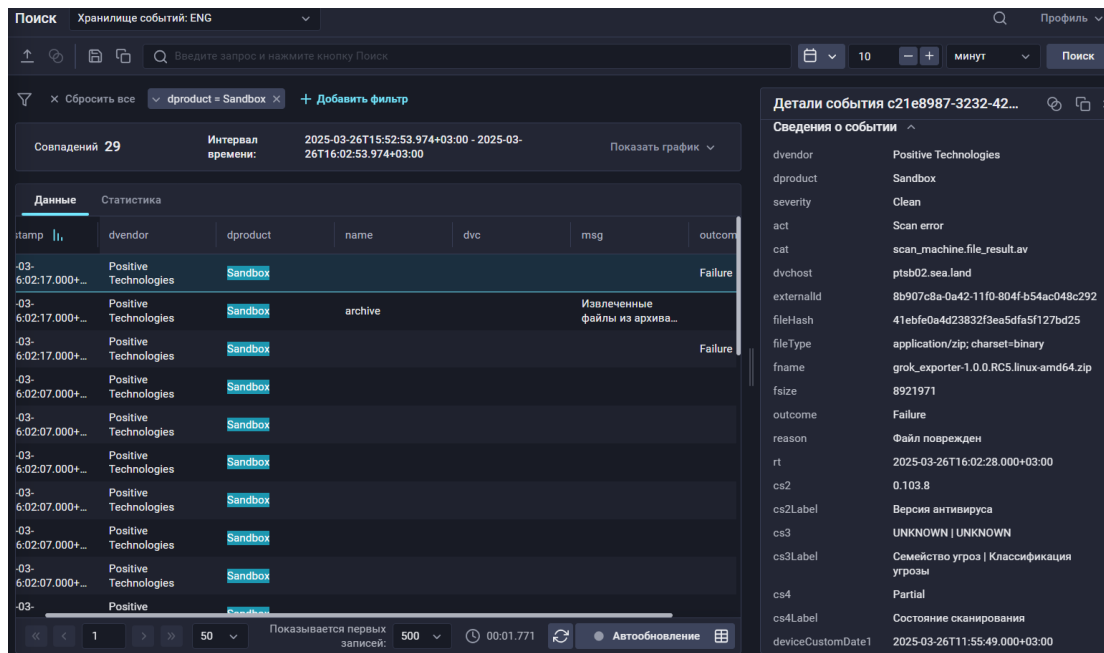


Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

R-Vision

Данный раздел содержит список систем для настройки от компании R-Vision, а также дополнительные инструменты, которые могут помочь в сборе событий источников:

- [R-Vision TDP](#)
- [R-Vision TIP](#)
- [Универсальный коннектор CEF](#)

R-Vision TDP

Данное руководство описывает процесс настройки сбора и отправки событий R-Vision Threat Deception Platform (R-Vision TDP) в R-Vision SIEM.

Настройка R-Vision TDP

Для настройки отправки событий выполните следующие действия:

1. Войдите в веб-интерфейс R-Vision TDP.
2. Перейдите в раздел **Настройки** → **Интеграции** → **Syslog**.
3. В открывшейся вкладке нажмите кнопку **Добавить**.
4. В текущем окне заполните параметры интеграции:
 - **Адрес сервера** — IP-адрес или FQDN ноды кластера R-Vision SIEM.
 - **Порт** — порт Syslog-сервера.
 - **Протокол** — сетевой протокол (**tcp** или **udp**).
5. Нажмите на кнопку **Далее**.

Добавление интеграции Syslog

1

Параметры интеграции

2

Выгружаемые события

Параметры интеграции

Название

SIEM

Адрес сервера

siem.k8s.rvision

Порт

30152

Протокол

TCP

Отменить

Далее

6. Выберите типы событий для отправки.

7. Нажмите на кнопку **Добавить**.

Добавление интеграции Syslog

1

Параметры интеграции

2

Выгружаемые события

Выгружаемые события

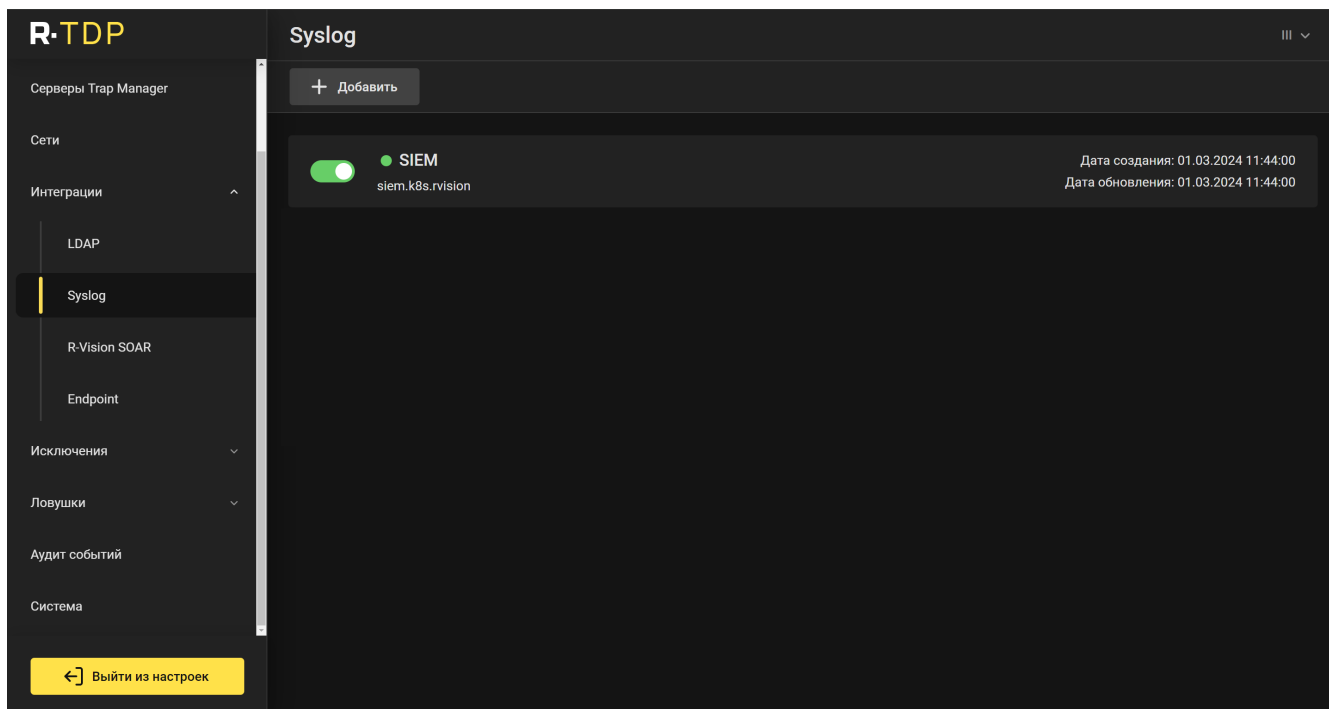
☒ Все события

☐ События по фильтрам

Назад

Добавить

Если настройка на стороне TDP проведена корректно, в разделе Syslog отобразится добавленная вами интеграция.

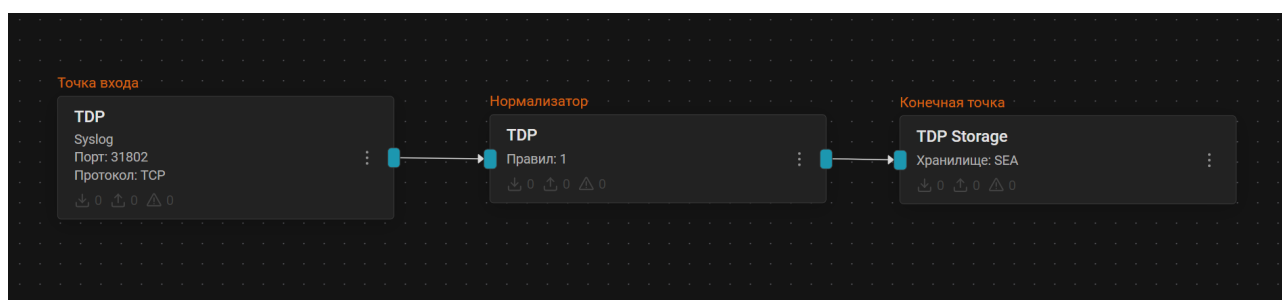


Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Syslog.
 - Порт точки входа и протокол: в соответствии с настройками на стороне [R-Vision Threat Deception Platform](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом R-Vision Threat Deception Platform (идентификатор правила: RV-N-102). Соедините нормализатор с точкой входа.
4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
5. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события R-Vision TDP.



Найти события R-Vision TDP в хранилище можно по следующему фильтру:

```
dproduct = "TDP"
```

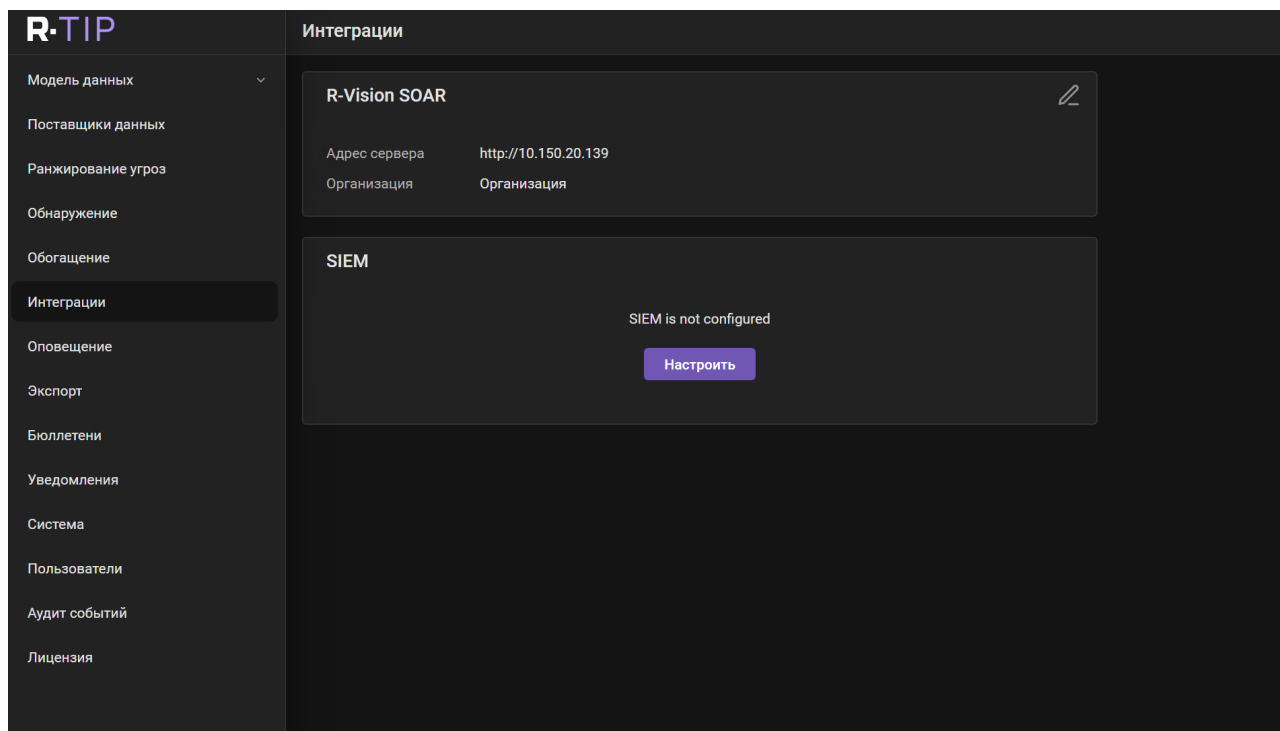
R-Vision TIP

Данное руководство описывает процесс настройки сбора и отправки событий источника R-Vision TIP (Threat Intelligence Platform) в R-Vision SIEM.

Настройка R-Vision TIP

Чтобы настроить R-Vision TIP:

1. В веб-интерфейсе R-Vision TIP нажмите на кнопку **Настройки** (⚙️).
2. Перейдите в раздел **Интеграции**.
3. Нажмите на кнопку **Настроить**.



4. Заполните поля **Адрес сервера**, **Порт** и **Протокол**.
5. Нажмите на кнопку **Сохранить**.

Настройка SIEM

Адрес сервера

10.150.30.89

Порт

30128

Протокол

TCP

Отменить

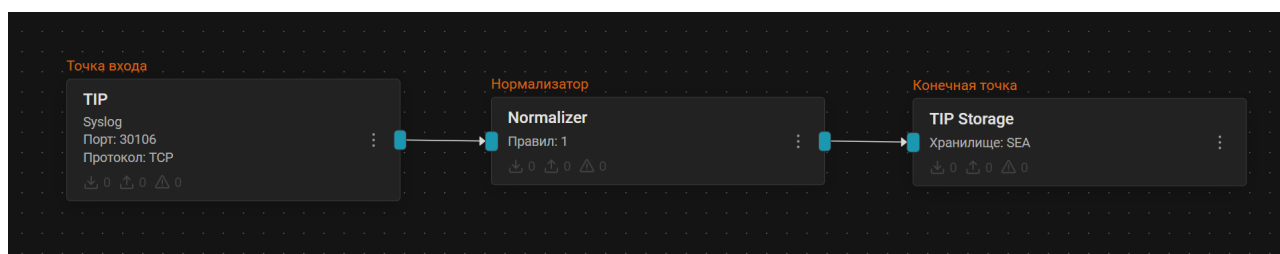
Сохранить

Настройка в R-Vision SIEM

Для настройки сбора событий от источника в R-Vision SIEM выполните следующие шаги:

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Ресурсы** → **Коллекторы** и создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Syslog.
 - Порт точки входа и протокол: в соответствии с настройками на стороне [R-Vision TIP](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом R-Vision Threat Intelligence Platform (идентификатор правила: RV-N-103). Соедините нормализатор с точкой входа.
4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
5. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события TIP.



Найти события TIP в хранилище можно по следующему фильтру:


```
dproduct = "TIP"
```

Изменить фильтр

☐ Инвертировать (NOT)

Поле: dproduct Оператор: =

Значение: TIP

☐ Настроить заголовок

Отменить Сохранить

Универсальный коннектор CEF

Данное руководство содержит инструкции по настройке подключения к системе R-Vision SIEM источников событий, передающих данные в формате Common Event Format (CEF) через syslog.

Подключение источников событий, передающих данные в формате CEF, требует выполнения настроек на стороне источников, syslog-сервера и коллектора в R-Vision SIEM. После завершения настройки обеспечивается централизованный сбор, хранение и анализ событий безопасности от источников, поддерживающих логирование в формате CEF.



Корреляция событий, нормализованных универсальным коннектором CEF, в настоящий момент не поддерживается. Если для источника есть отдельные правила нормализации и корреляции, то источник следует подключать по инструкции для данного источника событий.

- [Предварительные требования](#)
 - [Настройка syslog-сервера](#)
 - [Настройка сетевой связности](#)
- [Настройка источника событий](#)
- [Настройка syslog-сервера](#)
- [Настройка в R-Vision SIEM](#)
- [Проверка получения событий](#)
- [Решение проблем](#)

Предварительные требования

Настройка syslog-сервера

Для настройки syslog-сервера выполните следующие шаги:

1. Убедитесь, что syslog-сервер настроен на прослушивание порта. Как правило, для протоколов UDP и TCP используется порт 514.
2. Проверьте, что syslog-сервер принимает сообщения в формате CEF.

Настройка сетевой связности

Для настройки сетевой связности выполните следующие шаги:

1. Откройте порты 514 для UDP или TCP на сетевых устройствах.
2. Убедитесь, что источники событий имеют доступ к syslog-серверу.

Настройка источника событий

Убедитесь, что устройство или приложение поддерживает формат CEF и протокол syslog.



Способ настройки отправки событий может отличаться в зависимости от типа источника. Рекомендуем использовать официальную документацию источника при настройке логирования и отправки событий.

Для настройки источника событий для отправки сообщений в формате CEF выполните следующие шаги:

1. Укажите формат отправки — CEF.
2. Задайте адрес syslog-сервера.
3. Укажите порт. В примере ниже введен порт 514.

Пример 4. Пример команды настройки

```
log_format CEF
log_server <syslog-server-IP>
log_port 514
```

Настройка syslog-сервера

Для настройки syslog-сервера выполните следующие шаги:

1. Откройте конфигурационный файл rsyslog в директории **/etc/rsyslog.d/**.
2. Добавьте в файл правило обработки CEF-сообщений:

```
# Настройка для приема сообщений на порте 514 протокол UDP
module(load="imudp")
input(type="imudp" port="514")

# Направление CEF-сообщений в R-Vision SIEM
if $msg contains "CEF:" then {
    action(type="omfwd" Target="<siem>" Port="<port>" Protocol="tcp")
}
```

Здесь:

- **<siem>** — IP-адрес или полное доменное имя (FQDN) узла кластера Kubernetes, на котором запущен коллектор SIEM.
- **<port>** — порт точки входа Syslog для отправки событий на конвейер SIEM — любой свободный порт в диапазоне 30000–32767.

3. Перезапустите syslog-сервер с помощью команды:

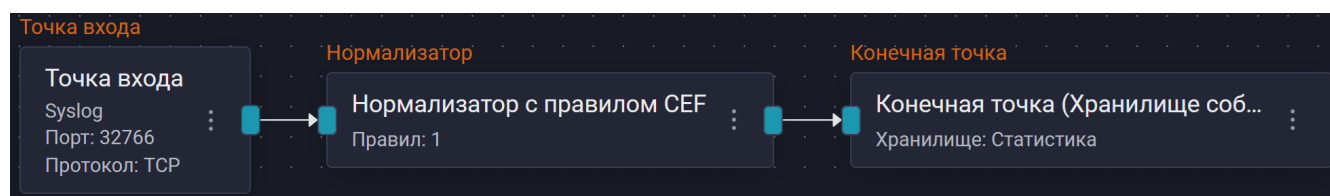
```
sudo systemctl restart rsyslog
```

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Syslog**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [syslog-сервера](#).
 - Протокол: выберите вариант в соответствии с настройками на стороне [syslog-сервера](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Universal CEF** (идентификатор правила: **RV-N-18**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события источника.



Найти события источника в хранилище можно по следующему фильтру:

```
dproduct = "<Device Product>"
```

где **<Device Product>** — имя продукта, установленное вендором в поле **Device**

Product CEF-заголовок события:

```
Jan 18 11:07:53 host CEF:Version|Device Vendor|Device Product|Device  
Version|Device Event Class ID|Name|Severity|[Extension]
```

Проверка получения событий

Для проверки корректности настройки источника событий выполните следующие шаги:

1. Используйте утилиту **logger** для отправки тестового сообщения:

```
logger -P 514 -n <syslog-server-IP>  
"CEF:0|Vendor|Product|Version|SignatureID|Name|Severity|Extension"
```

где **<syslog-server-IP>** — адрес syslog-сервера.

2. Убедитесь, что события поступают в R-Vision SIEM и записываются в указанное хранилище.
3. Проверьте логи на syslog-сервере для подтверждения получения отправленного сообщения.
4. В случае отсутствия событий в SIEM убедитесь в корректности настроек порта, протокола и формата сообщений на стороне источника и syslog-сервера.

Решение проблем

Некорректный формат события может стать причиной неработающего правила нормализации.

Для устранения проблемы выполните следующие шаги:

1. Проверьте, соответствует ли событие одному из допустимых форматов:

```
CEF:0|Vendor|Product|Version|SignatureID|Name|Severity|Extension  
'Syslog header' CEF:0|Vendor|Product|Version|SignatureID|Name|Severity|Extension
```

2. Удалите из события префикс **syslog** и проверьте, работает ли правило нормализации.
3. Если проблема сохраняется, проверьте событие на наличие лишних символов. Например, после разделителя **|** не должно быть пробелов.

Пример с ошибкой:

```
CEF:0|R-Vision|SEA|1.0|empty|empty|2| RealTime=09/13/2024 07:49:57
```

Корректный формат:

```
CEF:0|R-Vision|SEA|1.0|empty|empty|2|RealTime=09/13/2024 07:49:57
```

4. В RObject-конфигурации правила нормализации замените VRL-функцию `parse_cef` на `rv_parse_cef`, которая поддерживает заголовки syslog. Например:

```
normalizer: !vrl |
  # event = parse_cef(.raw.message) ?? {}
  event = rv_parse_cef(.raw.message) ?? {}
```

Redis Enterprise

Данное руководство описывает процесс настройки сбора и отправки событий Redis в R-Vision SIEM.

Настройка Redis

Настройка Redis состоит из следующих этапов:

1. [Настройка подсистемы журналирования Redis](#)
2. [Настройка отправки событий Redis](#)

Настройка подсистемы журналирования Redis

Чтобы настроить аудит БД Redis Enterprise:

1. Откройте инструмент rladm командой:

```
/opt/redislabs/bin/rladm
```

2. Настройте аудит кластера с помощью команды:

```
cluster config auditing db_conns audit_protocol TCP audit_address <connector_ip>  
audit_port <connector_port>
```

Здесь:

- **<connector_ip>** — IP-адрес коннектора.
- **<connector_port>** — порт коннектора.

3. Настройте аудит для экземпляров баз данных:

- a. Для новых экземпляров выполните команду:

```
tune cluster db_conns_auditing enabled
```

- b. Для уже имеющихся экземпляров выполните команду:

```
tune db db:1 db_conns_auditing enabled
```

Настройка отправки событий Redis

Чтобы отправлять события Redis, настройте аудит управления кластером.

Для этого создайте файл **/etc/rsyslog.d/10-redis.conf** со следующим содержимым:

```

module(load="imfile" mode="inotify")
input(
    type="imfile"
    File="event_log"
    Tag="RedisEnterpriseSoftware"
    Severity="info"
    Facility="local7"
)

if $syslogtag == 'RedisEnterpriseSoftware' then {
    action(type="omfwd" Target="" Port="" Protocol="")
    stop
}

```

Здесь:

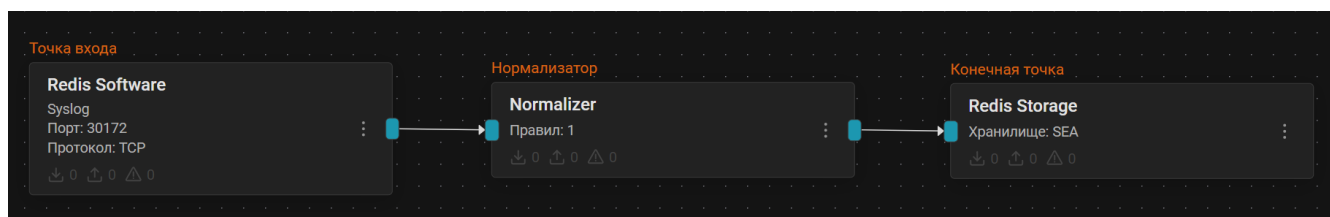
- **<target>** — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- **<port>** — порт точки входа Syslog в конвейере SIEM.
- **<protocol>** — сетевой протокол: **tcp** или **udp**.

Настройка интеграции с R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Ресурсы** → **Коллекторы** и создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Syslog.
 - Порт точки входа и протокол: в соответствии с настройками на стороне [Redis](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом Redis Enterprise Software (идентификатор правила: RV-N-105). Соедините нормализатор с точкой входа.
4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
5. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события Redis.

Найти события Redis в хранилище можно по следующему фильтру:

```
dproduct = "Redis Enterprise Software"
```



Изменить фильтр ×

☐ Инвертировать (NOT)

Поле

dproduct ▼

Оператор

= ▼

Значение

Redis Enterprise Software ×

☐ Настроить заголовок

Отменить

Сохранить

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

SberTech (СберТех)

Данный раздел содержит список систем для настройки от компании SberTech (СберТех):

- [Pangolin SE](#)

Pangolin SE

Данное руководство описывает процесс настройки пересылки логов аудита с сервера Pangolin SE в R-Vision SIEM с использованием службы rsyslog.

Подготовка сервера Pangolin SE

Для настройки пересылки логов аудита через syslog выполните шаги, перечисленные ниже.

Настройка конфигурации PostgreSQL

1. Откройте конфигурационный файл `/pgdata/<product-version>/data/postgresql.conf`.

Здесь:

- `<product-version>` — версия установленного экземпляра Pangolin SE.

2. Отредактируйте значения параметров конфигурации следующим образом:

```
listen_addresses = '*'
log_destination = 'syslog'
logging_collector = on
log_min_messages = debug5
log_min_error_statement = debug5
log_checkpoints = on
log_connections = on
log_disconnections = on
log_error_verbosity = verbose
# Для префикса log_line_prefix написано регулярное выражение в правиле нормализации SIEM
log_line_prefix = '%m [%p] %u %r '
```

3. Перезапустите экземпляр Pangolin SE:

```
pg_ctl -D /pgdata/<product-version>/data/ -l /pgerrorlogs/<product-version>/postgresql.log restart
```

Здесь:

- `<product-version>` — версия установленного экземпляра Pangolin SE.

Настройка службы rsyslog

1. Откройте конфигурационный файл `/etc/rsyslog.d/10-pangolin.conf`.
2. Добавьте следующее правило:

```
if $programname == 'postgres' or $syslogtag == 'postgres' then {  
    action(type="omfwd" Target="<target>" Port="<port>" Protocol="<protocol>")  
    stop  
}
```

Здесь:

- **<target>** — IP-адрес или полное доменное имя (FQDN) централизованного syslog-сервера, с которого будет осуществляться отправка сообщений в SIEM.
- **<port>**:
 - либо порт точки входа Syslog в конвейере SIEM — любой свободный порт больше 30000;
 - либо порт сервера rsyslog — **514**.
- **<protocol>** — **tcp** или **udp**.

3. Перезапустите службу rsyslog:

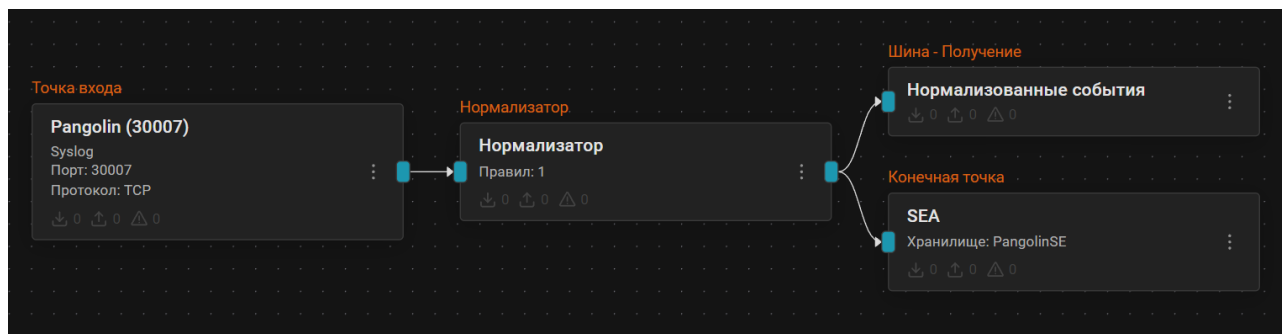
```
sudo systemctl restart rsyslog
```

Настройка интеграции с R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте в конвейер элемент **Точка входа** со следующими параметрами:
 - a. **Тип точки входа** — Syslog;
 - b. **Порт** и **Протокол** — значения должны совпадать с [настройками на стороне Pangolin SE](#).
3. Соедините с точкой входа **Нормализатор** с добавленным правилом нормализации для SberTech Pangolin SE с ID **RV-N-107**.
4. Соедините с нормализатором шину. Настройте данный элемент на получение данных.
5. Соедините с нормализатором конечную точку типа **Хранилище событий**.
6. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера



Если настройка выполнена корректно, в хранилище начнут поступать события Pangolin SE.

Список типов событий

- Connection
- Disconnection
- REQUEST
- TRANSACTIONS
- TABLE
- INDEX
- TABLE_DATA_MANIPULATION
- PG_DUMP
- PG_RESTORE
- REPLICATION
- AUDIT
- START_STOP_SERVER

Таблица маппинга

Параметр	Значение
dvendor	SberTech
dproduct	Platform V Pangolin SE
dversion	6+
name	
cat	<code>parsed.NAME</code>
sourceSessionId	<code>parsed.ID</code>
dvchost	<code>.raw.hostname</code>
severity	<code>get(severityMap, [.raw.severity])</code>
msg	<code>parsed.MSG .raw.message</code>
rt	<code>parse_timestamp(parsed.DATE,"%Y-%m-%d %X%.f")</code>
outcome	Success/Failure
suser	<code>parsed.SUSER</code>

Параметр	Значение
shost	<code>parsed.SHOST</code>
spt	<code>to_int(parsed.SPORT)</code>
request	<code>parsed.MSG</code>
objPath	
objName	
duser	
accessList	<code>accessList = parsed2.privileges</code>

Solar (Солар)

Данный раздел содержит список систем для настройки от компании Solar (Солар):

- [Solar Dozor](#)

Solar Dozor

Данное руководство содержит инструкции по настройке подключения Solar Dozor к системе R-Vision SIEM.

Настройка syslog-ng

1. Проверьте, что в системе установлен инструмент syslog-ng. При необходимости установите его с помощью команды:

```
apt install syslog-ng
```



У учетной записи должны быть привилегии для установки сторонних пакетов.

2. Создайте конфигурацию источника, как описано в документации Dozor. Разместите ее в файле `/etc/syslog-ng/conf.d/dozor.conf`. Если настройка выполнена корректно, то записанные события будут собираться в директории `/var/log/dozor`:

Пример 5. Пример конфигурации

```
@define allow-config-dups 1
# Адрес и порт сервера syslog:
@define REMOTE_SERVER "c7-syslog.example.com"
@define REMOTE_PORT 10514
filter f_dozor_unit {match("dozor" value (".journald._SYSTEMD_UNIT"));};
filter f_syslog3 { not facility(auth, authpriv, mail) and not filter(f_debug) and
not filter(f_dozor_unit);
};
destination d_tcp_q {
    syslog("`REMOTE_SERVER`" transport("tcp") port(`REMOTE_PORT`)
    disk-buffer(
        reliable(yes)
        dir("/var/lib/syslog-ng")
        disk-buf-size(524288000)
        mem-buf-size(134217728)
        qout-size(10000)
    )
};
destination d_dozor {
    file("/var/log/dozor/${PROGRAM}.log"
    create-dirs(yes) dir-group("dozor") dir-owner("dozor") dir-perm(0755)
```

```

    group("dozor") owner("dozor") perm(0640)
    );
};
log {
    source(s_src); filter(f_dozor_unit); destination(d_dozor);
};
log {
    source(s_src);
    filter(f_dozor_unit);
    destination(d_tcp_q);
    flags(final,flow-control);
};

```

3. Найдите все необходимые файлы логов в директории `/var/log/dozor` следующей командой:

```
find /var/log/dozor -type f -printf 'file("%p" flags(no-parse));\n
```

4. Дополните `dozor.conf` следующим содержимым:

```

    source sys_input {
        file("/var/log/dozor/software-center-database.log" flags(no-parse));
        <files>
    };

    destination d_siem {
        network("<target>" port(<port>) transport(<protocol>));
    };

    log {
        source(sys_input);
        destination(d_siem);
    };

```

Здесь:

- `<files>` — источники `file()` с указанием путей к файлам, полученным на предыдущем шаге;
- `<target>` — IP-адрес или полное доменное имя кластера Kubernetes, где будет запущен конвейер для обработки событий;
- `<port>` — порт, на который принимаются события;
- `<protocol>` — какой протокол использовать (`tcp` или `udp`).

5. Перезагрузите службу syslog-ng командой:

```
systemctl restart syslog-ng
```

6. Проверьте, что события отправляются командой:

```
tail -f /var/log/syslog
```

Настройка интеграции с R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие шаги:

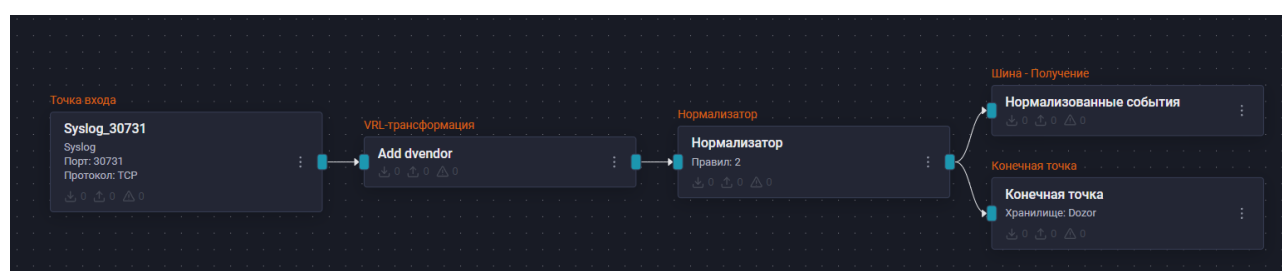
1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - a. **Тип точки входа** — Syslog;
 - b. **Порт точки входа** и **Протокол** — в соответствии с настройками на стороне [сервера syslog](#);
3. Добавьте на конвейер элемент **VRL-трансформация** со следующим кодом:

```
.dvendor = "Solar"  
.dproduct = "Dozor"
```

Соедините VRL-трансформацию с точкой входа.

4. Добавьте на конвейер **Нормализатор** с правилом **Solar Dozor** (идентификатор RV-N-113). Соедините нормализатор с VRL-трансформацией.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
6. Для отправки событий в коррелятор добавьте шину, настроенную на получение, и соедините ее с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера



Squid

Данное руководство описывает процесс настройки сбора и отправки событий Squid в R-Vision SIEM.

Настройка Squid

Описание подсистемы журналирования

По умолчанию журнал событий сервиса Squid хранится в каталоге `/var/log/squid`. В нём имеются следующие файлы с событиями:

- **access.log** — содержит обращения сетевых хостов к ресурсам.
- **cache.log** — содержит сообщения об ошибках и другую информацию, необходимую для отладки.

Настройка подсистемы журналирования Squid

Чтобы выполнить настройку подсистемы журналирования Squid, настройте корректный формат сообщений на сервере Squid. Для этого:

1. Добавьте в конец файла `/etc/squid/squid.conf` следующие строки:

```
logformat custom %>a - %un [%tl] "%rm %ru %Sh/%<A %mt %Ss" %03>Hs %<st  
access_log daemon:/var/log/squid/access.log custom
```

2. Перезагрузите Squid для применения настроек:

```
systemctl restart squid
```

Настройка отправки событий Squid

Чтобы настроить отправку событий Squid, настройте передачу событий из файла, для этого:

1. Создайте файл `/etc/rsyslog.d/10-squid.conf` со следующим содержимым:

```
module(load="imfile" mode="inotify")  
input(  
    type="imfile"  
    File="access"  
    Tag="Squid"  
    Severity="info"  
    Facility="local4"  
)  
  
if $syslogtag == 'Squid' then {  
    action(type="omfwd" Target="" Port="" Protocol="")  
    stop  
}
```



```
}
```

Здесь:

- **<target>** — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- **<port>** — порт точки входа Syslog в конвейере SIEM.
- **<protocol>** — сетевой протокол: **tcp** или **udp**.

2. Перезапустите службу `rsyslog.service` с помощью команды:

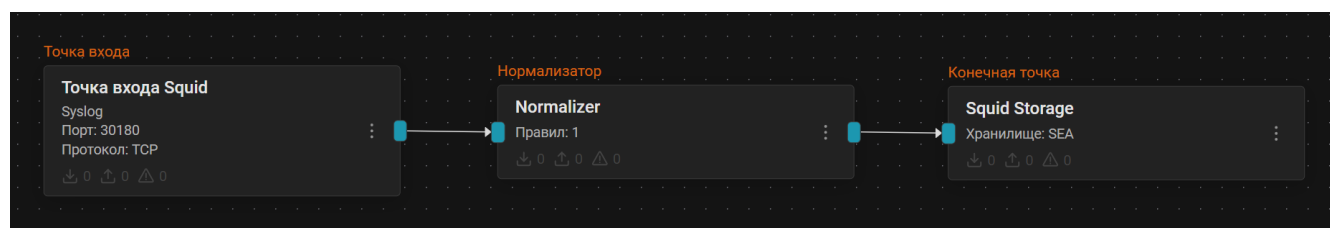
```
systemctl restart rsyslog.service
```

Настройка интеграции с R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Ресурсы** → **Коллекторы** и создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Syslog.
 - Порт точки входа и протокол: в соответствии с настройками на стороне [Squid](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом Squid (идентификатор правила: RV-N-117). Соедините нормализатор с точкой входа.
4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
5. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события Squid.



Найти события Squid в хранилище можно по следующему фильтру:

```
dproduct = "Squid"
```

Изменить фильтр

☐ Инвертировать (NOT)

Поле

dproduct

Оператор

=

Значение

Squid

☐ Настроить заголовок

Отменить

Сохранить

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Usergate (Entensys)

Данный раздел содержит список систем для настройки от компании UserGate, также известной как Entensys.

- [Usergate UTM](#)

Usergate UTM

Данное руководство описывает настройку сбора событий универсального шлюза безопасности UserGate и их отправки в хранилище R-Vision SIEM.

Настройка Usergate UTM для отправки логов на сервер syslog

Чтобы настроить Usergate UTM для отправки логов:

1. Авторизуйтесь в веб-интерфейсе Usergate UTM под учетной записью с правами администратора.



Данные учетной записи, созданной по умолчанию, см. в [документации Usergate UTM](#).

2. Перейдите в раздел **Logs & Reports**.
3. Добавьте новый Syslog-сервер. Для этого:
 - Нажмите **Add Log Source**.
 - Выберите **Syslog** в качестве типа источника логов.
 - Введите IP-адрес и порт коллектора SIEM.
4. Настройте параметры отправки логов:
 - Укажите, какие типы событий и уровни важности логов нужно отправлять.
 - При необходимости настройте фильтры и правила для обработки логов.

Настройка Usergate UTM для сбора логов

Чтобы настроить Usergate UTM для сбора логов с устройств:

- В веб-интерфейсе Usergate UTM перейдите в раздел **Devices**.
- Добавьте устройства, с которых вы хотите собирать логи.
- Настройте параметры сбора логов для каждого устройства.

Настройка коллектора SIEM для сбора логов.

Для интеграции источника с R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - а. **Тип точки входа** — Syslog;

б. **Порт точки входа** и **Протокол** — в соответствии с настройками на [устройстве Usergate](#).

3. Добавьте на конвейер элемент **VRL-трансформация** со следующим кодом:

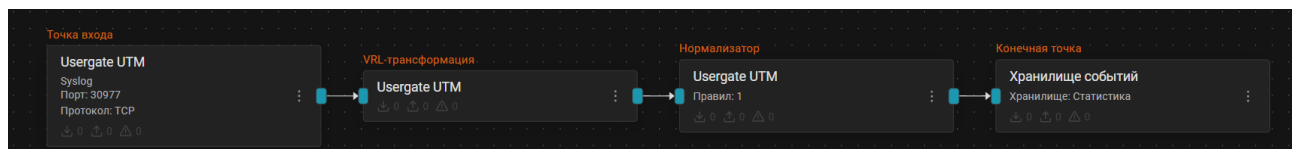
```
.dvendor = "Usergate"  
.dproduct = "UTM"
```

4. Добавьте на конвейер **Нормализатор** с правилом **Usergate UTM 6** (идентификатор **RV-N-36**). Соедините нормализатор с VRL-трансформацией.

5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.

6. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера



VMware

Данный раздел содержит список систем для настройки от компании VMware:

- [ESXi](#)
- [Horizon](#)
- [vCenter](#)

ESXi

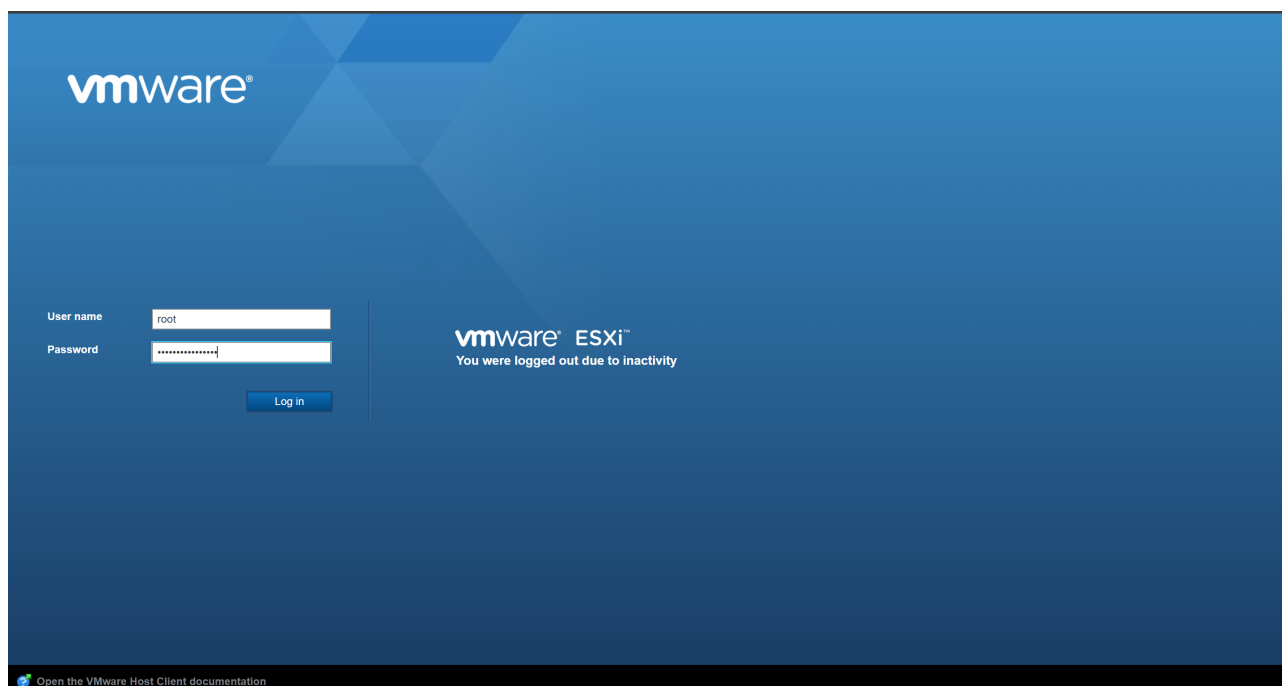
Данное руководство описывает процесс отправки событий источника VMware ESXi в R-Vision SIEM.

- [Настройка VMware ESXi](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

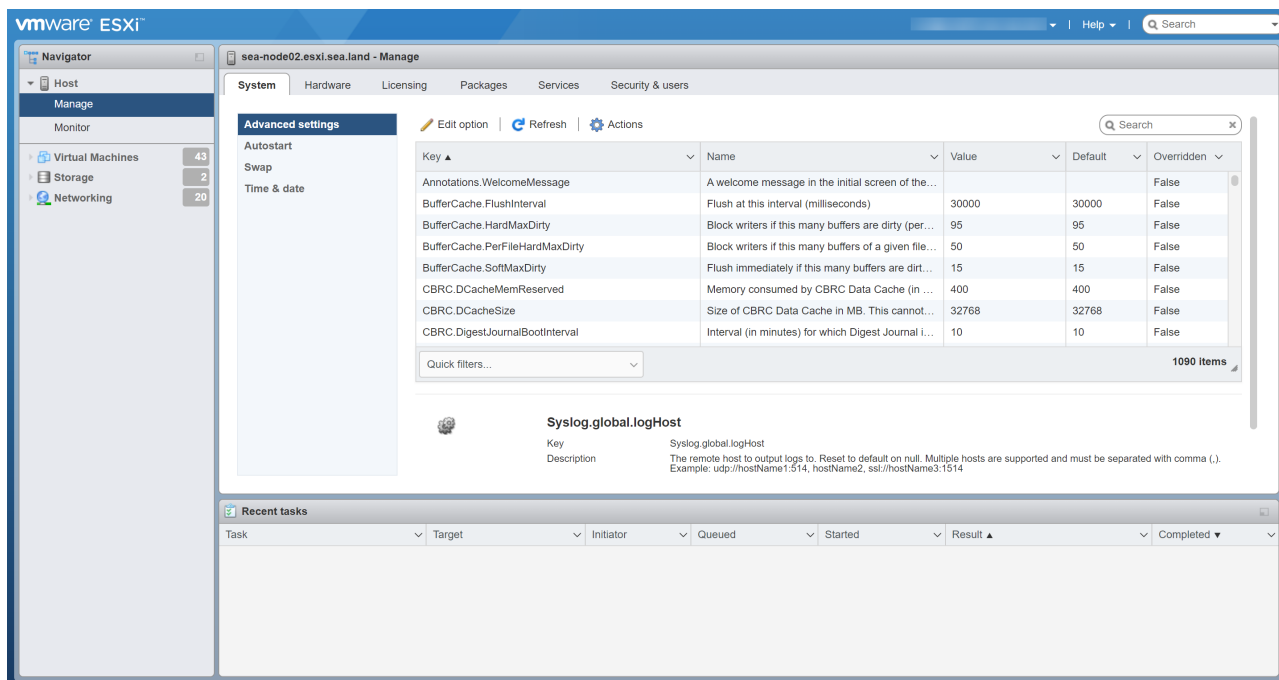
Настройка VMware ESXi

Для настройки источника выполните следующие шаги:

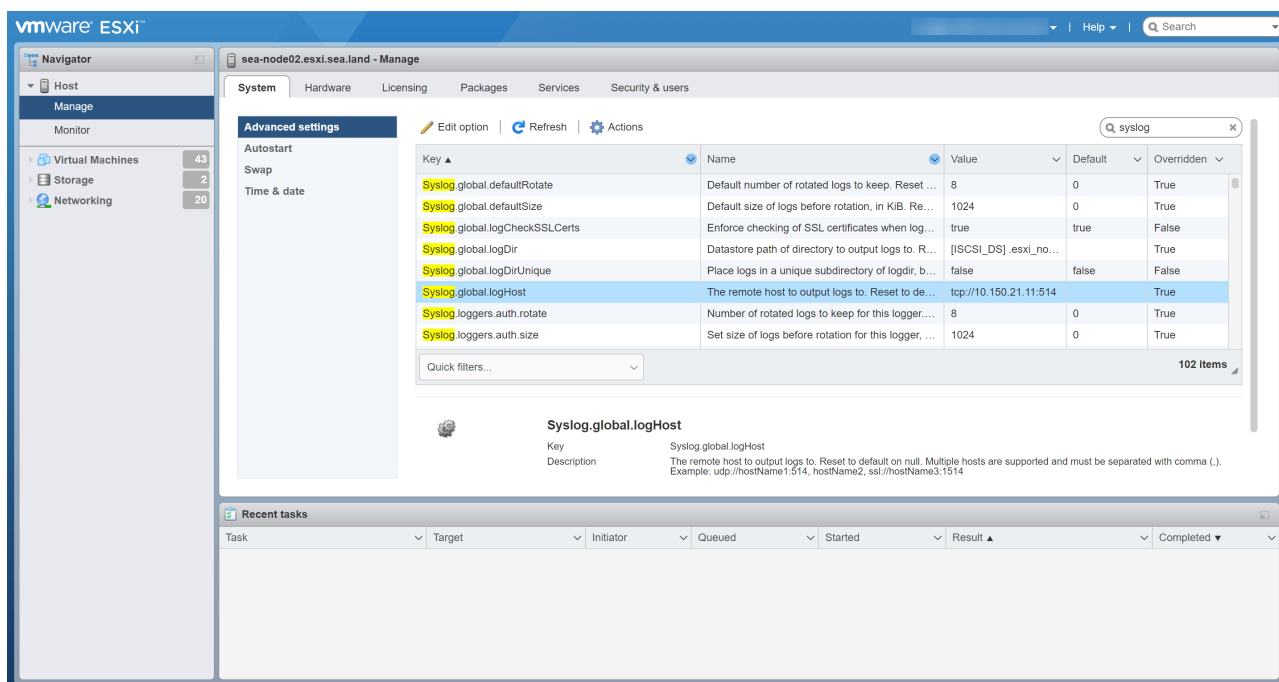
1. Войдите в web-интерфейс VMware ESXi.



2. Перейдите в раздел **Manage**.

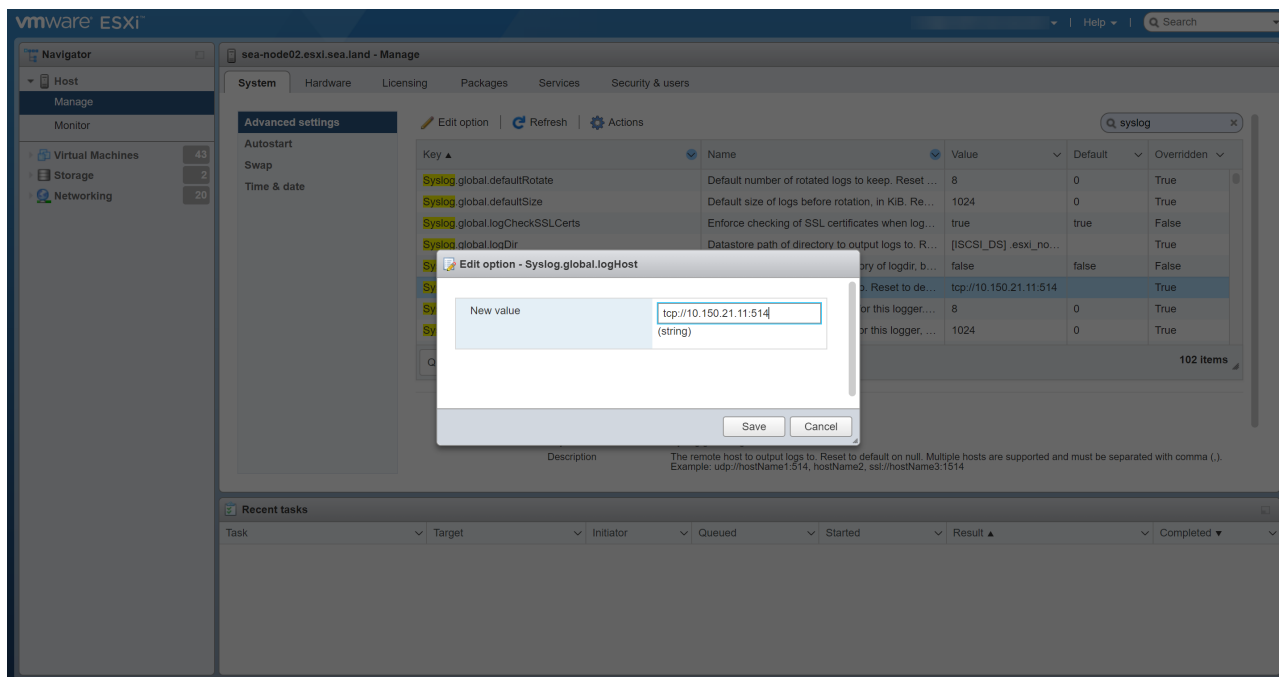


3. На вкладке **System** в разделе **Advanced settings** выберите параметр **Syslog.global.logHost**.

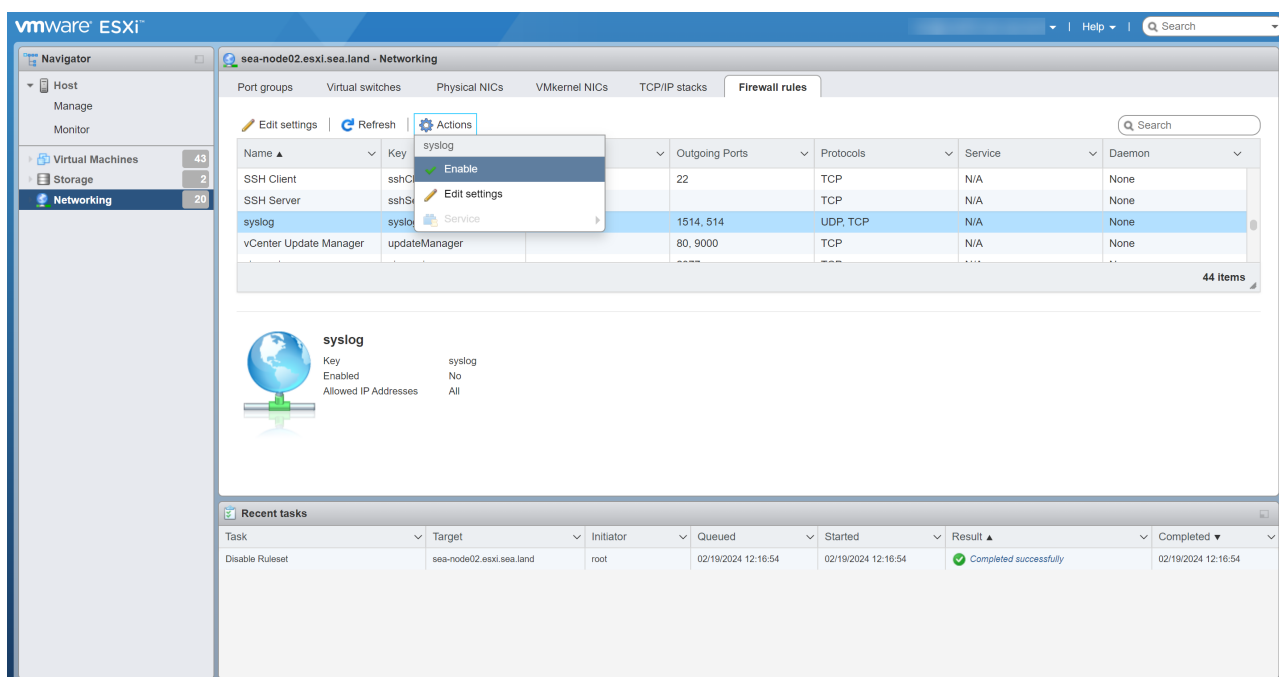


4. Нажмите на кнопку **Edit option**. Откроется окно настроек параметра.

5. Укажите адрес коллектора SIEM, порт точки входа и протокол.



6. Нажмите на кнопку **Save**.
7. Перейдите в раздел **Networking**.
8. На вкладке **Firewall rules** выберите из выпадающего списка **Actions** опцию **Enable**, чтобы включить сервис **syslog**.



9. Настройка на стороне источника завершена.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:

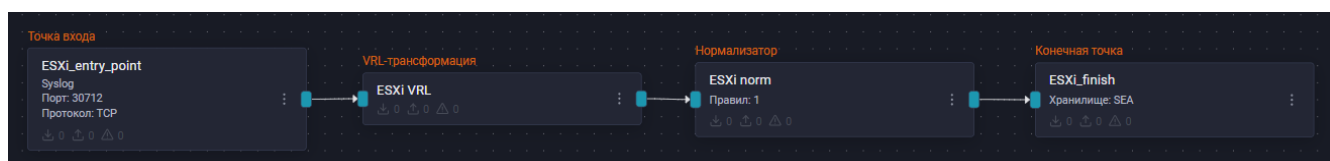
- Название: введите название точки входа.
- Тип точки входа: выберите вариант **Syslog**.
- Порт точки входа: введите значение в соответствии с настройками на стороне [ESXi](#).
- Протокол: выберите вариант в соответствии с настройками на стороне [ESXi](#).

3. Добавьте VRL-трансформацию:

```
.dproduct = "ESXi"
```

4. Соедините добавленную точку входа и VRL-трансформацию.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **VMware ESXi** (идентификатор правила: **RV-N-119**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события ESXi.

Найти события ESXi в хранилище можно по следующему фильтру:

```
dproduct = "ESXi"
```



Добавить фильтр

☐ Инvertировать (NOT)

Поле

dproduct

Оператор

=

Значение

ESXi

☐ Настроить заголовок

Отменить

Добавить

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Horizon

Данное руководство описывает процесс настройки сбора и отправки событий платформы виртуализации рабочих мест VMWare Horizon в R-Vision SIEM.

Настройка сбора событий на стороне источника

Настройка подсистемы журналирования

Чтобы настроить подсистему журналирования событий в VMware Horizon, выполните следующие шаги:

1. Перейдите в раздел **Event Configuration**.
2. На вкладке **Event Database** нажмите на кнопку **Edit**.
3. Введите данные базы для сохранения событий:

Edit Event Database



Asterisk (*) denotes required field

* Database Server

Database Type

* Port

* Database Name

* User Name

* Password

* Confirm Password

4. Нажмите на кнопку **OK**. Логирование настроено.

Настройка отправки событий в SIEM на стороне источника

Для того чтобы настроить отправку событий в SIEM через веб-интерфейс VMware Horizon, выполните следующие шаги:

1. Перейдите в раздел **Event Configuration**.
2. На вкладке **Syslog** нажмите на кнопку **Add**.
3. В открывшемся окне укажите адрес и порт syslog-сервера:
 - a. В поле **Server Address** введите IP-адрес централизованного syslog-сервера, с которого будет осуществляться отправка сообщений в SIEM.
 - b. В поле **UDP Port** введите 514.

Add Syslog Server



Asterisk (*) denotes required field

Add the server, to send syslog events.

* Server Address

* UDP Port

Cancel

OK

4. Нажмите на кнопку **OK**. Отправка событий в SIEM на стороне источника настроена.

Настройка syslog-сервера

Для настройки syslog-сервера выполните следующие шаги:

1. Откройте конфигурационный файл rsyslog (**/etc/rsyslog.conf** или **/etc/rsyslog.d/**).
2. Добавьте правило обработки CEF-сообщений:

```
if $hostname == 'vmware.horizon.com' then {  
    action(type="omfwd" Target="siem.com" Port="<port>" Protocol="tcp")  
    stop  
}
```

Здесь:

- **<port>** — порт точки входа Syslog в конвейере SIEM — любой свободный порт больше 30000.

3. Перезапустите rsyslog для применения изменений:

```
sudo systemctl restart rsyslog
```

Настройка интеграции с R-Vision SIEM

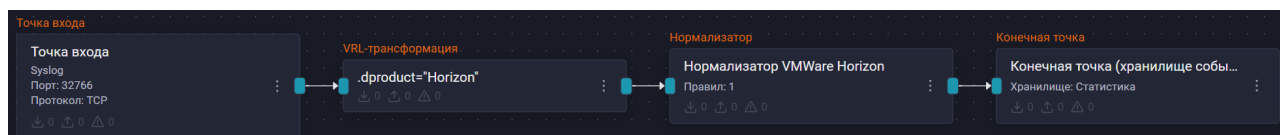
Для интеграции источника с R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте в конвейер элемент **Точка входа** со следующими параметрами:
 - a. **Тип точки входа** — Syslog.
 - b. **Порт точки входа** — в соответствии с настройками на стороне [syslog-сервера](#).
 - c. **Протокол** — TCP.
3. Добавьте VRL-трансформацию:

```
.dproduct="Horizon"
```

4. Соедините с VRL-трансформацией **Нормализатор** с добавленным правилом для VMware Horizon.
5. Соедините с нормализатором конечную точку типа **Хранилище событий**.
6. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера



Список типов событий

Описание событий доступно на [GitHub](#).

vCenter

Данное руководство описывает процесс отправки событий источника VMware vCenter в R-Vision SIEM.

- [Настройка VMware vCenter](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Настройка VMware vCenter

Для настройки источника выполните следующие шаги:

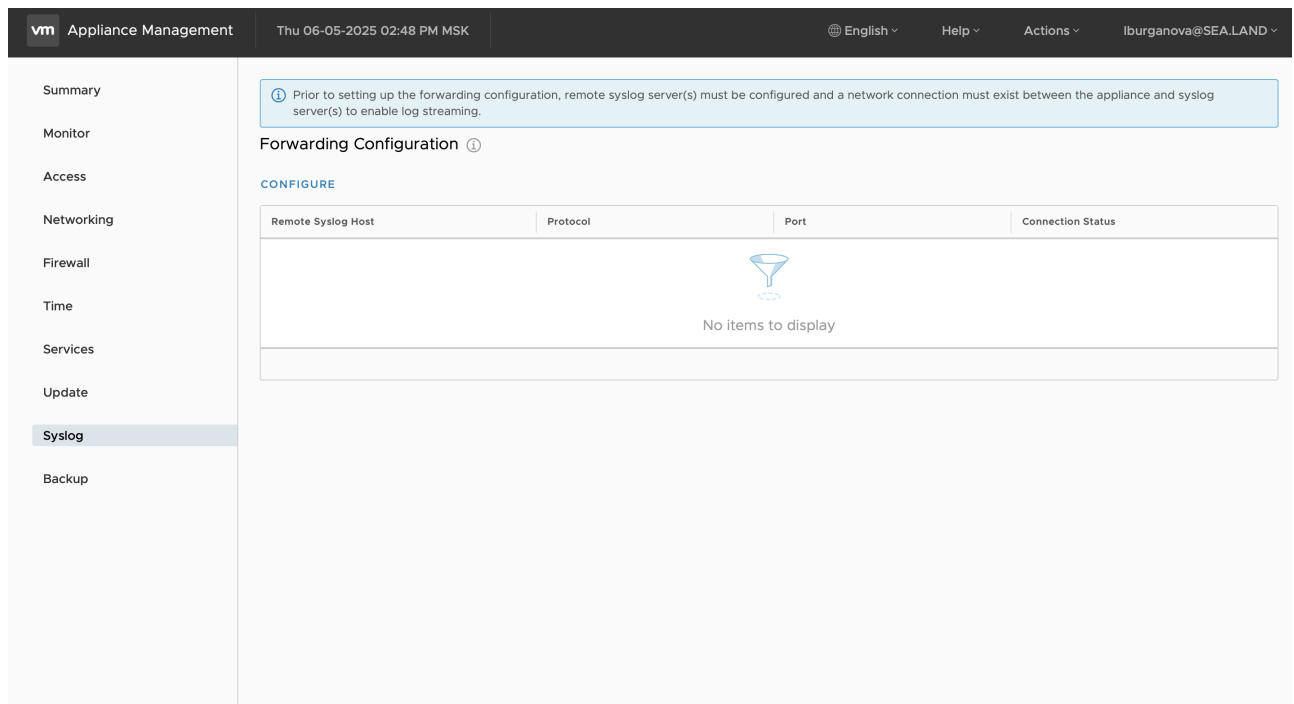
1. Войдите в интерфейс управления VMware vCenter Server Appliance (VCSA) Management:

- a. Откройте веб-браузер.
- b. Перейдите по адресу:

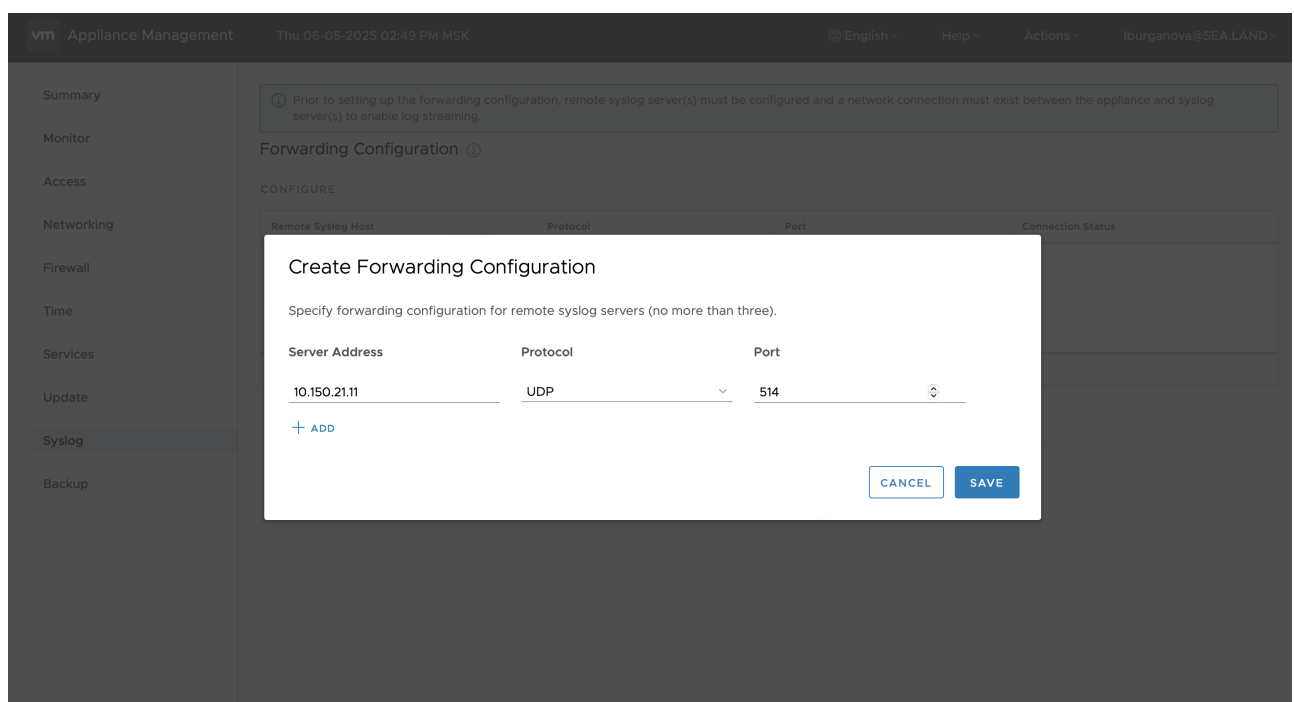
`https://<IP-адрес-или-FQDN>:5480`

где **<IP-адрес-или-FQDN>** — актуальные данные вашей системы.

2. Перейдите в раздел **Syslog**.
3. Нажмите на кнопку **CONFIGURE**. Откроется окно создания конфигурации переадресации.



4. Укажите адрес удаленного syslog-сервера или конвейера в SIEM, а также протокол и порт.



5. Нажмите на кнопку **SAVE**.
6. Настройка на стороне источника завершена.

Настройка в R-Vision SIEM

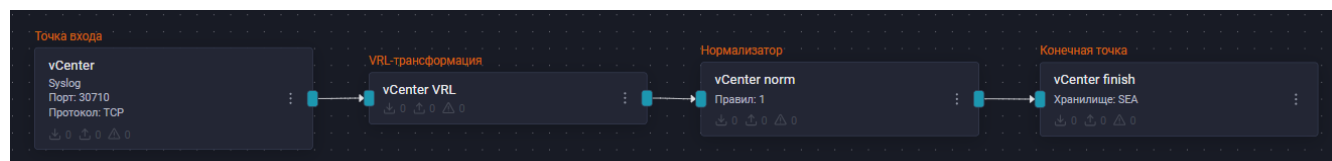
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Название: введите название точки входа.
 - Тип точки входа: выберите вариант **Syslog**.
 - Порт точки входа: введите значение в соответствии с настройками на стороне [vCenter](#).
 - Протокол: выберите вариант в соответствии с настройками на стороне [vCenter](#).
3. Добавьте VRL-трансформацию:

```
.dproduct = "vCenter"
```

4. Соедините добавленную точку входа и VRL-трансформацию.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **VMware vCenter** (идентификатор правила: **RV-N-121**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события vCenter.



Найти события vCenter в хранилище можно по следующему фильтру:

```
dproduct = "vCenter"
```

Добавить фильтр

☐ Инвертировать (NOT)

Поле

dproduct

Оператор

=

Значение

vCenter

☐ Настроить заголовок

Отменить

Добавить

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Zabbix

Данная инструкция описывает настройку сбора событий на сервере Zabbix и их последующей отправки в R-Vision SIEM.

- [Предварительные требования](#)
- [Настройка Zabbix](#)
 - [Описание подсистемы журналирования](#)
 - [Настройка журналирования](#)
 - [Создание сервисной учетной записи](#)
 - [Включение сбора событий аудита](#)
- [Настройка в R-Vision SIEM](#)
- [Таблица маппинга](#)

Предварительные требования

Перед настройкой Zabbix убедитесь, что у вас имеется:

- Сетевой доступ к БД;
- Учетная запись в СУБД с правами администратора на доступ к БД zabbix в вашей системе управления базами данных (далее — СУБД).

Настройка Zabbix

Описание подсистемы журналирования

Zabbix записывает свои события в базу данных zabbix вашей СУБД.



База данных zabbix создается автоматически при установке сервера Zabbix версии 6.0 и выше. Если вы используете более старую версию, обратитесь к [документации Zabbix](#) для первичной настройки.



Названия таблиц в вашей СУБД могут отличаться от названий таблиц, приведенных в данной инструкции. Если вы не можете найти необходимые таблицы в вашей СУБД или получаете ошибки существования таблиц, обратитесь к [разделу документации, соответствующему вашей версии сервиса](#), для поиска соответствий.

Настройка журналирования

Создание сервисной учетной записи

Для осуществления сбора логов из базы данных требуется подключиться к ней с использованием специализированной учетной записи (далее — УЗ). Данная УЗ предназначена для обеспечения доступа к базе данных автоматическим сервисом.

Чтобы создать сервисную УЗ, подключитесь к СУБД с правами администратора. Для этого выполните следующие действия на сервере с установленной СУБД:



В качестве примера используется СУБД PostgreSQL.

1. Выполните следующую команду от имени пользователя с правами администратора:

```
sudo -u <admin> psql
```

где **<admin>** — название учетной записи с правами администратора.

2. Создайте сервисную учетную запись, выполнив следующие команды:

```
CREATE USER "<new_user>";  
ALTER ROLE <new_user> WITH PASSWORD '<passw0rd>';
```

где:

- **<new_user>** — имя созданной УЗ.
 - **<passw0rd>** — пароль для созданной УЗ.
3. Предоставьте права на подключение к базе данных и чтение таблицы. К правам пользователя предъявляются следующие требования:
 - возможность подключения к базе данных zabbix;
 - возможность выполнения SELECT-запросов к таблицам audit и alerts базы данных zabbix.

Пример 6. Пример запроса для создания пользователя в PostgreSQL 14.0

```
GRANT CONNECT ON DATABASE zabbix TO <new_user>;  
GRANT USAGE ON SCHEMA public TO <new_user>;  
GRANT SELECT ON ALL TABLES IN SCHEMA public TO <new_user>;
```

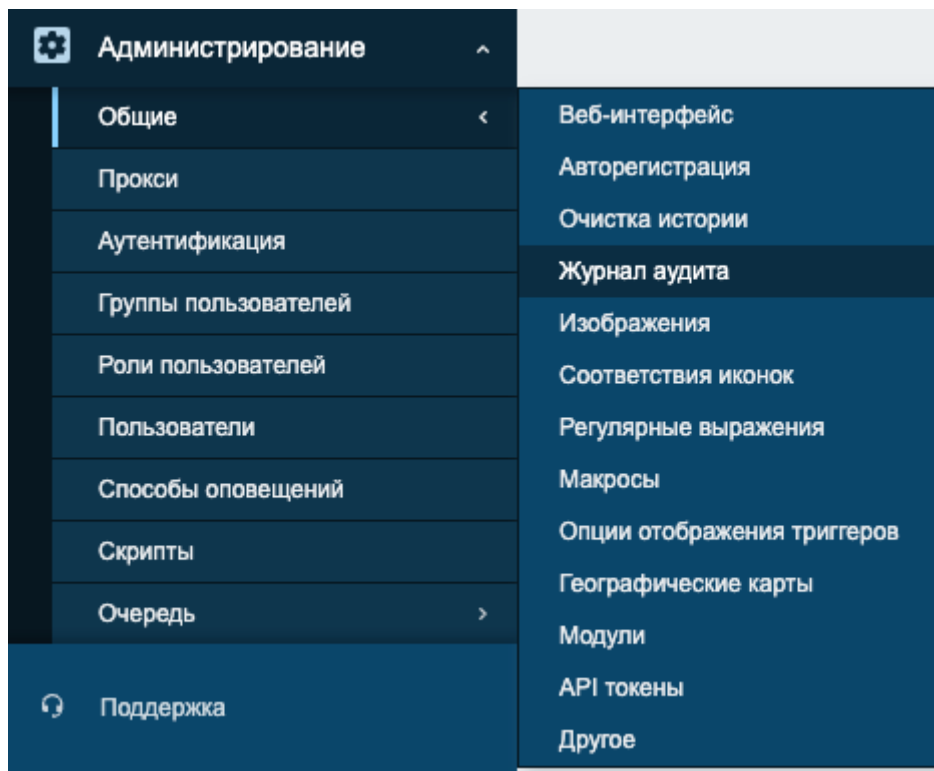


Вы также можете ограничить доступ УЗ к таблицам, предоставив SELECT-привилегии только для таблиц audit и alerts.

Включение сбора событий аудита

Для настройки логирования событий аудита в Zabbix выполните следующие действия:

1. Подключитесь к веб-интерфейсу Zabbix.
2. Войдите в веб-интерфейс с помощью УЗ, имеющей права администратора Zabbix.
3. Перейдите в раздел **Администрирование** → **Общие** → **Журнал аудита**.



Если вы используете английскую версию Zabbix, перейдите в раздел **Administration** → **General** → **Audit Log**.

4. Установите флажок напротив параметра **Включить журналирование аудита**.



В английской версии Zabbix установите флажок напротив параметра **Enable Audit Log**.

Журнал аудита ▾

5. После настройки журналирования события аудита начнут записываться в вашу СУБД.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
 - а. Перейдите в **Ресурсы** → **Секреты** → **Создать**.

b. В раскрывшемся окне создания секрета заполните поля:

- Название: введите название секрета.
- Описание (опционально): опишите, для чего будет использоваться секрет.
- Тип секрета: выберите вариант **Строка подключения**.
- Строка подключения — введите строку вида:

```
jdbc:postgresql://<ip-  
address>:<port>/zabbix?user=<svc_rvision_siem>&password=<passw0rd>
```

где:

- **<ip-address>** — данные вашего сервера СУБД zabbix.
- **<port>** — порт подключения к вашей СУБД. По умолчанию используется порт **5432**.
- **<svc_rvision_siem>** — пример имени пользователя для подключения к СУБД zabbix.
- **<passw0rd>** — пример пароля пользователя СУБД zabbix.

Создание секрета

Название
Zabbix

Описание (опционально)
Введите описание

Тип секрета
Строка подключения

Строка подключения
jdbc:postgresql://<ip-address>:<port>/zabbix?
<user=svc_rvision_siem>&<password=passw0rd>

Отменить Создать

c. Нажмите на кнопку **Создать**.

2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.

3. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:

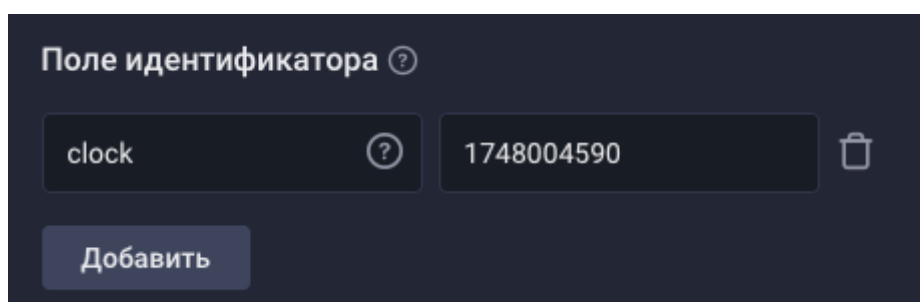
- Название: введите название точки входа.

- Тип точки входа: выберите вариант **Database**.
- Драйвер базы данных: выберите вариант **PostgreSQL**.
- Адрес подключения: выберите секрет, созданный ранее.
- SQL-запрос — для сбора логов из таблицы audit добавьте следующую команду:

```
SELECT 'Zabbix_Audit' AS appname,
auditid,
username,
clock,
ip,
action,
resourcename,
resourcetype,
details FROM audit WHERE clock > ?::integer ORDER BY clock ASC;
```

- Поле идентификатора: введите ключ **clock** со значением текущего времени в формате Unix time.

Пример указания параметра **Поле идентификатора**:



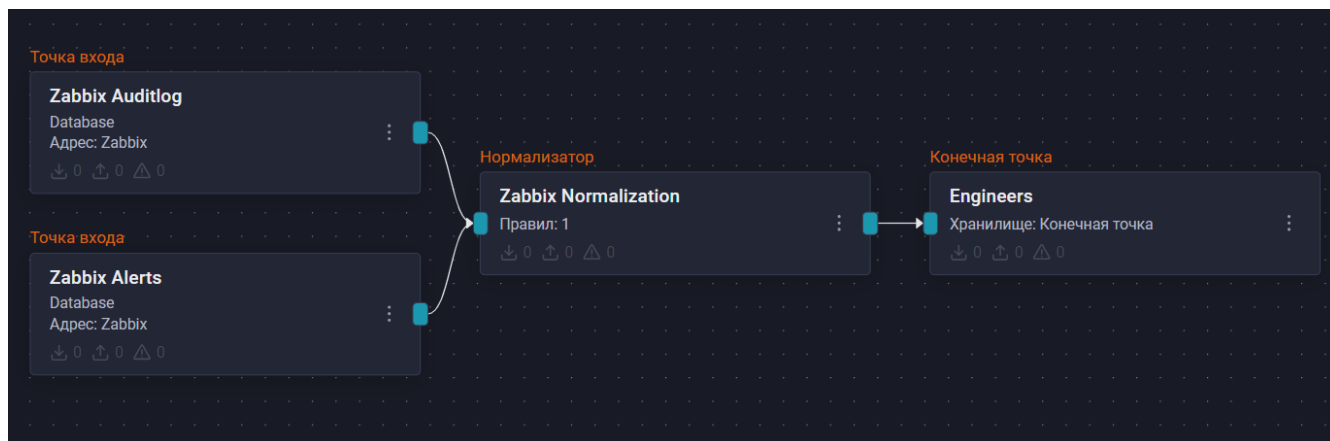
4. Добавьте на конвейер еще один элемент **Точка входа** со следующими параметрами:

- Название: введите название точки входа.
- Тип точки входа: выберите вариант **Database**.
- Драйвер базы данных: выберите вариант **PostgreSQL**.
- Адрес подключения: выберите секрет, созданный ранее.
- SQL-запрос — для сбора логов из таблицы alerts добавьте следующую команду:

```
SELECT 'Zabbix_Alerts' AS appname,
alertid,
actionid,
eventid,
userid,
clock,
subject,
status,
message,
retries FROM alerts WHERE clock > ?::integer ORDER BY clock ASC;
```

- Поле идентификатора: введите ключ **clock** со значением текущего времени в формате Unix time.
- Добавьте на конвейер элемент **Нормализатор** с правилом **Zabbix** (идентификатор правила: **RV-N-124**).
 - Соедините нормализатор с точками входа.
 - Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
 - Соедините конечную точку с нормализатором.
 - Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события Zabbix.

Найти события Zabbix в хранилище можно по следующему фильтру:

```
dproduct = "Zabbix"
```



Добавить фильтр

☐ Инвертировать (NOT)

Поле

dproduct

Оператор

=

Значение

Zabbix

☐ Настроить заголовок

Отменить

Добавить

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по](#)

ссылке.

ИнфоТеКС

Данный раздел содержит список систем для настройки от компании ИнфоТеКС:

- [ViPNet Coordinator 4](#)
- [ViPNet IDS NS](#)
- [ViPNet TIAS](#)

ViPNet Coordinator 4

Данное руководство описывает процесс настройки сбора и отправки событий системы обнаружения компьютерных атак ViPNet Coordinator 4 в R-Vision SIEM.

- [Настройка ViPNet Coordinator 4](#)
- [Настройка в R-Vision SIEM](#)
- [Типы обрабатываемых событий](#)
- [Таблица маппинга](#)

Настройка ViPNet Coordinator 4

Для настройки отправки событий ViPNet Coordinator 4 в SIEM-систему в формате syslog выполните следующие действия:

1. Войдите в интерфейс командной строки ViPNet Coordinator.
2. Перейдите в режим администратора:

```
enable
```

3. Укажите целевой IP-адрес для отправки событий с помощью команды:

```
machine set loghost <IP-адрес коллектора>
```

где **<IP-адрес коллектора>** — адрес коллектора R-Vision SIEM, в рамках которого планируется осуществлять сбор событий ViPNet Coordinator 4.

4. Остановите работу службы iplir:

```
iplir stop
```

5. Откройте файл конфигурации службы iplir:

```
iplir config
```

6. В секции **misc** введите следующие значения:

```
cef_ip = <IP-адрес коллектора>
cef_port = <Порт коллектора>
cef_format= xf
cef_enabled = yes
```

Здесь:

- **<IP-адрес коллектора>** — адрес коллектора R-Vision SIEM, с помощью которого планируется осуществлять сбор событий ViPNet Coordinator 4.
- **<Порт коллектора>** — порт, указанный для сбора событий на конвейере.

7. Сохраните изменения.

8. Закройте файл.

9. Откройте конфигурацию интерфейса, с которого необходимо получать события о трафике:

```
iplir config eth<номер интерфейса>
```

10. В конфигурации интерфейса укажите следующие значения:

```
[db]
maxsize= 50 MBytes
timedif= 60
registerall= on #по умолчанию off
registerbroadcast= off
omittcpclientport= off
registerevents= on

[cef]
# для регистрации всех событий значение - all
# для регистрации заблокированных пакетов - blocked
event= all
```

11. Сохраните изменения с помощью сочетания клавиш CTRL+O.

12. Закройте файл.

13. Включите службу iplir:

```
iplir start
```

14. Добавьте правило фильтрации:

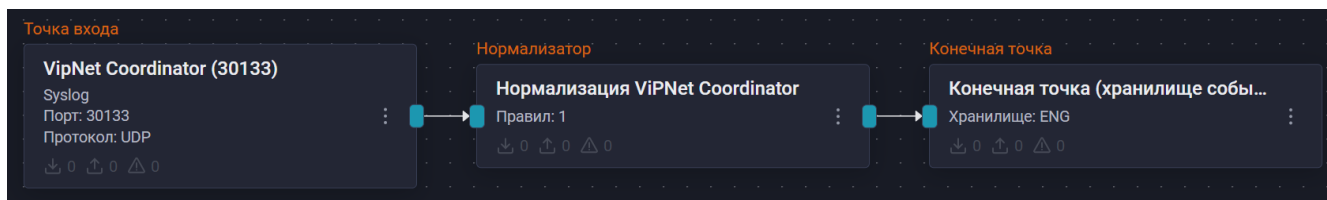
```
firewall local add 3 rule "Allow Syslog" src @local dst <IP-адрес коллектора> udp
```

```
dport <Порт коллектора> pass
```

Настройка отправки событий ViPNet Coordinator 4 завершена.

Настройка в R-Vision SIEM

Общий вид рабочего конвейера для обеспечения получения и отображения событий:



Для настройки сбора событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM перейдите в раздел **Ресурсы** → **Коллекторы** и откройте карточку коллектора.
2. На вкладке **Обогащение** добавьте таблицу обогащения **hw_fw_events** коллектора.
3. В том же коллекторе создайте новый конвейер.
4. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Syslog.
 - Порт точки входа и протокол: в соответствии с настройками на стороне [ViPNet Coordinator 4](#).
5. Добавьте на конвейер элемент **Нормализатор** с правилом ViPNet Coordinator 4 (идентификатор правила: RV-N-46). Соедините нормализатор с точкой входа.
6. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
7. Соедините конечную точку с нормализатором.
8. Сохраните и установите конфигурацию конвейера.

После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события ViPNet Coordinator 4.

Найти события ViPNet Coordinator 4 в хранилище можно по следующему фильтру:

```
dproduct = "hw"
```



timestamp	dvendor	dproduct	name	dvc	msg	outcome
2025-04-10T17:46:32.000+03:00	infotecs	hw	Non-encrypted IP packet allowed	10.150.49.79	Пропущен незашифрованный IP...	
2025-04-10T17:46:32.000+03:00	infotecs	hw	Non-encrypted IP packet allowed	10.150.49.79	Пропущен незашифрованный IP...	
2025-04-10T17:45:31.000+03:00	infotecs	hw	Non-encrypted IP packet allowed	10.150.49.79	Пропущен незашифрованный IP...	
2025-04-10T17:44:30.000+03:00	infotecs	hw	Non-encrypted IP packet allowed	10.150.49.79	Пропущен незашифрованный IP...	
2025-04-10T17:44:30.000+03:00	infotecs	hw	Local IP packet blocked by Public Network filter	10.150.49.79	Локальный пакет заблокирован фильтро...	
2025-04-10T17:44:30.000+03:00	infotecs	hw	Non-encrypted IP packet allowed	10.150.49.79	Пропущен незашифрованный IP...	

Типы обрабатываемых событий

Правилом нормализации обрабатываются следующие типы событий:

1. аутентификация пользователя в веб-интерфейсе/консоли;
2. переход в привилегированный режим;
3. ввод команд;
4. смена пароля пользователя;
5. изменения настроек сетевых интерфейсов;
6. открытие/закрытие конфигурационных файлов;
7. изменение настроек логирования;
8. удаление журналов;
9. включение/изменение/удаление правил межсетевого экрана;
10. события безопасности межсетевого экрана.

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

ViPNet IDS NS

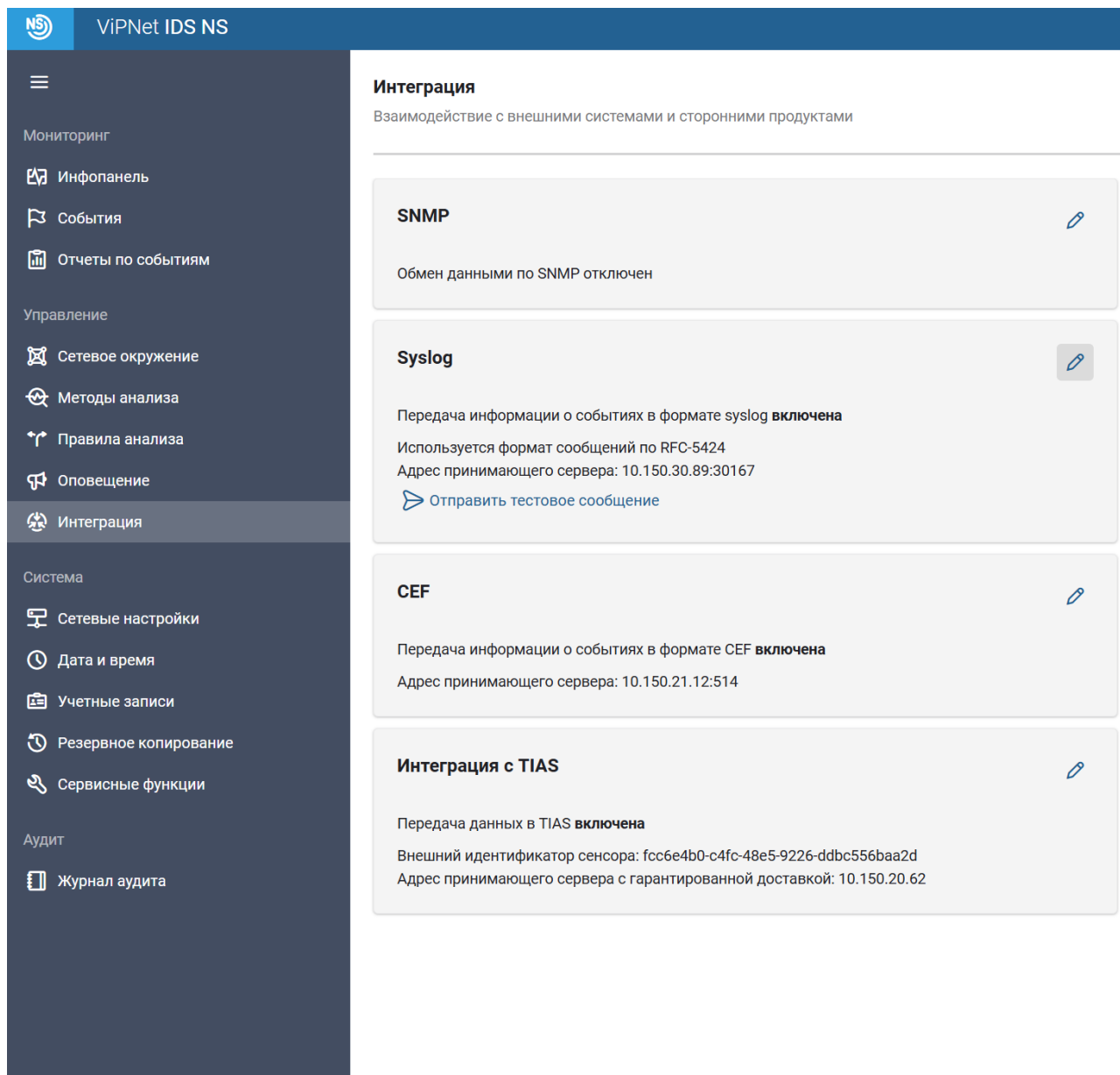
Данное руководство описывает процесс настройки сбора и отправки событий системы обнаружения компьютерных атак ViPNet IDS NS в R-Vision SIEM.

- [Настройка ViPNet IDS NS](#)
- [Настройка в R-Vision SIEM](#)
- [Типы обрабатываемых событий](#)
- [Таблица маппинга](#)

Настройка ViPNet IDS NS

Для настройки отправки событий ViPNet IDS NS в SIEM-систему в формате syslog выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet IDS NS.
2. В боковом меню откройте раздел **Интеграция**.
3. В форме **Syslog** откройте окно редактирования.



4. В открывшемся окне установите переключатель **Передавать информацию о событиях в формате syslog** в активное положение.
5. Нажмите на кнопку **Добавить**.
6. Установите флажок **Использовать формат сообщений по RFC-5424**.
7. В поле **Адрес принимающего сервера** введите IP-адрес коллектора SIEM, в рамках которого планируется осуществлять сбор событий ViPNet IDS NS.
8. В поле **Порт** введите значение порта больше 30000.

Syslog



☒ Передавать информацию о событиях в формате syslog

☒ Использовать формат сообщений по RFC-5424



Сохранить



Отмена

Адрес принимающего сервера

Порт

10.150.30.89

30167

Сохранить

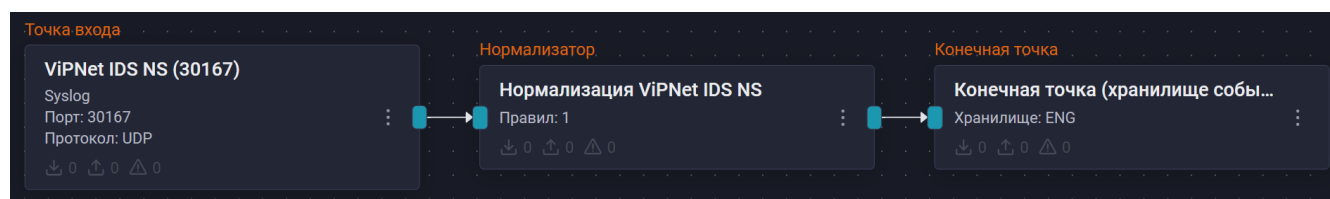
Отмена

9. Нажмите на кнопку **Сохранить**.

Настройка на стороне ViPNet IDS NS завершена.

Настройка в R-Vision SIEM

Общий вид рабочего конвейера для обеспечения получения и отображения событий:



Для настройки сбора событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Syslog.
 - Порт точки входа и протокол: в соответствии с настройками на стороне [ViPNet IDS NS](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом Infotecs ViPNet IDS NS (идентификатор правила: RV-N-145).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
6. Сохраните и установите конфигурацию конвейера.

После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события ViPNet IDS NS.

Найти события от ViPNet IDS NS в хранилище можно по следующему фильтру:

```
dproduct = "IDS NS"
```



timestamp	dvendor	dproduct	name	dvc	msg	outcome
2025-04-10T16:48:35.000+03:00	infotecs	IDS NS	AM DNS Query for net.anydesk.com (Comet...		На сенсоре IDS NS (ID:931854959)...	success
2025-04-10T16:48:35.000+03:00	infotecs	IDS NS	AM DNS Query for net.anydesk.com (Comet...		На сенсоре IDS NS (ID:931854959)...	success
2025-04-10T16:48:35.000+03:00	infotecs	IDS NS	AM DNS Query for net.anydesk.com (Comet...		На сенсоре IDS NS (ID:931854959)...	success
2025-04-10T16:48:35.000+03:00	infotecs	IDS NS	ET POLICY Powershell Activity Over SMB - Likely...		На сенсоре IDS NS (ID:931854959)...	success
2025-04-10T16:48:35.000+03:00	infotecs	IDS NS	AM DNS Query for net.anydesk.com (Comet...		На сенсоре IDS NS (ID:931854959)...	success
2025-04-10T16:48:35.000+03:00	infotecs	IDS NS	AM DNS Query for net.anydesk.com (Comet...		На сенсоре IDS NS (ID:931854959)...	success
2025-04-10T16:48:35.000+03:00	infotecs	IDS NS	AM DNS Query for net.anydesk.com (Comet...		На сенсоре IDS NS (ID:931854959)...	success
2025-04-10T16:48:35.000+03:00	infotecs	IDS NS	AM DNS Query for net.anydesk.com (Comet...		На сенсоре IDS NS (ID:931854959)...	success

Типы обрабатываемых событий

Правилом нормализации обрабатываются события, генерируемые сигнатурными правилами IDS NS.

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

ViPNet TIAS

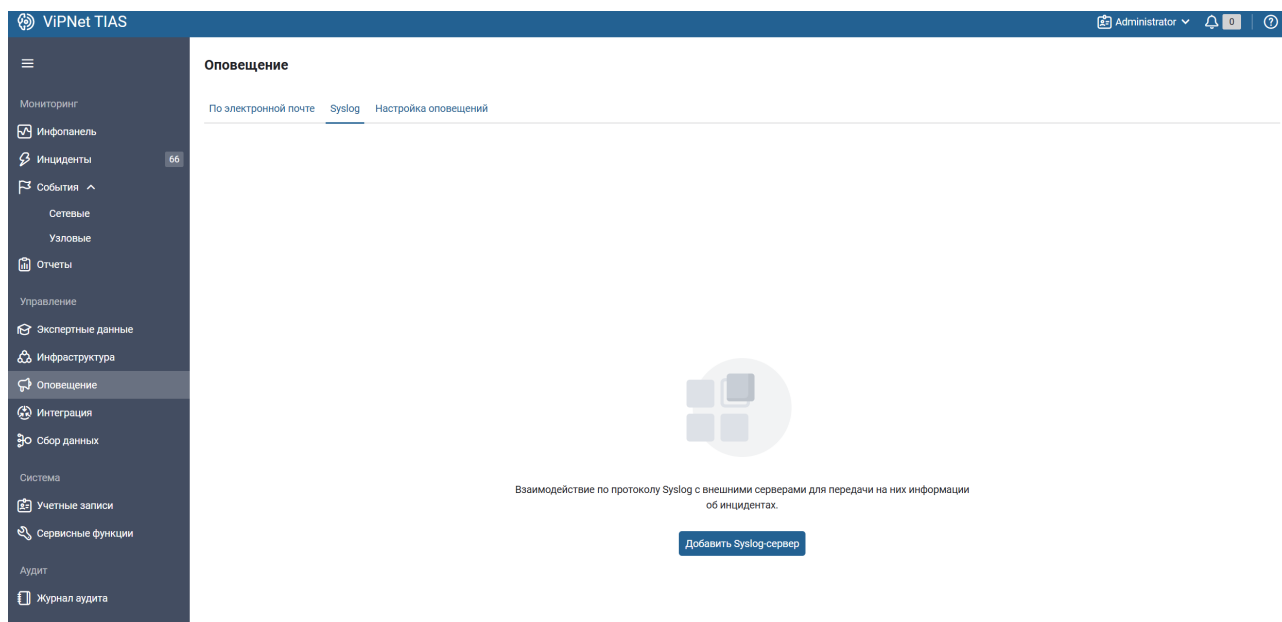
Данное руководство описывает процесс настройки сбора и отправки событий системы обнаружения компьютерных атак ViPNet TIAS в R-Vision SIEM.

- [Настройка ViPNet TIAS](#)
- [Настройка в R-Vision SIEM](#)
- [Типы обрабатываемых событий](#)
- [Таблица маппинга](#)

Настройка ViPNet TIAS

Для настройки отправки событий ViPNet TIAS в SIEM-систему в формате syslog выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet TIAS.
2. В боковом меню откройте раздел **Оповещение**.
3. На вкладке **Syslog** нажмите на кнопку **Добавить Syslog-сервер**. Откроется окно настроек оповещений об инцидентах по протоколу Syslog.



4. В поле **Протокол** выберите значение **TCP** или **UDP**.
5. В поле **Адрес Syslog-сервера** введите адрес коллектора R-Vision SIEM, в рамках которого планируется осуществлять сбор событий ViPNet TIAS.
6. Введите значение порта больше 30000.
7. Выберите русский язык для оповещения.
8. Установите флажки в остальных полях.
9. Выберите необходимые объекты инфраструктуры.
10. Нажмите на кнопку **Сохранить**.

Настройка оповещений об инцидентах по протоколу Syslog ✕

Общие

* Протокол

UDP



* Адрес Syslog-сервера

10.150.30.89

* Порт

30168

Язык оповещения



Русский



Английский

* Тип события



Регистрация инцидента



Обновление информации об инциденте



Изменение статуса инцидента

Инциденты

Укажите параметры инцидентов, о которых необходимо оповещать.

* Метод обнаружения



Аналитический



Сигнатурный



Эвристический

* Уровень важности инцидента



Высокий



Средний



Низкий

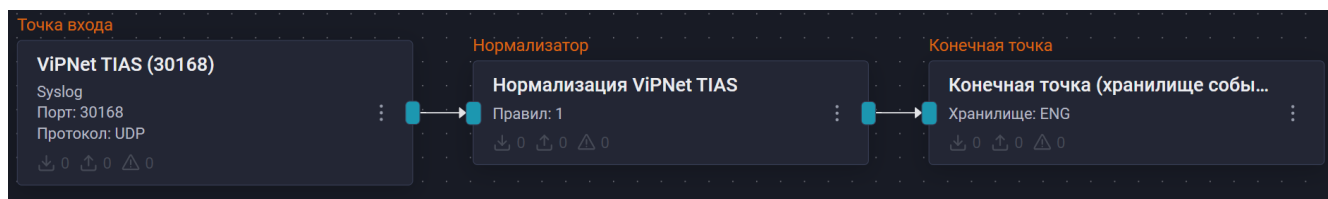
Сохранить

Отмена

Настройка на стороне ViPNet TIAS завершена.

Настройка в R-Vision SIEM

Общий вид рабочего конвейера для обеспечения получения и отображения событий:



Для настройки сбора событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Syslog.
 - Порт точки входа и протокол: в соответствии с настройками на стороне [ViPNet TIAS](#).
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Infotecs ViPNet TIAS** (идентификатор правила: **RV-N-146**). Соедините нормализатор с точкой входа.
4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
5. Соедините конечную точку с нормализатором.
6. Сохраните и установите конфигурацию конвейера.

После [настройки передачи событий](#), если настройка выполнена корректно, в хранилище начнут поступать события ViPNet TIAS.

Найти события ViPNet TIAS в хранилище можно по следующему фильтру:

```
dproduct = "ViPNet TIAS"
```



timestamp	dvendor	dproduct	name	dvc	msg	outcome
2025-04-22T11:43:39.000+03:00	Infotecs	ViPNet TIAS	Выявлен инцидент для Windows	10.150.20.63	Зафиксирован инцидент с id:24a9b428-7674-480e...	success
2025-04-22T11:43:39.000+03:00	Infotecs	ViPNet TIAS	new incident	10.150.20.63	Изменена информация инцидента с id:50064ac...	success
2025-04-22T11:43:33.000+03:00	Infotecs	ViPNet TIAS	new incident	10.150.20.63	Изменена информация инцидента с id:50064ac...	success
2025-04-22T11:43:33.000+03:00	Infotecs	ViPNet TIAS	Выявлен инцидент для Windows	10.150.20.63	Зафиксирован инцидент с id:24a9b428-7674-480e...	success
2025-04-22T11:43:28.000+03:00	Infotecs	ViPNet TIAS	Выявлен инцидент для Windows	10.150.20.63	Зафиксирован инцидент с id:24a9b428-7674-480e...	success
2025-04-22T11:43:28.000+03:00	Infotecs	ViPNet TIAS	new incident	10.150.20.63	Изменена информация инцидента с id:50064ac...	success

Типы обрабатываемых событий

Правилом нормализации обрабатываются следующие типы событий:

1. создание инцидента;

2. изменение инцидента.

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Код Безопасности

Данный раздел содержит список систем для настройки от компании Код Безопасности:

- [Secret Net LSP](#)
- [Secret Net Studio](#)
- [Континент 4](#)

Secret Net LSP

Данное руководство содержит инструкции по настройке отправки событий в систему R-Vision SIEM из продукта Secret Net LSP.

События Secret Net LSP



Подробная информация о записываемых событиях приведена в [документации Secret Net LSP](#).

Secret Net LSP записывает события в две базы данных: **Системная** и **БД аудита**.

Syslog читает события только из системной БД, поскольку журналы в БД аудита зашифрованы. Правило, указанное в данной инструкции, нормализует только события из системной БД, которые относятся к следующим типам:

- [Аутентификация](#) через графический интерфейс или SSH;
- [Повышение привилегий](#);
- [Изменение политик](#);
- [Настройка аудита](#);
- [Резервное копирование](#);
- [Взаимодействие с журналами](#);
- [Взаимодействие с правилами МЭ](#);
- [Блокировка или разблокировка APM](#).

Сбор событий из БД аудита осуществляется посредством сервера безопасности Secret Net Studio, под управлением которого может находиться Secret Net LSP.

Настройка источника для отправки событий в R-Vision SIEM

Для отправки событий Secret Net LSP в R-Vision SIEM:

1. Откройте файл `/opt/secretnet/etc/syslog-ng/syslog-ng.conf`:

```
sudo nano /opt/secretnet/etc/syslog-ng/syslog-ng.conf
```

2. Дополните файл строками:

- Для передачи событий по протоколу UDP:

```
destination rcollector { udp("<ip-адрес коллектора>" port(<слушаемый порт>));};
```

- Для передачи событий по протоколу TCP:

```
destination rcollector { tcp("<ip-адрес коллектора>" port(<слушаемый порт>) log-  
fifo-size(1000));};
```

Сохраните изменения:

```
log { source(src_main); destination(rcollector);};
```

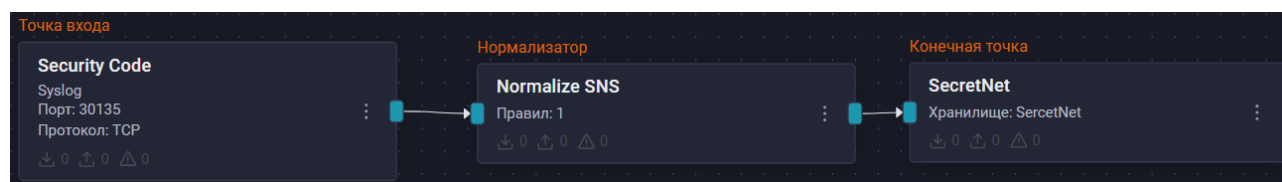
3. Перезагрузите рабочую станцию.

Настройка интеграции с R-Vision SIEM

Для получения событий аудита с Secret Net LSP необходимо настроить следующий конвейер:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - a. **Тип точки входа** — Syslog;
 - b. **Название** — любое понятное.
 - c. **Порт точки входа** и **Протокол** — в соответствии с настройками на стороне [syslog-сервера](#).
3. Добавьте **Нормализатор** с правилом **Security Code Secret Net LSP** (идентификатор **RV-N-108**)
Соедините нормализатор с точкой входа.
4. Добавьте элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
5. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера



При успешном включении в выбранном хранилище появятся события Secret Net LSP.

Таблицы маппинга

Таблица 14. Общий маппинг

Поле события	Значение поля
dvendor	"Код Безопасности"
dproduct	"Secret Net LSP"
dvchost	<code>.raw.hostname</code>
msg	Сообщение, приведенное к человекопонятному виду. Подробности см. в следующих таблицах.
rt	<code>.raw.timestamp</code>
severity	<code>.raw.severity</code>
externalId	<code>.raw.message.code</code>
facility	<code>.raw.facility</code>
destinationServiceName	<code>.raw.appname</code>
outcome	"success" либо "failure"
cat	<code>.raw.message[0]</code>

Таблица 15. Аутентификация

Поле события	Значение поля
msg	Сообщение, приведенное к человекопонятному виду + <code>.suser</code>
name	Извлекается из поля <code>.raw.message</code>
suser	Извлекается из поля <code>.raw.message</code>

Таблица 16. Повышение привилегий

Поле события	Значение поля
name	"root session closed opened"
suser	Извлекается из поля <code>.raw.message</code>

Таблица 17. Изменение политик

Поле события	Значение поля	Для плагинов	Для аутентификации (token_mgr)
msg		Сообщение, приведенное к человекопонятному виду + <code>.objName</code> + <code>.suser</code>	Сообщение, приведенное к человекопонятному виду + <code>.objName</code> + <code>.cs2</code>
name	"setting policy"		
suser	Извлекается из поля <code>.raw.message</code>		
objType	"plugin" либо "settings policy"		
objName	<code>.raw.message.objname</code>		
cs2			<code>.raw.message.objvalue</code>

Поле события	Значение поля	Для плагинов	Для аутентификации (token_mgr)
cs2Label			"Новое значение параметра"

Таблица 18. Настройка аудита

Поле события	Значение поля
msg	Сообщение, приведенное к человекопонятному виду + .objName + .cn1
name	"add new rule", "object set on audit" или "deleted rule"
cn1	Извлекается из поля .raw.message (ID правила)
objName	Извлекается из поля .raw.message

Таблица 19. Резервное копирование

Поле события	Значение поля
msg	Сообщение, приведенное к человекопонятному виду + .objName + .cn2
name	"backup not found" либо "backup setting"
cn2	Извлекается из поля .raw.message
cn2Label	"backup id"

Таблица 20. Взаимодействие с журналами

Поле события	Управление журналами (all)	Управление журналами (содержит before/after)	Управление журналами (содержит from-to)	Запрос журналов
msg	Сообщение, приведенное к человекопонятному виду + .act + .cs4	Сообщение, приведенное к человекопонятному виду + .raw.message.action + .cs4	Сообщение, приведенное к человекопонятному виду + .act + .c2 + .cs3 + .cs4	Сообщение, приведенное к человекопонятному виду + .objName + .suser
name	.act + "records"			event log query
cs2		.raw.message.preposition	Извлекается из поля .raw.message	
cs2Label		"preposition"	"from time"	
cs3		.raw.message.time	Извлекается из поля .raw.message	
cs3Label		"time"	"to time"	
cs4		Извлекается из поля .raw.message		

Поле события	Управление журналами (all)	Управление журналами (содержит before/after)	Управление журналами (содержит from-to)	Запрос журналов
cs4Label		"database type"		
act	.raw.message[0]	.raw.message[-2]	.raw.message[3]	

Таблица 21. Взаимодействие с правилами межсетевого экрана

Поле события	Значение поля
msg	Сообщение, приведенное к человекопонятному виду + .act
cs2	Извлекается из поля .raw.message
cs2Label	"Firewall rule id"
cs3	(кроме случаев, когда поле .act равно deleted) Извлекается из поля .raw.message
cs3Label	(кроме случаев, когда поле .act равно deleted) "Rule parameters"
act	Извлекается из поля .raw.message

Таблица 22. Блокировка или разблокировка APM.

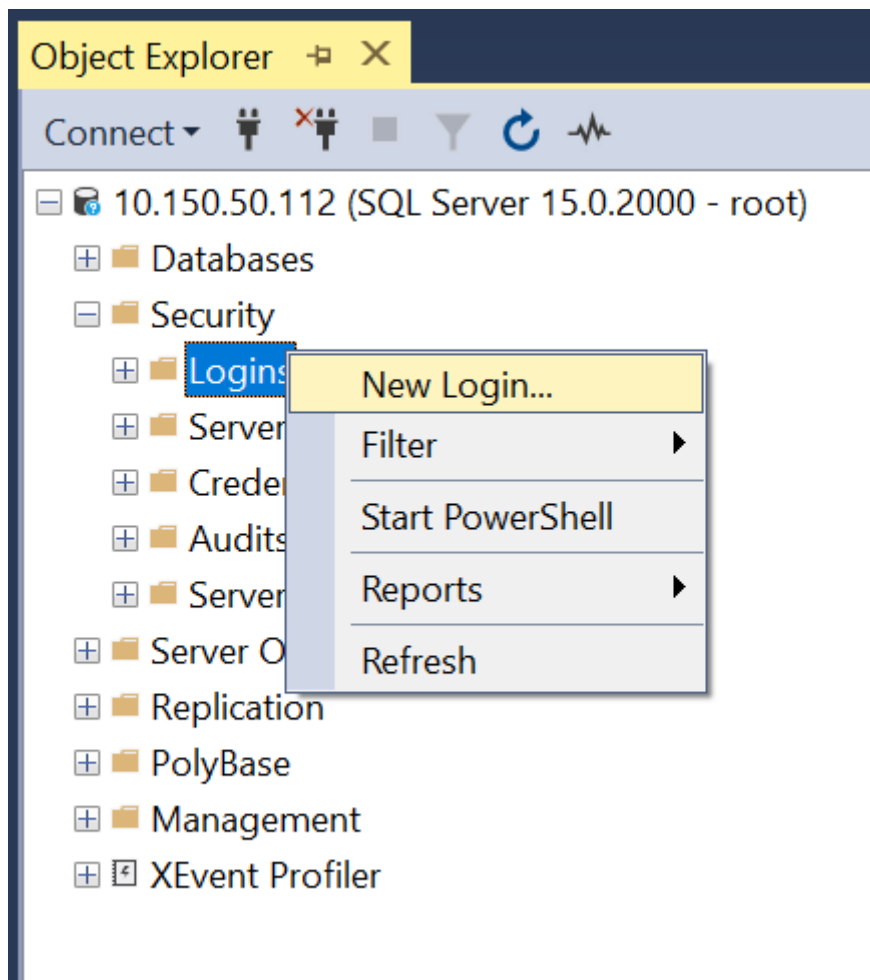
Поле события	Значение поля
msg	"Рабочая станция разблокирована заблокирована"

Secret Net Studio

Secret Net Studio средство защиты информации от несанкционированного доступа, выполняющее функции контроля конфиденциальности, целостности и доступа к информации на рабочих станциях.

Настройка СУБД MSSQL

1. Для создания сервисной УЗ необходимо подключиться к СУБД посредством SQL Server Management Studio административной УЗ. Вызовите контекстное меню для **Security** → **Logins** и выберите опцию **New Login**.



2. И создайте сервисную УЗ со следующими параметрами:

- Login name - произвольное
- Метод аутентификации - SQL Server authentication
- Default database - База данных Secret Net Studio

Login - New

Select a page

General

Server Roles

User Mapping

Securables

Status

Connection

Server:

10.150.50.112

Connection:

root

View connection properties

Progress

Ready

Script Help

Login name:

extsns

Search...

☐ Windows authentication
 ☒ SQL Server authentication

Password:

.....

Confirm password:

.....

☐ Specify old password

Old password:

☐ Enforce password policy
 ☐ Enforce password expiration
 ☐ User must change password at next login

☐ Mapped to certificate

☐ Mapped to asymmetric key

☐ Map to Credential

Mapped Credentials

Credential	Provider

Add

Remove

Default database:

SN7_SERVER_SCHEMA

Default language:

<default>

OK

Cancel

3. Перейдите в раздел **User Mapping**, отметьте галочкой базу данных Secret Net Studio и выберите для пользователя роли **public** и **db_datareader**

Login - New

Select a page

General

Server Roles

User Mapping

Securables

Status

Connection

Server:

10.150.50.112

Connection:

root

View connection properties

Progress

Ready

Script Help

Users mapped to this login:

Map	Database	User	Default Schema
☐	master		
☐	model		
☐	msdb		
☒	SN7_SERVER_SCHEMA	extsns	
☐	tempdb		

☐ Guest account enabled for: SN7_SERVER_SCHEMA

Database role membership for: SN7_SERVER_SCHEMA

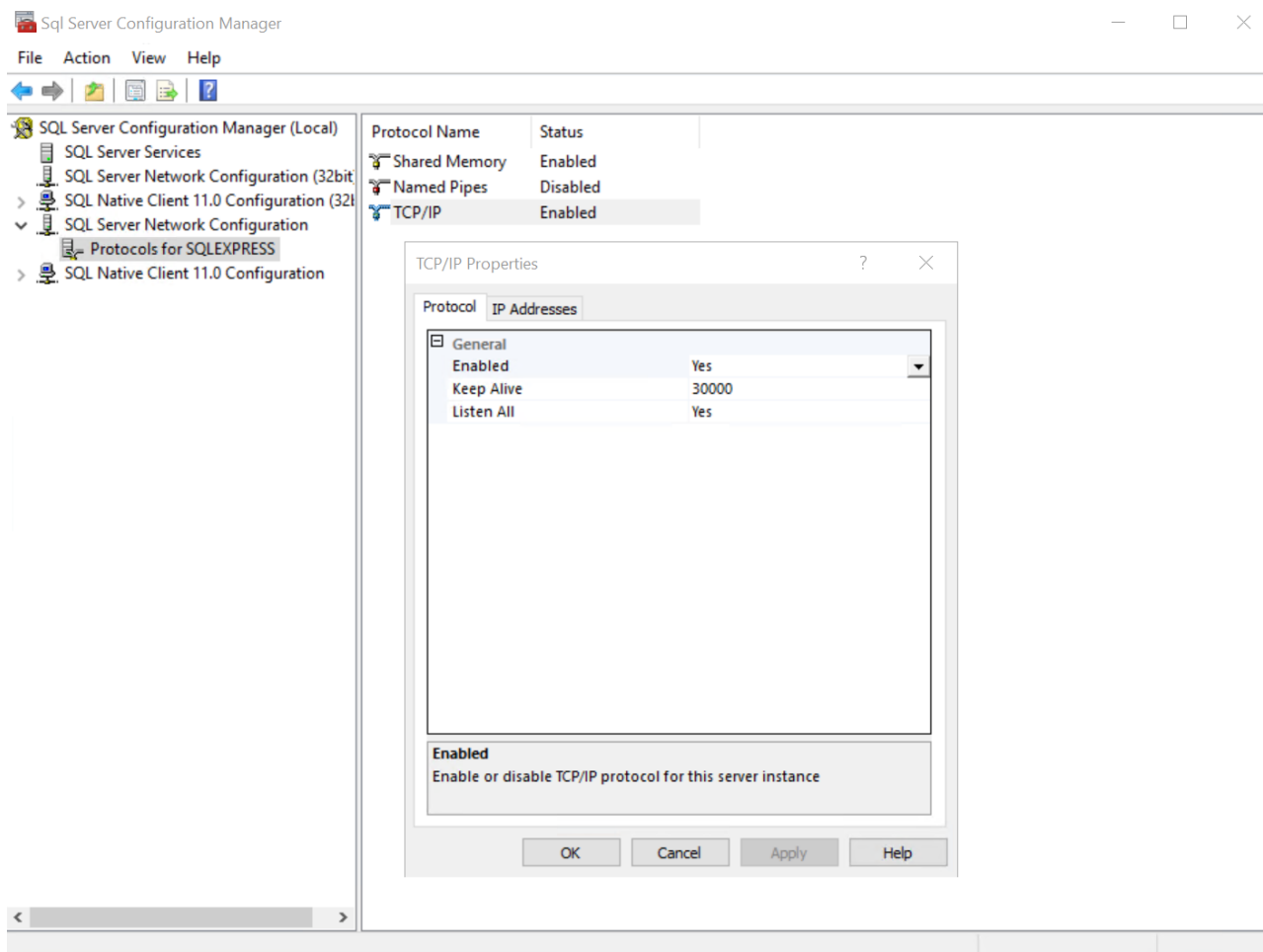
☐ db_accessadmin
☐ db_backupoperator
☒ db_datareader
☐ db_datawriter
☐ db_ddladmin
☐ db_denydatareader
☐ db_denydatawriter
☐ db_owner
☐ db_securityadmin
☒ public
☐ SN7SERVER

OK

Cancel

- В настройках SQL Server Configuration Manager убедитесь, что TCP/IP включен в конфигурации сети SQL Server.

308



Настройка Secret Net Studio

1. Запустите "Центр управления Secret Net Studio".
2. В левом меню нажмите на вкладку **Компьютеры**.
3. В открывшейся панели выберите группу узлов/ узел для настройки.
4. Нажмите на вкладку **Настройки**.
5. В списке выберите раздел **Регистрация событий**.
6. Включите типы событий, необходимые для журналирования. **Внимание** Рекомендуется включить журналирование для всех типов событий, кроме **Запуск процесса, Завершение процесса** в категории **Контроль приложений**.
7. Перейдите во вкладку **Параметры** → **Сбор журналов**.
8. Включите следующие функции:
 - **Производить сбор журналов при подключении агента к серверу безопасности.**
 - **Производить сбор журналов при заполнении на 80% и более.**
9. Снимите флажки для **Приложений, Системный** и **Безопасности**.
10. Раскройте список Расписание сбора журналов, выберите Периодическое и укажите интервал в **1 минуту**.
11. Примените изменения.

Сбор событий безопасности для защищаемых АРМ (Настройка SIEM)

Для сбора событий SIEM необходимо создать конвейер:

1. Точка входа:

- Название - любое понятное.
- Тип точки входа - Database.
- Драйвер базы данных - необходимый для MSSQL.
- Адрес подключения - укажите подготовленный секрет.
- SQL-запрос - введите следующий:

```
SELECT
    EventLogRecID as event_id,
    DATEADD (
        hour,
        DATEDIFF (hour, GETUTCDATE (), GETDATE ()),
        TimeWritten
    ) as rt,
    Version as dversion,
    EventCategory as deviceEventClassId,
    CategoryMessage as cat,
    EventMessage as msg,
    TypeDescription as facillity,
    SourceName as destinationServiceName,
    Computername as shost,
    Msid as machineid,
    UserSid as suid,
    UserName as suser,
    UserDomainName as sntdom,
    ThreatLevel as severity,
    LogName as dproduct,
    replace(@@SERVERNAME,@@SERVICENAME, '') + DEFAULT_DOMAIN() as dvchost
,
    CONNECTIONPROPERTY ('local_net_address') AS dvc,
    'SNS security events' as EventFilter
FROM
    SN7_SERVER_SCHEMA.dbo.EventLogRec as ev
    LEFT JOIN dbo.EventLog as evlog ON ev.EventLogType = evlog.LogType
    LEFT JOIN dbo.Client as clients ON ev.ClientId = clients.ClientID
WHERE
    EVENTLOGTYPE = 4
    AND EVENTLOGRECID > ?
```

- Поле идентификатор - введите event_id со значением 1.
- Интервал запроса - 60 секунд.

2. Нормализатор - выберите правило с id: RV-N-109

3. Хранилище:

- Название - любое понятное.
- Тип конечной точки - на усмотрение (по умолчанию хранилище событий).
- Хранилище событий - выберите необходимое хранилище.
- Модель события - универсальная модель события.

Сбор событий аудита сервера безопасности Secret Net Studio (Настройка SIEM)

Конвейер для сбора событий аудита СБ Secret Net Studio аналогичен описанному выше, поэтому далее уточняются только параметры, которые будут отличаться (если параметр не указан, опирайтесь в его настройке на инструкцию описанную выше для событий безопасности).

1. Точка входа:

- SQL-запрос - введите следующий:

```
SELECT
    ClientClass,
    ClientType,
    MName,
    MSid,
    UName,
    USid,
    DATEADD (
        hour,
        DATEDIFF (hour, GETUTCDATE (), GETDATE ()),
        DateStart
    ) as DateStart,
    DATEADD (
        hour,
        DATEDIFF (hour, GETUTCDATE (), GETDATE ()),
        DateEnd
    ) as DateEnd,
    ExitCode,
    SessionGUID,
    ActionCode,
    TemplateCode,
    DATEADD (
        hour,
        DATEDIFF (hour, GETUTCDATE (), GETDATE ()),
        ActionTime
    ) as ActionTime,
    ActionParameters as msg,
    ResultCode,
    ClientSessionID,
    SessionActionID,
    GETDATE () as rt,
    replace(@@SERVERNAME,@@SERVICENAME, '') + DEFAULT_DOMAIN() as dvchost
,
```

```

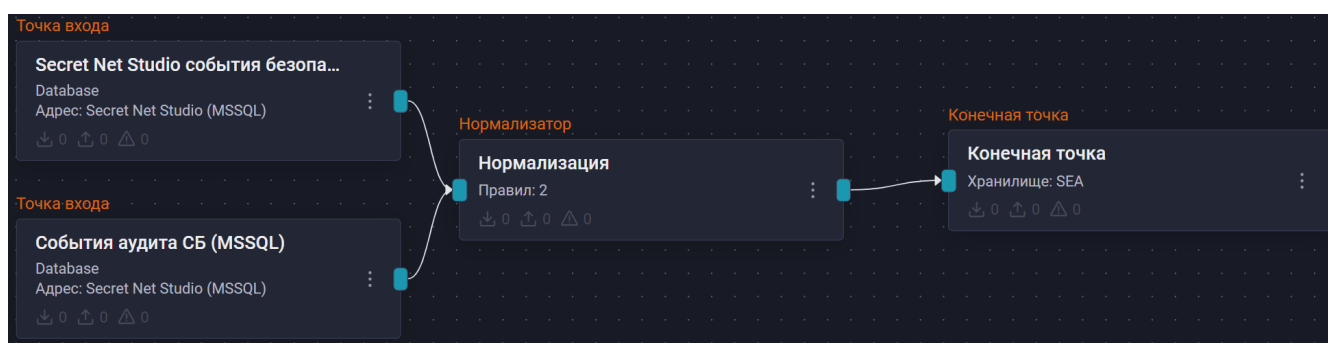
CONNECTIONPROPERTY ('local_net_address') AS dvc,
'SNS audit events' as EventFilter
FROM
    SN7_SERVER_SCHEMA.dbo.ServerLog
where
    (
        DATEADD (
            hour,
            DATEDIFF (hour, GETUTCDATE (), GETDATE ()),
            ActionTime
        ) >= DATEADD (SECOND, -15, GetDate ())
    )

```

- Поле идентификатор - не нужно.
- Интервал запроса - 15 секунд.

2. Нормализатор - выберите правило с id: RV-N-110 Таким образом заведение событий Secret Net Studio в SIEM успешно завершено.

Пример конфигурации конвейера



Континент 4

Данное руководство описывает процесс настройки сбора и отправки событий аппаратно-программного комплекса шифрования (АПКШ) Континент-4 в R-Vision SIEM.

Настройка сбора событий на стороне источника



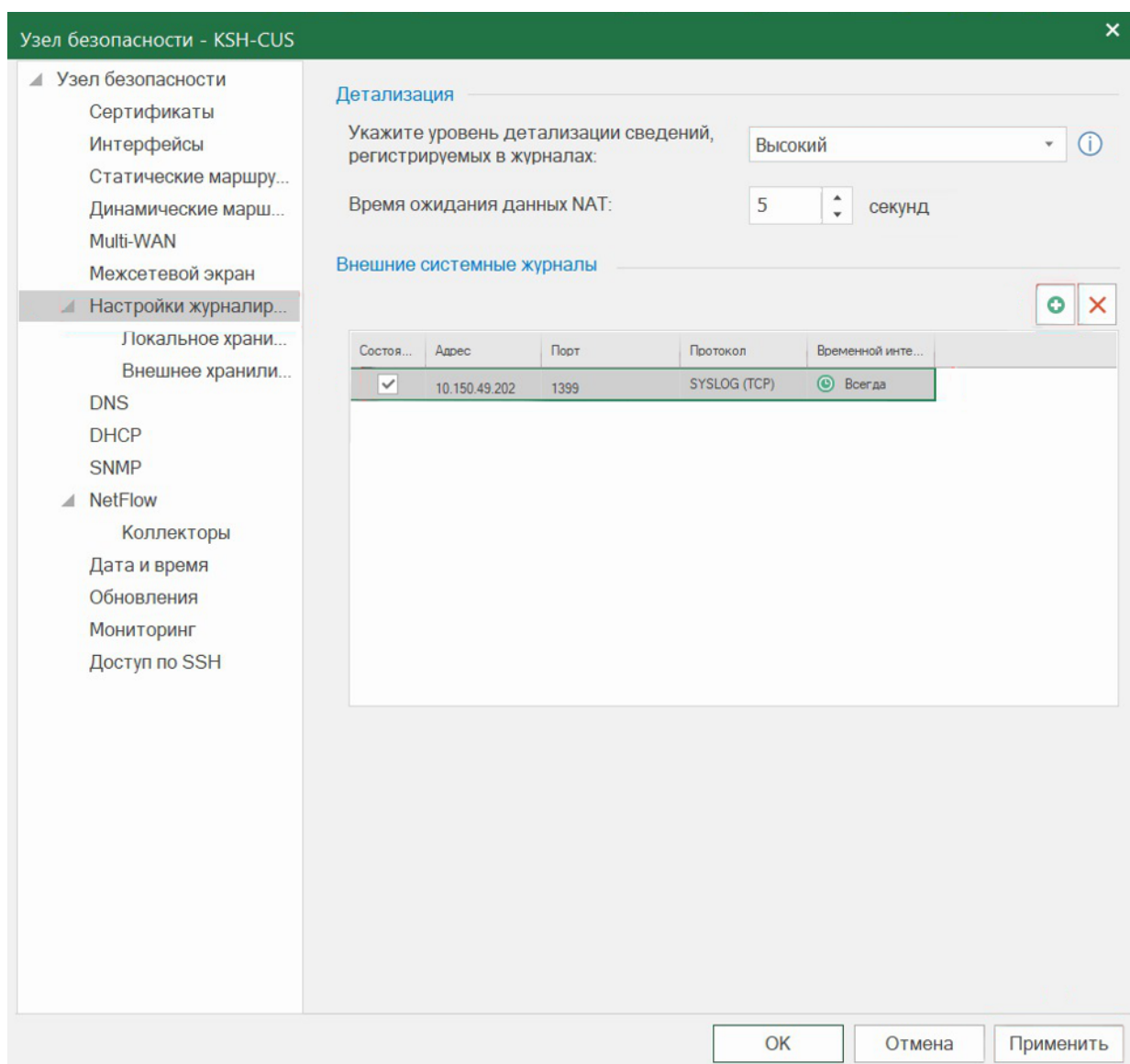
Система позволяет отправлять события аудита во внешние системы посредством syslog. Функциональные события АПКШ Континент 4 во внешние системы посредством syslog не передаются и не покрываются текущими правилами нормализации R-Vision SIEM.

Для настройки syslog на АПКШ Континент 4:

1. Подключитесь к центру управления сетью (далее – ЦУС) с помощью ПО "Континент. Менеджер конфигурации".
2. Перейдите во вкладку **Структура**.
3. Выберите узел безопасности (далее – УБ), с которого необходимо отправлять события в SIEM.

4. Вызовите контекстное меню для УБ и выберите **Свойства**. Откроется меню настроек УБ.
5. Перейдите во вкладку **Настройки журналирования**.
6. Для параметра **Детализация** задайте значение **Высокий**.
7. Нажмите на кнопку добавления внешнего системного журнала.
8. Заполните параметры:
 - IP-адрес коллектора SIEM или syslog-сервера, через который будут передаваться данные в SIEM;
 - порт, который планируется прослушивать;
 - протокол.

Настройки журналирования должны выглядеть следующим образом:



Узел безопасности - KSH-CUS

Настройки журналирования

Детализация

Укажите уровень детализации сведений, регистрируемых в журналах: Высокий

Время ожидания данных NAT: 5 секунд

Внешние системные журналы

Состоя...	Адрес	Порт	Протокол	Временной интер...
☒	10.150.49.202	1399	SYSLOG (TCP)	Всегда

ОК Отмена Применить

9. Нажмите на кнопки **Применить** и **ОК**.
10. Отправьте конфигурацию на УБ. Для этого:
 - a. В общем меню нажмите на вторую иконку в верхнем левом углу.
 - b. Отметьте УБ, для которого настраивалось внешнее журналирование.

с. Нажмите на кнопку **OK**.

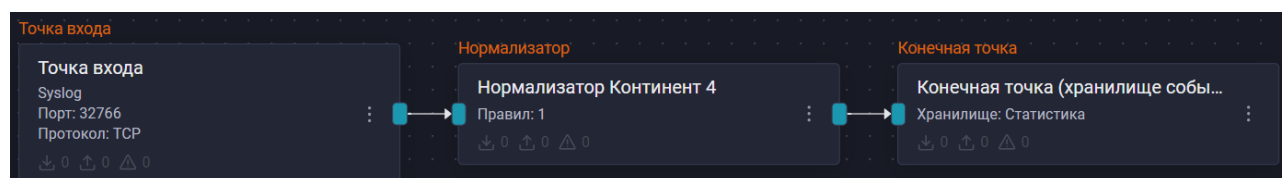
Настройка на стороне АПКШ Континент 4 завершена.

Настройка интеграции с R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте в конвейер элемент **Точка входа** со следующими параметрами:
 - a. **Тип точки входа** — Syslog;
 - b. **Порт точки входа** и **Протокол** — в соответствии с настройкой АПКШ Континент 4.
3. Соедините с точкой входа **Нормализатор** с добавленным правилом нормализации с ID **74d77206-86cb-480f-97bf-4162ddc5ea93**.
4. Соедините с нормализатором конечную точку типа **Хранилище событий**.
5. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера



Таблицы маппинга

Таблица 23. Общий маппинг

Поле модели событий	Значение
dvendor	Код Безопасности
dproduct	Континент 4
dversion	4.1.0
dvc	.raw.hostname
dvchost	.raw.hostname
msg	.raw.message
rt	.raw.timestamp
severity	.raw.severity
facility	.raw.facility
name	.raw.appname
outcome	success/failure

Таблица 24. Аутентификация

Поле модели событий	Значение
act	authentication success/failure

Поле модели событий	Значение
duser	account name
src	source ip
spt	source port

Таблица 25. Выполнение команд sudo

Поле модели событий	Значение
duser	account name
cmd	raw.message.COMMAND

Таблица 26. Конфигурирование

Поле модели событий	Значение
act	implement
objType	configuration
objName	path to config file

Таблица 27. Сессия su

Поле модели событий	Значение
act	session opened/closed
duser	account name

Таблица 28. Disconnect ssh

Поле модели событий	Значение
act	Disconnected ssh session
duser	account name

Конфидент

Данный раздел содержит список систем для настройки от компании Конфидент:

- [Dallas Lock ЕЦУ](#)
- [Dallas Lock Сервер Безопасности 8.0](#)

Dallas Lock Сервер Безопасности 8.0

Описание источника

СЗИ Dallas Lock 8.0 предназначена для предотвращения получения защищаемой информации заинтересованными лицами с нарушением установленных норм и правил и обладателями информации с нарушением установленных правил разграничения доступа к защищаемой информации и осуществления контроля за потоками информации, поступающими в автоматизированную систему (далее – АС) и выходящими за ее пределы, обеспечения защиты информации в АС посредством ее фильтрации.

Также Dallas Lock 8.0 имеет возможность централизованного управления посредством Dallas Lock 8.0 Сервер Безопасности.

Данный раздел содержит список инструкций по настройке источника Dallas Lock 8.0:

- [Сбор событий из СУБД MS SQL](#)
- [Сбор событий в формате CEF](#)

Сбор событий в формате CEF

Данное руководство описывает процесс настройки сбора и отправки событий Dallas Lock 8.0 Сервер безопасности в R-Vision SIEM.

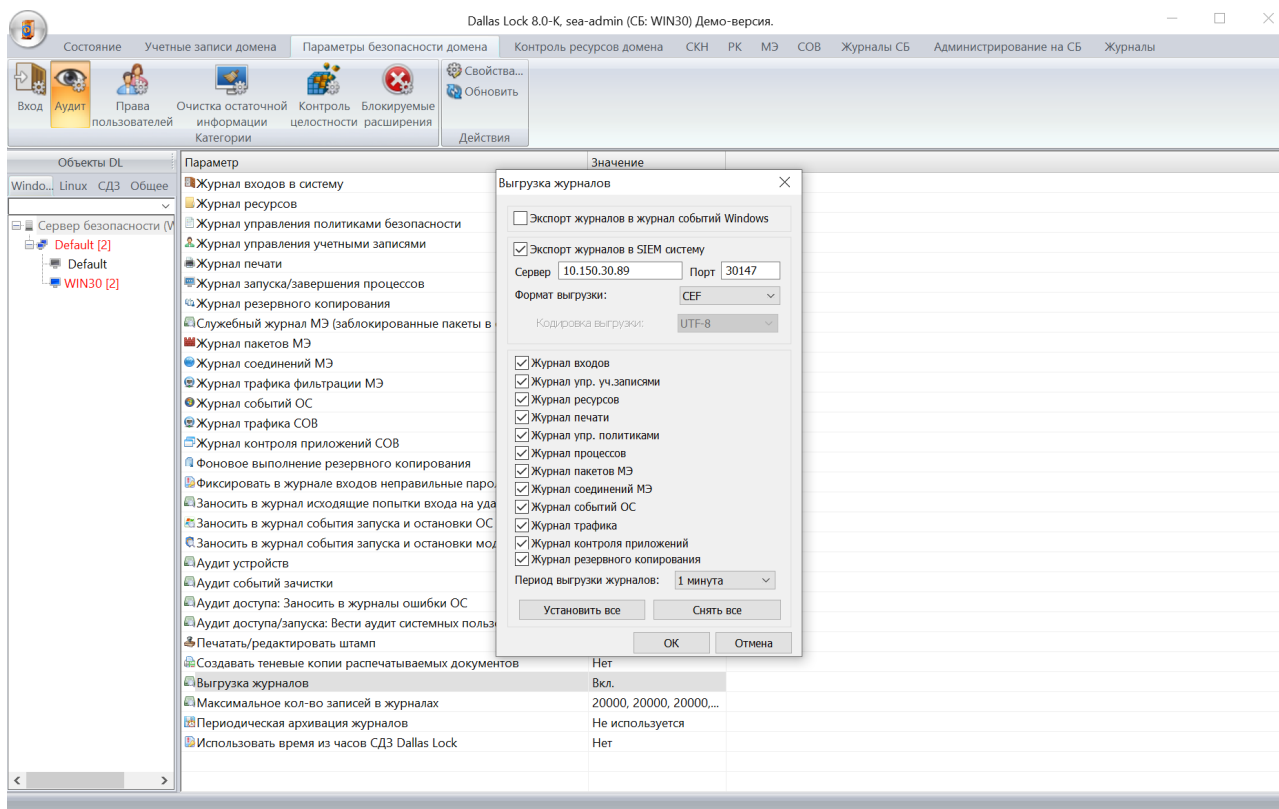
Настройка Dallas Lock 8.0



Настройка сбора событий с Dallas Lock 8.0 Сервер Безопасности производится аналогично.

Для пересылки событий, зарегистрированных Dallas Lock 8.0, в R-Vision SIEM в формате CEF выполните следующие действия:

1. Перейдите на вкладку **Параметры безопасности домена**.
2. Перейдите в **Аудит**.
3. Найдите параметр **Выгрузка журналов**.
4. Укажите IP-адрес и порт коллектора, выберите формат CEF, отметьте все журналы и установите период выгрузки.



5. Нажмите **ОК**.

Источник настроен.

Настройка интеграции с R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие действия:

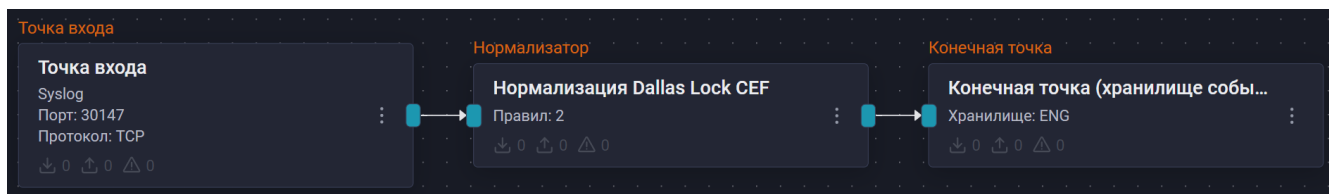
1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Syslog.
 - Порт точки входа и протокол: в соответствии с настройкой Dallas Lock 8.0.
3. Добавьте на конвейер элемент **Нормализатор** с правилом "RV-N-135". Соедините нормализатор с точкой входа.



Правило "RV-N-135" также нормализует события, получаемые из Dallas Lock ЕЦУ в формате CEF.

4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
5. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



Если настройка выполнена корректно, в хранилище начнут поступать события от Dallas.



Найти события от Dallas в хранилище можно по следующему фильтру:

`dvendor = Confident`

timestamp	dvendor	dproduct	name	dvc	msg	outcome
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Архивация журнала соединений МЭ		Архивация журнала соединений МЭ...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Сбор событий из СУБД MS SQL

Данное руководство описывает процесс настройки сбора и отправки событий Dallas Lock 8.0 Сервер безопасности в R-Vision SIEM.

Предварительные требования

- Сетевая доступность между R-Vision SIEM и СУБД Dallas Lock 8.0 Сервер Безопасности (tcp/1433).
- Учетная запись в СУБД с правами на чтение таблиц используемых Dallas Lock (Сбор событий из БД).

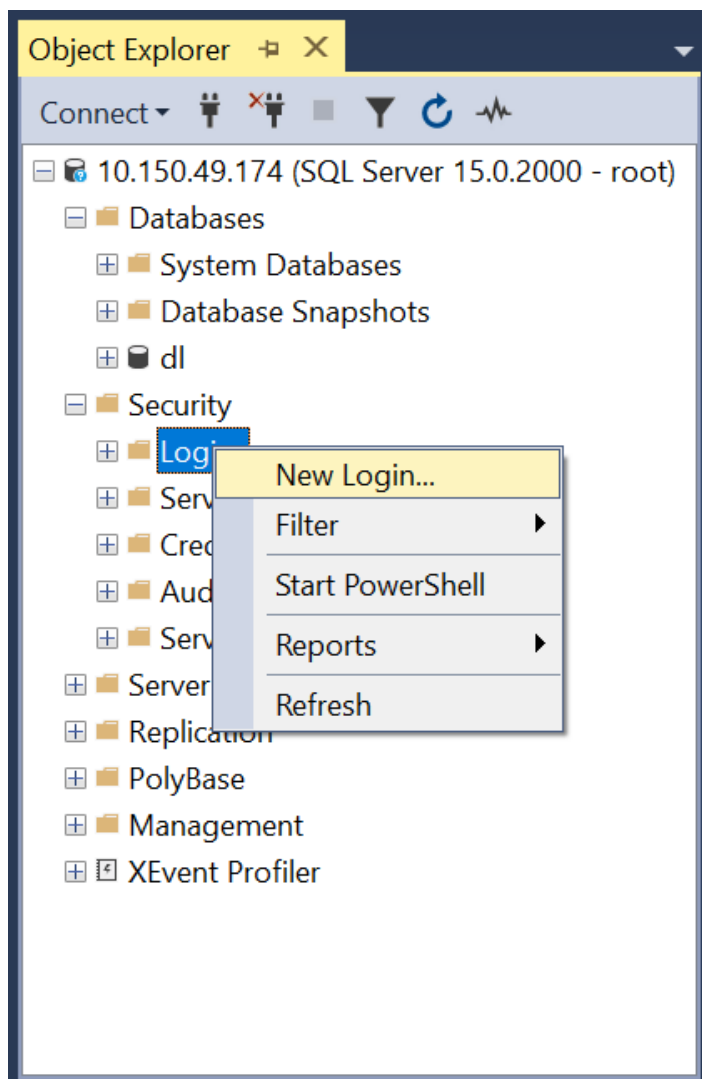
Настройка в СУБД MS SQL

Для сбора событий Dallas Lock СБ из базы данных MS SQL необходимо настроить подключение R-Vision SIEM под служебной УЗ с соответствующими правами.

Создание учетной записи в СУБД MS SQL

Чтобы создать сервисную УЗ, подключитесь к СУБД с правами администратора. Для этого выполните следующие действия в SQL Server Management Studio:

1. Выберите **New Login** в контекстном меню для **Security/Logins**.



2. Создайте сервисную учетную запись.

Login - New

Select a page

- General
- Server Roles
- User Mapping
- Securables
- Status

Connection

Server: 10.150.49.174

Connection: root

[View connection properties](#)

Progress

Ready

Script Help

Login name: dl_reader Search...

☐ Windows authentication
☒ SQL Server authentication

Password:

Confirm password:

☐ Specify old password
 Old password:

☐ Enforce password policy
☐ Enforce password expiration
☐ User must change password at next login

☐ Mapped to certificate
☐ Mapped to asymmetric key
☐ Map to Credential Add

Credential	Provider
------------	----------

Remove

Default database: dl

Default language: <default>

OK Cancel

3. Предоставьте учетной записи права на чтение базы Dallas Lock.

Login - New

Select a page

- General
- Server Roles
- User Mapping
- Securables
- Status

Connection

Server: 10.150.49.174

Connection: root

[View connection properties](#)

Progress

Ready

Script Help

Users mapped to this login:

Map	Database	User	Default Schema
☒	dl	dl_reader	
☐	master		
☐	model		
☐	msdb		
☐	tempdb		

☐ Guest account enabled for: dl

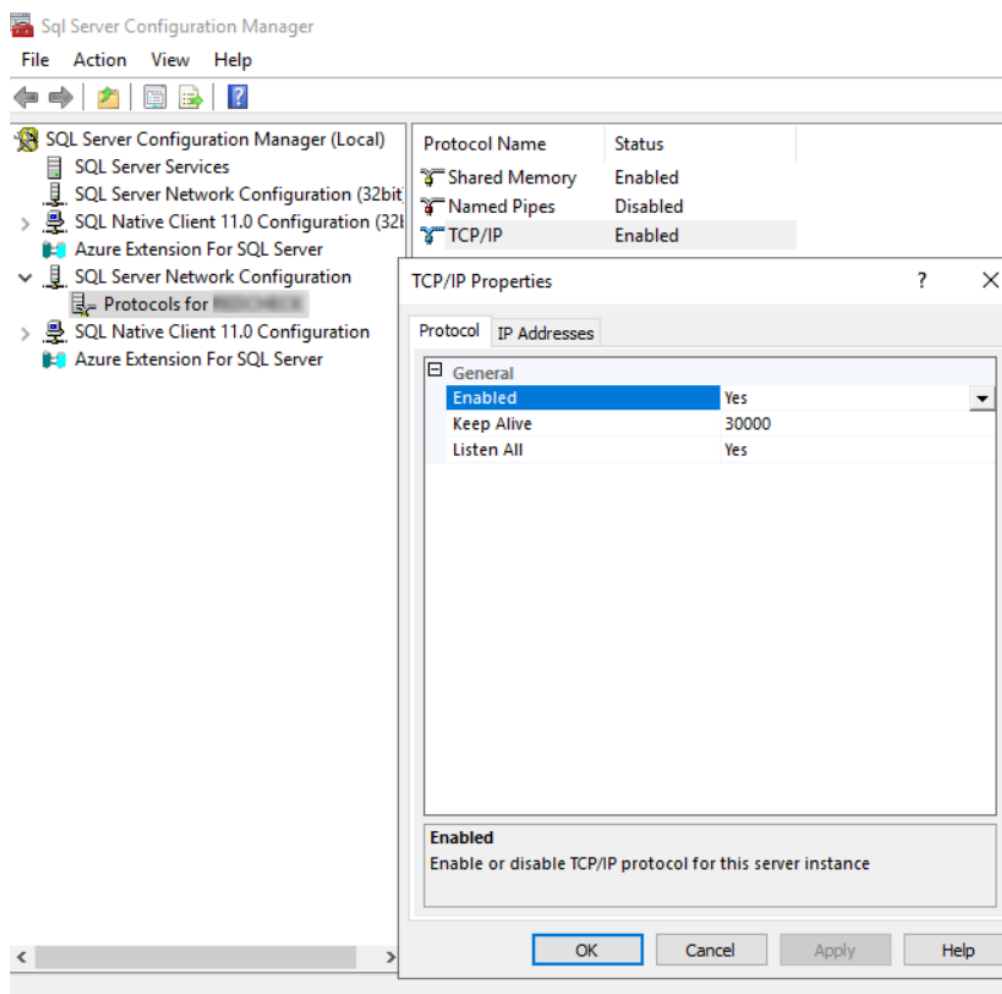
Database role membership for: dl

- ☐ db_accessadmin
- ☐ db_backupoperator
- ☒ db_datareader
- ☐ db_datawriter
- ☐ db_ddladmin
- ☐ db_denydatareader
- ☐ db_denydatawriter
- ☐ db_owner
- ☐ db_securityadmin
- ☒ public

OK Cancel

Настройка сервера MS SQL

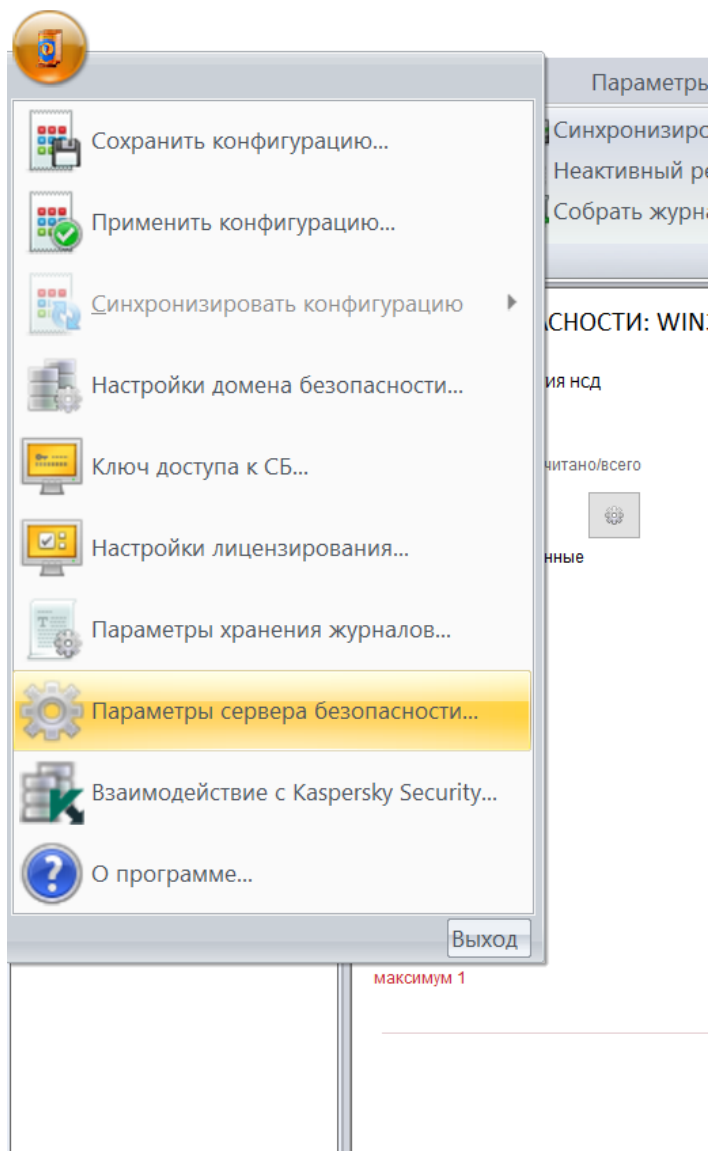
В настройках SQL Server Configuration Manager убедитесь, что TCP/IP включен в конфигурации сети SQL Server.



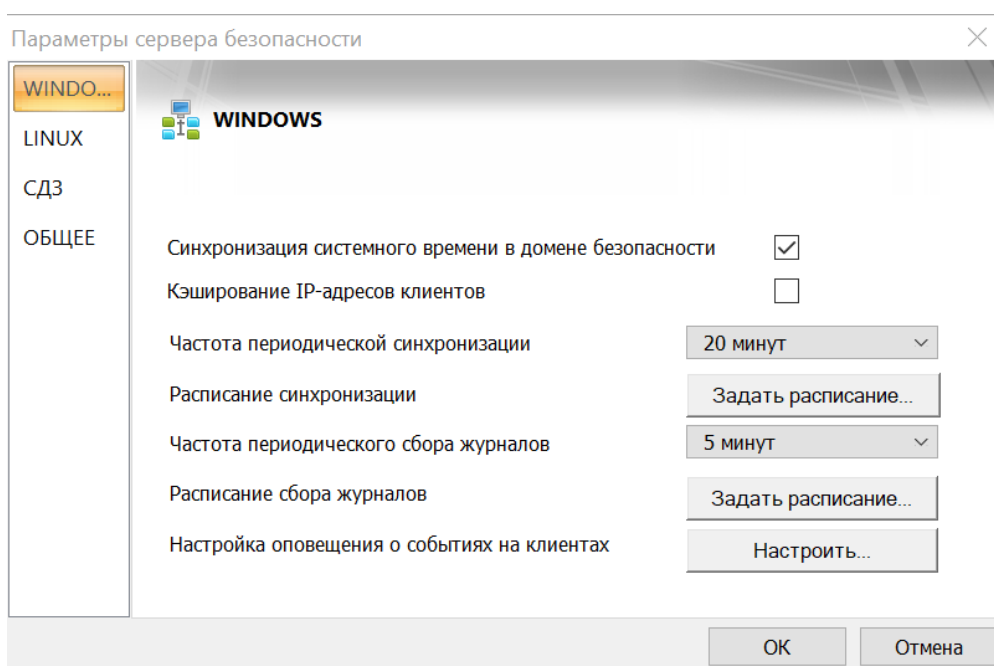
Настройка Dallas Lock 8.0 Сервер Безопасности

Необходимо настроить периодичность сбора событий с конечных АРМ на Сервер Безопасности. Для этого:

1. Нажмите на значок в левом верхнем углу и в раскрывшемся меню нажмите **Параметры сервера безопасности**.



2. На вкладках **WINDOWS** и **LINUX** установите минимально возможную частоту сбора журналов: 5 минут.



3. Нажмите **ОК**.

Сервер Безопасности Dallas Lock настроен.

Настройка в R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие действия:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Database.
 - SQL-запрос:

▼ SQL-запрос

```
SELECT TOP 10000 'CONNECT' AS journal_name
,recID AS connect_rec_id
,dateAndTime AS event_date
,clientName AS client_name
,mandatLevel AS mandat_level
,userName AS user_name
,result AS result
,processName AS process_name
,processID as process_id
,permit AS permit
,EventOnConnect AS event_on_connect
,DnsName AS dns_name
,protocol AS protocol
,localAddress AS local_address
,(LocalPort & 255) * 256 | cast((LocalPort/256) & 255 as bigint) AS
local_port
,RemoteAddress AS remote_address
,(RemotePort & 255) * 256 | cast((RemotePort/256) & 255 as bigint) AS
remote_port
,inDataLen AS in_bytes
,outDataLen AS out_bytes
,ruleId AS rule_id
,NULL AS alarm_level
,NULL AS rule_action
,AddressType AS address_type
,NULL AS src_address
,NULL AS dst_address
,NULL AS signature_number
,NULL AS signature_info
,NULL AS computer_name
,NULL AS comment
,NULL as parameter
,NULL as action
,NULL as type_of_attack
,NULL as target_user_name
```

```

, NULL AS latest_protocol_id
, NULL AS direction
, NULL AS bytes
, NULL AS resource
, NULL AS printer_name
, NULL AS document
, NULL AS printer_port
, NULL AS pages_printed
, NULL AS copies_printed
, NULL AS shadow_copy
, NULL AS wrong_user_pw
, NULL AS logon_mode
FROM [dbo].[Connect] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
UNION ALL

SELECT TOP 10000 'PACKETS' AS journal_name
, recID AS packets_rec_id
, dateAndTime AS event_date
, clientName AS client_name
, mandatLevel AS mandat_level
, userName AS user_name
, result AS result
, processName AS process_name
, processID as process_id
, permit AS permit
, NULL AS event_on_connect
, DnsName AS dns_name
, NULL AS protocol
, localAddress AS local_address
, (LocalPort & 255) * 256 | cast((LocalPort/256) & 255 as bigint) AS
local_port
, RemoteAddress AS remote_address
, (RemotePort & 255) * 256 | cast((RemotePort/256) & 255 as bigint) AS
remote_port
, NULL AS in_bytes
, NULL AS out_bytes
, ruleId AS rule_id
, NULL AS alarm_level
, NULL AS rule_action
, AddressType AS address_type
, NULL AS src_address
, NULL AS dst_address
, NULL AS signature_number
, NULL AS signature_info
, NULL as computer_name
, NULL AS comment
, NULL as parameter
, NULL as action
, NULL as type_of_attack
, NULL as target_user_name
, LatestProtocolID AS latest_protocol_id

```



```

,direction AS direction
,length AS bytes
,NULL AS resource
,NULL AS printer_name
,NULL AS document
,NULL AS printer_port
,NULL AS pages_printed
,NULL AS copies_printed
,NULL AS shadow_copy
,NULL AS wrong_user_pw
,NULL AS logon_mode
FROM [dbo].[Packets] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
UNION ALL

```

```

SELECT TOP 10000 'IPS_TRAFFIC' AS journal_name
,recID AS traffic_rec_id
,dateAndTime AS event_date
,clientName AS client_name
,mandatLevel AS mandat_level
,userName AS user_name
,result AS result
,processName AS process_name
,processID AS process_id
,NULL AS permit
,NULL AS event_on_connect
,NULL AS dns_name
,protocol AS protocol
,NULL AS local_address
,NULL AS local_port
,NULL AS remote_address
,NULL AS remote_port
,NULL AS in_bytes
,NULL AS out_bytes
,NULL AS rule_id
,AlarmLevel AS alarm_level
,ruleAction AS rule_action
,AddressType AS address_type
,SourceAddress AS src_address
,DestAddress AS dst_address
,SignatureNumber AS signature_number
,Info AS signature_info
,NULL AS computer_name
,comment AS comment
,NULL AS parameter
,NULL AS action
,NULL AS type_of_attack
,NULL as target_user_name
,NULL AS latest_protocol_id
,NULL AS direction
,NULL AS bytes
,NULL AS resource

```

```

, NULL AS printer_name
, NULL AS document
, NULL AS printer_port
, NULL AS pages_printed
, NULL AS copies_printed
, NULL AS shadow_copy
, NULL AS wrong_user_pw
, NULL AS logon_mode
FROM [dbo].[IPS_Traffic] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
UNION ALL

SELECT TOP 10000 'PROCESS' AS journal_name
, recID AS processes_rec_id
, dateAndTime AS event_date
, clientName AS client_name
, mandatLevel AS mandat_level
, userName AS user_name
, result AS result
, processName AS process_name
, processID AS process_id
, NULL AS permit
, NULL AS event_on_connect
, NULL AS dns_name
, NULL AS protocol
, NULL AS local_address
, NULL AS local_port
, NULL AS remote_address
, NULL AS remote_port
, NULL AS in_bytes
, NULL AS out_bytes
, NULL AS rule_id
, NULL AS alarm_level
, NULL AS rule_action
, NULL AS address_type
, NULL AS src_address
, NULL AS dst_address
, NULL AS signature_number
, NULL AS signature_info
, NULL AS computer_name
, NULL AS comment
, NULL AS parameter
, action AS action
, NULL AS type_of_attack
, NULL AS target_user_name
, NULL AS latest_protocol_id
, NULL AS direction
, NULL AS bytes
, NULL AS resource
, NULL AS printer_name
, NULL AS document
, NULL AS printer_port

```

```
,NULL AS pages_printed
,NULL AS copies_printed
,NULL AS shadow_copy
,NULL AS wrong_user_pw
,NULL AS logon_mode
FROM [dbo].[Process] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
UNION ALL
```

```
SELECT TOP 10000 'IPS_APP_CTRL' AS journal_name
,recID AS app_ctrl_rec_id
,dateAndTime AS event_date
,clientName AS client_name
,mandatLevel AS mandat_level
,userName AS user_name
,result AS result
,processName AS process_name
,processID AS process_id
,permit AS permit
,NULL AS event_on_connect
,NULL AS dns_name
,NULL AS protocol
,NULL AS local_address
,NULL AS local_port
,NULL AS remote_address
,NULL AS remote_port
,NULL AS in_bytes
,NULL AS out_bytes
,NULL AS rule_id
,NULL AS alarm_level
,NULL AS rule_action
,NULL AS address_type
,NULL AS src_address
,NULL AS dst_address
,NULL AS signature_number
,NULL AS signature_info
,NULL AS computer_name
,comment AS comment
,NULL AS parameter
,NULL AS action
,TypeOfAttack AS type_of_attack
,NULL as target_user_name
,NULL AS latest_protocol_id
,NULL AS direction
,NULL AS bytes
,NULL AS resource
,NULL AS printer_name
,NULL AS document
,NULL AS printer_port
,NULL AS pages_printed
,NULL AS copies_printed
,NULL AS shadow_copy
```

```
,NULL AS wrong_user_pw
,NULL AS logon_mode
FROM [dbo].[IPS_App_Ctrl] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
UNION ALL
```

```
SELECT TOP 10000 'ACCOUNT' AS journal_id
,recID AS accounts_rec_id
,dateAndTime AS event_date
,clientName AS client_name
,mandatLevel AS mandat_level
,userName AS user_name
,result AS result
,NULL AS process_name
,NULL AS process_id
,NULL AS permit
,NULL AS event_on_connect
,NULL AS dns_name
,NULL AS protocol
,NULL AS local_address
,NULL AS local_port
,NULL AS remote_address
,NULL AS remote_port
,NULL AS in_bytes
,NULL AS out_bytes
,NULL AS rule_id
,NULL AS alarm_level
,NULL AS rule_action
,NULL AS address_type
,NULL AS src_address
,NULL AS dst_address
,NULL AS signature_number
,NULL AS signature_info
,computerName AS computer_name
,comment AS comment
,NULL AS parameter
,action AS action
,NULL AS type_of_attack
,targetUserName as target_user_name
,NULL AS latest_protocol_id
,NULL AS direction
,NULL AS bytes
,NULL AS resource
,NULL AS printer_name
,NULL AS document
,NULL AS printer_port
,NULL AS pages_printed
,NULL AS copies_printed
,NULL AS shadow_copy
,NULL AS wrong_user_pw
,NULL AS logon_mode
FROM [dbo].[Account] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
```

UNION ALL

```
SELECT TOP 10000 'POLICY' AS journal_name
,recID AS policies_rec_id
,dateAndTime AS event_date
,clientName AS client_name
,mandatLevel AS mandat_level
,userName AS user_name
,result AS result
,NULL AS process_name
,NULL AS process_id
,NULL AS permit
,NULL AS event_on_connect
,NULL AS dns_name
,NULL AS protocol
,NULL AS local_address
,NULL AS local_port
,NULL AS remote_address
,NULL AS remote_port
,NULL AS in_bytes
,NULL AS out_bytes
,NULL AS rule_id
,NULL AS alarm_level
,NULL AS rule_action
,NULL AS address_type
,NULL AS src_address
,NULL AS dst_address
,NULL AS signature_number
,NULL AS signature_info
,computerName AS computer_name
,comment AS comment
,parameter AS parameter
,action AS action
,NULL AS type_of_attack
,NULL AS target_user_name
,NULL AS latest_protocol_id
,NULL AS direction
,NULL AS bytes
,NULL AS resource
,NULL AS printer_name
,NULL AS document
,NULL AS printer_port
,NULL AS pages_printed
,NULL AS copies_printed
,NULL AS shadow_copy
,NULL AS wrong_user_pw
,NULL AS logon_mode
FROM [dbo].[Policy] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
UNION ALL
```

```
SELECT TOP 10000 'ACCESS' AS journal_name
```

```

,recID AS access_rec_id
,dateAndTime AS event_date
,clientName AS client_name
,mandatLevel AS mandat_level
,userName AS user_name
,result AS result
,processName AS process_name
,NULL AS process_id
,NULL AS permit
,NULL AS event_on_connect
,NULL AS dns_name
,NULL AS protocol
,NULL AS local_address
,NULL AS local_port
,NULL AS remote_address
,NULL AS remote_port
,NULL AS in_bytes
,NULL AS out_bytes
,NULL AS rule_id
,NULL AS alarm_level
,NULL AS rule_action
,NULL AS address_type
,NULL AS src_address
,NULL AS dst_address
,NULL AS signature_number
,NULL AS signature_info
,computerName AS computer_name
,NULL AS comment
,NULL AS parameter
,action AS action
,NULL AS type_of_attack
,NULL AS target_user_name
,NULL AS latest_protocol_id
,NULL AS direction
,NULL AS bytes
,resource AS resource
,NULL AS printer_name
,NULL AS document
,NULL AS printer_port
,NULL AS pages_printed
,NULL AS copies_printed
,shadowCopy AS shadow_copy
,NULL AS wrong_user_pw
,NULL AS logon_mode
FROM [dbo].[Access] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
UNION ALL

SELECT TOP 10000 'PRINT' AS journal_name
,recID AS print_rec_id
,dateAndTime AS event_date
,clientName AS client_name

```

```

,mandatLevel AS mandat_level
,userName AS user_name
,result AS result
,processName AS process_name
,NULL AS process_id
,NULL AS permit
,NULL AS event_on_connect
,NULL AS dns_name
,NULL AS protocol
,NULL AS local_address
,NULL AS local_port
,NULL AS remote_address
,NULL AS remote_port
,NULL AS in_bytes
,NULL AS out_bytes
,NULL AS rule_id
,NULL AS alarm_level
,NULL AS rule_action
,NULL AS address_type
,NULL AS src_address
,NULL AS dst_address
,NULL AS signature_number
,NULL AS signature_info
,computerName AS computer_name
,NULL AS comment
,NULL AS parameter
,NULL AS action
,NULL AS type_of_attack
,NULL as target_user_name
,NULL AS latest_protocol_id
,NULL AS direction
,NULL AS bytes
,NULL AS resource
,printerName AS printer_name
,document AS document
,port AS printer_port
,pagesPrinted AS pages_printed
,copies AS copies_printed
,shadowCopy AS shadow_copy
,NULL AS wrong_user_pw
,NULL AS logon_mode
FROM [dbo].[Printer] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
UNION ALL

SELECT TOP 10000 'LOGON' AS journal_name
,recID AS logon_rec_id
,dateAndTime AS event_date
,clientName AS client_name
,mandatLevel AS mandat_level
,userName AS user_name
,result AS result

```

```

,NULL AS process_name
,NULL AS process_id
,NULL AS permit
,NULL AS event_on_connect
,NULL AS dns_name
,NULL AS protocol
,NULL AS local_address
,NULL AS local_port
,NULL AS remote_address
,NULL AS remote_port
,NULL AS in_bytes
,NULL AS out_bytes
,NULL AS rule_id
,NULL AS alarm_level
,NULL AS rule_action
,NULL AS address_type
,NULL AS src_address
,NULL AS dst_address
,NULL AS signature_number
,NULL AS signature_info
,computerName AS computer_name
,NULL AS comment
,NULL AS parameter
,NULL AS action
,NULL AS type_of_attack
,NULL AS target_user_name
,NULL AS latest_protocol_id
,NULL AS direction
,NULL AS bytes
,NULL AS resource
,NULL AS printer_name
,NULL AS document
,NULL AS printer_port
,NULL AS pages_printed
,NULL AS copies_printed
,NULL AS shadow_copy
,wrongUserPW AS wrong_user_pw
,logonMode AS logon_mode
FROM [dbo].[Logon] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())

```



В представленном запросе из каждой таблицы собирается по 10 000 событий. Если возникает проблема с выгрузкой событий рекомендует понизить количество событий, собираемых одним запросом.

- База данных: MS SQL.
- Интервал запроса: 120 секунд.
- Поле идентификатора: нет.
- Строка подключения в секрете:


```
jdbc:sqlserver://DBSERVER:1433;encrypt=false;databaseName=DBNAME;user=dl_reader;password=passwd
```

Здесь:

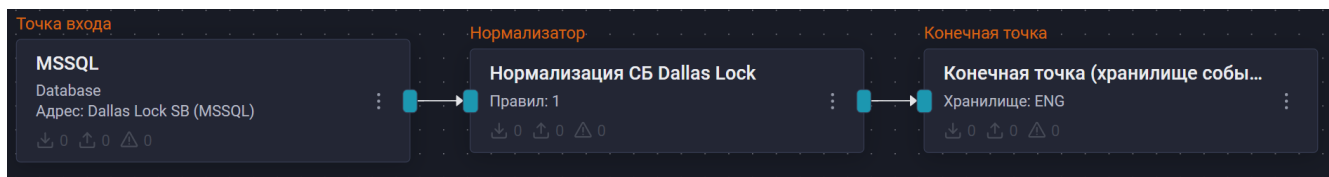
- **DBSERVER** — FQDN или IP-адрес сервера СУБД.
- **DBNAME** — название экземпляра БД.
- **1433** — порт подключения.



Создание секрета описано в разделе [Настройка секрета database в R-Vision SIEM](#).

3. Добавьте на конвейер элемент **Нормализатор** с правилом "RV-N-134". Соедините нормализатор с точкой входа.
4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
5. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



Если настройка выполнена корректно, в хранилище начнут поступать события из MS SQL.



Найти события из MS SQL в хранилище можно по следующему фильтру:

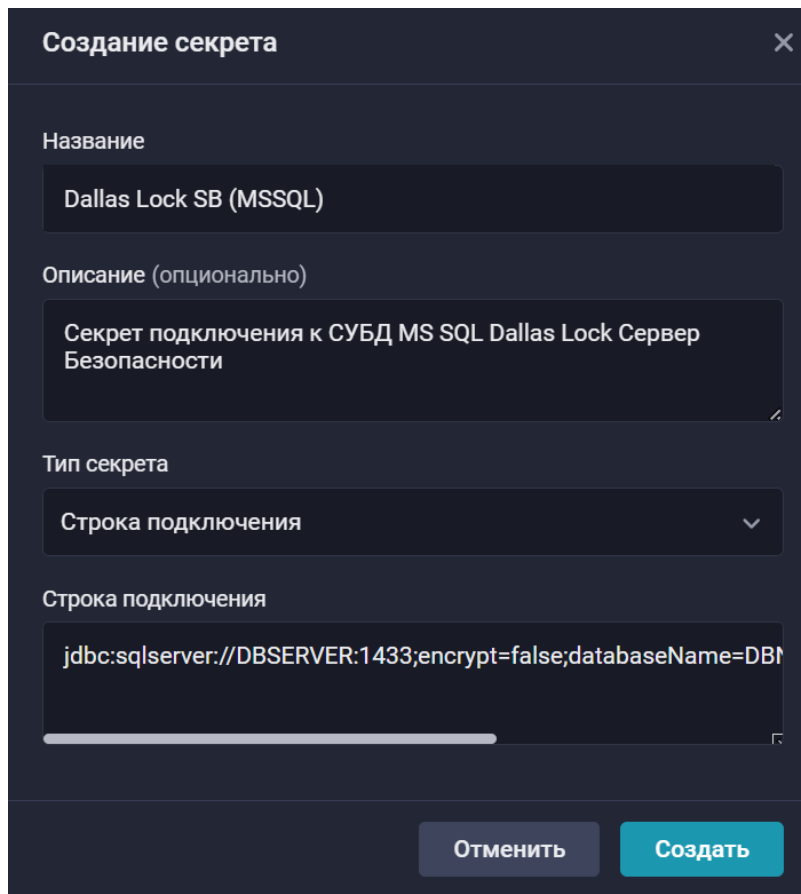
```
dvendor = Confident
```

timestamp	dvendor	dproduct	name	dvc	msg	outcome
2025-04-04T10:50:27.000+03:00	Confident	Единый центр управления	Очистка журнала событий безопасности	10.150.20.29	Очистка журнала событий безопасности	success
2025-04-04T10:49:42.000+03:00	Confident	Единый центр управления	Изменение политики безопасности	10.150.20.29	Значение политики 'Минимальная длина...	success
2025-04-04T10:49:27.000+03:00	Confident	Единый центр управления	Подключение консоли ЕЦУ	10.150.20.29	Подключение консоли ЕЦУ	success

Настройка секрета database в R-Vision SIEM

Чтобы создать секрет подключения к СУБД:

1. В интерфейсе R-Vision SIEM перейдите в раздел **Ресурсы** → **Секреты**.
2. Нажмите на кнопку **Создать**.
3. В открывшемся окне заполните поля:
 - **Название** — введите название секрета.
 - **Описание** (опционально) — введите назначение секрета.
 - **Тип секрета** — выберите вариант **Строка подключения**.
 - **Строка подключения** — укажите данные для подключения к СУБД.
4. Нажмите на кнопку **Создать**.



Создание секрета

Название

Dallas Lock SB (MSSQL)

Описание (опционально)

Секрет подключения к СУБД MS SQL Dallas Lock Сервер Безопасности

Тип секрета

Строка подключения

Строка подключения

jdbc:sqlserver://DBSERVER:1433;encrypt=false;databaseName=DBI

Отменить Создать

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Dallas Lock ЕЦУ

Описание источника

Единый центр управления Dallas Lock — кроссплатформенное изделие в продуктовой линейке Dallas Lock, предназначенное для решения следующих задач:

- Создание единого отказоустойчивого домена безопасности (далее — ДБ) и организация централизованного управления средствами защиты информации линейки Dallas Lock:

- СЗИ НСД Dallas Lock 8.0 редакций «К» и «С» (далее — DL8.0);
 - СЗИ НСД Dallas Lock Linux;
 - СЗИ ВИ Dallas Lock;
 - СДЗ Dallas Lock;
 - СДЗ УБ Dallas Lock;
 - WAF Dallas Lock.
- Удаленное управление рабочими станциями и серверами.
 - Удаленная настройка, а также сбор журналов и отчетов с рабочих станций и серверов при помощи Агента ЕЦУ.
 - Контроль целостности настроек сетевого оборудования (по SNMP/SSH) и сбор событий по Syslog.

Система имеет два способа сбора событий:

1. [Сбор событий из СУБД PostgreSQL](#)
2. [Сбор событий в формате CEF](#)

Сбор событий в формате CEF

Данное руководство описывает процесс настройки сбора и отправки событий Dallas Lock 8.0 Сервер безопасности в R-Vision SIEM.

Настройка Dallas Lock ЕЦУ

Для пересылки событий, зарегистрированных Dallas Lock ЕЦУ, в R-Vision SIEM в формате CEF выполните следующие действия:

1. Откройте консоль управления ЕЦУ.
2. Раскройте меню в левом верхнем углу и нажмите **Экспорт ИБ**.

Консоль управления ЕЦУ [Домен безопасности: secdom, Сервер: escu.dl01.local:17900]

Ввод/Вывод в подчинение

Параметры кластера ДБ

Подключение к Kaspersky Security Center

Экспорт ИБ

Настройка конфигурационных файлов

Установка ключа доступа

Принадлежность к домену Active Directory

Параметры...

Утилиты

Сохранить конфигурацию...

Применить конфигурацию...

О программе

Выход

7504

7495

7495

3

7492

7491

1

6

УДАЛЕННЫЕ ОБЪЕКТЫ

Сводка

Пользователи и группы

Информация об объекте

Серверы домена безопасности escu.dl01.local:17900

Родительский домен Нет



ПАРАМЕТРЫ

АРМ

Сетевые у

Подчинен

ПРОЦЕСС

Инциденты безопасности

За период: Сегодня

01.04.2025

☐ Только непрочитанные

5

--	--	--

3. В открывшемся меню установите флажок **Экспорт инцидентов безопасности в SIEM-систему**. Заполните поля:

- Формат: CEF.
- Сервер: IP-адрес коллектора.
- Протокол: протокол точки входа.
- Порт: порт точки входа.

Экспорт ИБ

✕

☒ Экспорт инцидентов безопасности в SIEM-систему

Формат: CEF

Сервер: 10.150.30.89

Протокол: TCP

Порт: 30147

Применить

Отмена

4. Нажмите на кнопку **Применить**

Настройка интеграции с R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие действия:

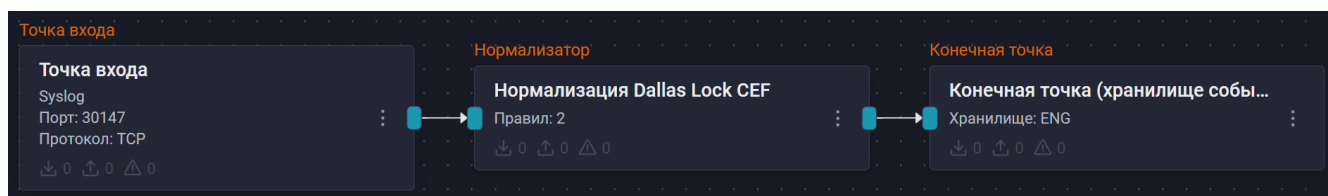
1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Syslog.
 - Порт точки входа и протокол: в соответствии с настройкой Dallas Lock ЕЦУ.
3. Добавьте на конвейер элемент **Нормализатор** с правилом "RV-N-135". Соедините нормализатор с точкой входа.



Правило "RV-N-135" также нормализует события, получаемые из Dallas Lock ЕЦУ в формате CEF.

4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
5. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



Если настройка выполнена корректно, в хранилище начнут поступать события от Dallas.



Найти события от Dallas в хранилище можно по следующему фильтру:

dvendor = Confident

Введите запрос и нажмите кнопку Поиск

1

—

+

минута

Поиск

×

Сбросить все

▼

dvendor = Confident

×

+

Добавить фильтр

Совпадений 21

Интервал времени: 2025-04-04T10:57:10.937+03:00 - 2025-04-04T10:58:10.937+03:00

Показать график ▼

Данные

Статистика

timestamp	dvendor	dproduct	name	dvc	msg	outcome
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Архивация журнала соединений МЭ		Архивация журнала соединений МЭ...	OK
2025-04-04T10:57:32.000+03:00	Confident	Dallas Lock	Срабатывание правила		Было зафиксировано срабатывание правила...	OK

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

Сбор событий из СУБД PostgreSQL

Данное руководство описывает процесс настройки сбора и отправки событий Dallas Lock 8.0 Сервер безопасности в R-Vision SIEM.

Предварительные требования

- Dallas Lock ЕЦУ хранит журналы на внешней СУБД.
- Сетевой доступ к БД Dallas Lock ЕЦУ.
- Учетная запись в СУБД с правами на чтение таблиц базы данных (сбор из БД).

Настройки СУБД PostgreSQL

Для настройки сбора логов из базы данных необходимо к ней подключиться. Чтобы подключиться к БД, используйте специально созданную сервисную учетную запись (далее — УЗ).

Создание учетной записи в СУБД PostgreSQL

Чтобы создать сервисную УЗ, подключитесь к СУБД с правами администратора. Для этого выполните следующие действия на сервере с установленной СУБД:

1. Выполните следующую команду из-под пользователя postgres:

```
sudo -u postgres psql
```

2. Создайте сервисную учетную запись, выполнив следующие команды:

```
CREATE USER "dl_reader";  
ALTER ROLE dl_reader WITH PASSWORD 'passw0rd';
```

3. Выдайте права на подключение к базе и чтение таблицы:

```
GRANT CONNECT ON DATABASE dallaslock to dl_reader;  
GRANT SELECT ON ALL TABLES IN SCHEMA public TO dl_reader;
```

Настройка в R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие действия:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
 - Тип точки входа: Database.
 - SQL-запрос:

```
SELECT record_id as record_id  
      ,timestamp as timestamp  
      ,timestamp_timezone as timezone  
      ,user as user  
      ,event_id as event_id  
      ,obj_name as obj  
      ,status as status  
      ,comment as comment  
      ,guid as guid  
      ,(SELECT vers_t.value FROM public.ucc_metainfo vers_t WHERE vers_t.key =  
'version') as version  
      ,'DL_PSQL' as filter  
      ,inet_server_addr() AS dvc  
FROM public.jrn_uccmainjournal  
WHERE record_id > CAST(? AS BIGINT)  
ORDER BY record_id ASC;
```

- База данных: PostgreSQL.
- Интервал запроса: 300 секунд.
- Поле идентификатора:
 - Ключ: record_id.
 - Значение: 1.
- Строка подключения в секрете:

```
jdbc:postgresql://DBSERVER:5432/DBNAME?user=dl_reader&password=passwd
```

Здесь:

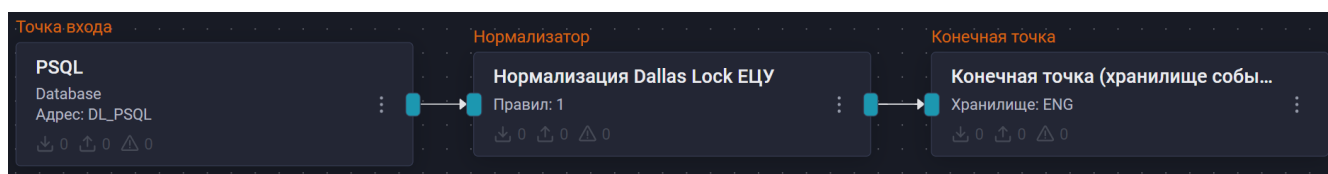
- **DBSERVER** — FQDN или IP-адрес сервера СУБД.
- **5432** — порт подключения



Создание секрета описано в разделе [Настройка секрета database в R-Vision SIEM](#).

3. Добавьте на конвейер элемент **Нормализатор** с правилом "RV-N-133". Соедините нормализатор с точкой входа.
4. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**. Соедините конечную точку с нормализатором.
5. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



Если настройка выполнена корректно, в хранилище начнут поступать события из PostgreSQL.



Найти события из PostgreSQL в хранилище можно по следующему фильтру:

```
dproduct = Единый центр управления
```

Настройка секрета database в R-Vision SIEM

Чтобы создать секрет подключения к СУБД:

1. В интерфейсе R-Vision SIEM перейдите в раздел **Ресурсы** → **Секреты**.
2. Нажмите на кнопку **Создать**.
3. В открывшемся окне заполните поля:
 - **Название** — введите название секрета.
 - **Описание** (опционально) — введите назначение секрета.
 - **Тип секрета** — выберите вариант **Строка подключения**.
 - **Строка подключения** — укажите данные для подключения к СУБД.
4. Нажмите на кнопку **Создать**.

Создание секрета

×

Название

Dallas Lock ЕЦУ (MSSQL)

Описание (опционально)

Секрет подключения к СУБД PostgreSQL Dallas Lock ЕЦУ

Тип секрета

Строка подключения

Строка подключения

jdbc:postgresql://DBSERVER:5432/DBNAME?
user=dl_reader&password=passw0rd

Отменить

Создать

Таблица маппинга

Таблица соответствия полей события для всех рассмотренных типов событий [представлена по ссылке](#).

С-Терра

Шлюз 4.3